Федеральное государственное автономное образовательное учреждение
высшего образования
«Московский государственный юридический университет имени О.Е. Кутафина
(МГЮА)»

На правах рукописи

Лагаева Валентина Петровна

Правовое регулирование применения искусственного интеллекта при осуществлении государственного контроля (надзора)

5.1.2 Публично-правовые (государственно-правовые) науки

ДИССЕРТАЦИЯ
на соискание ученой степени
кандидата юридических наук

Научный руководитель:
доктор юридических наук, доцент
Ефремов Алексей Александрович

Москва - 2026

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ ……..... 4

ГЛАВА 1. Применение технологий искусственного интеллекта как элемент системы информационного обеспечения государственного контроля (надзора)…19

§ 1.1. Информационное обеспечение государственного контроля (надзора) как функции государственного управления ……..……..……..19

§ 1.2. Роль информационных технологий в реализации профилактической функции государственного контроля (надзора)…….....43

§ 1.3. Виды управленческой информации государственного контроля (надзора) 51

§ 1.4. Система искусственного интеллекта и информационные системы государственного контроля (надзора).....60

ГЛАВА 2. Перспективная модель публично-правового регулирования отношений в сфере применения искусственного интеллекта при осуществлении государственного контроля (надзора) 70

§ 2.1. Российский опыт применения искусственного интеллекта в контрольно-надзорной деятельности государственных органов.....70

§ 2.2. Зарубежный опыт применения искусственного интеллекта в контрольно-надзорной деятельности государственных органов.....82

§ 2.3. Цели и принципы правового регулирования отношений по применению искусственного интеллекта при осуществлении государственного контроля (надзора).....97

ГЛАВА 3. Проблемы и приоритеты правового регулирования применения искусственного интеллекта при осуществлении государственного контроля (надзора).....106

§ 3.1. Проблема правосубъектности искусственного интеллекта 106

§ 3.2. Риски применения искусственного интеллекта при проведении контрольных (надзорных) мероприятий.....118

§ 3.3. Приоритетная роль систем искусственного интеллекта в реализации риск-ориентированного подхода государственного контроля (надзора).....125

§ 3.4. Роль искусственного интеллекта в обеспечении эффективности государственного контроля (надзора).....132
ЗАКЛЮЧЕНИЕ…….....137
СПИСОК СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ.....143
СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ 145

ВВЕДЕНИЕ

Актуальность темы диссертационного исследования. В современном мире информационные технологии оказывают непосредственное влияние на сферу государственного управления. Информационные технологии, в том числе методы искусственного интеллекта, активно внедряются в предоставление государственных и муниципальных услуг и исполнение государственных (муниципальных) функций, что способствует повышению качества и скорости обработки данных в государственных информационных системах, а также обеспечивает связанность обрабатываемых данных для обеспечения комфортных условий для граждан и организаций, при которых исключается необходимость предоставления одних и тех же сведений и документов в государственные и муниципальные органы и учреждения. Информационное взаимодействие государственных органов с гражданами и организациями осуществляется в том числе посредством чат-ботов (алгоритмов), предоставляющих сведения по наиболее актуальным вопросам.

К национальным целям развития Российской Федерации на период до 2030 года и на перспективу до 2036 года, утвержденным Указом Президента Российской Федерации от 7 мая 2024 года № 309, отнесена цифровая трансформация государственного управления, под которой рассматривается совокупность действий, направленных на исполнение государственных функций в электронном виде за счет использования ИТ-активов, на достижение цифровой зрелости, то есть автоматизации большей части транзакций в рамках единых отраслевых цифровых платформ и модели управления на основе данных с учетом ускоренного внедрения технологий обработки больших объемов данных, машинного обучения и искусственного интеллекта.

Использование искусственного интеллекта для осуществления такой функции государственного управления, как контрольно-надзорная деятельность, требует от юридической науки проведения правовой оценки общественных отношений, складывающихся под влиянием цифровых технологий, создает вызовы

как для государственно-правовых наук, так и для законодательства, сформированного преимущественно в индустриальную эпоху и нуждающегося в реформировании и цифровой трансформации.

В Российской Федерации разработан и реализуется национальный проект «Экономика данных и цифровая трансформация государства», в состав которого входит федеральный проект «Цифровое государственное управление», предусматривающий тотальную цифровизацию государственного управления с переходом на электронный документооборот в полном объеме в целях упрощения процессов и повышения эффективности деятельности государственных органов.

15 февраля 2024 года вступила в силу новая редакция Национальной стратегии развития искусственного интеллекта на период до 2030 года, в которой отмечается новый вызов для Российской Федерации, а именно низкий уровень внедрения технологий искусственного интеллекта (ИИ) в государственном управлении. К основным задачам развития ИИ в Российской Федерации отнесено создание комплексной системы нормативно-правового регулирования общественных отношений, связанных с развитием и использованием технологий ИИ, в том числе законодательное обеспечение возможности доступа разработчиков технологий искусственного интеллекта к различным видам данных, включая наборы государственных данных. В числе основных направлений внедрения доверенных технологий искусственного интеллекта в органах публичной власти указаны нормативно-правовое обеспечение такого внедрения и формирование правил получения наборов данных от коммерческих и некоммерческих организаций в целях повышения эффективности государственного управления.

Правотворческая деятельность в сфере регулирования ИИ ведется также в иностранных юрисдикциях. 01.08.2024 года вступили в силу отдельные положения Регламента Европейского союза об искусственном интеллекте - Регламент (ЕС) 2024/1689 Европейского парламента и Совета от 13 июня 2024 года.

Запрос общества на введение правового регулирования искусственного интеллекта подтверждается активным участием представителей рынка в формировании этических правил создания, внедрения и применения данной

технологии. В 2021 году компаниями Яндекс, Сбербанк, МТС, ВКонтакте, Газпром нефть, Ростелеком, Росатом, ЦИАН и др. был подписан Кодекс этики в сфере искусственного интеллекта, к которому присоединилось свыше 900 организаций, в том числе федеральные и региональные органы государственной власти (Роструд, Росреестр, Ространснадзор, Росздравнадзор, ФАС России, ФТС России, ФНС России и др.).

Многие вопросы, возникающие по поводу использования искусственного интеллекта в сфере государственного контроля (надзора), требуют правовой оценки не только с точки зрения действующего законодательства, но и с позиции достижения оптимального правового регулирования, которое бы отвечало интересам контролируемого лица, его клиентов и органов надзора - нормативная база в области искусственного интеллекта должна быть основана на системе научно-выверенных положений, отражающих юридическую сущность искусственного интеллекта и правовой режим его использования.

Степень научной разработанности темы диссертационного исследования.

Проблемы правового регулирования государственного контроля (надзора) являются предметом исследований юридической науки (А.Б. Агапов, В.П. Беляев, Л.Л. Попов, В.В. Ершов, С.М. Зубарев, С.М. Зырянов, В.Я. Кикоть, Б.В. Россинский, О.В. Романовская, Е.А. Соломатина, Ю.Н. Старилов, Ю.В. Степаненко, А.И. Стахов, А.В. Мартынов, Е.А. Дмитрикова и др.). Вместе с тем комплексного исследования проблемных правовых вопросов использования искусственного интеллекта и основанных на нем информационных технологий в сфере государственного контроля (надзора), муниципального контроля до настоящего времени не проводилось.

Научно-правовые исследования относительно искусственного интеллекта многочисленны, однако в основном они направлены на изучение основополагающих проблем (например, правосубъектность искусственного интеллекта) или сфокусированы на одной из сфер применения рассматриваемой

сквозной технологии (создание объектов интеллектуальной собственности (музыкальные произведения, картины и пр.), телемедицинские услуги и др.).

Научный интерес также представляют диссертационные исследования П.М. Морхата и А.А. Щитовой, посвященные теоретической разработке правовых проблем в области правового регулирования искусственного интеллекта.

Важно отметить научные работы по изучению возможности применения искусственного интеллекта в государственном управлении (М.Б. Добробаба, К.С. Евсиков, С.Е. Чаннов, Э.В. Талапина, А.А. Ефремов, С.С. Зенин, В.Н. Южаков, И.А. Черешнева и др.). При этом цифровая трансформация контрольно-надзорной деятельности на основе применения искусственного интеллекта пока изучена недостаточно (отдельные работы Мартынова А.В., Бундина М.В.) и нуждается в отдельном научном исследовании.

Объектом исследования являются общественные отношения, возникающие в связи с использованием искусственного интеллекта при осуществлении государственного контроля (надзора), включая применение искусственного интеллекта преимущественно в информационно-правовых отношениях по обработке данных в государственных информационных системах и в информационных системах контрольных (надзорных) органов, хотя отдельные вопросы представляют актуальность и для административно-правовых отношений, непосредственно связанных с информационным обеспечением государственного контроля (надзора), например, по проведению профилактических мероприятий (информирование, консультирование, профилактические визиты).

Предметом исследования являются нормы информационного и административного права; доктринальные позиции, посвященные правовому регулированию общественных отношений, возникающих в связи с использованием искусственного интеллекта, в том числе в государственном управлении; документы стратегического планирования; нормативные правовые акты Российской Федерации и иностранных государств; акты «мягкого» права; стандарты по направлению «Искусственный интеллект» и методические рекомендации по применению сервисов ИИ.

Цель исследования заключается в разработке и обосновании информационно-правовых и теоретических основ, концептуальных подходов правового регулирования отношений в сфере применения технологий искусственного интеллекта при осуществлении государственного контроля (надзора), регулируемого Федеральным законом от 31 июля 2020 года N 248-ФЗ "О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации".

Для достижения данной цели поставлены следующие **задачи исследования**:

1) определить понятие «информационное обеспечение государственного контроля (надзора)»;

2) раскрыть роль информационных технологий в реализации превентивной функции государственного контроля (надзора);

3) определить виды информации (данных), обработка которых в информационных системах государственного контроля (надзора) может осуществляться посредством технологий искусственного интеллекта;

4) изучить правовой режим обработки информации в информационных системах государственного контроля (надзора) с применением искусственного интеллекта;

5) исследовать вопрос правового регулирования отношений по применению искусственного интеллекта в контрольно-надзорной деятельности в Российской Федерации;

6) исследовать опыт регулирования применения искусственного интеллекта в контрольно-надзорной деятельности отдельных стран БРИКС, Евросоюза;

7) определить цели, принципы и механизм правового регулирования отношений по применению искусственного интеллекта в государственном контроле (надзоре);

8) определить возможность признания систем искусственного интеллекта субъектом права в правоотношениях в области государственного контроля (надзора);

9) определить, распространяются ли риски искусственного интеллекта на случаи применения данной информационной технологии при проведении контрольных (надзорных) мероприятий;

10) определить роль систем искусственного интеллекта в реализации риск-ориентированного подхода государственного контроля (надзора), в том числе при категорировании объектов контроля, формировании цифрового профиля контролируемого лица;

11) определить значение искусственного интеллекта в обеспечении эффективности государственного контроля (надзора).

Методология диссертационного исследования. Для решения поставленных задач были применены общенаучные методы познания (анализ и синтез, индукция и дедукция, абстрагирование, обобщение, моделирование), частнонаучные и специально-юридические методы познания. Так, технико-юридический метод использован при разработке авторского определения понятия «информационное обеспечение государственного контроля (надзора)». Формально-логический метод задействован при исследовании отдельных норм информационного и административного законодательства. Сравнительно-правовой метод преобладал при сопоставлении отечественного и зарубежного опыта правового регулирования искусственного интеллекта. На каждом этапе диссертационного исследования были использованы различные комбинации общенаучных и частнонаучных методов познания.

Теоретической основой диссертации послужили научные работы ряда отечественных исследователей в целях определения теоретических подходов в определении и регулировании ИИ как в общеправовом поле, так и в сфере информационного и административного права, а именно труды ученых - юристов: О.В. Александров, И.Л. Бачило, В.П. Беляев, Л.Ю. Василевская, М.Б. Добробаба, К.С. Евсиков, С.Е. Чаннов, К.В. Исакова, С.М. Зубарев, С.М. Зырянов, Л.Л. Попов, М.Я. Клепцов, Н.В. Крысанова, А.Г. Киселев, А.В. Мартынов, А.В. Минбалеев, П.М. Морхат, Н.А. Назаров, А.А. Ефремов, Д.А. Поспелов, И.В. Понкин, А.И.

Редькина, В.М. Сергеев, М.С. Студеникина, Э.В. Талапина, В.Н. Южаков, А.А. Щитова, О.А. Ястребов и другие авторы.

Нормативно-правовую основу диссертационного исследования составили Конституция Российской Федерации, федеральные законы Российской Федерации, указы и распоряжения Президента Российской Федерации, постановления и распоряжения Правительства Российской Федерации, правовые акты федеральных органов исполнительной власти России, органов государственной власти субъектов Российской Федерации, международные правовые акты, касающиеся вопросов регулирования ИИ, национальные и наднациональные документы стратегического планирования в отношении регулирования ИИ и реформирования контрольно-надзорной деятельности, программные документы, зарубежное законодательство, правовые позиции органов государственной власти, проекты нормативных правовых актов, акты официального толкования норм права.

Эмпирическую основу диссертационного исследования составляют сведения об опыте применения российскими и зарубежными государственными органами контроля (надзора) и контролируемыми лицами искусственного интеллекта и иных цифровых технологий. Источниками данной информации выступили судебные акты, научные работы, данные ОЭСР и иные источники органов власти России и иностранных государств, публикации в средствах массовой информации, а также данные из открытой библиотеки “AI Russia Works”, размещенной в сети Интернет на веб-сайте Альянса в сфере искусственного интеллекта.

Теоретическая значимость результатов исследования. Полученные результаты способствуют приращению правового знания о наиболее значимых аспектах применения искусственного интеллекта в сфере государственного управления в целом и государственного контроля (надзора) в частности, а также открывают простор для дальнейших научных исследований в данном направлении.

Практическая значимость результатов исследования. Результаты исследования могут быть учтены при актуализации Концепции совершенствования контрольной (надзорной) деятельности до 2026 года, утвержденной распоряжением

Правительства Российской Федерации от 21 декабря 2023 года № 3745-р, а также могут быть использованы при модернизации законодательства об информации, информационных технологиях и о защите информации, о государственном контроле (надзоре) и формировании законодательства об искусственном интеллекте. Некоторые выводы, сделанные в работе, могут оказаться полезными для определения комплексной системы правового регулирования общественных отношений, возникающих в связи с разработкой и применением искусственного интеллекта и робототехники. Отдельные положения возможно использовать в качестве учебного материала для обучения по правовым дисциплинам и в рамках повышения квалификации государственных гражданских служащих.

Научная новизна диссертационного исследования. Приведена и обоснована комплексная правовая характеристика наиболее значимых аспектов использования искусственного интеллекта в сфере государственного контроля (надзора):

- сформулированы определения понятий «искусственный интеллект» и «информационное обеспечение государственного контроля (надзора)»;

- определены правовые особенности использования искусственного интеллекта для обработки данных в информационных системах государственного контроля (надзора);

- вопросы развития и применения искусственного интеллекта проанализированы на предмет достижения оптимального баланса интересов контролируемых лиц и государства;

- исследованы дискриминационные риски, связанные с возможной предвзятостью (необъективностью) и непредсказуемостью решений, принятых системами искусственного интеллекта;

- определены правовые пределы применения технологий искусственного интеллекта при проведении государственного контроля (надзора);

- определены факторы, способствующие внедрению искусственного интеллекта в сферу государственного контроля (надзора);

- выявлены правовые проблемы обеспечения прозрачности применения искусственного интеллекта в контрольно-надзорной деятельности;

- установлены общие подходы и специфика определения понятия «искусственный интеллект», текущие подходы в области регулирования и стратегии развития искусственного интеллекта в Российской Федерации;

- выполнен и системно представлен сравнительно-правовой анализ опыта государств – участников БРИКС в области регулирования применения искусственного интеллекта в государственном управлении, а также Регламента Евросоюза «AI Act», вступившего в силу 1 августа 2024 года;

- определен подход по применению искусственного интеллекта в целях реализации профилактической функции государственного контроля (надзора);

- обоснована необходимость сохранения за инспекторами полномочий по принятию решений по результатам контрольных (надзорных) мероприятий на основе анализа и рекомендаций, предоставленных системами искусственного интеллекта;

- обоснована необходимость обработки информации системами искусственного интеллекта на принципах прозрачности и достаточности, совершенствования законодательства об информации в целях распределения ответственности между участниками отношений по внедрению искусственного интеллекта в сферу государственного контроля (надзора);

- разработана правовая модель интеграции искусственного интеллекта в сферу государственного контроля (надзора).

Научная новизна исследования находит отражение **в положениях, выносимых на защиту:**

1. Обосновано, что информационное обеспечение государственного контроля (надзора) представляет собой комплекс информационных ресурсов, баз данных, информационных систем, технических средств, информационных технологий и информационно-телекоммуникационной сети. В рамках информационного обеспечения государственного контроля (надзора) технологии и системы искусственного интеллекта предназначены осуществлять обработку массива

данных, аналитическое прогнозирование, распознавание лиц или объектов, выработку предварительного решения для одобрения и утверждения должностным лицом органа государственного контроля (надзора) в рамках их полномочий.

2. Обосновано приоритетное значение технологий искусственного интеллекта для обеспечения прогностической функции государственного контроля (надзора), который в рамках цифровой трансформации может быть преобразован в государственную систему профилактики нарушений обязательных требований. Для реализации данной функции технологии и системы искусственного интеллекта могут применяться в мероприятиях по предупреждению нарушений обязательных требований (информирование, консультирование, самообследование и др.). Превалирующий объем обработки данных государственного контроля (надзора) должен приходиться на цифровые сервисы самообследования, расчета категорий риска («калькулятор рисков»), разработки новых индикаторов риска.

3. Обоснована необходимость трансформации информационных систем государственного контроля (надзора) в интеллектуальные системы для обработки данных технологиями искусственного интеллекта для обеспечения связанности данных, выявления на основе анализа данных закономерностей деятельности контролируемых лиц, прогнозирования нарушений обязательных требований, организации контрольно-надзорной деятельности с учетом алгоритмов искусственного интеллекта.

4. Раскрыта текущая модель публично-правового регулирования применения искусственного интеллекта российскими контрольно-надзорными органами, которая характеризуется следующими признаками:

- приоритет человеко-ориентированного подхода в правовой регламентации отношений в сфере систем искусственного интеллекта;

- преимущественное применение документов стратегического планирования и мягкого права;

- фрагментарный характер регламентации, осуществляемой в основном на уровне ведомственных правовых актов органов государственного контроля (надзора).

5. Раскрыта текущая модель публично-правового регулирования применения искусственного интеллекта контрольно-надзорными органами иностранных государств, которая характеризуется следующими признаками:

- доминирование в национальных законодательствах человеко-ориентированного подхода в правовой регламентации отношений в сфере систем искусственного интеллекта;

- отсутствие прямого нормативно - правового регулирования общественных отношений по применению искусственного интеллекта в сфере государственного контроля (надзора).

6. Обоснована перспективная модель публично-правового регулирования применения технологий и систем искусственного интеллекта в государственном контроле (надзоре), включающая:

- цели обеспечения эффективности контрольно-надзорной деятельности, сокращения нагрузки на добросовестных контролируемых лиц, а также цифровизации указанной деятельности посредством технологий искусственного интеллекта;

- общие принципы применения искусственного интеллекта: человеко-ориентированный и гуманистический подход; уважение автономии и свободы воли человека; соответствие закону; недопустимость дискриминации по признакам расовой, национальной, половой принадлежности, политических взглядов, религиозных убеждений, возраста, социального и экономического статуса или сведений о частной жизни; оценка потенциальных рисков применения искусственного интеллекта; ответственное отношение участников отношений в сфере искусственного интеллекта к вопросам влияния искусственного интеллекта на общество и граждан; непричинение вреда жизни и (или) здоровью человека, имуществу граждан и юридических лиц, окружающей среде; информирование пользователей об их взаимодействии с технологиями искусственного интеллекта и обеспечение возможности прекращения такого взаимодействия по желанию пользователя; безопасность работы с данными; информационная безопасность;

- специальные принципы применения искусственного интеллекта в государственном контроле (надзоре): сочетание правового и технического регулирования, прозрачность применения искусственного интеллекта органами контроля (надзора), приоритет использования искусственного интеллекта в профилактической деятельности органов контроля (надзора), обеспечение возможности прекращения взаимодействия контролируемого лица с системой искусственного интеллекта по желанию такого лица, недискриминационный доступ к государственным данным для разработчиков систем искусственного интеллекта, ответственность органа контроля (надзора) за нарушение прав и законных интересов контролируемых лиц в результате применения искусственного интеллекта;

- мониторинг эффективности контрольно-надзорной деятельности по расширенному кругу сведений и документов вследствие применения технологий искусственного интеллекта в соответствии с нормативными правовыми актами, устанавливающими порядок проведения указанного мониторинга.

7. Обосновано, что отсутствует объективная необходимость в дополнении системы субъектов административного права новыми лицами: «электронное лицо», искусственный интеллект (роботы и системы искусственного интеллекта) в качестве квазисубъекта права. Субъектами контрольно-надзорного правоотношения являются контролируемые лица, инспектор (должностное лицо, действующее от имени государственного органа) и орган контроля (надзора), в то время как искусственный интеллект является средством, инструментом контроля. Решения, предложенные искусственным интеллектом, подлежат последующему одобрению должностным лицом государственного контроля (надзора).

8. Выявлены и систематизированы риски применения искусственного интеллекта при проведении контрольных (надзорных) мероприятий. Для сферы государственного контроля (надзора) особую опасность представляют модели так называемого сильного искусственного интеллекта, для которых свойственны полная автономность функционирования и принятие решения по непрозрачным и неизвестным алгоритмам. В этой связи применение таких систем искусственного

интеллекта при осуществлении государственного контроля (надзора) должно быть запрещено законом.

Правовым средством минимизации рисков искусственного интеллекта являются риск-ориентированный подход к выбору и применению искусственного интеллекта, доступ органов контроля (надзора) только к доверенным технологиям искусственного интеллекта.

9. Определены факторы, способствующие внедрению искусственного интеллекта в сферу государственного контроля (надзора):

- установленные законом система управления рисками и приоритет профилактических мероприятий по отношению к контрольным (надзорным) мероприятиям, что требует развития прогностической функции государственного контроля (надзора), обеспечивающей эффективное предупреждение неправомерного поведения контролируемых лиц, в том числе посредством определения модели их поведения, категорирования объектов контроля, установления точных и обоснованных индикаторов риска нарушений обязательных требований;

- обеспечение связанности и анализа данных, получаемых органами контроля (надзора) из предусмотренных законом источников и обрабатываемых в информационных системах государственного контроля (надзора) (сведения об объекте контроля, данные Единого реестра видов контроля и др.);

- применение технологий искусственного интеллекта контролируемыми лицами;

- нехватка квалифицированных кадров в органах государственного контроля (надзора).

Теоретическая значимость работы заключается в дальнейшем развитии теории информационного права, расширении и углублении теоретического знания о правовой природе и особенностях публично-правового регулирования отношений в сфере применения искусственного интеллекта при осуществлении государственного контроля (надзора). Выводы исследования обеспечат совершенствование понятийного аппарата в исследуемой сфере, а также позволят

определить правовую природу и место института правового регулирования применения искусственного интеллекта при осуществлении государственного контроля (надзора) в системе информационного права. Результаты исследования могут быть использованы для научных исследований в области информационного права в части решения вопросов, затрагивающих способы и средства правового регулирования применения искусственного интеллекта при осуществлении государственного контроля (надзора).

Степень достоверности и обоснованности результатов проведенного исследования. Сформулированные в диссертации выводы, предложения и решения научно обоснованы, корректны, аргументированы и оценены с учетом положений и результатов, достигнутых наукой информационного права. Выводы и рекомендации диссертации основаны на всестороннем согласованном теоретическом и прикладном исследовании доктринальных источников, нормативных правовых актов, правоприменительной практики, на широком использовании эмпирических данных.

Апробация результатов диссертационного исследования. Результаты диссертационного исследования использовались автором:

1) в семи опубликованных статьях, в том числе в трех научных статьях в ведущих рецензируемых научных журналах и изданиях;

2) при выступлении с докладами, материалами и тезисами на круглых столах, международных и всероссийских конференциях: IX летняя школа молодых ученых «Новый технологический уклад и право» (д. Малюшина дача, 2023 г.); Международная научно-практическая конференция «Информационный суверенитет Российской Федерации: проблемы правового обеспечения в условиях современных вызовов и угроз» (г. Москва, 2023 г.); Седьмая Международная научно-практическая конференция «Бачиловские чтения» (г. Москва, 2024 г.); VII Международная научно-практическая конференция «Актуальные проблемы информационного права» (г. Москва, 2024 г.); XI Московский международный юридический форум (г. Москва, 2024 г.); Научно-практический семинар «Цифровые платформы – новая среда взаимодействия» (г. Москва, 2024 г.); XIX

Международная Школа-практикум молодых ученых-юристов «Настоящее и будущее правового пространства БРИКС» (г. Казань, 2024 г.); Международный конгресс молодых ученых «Традиции и новации в системе современного российского права» (г. Москва, 2025 г.) и на других научных мероприятиях.

Соответствие диссертации паспорту специальности 5.1.2 – Публично-правовые (государственно-правовые) науки (юридические науки). Область исследований: 25. Публично-правовое регулирование в сфере информации и информационных (цифровых) технологий, архивного дела и защиты информации; 26. Правовое регулирование использования информационных (цифровых) технологий при осуществлении публичной власти и в публичном управлении.

Структура и объем диссертационного исследования. Диссертация состоит из введения, трех глав, включающих 11 параграфов, заключения, списка сокращений и условных обозначений, а также списка используемых источников и литературы.

ГЛАВА 1. Применение технологий искусственного интеллекта как элемент системы информационного обеспечения государственного контроля (надзора)

§ 1.1. Информационное обеспечение государственного контроля (надзора) как функции государственного управления

В целях всестороннего и полного исследования темы диссертационной работы необходимо прежде всего провести анализ информационного обеспечения государственного контроля (надзора), являющегося функцией (отдельным направлением) государственного управления, в целях определения роли и функций информационных технологий, в том числе технологии искусственного интеллекта, а также основанных на применении указанных технологий информационных систем.

Государственное управление в общем виде представляет собой «деятельность государства (государственных органов, должностных лиц) по обеспечению условий для жизни человека, развития его способностей и возможности достижения его человеческих целей, среди которых главное место занимают безопасность и благосостояние»[1]. Указанную деятельность осуществляет государство в целом, то есть все ветви власти (законодательные, исполнительные, судебные органы), публичные органы и организации, а также структуры местного самоуправления.

Государственное управление в узком смысле — это управление делами общества органами исполнительной власти посредством соответствующей формы исполнительно-распорядительной и контрольно-надзорной деятельности. Государственное управление в этом смысле носит четко выраженный организующий, координирующий и распорядительный характер. По мнению Э.В.

[1] *Андрюхина Э.П., Ахрем И.В., Бакурова Н.Н. и др.* Правовое обеспечение государственного управления и исполнительная власть: учебник для магистров / Под ред. С.А. Старостина. М.: Проспект, 2017. С. 21. См. также: *Тихомиров Ю.А.* Публичное право. М., 1995. С. 102; *Комаров К.Б.* Государственное управление: средства в экономической сфере: автореф. дис. ... канд. юрид. наук. Екатеринбург, 2000. С. 10.

Талапиной, Правительство Российской Федерации осуществляет исполнительную власть, то есть государственное управление в узком смысле слова[2].

В настоящем диссертационном исследовании понятие «государственное управление» рассматривается применительно к осуществлению контрольно-надзорных функций исполнительной власти в условиях цифровой трансформации государственного управления, заключающейся в переходе «на модель использования самых современных (прорывных) технологий в цифровой форме»[3].

Органы исполнительной власти, являющиеся субъектами государственного управления, выполняют различные функции, в том числе предоставление государственных (публичных) услуг и осуществление контроля и надзора.

Эффективность государственного управления в существенной степени определяется управленческим информационным воздействием, как исходящим от органов исполнительной власти (сведения о соответствующих управленческих решениях, в том числе правовых актах управления), так и полученными такими органами от объектов управления и в порядке межведомственного взаимодействия (механизм «обратной связи» в управлении).

Информационное обеспечение государственного управления определяется как целесообразная, повседневная деятельность органов власти и управления различных уровней и иных субъектов (например, подведомственных государственных организациях, участвующих в осуществлении такого обеспечения) с целью повышения эффективности реализуемых ими управляющих воздействий[4]. Основное назначение указанной деятельности заключается в удовлетворении информационных потребностей пользователей, направленных на осуществление деятельности органов власти и управления, соответственно,

---

[2] *Талапина Э.В.* Государственное управление: проблемы и перспективы правового регулирования // Законы России: опыт, анализ, практика. 2015. № 3. С. 96-101. См. также: *Попов Л.Л.* Ренессанс государственного управления в России. Избранное. М., 2019. С. 22.

[3] *Кузнецов П.У.* Цифровая трансформация государственного управления как этап развития информатизации в России // Вестник Южно-Уральского государственного университета. Серия: Право. 2021. Т. 21. № 1. С. 91. См. также: *Москвитина Н. В.* Цифровая трансформация государственного управления // Социология. 2021. № 4. С. 114 - 128.

[4] *Ковалева Н.Н.* Административно-правовое регулирование использования информационных технологий в государственном управлении: Автореф. дис. … д-ра юрид. наук. Саратов, 2014. С. 22.

информационное обеспечение государственного управления целесообразно представить как «совокупность развивающихся операционных систем»[5].

Как справедливо указывают А.А. Ефремов и Л.К. Терещенко, «современный этап развития государственного управления в России и зарубежных странах характеризуется активным внедрением цифровых технологий.... Цифровизация государственного управления позволяет повысить эффективность исполнения государственных функций как в результате внедрения гибких моделей управления, так и в результате принятия решений на основе актуальных, своевременных и достоверных данных»[6].

По мнению Э.В. Талапиной, к электронным способам размещения информации государственных органов подлежат применению следующие требования: «ценность и полезность информации, полнота и систематичность, непрерывность поступления и обработки информации, своевременность доведения и получения информации, оптимальный уровень размещения, распределения информации»[7].

На всех стадиях государственного управления (подготовка и принятие решения, в том числе планирование, организация исполнения и наделение компетенцией, непосредственное исполнение, мониторинг и контроль результата, коррекция принятых решений (планов))[8] осуществляется обработка информации, которая способствует принятию управленческого решения.

Постоянное информационное взаимодействие органов исполнительной власти (в том числе с гражданами, организациями, органами законодательной и судебной власти) можно характеризовать как необходимое условие стабильного развития государства, сохранения его суверенитета. В этой связи информационное обеспечение деятельности системы органов государственной власти, позволяющее осуществлять постоянный обмен сведениями, данными, документами,

---

[5] *Ковалева Н.Н.* Указ. соч. С. 24.

[6] Цифровая трансформация и государственное управление: научно-практическое пособие / А.С. Емельянов, А.А. Ефремов, А.В. Калмыкова [и др.]. М.: Инфотропик Медиа, 2022. С. 126.

[7] *Талапина Э.В.* Модернизация государственного управления в информационном обществе: информационно-правовое исследование: Дис. … д-ра юрид. наук. Москва. 2015. С. 226 – 227.

[8] *Южаков В.Н., Александров О.В., Талапина Э.В.* О системности правового регулирования государственного управления в Российской Федерации // Журнал российского права. 2015. № 7. С. 114 - 121.

своевременно их актуализировать и защищать, является важнейшим условием устойчивого и эффективного функционирования государственного механизма, реализации всех стадий процесса государственного управления во благо граждан и общества.

Элементами информационного обеспечения государственного управления являются информационный ресурс, поставщики и пользователи информации, системы обработки информации, программное обеспечение, технические устройства, информационно-телекоммуникационные сети.

Фундаментальной основой надлежащего и эффективного функционирования всей системы государственных органов являются принципы государственного управления[9]:

- конституционные (в том числе, законность, участие политических партий в управлении, демократизм государственного управления, федерализм);

- организационные (в частности, распределение и нормативное установление функций и полномочий, централизация и децентрализация государственного управления, отраслевое и межотраслевое управление).

Одним из конституционных принципов государственного управления является гласность, под которой понимается право каждого на ознакомление с документами и материалами, непосредственно затрагивающими их права и свободы (часть 2 статьи 24 Конституции РФ). Законом обеспечивается доступ граждан (физических лиц), организаций (юридических лиц), общественных объединений (далее – пользователи), к информации о деятельности государственных органов[10]. Организация доступа к вышеуказанной информации, размещаемой в сети Интернет, осуществляется посредством создания официальных сайтов государственных органов с указанием адресов электронной почты для обеспечения обратной связи с пользователями (направление запросов и

---

[9] *Братановский С.Н., Деменчук Д.В.* Обеспечение законности в государственном управлении. Учебное пособие. М., 2016. С. 22 - 26.

[10] Федеральный закон от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» // Собрание законодательства РФ. 2009. № 7. Ст. 776.

ответов на них). Федеральными законами может быть предусмотрено создание единого портала для размещения на нем нескольких официальных сайтов государственных органов.

Государственные органы обязаны размещать информацию также на своих официальных интернет-страницах и осуществлять взаимодействие с пользователями с использованием инфраструктуры, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме, предусмотренной Федеральным законом от 27 июля 2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», в порядке, установленном Правительством РФ.

Отметим необходимость для государственного управления получать и хранить сведения и документы с обеспечением возможности их оперативного и качественного поиска, что безусловно является стимулом использования передовых информационных технологий в государственных информационных системах и иных информационных системах государственных органов.

Понятие «информационное обеспечение государственного управления» не является однозначным, имеются различные подходы к его определению. И.Л. Бачило определяет рассматриваемое понятие как «совокупность информационного ресурса (ИР), информационных систем, коммуникаций и всех иных объектов информационной инфраструктуры»[11]. По ее мнению, государство в лице своих органов исполнительной власти должно «все знать», поскольку именно оно осуществляет регулирование всех сфер национальной экономики, несет ответственность за обеспечение национальной безопасности и выполняет внешние функции на международном уровне. Ученый отмечает важность установления правил сбора, предоставления и порядка использования информационного ресурса, утверждения стандартов и порядка применения указанных правил и порядка

[11] *Бачило И.Л.* Информационное обеспечение государственного регулирования в области экономики. Правовые проблемы // Информационное общество. 1999. № 2. С. 19.

предоставления официальной и правовой информации в организованном виде потребителю – участнику экономической деятельности.

И.Л. Бачило указаны следующие уровни интеграции и анализа информации в связи с управленческими задачи в области экономики:

- макроуправление (прогнозы, концепции, политика);

- тактическое управление (программы, кооперация и т.д.);

- оперативное управление (производство, обмен, потребление).

Рассмотренные выше взгляды И.Л. Бачило можно охарактеризовать как широкое понимание информационного обеспечения. Ряд авторов понимают рассматриваемое понятие в узком смысле, в частности, как совокупность информации об изучаемом объекте[12] либо баз данных, содержащих информацию, связанную с решением соответствующих функциональных задач[13]. Другие определяют его как совокупность следующих информационных элементов: показателей, документов, методов их обработки[14]. При этом Н.Г. Твердохлеб относит к информационному обеспечению помимо методов обработки информации также средства и формы организации информации[15]. К информационному обеспечению В.М. Жеребин относит информационные языки[16].

В понимании А.Г. Киселева информационное обеспечение – это «органически взаимосвязанная совокупность элементов (информация, информационные ресурсы, информационные языки), взаимодействие которых организовано и оформлено в единую информационную технологию, реализующую правила и методологические принципы эффективного преобразования сведений (фактов, цифр, оценок, мнений) в соответствии с потребностями управления»[17].

---

[12] *Титаренко Г.А., Федорова Г.С.* Введение в проблематику информационного обеспечения АСУ. М., 1975. С. 56.

[13] *Клепцов М.Я.* Информационные системы органов государственного управления. М., 1996. С. 28.

[14] *Синяк В.С., Агаджанян С.И.* Информационное обеспечение ОАСУ. М., 1976. С. 12.

[15] *Твердохлеб Н.Г.* Машинная обработка экономической информации промышленных предприятий и объединений. М., 1979. С. 59.

[16] *Жеребин В.М.* Информационное обеспечение АСУ. М., 1975. С. 43 – 44.

[17] *Киселев А. Г.* Информация и коммуникация в государственном управлении: Монография. М.: ИНФРА-М, 2019. С. 178 – 179.

Анализ вышеприведенных подходов приводит к выводу об общности понимания ученых необходимости в указании на информацию и данные как необходимых компонентов информационного обеспечения государственного управления.

В организации государственного контроля (надзора), регулируемого Федеральным законом от 31 июля 2020 года № 248-ФЗ, информационное обеспечение играет ключевую роль, подтверждением чего является то, что именно положения об информационных системах, межведомственном взаимодействии и документах, составляемых и используемых при осуществлении государственного контроля (надзора) в первую очередь предусмотрены в одноименном разделе указанного закона.

