

Ссылка для цитирования этой статьи:

Магомедов Д.Б., Гаджиев М.А. Искусственный интеллект в противодействии терроризму: правовые вызовы // Human Progress. 2025. Том 11, Вып. 12. С. 30. URL: http://progress-human.com/images/2025/Tom11_12/Magomedov.pdf DOI 10.46320/2073-4506-2025-12a-33.

УДК 323.28

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ПРОТИВОДЕЙСТВИИ ТЕРРОРИЗМУ: ПРАВОВЫЕ ВЫЗОВЫ

Магомедов Давди Бадавиевич

кандидат педагогических наук, доцент,
Юридический институт,
Дагестанский государственный университет,
г. Махачкала, Российская Федерация

Гаджиев Малик Амирович

магистрант,
Юридический институт,
Дагестанский государственный университет,
г. Махачкала, Российская Федерация;
независимый исследователь

Аннотация. В статье «искусственный интеллект в противодействии терроризму: правовые вызовы» рассматривается двойственная роль искусственного интеллекта в сфере противодействия терроризму, анализируются правовые и этические вызовы, возникающие при использовании искусственного интеллекта государственными органами, а также угрозы использования технологий террористическими группами, особое внимание уделяется вопросам соблюдения прав человека, проблемам трансграничной передачи данных и перспективам международно-правового регулирования.

В работе детально рассматриваются такие ключевые правовые вызовы как нарушение неприкосновенности частной жизни и защиты персональных данных при использовании систем массового наблюдения и трансграничной передаче данных, проблема алгоритмической предвзятости и дискриминации уязвимых групп населения, вопросы обеспечения прозрачности и объяснимости решений принимаемых системами искусственного интеллекта, сложность определения субъекта ответственности за вред причиненный автономными системами, а также отсутствие эффективных механизмов правовой защиты для лиц пострадавших от решений принятых алгоритмами. Особое внимание уделяется анализу юрисдикционных коллизий возникающих при трансграничном использовании систем

искусственного интеллекта в контртеррористических целях, включая сравнительный анализ подходов Соединенных Штатов Америки где приоритет отдается национальной безопасности и широкой оперативной автономии правоохранительных органов, и Европейского Союза с его правозащитным подходом и строгим регулированием на основе Общего регламента по защите данных и Акта об искусственном интеллекте.

Также поднимается проблема прозрачности алгоритмов: пользователи и пострадавшие от решений ИИ должны иметь возможность понимать логику работы систем и обжаловать их действия.

Ключевые слова: искусственный интеллект, терроризм, правовое регулирование, ответственность, прозрачность алгоритмов, защита данных.

Цель статьи — комплексно проанализировать правовые проблемы, возникающие при использовании технологий искусственного интеллекта (ИИ) в сфере противодействия терроризму, и предложить подходы к их решению для достижения баланса между повышением безопасности и защитой прав человека.

Искусственный интеллект (ИИ) становится ключевым инструментом в противодействии терроризму в Российской Федерации, обеспечивая автоматизированный анализ петабайтов данных из систем СОПМ, видеонаблюдения, соцсетей (ВКонтакте, Telegram) и даркнета для выявления паттернов поведения, связанных со ст. 205 УК РФ (террористический акт), ст. 205.2 (публичные призывы к терроризму).

Интеграция технологий искусственного интеллекта в операции по противодействию терроризму знаменует собой парадигмальный сдвиг в современном управлении безопасностью с одной стороны искусственный интеллект открывает беспрецедентные возможности для анализа больших данных прогнозирования угроз и автоматизации безопасности с другой стороны использование искусственного интеллекта создает серьезные риски для прав человека и верховенства закона что делает эту тему критически важной для научного и правового анализа.

Один из ключевых вызовов — определение ответственности за решения ИИ. Поскольку алгоритмы не могут быть субъектами права, возникает вопрос о том, кто несёт ответственность за ошибки или негативные последствия решений, принятых на основе ИИ: разработчик системы, оператор, государственный орган или организация, использующая ИИ. В международной практике считается, что конечная ответственность остаётся за субъектом, использующим ИИ.

