

УДК 004.8; 342

ПРАВОВЫЕ РИСКИ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО  
ИНТЕЛЛЕКТА В ГОСУДАРСТВЕННОМ УПРАВЛЕНИИ

*Колюхов Вадим*, студент РЭУ им. Г.В. Плеханова

*Абрамян Алика*, студентка РЭУ им. Г.В. Плеханова.

Научный руководитель: *Лозовицкая Галина Петровна*, доктор юридических

наук, доцент, профессор кафедры государственно-правовых и уголовно-

правовых дисциплин РЭУ им. Г.В. Плеханова

Город Москва, Стремянный переулок, дом 36.

**Аннотация:** Статья посвящена анализу правовых рисков, связанных с использованием технологий искусственного интеллекта (ИИ) в государственном управлении. В условиях стремительного развития ИИ и его интеграции в различные сферы общественной жизни актуальность рамочности правовых границ неуклонно возрастает. Основное внимание уделяется основным рискам, которые могут возникнуть при внедрении ИИ в процессы принятия решений, включая вопросы ответственности, защиты персональных данных, а также соблюдения нормативных актов.

**Ключевые слова:** искусственный интеллект, государственное управление, правовые риски, ответственность, защита данных, нормативное регулирование, этика, интеграция технологий.

**Legal risks of using artificial intelligence in public administration**

Vadim Kolyukhov, a student of Plekhanov Russian University of Economics

Alika Abramian, a student of Plekhanov Russian University of Economics.

Scientific supervisor: Galina Petrovna Lozovitskaya, Doctor of Law, Associate Professor, Professor of the Department of State Law and Criminal Law Disciplines at Plekhanov Russian University of Economics

36 Stremyanny Lane, Moscow

**Abstract:** The article is devoted to the analysis of legal risks associated with the use of artificial intelligence (AI) technologies in public administration. With the rapid development of AI and its integration into various spheres of public life, the relevance of the legal framework is steadily increasing. The focus is on the main risks that may

arise when implementing AI in decision-making processes, including issues of responsibility, personal data protection, and compliance with regulations.

**Keywords:** artificial intelligence, public administration, legal risks, responsibility, data protection, regulatory regulation, ethics, technology integration.

### Введение

Современное общество переживает уникальный этап своей эволюции, характеризующийся прорывными технологиями, которые кардинально меняют формы взаимодействия людей, бизнеса и государства. Одной из наиболее значимых инноваций стал искусственный интеллект (ИИ). Технологии ИИ быстро проникают в самые различные сферы, включая здравоохранение, образование, оборону, промышленность и, что важно, государственное управление. Именно в этой области потенциал ИИ кажется особенно перспективным: используются интеллектуальные системы для анализа больших данных, цифровизации услуг, предиктивной аналитики, автоматизации принятий решений и оптимизации управленческих процессов.

С внедрением ИИ возрастают не только возможности для повышения эффективности работы государственных органов, но и серьезные вызовы, в том числе на правовом уровне. Использование ИИ в управлении государственными институтами связано с формированием новых норм и стандартов, а также с необходимостью поиска баланса между инновациями, соблюдением прав и свобод граждан, прозрачностью принятий решений и национальной безопасностью.

В данной статье проводится комплексный анализ правовых рисков, связанных с использованием искусственного интеллекта в государственном управлении. Изучаются существующие подходы к регулированию ИИ в государственных структурах, проблемы, возникающие в процессе интеграции технологий в юридическую практику, и возможные пути их преодоления.

### Цели и задачи авторского исследования

Целью настоящей статьи является всесторонний анализ правовых рисков при использовании искусственного интеллекта в государственном управлении, а

также выработка предложений по минимизации указанных рисков на основе российских и международных практик.

Для достижения поставленной цели были определены следующие задачи:

- дать определение искусственного интеллекта как объекту регулирования;
- проанализировать историю формирования вопроса правовых рисков при внедрении ИИ;
- выявить ключевые правовые риски при использовании ИИ в государственных структурах;
- проанализировать современные российские и зарубежные подходы к регулированию данных рисков;
- сформулировать выводы и предложения, направленные на совершенствование законодательства и практики применения ИИ в государственном управлении.