Исходя из того, что термин «обеспечение» предполагает создание возможности функционирования какого-либо процесса, то *информационное обеспечение государственного контроля (надзора)* представляет собой комплекс информационных ресурсов, баз данных, информационных систем, технических средств, информационных технологий и информационно-телекоммуникационной сети. Указанный комплекс создает возможность предупреждать и выявлять нарушения обязательных требований посредством использования информации и включает в себя следующие ключевые элементы:

- управленческая информация;

- информационный ресурс, в том числе документы и массивы документов, сайты в сети Интернет[18];

- системы обработки информации (информационные системы, базы данных);

- программное обеспечение, программные продукты (программы для ЭВМ), информационные технологии для обработки данных;

[18] ГОСТ Р 7.0.56-2017. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Международный стандартный сериальный номер (ISSN). Издательское оформление и использование / Утвержден и введен в действие приказом Росстандарта от 19 декабря 2017 г. № 2027-ст. М.: Стандартинформ, 2018.

- устройства, техническая инфраструктура (компьютерное и сетевое оборудование, центры обработки данных, маршрутизаторы и иное телекоммуникационное оборудование);

- средство защиты информации (техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации);

- субъекты (поставщики и получатели информации).

Рассмотрим подробнее вышеперечисленные элементы информационного обеспечения государственного контроля (надзора).

Эффективная деятельность органа контроля (надзора) нуждается в актуальной и достоверной информации, являющейся средством познания управляемых процессов, явлений. К **управленческой информации** следует отнести сведения о состоянии и свойствах управляемой системы (объекта управления), которые используются для оценки ситуации и разработки управленческих решений. Такая информация должна быть актуальной, достоверной, достаточной, непротиворечивой.

В зависимости от источника получения управленческая информация может быть внутренняя (в частности, полученная от подразделений контрольного (надзорного) органа, его сотрудников и технических устройств дистанционного контроля) и внешняя (в том числе, полученная от других государственных органов, от контролируемых лиц, объектов контроля, средств массовой информации и социальных сетей).

Управленческая информация может быть классифицирована по следующим критериям:

- по источнику: внутренняя и внешняя; официальная и неофициальная;

- по временной характеристике: информация о прошлом, текущем и будущем состоянии объекта контроля;

- по широте распространения: федеральная, региональная, местная;

- по назначению (так, отчетная информация необходима для аналитической работы органа контроля (надзора); оперативная - для применения профилактических мер или проведения контрольных (надзорных) мероприятий);

- по степени готовности для использования (первичная, промежуточная, итоговая);

- по полноте (частичная или комплексная информация);

- по степени надежности (достоверная и проверенная, подлежащая дополнительной проверке);

- по способам распространения (устная, письменная и комбинированная информация).

К **информационному ресурсу** относятся источники информации, в том числе выполненные в бумажном или электронном виде отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах[19]. К источникам управленческой информации можно отнести нормативные правовые акты, обращения граждан и организаций в контрольные (надзорные) органы, сайты в сети Интернет, личный кабинет контролируемого лица на Едином портале госуслуг (ЕПГУ) и других информационных системах государственного контроля (надзора).

Создаваемые и получаемые контрольным (надзорным) органом массивы управленческой информации нуждаются в систематизации, анализе, защите и хранении, что обеспечивается государственными и иными **информационными системами**, представляющими собой совокупность содержащихся в базах данных сведений (сообщений, данных) и обеспечивающих их обработку информационных технологий и технических средств[20].

---

[19] ГОСТ Р 43.0.2-2006. Национальный стандарт Российской Федерации. Информационное обеспечение техники и операторской деятельности. Термины и определения. / Утвержден и введен в действие приказом Ростехрегулирования от 9 ноября 2006 г. № 245-ст. М.: Стандартинформ. 2007.

[20] Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. 2006. № 31 (1 ч.). Ст. 3448.

Информационное обеспечение государственного контроля (надзора) включает в себя[21]:

- государственные информационные системы ("Типовое облачное решение по автоматизации контрольной (надзорной) деятельности" (ГИС ТОР КНД); Единый реестр видов федерального государственного контроля (надзора), регионального государственного контроля (надзора), муниципального контроля; Единый реестр контрольных (надзорных) мероприятий и другие);

- информационные системы контрольных (надзорных) органов;

- иные информационные системы, созданные в целях обеспечения организации и осуществления государственного контроля (надзора).

Программой для ЭВМ является представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения[22]. Благодаря программным средствам (software) аппаратная часть компьютерной системы выполняет свои функции.

В качестве примера программного продукта, применяемого в контрольной (надзорной) деятельности, можно указать на мобильное приложение "Инспектор", являющееся программным обеспечением, применяемым контрольными (надзорными) органами и контролируемыми лицами с использованием компьютерного устройства (мобильного телефона, смартфона или компьютера, включая планшетный компьютер)[23]. Указанное программное решение может быть использовано для проведения профилактического визита, инспекционного визита, выездной проверки, рейдового осмотра, досмотра, экспертизы и эксперимента.

---

[21] Федеральный закон от 31 июля 2020 г. № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» // Собрание законодательства РФ. 2020. № 31 (1 ч.). Ст. 5007.

[22] Гражданский кодекс Российской Федерации (часть четвертая) от 18 декабря 2006 г. № 230-ФЗ // Собрание законодательства РФ.2006. № 52 (1 ч.). Ст. 5496.

[23] Федеральный закон от 31 июля 2020 г. № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» // Собрание законодательства РФ. 2020. № 31 (1 ч.). Ст. 5007.

Сбор, накопление, обработка, хранение, представление и распространение информации обеспечивается **информационными технологиями (ИТ):** процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов[24].

Классификация ИТ возможна по различным критериям (назначение, пользовательский интерфейс, построение, способ управления и другие). В частности, по способу организации сетевого взаимодействия выделяют локальные, многоуровневые, распределенные. организации сетевого взаимодействия: локальные, многоуровневые, распределенные. По степени охвата задач выделяют следующие виды ИТ:

- информационные технологии обработки данных.
- информационные технологии автоматизации офисной деятельности.
- информационные технологии поддержки принятия решений.
- информационные технологии экспертных систем.

Разновидностью ИТ являются цифровые технологии, в том числе технология распределенного реестра, включая блокчейн, алгоритмы обработки больших данных, искусственный интеллект, облачные вычисления[25].

Для обеспечения обработки управленческой информации, использования программного обеспечения и применения цифровых технологий необходима **материальная инфраструктура**, включающая в себя центры обработки данных, ЭВМ, средства и линии связи, пользовательские устройства, средства защиты информации. Технические средства позволяют фиксировать, создавать, хранить и передавать данные[26], что создает возможности для функционирования информационных систем, цифровых технологий, облачных вычислений.

---

[24] Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. 2006. № 31 (1 ч.). Ст. 3448.

[25] LegalTech, FinTech, RegTech etc.: правовые аспекты использования цифровых технологий в коммерческой деятельности: коллективная монография. М., 2021. С. 25. См. также: *Зубарев С.М., Лебедева Е.А., Сабаева С.В., Сладкова А.В*. Цифровые технологии в системе государственного и общественного контроля: теоретико-правовые аспекты: Монография. М.: Проспект, 2022. С. 6 - 18.

[26] Согласно ГОСТ Р 52292-2004 «Информационная технология. Электронный обмен информацией. Термины и определения» данные – это интерпретируемое формализованным способом представление информации, пригодное для коммуникации, интерпретации или обработки.

Рассмотрим в качестве примера инфраструктуру, обеспечивающую информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме[27]. Указанная инфраструктура взаимодействия включает в себя инженерные и вспомогательные элементы в следующем составе:

- система обеспечения информационной безопасности;
- информационно-телекоммуникационные сети (ИТКС), обеспечивающие взаимодействие информационных систем, включая сеть передачи данных органов власти;
- сеть центров обработки данных, обеспечивающих функционирование инфраструктуры взаимодействия;
- государственная единая облачная платформа.

Центр обработки данных (ЦОД, дата-центр) - специализированный объект информатизации, представляющий собой связанную систему ИТ-инфраструктуры и инженерной инфраструктуры, оборудование и части которых размещены в здании или помещении, подключенном к внешним сетям, как инженерным, так и телекоммуникационным[28].

Согласно требованию закона **технические средства**, предназначенные для обработки информации, содержащейся в государственных информационных системах, в том числе программно-технические средства и средства защиты информации, должны соответствовать требованиям законодательства РФ о техническом регулировании. При этом законодательство РФ регулирует вопросы, связанные с разработкой и применением обязательных требований к продукции, а также с порядком оценки соответствия продукции таким требованиям.

---

[27] Постановление Правительства РФ от 8 июня 2011 г. № 451 «Об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме» // Собрание законодательства РФ. 2011. № 24. Ст. 3503.

[28] Приказ Минкомсвязи России от 30 апреля 2019 г. № 178 «Об утверждении методик расчета целевых показателей национальной программы "Цифровая экономика Российской Федерации» // СПС «КонсультантПлюс».

Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» установлено требование о размещении на территории Российской Федерации технических средств информационных систем, используемых государственными органами, органами местного самоуправления, государственными и муниципальными унитарными предприятиями или государственными и муниципальными учреждениями. Кроме того, операторы государственных информационных систем (ГИС) не должны допускать использования размещенных за пределами территории Российской Федерации баз данных и технических средств, не входящих в состав таких информационных систем.

Для обработки управленческой информации необходимо также использование **информационно-телекоммуникационной сети (ИТКС)**, под которой понимается технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники[29]. Без ИТКС было бы невозможно организовать взаимодействие государственного органа с гражданами и организациями, в том числе для оказания государственных услуг и проведения мероприятий государственного контроля (надзора).

В отношении государственных органов установлены требования по **защите информации**, обрабатываемой в электронной форме, применительно к

[29] Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. 2006. № 31 (1 ч.). Ст. 3448.

информационным системам[30] и взаимодействию в электронной форме, в том числе с гражданами (физическими лицами) и организациями[31].

К **средствам защиты информации** отнесены технические, криптографические, программные и другие средства, предназначенные для защиты сведений, средства, в которых они реализованы, а также средства контроля эффективности защиты информации[32]. Такие средства подлежат обязательной сертификации. При этом криптографические (шифровальные) средства должны быть отечественного производства и выполнены на основе криптографических алгоритмов, рекомендованных Федеральной службой безопасности РФ.

Информационное обеспечение государственного контроля (надзора) включает в себя лиц, осуществляющих работу с управленческой информацией и ответственных за ее надлежащую обработку. **Участники информационного взаимодействия**, осуществляемого в процессе функционирования информационных систем, цифровых платформ, определяются в нормативных правовых актах о функционировании таких систем. Так, применительно к ГИС «Единая централизованная цифровая платформа в социальной сфере» указаны в качестве поставщиков информации, в частности, Фонд пенсионного и социального страхования РФ, органы государственной власти (государственные органы), органы местного самоуправления и организации, предоставляющие меры социальной защиты (поддержки), федеральные учреждения медико-социальной экспертизы, органы опеки и попечительства, страхователи по обязательному пенсионному

---

[30] Постановление Правительства РФ от 6 июля 2015 г. № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации» // Собрание законодательства РФ. 2015. № 28. Ст. 4241; Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Собрание законодательства РФ. 2012. № 45. Ст. 6257; Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (Зарегистрировано в Минюсте России 31.05.2013 № 28608) // "Российская газета". № 136. 26.06.2013 г.; Приказ ФСБ России от 24 октября 2022 г. № 524 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств» (Зарегистрировано в Минюсте России 23.11.2022 № 71073) // Официальный интернет-портал правовой информации http://pravo.gov.ru, 23.11.2022.

[31] Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. 2006. № 31 (1 ч.). Ст. 3448.

[32] Постановление Правительства РФ от 26 июня 1995 г. № 608 «О сертификации средств защиты информации» // Собрание законодательства РФ. 1995. № 27. Ст. 2579.

страхованию и обязательному социальному страхованию[33]. Важно отметить, что поставщики информации могут быть привлечены к ответственности в соответствии с законодательством Российской Федерации за непредоставление сведений или за предоставление недостоверных сведений или документов.

Также нормативными правовыми актами определяются пользователи управленческой информации посредством регулирования отношений по доступу к указанной информации, содержащихся в ГИС и иных информационных системах государственного управления. Доступ может быть предоставлен посредством размещения сведений на официальном сайте соответствующей информационной системы для неопределенного круга лиц (открытая часть сайта) и для авторизованных пользователей (закрытая часть сайта).

Понятие «информационное обеспечение государственного контроля (надзора)» включает также следующие **информационные процессы**:

а) целенаправленный сбор, первичная обработка и распределение информационных потоков, анализ, оценка, закрепление и распространение информации;

б) организация свободного доступа заинтересованных субъектов к информационным ресурсам;

в) своевременное и достоверное получение информационных ресурсов для использования в управленческих целях;

г) защита управленческой информации.

Нормативные правовые акты, посредством которых в России осуществляется правовое регулирование информационного обеспечения государственного контроля (надзора), можно классифицировать по их функциональному содержанию, выделив следующие уровни:

- конституционно-правовой (основополагающий);

- стратегический;

---

[33] Федеральный закон от 10 июля 2023 г. № 293-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных законодательных актов (положений законодательных актов) Российской Федерации» // Официальный интернет-портал правовой информации http://pravo.gov.ru, 10.07.2023.

- текущий, на котором реализуются документы стратегического планирования.

Рассмотрим отдельно каждый уровень правового регулирования.

Конституция Российской Федерации (статьи 2, 15, 24, 29, 32, 33, 42, 55, 68, 71 и 103.1)[34] предусматривает следующие основополагающие положения применительно к информационному обеспечению государственного контроля (надзора). В частности, установлено, что законы подлежат официальному опубликованию, а неопубликованные законы не применяются. Органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Граждане Российской Федерации имеют право обращаться лично, а также направлять индивидуальные и коллективные обращения в государственные органы и органы местного самоуправления.

Нормативные правовые акты **стратегического уровня** правового регулирования информационного обеспечения государственного управления принимаются рамках целеполагания, прогнозирования, планирования и программирования как на федеральном уровне, так и на уровне субъектов Российской Федерации. К таким документам относятся ежегодное послание Президента Российской Федерации Федеральному Собранию Российской Федерации; стратегии развития и национальной безопасности Российской Федерации; доктрины и другие документы в сфере обеспечения национальной безопасности Российской Федерации; государственные программы Российской Федерации.

В **Послании Президента РФ Федеральному Собранию от 29.02.2024** определено развитие России в том числе по следующим направлениям:

[34] Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 года, с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 года) // Официальный интернет-портал правовой информации http://pravo.gov.ru, 06.10.2022.

- внедрение цифровых технологий в государственное управление, при этом Президентом России В.В. Путиным особо отмечено, что «всегда и по каждому из этих направлений нужно использовать искусственный интеллект - к этому стремиться»[35];

- переход в полном объеме с 1 января 2025 года на риск-ориентированный подход при проведении проверок бизнеса. Указано, что «там, где риски отсутствуют, надо применять профилактические меры и таким образом минимизировать число проверок.»[35]. Основываясь на указанном положении, можно утверждать, что информационные технологии должны быть в приоритетном порядке направлены на профилактику нарушений обязательных требований;

- создание цифровых платформ, важным элементом которых являются алгоритмы искусственного интеллекта. Президент России В.В. Путин указал на то, что «для государства такие технологии, интегральные платформы открывают огромные возможности для планирования и развития экономики отдельных отраслей, регионов и городов, для эффективного управления нашими программами и национальными проектами.»[35].

Указом Президента РФ от 7 мая 2024 г. № 309 определены **национальные цели развития Российской Федерации на период до 2030 года и на перспективу до 2036 года**[36], в числе которых предусмотрена цифровая трансформация государственного и муниципального управления, направленная на предоставление государственных (муниципальных) услуг и исполнение государственных (муниципальных) функций в электронном виде за счет использования ИТ-активов[37]. Определен курс государства на автоматизацию большей части транзакций в рамках единых отраслевых цифровых платформ и модели управления

[35] Послание Президента РФ Федеральному Собранию от 29 февраля 2024 г. // "Российская газета". № 46. 01.03.2024.

[36] Указ Президента РФ от 7 мая 2024 г. № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» // Официальный интернет-портал правовой информации http://pravo.gov.ru, 07.05.2024.

[37] Постановление Правительства РФ от 1 июля 2024 г. № 900 «О порядке учета ИТ-активов, используемых для осуществления деятельности по цифровой трансформации системы государственного (муниципального) управления» // Официальный интернет-портал правовой информации http://pravo.gov.ru, 01.07.2024.

на основе данных с учетом ускоренного внедрения технологий обработки больших объемов данных, машинного обучения и искусственного интеллекта.

Следующим документом стратегического планирования является **Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы**, утвержденная Указом Президента РФ от 9 мая 2017 г. № 203[38]. В ней предусматриваются в качестве основных принципов обеспечение прав граждан на доступ к информации; обеспечение законности и разумной достаточности при сборе, накоплении и распространении информации о гражданах и организациях; обеспечение государственной защиты интересов российских граждан в информационной сфере.

Указанная Стратегия определяет инфраструктуру электронного правительства как совокупность размещенных на территории Российской Федерации государственных информационных систем, программно-аппаратных средств и сетей связи, обеспечивающих при оказании услуг и осуществлении функций в электронной форме взаимодействие органов государственной власти Российской Федерации, органов местного самоуправления, граждан и юридических лиц.

К актам стратегического уровня правового регулирования информационного обеспечения государственного контроля (надзора) относятся в том числе:

- Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 5 декабря 2016 г. № 646[39];

- Стратегия развития отрасли информационных технологий в Российской Федерации на 2014 - 2020 годы и на перспективу до 2025 года, утвержденная распоряжением Правительства Российской Федерации от 1 ноября 2013 г. № 2036-р[40];

---

[38] Указ Президента РФ от 9 мая 2017 г. № 203 «Об утверждении Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы» // Собрание законодательства РФ. 2016. № 50. Ст. 7074.

[39] Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства РФ. 2017. № 20. Ст. 2901.

[40] Распоряжение Правительства РФ от 1 ноября 2013 г. № 2036-р // Собрание законодательства РФ. 2013. № 46. Ст. 5954.

- Государственная программа Российской Федерации "Информационное общество", утвержденная постановлением Правительства РФ от 15 апреля 2014 г. № 313[41], которая является главным программным документом, определяющим содержательные основы информатизации и внедрения информационно-коммуникационных технологий в систему государственного управления в целях повышения эффективности государственного управления и местного самоуправления, качества и оперативности предоставления государственных услуг;

- Национальная программа «Цифровая экономика Российской Федерации», включающая в себя федеральный проект «Цифровое государственное управление» (Паспорт Программы утвержден протоколом заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 4 июня 2019 г. № 7[42]);

- Национальная стратегия развития искусственного интеллекта на период до 2030 года[43].

К **текущему уровню правового регулирования** информационного обеспечения государственного контроля (надзора) относятся нормативные правовые акты, регулирующие отдельные общественные отношения в сфере обработки управленческой информации, информатизации государственных органов, создания и эксплуатации информационных систем, приобретения программ и средств информационной инфраструктуры. Это федеральные законы от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27 июля 2006 г. № 152-ФЗ «О персональных данных», от 09 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления», от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных

[41] Постановление Правительства РФ от 15 апреля 2014 г. № 313 «Об утверждении государственной программы Российской Федерации «Информационное общество» // Собрание законодательства РФ. 2014. № 18 (часть II). Ст. 2159.

[42] Паспорт федерального проекта «Цифровое государственное управление» (утв. президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности, протокол от 28.05.2019 № 9) // СПС «КонсультантПлюс».

[43] Указ Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» // Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 11.10.2019.

услуг», от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи», от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере товаров, работ, услуг для обеспечения государственных и муниципальных нужд», от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», от 31 июля 2020 г. № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» и другие федеральные законы.

Подзаконные акты рассматриваемого уровня правового регулирования[44] принимаются Президентом Российской Федерации, Правительством Российской Федерации, федеральными органами исполнительной власти и органами государственной власти субъектов Российской Федерации. Кроме того, отношения по межведомственному информационному взаимодействию регулируются также диспозитивным методом, а именно на основе соглашений, административных договоров.

К целям информационного обеспечения государственного контроля (надзора) можно отнести:

- получение качественной, обработанной информации на основе анализа исходных данных для принятия эффективных управленческих решений;

- актуализация и поддержание непрерывной связи государственных органов с внешней средой, способствование интеграции управления с другими системами;

- содействие координации управленческой деятельности по наиболее эффективному использованию кадров;

- повышение эффективности деятельности контрольных (надзорных) органов.

Для достижения указанных выше целей выполняются следующие *задачи* информационного обеспечения государственного контроля (надзора):

---

[44] См.: Указ Президента РФ от 22 мая 2015 г. № 260 «О некоторых вопросах информационной безопасности Российской Федерации» // Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 22.05.2015; Постановление Правительства РФ от 6 июля 2015 г. № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации» // Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 08.07.2015.

- сбор и аккумулирование первичной управленческой информации, а также ее распределение внутри системы государственного управления;

- подготовка к переработке и последующая переработка информации;

- предоставление государственному органу информации в переработанном, пригодном для использования виде и ее последующий анализ;

- обеспечение прямых и обратных связей ее передачи.

Допустимость различных уровней (федерального и регионального) правового регулирования процессов информатизации и цифровой трансформации государственного управления не должно препятствовать унификации информационного обеспечения государственного контроля (надзора). Федеральные информационные ресурсы (например, ГИС ТОР КНД) не могут функционировать в полном объеме в условиях наличия несовместимых между собой и с ГИС ТОР КНД информационных систем органов государственного контроля (надзора). В этой связи требуется регламентация на уровне федерального закона отношений по координации мероприятий по цифровизации государственного управления на федеральном и региональном уровнях, а также установление единого порядка планирования и реализации на указанных уровнях управления мероприятий по информатизации.

Относительно актуальности сведений, размещенных в информационных системах органов государственного управления, можно отметить отсутствие в законодательстве Российской Федерации отдельного регулирования отношений по проверке соблюдения операторами информационных систем и поставщиками информации требований закона о полноте, достоверности и актуальности данных, по внесению исправлений по инициативе оператора информационной системы или поставщика информации[45].

Также вследствие правовой неопределенности понятия «государственная информационная система» и отсутствия унифицированного законодательного акта по регулированию отношений по созданию, вводу в эксплуатацию, использованию

[45] *Назаров Н.А.* Обеспечение качества данных при автоматизированном принятии решений в государственном управлении // Журнал российского права. 2024. № 5. С. 140 - 155.

и развития информационных систем для нужд государственного управления, в настоящее время отмечается избыточное количество таких систем с дублирующими функциями, что крайне затратно для государственного бюджета. Вследствие такого разнообразия информационных ресурсов государственных органов может быть затруднено проведение единой политики по внедрению и применению цифровых технологий.

Учеными С.М. Зубаревым и С.В. Сабаевой отмечена активность органов государственной власти субъектов Российской Федерации по разработке и принятию базовых законов о государственных информационных системах (государственных информационных ресурсах), при этом разнообразие понятийно-категориального аппарата в законодательных актах регионов России вряд ли способствует определенности и унификаций понятий[46]. В этой связи важно разработать и принять федеральный закон о государственных информационных системах для обеспечения успешной реализации цифровой трансформации государственного управления и преодоления ведомственной разрозненности.

Следует согласиться с мнением С.М. Зубарева о необходимости «придания правовой формы цифровым технологиям посредством их регламентации как в базовых (статутных) законах (ФКЗ о правительстве, ФЗ об общих принципах организации и функционирования органов законодательной (представительной) и исполнительной власти субъектов РФ, ФЗ о системе государственной службы, и др.), так и в отраслевых законах, регулирующих отдельные направления деятельности органов исполнительной власти (стратегическое планирование, техническое регулирование, регистрация, лицензирование, контроль и надзор и т.д.).»[47].

Высказанные учеными – правоведами суждения о том, что выполнение информационными технологиями преимущественно информационной и

---

[46] *Зубарев С.М., Сабаева С.В.* Правовое регулирование цифровых технологий государственного контроля: опыт субъектов Российской Федерации // Российская юстиция. 2020. № 7. С. 17 – 21.

[47] *Зубарев С.М.* Правовые риски цифровизации государственного управления // Актуальные проблемы российского права. 2020. № 6. С. 23 – 32; См. также: *Зубарев С.М.* Цифровизация государственного управления: новая административная реформа? // Административное право и процесс. 2020. № 7. С. 17 - 21.

контрольно-учетной функции явно недостаточно для обеспечения сокращения коррупционных нарушений государственными служащими[48], в полной мере являются применимы и к контрольно-надзорной сфере[49].

Не предусматривается прогностическая функция обработки данных ГКН, а ведь цифровые технологии способны сформировать знания о будущих сценариях развития, о наиболее вероятных нарушениях обязательных требований определенной категорией контролируемых лиц.

В этой связи обратимся к технологиям ИИ.

Национальная стратегия развития ИИ[50] под «технологиями ИИ» рассматривает совокупность технологий, включающую в себя компьютерное зрение, обработку естественного языка, распознавание и синтез речи, интеллектуальную поддержку принятия решений и перспективные методы ИИ.

Потребность в переходе к более совершенному инструментарию обработки данных отмечена А.А. Косоруковым, по мнению которого «инструментарий искусственного интеллекта использует принципы и подходы, аналогичные человеческому интеллекту, позволяя в автоматическом режиме обрабатывать значительные объемы данных, что обеспечивает более оперативное и релевантное решение задач по управлению государством.»[51].

Можно согласиться и признать справедливой оценку О.А. Бояринцевой состава сведений в публичных базах данных как негармонизированного вследствие того, что государственные органы в первую очередь решали задачу перевода бумажных документов в цифровой вид[52].

---

[48] *Добробаба М.Б., Чаннов С.Е.* Применение цифровых технологий в целях противодействия совершения дисциплинарных коррупционных правонарушений в системе государственной службы // Информационное право. 2022. № 3 (73). С. 27.

[49] См. также: *Лагаева В.П.* Правовые основания применения технологий искусственного интеллекта в обработке данных государственного контроля (надзора) // Формирование многополярного мира: вызовы и перспективы: Сборник докладов XI Московского юридического форума. В 3 ч. Ч. 3 / редколлегия: С. М. Зубарев [и др.]. М.: Издательский центр Университета имени О.Е. Кутафина (МГЮА), 2024. С. 653 – 654.

[50] Указ Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» // Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 11.10.2019.

[51] *Косоруков А.А.* Технологии искусственного интеллекта в современном государственном управлении // Социодинамика. 2019. № 5. С. 45.

[52] *Бояринцева О. А.* Актуальные вопросы правового регулирования баз данных в условиях цифровой трансформации государственного управления // Аграрное и земельное право. 2020. № 7 (187). С. 122.

Важная роль цифровых технологий в информационном обеспечении государственного управления отмечена Президентом России В.В. Путиным: «За последние несколько лет нам удалось выстроить систему управления, а также реализации национальных проектов на новых принципах, на основе больших массивов данных, современных цифровых технологий, что позволило повысить эффективность работы, контролировать риски, учитывать весь объем информации, постоянно донастраивать проекты и программы, опираясь на обратную связь с гражданами.»[53].

В области государственного контроля (надзора) цифровые ИТ позволяют оперативно и эффективно обрабатывать массивы данных из различных источников, включая информационно-телекоммуникационную сеть Интернет[54].

Верно отмечено С.М. Зубаревым и А.В. Сладковой, что «цифровые технологии контроля в сфере государственного управления основываются на широком применении интернета, компьютеров, мобильных устройств, операционных систем и специальных программ, активном участии в информационном процессе пользователей, использовании режима реального времени при доступе пользователей к удаленным базам данных»[55].

Согласно Концепции совершенствования контрольно-надзорной деятельности до 2026 года в Российской Федерации уже сформирована единая модель данных в сфере контроля. Существенная экономия рабочего времени инспекторов достигается путем фокусирования их внимания только на случаи, выявленные интеллектуальной информационной системой (например, камеры с функцией распознавания лиц или объектов способствуют выявлению нарушений обязательных требований без необходимости проведения инспектором мониторинга лично).

---

[53] Послание Президента РФ Федеральному собранию // «Российская газета», № 46, 01.03.2024.

[54] См. также: *Лагаева В.П.* Правовые основания применения технологий искусственного интеллекта в обработке данных государственного контроля (надзора) // Формирование многополярного мира: вызовы и перспективы: Сборник докладов XI Московского юридического форума. В 3 ч. Ч. 3 / редколлегия: С. М. Зубарев [и др.]. М.: Издательский центр Университета имени О.Е. Кутафина (МГЮА), 2024. С. 654.

[55] *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.

Технология, функционирующая исключительно в соответствии с алгоритмами, не обладает субъективным восприятием и, как следствие, более устойчива к внешним влияниям, нежели человек, подверженный эмоциям и предубеждениям.

Применение голосовых помощников (чат-ботов) позволяет предоставить необходимую информацию по запросам пользователей в сжатые сроки, не отвлекая сотрудников контрольного (надзорного) органа на подготовку ответа на каждый поступивший запрос.

Представляется возможным сделать следующие промежуточные выводы в рамках настоящего параграфа диссертационного исследования.

Информационное обеспечение государственного контроля (надзора) – это комплекс ресурсов, методов, средств, процессов, создающий возможность предупреждать и выявлять нарушения обязательных требований посредством использования информации и включающий в себя следующие ключевые элементы: управленческая информация, информационный ресурс, системы обработки информации, программное обеспечение, информационные технологии, техническая инфраструктура, средства защиты информации и субъекты (поставщики и получатели информации).

Ключевую роль в информационном обеспечении государственного контроля (надзора) играют цифровые технологии, включая алгоритмы больших данных, блокчейн, искусственный интеллект.

§ 1.2. Роль информационных технологий в реализации профилактической функции государственного контроля (надзора)

В законодательстве РФ понятие «обязательные требования»[56] определяется как требования, содержащиеся в нормативных правовых актах и связанные с

[56] Федеральный закон от 31 июля 2020 г. № 247-ФЗ «Об обязательных требованиях в Российской Федерации» // Собрание законодательства РФ. 2020. № 31 (часть I). Ст. 5006. См. также: *Ермолова О.Н.* Обязательные требования к предпринимательской деятельности: вопросы контроля и ответственности // Имущественные отношения в Российской Федерации. 2022. № 5. С. 60-75.

осуществлением предпринимательской и иной экономической деятельности. Содержание рассматриваемых требований составляют условия, ограничения, запреты, обязанности.

Контроль как способ государственного публичного воздействия представляет собой установление обязанности органов государства и местного самоуправления наблюдать и в определенных законом случаях проверять соблюдение обязательных требований, а в предусмотренных законом случаях - принимать надлежащие меры. Государственный контроль и надзор представляют собой отдельную функцию государственного управления[57].

Государственный контроль (надзор) как самостоятельный вид публичного воздействия на граждан и организации предназначен для профилактики нарушений обязательных требований, для оценки соответствия деятельности контролируемых лиц обязательным требованиям и восстановления состояния, которое было до совершения указанных нарушений.

Административный надзор, по мнению А.В. Мартынова, представляет собой «активное наблюдение и проверку деятельности поднадзорного объекта для возможного управленческого воздействия с целью предотвращения угроз безопасности»[58]. Полное раскрытие рассматриваемого понятия осуществлено М.С. Студеникиной, которая определяет административный надзор как проверку установленных правил и норм, но не в масштабах всей деятельности поднадзорного лица, а лишь в части выполнения норм и правил[59].

В российской науке административного права административный надзор рассматривается как «особый вид государственной деятельности специально уполномоченных органов исполнительной власти и их должностных лиц, направленный на строгое и точное исполнение органами исполнительной власти, коммерческими и некоммерческими организациями, а также гражданами

---

[57] *Зубарев С.М.* Система контроля в сфере государственного управления: Монография. М.: Норма, ИНФРА-М, 2022. С. 12.

[58] *Мартынов А.В.* Проблемы правового регулирования административного надзора в России. Административно-процессуальное исследование. Монография. М.: NOTA BENE, 2010. С. 34.

[59] *Студеникина М. С.* Государственные инспекции в СССР. М., 1987. С. 25.

общеобязательных правил, имеющих важное значение для общества и государства.»[60]. По мнению С.М. Зубарева, «надзор имеет внешнюю направленность и призван обеспечить безопасность деятельности физических и юридических лиц в различных сферах общественных отношений»[61].

Государственные органы контроля (надзора) можно рассматривать в качестве органов административно-правового обеспечения безопасности, характерные признаки которых определены А.И. Стаховым[62].

Важно учитывать то обстоятельство, что цель административного надзора по обеспечению законности и безопасности достигается не только посредством наблюдения за действиями поднадзорных объектов и применения мер административного принуждения к ним в случае выявления должностным лицом нарушений обязательных требований, но и через деятельность органа надзора по профилактике нарушений обязательных требований[63].

Учеными – юристами подчеркивается предупредительный характер государственного контроля и надзора, который означает специализированную деятельность уполномоченных органов исполнительной власти по недопущению нарушения определенных норм и правил (обязательные требования), а равно по предотвращению неблагоприятных последствий, например, аварий на промышленных предприятиях, экологических катастроф и т.п.[64].

Важно отметить, что Закон № 248-ФЗ в качестве принципа государственного контроля (надзора) предусматривает **стимулирование добросовестного**

---

[60] Административное право: учебник / под ред. Л.Л. Попова, М.С. Студеникиной. 3-е изд., перераб. и доп. М.: Норма, ИНФРА-М, 2021. С. 316.

[61] *Зубарев С. М.* Система контроля в сфере государственного управления: Монография. М.: Норма, ИНФРА-М, 2022. С. 28.

[62] *Стахов А.И.* Административно-публичное обеспечение безопасности в Российской Федерации: Монография. М., 2015. С. 98 – 101; *Стахов А. И.* Нормативное регулирование и обеспечение безопасности в административно-правовой сфере: Монография. М.: Юрлитинформ, 2014. С. 129 – 140.

[63] См.: *Смирнова Е.Н.* Профилактика нарушений обязательных требований как важнейшее направление деятельности органов исполнительной власти, осуществляющих функции контроля и надзора // Административное право и процесс. 2018. № 4. С. 44 – 47; *Лагаева В. П.* Профилактика нарушений обязательных требований: понятие, цели и функции // Правовое обеспечение суверенитета России: проблемы и перспективы: сборник докладов XIII Московской юридической недели: в 4 ч. Ч. 4 / редколлегия: С. М. Зубарев [и др.]. – М.: Издательский центр Университета имени О.Е. Кутафина (МГЮА), 2024. – С. 108 - 112.

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

соблюдения обязательных требований, что обеспечивается приоритетным проведением профилактических мероприятий, а не проверок; нематериальным поощрением контролируемых лиц, соблюдающих обязательные требования; сокращением возможной выгоды от нарушений обязательных требований[65].

Законом № 248-ФЗ предусмотрены организация и проведение таких профилактических мероприятий, как информирование, обобщение правоприменительной практики, меры стимулирования добросовестности, объявление предостережения, консультирование, самообследование и профилактический визит Кроме того, закон устанавливает, что орган контроля (надзора) признает результаты независимой оценки соблюдения контролируемыми лицами обязательных требований, проводимой организациями, аккредитованными в национальной системе аккредитации в форме органа инспекции.

В целях профилактики нарушений обязательных требований обеспечиваются открытость и доступность информации об обязательных требованиях, являющихся предметом конкретного вида контроля (надзора), прозрачность процесса взаимодействия контрольных (надзорных) органов с гражданами и организациями, ограничение сфер для административного усмотрения[66]. В этом направлении информационные технологии играют ключевую роль.

Положительным является то обстоятельство, что Закон № 248-ФЗ не ограничивает форму информирования по вопросам соблюдения обязательных требований, что позволяет органам контроля (надзора) активно применять в том числе передовые цифровые решения. Нельзя не согласиться с С.М. Зубаревым и А.В. Сладковой в том, что «цифровые технологии контроля в сфере государственного управления основываются на широком применении интернета, компьютеров, мобильных устройств, операционных систем и специальных программ, активном участии в информационном процессе пользователей,

---

[65] *Фесько Д.С.* Административно-правовые гарантии обеспечения прав граждан и организаций при осуществлении государственного контроля (надзора): теория и практика: Монография / под науч. ред. В.В. Черникова. М.: Проспект, 2023. С. 47.

[66] *Фесько Д.С.* Административно-правовые гарантии обеспечения прав граждан и организаций .... С. 135.

использовании режима реального времени при доступе пользователей к удаленным базам данных»[67].