Не менее важна проблема прозрачности и объяснимости алгоритмов. Для доверия к ИИ и возможности обжалования его решений необходимо обеспечить прозрачность работы алгоритмов — особенно в случаях, когда ИИ используется для принятия решений, затрагивающих права человека (например, при блокировке контента или задержании подозреваемых). Отсутствие объяснимости может привести к нарушению права на справедливый суд и других базовых прав.

Серьёзный вызов представляет защита персональных данных. ИИ-системы часто обрабатывают чувствительные данные (биометрию, метаданные, информацию из социальных сетей), что создаёт риски нарушения права на конфиденциальность. В России обработка персональных данных регулируется Федеральным законом № 152-ФЗ, который запрещает принимать решения, влекущие правовые последствия, исключительно на основе автоматизированной обработки без согласия субъекта данных.

Ещё одна проблема — предвзятость и дискриминация. Модели ИИ могут наследовать социальные стереотипы и предвзятость, присутствующую в обучающих данных. Это способно привести к несправедливому отношению к определённым группам людей — например, к ошибкам в идентификации подозреваемых или дискриминации при мониторинге поведения [3].

Применение искусственного интеллекта (ИИ) смогло бы стать рациональным решением, которое помогло бы исключить возможные ошибки следствия, а также быстро проанализировать большой объем информации. Эта технология отлично подходит для роли вспомогательного инструмента, способного сэкономить время и уменьшить прилагаемые людьми усилия, взяв на себя часть нагрузки. При помощи искусственного интеллекта можно быстро обработать большой объем данных, систематизировать результаты, избавившись от рутинной работы, которая требует много времени.

Внутренние инструкции и ведомственные нормативно-правовые акты об оперативной документалистике требуют отражать наименование каждого оперативно-розыскного мероприятия, в результате которого были получены данные в документах. Кроме этого, должна быть отражена цель ОРМ и его правовая основа. Нужно фиксировать, каким образом и при каких обстоятельствах было получено то или иное доказательство, информация по делу, кто из сотрудников проводил ОРМ, участвовали ли в нем другие лица, если да, то кто именно, где именно и при каких обстоятельствах осуществлялось мероприятие. Это необходимо для того, чтобы была возможность проверить предоставленные данные. Поэтому важно, чтобы использованные технические средства, расходные материалы также были документально

зафиксированы. Значимые для следствия детали, информация, документы, материалы должны быть зафиксированы и описаны подробно [1].

Двойственная природа искусственного интеллекта в контексте терроризма проявляется двояко как инструмент борьбы и как потенциальное оружие искусственный интеллект как угроза использование террористами террористические организации все активнее используют искусственный интеллект для деструктивных целей что требует срочных законодательных и политических мер на международном уровне виртуальные платформы становятся ареной для террористической деятельности где искусственный интеллект помогает в выявлении подозрительных паттернов но также создает уязвимости искусственный интеллект как инструмент противодействия правительства все чаще внедряют искусственный интеллект в таких областях как наблюдение прогнозирование правоприменения биометрическая идентификация поведенческое профилирование и автоматизированное обнаружение угроз [4].

Основные правовые вызовы при использовании искусственного интеллекта включают вопросы прав человека и недискриминации использование искусственного интеллекта в контртеррористических целях затрагивает широкий спектр прав человека включая право на частную жизнь защиту данных свободу выражения мнений справедливое судебное разбирательство и право на эффективные средства правовой защиты главную озабоченность вызывает потенциальное непропорциональное воздействие на уязвимые группы и маргинализированные сообщества из за алгоритмической предвзятости также важны вопросы прозрачности и подотчетности системы искусственного интеллекта часто страдают от непрозрачности принятия решений и дефицита как прозрачности так и подотчетности существующие механизмы надзора не всегда эффективны в обеспечении человеческого контроля над использованием искусственного интеллекта в операциях по противодействию терроризму особую сложность представляет экстерриториальность и передача данных передача данных полученных в результате контртеррористической деятельности с использованием искусственного интеллекта через юрисдикции создает серьезные правовые коллизии контрастирующие правовые культуры США приоритет национальной безопасности и ес правозащитный подход создают нормативные разрывы которые осложняют совместные операции и взаимную правовую помощь.