### История проблемы и ее актуальность

Вопросы правового регулирования новых технологий неизменно следуют за их развитием. Искусственный интеллект в качестве прикладной технологии начал свое «победное шествие» в 1950–60-е годы, однако за рамки теоретических рассуждений и ограниченных приложений в научных центрах он долгое время не выходил. Настоящий рывок произошел с развитием вычислительной техники и накоплением соответствующих массивов данных в конце XX — начале XXI века.

В государственном секторе появление ИИ как инструмента управления было связано с необходимостью оптимизации бюрократических процедур, повышения прозрачности и уменьшения коррупционных рисков. Первые проекты автоматизации и цифровизации государственных услуг в Российской Федерации реализовывались как часть Электронного правительства (начиная с 2002 года). Однако на тот момент ключевой задачей была оцифровка и

стандартное распределение ресурсов и информации, а не полноценное делегирование принятия решений интеллектуальным системам [1, 9].

Постепенно роль ИИ стала увеличиваться с появлением интеллектуальных чат-ботов, систем предиктивной аналитики для прогнозов (например, экономических или демографических [10, 11]), а также внедрением автоматизированных комплексов в сфере государственного контроля и надзора. Однако уже достаточно быстро возник вопрос: до какой степени государство вправе делегировать свои функции усовершенствованным, но не человеческим «агентам»? Каким образом обеспечивается ответственность за решения, принимаемые с помощью ИИ? Кто отвечает за ошибочные или даже дискриминационные решения системы? Как обеспечить при этом безопасность?

Мировое сообщество также столкнулось с тем, что ИИ способен не только радикально ускорять обработку информации, но и создавать новые риски — от “ошибок” алгоритмов с тяжелыми последствиями до нарушения фундаментальных прав граждан [12], таких как право на справедливое разбирательство, защиту персональных данных и равенство перед законом.

Здесь возникает целый комплекс правовых коллизий, для которых современные правовые системы зачастую еще не имеют стройного инструментария.

#### Содержание исследования

1. Определение искусственного интеллекта и специфика его использования в государственном секторе

В широком смысле искусственный интеллект — это комплекс технологий, позволяющих вычислительным системам имитировать различные аспекты человеческого разума: восприятие, обучение, анализ, принятие решений и даже творчество. Ключевыми видами ИИ в государственном управлении выступают:

- Системы поддержки принятия решений (СППР), которые анализируют огромные массивы данных и предлагают управленцам обоснованные решения на основе прогнозной аналитики.

- Системы автоматизированной обработки обращений граждан, например, чат-боты и голосовые помощники.
- Интеллектуальные платформы для госуслуг, которые автоматизируют процесса взаимодействия граждан и государства (запись к врачу, оформление документов, приложения для сбора фидбека от пользователей).

Внедрение ИИ позволяет повысить скорость, объективность и прозрачность деятельности госорганов. Однако автоматизация требует юридически четких критериев безопасности и ответственности [2].

## 2. Классификация правовых рисков использования ИИ в государственном управлении

Правовые риски внедрения ИИ в государственный сектор можно разделить на следующие основные группы:

а) Риски, связанные с определением ответственности.

Передача функций принятия решений машине ведет к “размытию” субъектов ответственности. Если система, например, совершила ошибку, повлекшую за собой ущемление прав гражданина, неочевидно, кто юридически является ответственным: разработчик ПО, оператор, чиновник, подписавший документы, или само государство. Эту проблему обозначают как “проблему рассеянной ответственности”, пока не имеющую универсального решения.

б) Нарушение прав на защиту персональных данных и частной жизни.

Для эффективной работы ИИ требуется обработка массивов персональных и чувствительных данных. Это обуславливает дополнительные риски утечки, несанкционированного доступа, а также последующего дискриминационного использования информации об отдельных группах граждан.

в) Прозрачность и объяснимость решений ИИ.

Фактически часть алгоритмов, применяемых сегодня в ИИ, относятся к категории “черного ящика”: даже создателям системы затруднительно объяснить, почему она вынесла то или иное решение. Это угрожает ключевому

принципу административной справедливости — праву на получение объяснения решения. Гражданин, столкнувшийся с отказом (например, в начислении социальной выплаты), имеет право знать, почему так произошло и что может быть обжаловано.