В целях обеспечения систематизации обязательных требований и информирования о них заинтересованных лиц Законом № 247-ФЗ предусмотрено создание федеральной государственной информационной системы «**Реестр обязательных требований»** (далее – Реестр ОТ), включающей в себя перечень и содержание обязательных требований, сведения о нормативных правовых актах об утверждении обязательных требований и сроке их действия, об ответственности за нарушение обязательных требований, а также информацию о разъяснительных документах.

Реестр ОТ обеспечивает систематизацию в электронной форме содержащихся в нормативных правовых актах обязательных требований[68]. Оператором Реестра ОТ является Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации, а уполномоченным органом, осуществляющим методическое обеспечение наполнения Реестра ОТ, - Министерство экономического развития Российской Федерации.

Достоверность сведений в Реестре ОТ обеспечивается применением при их размещении усиленной квалифицированной электронной подписи должностного лица заинтересованного федерального органа исполнительной власти, уполномоченной организации в должности не ниже заместителя руководителя.

Реестр ОТ интегрирован с другими информационными системами государственного контроля (надзора), в том числе с Единым реестром контрольных (надзорных) мероприятий, что обеспечивает унификацию для органов контроля (надзора) и контролируемых лиц источника сведений об обязательных требованиях.

Представляется, что применение алгоритмов искусственного интеллекта допустимо для выполнения таких функций Реестра ОТ, как:

---

[67] *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.

[68] Постановление Правительства РФ от 6 февраля 2021 г. № 128 «Об утверждении Правил формирования, ведения и актуализации реестра обязательных требований» // Собрание законодательства РФ. 2021. № 7. Ст. 1132.

формирование рекомендаций по выделению обязательных требований из текстов нормативных правовых актов, загруженных заинтересованными федеральными органами исполнительной власти, уполномоченными организациями;

анализ практики применения обязательных требований, в том числе выявление дублирования обязательных требований и оценка затрат на соблюдение обязательных требований;

обеспечение автоматического предзаполнения сведений (атрибутов) каждого обязательного требования.

Реестр ОТ можно рассматривать как начальный этап систематизации законодательства Российской Федерации в электронном виде, которая, как утверждает А.В. Минбалеев, «облегчает задачу выявления проблем в области качества нормативных правовых актов и повышает эффективность правоприменения.»[69].

Кроме того, в соответствии с частью второй статьи 46 Закона № 248-ФЗ контрольный (надзорный) орган обязан размещать и поддерживать в актуальном состоянии на своем официальном сайте в сети «Интернет» тексты нормативных правовых актов, регулирующих осуществление государственного контроля (надзора), муниципального контроля, а также перечень нормативных правовых актов с указанием структурных единиц этих актов, содержащих обязательные требования, оценка соблюдения которых является предметом контроля, а также информацию о мерах ответственности, применяемых при нарушении обязательных требований, с текстами в действующей редакции.

Нельзя не согласиться с мнением Т.А. Поляковой о том, что «опубликование правовых актов на официальных сайтах органов государственной власти (...) является важным, электронным источником правовой информации.»[70].

---

[69] *Минбалеев А. В.* Формирование экономики данных в России в условиях многополярного мира: проблемы правового обеспечения // Экономика и управление. 2023. Т. 29. № 8. С. 959.

[70] *Полякова Т.А.* Влияние цифровой трансформации на развитие информационного права: тенденции, проблемы, перспективы // Мониторинг правоприменения. 2020. № 2 (35). С. 55.

Информирование контролируемых лиц и иных заинтересованных лиц по вопросам соблюдения обязательных требований осуществляется также посредством применения органом контроля (надзора) голосовых помощников, чат-ботов на официальных сайтах и страницах в социальных сетях, в мессенджерах, благодаря чему необходимые сведения можно получить незамедлительно, без ожидания, когда освободится инспектор. Верно отмечено С.И. Коневым, что применение ИИ расширяет возможности органа контроля (надзора) по информированию, объявлению предостережения, выдаче рекомендаций по соблюдению обязательных требований и консультированию[71].

При этом консультирование, разъяснения решений органов государственной и муниципальной власти, их должностных лиц рассматриваются учеными – юристами как виды убеждения, являющегося основным методом государственного управления, равно как и принуждение[72].

Обобщение правоприменительной практики, являющееся одним из профилактических мероприятий, проводится на основе анализа массива данных о выявленных нарушениях обязательных требований, поэтому технологии больших данных являются востребованным инструментом для контрольных (надзорных) органов. В случае цифровизации рассматриваемого мероприятия повышается точность выявления типичных нарушений обязательных требований, причин, факторов и условий, способствующих возникновению указанных нарушений.

Закон обязывает орган контроля (надзора) вести учет объявленных им предостережений о недопустимости нарушения обязательных требований (еще один вид профилактического мероприятия), который эффективно осуществлять с применением электронных документов для автоматизированной обработки информации.

В целях предупреждения нарушений обязательных требований проводится консультирование по обращениям контролируемых лиц и их представителей.

---

[71] *Конев С. И.* Контроль и надзор за соблюдением законодательства в области данных о личности в условиях роботизации // Государственная служба и кадры. 2020. № 3. С. 214 – 215.

[72] *Хатуаев В.У.* Об убеждении как основном общем методе реализации государственной власти: состояние и некоторые проблемы совершенствования // Административное право и процесс. 2022. № 1. С. 7 – 10.

Важно отметить, что обязанность давать разъяснения возложена законом на должностное лицо, а не орган контроля (надзора), из чего можно сделать вывод, что консультация осуществляется только с участием инспектора, без его замены на голосового помощника или чат-бота. При этом допускается применение дистанционных способов взаимодействия (видео-конференц-связь).

Такое профилактическое мероприятие, как самостоятельная оценка соблюдения обязательных требований (самообследование), проводится в автоматизированном режиме с использованием одного из способов, указанных на официальном сайте контрольного (надзорного) органа в сети "Интернет". Так, на официальном сайте Росреестра в разделе "Деятельность - Государственный надзор - Государственный земельный надзор" в подразделе "Самостоятельная оценка соблюдения обязательных требований" реализован сервис для самостоятельной оценки соблюдения обязательных требований, предназначенный для правообладателей земельных участков и землепользователей[73].

Закон № 248-ФЗ устанавливает, что контролируемое лицо должно иметь возможность осуществить самообследование без идентификации пользователя, что является гарантией обеспечения конфиденциальности самообследования для третьих лиц.

Возможность применения информационных технологий при проведении профилактического визита[74] предусмотрена законом путем указания на использование видео-конференц-связи или мобильного приложения «Инспектор», на подачу посредством единого портала государственных и муниципальных услуг или регионального портала государственных и муниципальных услуг контролируемым лицом заявления о проведении указанного мероприятия.

На основании вышеизложенного можно сделать вывод о том, что установленный законом приоритет профилактических мероприятий над

---

[73] Письмо Росреестра от 29 января 2024 г. № 16-0616-МС/24 «О направлении информации» // СПС «КонсультантПлюс».

[74] *Лагаева В. П.* О профилактическом визите как новом мероприятии профилактики нарушений обязательных требований индивидуальными предпринимателями и юридическими лицами // Административное право и процесс. 2023. № 6. С. 69 - 71.

контрольными (надзорными) мероприятиями является правовым основанием для использования цифровых интеллектуальных технологий в первую очередь в целях предупреждения нарушений обязательных требований.

Такой подход означает, что в приоритетном порядке по отношению к фискальным целям должны внедряться информационные технологии, обеспечивающие проведение контрольными (надзорными) органами превентивных мероприятий (информирование, консультирование, обобщение правоприменительной практики, самообследование и др.), применение в полном объеме риск-ориентированного подхода к объектам контроля.

§ 1.3. Виды управленческой информации государственного контроля (надзора)

В первом параграфе настоящей главы рассмотрены общие характеристики управленческой информации, являющейся ключевым элементом информационного обеспечения государственного контроля (надзора). Рассмотрим подробно виды информации, обрабатываемой контрольными (надзорными) органами, с целью последующего определения возможности применения технологий искусственного интеллекта, в том числе для анализа данных.

При осуществлении государственного контроля (надзора) в России используются следующие виды информации:

1) информация, содержащаяся в документах, принимаемых контрольным (надзорным) органом:

- проверочный лист (списки контрольных вопросов, ответы на которые свидетельствуют о соблюдении или несоблюдении контролируемым лицом обязательных требований);

- руководство по соблюдению обязательных требований;

- решения об отнесении объекта контроля к одной из категорий риска, об изменении категории риска объекта контроля;

- мотивированное представление о проведении контрольного (надзорного) мероприятия;

- решение о проведении контрольных (надзорных) мероприятий;

- акты контрольных (надзорных) мероприятий;

- решение об объявлении предостережения о недопустимости нарушения обязательных требований;

- предостережение о недопустимости нарушения обязательных требований;

- решение и уведомление о проведении профилактического визита (обязательного профилактического визита);

- акт профилактического визита;

- решение об отказе в проведении профилактического визита;

- предписание об устранении выявленных нарушений;

- акты по фактам непредставления или несвоевременного представления контролируемым лицом документов и материалов, запрошенных при проведении контрольных (надзорных) мероприятий, невозможности провести опрос должностных лиц и (или) работников контролируемого лица, ограничения доступа в помещения, воспрепятствования иным мерам по осуществлению контрольного (надзорного) мероприятия;

- рекомендации по обеспечению безопасности и предотвращению нарушений обязательных требований, по соблюдению обязательных требований;

- доклад о виде контроля с указанием сведений о достижении ключевых показателей и сведений об индикативных показателях видов контроля, в том числе о влиянии профилактических мероприятий и контрольных (надзорных) мероприятий на достижение ключевых показателей;

- решение о приостановлении или об отказе в приостановлении исполнения обжалуемого решения контрольного (надзорного) органа;

- решения по итогам рассмотрения жалобы контролируемого лица;

- программа профилактики рисков причинения вреда;

- доклад о правоприменительной практике;

- ежегодный доклад контрольного (надзорного) органа о состоянии государственного контроля (надзора);

- журналы учета консультирования, объявленных предостережений, профилактических визитов, контрольных (надзорных) мероприятий, проводимых без взаимодействия с контролируемым лицом;

- методические рекомендации по проведению контролируемым лицом самообследования и подготовке им декларации соблюдения обязательных требований;

- задание на проведение контрольного (надзорного) мероприятия без взаимодействия с контролируемым лицом;

- ежегодный план контрольных (надзорных) мероприятий;

- акт о невозможности проведения контрольного (надзорного) мероприятия, предусматривающего взаимодействие с контролируемым лицом;

- протокол о проведении мониторинговой закупки и направлении продукции (товаров), результатов выполненных работ, оказанных услуг на инструментальное обследование, испытание или экспертизу;

- протоколы осмотра, досмотра, опроса, отбора проб (образцов), инструментального обследования или испытания;

- требование о представлении необходимых и (или) имеющих значение для проведения оценки соблюдения контролируемым лицом обязательных требований документов и (или) их копий, в том числе материалов фотосъемки, аудио- и видеозаписи, информационных баз, банков данных, а также носителей информации;

- акт контрольного (надзорного) мероприятия;

- решение об отсрочке исполнения решения контрольного (надзорного) органа;

- решения о разъяснении способа и порядка исполнения решения контрольного (надзорного) органа, об отсрочке, о приостановлении, возобновлении или прекращении исполнения решения;

- решение о прекращении осуществления мониторинга (режим дистанционного государственного контроля (надзора);

- иные документы.

2) информация, содержащаяся в документах, исходящих от контролируемых лиц:

- жалоба, обращение, запрос, ходатайство;

- заявление об изменении категории риска деятельности или объекта контроля, о проведении профилактического визита, о прекращении осуществления мониторинга (режим дистанционного государственного контроля (надзора);

- письменные объяснения по фактам нарушений обязательных требований, выявленных при проведении контрольных (надзорных) мероприятий;

- возражения в отношении предостережения о недопустимости нарушения обязательных требований;

- отказ от проведения профилактического визита;

- декларация соблюдения обязательных требований;

- уведомление о начале осуществления отдельных видов деятельности; об отзыве заявления о проведении профилактического визита;

- иные документы.

3) информация, содержащаяся в документах, поступающих в орган контроля (надзора):

- разъяснения Минэкономразвития России по вопросам применения Закона № 248-ФЗ;

- документы, предоставленные иными государственными органами, органами местного самоуправления либо организациями, подведомственными государственным органам или органам местного самоуправления;

- заключение эксперта, экспертной организации, специалиста;

- заключение о подтверждении соблюдения обязательных требований;

- поручение Президента Российской Федерации, поручение Правительства Российской Федерации, высшего должностного лица субъекта Российской Федерации о проведении обязательного профилактического визита или контрольных (надзорных) мероприятий;

- требование прокурора о проведении контрольного (надзорного) мероприятия в рамках контроля (надзора) за исполнением законов, соблюдением

прав и свобод человека и гражданина по поступившим в органы прокуратуры материалам и обращениям;

- решение прокурора о согласовании проведения внепланового контрольного (надзорного) мероприятия или об отказе в согласовании его проведения;

- обращение (заявление) граждан в связи с защитой (восстановлением) своих нарушенных прав;

- обращение (заявление) от работников контролируемого лица о массовых (более 10 процентов среднесписочной численности или более 10 человек) нарушениях работодателями их трудовых прав, связанных с полной или частичной невыплатой заработной платы свыше одного месяца;

- иные документы.

Также законодательством РФ предусмотрена обработка органом контроля (надзора) **следующей информации (сведений)**:

- сведения, ставшие известными в ходе проведения контрольных (надзорных) мероприятий;

- про имущественное и финансовое положение контролируемого лица;

- сведения для учета объектов контроля и установления их принадлежности контролируемому лицу;

- сведения о соглашениях о надлежащем устранении выявленных нарушений обязательных требований;

- материалы, прикладываемые к ходатайству, заявлению, жалобе контролируемого лица, в том числе фото- и видеоматериалы;

- сведения, используемые для оценки и управления рисками причинения вреда (ущерба);

- сведения о реализации контролируемым лицом мероприятий по снижению риска причинения вреда (ущерба) и предотвращению вреда (ущерба) охраняемым законом ценностям; о наличии внедренных сертифицированных систем внутреннего контроля в соответствующей сфере деятельности;

- информация об обязательных требованиях, предъявляемых к деятельности контролируемого лица 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;

- сведения о причинении вреда (ущерба) или об угрозе причинения вреда (ущерба) охраняемым законом ценностям;

- данные и результаты инструментального обследования, испытания или экспертизы;

- данные, полученные с использованием работающих в автоматическом режиме технических средств фиксации правонарушений, имеющих функции фото- и киносъемки, видеозаписи;

- письменные свидетельства, имеющие значение для проведения оценки соблюдения контролируемым лицом обязательных требований, от контролируемого лица или его представителя, свидетелей, располагающих такими сведениями;

- сведения о распространении (предоставлении) баз данных (их части) с персональными данными в сети Интернет;

- иные сведения.

Важно отметить, что в настоящее время подавляющее большинство из указанных выше документов, принимаемых органом контроля (надзора), унифицированы только в пределах конкретного вида федерального или регионального государственного контроля (надзора). Так, форма предписания об устранении выявленного нарушения требований земельного законодательства Российской Федерации, утвержденная Россельхознадзором[75], отличается от формы предписания об устранении выявленных нарушений, утвержденной МЧС России[76].

[75] Приказ Россельхознадзора от 5 февраля 2024 г. № 132 «Об утверждении форм документов, используемых при осуществлении Федеральной службой по ветеринарному и фитосанитарному надзору и ее территориальными органами федерального государственного земельного контроля (надзора) на землях сельскохозяйственного назначения, оборот которых регулируется Федеральным законом «Об обороте земель сельскохозяйственного назначения», виноградопригодных земель» (Зарегистрировано в Минюсте России 16.05.2024 № 78167) // Официальный интернет-портал правовой информации http://pravo.gov.ru, 16.05.2024.

[76] Приказ МЧС России от 20.12.2021 № 889 «Об утверждении форм документов, используемых при осуществлении федерального государственного контроля (надзора) за безопасностью людей на водных объектах»

Минэкономразвития России, являющееся уполномоченным органом по осуществлению функции по выработке государственной политики и нормативно-правовому регулированию в области государственного контроля (надзора) и муниципального контроля, утвердило типовые формы для ограниченного числа документов, в том числе для:

- решений о проведении контрольных (надзорных) мероприятий: контрольная закупка, мониторинговая закупка, выборочный контроль, инспекционный визит, рейдовый осмотр, документарная проверка, выездная проверка;

- актов контрольных (надзорных) мероприятий: контрольная закупка, мониторинговая закупка, выборочный контроль, инспекционный визит, рейдовый осмотр, документарная проверка, выездная проверка;

- предостережений о недопустимости нарушения обязательных требований.

Отметим, что небольшой объем унифицированных документов в контрольно-надзорной сфере может осложнить интеграцию информационных систем и использование методов искусственного интеллекта для предиктивного анализа данных.

Несомненным достоинством Закона № 248-ФЗ является его стратегическая направленность на электронную коммуникацию как между государственными органами, так и между органом контроля (надзора) и контролируемыми лицами. В частности, документы, создаваемые контрольным (надзорным) органом в процессе государственного или муниципального контроля, а также специалистами и экспертами, привлекаемыми для проведения контрольных мероприятий, оформляются в виде электронных документов и подписываются усиленной квалифицированной электронной подписью.

Кроме того, сведения о совершаемых должностными лицами контрольного (надзорного) органа и иными уполномоченными лицами действиях и принимаемых решениях подлежат размещению в едином реестре контрольных (надзорных)

(Зарегистрировано в Минюсте России 20.04.2022 № 68275) // Официальный интернет-портал правовой информации http://pravo.gov.ru, 20.04.2022.

мероприятий и в обязательном порядке доводятся до сведения контролируемых лиц посредством инфраструктуры, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме, в том числе через ЕПГУ и (или) через региональный портал государственных и муниципальных услуг.

Контролируемые лица вправе подать жалобу на действия или решения органа контроля (надзора) исключительно в электронном виде через ЕПГУ и (или) региональные порталы государственных и муниципальных услуг. Электронная форма предусмотрена и в отношении материалов, прикладываемых контролируемыми лицами к ходатайству, заявлению, жалобе, в том числе фото- и видеоматериалов.

Предусмотренное законом требование о ведении электронного документооборота соответствует стратегическому направлению развития Российской Федерации в сторону цифровой трансформации государственного управления, поскольку информация в электронной форме может быть сгруппирована по определённым признакам в виде структурированного массива данных (набора данных, датасет), необходимых для разработки программ для ЭВМ на основе ИИ.

Закон № 248-ФЗ устанавливает *требования, запреты и ограничения* в отношении обработки информации и принятии документов органами контроля (надзора), в том числе следующие условия:

- решения должностных лиц ГКН должны быть объективными и подтверждаться фактическими данными и документами, содержащими достоверную информацию;

- запрещаются решения, унижающие достоинство личности либо умаляющие деловую репутацию организации, индивидуального предпринимателя;

- информация, составляющая коммерческую, служебную или иную охраняемую законом тайну и полученная должностными лицами контрольного (надзорного) органа при осуществлении государственного контроля (надзора),

муниципального контроля, не подлежит разглашению, за исключением случаев, установленных федеральными законами. За разглашение информации, составляющей коммерческую, служебную или иную охраняемую законом тайну, должностные лица контрольного (надзорного) органа несут ответственность, предусмотренную федеральными законами;

- не требовать от контролируемых лиц документы и иные сведения, представление которых не предусмотрено законодательством Российской Федерации либо которые находятся в распоряжении государственных органов и органов местного самоуправления.

Информация, содержащаяся в информационных ресурсах органов ГКН и иных уполномоченных лиц, относится к государственным данным, на основе которых происходит в том числе обучение моделей ИИ. В этой связи установленные законом требования к информации позволяют обеспечить достоверность исходных данных, их непредвзятость, что в свою очередь является залогом создания и применения безопасных (доверенных) технологий ИИ, в том числе для производства машинной правовой аналитики[77].

Объем информации и данных, на основе использования которых осуществляется государственный контроль (надзор), имеет тенденцию к росту вследствие совершенствования Закона № 248-ФЗ. Так, с 28 декабря 2024 года[78] дополнился перечень документов, принимаемых органами контроля (надзора), мотивированным представлением о проведении контрольного (надзорного) мероприятия в случае, если выявлено соответствие объекта контроля параметрам, утвержденным индикаторами риска нарушения обязательных требований, или отклонение объекта контроля от таких параметров. Также предусмотрены поручения Президента Российской Федерации, Правительства Российской Федерации, высшего органа исполнительной власти субъекта Российской

[77] *Понкин И.В.* Машинная правовая аналитика: понятие, онтология и значение для правовой деятельности // Государственная служба. 2022. Т. 24. № 6. С. 40 – 46.

[78] Федеральный закон от 28 декабря 2024 г. № 540-ФЗ «О внесении изменений в Федеральный закон «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» // Официальный интернет-портал правовой информации http://pravo.gov.ru, 28.12.2024.

Федерации о проведении обязательного профилактического визита, от которого контролируемое лицо не вправе отказаться. Расширен перечень сведений, включаемых в Единый реестр контрольных (надзорных) мероприятий, предписаниями, выданными по итогам контрольного (надзорного) мероприятия без взаимодействия с контролируемым лицом.

Перечень сведений, получаемых уполномоченными органами от контролируемых лиц, ограничивается законом заявлениями, уведомлениями, обращениями и декларациями, что представляется недостаточным на нынешнем этапе развития информационного общества. Действующим законодательством прямо не предусматриваются такие источники сведений и данных, как информационные ресурсы контролируемых лиц (сайт в сети Интернет, цифровые платформы, персональные страницы в социальных сетях и т.д.). Представляется важным законодательно возложить на государственные органы контроля (надзора) обязанности по постоянному мониторингу указанных информационных площадок, в том числе с применением сквозных цифровых технологий в профилактических целях и для всесторонней оценки соблюдения обязательных требований.

§ 1.4. Система искусственного интеллекта и информационные системы государственного контроля (надзора)

Целесообразно для последовательного рассмотрения предмета настоящего параграфа вначале раскрыть понятие «искусственный интеллект» (ИИ).

Поскольку указанный термин первоначально возник и стал применяться в области информационных технологий, то прежде всего обратимся к пониманию ИИ в технических науках.

Основатель Российской (Советской) Ассоциации искусственного интеллекта, доктор технических наук, профессор, академик РАЕН Дмитрий Александрович Поспелов считал, что невозможно пока определить понятия ИИ и интеллектуальные системы, что «зыбки границы тех исследований в области интеллектуальных систем, которые отделяют их от собственно кибернетических

исследований, исследований в области программирования, вычислительных машин, математической психологии и структурной лингвистики. Где-то на стыке многих научных дисциплин происходит в наши дни вычленение нового научного направления со своим предметом исследования, своими специфическими методами и мировоззрением»[79].

Д.А. Поспелов определил следующие основные значения рассматриваемого термина, являющегося скорее всего метафорой:

1. «Научное направление, в рамках которого ставятся и решаются задачи аппаратного или программного моделирования тех видов человеческой деятельности, которые традиционно считаются интеллектуальными. Предмет исследования – изучение психики человека для имитации ее в технических системах. Со своим специфическим научным языком и со своими методами решения проблем»[80].

2. «Свойство интеллектуальных систем выполнять функции (творческие), которые традиционно считаются прерогативой человека»[81].

В рамках информатики – дисциплины, посвященной методам и процессам сбора, хранения, обработки, передачи, анализа и оценки информации с использованием компьютерных технологий, которые позволяют применять данные для принятия решений – особо выделяют материальную основу ИИ. Эту основу представляют собой интеллектуальные системы (ИС).

Среди функций, воспроизводимых ИИ, выделяются обучение и логический вывод. Примерами областей применения ИИ являются игры, логический вывод, обучение, распознавание естественных языков, построение планов, прогнозирование, понимание устной речи, доказательство теорем, а также зрительное восприятие.

---

[79] *Поспелов Д.А.* Фантазия или наука: на пути к искусственному интеллекту. М.: Наука. Главная редакция физико-математической литературы, 1982. С. 3.

[80] *Поспелов Д.А.* Указ. соч. С. 211.

[81] *Аверкин А.Н., Гаазе-Рапопорт М.Г., Поспелов Д.А.* Толковый словарь по искусственному интеллекту. М.: Радио и связь, 1992. С. 38 - 39.

ИИ рассматривается как «предмет науки, посвященной разработке компьютеров и компьютерных программ, которые моделируют работу человеческого мозга. Наиболее распространенная форма ИИ — это компьютер, запрограммированный на ответы по какой-то определенной теме»[82].

По мнению А.В. Минбалеева, «искусственный интеллект представляет собой совокупность информационных технологий, в том числе цифровых, позволяющих решать на основе тех или иных систем проблемы, связанные с возможностью их решения преимущественно на уровне человеческого интеллекта»[83].

А.А. Щитова определяет правовую природу системы ИИ как вида интеллектуальных информационных систем, обосновывает отличие систем ИИ от информационных систем и необходимость введения на основании приема юридической фикции конструкции электронного лица[84].

В своей работе «Системы искусственного интеллекта» С.Н. Павлов указывает на многообразие определений рассматриваемого понятия, в том числе на понимание ИИ как информационной технологии, связанной с процессами логического вывода, обучения и восприятия[85].

О недопустимости смешивания понятий «искусственный интеллект» и «система автоматизации» указывает К.С. Евсиков[86], аргументируя свое мнение тем, что при когнитивной автоматизации «компьютерная программа сопоставляет данные, а искусственный интеллект, это технология, которая позволяет машине «понимать» данные».

По мнению Г.А. Грищенко, применение ИИ может означать использование «модели нейронных сетей как одного из видов машинного обучения, способных

---

[82] Научно-технический словарь // URL: https://gufo.me/dict/scientific/ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ (дата обращения: 20.11.2023). См. также: Allen J. AI Growing up / J. Allen // AI MAGAZINE. — 1998. — V. 19. — №4. P. 13–23.

[83] *Минбалеев А.В.* Понятие искусственный интеллект в праве // Вестник Удмуртского университета. 2022, Т. 32, вып. 6. С. 1097 – 1098. См. также: *Архипов В. В., Грачёва А. В., Минбалеев А. В., Наумов В. Б., Полякова Т. А.* Определение искусственного интеллекта в контексте российской правовой системы: критический подход // Государство и право. 2022. Номер 1. С. 168-178.

[84] *Щитова А.А.* Правовое регулирование информационных отношений по использованию систем искусственного интеллекта: автореф. дисс. … канд. юрид. наук. Москва. 2022. С. 29.

[85] *Павлов С.Н.* Системы искусственного интеллекта: учеб. пособие: в 2-х ч. Ч.1. Томск: Эль Контент, 2011. С. 10 – 11.

[86] *Добробаба М.Б., Чаннов С.Е., Евсиков К.С.* Правовое обеспечение применения цифровых технологий в государственном управлении: Монография. Саратов: Амирит, 2024. С. 55.

выявлять закономерности между входными и выходными данными и выдавать верный результат даже для тех данных, которых не было в изначальной выборке.»[87].

По мнению Е.В. Холодной, «как объект права технология искусственного интеллекта - это программа для ЭВМ или система таких программ (информационная система), предназначенная для имитирования интеллектуальной деятельности человека»[88].

Нормативное определение ИИ содержится в Национальной стратегии развития искусственного интеллекта на период до 2030 года[89] (далее – Стратегия развития ИИ), в соответствии с которой ИИ является комплексом технологических решений, позволяющим имитировать когнитивные функции человека (включая поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека или превосходящие их. ИИ 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. Указанное определение также содержится в Федеральном законе от 24.04.2020 N 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации - городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных».

Вышеуказанной Стратегией развития ИИ к технологиям ИИ отнесена совокупность технологий, включающая в себя компьютерное зрение, обработку естественного языка, распознавание и синтез речи, интеллектуальную поддержку принятия решений и перспективные методы ИИ. Можно расширить приведенный

---

[87] *Грищенко Г.А.* Искусственный интеллект в государственном управлении // Российский юридический журнал. 2018. № 6. С. 27 - 31.

[88] *Холодная Е.В.* О перспективных направлениях правового регулирования в сфере технологии искусственного интеллекта // Вестник Университета имени О.Е. Кутафина (МГЮА). 2019. № 12. С. 90.

[89] Указ Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» // Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 11.10.2019.

перечень технологий ИИ, указав также синхронный перевод, распознавание лиц, массовое наблюдение (тотальная слежка)[90].

В своей работе я исхожу из понимания ИИ как программы для ЭВМ, созданной при помощи машинного обучения и иных технических методов и может быть использована для анализа массива данных в целях выявления закономерностей в таких данных и для решения задач, связанных с контрольно-надзорной деятельностью, без постоянного контроля и руководства со стороны человека.

Обратимся к информационным системам, созданным для информационного обеспечения государственного контроля (надзора).

Законом № 248-ФЗ предусмотрено использование органом контроля (надзора) следующих **информационных систем и ресурсов** для обработки информации (данных):

- Единый реестр видов федерального государственного контроля (надзора), регионального государственного контроля (надзора), муниципального контроля (оператор – Минэкономразвития России);

- Федеральная государственная информационная система «Единый реестр контрольных (надзорных) мероприятий» (оператор – Генеральная прокуратура Российской Федерации);

- Федеральная государственная информационная система "Единый портал государственных и муниципальных услуг (функций)" (далее – ФГИС ЕПГУ) и региональный портал государственных и муниципальных услуг;

- информационная система (подсистема ФГИС ЕПГУ) досудебного обжалования;

- реестр заключений о подтверждении соблюдения обязательных требований (реестр заключений о соответствии) национального органа по аккредитации;

- информационные системы контрольных (надзорных) органов;

---

[90] Возможности применения искусственного интеллекта в государственном управлении и юридические экспертизы / *Э.В.Талапина, В.Н.Южаков, А.А.Ефремов, И.А.Черешнева.* М.: Издательский дом «Дело» РАНХиГС, 2022. С.8.

- иные информационные системы в целях обеспечения организации и осуществления государственного контроля (надзора), муниципального контроля, создаваемые в соответствии с законодательством Российской Федерации, законодательством субъектов Российской Федерации, муниципальными правовыми актами[91].

Для унификации информационного обмена Закон № 248-ФЗ предусматривает в отношении информационных систем контрольных (надзорных) органов, иных информационных систем, созданных в целях обеспечения организации и осуществления государственного контроля (надзора), муниципального контроля, требования о передаче необходимых сведений в единый реестр видов контроля и единый реестр контрольных (надзорных) мероприятий.

Информационное взаимодействие информационных систем государственного контроля (надзора) осуществляется посредством единой системы межведомственного электронного взаимодействия, а также иными способами, предусмотренными положениями об указанных системах, правилами формирования и ведения единого реестра контрольных (надзорных) мероприятий.

Порядок формирования и ведения единых реестров видов государственного контроля (надзора) и контрольных (надзорных) мероприятий устанавливается следующими актами Правительства РФ:

- постановление Правительства РФ от 02.04.2021 № 528 «О внесении изменений в некоторые акты Правительства Российской Федерации в части создания, эксплуатации и развития единого реестра видов федерального государственного контроля (надзора), регионального государственного контроля (надзора), муниципального контроля» (далее – ПП 528);

- постановление Правительства РФ от 16.04.2021 № 604 «Об утверждении Правил формирования и ведения единого реестра контрольных (надзорных)

[91] Примером таких информационных систем являются реестр обязательных требований, содержащихся в нормативных правовых актах Московской области (Постановление Правительства Московской области от 29 декабря 2021 г. № 1519/44) и государственная информационная система "Единая государственная информационная система обеспечения контрольно-надзорной деятельности Московской области" (Приказ министра Мингосуправления Московской области от 22 мая 2023 г. № 11-74/П-09).

мероприятий и о внесении изменения в постановление Правительства Российской Федерации от 28 апреля 2015 г. N 415» (далее – ПП 604).

Рассмотрим, как в вышеприведенных правительственных актах регулируется применение цифровых технологий при формировании и ведении единых реестров.

В ПП 528 указаны сведения, которые включает в себя единый реестр видов контроля (далее – Реестр). Кроме того, предусматривается визуальное отображение количественной информации о видах контроля и иной содержащейся в Реестре информации, наличие публичной и закрытой частей Реестра. В состав функций оператора Реестра включена проверка информации, включаемой в Реестр контрольными (надзорными) органами, перед ее публикацией в Реестре на предмет полноты и достоверности. На Минцифры России возложено техническое обеспечение функционирования Реестра. Однако в ПП 528 не уточнено, каким способом и с применением каких технологий осуществляются проверка сведений, визуализация информации, техническое обеспечение.

Также обращает на себя внимание несоответствие целей создания Реестра и предусмотренного правительственным актом функционала программно-технических средств, посредством которых осуществляется ведение Реестра. Так, одной из целей является систематизация сведений, но в требованиях к программно-техническим средствам Реестра такая функция, как систематизация информации, не поименована.

Теперь обратимся к ПП 604, определяющему порядок формирования и ведения единого реестра контрольных (надзорных) мероприятий (далее – ЕРКНМ).

Указано на использование инфраструктуры, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме. ЕРКНМ в автоматическом и (или) автоматизированном режиме обеспечивает ведение электронных журналов учета операций, произведенных в едином реестре; фиксацию и отображение момента внесения сведений, содержащихся в едином реестре; фиксацию способа внесения сведений (с использованием личного

кабинета контрольного (надзорного) органа или путем информационного взаимодействия с ведомственной информационной системой контрольного (надзорного) органа). В указанном функционале ничего не сказано касательно анализа собранных сведений.

На примере рассмотренных актов Правительства РФ (ПП 528 и ПП 604) можно сделать вывод о правовом регулировании общественных отношений по формированию, ведению, использованию информационных систем в сфере государственного контроля (надзора) *в неполном объеме*, поскольку предусматривается только *статичная роль* указанных систем по накоплению, учету и поиску информации, но отсутствует функционал по анализу, в том числе с применением технологий ИИ, огромного массива данных, содержащихся в реестрах и иных информационных ресурсах[92].

Возможно, указанный пробел обусловлен тем, что в Федеральном законе «Об информации, информационных технологиях и о защите информации» не предусмотрены требования по использованию в государственных информационных системах информационных технологий, включая технологии ИИ, для создания аналитической и прогностической информации на основе обрабатываемых данных[93].

Для реализации принципа государственного контроля (надзора) о приоритете профилактики нарушений обязательных требований над контрольными (надзорными) мероприятиями представляется необходимым в Законе № 248-ФЗ предусмотреть обязательную для каждой информационной системы государственного контроля (надзора) обработку информации посредством технологий ИИ для проведения аналитической работы по определению условий и причин противоправного поведения контролируемых лиц как в общем виде

[92] См. также: *Лагаева В. П.* Влияние искусственного интеллекта на цифровой суверенитет России // Правовое обеспечение суверенитета России: проблемы и перспективы: Сборник докладов XIII Московской юридической недели: в 4 ч. Ч.1 / редколлегия: А. В. Корнев [и др.]. – М.: Издательский центр Университета имени О.Е. Кутафина (МГЮА), 2024. С. 201-204.

[93] См. также: *Лагаева В.П.* Правовые основания ... С. 653 – 654.

(применительно к неопределенному кругу лиц), так и в частном виде (применительно к конкретному контролируемому лицу).

Обработка большого объема электронной информации, являющееся разнообразной и постоянно меняющейся, осуществляется посредством технологии обработки, хранения и интеграции структурированных и неструктурированных, постоянно изменяющихся данных больших объемов (технология Big Data)[94]. Применение искусственного интеллекта для управления крупными массивами данных (Big Data) предполагает использование широкого спектра методов машинного обучения, ориентированных на повышение ценности, получаемой в результате анализа больших данных. Согласно опросу, 76,5% его участников считают, что Big Data и ИИ все больше переплетаются и помогают развивать когнитивные способности компаний[95].

Несмотря на различия в принципах функционирования рассматриваемых здесь технологий, они обладают высокой степенью взаимодополняемости. Это объясняется тем, что ИИ необходимы значительные объемы данных для выработки интеллектуальных решений, тогда как технология Big Data обеспечивает доступность этих данных для ИИ.

Интеграция технологий больших данных и ИИ способна качественно изменить государственную функцию по контролю и надзору, повысив во много раз ее оперативность и эффективность, а также точность прогнозирования[96].

При этом важно постоянно иметь в виду и учитывать, что технологии обработки больших данных и искусственного интеллекта «несут наибольшие риски для прав человека»[97].

---

[94] *Кириллова Е. А.* Правовой статус и принципы использования технологии больших данных (Big Data) // Российская юстиция. 2021. № 2. С. 68-69.

[95] Яндекс: Искусственный интеллект для управления большими данными Big Data [Электронный ресурс]. URL: https://yandex.ru/vc.ru/u/1266146-404/550756 (дата обращения: 18.03.2024).