В международной практике преобладает позиция, согласно которой юридическая ответственность за действия, совершенные с использованием искусственного интеллекта, сохраняется за субъектом, применяющим такие технологии. Группа разработки финансовых мер борьбы с отмыванием денег (ФАТФ) неоднократно подчеркивала, что, несмотря на активное внедрение инновационных решений, «конечная ответственность» за соблюдение

всех требований в сфере противодействия легализации доходов и финансированию терроризма должна возлагаться непосредственно на кредитные организации и субъекты финансового мониторинга. Аналогичная позиция находит отражение в аналитических докладах, посвященных использованию алгоритмов искусственного интеллекта в банковском надзоре, где в качестве обязательного условия рекомендуется сохранение принципа «human-in-the-loop», предполагающего наличие человека-контролера, который проверяет результаты автоматической обработки и принимает итоговое решение по каждой сомнительной операции.

Следовательно, внедряя технологии интеллектуальной обработки информации, финансовые институты обязаны нести полный груз ответственности за последствия функционирования таких систем, обеспечивая при этом действенный экспертный надзор и реальную возможность оперативного вмешательства со стороны уполномоченных сотрудников. Игнорирование указанных требований способно повлечь за собой квалификацию со стороны регулятора допущенных нарушений, поскольку даже при активном использовании автоматизированных алгоритмов банки продолжают нести обязанность по исполнению законодательных предписаний о проведении надлежащей проверки клиентов и тщательном документировании всех совершаемых действий.

В контексте реализации мероприятий по противодействию легализации преступных доходов указанные обстоятельства означают необходимость тщательного соблюдения баланса интересов при интеграции технологий искусственного интеллекта. С одной стороны, автоматизация контрольных процедур неизбежно вступает в определенное противоречие с императивными требованиями о недопустимости принятия решений, затрагивающих права граждан, исключительно на базе автоматизированной обработки данных. С другой стороны, кредитные организации сохраняют за собой право на внедрение современных технологических решений при условии надлежащего информирования клиентов и предоставления им действенных механизмов оспаривания полученных результатов.

Сложившаяся правоприменительная практика отчетливо демонстрирует необходимость обеспечения свойства «объяснимости» применяемых алгоритмов, поскольку в противном случае клиент получает возможность успешного оспаривания в судебном порядке правомерности отказа в совершении операции либо блокирования банковского счета. Центральный банк Российской Федерации в своих рекомендательных документах последовательно акцентирует внимание участников финансового рынка на существовании рисков, связанных с возможностью «принятия предвзятых или дискриминационных решений» со стороны систем искусственного интеллекта. Международные стандарты, в свою очередь, выделяют две ключевые формы обеспечения справедливости при использовании алгоритмов:

результативную, направленную на недопущение дискриминации, и процедурную, предполагающую прозрачность и понятность реализуемых процессов для всех вовлеченных сторон.

Помимо изложенного, международные акты в сфере защиты информации, включая Общий регламент по защите данных, действующий на территории Европейского Союза, а также разрабатываемые документы Организации экономического сотрудничества и развития, закрепляют принципы минимизации обрабатываемых сведений и обеспечения надлежащего уровня безопасности при их хранении. Применяемые в целях противодействия отмыванию доходов системы искусственного интеллекта должны ограничиваться обработкой исключительно необходимого объема данных, осуществлять такую обработку исключительно в пределах полученного согласия либо в рамках реализации законных интересов кредитной организации, а также гарантировать надежную защиту от несанкционированного доступа и киберугроз. Существенное значение приобретает и проблематика трансграничной передачи информации, поскольку при использовании международных сервисов, включая облачные платформы искусственного интеллекта, могут возникать дополнительные нормативные ограничения и коллизии юрисдикций. Таким образом, необходимость обеспечения защиты персональных данных и соблюдения законных прав клиентов формирует жесткие нормативные рамки для построения современных аналитических систем, обуславливая потребность во внедрении надежных протоколов защиты и проведении регулярного независимого аудита используемых алгоритмов.