г) Не дискриминация и принцип равенства.

Если ИИ работает на основе исторических данных, он может “унаследовать” предвзятость или дискриминацию по социальным, этническим, гендерным или иным признакам. Государство, использующее ИИ-системы при распределении ресурсов или принятии решений, обязано обеспечить равный доступ и защиту от дискриминационных алгоритмов.

д) Компетенция государственных органов и соблюдение административных процедур.

Закон устанавливает конкретные процедуры принятия управленческих решений и исчерпывающий перечень субъектов, наделенных соответствующими полномочиями. Делегирование функций ИИ без точной юридической регламентации может привести к конфликту с принципом легитимности власти.

### 3. Анализ международного и российского опыта регулирования.

#### Международные подходы

За последние годы проблема регулирования ИИ активно обсуждается на международной арене. Еще в 2019 году ОЭСР приняла "Руководящие принципы для развития ИИ", призывающие к обеспечению прозрачности, безопасности, ответственности и справедливости при внедрении ИИ. Европейский Союз стал одним из первых регионов мира, инициировавших создание специального законодательного акта об искусственном интеллекте — Artificial Intelligence Act, который в 2024 году находится на финальной стадии утверждения [3].

Принципиальные положения европейского регулирования:

- Классификация ИИ по уровням риска: запрещенные, высокорисковые, ограниченно рискованные и минимального риска системы; для первых двух категорий вводятся строгие требования по сертификации, прозрачности и возможности объяснения решений.

- Обязательство государственных органов обеспечивать защиту персональных данных при использовании ИИ, в том числе в цифровых госуслугах.
- Система аудита и контроля за ИИ-приложениями, используемыми в социально значимых областях.

Другим ориентиром для национальных законодательств служат документы ООН и Совета Европы, где значительное внимание уделяется вопросам соблюдения прав человека и предотвращения возможных злоупотреблений со стороны государства.

#### Российская действительность

В России первые попытки создать рамочное регулирование были предприняты в конце 2010-х годов. В 2019 году утвержден национальный проект "Искусственный интеллект", предусматривающий разработку стандартов и правовых актов в этой сфере. В июле 2020 года утверждена государственная программа «Цифровая экономика Российской Федерации», отдельный раздел которой посвящен развитию и внедрению ИИ.

Однако до сих пор российское законодательство не содержит отдельного федерального закона, полностью посвященного регламентации ИИ. Основные правовые нормы сформулированы в ряде федеральных законов (например, "О персональных данных", "Об информации, информационных технологиях и о защите информации"), а также в подзаконных актах и стандартах технического регулирования [4].

В 2020 году был принят региональный закон города Москвы "Об экспериментальном правовом режиме в сфере цифровых инноваций в Москве", который впервые создал "песочницу" для опробования ИИ в госуправлении с особыми условиями для защиты персональных данных и обеспечения отчетности.

В целом российская практика скорее отстает от законодательных инициатив ЕС, опираясь на рамочные подходы и развитие экспериментальных правовых режимов, а не на универсальное регулирование проблем.

#### 4. Практические примеры правовых рисков

Для понимания масштабов и характера правовых рисков предложения целесообразно рассмотреть конкретные кейсы из мировой и российской практики.

##### Пример 1: Проблема ответственности при ошибках системы

В Нидерландах в 2021 году широко обсуждался скандал с налоговой службой, которая с помощью автоматизированных систем ИИ анализировала заявки на социальную помощь и выявляла "подозрительные" случаи. В результате крайне чувствительный алгоритм неправомерно классифицировал десятки тысяч семей как мошенников, что повлекло возврат денежных средств и разрушение семей. Постфактум оказалось, что ни один государственный чиновник не мог объяснить логику работы системы или взять на себя персональную ответственность за ошибочные решения [5].