[96] См. например: *Талапина Э.В., Южаков В.Н., Двинских Д.Ю. и др.* Оборот данных в государственном управлении: перспективы правового регулирования. М., 2020. С. 220 – 221; *Савельев А. И.* На пути к концепции регулирования данных в условиях цифровой экономики // Закон. 2019. № 4. С. 174 – 195; *Лагаева В. П.* Правовые основания ... С. 651-656. *Лагаева В.П.* Влияние искусственного интеллекта на цифровой суверенитет России // Правовое обеспечение суверенитета России: проблемы и перспективы: Сборник докладов XIII Московской юридической недели: в 4 ч. Ч.1 / редколлегия: А. В. Корнев [и др.]. – М.: Издательский центр Университета имени О.Е. Кутафина (МГЮА), 2024. – С. 203.

[97] *Ефремов А. А.* Государственный суверенитет в условиях цифровой трансформации // Правоведение. 2019. Т. 63. № 1. С. 57.

Отслеживая посредством алгоритмов ИИ деятельность контролируемых лиц, контрольные (надзорные) органы могут корректировать свои программы по профилактике нарушений обязательных требований и вырабатывать предложения по совершенствованию нормативных правовых актов. Важно отметить, что контрольные (надзорные) органы обязаны ежегодно осуществлять подготовку предложений по результатам обобщения правоприменительной практики, при этом применение интеллектуальных программных продуктов позволит не упустить из фокуса внимания должностного лица все возможные отклонения от стандартов добросовестного поведения[98].

Требуется уточнить правовой режим информационных систем государственного контроля (надзора) с целью их трансформации в интеллектуальные информационные системы, что позволит не только аккумулировать и учитывать в них управленческую информацию, но и обрабатывать данные как в целом для оценки и управления рисками нарушений обязательных требований, так и для разработки модели поведения конкретного контролируемого лица с учетом его цифрового профиля, вырабатываются с использованием алгоритмов искусственного интеллекта предложения по совершенствованию обязательных требований. Это позволит не упустить ни одно ценное сведение при принятии должностными лицами органов контроля (надзора) решений в рамках своих полномочий.

В настоящее время информационные системы ГКН, согласно установленным правилам, эксплуатируются в основном в целях учета информации и обеспечения взаимодействия органов контроля (надзора) с органами прокуратуры, с другими государственными органами и контролируемыми лицами. Указанных целей явно недостаточно для внедрения и развития интеллектуальных систем и технологий ИИ.

---

[98] См.: *Лагаева В.П.* Влияние искусственного интеллекта на цифровой суверенитет России ... С. 203.

ГЛАВА 2. Перспективная модель публично-правового регулирования отношений в сфере применения искусственного интеллекта при осуществлении государственного контроля (надзора)

§ 2.1. Российский опыт применения искусственного интеллекта в контрольно-надзорной деятельности государственных органов

Нормативные правовые акты, регулирующие общественные отношения по организации и проведению государственного контроля (надзора) в Российской Федерации, в настоящее время не определяют специальный порядок применения ИИ, в том числе требования к формированию наборов данных для разработки, обучения и модернизации интеллектуальных систем. Как рассмотрено выше, применительно к государственным и иным информационным системам сферы ГКН не осуществляется на уровне законов и подзаконных актов четкое регламентирование процесса применения технологий ИИ.

Справедливо утверждение А.В. Минбалеева о необходимости осуществления этического регулирования применения ИИ на уровне Правительства Российской Федерации с привлечением Российской академии наук, профессиональных объединений и союзов, иных субъектов гражданского общества, что позволит разработать единые этические правила, дополняемые в рамках отдельных направлений использования ИИ[99].

Среди актов рекомендательного характера необходимо выделить Кодекс этики в сфере ИИ (далее – Кодекс), разработанный на площадке Альянса в сфере ИИ[100]. Ряд федеральных органов исполнительной власти (в том числе Минэкономразвития России, Росалкогольрегулирование, Росжелдор, Росрыболовство) и органов исполнительной власти субъектов Российской Федерации (Министерство цифрового развития и связи Кузбасса, Агентство по

[99] *Минбалеев А.В.* Регулирование использования искусственного интеллекта в России // Информационное право. 2020. № 1. С. 38.

[100] Кодекс этики в сфере ИИ. URL: https://ethics.a-ai.ru/ (дата обращения: 20.11.2023).

труду и занятости населения Сахалинской области и др.) присоединились к Кодексу. Представляется, что данное обстоятельство важно учитывать при введении правового регулирования отношений по применению ИИ при проведении государственного контроля (надзора), поскольку оно свидетельствует о признании органами контроля (надзора) приоритета человеко-ориентированного подхода, что подтверждает наличие предпосылок для имплементации отдельных норм Кодекса в нормативные правовые акты Российской Федерации.

Национальная стратегия развития искусственного интеллекта на период до 2030 года[101] признает в качестве необходимого условия своей реализации постепенный переход органов публичной власти к использованию технологий ИИ. В рамках федерального проекта «Цифровые технологии» национальной программы «Цифровая экономика Российской Федерации» были разработаны дорожные карты по развитию сквозных цифровых технологий. В 2019 году Правительственная комиссия по цифровому развитию одобрила семь дорожных карт по развитию сквозных технологий цифровой экономики и входящие в них субтехнологии, описанные в дорожных картах, в том числе «Дорожная карта развития «сквозной» цифровой технологии «Нейротехнологии и искусственный интеллект» (далее – Дорожная карта).

В Дорожной карте применительно к субтехнологии «Рекомендательные системы и интеллектуальные системы поддержки принятия решений» поставлена технологическая задача по обоснованию решений, принятых на основе искусственного интеллекта, в целях поддержки принятия и верификации решений контрольных (надзорных) органов. Для государственного управления может быть также полезна разработка подходов и алгоритмов по интерпретации и обоснованию принимаемого решения искусственного интеллекта (eXplainable AI).

Следующий документ стратегического планирования - Концепция развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года, утвержденная распоряжением Правительства

[101] Указ Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» // Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 11.10.2019.

Российской Федерации от 19 августа 2020 г. № 2129-р[102]. Отмечена необходимость установления специального правового регулирования применения ИИ и робототехники с обеспечением баланса интересов всех сторон рассматриваемых отношений, включая разработчиков систем ИИ, потребителей, общество, государство. Указанная Концепция в качестве ориентиров для нормотворчества определяет цели, задачи и принципы правового регулирования отношений в сфере технологий ИИ и робототехники, при этом сформулированы как общеотраслевые задачи регулирования, так и отраслевые направления совершенствования законодательства Российской Федерации в том числе в сфере государственного (муниципального) управления.

Федеральный закон от 24 апреля 2020 г. № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации - городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» устанавливает упрощенный порядок работы с персональными данными (без согласия субъектов персональных данных) для разработчиков, которые включены в реестр участников экспериментального режима. Такими участниками могут быть как юридические лица, так и индивидуальные предприниматели. Также согласно положениям данного закона устанавливаемый экспериментальный режим осуществляется под руководством Правительства Москвы, которое регламентирует условия, требования, порядок разработки, создания, внедрения и реализации ИИ-технологий, а также механизм обработки обезличенных персональных данных. Важно отметить, что одной из целей установления экспериментального правового режима является повышение эффективности государственного управления.

Федеральным законом от 31 июля 2020 года № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской

[102] Распоряжение Правительства РФ от 19 августа 2020 г. № 2129-р // Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 26.08.2020.

Федерации» осуществление государственного контроля (надзора) указано в качестве направления разработки, апробации и внедрения цифровых технологий, в том числе технологий ИИ (компьютерное зрение, обработка естественного языка, распознавание и синтез речи, машинные рекомендации и поддержка принятия решений)[103].

Протоколом президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 27 августа 2020 года № 17 был утвержден Паспорт федерального проекта «Искусственный интеллект» национальной программы «Цифровая экономика Российской Федерации». Указанный проект координирует Министерство экономического развития Российской Федерации.

Технологические задачи, на выполнение которых может быть направлен проект в области ИИ, определены Министерством экономического развития Российской Федерации[104] в разрезе таких технологий ИИ, как:

- компьютерное зрение;
- обработка естественного языка;
- распознавание и синтез речи;
- интеллектуальная поддержка принятия решений;
- перспективные методы искусственного интеллекта.

В октябре 2021 года Правительство РФ утвердило перечень инициатив социально-экономического развития Российской Федерации до 2030 года[105], в который вошли инициативы, сгруппированные по таким направлениям, как "социальная сфера", "строительство", "экология", "цифровая трансформация", "технологический рывок" и "государство для граждан".

---

[103] Постановление Правительства РФ от 28 октября 2020 г. № 1750 «Об утверждении перечня технологий, применяемых в рамках экспериментальных правовых режимов в сфере цифровых инноваций» // Официальный интернет-портал правовой информации http://pravo.gov.ru, 29.10.2020.

[104] Приказ Минэкономразвития России от 29 июня 2021 г. № 392 «Об утверждении критериев определения принадлежности проектов к проектам в сфере искусственного интеллекта» (Зарегистрировано в Минюсте России 28.07.2021 № 64430) // Официальный интернет-портал правовой информации http://pravo.gov.ru, 29.07.2021.

[105] Распоряжение Правительства РФ от 6 октября 2021 г. № 2816-р // Официальный интернет-портал правовой информации http://pravo.gov.ru, 07.10.2021.

В направлении «Государство для граждан» указана инициатива «Государство для людей»[106], за реализацию которой в целом ответственно Минэкономразвития России, а в части ИТ-решений для внедрения качественно новых изменений участвует Минцифры России.

Представляется, что технологии ИИ полезны для обеспечения простоты и удобства диалога государства и граждан, включая представителей контролируемых лиц, для автоматизации процесса государственного контроля (надзора). В частности, созданный в 2021 году на основе технологий ИИ чат-бот «Онлайн-инспектор» на сайте Федеральной службы по надзору в сфере труда предоставил более 90 тысяч консультаций (по состоянию на сентябрь 2022 г.). Доступный в мессенджере Telegram чат-бот «Свободный доступ» упрощает сотрудничество жителей Москвы с органами контроля, позволяя оперативно восстановить доступ к общественным пространствам, ограниченный незаконно установленными шлагбаумами, заборами, парковочными столбиками, барьерами и полусферами, а также сообщить о незаконных парковках и захвате общественных пространств[107].

В 2022 году начал свою работу Национальный центр развития искусственного интеллекта при Правительстве Российской Федерации - площадка для отбора ИИ-решений для бизнеса, науки и государства, которая занимается экспертизой документов о регулировании ИИ, а также экспертным сопровождением внедрения ИИ в госуправлении и в секторах экономики[108].

В России создана Ассоциация «Альянс в сфере искусственного интеллекта», участником которой являются «Яндекс», VK, Сбер, Газпромнефть, Российский фонд прямых инвестиций, группа компаний «Самолет», АО "ОХК "Уралхим", ООО "Группа компаний "Русагро", ПАО «Сибур», ПАО «Северсталь», АО «ТБанк», ПАО «Ростелеком», АО «Лаборатория Касперского» и ПАО МТС[109]. Миссия Альянса

---

[106] «Государство для людей» — Федеральный проект. URL: https: //xn--80aebecah6apa1adyldqm2sra.xn--p1ai (дата обращения: 02.08.2024).

[107] «Чат-ботом «Свободный доступ» воспользовались около 1,7 тысячи москвичей». URL: https://www.mos.ru/news/item/129014073/ (дата обращения: 12.11.2023).

[108] Национальный центр развития ИИ при Правительстве Российской Федерации. URL: https://ai.gov.ru/ (дата обращения: 01.08.2024).

[109] Ассоциация "Альянс в сфере искусственного интеллекта". URL: https://a-ai.ru/ (дата обращения: 01.08.2024).

состоит в создании центра развития ИИ в России, обеспечении технологического лидерства России на глобальном технологическом рынке.

Рассмотрим российский опыт внедрения ИИ на примере отдельных органов государственного контроля (надзора): МВД России, Росреестр, Роскомнадзор и Ространснадзор.

Министерство внутренних дел Российской Федерации (МВД России) является федеральным органом исполнительной власти, осуществляющим правоприменительные функции по федеральному государственному контролю (надзору) в сфере внутренних дел.

Департамент информационных технологий, связи и защиты информации МВД России[110] выполняет в том числе функцию по организации и координации деятельности по внедрению ИИ в аппаратно-программные комплексы и сервисы ИСОД МВД России.

Ведомственная программа цифровой трансформации МВД России на 2022 - 2024 годы[111] предусматривает в числе прочих задачу по ликвидации имеющихся отставаний по вопросам применения технологий ИИ, а в качестве показателей результативности программы устанавливает, в частности, следующие параметры:

- реализация плана внедрения искусственного интеллекта в деятельность МВД России, включающего проекты (мероприятия), предусматривающие использование и (или) разработку технологий, основанных на использовании искусственного интеллекта, включая компьютерное зрение, обработку естественного языка, распознавание и синтез речи, интеллектуальную поддержку принятия решений и перспективные методы искусственного интеллекта, и создание дата-сетов;

- количество доступных дата-сетов (наборов данных) для реализации задач искусственного интеллекта.

---

[110] Приказ МВД России от 15 июня 2021 г. № 444 «Об утверждении Положения о Департаменте информационных технологий, связи и защиты информации Министерства внутренних дел Российской Федерации» // СПС «КонсультантПлюс».

[111] Распоряжение МВД России от 11 января 2022 г. № 1/37 // СПС «КонсультантПлюс».

Рассматриваемая программа ссылается на план внедрения ИИ в деятельность МВД России на 2021 год и плановый период 2022 и 2023 годов, включающий проекты (мероприятия), в том числе кросс-ведомственные, предусматривающие использование и (или) разработку технологий, основанных на использовании искусственного интеллекта.

Отметим, что в нормативных правовых актах, регулирующих контрольную (надзорную) деятельность МВД России, не предусматривается применение специальных технических средств, основанных на методах ИИ, например, с функцией распознавания лиц.

Федеральная служба государственной регистрации, кадастра и картографии (Росреестр) является федеральным органом исполнительной власти, осуществляющим федеральный государственный земельный контроль (надзор). В составе Росреестра функционирует Управление стратегического развития и цифровой трансформации, одной из основных функций которого является координация мероприятий, связанных с внедрением искусственного интеллекта и других инновационных технологий в области ИТ в информационные системы Росреестра, например, в сервис по распознаванию документов для сокращения трудозатрат на создание электронного архива, а также на проверку документов и извлечение необходимой информации[112].

Кроме того, Росреестр совместно с Минцифры России на базе федеральной государственной информационной системы "Единый портал государственных и муниципальных услуг (функций)" (далее - ЕПГУ) реализует онлайн-сервис по проверке объектов недвижимости, подготовке и согласованию документов между участниками сделки, регистрации прав (ограничений, обременений) на недвижимое имущество, в том числе с ипотекой (далее - суперсервис "Мое жилье"). Суперсервис "Мое жилье" на базе ЕПГУ позволит в том числе проводить предварительную проверку пакета документов и состава документов до подачи

[112] Госуслуги будущего: как ИИ, чат-боты и онлайн-сервисы изменят Росреестр. URL: https://trends.rbc.ru/trends/innovation/cmrm/5fa58d829a79472be3ef41c2?from=copy (дата обращения: 29.03.2024).

заявления на государственную регистрацию прав, в том числе с применением технологий искусственного интеллекта.

При этом важно обратить внимание на отсутствие нормативного правового акта, регулирующего отношения по оказанию и пользования вышеуказанным суперсервисом, что в очередной раз иллюстрирует ситуацию с практикой внедрения цифровых технологий до установления соответствующего нормативного правового регулирования.

Ведомственная программа цифровой трансформации Росреестра на 2022 финансовый год и плановый период 2023 - 2024 годов[113] устанавливает показатель Программы по направлению «Государственные данные»: «Количество доступных датасетов (наборов данных) для реализации задач искусственного интеллекта».

На основе технологии ИИ Росреестр планирует создать систему поддержки принятия решений «Цифровой помощник». Предполагается, что искусственный интеллект будет формировать «второе мнение» для государственного регистратора прав, при этом окончательное решение будет оставаться за человеком[114].

Правительством РФ установлено[115], что ФГИС ведения Единого государственного реестра недвижимости предназначена для автоматизации и оптимизации учетно-регистрационных процессов, в том числе с использованием технологий искусственного интеллекта, и в этой связи в структуру рассматриваемой в настоящем абзаце ФГИС включен такой структурный элемент, как подсистема искусственного интеллекта, предназначенная для поддержки принятия решений с использованием нейросетевых методов обработки данных.

---

[113] Приказ Росреестра от 29 декабря 2021 г. № П/0642 «Об утверждении ведомственной программы цифровой трансформации Федеральной службы государственной регистрации, кадастра и картографии на 2022 финансовый год и плановый период 2023 - 2024 годов» // СПС «КонсультантПлюс».

[114] Госуслуги будущего: как ИИ, чат-боты и онлайн-сервисы изменят Росреестр. URL: https://trends.rbc.ru/trends/innovation/cmrm/5fa58d829a79472be3ef41c2?from=copy (дата обращения 29.03.2024).

[115] Постановление Правительства РФ от 29 апреля 2023 г. № 683 «Об утверждении Положения о федеральной государственной информационной системе ведения Единого государственного реестра недвижимости и о внесении изменения в пункт 3 Правил информационного взаимодействия федеральной государственной информационной системы ведения Единого государственного реестра недвижимости с иными государственными или муниципальными информационными системами» // Официальный интернет-портал правовой информации http://pravo.gov.ru, 03.05.2023.

В государственной программе Российской Федерации «Национальная система пространственных данных»[116] указано на необходимость реализации мероприятий, направленных на сохранение и развитие полученных результатов на основе технологий ИИ. В числе проблем в сфере земельных и имущественных отношений, развития инфраструктуры пространственных данных указано, в частности, на ограниченное использование ИИ для повышения эффективности цифровизации указанной сферы.

В рамках указанной программы Росреестр применяет беспилотные летательные аппараты, функционирующие на основе технологий ИИ, для осуществления государственного земельного надзора[117]. Однако ни федеральными законами (Земельный кодекс Российской Федерации, Закон № 248-ФЗ), ни Положением о федеральном государственном земельном контроле (надзоре), утвержденном Правительством РФ, не установлены правила применения контрольным (надзорным) органом беспилотных систем.

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) является федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации и массовых коммуникаций, информационных технологий и связи, функции по контролю и надзору за обработкой персональных данных.

Для повышения эффективности своей работы Роскомнадзор осуществляет техническое обновление, внедряет новые информационные системы, в том числе с использованием технологий искусственного интеллекта[118].

На базе Научно-технического центра ФГУП ГРЧЦ (подведомственное предприятие Роскомнадзора) создан в марте 2021 года Экспертный совет по ИИ в целях анализа передовых технологий в области ИИ и оценки возможности их

---

[116] Постановление Правительства РФ от 1 декабря 2021 г. № 2148 «Об утверждении государственной программы Российской Федерации "Национальная система пространственных данных» // Официальный интернет-портал правовой информации http://pravo.gov.ru, 07.12.2021.

[117] Использование БПЛА при земельном надзоре Росреестра в Калужском регионе. URL: https://www.kaluga-gov.ru/news/45596/ (дата обращения 01.08.2024).

[118] Состоялось расширенное заседание коллегии Роскомнадзора. URL: https://rkn.gov.ru/press/news/news73648.htm (дата обращения 01.08.2024).

применения при реализации задач Роскомнадзора и ГРЧЦ. В состав Экспертного совета входят представители Технического комитета по стандартизации №164 «Искусственный интеллект» (ТК 164), МФТИ, Сбер, НИЦ «Курчатовский институт», Ассоциации больших данных, Университета Сириус и др.

Одной из задач Ведомственной программы цифровой трансформации Роскомнадзора на 2022 - 2024 годы[119] является повышение эффективности и безопасности реализации контрольно-надзорных и государственных функций за счет внедрения современных электронных технологий в государственное управление (единый модуль анализа на базе технологий искусственного интеллекта, автоматизированная система прогнозирования рисков, система контроля качества услуг связи).

Одним из показателей ведомственной программы цифровой трансформации Роскомнадзора является количество доступных дата-сетов (наборов данных) для реализации задач искусственного интеллекта.

При наличии вышеприведенных фактов, подтверждающих вовлеченность Роскомнадзора в развитие и применение методов ИИ, в нормативных правовых актах, регулирующих отношения в сфере ГКН, находящейся в области деятельности указанного ведомства, отсутствуют положения касательно использования сквозных цифровых технологий.

Федеральная служба по надзору в сфере транспорта (Ространснадзор) имеет в своей структуре Управление программ развития, цифровизации, информатизации и аналитики, выполняющее в том числе следующие функции:

- координация реализации мероприятий, связанных с внедрением и развитием технологий искусственного интеллекта, других инновационных технологий в информационные системы Ространснадзора – по вопросам стратегического планирования в области цифровой трансформации контрольной (надзорной) деятельности в сфере транспорта;

---

[119] «Ведомственная программа цифровой трансформации Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций на 2022–2024 годы» // СПС «КонсультантПлюс».

- обеспечение внедрения и использования технологий искусственного интеллекта в информационных системах Ространснадзора – по вопросам создания, развития, ввода в эксплуатацию, эксплуатации и выводу из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации.

Также Ространснадзором создано Управление развития дистанционного автоматизированного контроля (надзора), одной из функций которого являются участие во внедрении и развитии технологий искусственного интеллекта в деятельность Ространснадзора в рамках применения дистанционного автоматизированного контроля (надзора), в том числе:

- участие в мероприятиях по внедрению и развитию технологий искусственного интеллекта (нейронных сетей);

- подготовка предложений по развитию технологий искусственного интеллекта в контрольной (надзорной) деятельности в сфере транспорта;

- изучение опыта применения технологий искусственного интеллекта зарубежных стран и органов власти Российской Федерации с целью использования лучших практик в деятельности Ространснадзора.

«Публичная декларация ключевых целей и приоритетных задач Федеральной службы по надзору в сфере транспорта на 2024 год» (утверждена Ространснадзором 22.03.2024) включает в себя такую цель, как цифровая трансформация контрольной (надзорной) деятельности в сфере транспорта, автоматизация инструментов дистанционного контроля (надзора). Для достижения указанной цели Ространснадзором поставлены задачи по обеспечению развития и модернизации информационных систем Ространснадзора, применению и совершенствованию методов дистанционного контроля (надзора), разработке и использованию технологий искусственного интеллекта в контрольной (надзорной) деятельности в сфере транспорта, обеспечению информационной и кибербезопасности.

Уточним, что дистанционный контроль (надзор) или мониторинг согласно статье 96 Закона № 248-ФЗ является специальным режимом ГКН и представляет собой осуществляемыми контрольными (надзорными) органами

целенаправленное, постоянное (систематическое, регулярное, непрерывное), опосредованное получение и анализ 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.

Согласно указанной выше Публичной декларации ключевых целей и приоритетных задач Ространснадзора на 2024 год ожидаемые результаты по приоритетной задаче разработки и внедрения технологий искусственного интеллекта в деятельность Ространснадзора следующие:

- разработка и применение ИИ-решений при оказании услуги по выдаче свидетельства, подтверждающего право на управление курсирующими по железнодорожным путям локомотивом, мотор-вагонным подвижным составом и (или) специальным самоходным подвижным составом;

- повышение квалификации сотрудников Ространснадзора по вопросам внедрения, применения и развития искусственного интеллекта в сфере транспорта;

- участие в проведении ИИ-олимпиад, хакатонов.

Необходимо отметить, что, как и в случае с Росреестром и Роскомнадзором, в нормативных правовых актах, регулирующих отношения по организации и осуществлению федерального государственного контроля (надзора) в сфере транспорта, не содержатся специальные положения о применении цифровых технологий в указанном виде ГКН.

На основании изложенной в настоящем параграфе информации можно утверждать, что на момент проведения настоящего исследования российское законодательство не предусматривает специального правового регулирования отношений по применению технологий ИИ при проведении государственного контроля (надзора). Превалирующий уровень регулирования сейчас составляет так называемое «мягкое право» (например, Кодекс этики в сфере ИИ) и стратегические документы (концепции, программы и иные). При этом внедрение методов ИИ в информационные системы государственных органов контроля (надзора) имеет место быть, что подтверждается ведомственными программами по цифровой

трансформации указанных органов. Такая ситуация указывает на наличие пробела в правовом регулировании государственного контроля (надзора) в аспекте применения передовых цифровых технологий.

Ведомственные программы по цифровой трансформации государственных органов контроля (надзора) не содержат, как правило, информации о том, какие именно технологии ИИ планируется применять или уже применяются при осуществлении контроля (надзора), что не обеспечивает прозрачность этого процесса.

§ 2.2. Зарубежный опыт применения искусственного интеллекта в контрольно-надзорной деятельности государственных органов

Исследование зарубежного опыта внедрения технологий ИИ предлагается начать с дружественных Российской Федерации государств – участников БРИКС.

В настоящее время международное регулирование использования ИИ и робототехники не замедляет свой активный ход развития, главные направления которых указаны А.В. Минбалеевым[120].

По состоянию на 1 января 2025 года БРИКС является союзом следующих стран: Бразилия, Россия, Индия, Китайская Народная Республика (КНР), Южно-Африканская Республика (ЮАР), Объединенные Арабские Эмираты (ОАЭ), Иран, Египет, Эфиопия, Саудовская Аравия и Республика Индонезия.

Участники БРИКС активно внедряют в государственное управление технологии ИИ. Так, в Эфиопии в фокусе внимания государства находятся услуги электронного правительства, но при этом согласно Индексу развития электронного правительства ООН (далее – Индекс EGDI) в 2024 году Эфиопия заняла лишь 169 место в мире[121]. Разрабатываются и вводятся в эксплуатацию цифровые платформы

---

[120] *Минбалеев А.В.* Механизмы регулирования использования искусственного интеллекта // Право цифровой среды: Монография. М.: Проспект, 2022. С. 700 - 701.

[121] Индекс развития электронного правительства | Эфиопия | Средневзвешенный. URL: https://statbase.ru/data/eth-e-government-development-index/ (дата обращения: 10.06.2025). https://statbase.ru/datasets/indexes-and-ratings/e-government-development-index/?ysclid=ms8yhpd2kd533248404

(в том числе портал государственных услуг, Единая информационная система государственных закупок)[122].

Египет применяет интеллектуальные цифровые технологии для оптимизации работы правительства, совершенствования процесса принятия управленческих решений государственными учреждениями, улучшение государственных услуг, что непременно ведет к повышению доверия граждан к государству. Немаловажную роль сыграл ИИ в том, что Египет по состоянию на 2024 год занял 95 место согласно Индексу EGDI (по сравнению со 103 местом, которое занимал Египет в 2022 году).

В Бразилии судебная система использует цифровую технологию под названием Sinapses, являющуюся платформой для разработки и применения моделей ИИ. Благодаря указанной технологии происходит автоматизация повторяющихся процессуальных задач и однотипных дел, осуществляется генерация текстов, что ускоряет работу судебных секретарей и помощников судей при анализе судебных решений.

Согласно Индексу EGDI в 2024 году Королевство Саудовской Аравии занимало 6 место в группе стран «с очень высоким уровнем» развития.

В соответствии с Индексом EGDI в 2024 году Индия заняла 97 место среди 193 государств – членов ООН за счет улучшения предоставления онлайн-услуг. Технологии ИИ применяются органами судебной власти.

Согласно Глобальному инновационному индексу за 2024 год[123] Китай занимает 11 позицию. В соответствии с Индексом EGDI в 2024 году Китай занял 35 позицию в мире, между Францией и Грецией. ИИ занимает важное место в концепции «умного управления» (smart governance), которую в последние годы активно продвигает Коммунистическая партия Китая. Планируется усиление возможностей органов общественной безопасности за счет внедрения систем «умного мониторинга». Также рекомендуется активно внедрять ИИ в системы

[122] Особенности политики государств-участников БРИКС в сфере развития ИКТ, обеспечения национальной и международной информационной безопасности. URL: https://namib.online/wp-content/uploads/2024/05/BRICS.pdf (дата обращения: 10.06.2025).

[123] Глобальный инновационный индекс за 2024 год. URL: https://www.wipo.int/edocs/pubdocs/ru/wipo-pub-2000-2024-exec-ru-global-innovation-index-2024.pdf (дата обращения: 10.06.2025).

мониторинга общественного мнения и системы «информационной безопасности в Интернете». Судебное производство в КНР является направлением государственного управления, в которой технологии ИИ применяются более активно.

По Индексу EGDI Объединенные Арабские Эмираты (ОАЭ) в 2024 году занимали 11 место, что является высоким показателем. Реализуется проект по созданию электронного правительства UAE mGovernment. Внедряется инициатива Think AI по интеграции технологий ИИ в стратегические секторы, в том числе государственное управление, а также создан Совет по надзору за интеграцией ИИ в государственном и образовательном сферах[124].

ЮАР активно развивает направление по внедрению искусственного интеллекта и занимает 40 место согласно Индексу EGDI за 2024 год. Кроме того, ЮАР вошла в Пятерку африканских стран с высокими показателями в области "государственного управления", которые включают такие критерии, как наличие национального видения искусственного интеллекта, развитие онлайн-сервисов, наличие законов о защите данных и конфиденциальности, а также разработка стратегий кибербезопасности.

Чат-бот MomConnect, созданный Национальным департаментом здравоохранения ЮАР, предоставляет примерно 1,8 миллионам будущих матерей услуги до и послеродового периода. Зарегистрированные женщины могут общаться в чате с помощью приложения и получать медицинские консультации, касающиеся их беременности.

Согласно Индексу EGDI в 2024 году Иран входил в группу стран с высоким индексом развития электронного правительства и занимал 101 место в мире. При этом использование государством методов ИИ осуществляется в том числе для выявления женщин, нарушающих требование о ношении хиджаба, для улучшения контроля за цифровыми платформами и идентификации граждан, пытающихся обойти брандмауэры, блокирующие доступ к запрещенным информационным

[124] *Минбалеев А.В., Полякова Т.А., Добробаба М.Б. и др.* Перспективные направления правового регулирования искусственного интеллекта: Монография / Под ред. А.В. Минбалеева. Саратов: Амирит, 2023. С. 129.

ресурсам. Кроме того, внедрение Ираном технологии искусственного интеллекта знаменует собой значительный прогресс в мониторинге и обеспечении соблюдения экологических норм. Было выявлено более 40 000 случаев, что свидетельствует об эффективности ИИ в охране примерно 20 000 гектаров земли по всему Ирану[125].

В Индонезии с 2003 года происходит процесс оцифровки данных в рамках работы по внедрению электронного правительства. Государственные учреждения постепенно переходят от составления документов на бумажном носителе к созданию электронных документов. В настоящее время по Указу Президента Республики Индонезия № 39 от 12 июня 2019 г.[126] проводится стандартизация процедур владения, хранения и контроля качества данных.

Ни в одной из стран – участниц БРИКС не осуществляется комплексное единое правовое регулирование отношений по использованию технологий ИИ, в том числе в сфере государственного контроля (надзора), отсутствует единый законодательный акт в сфере ИИ.

В Бразилии Национальным конгрессом рассматривается законопроект, в котором предложены основы и принципы развития и применения ИИ. Эксперты отмечают, что бразильский закон об ИИ предусматривает «обязательный человеческий надзор, права на объяснение и оспаривание решений ИИ и строгие требования к использованию ИИ в государственном секторе»[127].

На уровне бразильского штата Сеара принят 11 августа 2021 года Закон № 17.611, устанавливающий обязательства и руководящие принципы по внедрению и использованию систем ИИ в указанном штате. Этот закон предусматривает, что системы ИИ должны проектироваться безопасным образом на основе этики и в соответствии с законодательством Бразилии. Он определяет систему ИИ как технологии компьютерных наук, которые позволяют компьютерам

---

[125] AI-Powered Land Monitoring Reveals Over 40,000 Cases of Unauthorized Land Use Change in Iran. URL: https://www.cryptopolitan.com/ai-detects-unlawful-land-use-in-iran/?ysclid=mscy6yytnu374924249 (дата обращения: 30.04.2025).

[126] Указ Президента Республики Индонезия № 39 от 12 июня 2019 г. URL: https://peraturan.bpk.go.id/Details/108813/perpres-no-39-tahun-2019 (дата обращения: 13.01.2025).

[127] Brazil's AI Act: A New Era of AI Regulation. URL: https://gdprlocal.com/brazils-ai-act-a-new-era-of-ai-regulation/#:~:text=The%20proposed%20Brazilian%20AI%20Act,%2C%20accountability%2C%20and%20consumer%20protection.&text=other%20risks%20(basic%20requirements) (дата обращения: 30.04.2025).

взаимодействовать с людьми с помощью технологических механизмов, позволяющих имитировать человеческое мышление.

Отдельные случаи регионального нормативно-правового регулирования применения ИИ отмечены и в Китайской Народной Республике. Так, приняты Положение о продвижении индустрии искусственного интеллекта в Шэньчжэне (the Regulations on the Promotion of Artificial Intelligence Industry in Shenzhen)[128] и Шанхайские правила содействия развитию индустрии искусственного интеллекта (Regulations of Shanghai on Promoting the Development of Artificial Intelligence Industry)[129].

Кроме того, в ряде государств БРИКС издаются нормативные правовые акты о регулировании отношений по применению отдельных технологий ИИ или по использованию ИИ в отдельных сферах. Так, в Бразилии принято Постановление N 271 от 2020 г., которое регулирует использование ИИ в деятельности судов. Дополнительно Постановление N 332 от 2020 г. обеспечивает этичность использования, прозрачность и контролируемость при разработке алгоритмов и использовании ИИ в судебной системе. Оба указанных акта направлены на то, чтобы весь процесс разработки и внедрения моделей ИИ в деятельность судов соответствовал концепции этнического и социокультурного многообразия в самом широком смысле, включая: пол, расу, этническую принадлежность, цвет кожи, сексуальную ориентацию, людей с ограниченными возможностями, а также другие индивидуальные характеристики.

В Индии Центр правовой политики Видхи (Vidhi Centre for Legal Policy ("Vidhi") совместно с Исследовательским и образовательным центром TCG в науке и технике (TCG Centers of Research and Education in Science and Technology) разработал стратегический документ "Ответственный ИИ для Индийской системы правосудия" ("Responsible Artificial Intelligence for the Indian Justice System")[130], который регулирует использование ИИ в системе правосудия Индии.

---

[128] URL: http://www.szrd.gov.cn/rdlv/chwgg/content/post_834228.html (дата обращения: 14.04.2023).

[129] URL: http://www.shrd.gov.cn/n8347/n8467/u1ai248931.html (дата обращения: 14.04.2023).

[130] URL: https://vidhilegalpolicy.in/research/responsible-ai-for-the-indian-justice-system-a-strategy-paper/ (дата обращения: 04.07.2023).

В 2021 году SFDA (Управление по санитарному надзору за качеством пищевых продуктов и медикаментов Саудовской Аравии) выпустило Руководство по медицинским устройствам на основе ИИ и больших данных (Guidance on AI and Big Data-based medical devices)[131], устанавливающее требования к выдаче разрешения на использование медицинских изделий на основе ИИ.

В ряде стран БРИКС созданы и функционируют экспериментальные правовые режимы. Так, в Саудовской Аравии с 2019 года функционирует регуляторная "песочница" в сфере FinTech, где можно протестировать новые технологии (в том числе ИИ) в безопасной зоне и с исключением законодательных барьеров. ОАЭ используют регуляторные «песочницы», например ADGM RegLab для тестирования инновационных FinTech-решений. В Индии создана регуляторная "песочница" под эгидой Резервного банка Индии (Reserve Bank of India), которая позволяет осуществлять тестирование инновационных продуктов.

В настоящее время в странах БРИКС преобладает применение рекомендательных норм в сфере инноваций, включая и технологии ИИ.

Саудовской Аравией создан Международный центр исследований и этики в области искусственного интеллекта[132], одной из целей которого является предоставление рекомендаций, касающихся политики в области ИИ, а также наращивание возможностей ИИ.

Индийским советом медицинских исследований (ICMR) опубликованы Этические рекомендации по применению искусственного интеллекта в биомедицинских исследованиях и здравоохранении (Ethical Guidelines for Application of Artificial Intelligence in Biomedical Research and Healthcare)[133]. Кстати, в Индии компании стали принимать корпоративные принципы применения ИИ. Так, Tata Consultancy Services (индийская транснациональная компания,

---

[131] URL: https://beta.sfda.gov.sa/sites/default/files/2021-04/SFDAArtificial%20IntelligenceEn.pdf (дата обращения: 18.07.2023).

[132] https://www.dataguidance.com/news/saudi-arabia-sdaia-advances-ai-development-new (дата обращения: 05.08.2024). International Center for Artificial Intelligence Research and Ethics (ICAIRE). URL: https://saudipedia.com/en/international-center-for-artificial-intelligence-research-and-ethics-icaire (дата обращения: 26.08.2024).