Мировой опыт внедрения ИИ в финансах демонстрирует широкий разрыв между технологическими возможностями и правовым регулированием. ФАТФ и Всемирный банк активно продвигают технологические стандарты: они считают, что ИИ и машинное обучение способны «значительно облегчить сбор, обработку и анализ данных, а также помочь субъектам выявлять риски» ПОД/ФТ более эффективно. При этом ФАТФ предупреждает о «потенциально существенных рисках» в отношении прозрачности и ответственности. В Европе ЕБА отмечает, что большинство банков ЕС уже применяют ИИ, в том числе для «fraud и AML/CFT» — анализа больших массивов данных для выявления подозрительных схем. Европейский регуляторский пакет «Акт об ИИ» (очередной этап которого ожидается в 2025–2026 гг.) вводит требования к управлению рисками ИИ-систем высокого класса (например, системы, влияющие на права человека) — что затронет и банковские приложения [5].

Российский опыт пока менее формализован, но тенденции схожи. Уже сегодня ФНС и финансовые органы используют алгоритмы анализа данных для операций «сцепления» сумм и незаконных схем. Кредитные организации в России показывают активный интерес к ИИ:

например, Сбербанк и другие цифровые лидеры сообщают об использовании нейросетевых скоринговых моделей и чат-ботов-помощников. При этом правовая основа остается прежней: банки обязаны выполнять требования 115-ФЗ и внутренних регламентов Банка России. В 2022–2023 годах Центральный банк и Росфинмониторинг создали несколько пилотных RegTech-площадок и «песочниц», где тестируются методы машинного обучения в контроле финансовых потоков.

На федеральном уровне технологии ИИ применяются для аналитической поддержки законотворческого процесса. Например, в Государственной Думе РФ используются системы автоматизированного анализа законопроектов и машинной обработки массива обращений граждан, что позволяет выявлять типичные вопросы и актуальные общественные запросы. В Правительстве РФ технологии используются для прогнозирования социально-экономических показателей и моделирования последствий управленческих решений [2].

Подробный анализ правовых вызовов, возникающих при использовании искусственного интеллекта (ИИ) в сфере противодействия терроризму, позволяет выделить несколько ключевых блоков проблем. Эти вызовы носят комплексный характер и затрагивают как фундаментальные права человека, так и вопросы международного и национального нормотворчества.

1. Вызовы в сфере прав человека и фундаментальных свобод

Это, пожалуй, самый обширный и обсуждаемый блок проблем. Применение ИИ может непреднамеренно нарушать базовые права, гарантированные международным правом.

•**Неприкосновенность частной жизни и защита данных:** Использование ИИ для массового наблюдения, биометрической идентификации и анализа больших данных создает беспрецедентные риски слежки. Способность ИИ обрабатывать колоссальные объемы информации усиливает угрозу неправомерного вмешательства в частную жизнь. Особую озабоченность вызывает трансграничная передача данных, полученных в ходе контртеррористической деятельности, что создает серьезные правовые коллизии между юрисдикциями с разными стандартами защиты данных.

•**Дискриминация и алгоритмическая предвзятость:** Системы ИИ могут проявлять предвзятость, если они обучаются на нерепрезентативных или исторически искаженных данных. Это приводит к непропорциональному воздействию на уязвимые группы и маргинализированные сообщества. Например, алгоритмы профилирования рисков могут необоснованно относить людей определенного этнического происхождения или религии к категории потенциальных террористов, что нарушает право на равенство и недискриминацию.

•Справедливое судебное разбирательство и presumption of innocence: Использование непрозрачных алгоритмов для оценки "опасности" человека может подорвать право на справедливый суд. Если решение, например, о включении в "черные списки" или применении мер превентивного задержания, принимается на основе работы "черного ящика", у человека нет возможности эффективно оспорить это решение, так как он не может понять лежащую в его основе логику.