##### Пример 2: Дискриминация по этническому признаку

В США системы ИИ применялись для прогнозирования рецидива преступлений, на основе чего принимались решения о мере пресечения. Позднее стало ясно, что алгоритмы имеют сильную "афроамериканскую" предвзятость, что привело к дискриминации по расовому признаку. Апелляции отклонялись на основании непрозрачности процесса — система ИИ считалась "необъяснимой".

##### Пример 3: Российская "песочница" в Москве

В ходе эксперимента с внедрением ИИ в сфере электронных госуслуг выявлено множество сопутствующих рисков: неурегулированность порядка обжалования "автоматических" отказов, вопросы о достаточности уведомления граждан о факте использования ИИ, отсутствие четкой процедуры уведомления о взломе системы и утечках данных.

##### Пример 4: Обработка и хранение персональных данных



В ряде регионов России предпринимались попытки внедрить интеллектуальные системы видеонаблюдения для распознавания лиц в общественных местах с целью обеспечения общественного порядка и предотвращения правонарушений. Однако в отсутствие четкого регулирования таких систем возникает опасность злоупотребления и нарушения Конституционного права на частную жизнь и тайну личной информации граждан [6].

#### 5. Проблема этики и легитимности решений, принимаемых с помощью ИИ

Помимо традиционных юридических норм, значимую роль играют вопросы этики. Решение, принимаемое ИИ-системой, должно соответствовать не только букве закона, но и общепринятым представлениям о справедливости, уважении к человеческому достоинству, равенству и прозрачности. Например, решение об отказе в выплате пособия должно быть максимально прозрачным и объяснимым, равно как и решение о наложении штрафа.

Однако возможны ситуации, в которых система вынесла "правильное" по формальным признакам решение, но оно крайне несправедливо в моральном измерении. Это требует внедрения этических стандартов на этапе разработки и обучения алгоритмов, а также привлечение независимых экспертов к аудиту и оценке социальной значимости решения.

#### 6. Пути минимизации правовых рисков

На основе анализа сложившейся практики и теоретических подходов возможны следующие меры по минимизации правовых рисков:

- Разработка и утверждение федерального закона “О государственном регулировании искусственного интеллекта”, где будут определены сферы допустимого применения, основания и пределы автоматизации, субъекты ответственности и процедуры обжалования решений, принимаемых ИИ.
- Обязательное требование “объяснимости” ИИ. Программная система должна обеспечивать возможность формирования понятного

пользователю объяснения принятого решения с указанием задействованных аргументов и критериев.

- Введение института “этических комиссий” при государственных органах, в функции которых входит аудит корректности, недискриминационности и прозрачности алгоритмов.
- Регистрация и обязательная сертификация разработчиков (поставщиков) программных решений ИИ для государственных нужд, а также введение системы аудита исходного кода на предмет "закладок", криминальных уязвимостей и несанкционированного доступа.
- Разработка и внедрение процедур информирования граждан о факте использования ИИ, порядке сбора, хранения и обработки данных, возможности отказа или обжалования решения системы.
- Установление четких регламентов хранения и обезличивания персональных данных, обработанных ИИ-системами государственного сектора, а также процедур контроля за соблюдением соответствующего законодательства [7].

#### Результаты исследования

Проведенный анализ выявил, что интеграция искусственного интеллекта в государственное управление сопряжена с целым рядом правовых рисков, способных не только привести к нарушению индивидуальных прав, но и подорвать доверие общества к самому государству. Главными проблемами стали безадресность ответственности, угроза персональным данным, дефицит прозрачности, потенциальная дискриминация отдельных групп населения и отсутствие единых стандартов этики при автоматизации процедур принятия решений.

Отмечается недостаточность существующей нормативной базы в Российской Федерации, отсутствие специализированного “закона об искусственном интеллекте”, разрозненность и ведомственный характер

регулирования. Ключевые принципы международных актов пока не внедрены в российское право в полном объеме. Наблюдается очевидная необходимость унификации нормативной базы и разработки актуальных стандартов этики, ответственности и безопасности.

Практика показывает, что эксперименты с внедрением ИИ без достаточной нормативной подготовки приводят к затяжным скандалам, массовым судебным разбирательствам и эрозии общественного доверия — однако без технологического развития уже невозможно эффективное управление на современном этапе [8].