[133] URL: https://www.thehindu.com/sci-tech/health/icmr-releases-the-countrys-first-ethical-guidelines-for-application-of-ai-in-biomedical-research-and-healthcare/article66657158.ece (дата обращения: 27.03.2023).

предоставляющая услуги в области информационных технологий, IT-консалтинга и IT-решений для бизнеса) стала первой индийской компанией, которая разработала и приняла свои корпоративные принципы этики ИИ[134].

В Китае государственные ведомства и окологосударственные объединения начали разрабатывать белые книги (по стандартизации и безопасности ИИ, по стандартизации безопасности ИИ, по управлению ИИ) и концепции регулирования сферы ИИ[135].

В разработанных Пекинской академией искусственного интеллекта Пекинских принципах ИИ (Beijing AI Principles)[136] предусмотрены принципы исследования, использования и регулирования ИИ. Концептуальным ядром выступает императив проактивной адаптации регуляторных механизмов, призванной амортизировать турбулентность на рынке труда. Особую значимость приобретает вектор на мультидисциплинарную конвергенцию и синергию, что позиционирует ИИ не как изолированный технологический феномен, а как стратегический драйвер достижения просоциального баланса и общественного блага.

Принятая в 2023 г. Египетская хартия ответственного искусственного интеллекта (Egyptian Charter for Responsible AI)[137] определяет основополагающие положения и рекомендации, распространяющиеся на всех участников отношений по развитию и внедрению ИИ.

Государства БРИКС, за исключением Ирана, имеют утвержденные или проектируемые документы стратегического планирования касательно национального развития технологий ИИ:

---

[134] URL: https://www.tcs.com/content/dam/tcs/pdf/Services/Analytics-Insights/Insights/sustainable-ethical-trustworthy-ai-solutions.pdf (дата обращения: 17.11.2023).

[135] URL: https://cset.georgetown.edu/publication/artificial-intelligence-standardization-white-paper-2021-edition/ (дата обращения: 11.07.2024); См. также: Цифровое право: учебник. 2-е издание, перераб. и доп. М.: Проспект, 2025. С. 280 – 281.

[136] URL: https://www-pre.baai.ac.cn/news/beijing-ai-principles-en.html (дата обращения: 12.10.2023).

[137] https://aicm.ai.gov.eg//en/Resources/EgyptianCharterForResponsible_AIEnglish-v1.0.pdf (дата обращения: 12.10.2023).

- План развития искусственного интеллекта следующего поколения (A Next Generation Artificial Intelligence Development Plan)[138] (Китай, 2017);

- Национальная стратегия ОАЭ в области ИИ до 2031 года (UAE National AI Strategy 2031)[139] (ОАЭ, 2019);

- Национальная стратегия развития ИИ (National Strategy For Artificial Intelligence #AIforAll)[140] (Индия, 2018);

- Стратегия Саудовской Аравии в области ИИ (Saudi Arabia's National AI Strategy - Vision 2030)[141] (Саудовская Аравия, 2019);

- Национальная стратегия ИИ (Egypt National Artificial Intelligence Strategy)[142] (Египет, 2021);

- Стратегия Бразилии в области искусственного интеллекта (BSAI/EBIA)[143] (Бразилия, 2021);

- Национальная политика в области искусственного интеллекта (Ethiopian National AI Policy)[144] (Эфиопия, 2024);

- Национальная стратегия развития цифровых и будущих навыков (National Digital and Future Skills Strategy South Africa)[145] (ЮАР, 2020);

- Национальная стратегия развития ИИ в Индонезии на период 2020 - 2045 годов (Strategi Nasional Kecerdasan Artifisial Indonesia)[146] (Индонезия, 2020).

В ряде вышеуказанных стратегиях предусматривается в качестве одного из ключевых направлений государственной политики разработка и совершенствование нормативно-правовой базы для обеспечения эффективной

---

[138] URL: https://chinacopyrightandmedia.wordpress.com/2017/07/20/a-next-generation-artificial-intelligence-development-plan/ (дата обращения: 23.05.2024).

[139] URL: https://ai.gov.ae/wp-content/uploads/2021/07/UAE-National-Strategy-for-Artificial-Intelligence-2031.pdf (дата обращения: 19.07.2023).

[140] URL: https://indiaai.gov.in/research-reports/national-strategy-for-artificial-intelligence (дата обращения: 30.06.2023).

[141] URL: https://oecd.ai/en/dashboards/policy-initiatives/http:%2F%2Faipo.oecd.org%2F2021-data-policyInitiatives-26017 (дата обращения: 18.07.2023).

[142] URL: https://andp.unescwa.org/sites/default/files/2021-11/Publications_672021000_Egypt-National-AI-Strategy-English.pdf (дата обращение: 24.10.2023).

[143] URL:https://www.gov.br/mcti/pt-br/acompanhe-o- mcti/transformacaodigital/arquivosinteligenciaartificial/ebia-summary_brazilian_4-979_2021.pdf (дата обращения: 24.10.2023).

[144] URL: https://aii.et/the-council-of-ministers-unanimously-decide-to-implement-the-national-artificial-intelligence-policy/ (дата обращения: 13.01.2025).

[145] URL: https://www.gov.za/sites/default/files/gcis_ document/202009/43730gen513.pdf (дата обращения: 13.10.2023).

[146] URL: https://ai-innovation.id/images/gallery/ebook/stranas-ka.pdf (дата обращения: 13.01.2025).

работы с данными и ИИ. В частности, Бразилия признает в качестве стратегического действия следующее: «обозначить нормативные барьеры на пути развития ИИ в Бразилии и определить аспекты бразильского законодательства, которые могут потребовать обновления, чтобы способствовать большей правовой определенности для цифровой экосистемы.»[147].

Рассмотрим состояние нормативно-правовой базы стран БРИКС в сфере развития информационно-коммуникационных технологий, к которым относятся и методы ИИ.

Так, нормативные правовые акты о защите персональных данных, об электронной подписи приняты во всех государствах – участников БРИКС. Правда, в Иране отсутствует унифицированный законодательный акт о защите данных, однако в ряде законов и нормативных актов содержатся положения о защите данных. Проект закона Ирана о безопасности персональных данных и защите разработан в 2019 году и до настоящего времени не принят.

Также приняты нормативные правовые акты в сфере цифровизации и обеспечения информационной безопасности, в том числе законы «О цифровой идентификации» (Эфиопия, 2023)[148] и «О допуске и контроле продуктов информационных технологий» (Эфиопия, 2023)[149], Положение «Об управлении Deep Synthesis технологиями на информационных сервисах в Интернете» (Китай, 2022)[150].

Можно утверждать, что в странах БРИКС сформирована достаточная правовая основа (как на уровне стратегических документов, так и нормативных правовых актов) для разработки специального правового регулирования отношений по использованию цифровых технологий ИИ.

---

[147] *Васин Е.О., Гвоздырева А.Д., Дейнека А.П., Замулина А.Ю., Кривошеева А.В., Незнамов А.В., Фокина С.А., Чаче Э.Г., Черемных И.А., Чурилова Д.Ю.* Глобальный атлас регулирования искусственного интеллекта. Вектор БРИКС / под ред. А.В. Незнамова. 3-е изд., перераб. и доп. // СПС «КонсультантПлюс». 2024.

[148] Digital ID Proclamation № 1284/2023, 2 July 2023. URL: https://www.lawethiopia.com/index.php/volume-3/6967- digital-id-proclamation-no-1284-2023 (дата обращения: 25.10.2024).

[149] Information Technology Products Security Clearance and Control Proclamation. URL: https://lawethiopiacomment.wordpress.com (дата обращения: 15.03.2024).

[150] URL: https://digichina.stanford.edu/work/translation-internet-information-service-deep-synthesis-management-provisions-draft-for-comment-jan-2022/ (дата обращения: 15.03.2024).

Согласно Пекинской Декларации XIV саммита БРИКС (23 июня 2022 года)[151] страны-участники объединения БРИКС солидарны в стремлении обмениваться информацией и сотрудничать в области технологий ИИ в целях усиления доверительного и безопасного взаимодействия государств, а также открытого и ответственного развития доверенного ИИ, который необходимо применять в общественных интересах. Также зафиксирована обеспокоенность указанных государств угрозами от использования ИИ (дискриминационные риски, рост безработицы и др.).

На XV саммите БРИКС в Йоханнесбурге (ЮАР, август 2023) Китай призвал создать общую структуру управления ИИ для выработки единого подхода к использованию и контролю технологий ИИ. Как заявил Председатель КНР Си Цзиньпин, «(необходимо) продолжить расширять сотрудничество в области искусственного интеллекта, усилить обмен информацией и техническое сотрудничество, совместно работать по предотвращению рисков, на основе широкого консенсуса сформировать структуру управления искусственным интеллектом и стандартов»[152].

Представляется, что общая структура управления ИИ БРИКС будет включать в себя:

- Институт будущей сети БРИКС (ИБСБ), в рамках которого функционирует Рабочая группа по ИИ, нацеленная на важнейшие технологии, алгоритмы, стандарты и сферы применения ИИ[153];

- Исследовательский комитет БРИКС, одной из задач которого являются мониторинг и анализ достижений в области ИИ[154];

- Рабочая группа «Этика новых технологий».

Ожидается создание новых рабочих групп БРИКС, в том числе по внедрению ИИ, по созданию моделей правового регулирования ИИ.

---

[151] URL: http://www.kremlin.ru/supplement/5819 (дата обращения: 25.10.2023).

[152] URL: https://rfi.mnr.gov.ru/news/Mass_media_about_digitalization/si-tszinpin-prizval-briks-sformirovat-obshchuyu-strukturu-upravleniya-ii (дата обращения: 01.10.2023).

[153] https://www.bifn.org/ru/study_groups/ai_sg.html (дата обращения: 15.10.2024)

[154] https://news.rambler.ru/tech/52853325-razvitie-tehnologiy-i-iskusstvennogo-intellekta-v-stranah-briks/?ysclid=msa1tio99s643549087 (дата обращения: 15.10.2024)

Предполагается, что общая структура управления ИИ БРИКС будет выполнять функции по проведению оценки инновационных разработок на основе ИИ и выдаче заключений, в каких отраслях и какой аудитории можно использовать конкретное технологичное решение; по разработке проектов соглашений БРИКС по вопросам применения ИИ.

В качестве ожидаемых результатов работы рассматриваемой общей структуры видится следующее:

- принятие странами БРИКС добровольного согласованного решения об отказе от технологий ИИ, созданных для принудительного влияния на подсознание людей и дипфейков, от систем биометрического распознавания, работающих в режиме реального времени для тотального слежения;

- согласование странами БРИКС условий использования некоторых технологий ИИ, например генеративного ИИ и Большой языковой модели;

- выработка унифицированных принципов предоставления доступа разработчиков систем ИИ к государственным данным.

Европейский опыт регулирования отношений по разработке и использованию технологий ИИ рассмотрим на примере Регламента (ЕС) 2024/1689 Европейского парламента и Совета от 13 июня 2024 года, устанавливающего гармонизированные правила об искусственном интеллекте (далее – Регламент)[155].

Структура Регламента включает в себя вводную часть, состоящую из 180 пунктов, и основную часть (13 глав и 13 приложений). Сложная, разветвленная структура Регламента обусловлена его комплексным характером регулирования, направленным на повышение функционирования внутреннего рынка ЕС посредством единой правовой базы, в том числе для разработки, продвижения на

[155] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act): URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng (дата обращения: 02.08.2024).

рынке, использования систем ИИ, в соответствии с ценностями ЕС, а также на способствование внедрению человекоцентричного и доверенного ИИ.

Регламент регулирует применение систем и моделей ИИ:

- определенных Регламентом систем искусственного интеллекта (в частности, системы ИИ, предназначенные для непосредственного взаимодействия с физическими лицами);

- система ИИ с высоким уровнем риска (например, системы ИИ, предназначенные для использования государственными органами или от имени государственных органов для оценки права физических лиц на получение основных льгот и услуг в рамках государственной помощи, включая медицинские услуги, а также для предоставления, сокращения, отмены или аннулирования таких льгот и услуг);

- модель ИИ общего назначения (в т.ч. являющаяся частью системы ИИ);

- модель ИИ общего назначения с системными рисками.

Действие Регламента распространяется в полном объеме на все государства – члены Союза, которые не вправе вводить ограничения на разработку, маркетинг и использование систем ИИ, за исключением случаев, прямо разрешенных Регламентом.

Из сферы действия Регламенты исключены системы ИИ для военных целей, обороны и национальной безопасности государства; системы ИИ только для научных исследований и разработок; иные указанные прямо в Регламенте.

Регламент определяет некоторые используемые понятия, в том числе «система ИИ» и «развертыватель» (deployer).

Система ИИ раскрывается через категорию машинной системы, предназначенной для работы с различными уровнями автономии и проявляющая адаптивность после развертывания, то есть такая система способна для достижения явных или неявных целей делать выводы из получаемых входных данных, генерировать выходные данные, такие как прогнозы, контент, рекомендации или решения, которые могут повлиять на физическую или виртуальную окружающую среду.

Рассматриваемым законом ЕС обозначена позиция о квалификации ИИ в качестве инструмента для людей, который должен быть ориентирован на человека. Можно предположить, что Регламент однозначно не считает возможным признавать правосубъектность за системами ИИ.

Применительно к теме настоящего диссертационного исследования представляет интерес следующий субъект, предусмотренный Регламентом: «развертыватель» (deployer). Таким субъектом права является лицо (физическое или юридическое лицо, государственный орган, агентство или иная организация), использующее систему ИИ в рамках своих полномочий, за исключением случаев, когда система ИИ используется в ходе личной непрофессиональной деятельности. Представляется, что орган государственного контроля (надзора), использующий технологию ИИ, является таким развертывателем согласно Регламенту.

Регламентом установлена обязанность развертывателей высокорисковых систем ИИ принимать меры для обеспечения, в максимальной степени, достаточного уровня грамотности в области ИИ своих сотрудников и других лиц, занимающихся эксплуатацией и использованием систем ИИ от их имени, принимая во внимание их технические знания, опыт, образование и подготовку, а также контекст, в котором используются системы ИИ. Такая обязанность следует из того, системы ИИ с высоким риском должны находиться под надзором человека согласно статье 14 Регламента, что безусловно требует надлежащего уровня подготовки и грамотности ответственного сотрудника развертывателя.

В статье 5 Регламента установлен перечень запрещенных методов ИИ, в том числе воздействующие на подсознание человека, недоступные его сознанию, целенаправленные манипулятивные или вводящие в заблуждение методы.

Регламентом предусмотрено специальное регулирование в отношении систем ИИ с высокой степенью риска (high-risk AI systems), перечень которых приведен в статье 6 и Приложении III к Регламенту. Установлены требования к таким системам (раздел 2 главы 3 Регламента), в частности, об утверждении и поддержке в актуальном состоянии системы управления рисками, под которой законом понимается непрерывный и повторяющийся процесс, планируемый и

выполняемый на протяжении всего жизненного цикла высокорисковой системы ИИ , требующий регулярного систематического анализа и обновления.

Системы ИИ с высоким уровнем риска должны сопровождаться инструкциями по использованию, содержащими краткую, полную, корректную и четкую информацию, которая должна быть актуальной, доступной и понятной для развертывателей (deployers).

Предусмотрены Регламентом обязательства поставщиков, развертывателей, импортеров, дистрибьюторов высокорисковых систем ИИ.Так, согласно статье 49 Регламента перед выпуском на рынок или вводом в эксплуатацию системы ИИ, указанной в Приложении III к Регламенту, за исключением высокорисковых систем ИИ – компонентов безопасности при управлении и эксплуатации критической цифровой инфраструктуры, дорожном движении или при подаче воды, газа, отопления или электричества, поставщик или уполномоченный представитель поставщика должен зарегистрировать себя и свою систему ИИ в базе данных ЕС, указанной в статье 71 Регламента.

Для определенных систем ИИ предусмотрены обязательства поставщиков и развертывателей по обеспечению прозрачности (статья 50 Регламента). В частности, поставщики систем ИИ, генерирующих синтетический аудио-, графический, видео- или текстовый контент, должны обеспечить, чтобы выходные данные системы ИИ были помечены в машиночитаемом формате и определялись как искусственно созданные или обработанные.

Применительно к моделям ИИ общего назначения:

- предусмотрена классификация моделей общего назначения с системным риском (статья 51 Регламента);

- установлены обязательства поставщиков моделей ИИ общего назначения, требования к уполномоченным представителям указанных поставщиков (статьи 53, 54 Регламента);

- установлены обязательства поставщиков моделей ИИ общего назначения с системным риском (статья 55 Регламента);

- ведение кодексов практики (статья 56 Регламента).

Определены меры по поддержке инноваций (глава 6 Регламента) в виде регуляторных «песочниц», мер для малых и средних предприятий, стартапов.

Определена система управления ИИ с двумя уровнями: Евросоюз (ЕС) и национальное государство в составе ЕС.

На уровне ЕС предусмотрены Офис ИИ и Европейский совет по ИИ, Консультативный форум, научная группа независимых экспертов.

На уровне государств – членов ЕС: национальные компетентные органы (уведомляющие органы и органы по надзору за рынком для целей Регламента).

Регламент предусматривает мониторинг после выхода на рынок со стороны поставщиков систем ИИ высокого риска, обмен информацией о серьезных инцидентах, контроль и надзор за системами ИИ на европейском рынке.

Касательно ответственности Регламент предусматривает обязанность государств-членов ЕС установить правила о штрафах и других принудительных мерах, которые могут также включать предупреждения и неденежные меры, применимые к нарушениям Регламента операторами, и должны принять все необходимые меры для обеспечения того, чтобы они применялись надлежащим образом. Несоблюдение запрета на использование методов ИИ, упомянутых в статье 5 Регламента, влечет наложение административного штрафа в размере до 35 000 000 евро или, если нарушителем является предприятие, до 7% от его общего годового оборота по всему миру за предыдущий финансовый год, в зависимости от того, что больше. Нарушение иных требований Регламента влечет наложение административного штрафа в размере до 15 000 000 евро или, если нарушителем является предприятие, до 3% от его общего годового оборота по всему миру за предыдущий период. финансовый год, в зависимости от того, что больше.

На основании рассмотренной в настоящем параграфе информации сделаем следующие выводы:

1. Рассмотренный зарубежный опыт регулирования ИИ позволяет утверждать, что государства солидарны в признании необходимости человеко-ориентированного подхода в правовом регулировании отношений в сфере систем ИИ.

2. Унифицированное правовое регулирование отношений по использованию технологий ИИ в контрольно-надзорной деятельности государственных органов практически отсутствует в законодательстве государств БРИКС и в Регламенте (ЕС) 2024/1689 Европейского парламента и Совета от 13 июня 2024 года.

§ 2.3. Цели и принципы правового регулирования отношений по применению искусственного интеллекта при осуществлении государственного контроля (надзора)

Концепция совершенствования контрольной (надзорной) деятельности до 2026 года (далее – Концепция)[156] предполагает внедрение цифровых инструментов в указанную функцию государственного управления. В частности, предусматривается дистанционное подтверждение устранения выявленных нарушений[157]. Вместе с тем в российском законодательстве, в том числе в Законе № 248-ФЗ, в настоящее время отсутствуют правовые нормы, регулирующие общественные отношения, связанные с применением цифровых технологий в рамках контрольно-надзорной деятельности.

О необходимости единой системы правового регулирования цифровых технологий государственного и общественного контроля (далее – контроль) справедливо заявлено С.М. Зубаревым[158]. Элементами указанной системы, по мнению ученого, являются:

- общественные отношения по организации и осуществлению контроля, по применению цифровых технологий уполномоченными субъектами контроля;
- методы правового регулирования: императивный и диспозитивный методы;
- принципы правового регулирования;

---

[156] Утв. распоряжением Правительства РФ от 6 октября 2021 г. № 2816-р «Об утверждении перечня инициатив социально-экономического развития Российской Федерации до 2030 года» // Собрание законодательства РФ. 2021. № 41. Ст. 7051.

[157] См.: *Лагаева В. П.* Правовое регулирование применения искусственного интеллекта в профилактике нарушений обязательных требований // Аграрное и земельное право. 2024. № 7(235). С. 95-98.

[158] *Зубарев С.М.* О единой системе правового регулирования цифровых технологий государственного и общественного контроля // Законы России: опыт, анализ, практика. 2021. № 11. С. 29 -37.

- стратегическая цель – формирование нормативной базы, позволяющей субъектам контроля эффективно и качественно применять цифровые технологии;

- субъект правового регулирования цифровых технологий контроля;

- механизм правового регулирования (правовые нормы, правовые отношения и акты реализации прав и обязанностей[159]).

Однако предусмотренные Законом № 248-ФЗ положения, касающиеся информационного обеспечения ГКН, ограничиваются определением видов информационных систем и регламентацией информационного взаимодействия органов контроля (надзора) с контролируемыми лицами и с иными государственными органами. На уровне подзаконных нормативных правовых актов о видах ГКН, о функционировании информационных систем ГКН также не содержатся требования к информационным технологиям, применяемым органами контроля (надзора).

Введение правового регулирования общественных отношений по применению органами контроля (надзора) технологий ИИ призвано восполнить указанный выше пробел и достичь следующих целей:

- обеспечение эффективности государственного контроля (надзора);

- сокращение нагрузки на добросовестных контролируемых лиц;

- цифровая трансформация сферы государственного контроля (надзора).

Эффективность ГКН существенно возрастает благодаря способности технологий ИИ обрабатывать значительные массивы данных. Применение методов ИИ обеспечивает сплошной, точный и детальный анализ информации, поступающей в контрольные (надзорные) органы в отношении контролируемых лиц и объектов, что позволяет в том числе автоматизировать процесс отнесения к категориям риска. В этой связи контрольные (надзорные) мероприятия могут проводиться эффективно, а именно только в случаях нарушений или наличия высокой степени угрозы несоблюдения обязательных требований.

---

[159] *Зубарев С.М.* О единой системе правового регулирования цифровых технологий государственного и общественного контроля // Законы России: опыт, анализ, практика. 2021. № 11. С. 29 -37.

Как отмечает А.В. Мартынов, технологии ИИ способны значительно повысить результативность профилактической деятельности контрольно-надзорных органов исполнительной власти, в том числе в части анализа восприятия контролируемыми лицами обязательных требований[160].

Использование в личном кабинете контролируемого лица в информационных системах ГКН методов ИИ для категорирования объектов контроля в порядке, установленном нормативными правовыми актами в области ГКН, обеспечивает оперативное информирование такого лица о присвоенной ему или его объекту контроля категории риска. Внедрение органами контроля (надзора) интеллектуальных систем для автоматизированного расчета категории риска будет способствовать соблюдению ими установленных сроков принятия решений о категорировании.

Нормативные правовые акты как ключевые инструменты правового регулирования, образующие механизм правового регулирования[161], призваны обеспечить правовую основу для постепенной и эффективной цифровой трансформации ГКН.

Достижение вышеуказанных целей должно основываться на принципах нормативно-правового регулирования общественных отношений, возникающих в связи с использованием ИИ в ГКН. Справедливо отмечено учеными – правоведами, что основополагающие положения выполняют «роль направляющего вектора для законодателя»[162].

Принципы правового регулирования применения ИИ в государственном контроле (надзоре) могут быть распределены по категориям общих и специальных, равно как и принципы информационного и цифрового права[163].

---

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

[161] *Исаков В. Б.* Механизм правового регулирования и правовые режимы // Проблемы теории государства и права / Под ред. С. С. Алексеева. М.: Высшая школа, 1987. С. 261.

[162] *Добробаба М.Б., Чаннов С.Е., Минбалеев А.В.* Квантовые коммуникации: перспективы правового регулирования // Вестник Университета имени О.Е. Кутафина (МГЮА). 2022. № 4 (92). С. 31.

[163] *Минбалеев А. В.* Проблемы цифрового права: Учебное пособие. Саратов: Амирит, 2022. С. 37 – 38; *Минбалеев А. В.* Принципы информационного права // Вестник ЮУрГУ. Серия: Право. 2015. № 1. С. 80.

К общим принципам, регулирующим в целом общественные отношения по использованию ИИ и являющихся актуальными для сферы ГКН, можно отнести следующие из предусмотренных и раскрытых в Национальной стратегии развития искусственного интеллекта на период до 2030 года и Кодексе этики в сфере ИИ:

человеко-ориентированный и гуманистический подход;

уважение автономии и свободы воли человека;

соответствие закону;

недопустимость дискриминации по признакам расовой, национальной, половой принадлежности, политических взглядов, религиозных убеждений, возраста, социального и экономического статуса или сведений о частной жизни;

оценка потенциальных рисков применения искусственного интеллекта;

ответственное отношение участников отношений в сфере искусственного интеллекта к вопросам влияния искусственного интеллекта на общество и граждан;

непричинение вреда жизни и (или) здоровью человека, имуществу граждан и юридических лиц, окружающей среде;

информирование пользователей об их взаимодействии с технологиями искусственного интеллекта и обеспечение возможности прекращения такого взаимодействия по желанию пользователя;

безопасность работы с данными;

информационная безопасность.

В качестве элементов целеполагания[164] к специальным принципам правового регулирования общественных отношений по применению ИИ при осуществлении ГКН предлагается отнести следующие:

сочетание правового и технического регулирования;

прозрачность применения искусственного интеллекта органами контроля (надзора);

---

[164] *Сивицкий В. А.* Принцип системности законодательства и его влияние на использование в федеральных законах принципов регулирования отношений в конкретных сферах // Юридическая техника. 2020. № 14. С. 305 - 307.

приоритет использования искусственного интеллекта в профилактической деятельности органов контроля (надзора);

обеспечение возможности прекращения взаимодействия контролируемого лица с системой искусственного интеллекта по желанию такого лица;

недискриминационный доступ к государственным данным для разработчиков систем искусственного интеллекта;

ответственность органа контроля (надзора) за нарушение прав и законных интересов контролируемых лиц в результате применения искусственного интеллекта.

Рассмотрим подробно каждый специальный принцип.

Принцип сочетания нормативно-правового регулирования и технического регулирования (стандарты и др.)[165] предусматривает обязательное привлечение экспертов в сфере информатики в том числе к разработке проектов нормативных правовых актов, регламентирующих применение технологий ИИ в контрольно-надзорной деятельности. Кроме того, учитывая, что не все понятия возможно определить в законе и (или) подзаконных нормативных правовых актах, то важно использовать определения (дефиниции), предусмотренные в документах технического регулирования, например, в отношении «информационного ресурса», «данных». В ряде случаев важно учитывать как легальную дефиницию понятия, так и его определение в стандартах, технических регламентах, что применимо, в частности, к «информационным системам».

При этом необходимо обеспечить, чтобы нормативные правовые акты и документы технического регулирования не противоречили друг другу, что позволит осуществлять сбалансированное и согласованное регулирование общественных отношений по применению искусственного интеллекта при осуществлении ГКН.

С обеспечением предусмотренных Законом № 248-ФЗ открытости и доступности информации об организации и осуществлении ГКН связан следующий специальный принцип прозрачности применения ИИ органами

---

[165] См.: *Талапина Э. В.* Сравнительное цифровое право: становление и перспективы // Журнал российского права. 2021. № 9. С. 18 - 32.

надзора. Для неопределенного лица круга лиц, в том числе контролируемых лиц, должна быть доступна информация об использовании методов и систем ИИ в контрольно-надзорной деятельности, за исключением случаев, установленных в статье 13 Закона № 248-ФЗ в целях защиты охраняемой законом тайны и прав, законных интересов и безопасности контролируемых и иных лиц, а также их чести, достоинства, деловой репутации.

Рассматриваемый принцип может быть реализован в том числе посредством установления требования указывать в положениях об информационных системах ГКН используемые в них методы ИИ. Также целесообразно предусмотреть обязательную маркировку информационного материала и документов, созданных с применением ИИ органом надзора. При взаимодействии с контролируемым лицом важно предварительно уведомить его представителя или работника, что с ним общается не инспектор, а голосовой помощник. Необходимость информировать про конкретную модель ИИ, его разработчика требуется для подтверждения того, что применяемый ИИ является доверенной технологией.

Исходя из важного правового принципа строгого соблюдения прав и личных интересов человека в информационном обмене[166] предлагается на уровне закона прямо установить право контролируемых лиц на получение от органа контроля (надзора) актуальной и достоверной информации об использовании технологий ИИ при проведении им профилактических и (или) контрольных (надзорных) мероприятий, в том числе информации о факте использования искусственного интеллекта; о категории данных, обрабатываемых искусственным интеллектом.

В настоящее время предусмотренное статьей 10.2-2 Федерального закона «Об информации, информационных технологиях и о защите информации» требование информировать пользователей о применении рекомендательных технологий, являющихся методами ИИ, на сайте, странице сайта и (или) ИС и (или) программе для ЭВМ не распространяется в силу прямого указания закона на государственные органы, в том числе на органы контроля (надзора). Такой исключительный подход

[166] *Рассолов М. М.* Информационное право. М.: Юристъ, 1999. С. 25.

не учитывает необходимость обеспечения информационных прав граждан и организаций. Как верно отмечено А.В. Мартыновым и М.В. Бундиным, «любое принятое с помощью ИИ решение должно быть обеспечено рациональным объяснением в форме, понятной человеку»[167].

Предусмотренная Законом № 248-ФЗ необходимость стимулирования добросовестного соблюдения обязательных требований приводит к принципу приоритетности использования ИИ в целях профилактики нарушений обязательных требований, что предполагает первоочередное применение интеллектуальных технологий для выявления причин и условий, способствующих противоправному поведению контролируемых лиц, а также для прогнозирования рисков несоблюдения обязательных требований.

В настоящее время наоборот наблюдается расширение области применения рассматриваемой сквозной технологии в проверках, а не в превентивных мерах. Реализация рассматриваемого специального принципа призвана изменить вектор использования ИИ в сфере ГКН в сторону профилактики, что может привести к качественному повышению уровня информированности контролируемых лиц и потребителей об установленных законом условиях ведения экономической и иной деятельности.

Принцип обеспечения возможности прекращения взаимодействия контролируемого лица с системой ИИ по желанию такого лица позволяет учитывать разные уровни освоения цифровых технологий участниками правоотношений в области ГКН. Кроме того, допустимо, что живое общение с должностным лицом способно принести больше пользы и достичь понимания, чем многократное прослушивание или просматривание информации, предоставляемой интеллектуальным сервисом. Особенно рассматриваемое положение актуально для случаев применения ИИ органом надзора для проведения такого профилактического мероприятия, как консультирование.

---

[167] *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. 65.

Принцип недискриминационного доступа к государственным данным для разработчиков систем ИИ обеспечивает конкуренцию среди поставщиков интеллектуальных сервисов, что позволит органам надзора применять современные и эффективные программные решения для предупреждения, выявления и пресечения нарушений обязательных требований. Обеспечить равное положение разработчиков возможно посредством установления Правительством Российской Федерации правил недискриминационного доступа к государственным данным, под которыми в настоящей работе понимаются данные, обрабатываемые в информационных система ГКН и входящие в наборы данных, формируемые органами надзора в том числе в рамках программ по цифровой трансформации ГКН, с соблюдением установленных законом ограничений и запретов по обороту сведений.

Принцип ответственности органов контроля (надзора) за нарушение прав и законных интересов контролируемых лиц в результате применения ИИ прямо следует из отнесения ИИ к средствам контроля, а не к категории субъектов контрольно-надзорных правоотношений. Вне зависимости от того, применялся ИИ или нет, орган надзора и его должностные лица являются ответственными в случае ненадлежащего исполнения закона, в том числе за несоблюдение сроков ответа на обращения или жалобы, за выдачу предписания, не соответствующего требованиям законодательства РФ.

При оценке результативности и эффективности деятельности органов надзора применение цифровых интеллектуальных сервисов не может являться обстоятельством, позволяющим не учитывать отрицательные результаты такой оценки.

Рассматриваемый специальный принцип позволяет обеспечить законные гарантии и защиту прав контролируемых лиц, а также надлежащую проверку органом надзора результатов, полученных посредством ИИ.

Правовое регулирование общественных отношений, складывающихся в связи с внедрением ИИ в сферу государственного контроля (надзора), должно

обеспечивать разумный баланс интересов трех сторон: контрольных (надзорных) органов, контролируемых субъектов, а также потребителей товаров, работ и услуг.

Как верно подмечено Н.А. Дмитрик, «правовое измерение цифровой экономики — это измерение интересов ее участников с целью нахождения баланса между ними и путей устранения правового неравенства, вызванного доступностью или недоступностью новых технологий»[168].

Интерес надзорных органов во внедрении ИИ в свою профилактическую деятельность заключается в том, чтобы контролируемым лицам и потребителям была доступна оперативно ясная и полная информация об обязательных требованиях, в том числе разъяснения, поскольку в таком случае повышается вероятность сокращения нарушений. Для сбалансированного подхода важно обеспечить право контролируемых лиц и потребителей знать, что доводимая до их сведения вышеуказанная информация подготовлена с применением алгоритмов на основе раскрытых органом надзора источников данных, чтобы такая информация могла быть перепроверена и уточнена.

Таким образом, стратегическое направление Российской Федерации на цифровизацию государственного контроля (надзора) важно обеспечить правовым механизмом реализации посредством установления федеральными законами целей и принципов правового регулирования отношений по применению технологий ИИ при осуществлении указанной функции государственного управления.

[168] *Дмитрик Н.А.* Цифровая трансформация: правовое измерение // Правоведение. 2019. Т. 63. № 1. С. 44.

ГЛАВА 3. Проблемы и приоритеты правового регулирования применения искусственного интеллекта при осуществлении государственного контроля (надзора)

§ 3.1. Проблема правосубъектности искусственного интеллекта

В настоящее время одним из активно обсуждаемых вопросов является правовой статус систем ИИ (СИИ), а именно отнесение таких систем к субъектам права.

По мнению Р.В. Амелина и С.Е. Чаннова, причиной научной дискуссии, обозначенной выше, является «автономность рассматриваемых систем, понимаемая в контексте возможности осуществления функций, ради которых они созданы, в течение более или менее длительного времени без участия человека»[169].

Также вследствие самообучаемости СИИ, необъяснимости их решений указанные авторы выделяют невозможность предвидеть действия СИИ, в связи с этим «объективно отсутствует субъект, который мог или должен был предвидеть последствия действий системы в конкретных обстоятельствах»[170], следовательно, затруднительно применение традиционного механизма юридической ответственности к рассматриваемым цифровым технологиям[171].

Представляет интерес **философский взгляд** на рассматриваемое понятие. По мнению В.М. Сергеева, «Искусственный интеллект – это «мир мыслей», воплощенных в техническом устройстве»[172]. При этом опыт создания программ ИИ является экспериментальной возможностью разрешить философские вопросы о природе разума[173]. Как указано К.В. Исаковой, «с философской точки зрения, в системе "машина-человек" мышлением обладает только человек, все проявления

---

[169] *Амелин Р.В., Чаннов С.Е.* Эволюция права под воздействием цифровых технологий. М.: НОРМА, 2023. С. 179.

[170] *Амелин Р.В., Чаннов С.Е.* Указ. соч. С. 179.

[171] См., например: *Апостолова, Н.Н.* Ответственность за вред, причиненный искусственным интеллектом // Северо-Кавказский юридический вестник. 2021. № 1. С. 112 – 119.

[172] *Сергеев В.М.* Искусственный интеллект: опыт философского осмысления // Будущее искусственного интеллекта. М.: Наука, 1991. С. 231.

[173] *Сергеев В.М.* Указ. соч. С. 236.

сознания у машины – это проявление мыслительной деятельности человека, её создателя»[174].

В психологии отмечается неадекватность термина ИИ[175], который рассматривается как подмена одной реальности другой, поскольку не прослеживается связь между достижениями вычислительной техники и интеллектом. В подтверждение вышеуказанного подхода приводятся в качестве примера молоток, топор, отвертка, пила, которые не называются человеческой рукой, человеческим действием, поскольку указанные предметы являются ручным инструментом, орудийным действием человека. Противники термина ИИ считают правильным такой же подход применять в случае с интеллектом, «со сложнейшей формой человеческой деятельности». По их мнению, компьютер следовало бы называть не ИИ, а инструментом интеллектуального воздействия, или инструментом интеллекта, который может существенно облегчать, ускорять, повышать точность принятия решения (к сожалению, в том числе неправильного решения).

По мнению В.П. Зинченко, идеи об общности, или близости, работы компьютера и человеческого интеллекта основаны либо на пренебрежении психологической реальностью, либо на смешении предметов изучения психологии и логики[176], поскольку ЭВМ может имитировать лишь самую незначительную часть не умственных способностей человека как целого, а лишь одного из компонентов этих способностей, а именно операционально-технический компонент.

О.К. Тихомиров полагает, что «… между существующими искусственными системами и человеческой интеллектуальной деятельностью существуют качественные различия и что поэтому выражение «искусственный интеллект» следует воспринимать как метафору»[177].