•Свобода выражения мнений и доступа к информации: Автоматизированные системы фильтрации контента, призванные блокировать террористическую пропаганду, могут по ошибке удалять или блокировать легитимный контент, ограничивая свободу слова и доступ к информации.

2. Пробелы в законодательстве и нормативном регулировании

Скорость развития технологий ИИ значительно опережает процесс законотворчества, что создает существенные правовые вакуумы.

•Разрыв между технологиями и правом: Наблюдается существенный разрыв между темпами развития новых технологий и скоростью формирования соответствующей нормативной правовой базы, как на национальном, так и на международном уровне. Государства часто не знают, как реагировать на инновации, предпочитая оставлять правовые пробелы, что ведет к неопределенности.

•Отсутствие международно-согласованных стандартов: Несогласованность подходов разных стран к оценке угроз и регулированию ИИ создает серьезные препятствия. Это осложняет совместные операции и взаимную правовую помощь. Существует риск "юридической гонки", когда отдельные страны пытаются вывести свое национальное регулирование на трансграничный уровень в качестве "золотого стандарта".

•Пробелы в отраслевом регулировании: Действующее законодательство часто не учитывает специфику использования ИИ. Это касается как отсутствия специальных норм для борьбы с новыми видами угроз (например, автономные атаки дронов или ИИ-вербовка), так и недостаточного регулирования ответственности разработчиков и операторов таких систем .

3. Экстерриториальность и трансграничное сотрудничество

Природа как терроризма, так и интернета является трансграничной, что порождает уникальные правовые сложности.

•Юрисдикционные коллизии: Передача данных через границы для анализа с помощью ИИ ставит вопрос о том, право какой страны должно применяться. Контрастирующие правовые культуры, например, подход США с приоритетом национальной безопасности и подход Европейского Союза с его правозащитным фокусом (GDPR), создают

нормативные разрывы. Государства могут пытаться применять свои законы за пределами своей территории (экстерриториально), что ведет к конфликтам.

•**Сложность международного согласования:** Необходимость поиска решений на глобальном уровне наталкивается на разные уровни развития стран, несовпадение их интересов и подходов к оценке угроз национальной безопасности, что затрудняет выработку единых позиций.

4. Прозрачность, подотчетность и проблема "черного ящика"

Сам характер технологий ИИ создает проблемы для классических правовых механизмов контроля.

•**Непрозрачность принятия решений (проблема "черного ящика"):** Многие системы ИИ, особенно основанные на глубоком обучении, работают по принципу "черного ящика", когда даже их создатели не всегда могут объяснить, почему было принято то или иное решение. Это делает невозможным выполнение требования об "объяснимости" и "предсказуемости" решений, затрагивающих права человека.

•**Дефицит подотчетности:** Сложно определить, кто несет ответственность за вред, причиненный системой ИИ — разработчик, оператор, государственное ведомство, ее использующее, или сама система? Существующие механизмы надзора не всегда эффективны в обеспечении человеческого контроля над использованием ИИ в операциях по противодействию терроризму.

•**Отсутствие эффективных средств правовой защиты:** Если права человека были нарушены в результате работы ИИ, у пострадавшего часто нет эффективного механизма для обжалования и получения компенсации, так как сложно доказать причинно-следственную связь и идентифицировать ответственного.

В конечном счёте, правовое регулирование искусственного интеллекта в сфере противодействия терроризму находится на начальном этапе формирования ключевой вызов заключается в поиске баланса между эффективностью обеспечения безопасности и незыблемостью фундаментальных прав человека дальнейшее развитие должно идти по пути гармонизации законодательства на международном уровне с обязательным учетом правозащитных стандартов и обеспечением прозрачности алгоритмических систем.

Существующие правовые механизмы зачастую отстают от темпов технологического развития: национальные законодательства и международные нормы не всегда содержат чёткие положения, регулирующие применение ИИ в сфере безопасности. При этом вопросы носят трансграничный характер, что делает критически важным развитие международного сотрудничества — как в части выработки общих стандартов (например, инициативы ООН и

проект глобального договора по ИИ 2025 года), так и в части обмена опытом и инцидентами. Отдельные шаги уже предпринимаются: Европейский союз внедрил AI Act с риск-ориентированным подходом, а Межпарламентская ассамблея СНГ разрабатывает модельные законы для противодействия использованию новых технологий в террористических целях.