### **Выводы**

Внедрение и использование искусственного интеллекта в государственном управлении — это сложный технологический и правовой вызов. Неравномерность и фрагментарность регулирования на фоне стремительного развития цифровых решений создают угрозу нарушения фундаментальных прав и свобод граждан.

Для обеспечения стабильности, прозрачности и легитимности деятельности государства, применяющего ИИ, требуется разработать целостную нормативно-правовую базу, в которой будут учтены вопросы объяснимости, ответственности, этики, защиты персональных данных и равенства сторон. Необходимо выработать понятные механизмы обжалования решений, принятых с использованием искусственного интеллекта, и внедрить инструменты аудита и общественного контроля.

### **Список литературы:**

1. Савельев, Денис А. 2018. «О создании и перспективах использования корпуса текстов российских правовых актов как набора открытых данных». Право. Журнал Высшей школы экономики 1: 26–44.
2. Соколова, Алла А. 2019. «Искусственный интеллект в юриспруденции: риски внедрения». Юридическая техника 13: 350–356.
3. Талапина, Эльвира В. 2021. «Об антикоррупционной экспертизе». Журнал российского права 5: 52–66.

4. Трунцевский, Юрий В. 2020. «Закон как данные в эпоху цифровизации». Язык правотворчества в условиях цифровизации общественных отношений, под общ. ред. Дмитрия А. Пашенцева, Максима В. Залоило, 66–73. М.: ИЗиСП, ИНФРА-М.
5. Dehaene, Stanislas. 2021. Apprendre! Les talents du cerveau, le défi des machines. Paris: éd. Odile Jacob.
6. Hänold, Stefanie. 2022. “Profiling and automated decision-making: Legal implications and shortcomings”. Robotics, AI and the future of law, eds Marcelo Corrales Compagnucci, Mark Fenwick, Nikolaus Forgó, 123–153. New York: Springer.
7. Susskind, Richard. 2020. The end of lawyers? Rethinking the nature of legal services. New York: Oxford University Press.
8. Villani, Cédric, Marc Schoenauer, Yann Bonnet, Charly Berthet, Anne-Charlotte Cornut, François Levin, Bertrand Rondepierre. 2018. “Donner un sens à l’intelligence artificielle: Pour une stratégie nationale et européenne”. Accessed February 3, 2021. [https://www.researchgate.net/publication/330179947\\_Donner\\_un\\_sens\\_a\\_l'intelligence\\_artificielle\\_Pour\\_une\\_strategie\\_nationale\\_et\\_europeenne](https://www.researchgate.net/publication/330179947_Donner_un_sens_a_l'intelligence_artificielle_Pour_une_strategie_nationale_et_europeenne).
9. Лозовицкая, Г. П. Искусственный интеллект: правовые проблемы использования / Г. П. Лозовицкая, Л. В. Маринкина // Стратегическое развитие системы МВД России: состояние, тенденции, перспективы : Сборник статей Международной научно-практической конференции, Москва, 23 октября 2020 года / Под общей редакцией И. Г. Чистобородова, А. Л. Ситковского, В. О. Лапина. – Москва: Академия управления Министерства внутренних дел Российской Федерации, 2020. – С. 517-521. – EDN JOAWVF.
10. Уголовно-исполнительные, правовые, криминологические и оперативно-розыскные проблемы преступности в сфере экономики, влияющие на уголовную ответственность за легализацию активов организованной преступности / Г. П. Лозовицкая, А. В. Логинов, В. А. Минеев, Ю. В. Соколинский // Закон и власть. – 2025. – № 3. – С. 176-185. – EDN YVVQDX.

11. Лозовицкая, Г. П. Прогнозирование уровня преступности в городах на основе демографических данных / Г. П. Лозовицкая, Ю. В. Соколинский, В. А. Шалько // Вестник Восточно-Сибирской Открытой Академии. – 2024. – № 53(53). – EDN GQEKPZ.

12. Григорьев, В.В., Лозовицкая, Г. П. Образование будущего, игры и метавселенные / В.В. Григорьев, Г. П. Лозовицкая // Вестник Восточно-Сибирской Открытой Академии. – 2024. – № 55(55).