---

[174] *Исакова К.В.* Проблемы философии искусственного интеллекта // Гуманитарный научный журнал. 2022. № 2. С. 127.

[175] Искусственный интеллект и парадоксы психологии // В.П. Зинченко. Будущее искусственного интеллекта. М.: Наука, 1991. С. 186.

[176] *Зинченко В.П.* Указ. соч. С. 187.

[177] *Тихомиров О.К.* Искусственный интеллект: взгляд психолога // Будущее искусственного интеллекта. М.: Наука, 1991. С. 193.

Как считает С.С. Лавров, слово «интеллект» в термине ИИ «отражает тот непреложный факт, что ЭВМ помогает человеку именно в его интеллектуальной, а не в какой-то иной деятельности. (…) они обрабатывают данные – знаки и символы, а вместе с тем заключенную в этих данных информацию. В этом – а на обозримое будущее только в этом – работа ЭВМ интеллектуальна»[178].

Правовые аспекты систем ИИ являются предметом пристального изучения теории государства и права, науки информационного права, гражданско-правовой, административно-правовой, уголовно-правовой и иных отраслей юридической науки.

Способность технологий ИИ имитировать когнитивные и коммуникативные способности человека и его эмпатию, а также саморазвиваться и самообучаться вызывает научные дискуссии о правосубъектности ИИ. Верно подмечено Ю.В. Волковым, что «традиционное представление о правосубъектности (как юридическая конструкция с основными элементами правоспособность и дееспособность) уже не удовлетворяет многих современных исследователей и практиков»[179].

Имеются сторонники признания ИИ в качестве самостоятельного субъекта права, которого можно наделить юридическими правами и обязанностями и привлечь к юридической ответственности в отрыве от его создателя, разработчика или владельца соответствующего программного обеспечения. Но значительно больше противников такого подхода, считающих ИИ техническим и программным средством, за функционирование которого ответственность должны нести лица, создавшие указанное средство или использующие его в своих интересах[180].

По мнению Е.А. Певцовой, «…в правовом поведении искусственный интеллект в настоящее время заменяет исключительно техническую

---

[178] *Лавров С.С.* Интеллект искусственный и естественный // Будущее искусственного интеллекта. М.: Наука, 1991. С. 199.

[179] *Волков Ю. В.* Информационная правосубъектность // Теория государства и права. 2021. № 4 (25). С. 80.

[180] *Крысанова Н. В.* К вопросу о правосубъектности и правовом развитии искусственного интеллекта // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Серия 4. Государство и право: реферативный журнал. 2021. № 1. С. 25.

составляющую тех действий, операций, которые всегда производил человек»[181]. Ученый указывает на необходимость принятия Международной правовой конвенции о невозможности наделения систем искусственного интеллекта правосубъектностью.

Ученый - цивилист Л.Ю. Василевская полагает, что являются несостоятельными рассуждения о правосубъектности ИИ. По ее мнению, необходимо разграничить материальную (цифровую) форму ИИ и его материальный носитель, которым является любой овеществленный объект (например, беспилотное устройство, кардиостимулятор). В результате такого разграничения Л.Ю. Василевская относит ИИ к сложному объекту, к результату интеллектуальной деятельности (РИД), следовательно, на ИИ признается исключительное право на РИД. Отсюда следует ее вывод о том, что на современном этапе развития информационных технологий искусственный интеллект представляет собой сложное программирование, созданное человеком для решения конкретных поставленных задач[182].

На мой взгляд, выполнение роботизированными системами с элементами ИИ (интеллектуальные роботы), а также интеллектуальными системами ряда действий, которые законом отнесены к полномочиям органа по контролю (надзору) и его должностных лиц, является поводом для обсуждения юристами-учеными вопроса о правосубъектности ИИ, в том числе, для урегулирования юридической ответственности за убытки, причиненные такими роботами и системами.

Представляется, что среди всех рассматриваемых в настоящее время юридической наукой правовых аспектов использования ИИ вопрос о его правосубъектности носит краеугольный характер, поскольку понятие «субъект права» является "главным компонентом (подсистемой) и одновременно центром, ядром правовой системы"[183]. От решения этой правовой проблемы зависит

---

[181] *Певцова Е.А.* Влияние искусственного интеллекта на правовую деятельность человека // Журнал российского права. 2020. № 9. С. 27.

[182] *Василевская Л.Ю.* Искусственный интеллект: проблемы гражданско-правовой квалификации // Вестник Университета имени О.Е. Кутафина (МГЮА). 2023. № 5. С. 32-40.

[183] *Алексеев С.С.* Теория государства и права: Учебник. М., 2005. С. 446.

определение юридической ответственности и распределение прав и обязанностей между участниками правоотношений, связанных с применением рассматриваемых сквозных технологий.

Важно указать на проведенное В.В. Архиповым, В.Б. Наумовым теоретическое исследование аспектов воли и правосубъектности касательно направлений развития законодательства о роботехнике[184].

Р.В. Амелин и С.Е. Чаннов обоснованно проецируют различные подходы юридической науки к понятию «субъект права» на вопрос о правосубъектности ИИ[185].

Так, при формально-юридическом (позитивистском) понимании для признания робота или СИИ субъектом права достаточно того, что закон наделит их правосубъектностью или ее отдельными элементами в рамках любых правоотношений. При этом, по мнению А.А. Антонова, необходимо «законодательно разграничить искусственный интеллект на объекты интеллектуальной собственности, не способные принимать самостоятельные решения и обладающие автономным разумом, позволяющим создавать технически сложные устройства, обладающие возможностью причинения вреда окружающим и иным системам ИИ.»[186].

Но чтобы не допустить произвольного нормативно-правового регулирования, необходимо установить объективные критерии для такого наделения, его необходимость и целесообразность. По мнению указанных авторов, рассматриваемый подход носит прикладной характер, а в теоретическом плане он не способен раскрыть сущности вопроса о правосубъектности ИИ.

Антропоцентрическая теория допускает признание правосубъектности за объединениями людей. Очевидно, что такое понимание позволяет рассматривать

---

[184] *Архипов В.В., Наумов В.Б.* О некоторых вопросах теоретических оснований развития законодательства о робототехнике: аспекты воли и правосубъектности // Закон. 2017. № 5. С. 157 - 170.

[185] *Амелин Р.В., Чаннов С.Е.* Эволюция права под воздействием цифровых технологий. М.: НОРМА, 2023. С. 181 – 184.

[186] *Антонов А.А.* Искусственный интеллект: вопросы правосубъектности // Юрист. 2023. № 9. С. 23 - 28.

роботов и СИИ, не представляющих собой объединение людей, исключительно как объекты права, а не как новый вид юридического лица.

Последователи юснатуралистического подхода выделяют сущностные признаки субъекта права, среди которых важное значение имеет наличие воли. Согласно мнениям ряда специалистов сильный ИИ идентичен человеческому сознанию, он способен мыслить и осознавать себя, это «сам разум в том же смысле, что и в отношении человека»[187] и поэтому именно такой вид ИИ, появление которого в обозримом будущем представляется маловероятным, может быть субъектом права.

Однако по мнению ряда авторов классификация ИИ на слабый и сильный виды базируется на различии в «объемах и алгоритмах мощности цифровых технологий, и только поэтому вопрос о расширении границ правосубъектности, появления новых субъектов права в зависимости от объемов возможности техники не имеет под собой явных и достаточных оснований.»[188].

Как видим, ни один из рассмотренных научных подходов не позволяет признать субъектом права существующие в настоящее время интеллектуальные системы. По мнению Р.В. Амелина и С.Е. Чаннова, такие системы могут быть отнесены к квазисубъектам, то есть к правовым образованиям, наделенным законодателем правами и (или) обязанностями (в единстве с юридической ответственностью)[189]. Кроме того, указанные авторы считают правильным постановку «вопроса о правосубъектности робота (СИИ) в качестве принципиально нового образования "электронного лица", дополняющего физических лиц и "социальных лиц" в качестве субъекта права.»[190].

---

[187] *Витко В.* Анализ научных представлений об авторе и правах на результаты деятельности искусственного интеллекта // ИС. Авторское право и смежные права. 2019. № 2. С. 8. См. также: *Бахтеев Д.В.* Искусственный интеллект: этико-правовые основы: монография. М.: Проспект. 2021. С. 30-33.

[188] *Дьяконова М. О., Ефремов А. А., Зайцев О. А. [и др.].* Цифровая экономика: актуальные направления правового регулирования: научно-практическое пособие / Под ред. И. И. Кучерова, С. А. Синицына. М.: ИЗиСП, НОРМА, 2022. С. 163.

[189] *Амелин Р.В., Чаннов С.Е.* Эволюция права под воздействием цифровых технологий. М.: НОРМА, 2023. С. 190 – 192.

[190] *Амелин Р.В., Чаннов С.Е.* Указ. соч. С. 183 - 184. См. также: *Залоило М.В.* Искусственный интеллект в праве. М., 2021. С. 99.

Формально-юридический (позитивистский) подход, который, на мой взгляд, оптимально подходит к понятию «субъект административного права», позволяет на уровне закона закрепить правосубъектность ИИ, но возникает вопрос в обоснованности такого признания на уровне законодателя.

Справедливо мнение Е.В. Пономаревой о присущих правосубъектности автономии, независимости и свободы субъекта (в определенных границах), а сама необходимость контроля над деятельностью ИИ «не соответствует правовым качествам субъекта права»[191]. Согласно превалирующей позиции в административно-правовой науке субъектом является «физическое лицо или организация, которые в соответствии с действующим законодательством Российской Федерации могут быть участниками (сторонами) регулируемых административным правом управленческих общественных отношений»[192]. Субъект административного права наделяется правами, обязанностями, полномочиями, компетенцией, ответственностью, способностью вступать в административно-правовые отношения, то есть основными составляющими его административно-правового статуса являются административная правоспособность и административная дееспособность.

Различаются мнения ученых – административистов о соотношении понятий «субъект административного права» и «субъект административно-правовых отношений». Ю.М. Козлов считал, что «субъекты административного права становятся субъектами административных правоотношений тогда, когда они обладают способностью реализовать свою административную правоспособность в рамках конкретных административно-правовых отношений»[193]. Другие авторы отождествляют субъектов административного права с участниками административно-правовых отношений[194].

---

[191] *Пономарева Е. В.* Феномен квазисубъекта права: вопросы теории: Монография. М.: Юрлитинформ, 2020. С. 66 – 67. См. также: Проблемы развития и перспективы предпринимательского права в современных экономических условиях: Моногр. / Отв. ред. С.С. Занковский. М.: Проспект, 2021. С. 313-314.

[192] *Алехин А. П.* Административное право Российской Федерации: учебник. Ч. 1: Сущность и основные институты административного права / А. П. Алехин, Ю. М. Козлов. М.: ТЕИС, 1994. С. 34.

[193] Административное право Российской Федерации: учебник для бакалавров/отв. ред. Л. Л. Попов. М.: РГ-Пресс, 2015. 568 с.

[194] *Габричидзе Б.Н.* Административное право. М.: Велби, 2003. 480 с.

Представляется более обоснованным подход, разграничивающий рассматриваемые понятия по критерию наличия административной дееспособности. Действительно, категория субъекта административного права является общей и включает в себя как участников административных правоотношений (обладающих дееспособностью), так и иных субъектов, правовой статус которых не позволяет им выступать сторонами административных правоотношений. Можно утверждать, что понятия «субъект административного права» и «субъект административно-правового отношения» соотносятся между собой как общее и частное (специальное). Применительно к рассматриваемому вопросу о правосубъектности ИИ возможно заключить, что закон может признать ИИ субъектом административного права, но такое признание не означает, что ИИ автоматически становится стороной правоотношений в сфере государственного контроля (надзора), участниками которых в настоящее время выступают государственные органы, их должностные лица (инспекторы) и контролируемые лица.

Важно также обратить внимание на то, что ИИ («электронный инспектор») в случае признания его правосубъектности может рассматриваться как властный субъект административного права, каковым сейчас признаются орган исполнительной власти и его должностное лицо. Таким субъектом является субъект, обладающий определенными юридическими государственно-властными полномочиями по отношению к иным субъектам административного права. В сфере государственного контроля (надзора) к полномочиям властного участника правоотношения отнесены в том числе принятие решений в отношении контролируемого лица (о проведении проверки, о выдаче предписания об устранении нарушения обязательного требования и др.). Но реализация властных полномочий детально регламентирована законом и обусловлена соблюдением инспектором своих обязанностей, некоторые из которых неотрывно связаны с нравственностью, моралью. В качестве примера укажем на требование закона не допускать при проведении проверок проявления неуважения в отношении богослужений, других религиозных обрядов и церемоний.

Также должностное лицо обязано доказывать обоснованность своих действий при их обжаловании, но как это исполнит ИИ, действия которого не подчиняются составленным разработчиком алгоритмам?

Можно предположить, что вследствие выполнения системами ИИ отдельных функций и полномочий инспектора и органа контроля (надзора) появится третья категория субъектов административного права, помимо частных лиц и властных субъектов, а именно «электронные лица», «которые несут ответственность за свои действия и могут принимать независимые решения или иным образом взаимодействовать с третьими лицами»[195].

В подавляющем большинстве работ учеными – юристами изучается правосубъектность ИИ применительно к гражданско-правовым отношениям, в частности, о правах и обязанностях генеративных интеллектуальных систем, создающих изображения, тексты, о правовой охране которых и правовом статусе автора не выработан унифицированный подход[196].

В настоящее время не проведено комплексное научное исследование касательно обоснованности и необходимости появления нового субъекта права в сфере государственного контроля (надзора). Однако теоретические разработки касательно научной несостоятельности идеи признания правосубъектности ИИ[197] в полной мере являются применимы и для контрольно-надзорных правоотношений.

Представляется, что определенный действующим законодательством Российской Федерации перечень субъектов административного права применительно к правоотношениям в рассматриваемой области является полным и достаточным. В указанный перечень входят специально уполномоченные органы исполнительной власти, контролируемые лица (коммерческие и некоммерческие

---

[195] *Морхат П.М.* Юнит искусственного интеллекта как электронное лицо // Вестник Московского государственного областного университета. Серия: Юриспруденция. 2018. № 2. С. 62.

[196] См. например: *Филиппова И.А., Коротеев В.Д.* Будущее искусственного интеллекта: объект или субъект права? // Journal of Digital Technologies and Law. 2023. № 1(2). С. 359-386.

[197] См., например: *Пономарева Е. В.* Феномен квазисубъекта права: вопросы теории: монография / под ред. С. И. Архипова. М.: Юрлитинформ, 2020.С. 65-80; *Гаджиев Г.А., Войниканис Е.А.* Может ли робот быть субъектом права (поиск правовых норм для регулирования цифровой экономики)? // Право. Журнал Высшей школы экономики. 2018. № 4. С. 24-48.

организации, физические лица), специалисты, экспертные организации и эксперты[198].

То обстоятельство, что органами контроля (надзора) применяются цифровые технологии для обработки массивов данных, повышения эффективности профилактических мероприятий и проверок, не вызывает необходимости в появлении нового субъекта права.

В настоящее время законодательством регулируется использование в целях государственного контроля и надзора различных средств[199]. Предусматривается возможность проведения мероприятий и совершение действий посредством технических средств (электронные устройства, инструменты анализа данных и др.); средств дистанционного взаимодействия (в том числе аудио- или видеосвязь); специального оборудования и (или) технических приборов (измерительные, испытательные приборы и инструменты, мини-лаборатории и переносные аппараты, государственные и иные информационные системы, программные средства); систем (методов) дистанционного контроля; специальных технических средств, имеющих функции фотосъемки, аудио- и видеозаписи, измерения; автоматизированных информационных систем сбора и обработки данных средства сбора или фиксации информации; автоматизированных технических средств фиксации правонарушений, имеющих функции фото- и киносъемки, видеозаписи; средств доступа к информации (аппаратно-программные средства, обеспечивающие в установленном законодательством порядке доступ к информации, содержащейся в государственных информационных системах).

Установлены требования к средствам:

- утверждение в установленном порядке в качестве применяемого испытательного оборудования;

- сертификация и метрологическая поверка;

---

[198] *Стахов А. И.* Административно-процессуальная деятельность органов государственного контроля и надзора: Учебное пособие. М.: РГУП. 2017. С. 176.

[199] Согласно ГОСТ Р 60.0.0.2-2016. Национальный стандарт Российской Федерации. Роботы и робототехнические устройства. Классификация" (утвержден и введен в действие Приказом Росстандарта от 29.11.2016 N 1842-ст): «робот - исполнительное устройство с двумя или более программируемыми степенями подвижности, обладающее определенным уровнем автономности и способное перемещаться во внешней среде с целью выполнения поставленных задач».

- создание ГИС и иных ИС, программных продуктов в соответствии с законодательством РФ;

- применительно к средствам доступа к информации - обеспечение соблюдения установленного законом порядка доступа к информации, содержащейся в ГИС.

Федеральными законами, положениями о виде государственного контроля, утверждаемыми Президентом РФ, Правительством РФ или высшим исполнительным органом государственной власти субъекта Российской Федерации, определяются случаи и порядок применения средств и систем, требования к ним. Так, законом предусмотрено, что досмотр в отсутствие проверяемого лица или его представителя осуществляется инспектором с обязательным применением видеозаписи.

Случаи, когда допустимо использование органом контроля (надзора) средств и систем, и порядок такого использования, включая требования к техническим средствам и определяются законом и положением о виде государственного контроля, утверждаемого Президентом РФ, Правительством РФ или высшим исполнительным органом государственной власти субъекта Российской Федерации.

Но правовое регулирование применения средств и систем отстает от современного уровня цифровой трансформации органов контроля (надзора). В частности, нормативными правовыми актами не регламентируются, какие виды цифровых технологий, включая ИИ, допускается использовать для обработки данных и проведения мероприятий (действий), не устанавливается порядок их использования для профилактики и выявления нарушений обязательных требований. Совершенствование рассматриваемого регулирования представляется более актуальным направлением, чем включение нового субъекта права в сферу ГКН. То, что вопрос о правосубъектности ИИ в отношениях по контрольно-надзорной деятельности не имеет актуальности, подтверждается его отсутствием в

указываемых юристами – учеными направлениях (проблемах) административного права[200].

Итак, можно констатировать, что:

1. Подходы к правосубъектности роботов (СИИ) могут различаться не только с учетом разных трактовок понятия «субъект права», но из-за отраслевой специфики. Так, цивилисты применительно к области интеллектуальной собственности допускают признании ИИ субъектом права или квазисубъектом, в то время как для административного права свойствен противоположный подход.

2. Так называемый «сильный» ИИ не соответствует целям и принципам ГКН в виду непрозрачных условий принятия им решений, поэтому его применение не должно допускаться законом.

3. Для осуществления полномочий в сфере ГКН важно значение имеет гуманистические свойства субъекта права: добросовестность, честность. Большую часть полномочий реализуется именно должностными лицами органа контроля (надзора).

4. ИИ в сфере ГКН – это объект права, его правовой режим соответствует правовому режиму технических и программных средств, применяемых органами контроля (надзора).

5. Отсутствует объективная необходимость в дополнении системы субъектов административного права новыми лицами: «электронное лицо», ИИ (роботы и системы ИИ) в качестве квазисубъекта права.

Применение технологий ИИ не влечет за собой необходимость признания лицами, осуществляющими государственный контроль (надзор), иных субъектов, помимо должностных лиц государственных органов контроля (надзора). Обоснованно ИИ рассматривать как техническое средство ГКН.

---

[200] Актуальные проблемы административного права и процесса: учебник для студентов вузов, обучающихся по направлению подготовки «Юриспруденция» / М. В. Костенников, А. В. Куракин. А. М. Кононов [и др.]. 3-е изд., перераб. и доп. М.: ЮНИТИ-ДАНА. 2019. 479 с.

§ 3.2. Риски применения искусственного интеллекта при проведении контрольных (надзорных) мероприятий

Технологии ИИ являются передовыми, качественно иными программными средствами, способные выполнять отдельные функции почти как человек, не нуждаясь в его постоянном контроле и руководстве. В настоящее время разрабатываются системы, которые самостоятельно вырабатывают и совершенствуют алгоритмы для своего функционирования, представляющие даже для их разработчиков «черный ящик» в отношении правил, по которым программа принимает решения и совершает действия.

Исходя из вышеуказанных способностей и потенциала интеллектуальных систем определяют не только преимущества, но и возможные риски их применения.

П.М. Морхат выделяет следующие виды угроз, обусловленные ИИ[201]:

- самоуправство сверхразумных машин, их выход за пределы назначенной им человеком специализации и возможная гибель человечества вследствие потери контроля за такими системами;

- риски, связанные с безопасностью интеллектуальных роботов, то есть со стандартами их производства и с их автономной работой;

- риски военного применения ИИ, для минимизации которых необходимо установить запрет на применение наступательных роботехнических систем дальнего радиуса действия.

Экспертами International Data Corporation (IDC) определены следующие основные риски внедрения и применения генеративного ИИ[202]:

- создание нейросетью вымышленных данных, фактов и объектов;

- предвзятость и ограниченная объяснимость;

- угроза репутации бренда;

---

[201] *Морхат П.М.* Риски и угрозы, связанные с применением искусственного интеллекта // Аграрное и земельное право. 2017. № 12 (156). С. 62-63.

[202] URL: www.tadviser.ru/index.php/Статья:Риски_использования_искусственного_интеллекта?ysclid=m51kfhe4hg769042846 (дата обращения: 25.11.2024).

- нарушение авторских прав;

- перерасход средств;

- воздействие на окружающую среду вследствие значительного потребления энергии системами ИИ;

- проблемы управления и безопасности;

- проблемы интеграции и взаимодействия;

- судебные разбирательства и соблюдение нормативных требований.

Эксперты относят к наиболее значимым следующие риски[203]:

- непрозрачность работы моделей ИИ;

- утечка информации, в том числе персональных данных;

- нарушение прав интеллектуальной собственности;

- сокращение рабочих мест;

- использование некачественных данных;

- дипфейки и кибер-мошенничество;

- зависимость от ИИ.

В исследовании консалтинговой компании «Яков и Партнёры» и Альянса в сфере искусственного интеллекта[204] указаны основные риски от генеративного ИИ[205], способного создавать новые данные (текст, программный код, изображения, видео):

- рост некачественного (недостоверного, фиктивного, ошибочного) контента в сети Интернет;

- принятие пользователем решения (инвестиционного или иного) на основе ложного ответа сервиса, что нанесет вред здоровью, жизни или финансам;

- структурные изменения на рынке труда и фрикционная безработица вследствие постепенного замещения некоторых профессий генеративным ИИ и возникновения новых профессий. Люди могут растерять некоторые навыки (снижение критичности мышления и др.);

---

[203] URL: https://monocle.ru/monocle/2024/50/kakiye-riski-neset-ispolzovaniye-iskusstvennogo-intellekta-v-biznese/?ysclid=m51ljhnsl437481835 (дата обращения: 25.11.2024).

[204] URL: https://yakovpartners.ru/publications/gen-ai-regulation/ (дата обращения: 15.01.2025).

[205] В частности, GPT-4 (OpenAI), YandexGPT («Яндекс»), GigaChat (Сбер).

- рост случаев цифрового мошенничества посредством синтеза речи, убедительных аудио- и видео дипфейков, фишинговых сайтов;

- рост объема контента, сгенерированного ИИ, или решения, не соответствующего этическим или культурным нормам (оскорбительного, дискриминационного, запрещенного для детей и др.).

Представляется обоснованным подход по признанию презумпции опасности ИИ[206].

На основании вышеизложенного можно предложить классифицировать рассмотренные риски на две основные группы в зависимости от объекта, на который направлено негативное влияние ИИ:

- антропоцентричные (в фокусе здоровье, права и интересы человека, общественные этические и культурные ценности), в том числе дипфейки, оскорбительный контент, дискриминационные решения, утечка данных;

- эколого-экономические (в центре окружающая среда и экономика), в частности, загрязнение природы вследствие выбросов вредных веществ в ходе выработки энергии, кардинальная реструктуризация видов экономической деятельности, переход к экономике данных.

Риски обусловлены тем, что:

- цифровым технологиям недоступны этические нормы;

- программа (программное обеспечение) применяет алгоритмы, созданные ею самостоятельно, по неизвестным даже разработчику правилам и условиям, что означает проблему алгоритмической прозрачности и подотчетности.

Некоторые из обозначенных выше рисков в полной мере являются актуальными и для использования ИИ при проведении контрольных (надзорных) мероприятий. В частности, генерация интеллектуальными системами недостоверной или вымышленной информации в результате сбора или обработки данных. Так, камера с функцией распознавания объектов может принять за запрещенный предмет иное имущество, которое лишь по отдельным признакам

---

[206] *Наумов В. Б.* Право в эпоху цифровой трансформации: в поисках решений // Российское право: образование, практика, наука. 2018. № 6 (108). С. 7.

подпадает под искомые параметры, и в этом случае только инспектор может всестороннее изучить выявленный предмет и принять решение о наличии или отсутствии нарушения обязательных требований. Кроме того, опасность дипфейка имеется и со стороны информации, поступающей от контролируемых лиц, применяющих рассматриваемую сквозную технологию с целью введения органа контроля (надзора) в заблуждение.

Из рассмотренных выше угроз наибольшую степень опасности, на мой взгляд, представляет возможность систем ИИ функционировать по неизвестным ни для пользователей, ни для их разработчиков алгоритмам, порой существенно отличающихся от предварительных программ и настроек. Такая способность технологий ИИ не соответствует целям и принципам контрольно-надзорной деятельности. Для интеллектуальных методов важным ориентиром должны быть обязательные требования, обеспечение соблюдения которых составляет основное предназначение государственного контроля (надзора).

Оценка посредством информационных технологий деятельности контролируемых лиц обязательно должна проводиться по тем критериям, которые предусмотрены нормативными правовыми актами, положения которых являются предметом контроля (надзора). Выполнение методами ИИ действий, отнесенных законодательством к компетенции органа контроля (надзора) и его должностных лиц, должно производиться в строгом соответствии с порядком, установленным законом и подзаконными актами. Только при таком условии минимизируется угроза дискриминационного, предвзятого подхода к контролируемым лицам. Примером может служить оценка добросовестности контролируемых лиц, которая проводится строго по перечню сведений, предусмотренному Законом 248-ФЗ с соблюдением принципов государственного контроля (надзора), что обеспечивает объективный, равный подход ко всем поднадзорным лицам.

В качестве специального риска применения ИИ в сфере государственного контроля (надзора) можно рассматривать указанное А.В. Мартыновым сокращение или исключение возможности административного усмотрения, в результате чего, по мнению ученого, «могут быть проигнорированы тяжелые жизненные ситуации,

финансовое состояние, трагедии человека, социально-политические условия и др. Тем самым применение искусственного интеллекта – «бездушной машины» не позволит решить цели и задачи государственного управления, основанного в том числе на принципах целесообразности, справедливости и гуманизма»[207].

Справедливо утверждение М.Б. Добробаба о необходимости установления «презумпции приоритета решений, принимаемых человеком, над решением ИИ, применяемую не только в судопроизводстве, но и в управленческой деятельности.»[208].

Выявленные риски позволяют правильно определить область применения ИИ, меры по минимизации ущерба и по восстановлению прежнего состояния.

Справедливо отмечено Ю.А. Тихомировым, что «право выполняет применительно к риску такие функции, как легальное признание и допущение их, установление средств предупреждения и минимизации риска, определение меры ответственности и компенсаторных средств»[209].

Необходимо учитывать технологическую нейтральность установленных законом принципов ГКН[210], в том числе о соразмерности вмешательства в деятельность контролируемых лиц и об охране прав и законных интересов, уважении достоинства личности, деловой репутации контролируемых лиц[211].

Указанные основополагающие правовые положения должны применяться вне зависимости от вида цифровых технологий, используемых органом ГКН при проведении контрольных (надзорных) и профилактических мероприятий и принятии решений по результатам указанных мероприятий. Так, решение,

---

[207] *Мартынов А.В.* Актуальные вопросы применения искусственного интеллекта при осуществлении контрольно-надзорной деятельности органов исполнительной власти // Вестник Нижегородского университета им. Н.И. Лобачевского. 2020. N 2. С. 184.

[208] *Добробаба М.Б., Чаннов С.Е., Евсиков К.С.* Правовое обеспечение применения цифровых технологий в государственном управлении: монография. Саратов: Амирит, 2024. С. 133.

[209] *Тихомиров Ю. А.* Правовые риски // Законы России: опыт, анализ, практика. 2012. № 2. С. 88.

[210] *Мартынов А.В.* Критический анализ общих положений Федерального закона от 31 июля 2020 г. № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» // Актуальные вопросы контроля и надзора в социально значимых сферах деятельности общества и государства: Материалы VI Всероссийской научно-практической конференции (Россия, г. Нижний Новгород, 1 июля 2021 г.) / Отв. ред. доктор юридических наук, профессор А.В. Мартынов. Н. Новгород: Изд-во Нижегородского государственного университета им. Н.И. Лобачевского, 2021. С. 53 – 58.

[211] См.: *Лагаева В. П.* Технологическая нейтральность принципов государственного контроля (надзора) // Аграрное и земельное право. 2024. № 10 (238). С. 120-121.

принятое на основании необъективной (дискриминационной) или недостоверной информации, должно подлежать отмене и в случае, когда указанная информация в отношении контролируемого лица или потребителя получена вследствие ошибок разработчика или особенностей алгоритмов от систем ИИ.

Применение ИИ в области государственного контроля (надзора) должно быть исключительно риск-ориентированным, при котором любое решение о внедрении умных цифровых технологий должно сопровождаться предварительной оценкой угроз и действий по их исключению или нейтрализации, баланса между потенциальной пользой от работы интеллектуальных программных продуктов и угрозами, исходящими от таких технологий.

Справедливо высказанное учеными – правоведами мнение о ключевой роли правовых экспериментов и специальных правовых режимов («регуляторные» или «регулятивные песочницы») для оценки рисков применения новых цифровых технологий и формирования нормативно-правовой базы[212].

Представляется важным, что Национальной стратегией развития искусственного интеллекта, утвержденной Указом Президента Российской Федерации от 10 октября 2019 г. № 490, предусмотрено обязательное внедрение доверенных технологий искусственного интеллекта в тех областях его использования, в которых может быть нанесен ущерб безопасности Российской Федерации, в том числе в органах публичной власти. При этом под указанными технологиями понимаются такие, которые отвечают стандартам безопасности, разработаны с учетом принципов объективности, недискриминации, этичности, исключающие при их использовании возможность причинения вреда человеку и нарушения его основополагающих прав и свобод, нанесения ущерба интересам общества и государства.

В связи с особым правовым режимом персональных данных и иной конфиденциальной информации, обрабатываемой в целях государственного

[212] *Ефремов А.А., Добролюбова Е.И., Талапина Э.В., Южаков В.Н.* Экспериментальные правовые режимы: зарубежный опыт и российский старт. М.: Дело, 2020. С. 7 – 8. См. также: Право искусственного интеллекта: учебник / под редакцией А.В. Минбалеева. – Саратов: Амирит. 2024. С. 86-96.

контроля (надзора), представляется важным применять исключительно доверенные технологии ИИ, которые исключают возможность причинения вреда физическим и юридическим лицам, обществу и государству, в том числе посредством обработки указанных сведений без участия человека[213].

Предусмотрено вышеназванной Стратегией формирование реестра апробированных доверенных технологий ИИ, включая большие фундаментальные модели, предназначенные для повышения эффективности работы государственных гражданских служащих, муниципальных служащих. Указанный реестр размещается на единой цифровой платформе Российской Федерации «ГосТех» (платформа «ГосТех»). Важным направлением совершенствования правового регулирования информационного обеспечения контрольно-надзорных органов является установление законом обязательного применения в целях предупреждения и выявления нарушений обязательных требований только тех технологий ИИ, которые включены в указанный выше реестр доверенных технологий ИИ, и сертифицированных решений в области ИИ.

Очевидно, что в сфере государственного контроля (надзора) перспективой внедрения обладают только такие доверенные технологии искусственного интеллекта, отвечающие высоким стандартам и разработанные с учетом принципов административного и информационного права, обладающих технологической нейтральностью.

Риски ИИ носят универсальный характер, то есть они в равной степени актуальны для каждой области применения указанных цифровых технологий и в обязательном порядке должны учитываться до принятия решения о внедрении рассматриваемых методов.

Для сферы государственного контроля (надзора) особую опасность представляют модели так называемого сильного ИИ, для которых свойственна полная автономность функционирования и принятие решение по непрозрачным и

---

[213] См. также: *Лагаева В. П.* Доверенные технологии искусственного интеллекта в сфере государственного контроля (надзора): правовые аспекты // Право для лидерства: сборник материалов XII Московского инновационного юридического форума / редколлегия: Е. В. Вавилин [и др.]. – М.: Издательский центр Университета имени О.Е. Кутафина (МГЮА). 2025. С. 102 – 104.

неизвестным алгоритмам. В этой связи такие системы ИИ должны запрещаться законом для применения органами контроля (надзора).

Правовым средством минимизации рисков ИИ являются риск-ориентированный подход к выбору и применению ИИ, доступ органов контроля (надзора) только к доверенным технологиям ИИ.

§ 3.3. Приоритетная роль систем искусственного интеллекта в реализации риск-ориентированного подхода государственного контроля (надзора)

Внедрению технологий ИИ в сферу ГКН способствуют следующие факторы:

- установленные законом система управления рисками и приоритет профилактических мероприятий по отношению к контрольным (надзорным) мероприятиям, что требует развития прогностической функции государственного контроля (надзора), обеспечивающей эффективное предупреждение неправомерного поведения контролируемых лиц, в том числе посредством определения модели их поведения, категорирования объектов контроля, установления точных и обоснованных индикаторов риска нарушений обязательных требований;

- обеспечение связанности и анализа данных, получаемых органами контроля (надзора) из предусмотренных законом источников и обрабатываемых в информационных системах ГКН (сведения об объекте контроля, данные Единого реестра видов контроля и др.);

- применение технологий ИИ контролируемыми лицами, обязанными соблюдать обязательные требования, составляющие предмет ГКН;

- нехватка квалифицированных кадров в органах государственного контроля (надзора), в том числе в связи с уровнем заработной платы, не соответствующей строгой ответственности должностного лица.

Применение ИИ особо полезно в таких направлениях профилактической деятельности ГКН, как категорирование объектов контроля, разработка и

применение индикаторов риска, развитие сервисов по разъяснению обязательных требований[214].

В законодательство Российской Федерации в области организации и осуществления государственного контроля (надзора), муниципального контроля понятие «риск-ориентированный подход» было введено Федеральным законом от 13 июля 2015 г. № 246-ФЗ для обозначения такого метода организации и осуществления государственного контроля (надзора), при котором в предусмотренных 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. Так, применительно к ГКН в сфере связи плановые проверки в отношении объектов контроля, отнесенных к категории низкого риска, не проводятся, а для объектов контроля, отнесенных к категории чрезвычайно высокого риска, такие проверки должны проводиться не более двух раз в год [215].

Рассматриваемый метод в силу фокусирования внимания контрольных (надзорных) органов на объектах, являющихся наиболее потенциально опасными, позитивно оценивается учеными – правоведами. При этом представляется обоснованным мнение о том, что «отнесение поднадзорных субъектов и объектов к определенной категории риска или классу (категории) опасности потребует значительное время и может продлиться не один год.»[216], поскольку органам надзора необходимо обработать значительный объем информации для оценки рисков.

---

[214] См. также: Лагаева В.П. Правовое регулирование применения искусственного интеллекта в профилактике нарушений обязательных требований // Аграрное и земельное право. 2024. № 7(235). С. 95-98.

[215] Постановление Правительства РФ от 29 июня 2021 года № 1045 «О федеральном государственном контроле (надзоре) в области связи» // Официальный интернет-портал правовой информации http://pravo.gov.ru, 01.07.2021.

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

С.А. Агамагомедова обоснованно рассматривает риск-ориентированный подход государственного контроля и надзора в разных ипостасях: принцип ГКН, условие рационального использования ресурсов органов надзора, средство обеспечения оптимального воздействия на контрольных лиц и стимулирования добросовестного соблюдения ими обязательных требований, способ организации и проведения ГКН[217].

О важности рассматриваемого метода ГКН свидетельствует то обстоятельство, что «не всегда в ходе проводимых проверок выявляются какие-либо существенные нарушения, что свидетельствует о неэффективной системе отбора кандидатов для проведения в отношении них контрольных мероприятий»[218].

В Законе № 248-ФЗ вместо понятия «риск-ориентированный подход» используется понятие «управление рисками причинения вреда (ущерба) охраняемым законом ценностям», которое является основной ГКН и означает осуществление профилактических и контрольных (надзорных) мероприятий на основе оценки указанных рисков в целях обеспечения допустимого уровня риска в соответствующей сфере подконтрольной деятельности (такой уровень может быть обусловлен, в частности, обстоятельствами непреодолимой силой (форс-мажор), эксплуатацией источника повышенной опасности).