Для минимизации рисков и обеспечения баланса между безопасностью и защитой прав человека необходим комплексный подход. Он должен включать: разработку чётких правовых норм с принципами прозрачности, подотчётности и недискриминации; обязательный аудит и валидацию ИИ-систем перед внедрением; сохранение решающей роли человека в принятии значимых решений; создание надзорных органов с полномочиями проверки и применения санкций; повышение медиаграмотности населения для противодействия пропаганде; а также укрепление международного диалога по этическим и правовым стандартам.

В итоге эффективное применение ИИ в борьбе с терроризмом возможно лишь при гармоничном сочетании технологических инноваций, продуманного правового регулирования и соблюдения этических принципов. Только такой подход позволит максимально использовать потенциал ИИ для защиты общества, одновременно минимизируя риски злоупотреблений и нарушений фундаментальных прав и свобод.

Список литературы

1. Аникин Д. Потенциальные угрозы, исходящие от ИИ-сервисов // Обзор.НЦПТИ. 2025. № 3. 42 с.
2. Баранов В.В. Правовое регулирование использования беспилотных воздушных судов с искусственным интеллектом в контексте предотвращения террористических угроз // Вестник Университета имени О.Е. Кутафина. 2025. № 4. 128 с.
3. Гедгафов М.М. Роль искусственного интеллекта в противодействии терроризму // Журнал прикладных исследований. 2023. № 8. 34 с.
4. Джураев М.З. Интеграция искусственного интеллекта в публичную сферу // Сфера науки. 2026. № 1. 12 с.
5. Клещина Е.Н., Байханов А.И. Киберпреступность в современных условиях цифровизации общества: детерминанты и направления противодействия // Закон и право. 2026. № 1. 34 с.

CONTRACT KILLING: FROM MOTIVE TO PUNISHMENT

Magomedov Davdi Badavievich

Candidate of Pedagogical Sciences, Associate Professor,
Law Institute,

Dagestan State University,
Makhachkala, Russian Federation

Gadzhiev Malik Amirovich

Master's Student,

Law Institute,

Dagestan State University,
Makhachkala, Russian Federation;

Independent Researcher

Annotation. The article "Artificial Intelligence in Countering Terrorism: Legal Challenges" examines the dual role of artificial intelligence in countering terrorism, analyzes the legal and ethical challenges that arise when artificial intelligence is used by government agencies, as well as the threats posed by the use of technology by terrorist groups. The article focuses on human rights issues, cross-border data transfer challenges, and the prospects for international legal regulation.

The paper examines in detail such key legal challenges as the violation of privacy and the protection of personal data when using mass surveillance systems and cross-border data transfer, the problem of algorithmic bias and discrimination against vulnerable groups, the issues of ensuring transparency and explainability of decisions made by artificial intelligence systems, and the complexity of determining the entity responsible for the harm caused by artificial intelligence.

Keywords: artificial intelligence, terrorism, legal regulation, responsibility, algorithm transparency, and data protection.

References

1. Anikin D. Potential Threats from AI Services // Review.NCPTI. 2025. No. 3. 42 p.
2. Baranov V.V. Legal Regulation of the Use of Unmanned Aerial Vehicles with Artificial Intelligence in the Context of Preventing Terrorist Threats // Bulletin of the Kutafin University. 2025. No. 4. 128 c.
3. Gedgafov M. M. The Role of Artificial Intelligence in Countering Terrorism // Journal of Applied Research. 2023. No. 8. 34 p.
4. Dzhuraev M.Z. Integration of Artificial Intelligence into the Public Sphere // Sfera Nauki. 2026. No. 1. 12 p.
5. Kleshchina E.N., Baykhanov A.I. Cybercrime in the Modern Conditions of Digitalization of Society: Determinants and Directions of Counteraction // Law and Law. 2026. No. 1. 34 p.