При оценке рисков важно определить круг охраняемых законом ценностей, находящихся в зоне ведения того или иного органа надзора. Затем определяется вероятность возникновения риска от того или иного объекта контроля и масштаб вреда (ущерба).

Необходимо отметить, что оценка рисков, заключающаяся в определении вероятности возникновения риска и масштаба вреда (ущерба) для охраняемых законом ценностей, напрямую отнесена законом к деятельности органов надзора, на которых в этой связи возложена обязанность по организации постоянного

---

[217] *Агамагомедова С.А.* Риск-ориентированный подход при осуществлении контрольно-надзорной деятельности: теоретическое обоснование и проблемы применения // Сибирское юридическое обозрение. 2021. Т. 18. № 4. С. 460-470.

[218] *Медведева Н.Г.* Ключевые направления реформирования и совершенствования правового обеспечения контрольно-надзорной деятельности в Российской Федерации // Общество: политика, экономика, право. 2021. № 8(97). С. 72.

мониторинга сведений, используемых для оценки и управления рисками. Очевидно, что для исполнения указанной функции органам надзора важно применять цифровые технологии, способные автоматизировать непрерывные процессы сбора, обработки, анализа и учета данных.

Управление рисками находит свою реализацию посредством категорирования объектов контроля (отнесения их к одной из категорий риска, установленных законом). Закон устанавливает, что критерии риска, в соответствии с которым органом надзора присваивается та или иная категория риска, должны учитывать тяжесть причинения вреда (ущерба) охраняемым законом ценностям, вероятность наступления негативных событий, влекущих причинение указанного вреда (ущерба), а также добросовестность контролируемых лиц.

Применительно к оценке тяжести причинения вреда (ущерба) и к оценке вероятности наступления негативных событий органы надзора не ограничены в законных источниках достоверных сведений об уровне риска в соответствующей сфере и о практике соблюдения обязательных требований в рамках вида ГКН. Это означает, что объем такой информации может быть значительным, учитывая, в том числе, данные, обрабатываемые в информационных системах, как в государственных, так и в иных информационных системах, обеспечивающих, в частности, закупочную деятельность, маркировку и прослеживаемость товаров, и иные сведения об объектах контроля.

Учитывая открытый перечень источников информации, очевидно, что в процессе категорирования объектов контроля органу контроля (надзора) необходимо осуществить сбор и анализ значительного массива данных, и без применения цифровых технологий (Big Data и ИИ) не получится решать задачи управления рисками эффективно, своевременно и с минимальной долей ошибок и погрешностей.

Рассматриваемый риск-ориентированный подход включает в себя не только категорирование объектов контроля, но и применение индикатора риска нарушения обязательных требований (далее – Индикатор), под которым понимается соответствие или отклонение от параметров объекта контроля, которые не

представляют собой нарушение обязательных требований, но с высокой степенью вероятности свидетельствуют о наличии такого нарушения и риска причинения вреда (ущерба) охраняемым законом ценностям (часть 9 статьи 23 Закона № 248-ФЗ).

Индикатор разрабатывается и утверждается федеральными органами исполнительной власти, государственными корпорациями, осуществляющими функции по нормативно-правовому регулированию в установленной сфере деятельности, высшим исполнительным органом государственной власти субъекта Российской Федерации, представительным органом муниципального образования, и подлежит размещению в сети "Интернет"[219].

То обстоятельство, что Индикатор должен свидетельствовать о высокой степени вероятности нарушения обязательных требований и риска причинения вреда (ущерба), позволяет сделать вывод о целесообразности применения методов ИИ с функцией прогнозирования для разработки Индикатора.

Законом не ограничены достоверные источники сведений, применяемых для определения и выявления Индикатора, за исключением того, что сбор, обработка, анализ и учет сведений об объектах контроля должны осуществляться без взаимодействия с контролируемыми лицами, кроме случаев обязательного профилактического визита. Как и при разработке критериев риска, определение Индикатора требует обработки внушительного массива данных, что невозможно без применения ИИ.

Несмотря на то, что в настоящее время разработано и утверждено более 180 индикаторов, однако не все они применяются органами контроля (надзора). Одним из возможных способов повышения уровня использования этого инструмента является цифровая трансформация процесса разработки индикаторов, позволяющая применять не только способности и рабочее время сотрудников органов контроля (надзора), но и задействовать информационных технологии ИИ

[219] См., например: Приказ Минцифры России от 16 сентября 2024 г. № 773 «Об утверждении перечня индикаторов риска нарушения обязательных требований при осуществлении федерального государственного контроля (надзора) в сфере идентификации и (или) аутентификации» (Зарегистрировано в Минюсте России 21.10.2024 N 79838) // Официальный интернет-портал правовой информации http://pravo.gov.ru, 22.10.2024.

для анализа наиболее часто нарушаемых требований и определения вероятности их нарушений.

Указанные технологии в сочетании друг с другом позволяют управлять большими информационными массивами данных, применять «широкий спектр методов машинного обучения, направленных на расширение ценности, обеспечиваемой оценкой больших данных»[220]. Органы контроля (надзора) могут использовать данные, генерируемые цифровыми следами пользователей контролируемых лиц, чтобы получить дополнительную информацию о деятельности указанных лиц, о соблюдении ими обязательных требований. Расширенная область сбора данных, обеспечиваемая применением интеллектуальных систем, позволит сформировать комплексный цифровой профиль контролируемых лиц и объектов.

Программные средства ИИ для анализа больших данных позволяют контрольному (надзорному) органу собирать данные в полном объеме; обрабатывать эти данные, в том числе с помощью передового машинного обучения; выводить эти данные и аналитические данные на поверхность с помощью информационных панелей, отчетов и многого другого; предоставлять информацию лицам, принимающим решения[221].

Присвоение категории риска основывается не только на сведениях, относящихся к действиям, совершенным контролируемым лицом ранее, но и на оценке вероятности наступления негативных событий, что позволяет применять предиктивную аналитику на основе ИИ. В результате повышается точность прогноза за счет осуществления алгоритмами детального анализа данных и точного выявления причинно-следственной связи между деятельностью контролируемых лиц и вредом (ущербом) охраняемым законом ценностям.

---

[220] *Липатов А.Г.* Возможности использования искусственного интеллекта для управления большими информационными массивами данных Big Data // «Инновации и инвестиции», № 5, 2023, с. 187.

[221] *Липатов А.Г.* Указ. соч. С. 188.

В 2023 году Правительство Российской Федерации утвердило Концепцию совершенствования контрольной (надзорной) деятельности до 2026 года[222], согласно которой для удобства контролируемых лиц будут созданы сервисы «калькуляторы рисков», позволяющие рассчитать для контролируемого лица в режиме реального времени категорию риска в рамках вида контроля и возможные факторы, влияющие на ее изменение. Такой «калькулятор рисков» будет выводиться в личном кабинете контролируемого лица на портале госуслуг. При определении нормативным правовым актом порядка предоставления указанного сервиса необходимо также предусмотреть описание применяемых информационных технологий, в том числе методов ИИ.

Другим важным нововведением, предусмотренным Концепцией совершенствования контрольной (надзорной) деятельности до 2026 года, является формирование цифровых систем управления инцидентами по категорированию объектов контроля. Это позволит повысить достоверность и актуальность управления рисками.

В процессе категорирования деятельности и объектов контролируемых лиц орган контроля (надзора) должен организовать сбор и анализ значительного массива данных с применением цифровых технологий (Big Data и ИИ), поскольку расширенная область сбора данных, обеспечиваемая применением интеллектуальных систем, позволит сформировать комплексный цифровой профиль контролируемых лиц и объектов.

Предиктивная аналитика ИИ повышает точность прогноза вероятности наступления негативных событий, что позволяет устанавливать достоверные и обоснованные критерии риска.

Представляется необходимым установить обязательное применение алгоритмов ИИ при разработке индикаторов риска нарушений обязательных требований, чтобы достичь их максимально возможной точности для сокращения затрат на проведение внеплановых контрольных (надзорных) мероприятий.

---

[222] Распоряжение Правительства РФ от 21 декабря 2023 г. № 3745-р // Официальный интернет-портал правовой информации http://pravo.gov.ru, 25.12.2023.

§ 3.4. Роль искусственного интеллекта в обеспечении эффективности государственного контроля (надзора)

Действующее правовое регулирование отношений в сфере государственного контроля (надзора) в Российской Федерации представляется сбалансированным и системным в виду того, что Законом № 248-ФЗ установлена система оценки результативности и эффективности ГКН, основанная на мониторинге и анализе деятельности органов надзора на предмет достижения целей и задач ГКН и соотношения полученных результатов и потраченных для этого ресурсов.

Положительным моментом является то, что указанная выше оценка проводится не только в целом по всем контрольно-надзорной деятельности, но и применительно к каждому виду ГКН[223], что позволяет более четко определить, в функционировании какого именно органа надзора имеются необходимые результаты и (или) недостатки.

Основу рассматриваемой оценки составляет система ключевых и индикативных показателей.

Указываемые в положении о виде ГКН ключевые показатели призваны согласно пункту 1 части 2 статьи 30 Закона № 248-ФЗ отражать уровни минимизации вреда (ущерба) охраняемым законом ценностям и устранения риска причинения вреда (ущерба) в соответствующей сфере деятельности. Так, применительно к федеральному государственному контролю (надзору) в области связи ключевым является следующий показатель: отношение объектов контроля, по которым изменена категория риска на более низкую, к объектам контроля, по которым изменена категория риска на более высокую категорию риска[224].

Индикативные показатели отражают соотношение между степенью устранения рисков и объемом ресурсов, а также уровень вмешательства органа

---

[223] Часть 1 статьи 30 Федерального закона от 20 июля 2020 года № 248-ФЗ Влияние искусственного интеллекта на цифровой суверенитет России // Правовое обеспечение суверенитета России: проблемы и перспективы: Сборник докладов XIII Московской юридической недели: в 4 ч. Ч.1 / редколлегия: А. В. Корнев [и др.]. – М.: Издательский центр Университета имени О.Е. Кутафина (МГЮА), 2024. – С. 203.

[224] Пункт 86 Положения о федеральном государственном контроле (надзоре) в области связи, утв. Постановлением Правительства РФ от 29 июня 2021 г. № 1045 «О федеральном государственном контроле (надзоре) в области связи» // Официальный интернет-портал правовой информации http://pravo.gov.ru, 01.07.2021.

надзора в деятельность контролируемых лиц. Индикативные показатели составляют значительный объем и охватывают в полном объеме деятельность указанных органов, включая процессы обжалования действий (бездействия) их должностных лиц. Так, применительно к федеральному государственному контролю (надзору) за соблюдением законодательства РФ о средствах массовой информации установлено двадцать три индикативных показателя (количество плановых и внеплановых проверок за отчетный период и др.), при этом утвержден только один ключевой показатель[225].

Согласно части 8 статьи 30 Закона № 248-ФЗ информация о достижении ключевых показателей и сведения об индикативных показателях подлежат включению органами надзора в подготавливаемые ими ежегодные доклады о виде ГКН посредством подсистемы сбора отчетности, обеспечивающей мониторинг и оценку эффективности контрольной (надзорной) деятельности и лицензирования, разрешительной деятельности, функционирующей в составе ГИС «Типовое облачное решение по автоматизации контрольной (надзорной) деятельности»[226].

Организация и проведение мониторинга эффективности вида ГКН проводится органом надзора по методике, утвержденной Правительством РФ[227].

Правительством Российской Федерации определен перечень документов и сведений, на основании сбора, обработки и анализа которых осуществляется мониторинг[228]. Отметим, что указанная информация позволяет провести всестороннюю оценку, поскольку охватывает как документы, издаваемые самим органом надзора, так и сведения, поступающие к нему от контролируемых лиц, граждан, государственных органов, средств массовой информации, экспертов и др.

---

[225] Приказ Минцифры России от 06.12.2021 № 1310 «Об утверждении индикативных показателей по федеральному государственному контролю (надзору) за соблюдением законодательства Российской Федерации о средствах массовой информации» // СПС «КонсультантПлюс».

[226] Постановление Правительства РФ от 7 декабря 2020 № 2041 «Об утверждении требований к подготовке докладов о видах государственного контроля (надзора), муниципального контроля и сводного доклада о государственном контроле (надзоре), муниципальном контроле в Российской Федерации» // Собрание законодательства РФ. 2020. № 50 (часть V). Ст. 8241.

[227] Постановление Правительства РФ от 5 апреля 2010 г. № 215 «Об утверждении Правил подготовки докладов об осуществлении государственного контроля (надзора), муниципального контроля в соответствующих сферах деятельности и об эффективности такого контроля (надзора)» // Собрание законодательства РФ. 2010. № 15. Ст. 1807.

[228] Методика проведения мониторинга эффективности государственного контроля (надзора) и муниципального контроля, утв. Постановлением Правительства РФ от 5 апреля 2010 г. № 215.

Мониторинг должен проводиться также с учетом документов, подтверждающих причинение вреда (ущерба) охраняемым законом ценностям в связи с деятельностью контролируемых лиц (в том числе о наличии случаев смерти, заболеваний (отравлений, несчастных случаев) людей, животных и растений, загрязнения окружающей среды, аварий, причинения вреда имуществу, возникновения чрезвычайных ситуаций природного и техногенного характера).

Правительством РФ не предусматривается применение цифровых технологий для проведения мониторинга эффективности контрольно-надзорной деятельности, расчета, анализа и оценке показателей эффективности. Однако цифровизация оценки работы органа контроля (надзора) представляется важным направлением совершенствования рассматриваемой функции государственного управления. В частности, учитываемые в ходе мониторинга документы могут находиться в распоряжении иных органов и не поступить напрямую в орган контроля (надзора), что делает необходимым обеспечить их поиск в информационных системах, в том числе посредством алгоритмов ИИ.

Сведения о достижении ключевых и индикативных показателей вида контроля должны соответствовать сведениям, включенным в единый реестр видов контроля, единый реестр контрольных (надзорных) мероприятий, информации, содержащейся в форме федерального статистического наблюдения об осуществлении государственного контроля (надзора), муниципального контроля[229]. Такое соответствие возможно обеспечить и контролировать с применением интеллектуальных систем и программных средств.

Некоторые сведения об организации и осуществлении видов контроля (в частности, о количестве контролируемых лиц, в отношении которых проведены контрольные (надзорные) мероприятия с взаимодействием с контролируемым лицом) представляются в электронной форме посредством подсистемы сбора отчетности, обеспечивающей мониторинг и оценку эффективности контрольной

[229] Постановление Правительства РФ от 7 декабря 2020 № 2041 «Об утверждении требований к подготовке докладов о видах государственного контроля (надзора), муниципального контроля и сводного доклада о государственном контроле (надзоре), муниципальном контроле в Российской Федерации» // Собрание законодательства РФ. 2020. № 50 (часть V). Ст. 8241.

(надзорной) деятельности и лицензирования, разрешительной деятельности, функционирующей в составе государственной информационной системы «Типовое облачное решение по автоматизации контрольной (надзорной) деятельности», с учетом методических рекомендаций, издаваемых Министерством экономического развития Российской Федерации. В этой связи целесообразно в положении о ГИС ТОР КНД предусмотреть порядок обработки указанных данных посредством алгоритмов ИИ.

Важно отметить, что в состав сведений, учитываемых при проведении мониторинга ГКН, не включены социологические данные (оценка контролируемыми лицами влияния КНД на снижение рисков причинения вреда в соответствующей подконтрольной сфере и др.[230]), что снижает качество и полноту оценки эффективности органов надзора. Расширение объема и вида сведений для анализа работы органа контроля (надзора) может быть обеспечено применением информационных технологий, способных осуществлять поиск и анализ данных в автоматическом режиме, в короткие сроки, без возложения на должностных лиц органа надзора чрезмерной нагрузки.

Положительное влияние оказывает внедрение цифровых технологий в контрольно-надзорную деятельность и в части снижения коррупционных рисков, в том числе вследствие сокращение случаев прямого взаимодействия инспекторов с контролируемыми лицами[231].

Применение ИИ позволит осуществлять постоянный, оперативный, точный и детальный мониторинг по показателям эффективности ГКН и выработать новые, более точные критерии оценки работы органа надзора.

Мониторинг эффективности ГКН возможно проводить по расширенному кругу сведений и документов вследствие применения технологий ИИ.

---

[230] *Добролюбова Е. И.* Оценка качества государственного управления: обоснованность, результативность, эффективность: монография / Е. И. Добролюбова, В. Н. Южаков, А. Н. Старостина. М.: Дело (РАНХиГС), 2021. С. 163.

[231] *Комиссаров А.В., Комиссаров М.А., Абакумова Е.Ю.* Современные подходы в правовом обеспечении механизма государственного контроля предпринимательской деятельности // Право и экономика. 2023. № 9. С. 35-40.

Использование ИИ для обработки данных о деятельности органов надзора должно регулироваться нормативными правовыми актами, устанавливающими в том числе порядок мониторинга эффективности ГКН и функционирование информационных систем ГКН.

ЗАКЛЮЧЕНИЕ

По результатам проведенного исследования можно сделать следующие выводы:

1. Информационное обеспечение государственного контроля (надзора) – это комплекс информационных ресурсов, баз данных, информационных систем, технических средств, информационных технологий и информационно-телекоммуникационной сети.

Ключевую роль в информационном обеспечении государственного контроля (надзора) играют цифровые технологии, включая алгоритмы больших данных, блокчейн, искусственный интеллект.

2. Установленный законом приоритет профилактических мероприятий над контрольными (надзорными) мероприятиями является правовым основанием для первоочередного использования цифровых технологий в целях предупреждения нарушений обязательных требований.

Такой подход означает, что в приоритетном порядке по отношению к фискальным целям должны внедряться информационные технологии, обеспечивающие проведение контрольными (надзорными) органами превентивных мероприятий (информирование, консультирование, обобщение правоприменительной практики, самообследование и др.), применение в полном объеме риск-ориентированного подхода к объектам контроля.

3. Перечень сведений, получаемых уполномоченными органами от контролируемых лиц, ограничивается федеральными законами о государственном контроле (надзоре) заявлениями, уведомлениями, обращениями и декларациями, что представляется недостаточным на нынешнем этапе развития информационного общества. Действующим законодательством прямо не предусматриваются такие источники сведений и данных, как информационные ресурсы контролируемых лиц (сайт в сети Интернет, цифровые платформы, персональные страницы в социальных сетях и т.д.). Представляется важным законодательно возложить на государственные органы контроля (надзора) обязанности по постоянному

мониторингу указанных информационных площадок с применением в том числе сквозных цифровых технологий в профилактических целях и для всесторонней оценки соблюдения обязательных требований.

Федеральным законом от 21 июля 2021 года № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» предоставлена возможность обеспечения систем ИИ достоверными и непредвзятыми исходными данными, но при этом в указанном федеральном законе не регулируется порядок доступа разработчиков систем ИИ к наборам государственных данных ГКН.

4. Требуется уточнить правовой режим информационных систем государственного контроля (надзора) с целью их трансформации в интеллектуальные информационные системы, что позволит не только аккумулировать и учитывать в них управленческую информацию, но и обрабатывать данные аналитическими методами ИИ. Это позволит не упустить ни одно ценное сведение при принятии должностными лицами органов контроля (надзора) решений в рамках своих полномочий, в том числе о присвоении категории риска объекту контроля, об утверждении индикаторов риска нарушений обязательных требований, о проведении профилактического или контрольного (надзорного) мероприятия, о предложениях по результатам обобщения правоприменительной практики.

В настоящее время информационные системы ГКН эксплуатируются в основном в целях учета информации и обеспечения взаимодействия органов контроля (надзора) с органами прокуратуры, с другими государственными органами и контролируемыми лицами. Указанных целей явно недостаточно при наличии интеллектуальных систем и технологий ИИ. Требуется трансформировать рассматриваемые информационные системы в аналитические и прогностические, в которых проводятся анализ данных как в целом для оценки и управления рисками нарушений обязательных требований, так и для разработки модели поведения конкретного контролируемого лица с учетом его цифрового профиля,

вырабатываются с использованием алгоритмов искусственного интеллекта предложения по совершенствованию обязательных требований.

5. В настоящее время российское законодательство не предусматривает специального правового регулирования отношений по применению технологий ИИ при проведении государственного контроля (надзора). Превалирующий уровень регулирования сейчас составляет так называемое «мягкое право» (например, Кодекс этики в сфере ИИ) и стратегические документы (концепции, программы и иные). При этом внедрение методов ИИ в информационные системы государственных органов контроля (надзора) имеет место быть, что подтверждается ведомственными программами по цифровой трансформации указанных органов. Такая ситуация указывает на наличие пробела в правовом регулировании государственного контроля (надзора) в аспекте применения цифровых инноваций.

Ведомственные программы по цифровой трансформации государственных органов контроля (надзора) не содержат, как правило, информации о том, какие именно технологии ИИ планируется применять или уже применяются при осуществлении контроля (надзора), что не обеспечивает прозрачность этого процесса.

6. Рассмотренный зарубежный опыт регулирования ИИ позволяет утверждать, что государства солидарны в признании необходимости человеко-ориентированного подхода в правовом регулировании отношений в сфере систем ИИ.

7. Унифицированное правовое регулирование отношений по использованию технологий ИИ в контрольно-надзорной деятельности государственных органов практически отсутствует в законодательстве государств БРИКС и в Регламенте (ЕС) 2024/1689 Европейского парламента и Совета от 13 июня 2024 года.

8. Стратегическое направление Российской Федерации на цифровизацию государственного контроля (надзора) важно обеспечить правовым механизмом реализации посредством установления федеральными законами целей и принципов

правового регулирования отношений по применению технологий ИИ при осуществлении указанной функции государственного управления.

К целям правового регулирования отношений по применению технологий ИИ при осуществлении государственного контроля (надзора) относятся обеспечение его эффективности, сокращение нагрузки на добросовестных контролируемых лиц, а также цифровизация указанной деятельности посредством технологий ИИ.

К принципам государственного регулирования рассматриваемых в настоящем исследовании отношений можно отнести: безопасность, открытость, сочетание правового и технического регулирования, приоритет использования ИИ в профилактической деятельности органов контроля (надзора), право контролируемого лица на отказ от применения ИИ в отношении данных о себе, недискриминационный доступ к государственным данным для разработчиков систем ИИ, ответственность органа контроля (надзора) за нарушение прав и законных интересов контролируемых лиц в результате применения ИИ.

9. Подходы к правосубъектности роботов (СИИ) могут различаться с учетом разных трактовок понятия «субъект права».

10. Так называемый «сильный» ИИ не соответствует целям и принципам ГКН в виду непрозрачных условий принятия им решений, поэтому его применение не должно допускаться законом.

11. Для осуществления полномочий в сфере ГКН важно значение имеет гуманистические свойства субъекта права: добросовестность, честность, в этой связи такие полномочия реализуются именно инспекторами - должностными лицами органа контроля (надзора).

12. ИИ в сфере ГКН – это объект права, его правовой режим соответствует правовому режиму технических и программных средств, применяемых органами контроля (надзора).

13. Отсутствует объективная необходимость в дополнении системы субъектов административного права новыми лицами: «электронное лицо», ИИ (роботы и системы ИИ) в качестве квазисубъекта права.

Применение технологий ИИ не влечет за собой необходимость отказа от признания лицами, осуществляющими государственный контроль (надзор), только должностных лиц государственных органов контроля (надзора). ИИ рассматривается как техническое средство.

14. Риски ИИ носят универсальный характер, то есть они в равной степени актуальны для каждой области применения указанных цифровых технологий и в обязательном порядке должны учитываться до принятия решения о внедрении рассматриваемых методов.

Для сферы государственного контроля (надзора) особый риск представляют модели так называемого сильного ИИ, для которых свойственна полная автономность функционирования и принятие решение по непрозрачным и неизвестным алгоритмам.

Правовым средством минимизации рисков от применения ИИ является риск-ориентированный подход к выбору и применению ИИ, а также доступ органов контроля (надзора) только к доверенным технологиям ИИ.

15. В процессе категорирования деятельности и объектов контролируемых лиц орган контроля (надзора) должен организовать сбор и анализ значительного массива данных с применением цифровых технологий (Big Data и ИИ), поскольку расширенная область сбора данных, обеспечиваемая применением интеллектуальных систем, позволит сформировать комплексный цифровой профиль контролируемых лиц и объектов.

Предиктивная аналитика ИИ повышает точность прогноза вероятности наступления негативных событий, что позволяет устанавливать достоверные и обоснованные критерии риска.

16. Представляется необходимым установить обязательное применение алгоритмов ИИ при разработке индикаторов риска нарушений обязательных требований, чтобы достичь их максимально возможной точности для сокращения затрат на проведение внеплановых контрольных (надзорных) мероприятий.

17. Мониторинг эффективности контрольно-надзорной деятельности возможно проводить по расширенному кругу сведений и документов вследствие применения технологий ИИ.

18. Использование ИИ для обработки данных о деятельности органов контроля (надзора) должно регулироваться нормативными правовыми актами, устанавливающими порядок мониторинга эффективности государственного контроля (надзора).

СПИСОК СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ

ГКН	Государственный контроль (надзор)
ГИС	государственная информационная система
ГИС ТОР КНД	государственная информационная система «Типовое облачное решение по автоматизации контрольной (надзорной) деятельности»
Единый реестр видов контроля	Единый реестр видов федерального государственного контроля (надзора), регионального государственного контроля (надзора), муниципального контроля
ЕРКНМ	Единый реестр контрольных (надзорных) мероприятий
ЕПГУ	Единый портал государственных и муниципальных услуг, федеральная государственная информационная система
Закон № 247-ФЗ	Федеральный закон от 31 июля 2020 года № 247-ФЗ "Об обязательных требованиях в Российской Федерации"
Закон № 248-ФЗ	Федеральный закон от 31 июля 2020 года № 248-ФЗ "О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации".
ИИ	Искусственный интеллект
ИТ-активы	информационные технологии, информационные системы, компоненты информационно-телекоммуникационной инфраструктуры, информационно-телекоммуникационные сети, программные, программно-технические комплексы,

	отдельные программы для ЭВМ и оборудование
НПА	нормативный правовой акт
ОТ	обязательное требование
РФ	Российская Федерация
СИИ	система искусственного интеллекта
ФГИС	федеральная государственная информационная система
ЭВМ	электронная вычислительная машина

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

I. Нормативные правовые акты, программные документы

Конституция, федеральные законы:

1. Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 года с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 года) // Официальный интернет-портал правовой информации http://pravo.gov.ru, 06.10.2022.

2. «Гражданский кодекс Российской Федерации (часть четвертая)» от 18 декабря 2006 г. № 230-ФЗ // Собрание законодательства РФ. 2006. № 52 (1 ч.). Ст. 5496.

3. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. 2006. № 31 (1 ч.). Ст. 3448.

4. Федеральный закон от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» // Собрание законодательства РФ. 2009. № 7. Ст. 776.

5. Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» // Собрание законодательства РФ. 2010. № 31. Ст. 4179.

6. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» // Собрание законодательства РФ. 2011. № 15. Ст. 2036.

7. Федеральный закон от 24 апреля 2020 г. № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации - городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона "О персональных данных» // Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 24.04.2020.

8. Федеральный закон от 31 июля 2020 г. № 247-ФЗ «Об обязательных требованиях в Российской Федерации» // Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 31.07.2020.

9. Федеральный закон от 31 июля 2020 г. № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» // Официальный интернет-портал правовой информации http://pravo.gov.ru, 31.07.2020.

10. Федеральный закон от 31 июля 2020 г. № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» // Официальный интернет-портал правовой информации http://pravo.gov.ru, 31.07.2020.

11. Федеральный закон от 10 июля 2023 г. № 293-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных законодательных актов (положений законодательных актов) Российской Федерации» // Официальный интернет-портал правовой информации http://pravo.gov.ru, 10.07.2023.

12. Федеральный закон от 28 декабря 2024 г. № 540-ФЗ «О внесении изменений в Федеральный закон "О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» // Официальный интернет-портал правовой информации http://pravo.gov.ru, 28.12.2024.

Указы и иные акты Президента Российской Федерации, постановления и распоряжения Правительства Российской Федерации:

13. Указ Президента РФ от 22 мая 2015 г. № 260 «О некоторых вопросах информационной безопасности Российской Федерации» // Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 22.05.2015.

14. Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 06.12.2016.

15. Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» // Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 10.05.2017.

16. Указ Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» // Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 11.10.2019.

17. Указ Президента РФ от 31 марта 2023 г. № 231 «О создании, развитии и эксплуатации государственных информационных систем с использованием единой цифровой платформы Российской Федерации «ГосТех» // Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 01.04.2023.

18. Указ Президента РФ от 7 мая 2024 г. № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» // Официальный интернет-портал правовой информации http://pravo.gov.ru, 07.05.2024.

19. Послание Президента РФ Федеральному Собранию от 29 февраля 2024 г. // "Российская газета", N 46, 01.03.2024, "Парламентская газета", N 8, 01-06.03.2024.

20. Постановление Правительства РФ от 26 июня 1995 г. № 608 «О сертификации средств защиты информации» // Собрание законодательства РФ. 1995. № 27. Ст. 2579.

21. Постановление Правительства РФ от 5 апреля 2010 г. № 215 «Об утверждении Правил подготовки докладов об осуществлении государственного контроля (надзора), муниципального контроля в соответствующих сферах деятельности и об эффективности такого контроля (надзора)» // Собрание законодательства РФ. 2010. № 15. Ст. 1807.

22. Постановление Правительства РФ от 8 июня 2011 г. № 451 «Об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и

муниципальных функций в электронной форме» // Собрание законодательства РФ. 2011. № 24. Ст. 3503.

23. Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Собрание законодательства РФ. 2012. № 45. Ст. 6257.

24. Постановление Правительства РФ от 15 апреля 2014 г. № 313 «Об утверждении государственной программы Российской Федерации «Информационное общество» // Официальный интернет-портал правовой информации http://pravo.gov.ru, 24.04.2014.

25. Постановление Правительства РФ от 6 июля 2015 г. № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации» // Собрание законодательства РФ. 2015. № 28. Ст. 4241.

26. 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» // Официальный интернет-портал правовой информации http://pravo.gov.ru, 26.08.2016.

27. Постановление Правительства РФ от 28 октября 2020 г. № 1750 «Об утверждении перечня технологий, применяемых в рамках экспериментальных правовых режимов в сфере цифровых инноваций» // Собрание законодательства РФ. 2020. № 44. Ст. 7003.

28. Постановление Правительства РФ от 7 декабря 2020 № 2041 «Об утверждении требований к подготовке докладов о видах государственного контроля (надзора), муниципального контроля и сводного доклада о государственном контроле (надзоре), муниципальном контроле в Российской Федерации» // Собрание законодательства РФ. 2020. № 50 (часть V). Ст. 8241.

29. Постановление Правительства РФ от 6 февраля 2021 г. № 128 «Об утверждении Правил формирования, ведения и актуализации реестра обязательных требований» // Собрание законодательства РФ. 2021. № 7. Ст. 1132.

30. Постановление Правительства РФ от 2 апреля 2021 г. № 528 «О внесении изменений в некоторые акты Правительства Российской Федерации в части создания, эксплуатации и развития единого реестра видов федерального государственного контроля (надзора), регионального государственного контроля (надзора), муниципального контроля» // Официальный интернет-портал правовой информации http://pravo.gov.ru, 06.04.2021.

31. Постановление Правительства РФ от 16 апреля 2021 г. № 604 «Об утверждении Правил формирования и ведения единого реестра контрольных (надзорных) мероприятий и о внесении изменения в постановление Правительства Российской Федерации от 28 апреля 2015 г. N 415» // Официальный интернет-портал правовой информации http://pravo.gov.ru, 21.04.2021.

32. Постановление Правительства РФ от 25 июня 2021 г. № 990 «Об утверждении Правил разработки, утверждения и актуализации контрольными (надзорными) органами программы профилактики рисков причинения вреда (ущерба) охраняемым законом ценностям» // Официальный интернет-портал правовой информации http://pravo.gov.ru, 28.06.2021.

33. Постановление Правительства РФ от 29 июня 2021 г. № 1045 «О федеральном государственном контроле (надзоре) в области связи» // Официальный интернет-портал правовой информации http://pravo.gov.ru, 01.07.2021.

34. Постановление Правительства РФ от 1 декабря 2021 г. № 2148 «Об утверждении государственной программы Российской Федерации "Национальная система пространственных данных» // Собрание законодательства РФ. 2021. № 50 (часть IV), Ст. 8542.

35. Постановление Правительства РФ от 16 декабря 2022 г. № 2338 «Об утверждении Положения о единой цифровой платформе Российской Федерации «ГосТех», о внесении изменений в постановление Правительства Российской Федерации от 6 июля 2015 г. № 676 и признании утратившим силу пункта 6

изменений, которые вносятся в требования к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации, утвержденных постановлением Правительства Российской Федерации от 11 мая 2017 г. № 555» // Официальный интернет-портал правовой информации http://pravo.gov.ru, 20.12.2022.

36. Постановление Правительства РФ от 29 апреля 2023 г. № 683 «Об утверждении Положения о федеральной государственной информационной системе ведения Единого государственного реестра недвижимости и о внесении изменения в пункт 3 Правил информационного взаимодействия федеральной государственной информационной системы ведения Единого государственного реестра недвижимости с иными государственными или муниципальными информационными системами» // Официальный интернет-портал правовой информации http://pravo.gov.ru, 03.05.2023.

37. Постановление Правительства РФ от 1 июля 2024 г. № 900 «О порядке учета ИТ-активов, используемых для осуществления деятельности по цифровой трансформации системы государственного (муниципального) управления» // Официальный интернет-портал правовой информации http://pravo.gov.ru, 01.07.2024.

38. Распоряжение Правительства РФ от 1 ноября 2013 г. № 2036-р «Об утверждении Стратегии развития отрасли информационных технологий в Российской Федерации на 2014 - 2020 годы и на перспективу до 2025 года» // Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 08.11.2013.

39. Распоряжение Правительства РФ от 17 мая 2016 г. № 934-р «Об утверждении основных направлений разработки и внедрения системы оценки результативности и эффективности контрольно-надзорной деятельности» // Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 20.05.2016.

40. Распоряжение Правительства РФ от 23 мая 2017 г. № 999-р «О внесении изменений в основные направления разработки и внедрения системы оценки результативности и эффективности контрольно-надзорной деятельности, утвержденные распоряжением Правительства РФ от 17.05.2017 № 934-р» // Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 29.05.2017.

41. Распоряжение Правительства РФ от 7 октября 2019 г. № 2324-р «О внесении изменений в распоряжение Правительства РФ от 17.05.2016 № 934-р» // Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 10.10.2019.

42. Распоряжение Правительства РФ от 19 августа 2020 г. № 2129-р «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года» // Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 26.08.2020.

43. Распоряжение Правительства РФ от 6 октября 2021 г. № 2816-р «Об утверждении перечня инициатив социально-экономического развития Российской Федерации до 2030 года» // Собрание законодательства РФ. 2021. № 41. Ст. 7051.

44. Распоряжение Правительства РФ от 21 декабря 2023 г. № 3745-р «Об утверждении Концепции совершенствования контрольной (надзорной) деятельности до 2026 года» // Официальный интернет-портал правовой информации http://pravo.gov.ru, 25.12.2023.

Нормативные правовые и иные акты органов исполнительной власти:

45. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (Зарегистрировано в Минюсте России 31.05.2013 № 28608) // Российская газета, № 136, 26.06.2013.

46. Приказ Минкомсвязи России от 30 апреля 2019 г. № 178 «Об утверждении методик расчета целевых показателей национальной программы "Цифровая экономика Российской Федерации» // СПС «КонсультантПлюс».

47. Приказ МВД России от 15 июня 2021 г. № 444 «Об утверждении Положения о Департаменте информационных технологий, связи и защиты информации Министерства внутренних дел Российской Федерации» // СПС «КонсультантПлюс».

48. Приказ Минэкономразвития России от 29 июня 2021 г. № 392 «Об утверждении критериев определения принадлежности проектов к проектам в сфере искусственного интеллекта» (Зарегистрировано в Минюсте России 28.07.2021 № 64430) // Официальный интернет-портал правовой информации http://pravo.gov.ru, 29.07.2021.

49. Приказ МЧС России от 20 декабря 2021 г. № 889 «Об утверждении форм документов, используемых при осуществлении федерального государственного контроля (надзора) за безопасностью людей на водных объектах» (Зарегистрировано в Минюсте России 20.04.2022 № 68275) // Официальный интернет-портал правовой информации http://pravo.gov.ru, 20.04.2022.

50. Приказ Минцифры России от 6 декабря 2021 года № 1310 «Об утверждении индикативных показателей по федеральному государственному контролю (надзору) за соблюдением законодательства Российской Федерации о средствах массовой информации» // СПС «КонсультантПлюс».

51. Приказ Минцифры России от 15 декабря 2021 г. № 1344 «Об утверждении индикативных показателей для федерального государственного контроля (надзора) в области связи» // СПС «КонсультантПлюс».

52. Приказ Росреестра от 29 декабря 2021 г. № П/0642 «Об утверждении ведомственной программы цифровой трансформации Федеральной службы государственной регистрации, кадастра и картографии на 2022 финансовый год и плановый период 2023 - 2024 годов» // СПС «КонсультантПлюс».

53. Распоряжение МВД России от 11 января 2022 г. № 1/37 // СПС «КонсультантПлюс».

54. Приказ ФСБ России от 24 октября 2022 г. № 524 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных

(криптографических) средств» (Зарегистрировано в Минюсте России 23.11.2022 № 71073) // Официальный интернет-портал правовой информации http://pravo.gov.ru, 23.11.2022.

55. Приказ Россельхознадзора от 5 февраля 2024 г. № 132 «Об утверждении форм документов, используемых при осуществлении Федеральной службой по ветеринарному и фитосанитарному надзору и ее территориальными органами федерального государственного земельного контроля (надзора) на землях сельскохозяйственного назначения, оборот которых регулируется Федеральным законом «Об обороте земель сельскохозяйственного назначения», виноградопригодных земель» (Зарегистрировано в Минюсте России 16.05.2024 № 78167) // Официальный интернет-портал правовой информации http://pravo.gov.ru, 16.05.2024.

56. Приказ Минцифры России от 16 сентября 2024 г. № 773 «Об утверждении перечня индикаторов риска нарушения обязательных требований при осуществлении федерального государственного контроля (надзора) в сфере идентификации и (или) аутентификации» (Зарегистрировано в Минюсте России 21.10.2024 № 79838) // Официальный интернет-портал правовой информации http://pravo.gov.ru, 22.10.2024.

57. Ведомственная программа цифровой трансформации Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций на 2022–2024 годы // СПС «КонсультантПлюс».

Нормативно-технические и иные официальные документы:

58. ГОСТ Р 52292-2004. Информационная технология. Электронный обмен информацией. Термины и определения. / Утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 29 декабря 2004 года № 135-ст. М.: ИПК Издательство стандартов, 2005.

59. ГОСТ Р 43.0.2-2006. Национальный стандарт Российской Федерации. Информационное обеспечение техники и операторской деятельности. Термины и

определения. / Утвержден и введен в действие приказом Ростехрегулирования от 9 ноября 2006 г. № 245-ст. М.: Стандартинформ, 2007.

60. ГОСТ Р 60.0.0.2-2016. Национальный стандарт Российской Федерации. Роботы и робототехнические устройства. Классификация. / Утвержден и введен в действие приказом Росстандарта от 29 ноября 2016 г. № 1842-ст. М.: Стандартинформ, 2016.

61. ГОСТ Р 7.0.56-2017. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Международный стандартный сериальный номер (ISSN). Издательское оформление и использование. / Утвержден и введен в действие приказом Росстандарта от 19 декабря 2017 г. № 2027-ст. М.: Стандартинформ, 2018.

62. Паспорт федерального проекта «Цифровое государственное управление» (утв. президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности, протокол от 28.05.2019 № 9) // СПС «КонсультантПлюс».

63. ГОСТ Р 113.00.12-2023. Национальный стандарт Российской Федерации. Наилучшие доступные технологии. Термины и определения. / Утвержден и введен в действие приказом Росстандарта от 25 октября 2023 г. № 1231-ст. М.: ФГБУ "Институт стандартизации", 2023.

64. Письмо Росреестра от 29 января 2024 г. № 16-0616-МС/24 «О направлении информации» // СПС «КонсультантПлюс».

II. Специальная юридическая и иная литература

Книги, комментарии законодательства, учебники и учебные пособия:

65. *Аверкин, А.Н., Гаазе-Рапопорт, М.Г., Поспелов, Д.А.* Толковый словарь по искусственному интеллекту. М.: Радио и связь. 1992. 256 с.

66. Административное право: учебник / под ред. Л.Л. Попова, М.С. Студеникиной. — 3-е изд., перераб. и доп. — Москва: Норма: ИНФРА-М, 2021. 316 с.

67. Актуальные проблемы административного права и процесса: учебник для студентов вузов, обучающихся по направлению подготовки «Юриспруденция» / М. В. Костенников, А. В. Куракин, А. М. Кононов [и др.]. - 3-е изд., перераб. и доп. - Москва: ЮНИТИ-ДАНА, 2019. 479 с.

68. *Алексеев, С.С.* Теория государства и права: Учебник. М., 2005. 496 с.

69. *Алехин, А. П.* Административное право Российской Федерации: Учебник. В 2 частях. Ч. 1. Сущность и основные институты административного права / А. П. Алехин, Ю. М. Козлов. – М.: ТЕИС, 1994. 279 с.

70. *Амелин, Р.В., Чаннов, С.Е.* Эволюция права под воздействием цифровых технологий. Москва: НОРМА, 2023. 278 с.

71. *Андрюхина, Э.П.*, *Ахрем, И.В.*, *Бакурова, Н.Н. и др.* Правовое обеспечение государственного управления и исполнительная власть: учебник для магистров. Москва: Проспект, 2017. 336 с.

72. *Братановский, С.Н., Деменчук, Д.В.* Обеспечение законности в государственном управлении. Учебное пособие. М. 2016. 190 с.

73. *Бахтеев, Д.В.* Искусственный интеллект: этико-правовые основы: монография. М.: Проспект. 2021. 280 с.

74. *Васин, Е.О., Гвоздырева, А.Д., Дейнека, А.П., Замулина, А.Ю., Кривошеева, А.В., Незнамов, А.В., Фокина, С.А., Чаче, Э.Г., Черемных, И.А., Чурилова, Д.Ю.* Глобальный атлас регулирования искусственного интеллекта. Вектор БРИКС / под ред. А.В. Незнамова. 3-е изд., перераб. и доп. // СПС «КонсультантПлюс». 2024.

75. *Габричидзе, Б.Н.* Административное право. М.: Велби, 2003. 480 с.

76. *Добролюбова, Е. И., Южаков, В.Н., Старостина, А.Н.* Оценка качества государственного управления: обоснованность, результативность, эффективность: Монография. Москва: Издательский дом «Дело» (РАНХиГС), 2021. 282 с.

77. *Добробаба, М.Б., Чаннов, С.Е., Евсиков, К.С.* Правовое обеспечение применения цифровых технологий в государственном управлении: монография. Саратов.: Амирит, 2024. 156 с.

78. *Дьяконова, М. О., Ефремов, А. А., Зайцев, О. А. [и др.].* Цифровая экономика: актуальные направления правового регулирования: научно-практическое пособие / Под ред. И. И. Кучерова, С. А. Синицына. М.: ИЗиСП, НОРМА, 2022. 376 с.

79. *Ефремов, А.А., Добролюбова, Е.И., Талапина, Э.В., Южаков, В.Н.* Экспериментальные правовые режимы: зарубежный опыт и российский старт. Москва.: Дело, 2020. 126 с.

80. *Жеребин, В.М.* Информационное обеспечение АСУ. М., 1975. 200 с.

81. *Зинченко, В.П.* Искусственный интеллект и парадоксы психологии. Будущее искусственного интеллекта. М.: Наука, 1991. 302 с.

82. *Зубарев, С.М.* Система контроля в сфере государственного управления: Монография. Москва.: Норма, ИНФРА-М, 2023. 152 с.

83. *Зубарев, С. М., Лебедева, Е. А., Сабаева, С. В., Сладкова, А. В.* Цифровые технологии в системе государственного и общественного контроля: теоретико-правовые аспекты: Монография. М.: Проспект, 2022. 184 с.

84. *Залоило, М.В.* Искусственный интеллект в праве: научно-практическое пособие. М.: Инфотропик Медиа, 2021. 132 с.

85. *Исаков, В. Б.* Механизм правового регулирования и правовые режимы // Проблемы теории государства и права / Под ред. С. С. Алексеева. М.: Высшая школа, 1987. 400 с.

86. *Киселев, А. Г., Киричёк, П.Н.* Информация и коммуникация в государственном управлении: Монография. М.: ИНФРА-М, 2019. 268 с.

87. *Клепцов, М.Я.* Информационные системы органов государственного управления. М., 1996. 207 с.

88. *Лавров, С.С.* Интеллект искусственный и естественный // Будущее искусственного интеллекта. М.: Наука, 1991. 302 с.

89. *Мартынов, А.В.* Проблемы правового регулирования административного надзора в России. Административно-процессуальное исследование. Монография. М.: NOTA BENE, 2010. 548 с.

90. *Минбалеев, А.В.* Механизмы регулирования использования искусственного интеллекта // Право цифровой среды: Монография. М.: Проспект, 2022. 896 с.

91. *Минбалеев, А. В.* Проблемы цифрового права: Учебное пособие. Саратов: Амирит, 2022. 234 с.

92. *Поспелов, Д.А.* Фантазия или наука: на пути к искусственному интеллекту. М., 1982. 224 с.

93. *Попов, Л.Л.* Ренессанс государственного управления в России. Избранное. М., 2019. 368 с.

94. *Павлов, С.Н.* Системы искусственного интеллекта: учеб. пособие: в 2-х ч. Ч.1. Томск: Эль Контент, 2011. 176 с.

95. *Пономарева, Е. В.* Феномен квазисубъекта права: вопросы теории: Монография / Под ред. С. И. Архипова. М.: Юрлитинформ, 2020. 154 с.

96. Право искусственного интеллекта: учебник. Саратов: Амирит, 2024. 422 с.

97. Перспективные направления правового регулирования искусственного интеллекта: Монография / Под ред. А.В. Минбалеева. Саратов: Амирит, 2023. 441 с.

98. Проблемы развития и перспективы предпринимательского права в современных экономических условиях: Монография / Отв. ред. С.С. Занковский. М.: Проспект, 2021. 656 с.

99. *Рассолов, М. М.* Информационное право. М.: Юристъ, 1999. 400 с.

100. *Синяк, В.С., Агаджанян, С.И.* Информационное обеспечение ОАСУ. М., 1976. 136 с.

101. *Стахов, А. И.* Административно-процессуальная деятельность органов государственного контроля и надзора: Учебное пособие. М.: РГУП, 2017. 176 с.

102. *Студеникина, М. С.* Государственные инспекции в СССР. М., 1987. 108 с.

103. *Сергеев, В.М.* Искусственный интеллект: опыт философского осмысления // Будущее искусственного интеллекта. М.: Наука, 1991. 231 с.

104. *Стахов, А. И.* Нормативное регулирование и обеспечение безопасности в административно-правовой сфере: Монография. М.: Юрлитинформ, 2014. 256 с.

105. *Стахов, А.И.* Административно-публичное обеспечение безопасности в Российской Федерации: Монография. М., 2015. 199 с.

106. *Талапина, Э.В., Южаков, В.Н., Ефремов, А.А., Черешнева, И.А*. Возможности применения искусственного интеллекта в государственном управлении и юридические экспертизы. М.: Издательский дом «Дело» РАНХиГС, 2022. 190 с.

107. *Титаренко, Г.А., Федорова, Г.С.* Введение в проблематику информационного обеспечения АСУ. М., 1975. 56 с.

108. *Твердохлеб, Н.Г.* Машинная обработка экономической информации промышленных предприятий и объединений. М., 1979. 294 с.

109. *Тихомиров, О.К.* Искусственный интеллект: взгляд психолога // Будущее искусственного интеллекта. М.: Наука, 1991. 302 с.

110. *Тихомиров, Ю.А.* Публичное право. М., 1995. 485 с.

111. *Талапина, Э.В., Южаков, В.Н., Двинских, Д.Ю. и др.* Оборот данных в государственном управлении: перспективы правового регулирования. М., 2020. 244 с.

112. *Фесько, Д.С.* Административно-правовые гарантии обеспечения прав граждан и организаций при осуществлении государственного контроля (надзора): теория и практика: Монография / Под науч. ред. В.В. Черникова. М.: Проспект, 2023. 224 с.

113. Цифровая трансформация и государственное управление: научно-практическое пособие // А.С. Емельянов, А.А. Ефремов, А.В. Калмыкова и др. М.: Инфотропик Медиа, 2022. 224 с.

114. Цифровое право: учебник. 2-е изд., перераб. и доп. М.: Проспект, 2025. 848 с.

115. LegalTech, FinTech, RegTech etc.: правовые аспекты использования цифровых технологий в коммерческой деятельности: коллективная монография. М., 2021. 310 с.

Статьи и иные публикации:

116. *Архипов, В.В., Наумов, В.Б.* О некоторых вопросах теоретических оснований развития законодательства о робототехнике: аспекты воли и правосубъектности // Закон. 2017. № 5. С. 157 - 170.

117. *Антонов, А.А.* Искусственный интеллект: вопросы правосубъектности // Юрист. 2023. № 9. С. 23 - 28.

118. *Апостолова, Н.Н.* Ответственность за вред, причиненный искусственным интеллектом // Северо - Кавказский юридический вестник. 2021. № 1. С. 112 – 119.

119. *Агамагомедова, С.А.* Риск-ориентированный подход при осуществлении контрольно-надзорной деятельности: теоретическое обоснование и проблемы применения // Сибирское юридическое обозрение. 2021. Т. 18, № 4. С. 460 – 470.

120. *Архипов, В. В., Грачёва, А. В., Минбалеев, А. В., Наумов, В. Б., Полякова, Т. А.* Определение искусственного интеллекта в контексте российской правовой системы: критический подход // Государство и право. 2022. № 1. С. 168-178.

121. *Бачило, И.Л.* Информационное обеспечение государственного регулирования в области экономики. Правовые проблемы // Информационное общество. 1999. № 2. С. 19 – 25.

122. *Бояринцева, О. А.* Актуальные вопросы правового регулирования баз данных в условиях цифровой трансформации государственного управления // Аграрное и земельное право. 2020. № 7 (187). С. 120 - 123.

123. *Василевская, Л.Ю.* Искусственный интеллект: проблемы гражданско-правовой квалификации // Вестник Университета имени О.Е. Кутафина (МГЮА). 2023. № 5 (105). С. 32 - 40.

124. *Витко, В.* Анализ научных представлений об авторе и правах на результаты деятельности искусственного интеллекта // Интеллектуальная собственность. Авторское право и смежные права. 2019. № 3. С. 5 - 22.

125. *Волков, Ю. В.* Информационная правосубъектность // Теория государства и права. 2021. № 4 (25). С. 80 - 95.

126. *Гаджиев, Г.А., Войниканис, Е.А.* Может ли робот быть субъектом права (поиск правовых норм для регулирования цифровой экономики)? // Право. Журнал Высшей школы экономики. 2018. № 4. С. 24 – 48.

127. *Грищенко, Г.А.* Искусственный интеллект в государственном управлении // Российский юридический журнал. 2018. № 6. С. 27 - 31.

128. *Добробаба, М.Б., Чаннов, С.Е.* Применение цифровых технологий в целях противодействия совершения дисциплинарных коррупционных правонарушений в системе государственной службы // Информационное право. 2022. № 3 (73). С. 25 – 30.

129. *Добробаба, М.Б., Чаннов, С.Е., Минбалеев, А.В.* Квантовые коммуникации: перспективы правового регулирования // Вестник Университета имени О.Е. Кутафина (МГЮА). 2022. № 4 (92). С. 25 - 37.

130. *Дмитрик, Н. А.* Цифровая трансформация: правовое измерение // Правоведение. 2019. Т. 63. № 1. С. 28 - 46.

131. *Евсиков, К.С.* Государственно-правовые концепции использования информационных технологий в государственном управлении // Lex Russica (Русский закон). 2022. № 1. С. 74 - 86.

132. *Ермолова, О.Н.* Обязательные требования к предпринимательской деятельности: вопросы контроля и ответственности // Имущественные отношения в Российской Федерации. 2022. № 5. С. 60 – 75.

133. *Ефремов, А. А.* Государственный суверенитет в условиях цифровой трансформации // Правоведение. 2019. Т. 63. № 1. С. 47 - 61.

134. *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.

135. *Зубарев, С.М.* Правовые риски цифровизации государственного управления // Актуальные проблемы российского права. 2020. № 6. С. 23 – 32.

136. *Зубарев, С.М.* Цифровизация государственного управления: новая административная реформа? // Административное право и процесс. 2020. № 7. С. 17 - 21.

137. *Зубарев, С.М., Сабаева, С.В.* Правовое регулирование цифровых технологий государственного контроля: опыт субъектов Российской Федерации // Российская юстиция. 2020. № 7. С. 17 – 21.

138. *Зубарев, С.М.* О единой системе правового регулирования цифровых технологий государственного и общественного контроля // Законы России: опыт, анализ, практика. 2021. № 11. С. 29 -37.

139. *Исакова, К.В.* Проблемы философии искусственного интеллекта // Гуманитарный научный журнал. 2022. № 2. С. 125 – 128.

140. *Крысанова, Н. В.* К вопросу о правосубъектности и правовом развитии искусственного интеллекта // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Серия 4. Государство и право: реферативный журнал. 2021. № 1. С. 23 – 31.

141. *Комиссаров, А.В., Комиссаров, М.А., Абакумова, Е.Ю.* Современные подходы в правовом обеспечении механизма государственного контроля предпринимательской деятельности // Право и экономика. 2023. № 9. С. 35 - 40.

142. *Косоруков, А.А.* Технологии искусственного интеллекта в современном государственном управлении // Социодинамика. 2019. № 5. С. 43 – 58.

143. *Кириллова, Е. А.* Правовой статус и принципы использования технологии больших данных (Big Data) // Российская юстиция. 2021. № 2. С. 68-69.

144. *Конев, С. И.* Контроль и надзор за соблюдением законодательства в области данных о личности в условиях роботизации // Государственная служба и кадры. 2020. № 3. С. 211 - 216.

145. *Кузнецов, П. У.* Цифровая трансформация государственного управления как этап развития информатизации в России // Вестник Южно-Уральского государственного университета. Серия: Право. 2021. Т. 21. № 1. С. 84 - 95.

146. *Лагаева, В. П.* Профилактика нарушений обязательных требований: понятие, цели и функции // Правовое обеспечение суверенитета России: проблемы и перспективы: Сборник докладов XIII Московской юридической недели. В 4 ч. Ч. 4 / редколлегия: С. М. Зубарев [и др.]. – М.: Издательский центр Университета имени О.Е. Кутафина (МГЮА), 2024. С. 108 - 112.

147. *Лагаева, В. П.* Влияние искусственного интеллекта на цифровой суверенитет России // Правовое обеспечение суверенитета России: проблемы и перспективы: Сборник докладов XIII Московской юридической недели. В 4 ч. Ч.1 / редколлегия: А. В. Корнев [и др.]. – М.: Издательский центр Университета имени О.Е. Кутафина (МГЮА), 2024. С. 201 – 204.

148. *Лагаева, В. П.* Правовые основания применения технологий искусственного интеллекта в обработке данных государственного контроля (надзора) // Формирование многополярного мира: вызовы и перспективы: Сборник докладов XI Московского юридического форума. В 3 ч. Ч. 3 / редколлегия: С. М. Зубарев [и др.]. М.: Издательский центр Университета имени О.Е. Кутафина (МГЮА), 2024. С. 651-656.

149. *Лагаева, В. П.* Технологическая нейтральность принципов государственного контроля (надзора) // Аграрное и земельное право. 2024. № 10 (238). С. 120-121.

150. *Лагаева, В. П.* Правовое регулирование применения искусственного интеллекта в профилактике нарушений обязательных требований // Аграрное и земельное право. 2024. № 7(235). С. 95-98.

151. *Лагаева, В. П.* О профилактическом визите как новом мероприятии профилактики нарушений обязательных требований индивидуальными предпринимателями и юридическими лицами // Административное право и процесс. 2023. № 6. С. 69-71.

152. *Лагаева, В. П.* Доверенные технологии искусственного интеллекта в сфере государственного контроля (надзора): правовые аспекты // Право для лидерства : Сборник материалов XII Московского инновационного юридического

форума / редколлегия: Е. В. Вавилин [и др.]. М.: Издательский центр Университета имени О.Е. Кутафина (МГЮА), 2025. С. 102 – 104.

153. *Липатов, А.Г.* Возможности использования искусственного интеллекта для управления большими информационными массивами данных Big Data // Инновации и инвестиции. 2023. № 5. С. 187 - 189.

154. *Мартынов, А.В.* Использование современных цифровых технологий при осуществлении профилактической деятельности контрольно-надзорных органов исполнительной власти // Юрист. 2020. № 10. С. 48 - 56.

155. *Мартынов, А.В.* Актуальные вопросы применения искусственного интеллекта при осуществлении контрольно-надзорной деятельности органов исполнительной власти // Вестник Нижегородского университета им. Н.И. Лобачевского. 2020. № 2. С. 175 - 186.

156. *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.

157. *Мартынов, А.В.* Критический анализ общих положений Федерального закона от 31 июля 2020 г. № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» // Актуальные вопросы контроля и надзора в социально значимых сферах деятельности общества и государства: Материалы VI Всероссийской научно-практической конференции (Россия, г. Нижний Новгород, 1 июля 2021 г.) / Отв. ред. доктор юридических наук, профессор А.В. Мартынов. Н. Новгород: Изд-во Нижегородского государственного университета им. Н.И. Лобачевского, 2021. С. 31 - 59.

158. *Мартынов, А.В.* Применение риск-ориентированного подхода при осуществлении государственного контроля и надзора как необходимое условие снижения давления на бизнес // Юрист. 2016. № 18. С. 22 – 27.

159. *Медведева, Н.Г.* Ключевые направления реформирования и совершенствования правового обеспечения контрольно-надзорной деятельности в

Российской Федерации // Общество: политика, экономика, право. 2021. № 8(97). С. 71 - 78.

160. *Минбалеев, А. В.* Принципы информационного права // Вестник ЮУрГУ. Серия: Право. 2015. № 1. С. 79 - 84.

161. *Минбалеев, А.В.* Регулирование использования искусственного интеллекта в России // Информационное право. 2020. № 1. С. 36 – 39.

162. *Минбалеев, А.В.* Понятие искусственный интеллект в праве // Вестник Удмуртского университета. 2022, Т. 32, вып. 6. С. 1097 – 1098.

163. *Минбалеев, А. В.* Формирование экономики данных в России в условиях многополярного мира: проблемы правового обеспечения // Экономика и управление. 2023. Т. 29. № 8. С. 956 - 963.

164. *Морхат, П.М.* Риски и угрозы, связанные с применением искусственного интеллекта // Аграрное и земельное право. 2017. № 12 (156). С. 62 – 63.

165. *Морхат, П.М.* Юнит искусственного интеллекта как электронное лицо // Вестник Московского государственного областного университета. Серия: Юриспруденция. 2018. № 2. С. 61 – 73.

166. *Москвитина, Н. В.* Цифровая трансформация государственного управления // Социология. 2021. № 4. С. 114 - 128.

167. *Назаров, Н.А.* Обеспечение качества данных при автоматизированном принятии решений в государственном управлении // Журнал российского права. 2024. № 5. С. 140 - 155.

168. *Наумов, В. Б.* Право в эпоху цифровой трансформации: в поисках решений // Российское право: образование, практика, наука. 2018. № 6 (108). С. 4 - 11.

169. *Певцова, Е.А.* Влияние искусственного интеллекта на правовую деятельность человека // Журнал российского права. 2020. № 9. С. 19 – 31.

170. *Понкин, И.В.* Машинная правовая аналитика: понятие, онтология и значение для правовой деятельности // Государственная служба. 2022. Т. 24. № 6. С. 40 - 46.

171. *Полякова, Т. А.* Влияние цифровой трансформации на развитие информационного права: тенденции, проблемы, перспективы // Мониторинг правоприменения. 2020. № 2 (35). С. 53 - 58.

172. *Савельев, А. И.* На пути к концепции регулирования данных в условиях цифровой экономики // Закон. 2019. № 4. С. 174 - 195.

173. *Смирнова, Е.Н.* Профилактика нарушений обязательных требований как важнейшее направление деятельности органов исполнительной власти, осуществляющих функции контроля и надзора // Административное право и процесс. 2018. № 4. С. 44 - 47.

174. *Сивицкий, В. А.* Принцип системности законодательства и его влияние на использование в федеральных законах принципов регулирования отношений в конкретных сферах // Юридическая техника. 2020. № 14. С. 305 - 307.

175. *Талапина, Э.В.* Государственное управление: проблемы и перспективы правового регулирования // Законы России: опыт, анализ, практика. 2015. № 3. С. 96 - 101.

176. *Талапина, Э. В.* Сравнительное цифровое право: становление и перспективы // Журнал российского права. 2021. № 9. С. 18 - 32.

177. *Тихомиров, Ю. А.* Правовые риски // Законы России: опыт, анализ, практика. 2012. № 2. С. 87 - 95.

178. *Филиппова, И.А., Коротеев, В.Д.* Будущее искусственного интеллекта: объект или субъект права? // Journal of Digital Technologies and Law. 2023. № 1(2). С. 359 – 386.

179. *Хатуаев, В.У.* Об убеждении как основном общем методе реализации государственной власти: состояние и некоторые проблемы совершенствования // Административное право и процесс. 2022. № 1. С. 7 – 10.

180. *Холодная, Е.В.* О перспективных направлениях правового регулирования в сфере технологии искусственного интеллекта // Вестник Университета имени О.Е. Кутафина (МГЮА). 2019. № 12. С. 89 - 96.

181. *Южаков, В.Н., Александров, О.В., Талапина, Э.В.* О системности правового регулирования государственного управления в Российской Федерации // Журнал российского права. 2015. № 7. С. 114 - 121.

182. Allen J. AI Growing up / J. Allen // AI MAGAZINE. 1998. V. 19. №4. P. 13–23.

Диссертации и авторефераты:

183. *Ковалева, Н.Н.* Административно-правовое регулирование использования информационных технологий в государственном управлении: автореф. дис. … д-ра юрид. наук. Саратов, 2014. 54 с.

184. *Комаров, К.Б.* Государственное управление: средства в экономической сфере: автореф. дис. ... канд. юрид. наук. Екатеринбург, 2000. 27 с.

185. *Морхат, П.М.* Правосубъектность искусственного интеллекта в сфере права интеллектуальной собственности: гражданско-правовые проблемы: дис. ... д-ра юрид. наук. Москва, 2018. 420 с.

186. *Талапина, Э.В.* Модернизация государственного управления в информационном обществе: информационно-правовое исследование: дис. … д-ра юрид. наук. Москва, 2015. 469 с.

187. *Щитова, А.А.* Правовое регулирование информационных отношений по использованию систем искусственного интеллект: автореф. дис. … канд. юрид. наук. Москва, 2022. 29 с.

Интернет-источники на русском языке:

188. Ассоциация "Альянс в сфере искусственного интеллекта". URL: https://a-ai.ru/ (дата обращения: 01.08.2024).

189. *Грамматчиков, А.* Бот выходит на охоту // Эксперт. URL: https://expert.ru/expert/2021/40/bot-vykhodit-na-okhotu/ (дата обращения: 01.12.2023).

190. Глобальный инновационный индекс 2024. Резюме. URL: https://www.wipo.int/edocs/pubdocs/ru/wipo-pub-2000-2024-exec-ru-global-innovation-index-2024.pdf (дата обращения: 10.06.2025).

191. «Государство для людей» - федеральный проект. URL: https://xn--80aebecah6apa1adyldqm2sra.xn--p1ai/?ysclid=lzd61texed443635177 (дата обращения: 02.08.2024).

192. Госуслуги будущего: как ИИ, чат-боты и онлайн-сервисы изменят Росреестр. РБК Тренды. URL: https://trends.rbc.ru/trends/innovation/cmrm/5fa58d829a79472be3ef41c2?from=copy (дата обращения 29.03.2024).

193. Жители ЦАО стали самыми активными пользователями чат-бота «Свободный доступ» / Новости города / Сайт Москвы. URL: https://www.mos.ru/news/item/124585073/?ysclid=m0y9rnvwtz893686925 (дата обращения: 04.08.2024).

194. «Чат-ботом «Свободный доступ» воспользовались около 1,7 тысячи москвичей». URL: https://www.mos.ru/news/item/129014073/ (дата обращения: 12.11.2023).

195. Использование БПЛА при земельном надзоре Росреестра в Калужском регионе. URL: https://www.kaluga-gov.ru/news/45596/ (дата обращения: 01.08.2024).

196. Кодекс этики в сфере искусственного интеллекта. URL: https://ethics.a-ai.ru/assets/ethics_files/2023/05/12/Кодекс_этики_20_10_1.pdf (дата обращения: 20.11.2023).

197. Индекс развития электронного правительства | Эфиопия. Данные по годам. URL: https://statbase.ru/data/eth-e-government-development-index/ (дата обращения: 10.06.2025).

198. ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ — Научно-технический словарь URL: gufo.me (дата обращения: 20.11.2023).

199. Национальный центр развития ИИ при Правительстве Российской Федерации. URL: https://ai.gov.ru/ (дата обращения: 01.08.2024).

200. Особенности политики государств-участников БРИКС в сфере развития ИКТ, обеспечения национальной и международной информационной безопасности. URL: https://namib.online/wp-content/uploads/2024/05/BRICS.pdf (дата обращения: 10.06.2025).

201. Национальный портал в сфере Искусственного интеллекта (ИИ) и применения нейросетей в России. URL: https://ai.gov.ru/?ysclid=mgba74yejg29248793 (дата обращения: 01.08.2024).

202. Роскомнадзор - Состоялось расширенное заседание коллегии Роскомнадзора. URL: https://rkn.gov.ru/press/news/news73648.htm (дата обращения: 01.08.2024).

203. Чат-бот «Онлайн-инспектор» предоставил свыше 90 тыс. консультаций. URL:https://rostrud.gov.ru/press_center/novosti/1152320/?ysclid=m0y9feqvw6632948876 (дата обращения: 02.08.2024).

204. Яндекс: Искусственный интеллект для управления большими данными Big Data [Электронный ресурс]. URL: https://yandex.ru/vc.ru/u/1266146-404/550756 (дата обращения: 18.03.2024).

205. Пекинская декларация XIV саммита БРИКС. URL: http://www.kremlin.ru/supplement/5819 (дата обращения: 25.10.2023).

206. Си Цзиньпин призвал БРИКС сформировать общую структуру управления ИИ. URL: https://rfi.mnr.gov.ru/news/Mass_media_about_digitalization/si-tszinpin-prizval-briks-sformirovat-obshchuyu-strukturu-upravleniya-ii (дата обращения: 01.10.2023).

207. Институт будущей сети БРИКС. URL: https://www.bifn.org/ru/study_groups/ai_sg.html (дата обращения: 15.10.2024).

208. Развитие технологий и искусственного интеллекта в странах БРИКС. URL: https://news.rambler.ru/tech/52853325-razvitie-tehnologiy-i-iskusstvennogo-intellekta-v-stranah-briks/?ysclid=msa1tio99s643549087 (дата обращения: 15.10.2024).

209. Риски использования искусственного интеллекта. URL: www.tadviser.ru/index.php/Статья:Риски_использования_искусственного_интеллекта?ysclid=m51kfhe4hg769042846 (дата обращения: 25.11.2024).

210. Какие риски несет использование искусственного интеллекта в бизнесе. URL: https://monocle.ru/monocle/2024/50/kakiye-riski-neset-ispolzovaniye-iskusstvennogo-intellekta-v-biznese/?ysclid=m51ljhnsl437481835 (дата обращения: 25.11.2024).

211. Регулирование генеративного ИИ. URL: https://yakovpartners.ru/publications/gen-ai-regulation/ (дата обращения: 15.01.2025).

Интернет-источники на иностранных языках:

212. Perpres Nomor 39 Tahun 2019 // URL: https://commons.wikimedia.org/wiki/File:Perpres_Nomor_39_Tahun_2019.pdf. (дата обращения: 13.01.2025).

213. Brazil’s AI Act: A New Era of AI Regulation - GDPR Local. URL: https://gdprlocal.com/brazils-ai-act-a-new-era-of-ai (дата обращения: 30.04.2025).

214. AI-Powered Land Monitoring Reveals Over 40,000 Cases of Unauthorized Land Use Change in Iran. URL: https://www.cryptopolitan.com/ai-detects-unlawful-land-use-in-iran/?ysclid=mscy6yytnu374924249 (дата обращения: 30.04.2025).

215. the Regulations on the Promotion of Artificial Intelligence Industry in Shenzhen. URL: http://www.szrd.gov.cn/rdlv/chwgg/content/post_834228.html (дата обращения: 14.04.2023).

216. Regulations of Shanghai on Promoting the Development of Artificial Intelligence Industry. URL: http://www.shrd.gov.cn/n8347/n8467/u1ai248931.html (дата обращения: 14.04.2023).

217. Responsible Artificial Intelligence for the Indian Justice System. URL: https://vidhilegalpolicy.in/research/responsible-ai-for-the-indian-justice-system-a-strategy-paper/ (дата обращения: 04.07.2023).

218. Guidance on AI and Big Data-based medical devices. URL: https://beta.sfda.gov.sa/sites/default/files/2021-04/SFDAArtificial%20IntelligenceEn.pdf (дата обращения: 18.07.2023).

219. International Center for Artificial Intelligence Research and Ethics, ICAIRE. URL: https://saudipedia.com/en/international-center-for-artificial-intelligence-research-and-ethics-icaire (дата обращение: 26.08.2024).

220. Ethical Guidelines for Application of Artificial Intelligence in Biomedical Research and Healthcare. URL: https://www.thehindu.com/sci-tech/health/icmr-releases-the-countrys-first-ethical-guidelines-for-application-of-ai-in-biomedical-research-and-healthcare/article66657158.ece (дата обращения: 27.03.2023).

221. Artificial Intelligence Standardization White Paper (2021 Edition). URL: https://cset.georgetown.edu/publication/artificial-intelligence-standardization-white-paper-2021-edition/ (дата обращения: 11.07.2024).

222. Beijing AI Principles. URL: https://www-pre.baai.ac.cn/news/beijing-ai-principles-en.html (дата обращения: 12.10.2023).

223. Egyptian Charter for Responsible AI. URL: https://aicm.ai.gov.eg//en/Resources/EgyptianCharterForResponsible AIEnglish-v1.0.pdf (дата обращения: 12.10.2023).

224. A Next Generation Artificial Intelligence Development Plan. URL: https://chinacopyrightandmedia.wordpress.com/2017/07/20/a-next-generation-artificial-intelligence-development-plan/ (дата обращения: 23.05.2024).

225. UAE National AI Strategy 2031. URL: https://ai.gov.ae/wp-content/uploads/2021/07/UAE-National-Strategy-for-Artificial-Intelligence-2031.pdf (дата обращения: 19.07.2023).

226. National Strategy For Artificial Intelligence #AIforAll. URL: https://indiaai.gov.in/research-reports/national-strategy-for-artificial-intelligence (дата обращения: 30.06.2023).

227. Saudi Arabia's National AI Strategy - Vision 2030. URL: https://oecd.ai/en/dashboards/policy-initiatives/http:%2F%2Faipo.oecd.org%2F2021-data-policyInitiatives-26017 (дата обращения: 18.07.2023).

228. Egypt National Artificial Intelligence Strategy. URL: https://andp.unescwa.org/sites/default/files/2021-11/Publications_672021000_Egypt-National-AI-Strategy-English.pdf (дата обращение: 24.10.2023).

229. BSAI/EBIA. URL: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ebia-summary_brazilian_4-979_2021.pdf (дата обращения: 24.10.2023).

230. Ethiopian National AI Policy. URL: https://aii.et/the-council-of-ministers-unanimously-decide-to-implement-the-national-artificial-intelligence-policy/ (дата обращения: 13.01.2025).

231. National Digital and Future Skills Strategy South Africa. URL: https://www.gov.za/sites/default/files/gcis_ document/202009/43730gen513.pdf (дата обращения: 13.10.2023).

232. Strategi Nasional Kecerdasan Artifisial Indonesia. URL: https://ai-innovation.id/images/gallery/ebook/stranas-ka.pdf (дата обращения: 13.01.2025).

233. Digital ID Proclamation № 1284/2023, 2 July 2023. URL: https://www.lawethiopia.com/index.php/volume-3/6967- digital-id-proclamation-no-1284-2023 (дата обращения: 25.10.2024).

234. Information Technology Products Security Clearance and Control Proclamation. URL: https://lawethiopiacomment.wordpress.com (дата обращения: 15.03.2024).

235. Regulation «On the Management of Deep Synthesis Technologies in Information Services on the Internet». URL: https://digichina.stanford.edu/work/translation-internet-information-service-deep-synthesis-management-provisions-draft-for-comment-jan-2022/ (дата обращения: 15.03.2024).

236. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and

(EU) 2020/1828 (Artificial Intelligence Act): URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng (дата обращения: 02.08.2024).