Научная статья
УДК 343
EDN: https://elibrary.ru/jgzagq
NIION: 2015-0066-1/26-377
MOSURED: 77/27-011-2026-01-576

Факторы риска в использовании искусственного интеллекта для профилактики преступности

Мевлуд Демуралович Давитадзе[1], Алексей Александрович Середин[2]
[1] Московский государственный юридический университет имени О.Е. Кутафина (МГЮА), Москва, Россия, md2063@mail.ru
[1] Московский университет имени С.Ю. Витте, Москва, Россия
[2] Открытый гуманитарно-экономический университет, Москва, Россия, aseredin@govvrn.ru

Аннотация. Статья посвящена рассмотрению факторов риска в использовании искусственного интеллекта для предупреждения преступности. Принят во внимание отечественный и зарубежный опыт применения ИИ в этой сфере, проанализированы нормативно закрепленные подходы и авторские предложения по минимизации рисков.

Ключевые слова: искусственный интеллект, профилактика преступности, права человека, алгоритм
Для цитирования: Давитадзе М. Д., Середин А. А. Факторы риска в использовании искусственного интеллекта для профилактики преступности // Вестник экономической безопасности. 2026. № 1. С. 36–41. EDN: JGZAGQ.

Original article

Risk factors in the use of artificial intelligence for crime prevention

Mevlud D. Davidadze[1], Alexey A. Seredin[2]
[1] Kutafin Moscow State Law University (MSAL), Moscow, Russia, md2063@mail.ru
[1] Moscow University named after S.Yu. Witte, Moscow, Russia
[2] Open University of Humanities and Economics, Moscow, Russia, aseredin@govvrn.ru

Abstract. The article is devoted to the consideration of risk factors in the use of artificial intelligence for crime prevention. Domestic and foreign experience of the application of AI in this area is taken into account, the normatively fixed approaches and the author's proposals for risk minimization are analyzed.

Keywords: artificial intelligence, crime prevention, human rights, algorithm
For citation: Davidadze M. D., Seredin A. A. Risk factors in the use of artificial intelligence for crime prevention. Bulletin of economic security. 2026;(1):36–41. (In Russ.). EDN: JGZAGQ.

На протяжении многих веков мысль о создании искусственного интеллекта (далее – ИИ) поражала воображение фантастов, а позднее – ученых и инженеров. На страницах художественной литературы ИИ демонстрируется в двух основных ролях: злодея, где он рассматривается в качестве потенциальной угрозы человечеству (А. Азимов, Ф. Герберт, Ф. Дик, А. Кларк и др.), и положительного героя (К. Исигуро, М. Уэллс и др.). Сегодня использование ИИ стало реальностью в правоохранительной сфере. Предпринимаются попытки его применения и в области профилактики преступности.

Десятки и сотни лет в деле профилактики ключевыми были традиционные методы общей и индивидуальной профилактики. В их числе: социально-экономические, организационные, правовые, технические, а также убеждение, оказание помощи, принуждение и др. Однако галопирующие темпы развития науки и технического прогресса существенно изменили подходы в данном вопросе. За последние 10 лет были апробированы и вошли в повседневность ряд «прорывных» технологий: высокопроизводительные, мультимодальные модели ИИ нового поколения, такие, например, как GPT-4 от OpenAI, Gemini Ultra от Google и GigaChat от Сбера. Они демонстрируют широкие способности в генерации и обработке видео, текста, изображений и звука, анализе сложных ситуаций и создании соответствующих выводов. Интеллектуальные системы PaLM-E и RT-2 позво-

лили создать роботизированные комплексы, способные вести логическую цепочку рассуждений, реагировать на изменения обстановки, использовать опыт, полученный при выполнении предыдущих задач, автономно управлять роботом. Вот только малая часть достижений, которые очевидно будут развиваться и вставать на службу противодействия преступности правоохранительной системой. Ключевая цель при этом – повысить производительность при снижении затрат путем внедрения новых решений в области предупреждения преступности, повышения уровня осведомленности в принятии решений, высвобождения людских ресурсов, экономии финансовых и материальных резервов.

Использование программных комплексов в этой сфере дает возможность снизить затраты, обрабатывать сложные массивы разнородных данных, что далеко выходит за пределы возможностей человека.

Сегодня в мире существует ряд программных комплексов, выполняющих правоохранительные функции: интеллектуальная система FACES, призванная осуществлять идентификацию транспортных средств и лиц посредством изображений с камер видеонаблюдения; Predpol – способна на основе данных о совершенных преступлениях и с использованием методов машинного обучения давать прогнозы относительно места и времени совершения преступлений в будущем; ShotSpotter – система обнаружения местонахождения стрелявшего на основе моделирования обстановки исходя из данных городской застройки, физических законов баллистики и др. [1, с. 24]. В нашей стране направление использования ИИ в целях профилактики преступности также развивается. Например, распространение получил комплекс «Криминалист» (выявляет потенциальных преступников и предлагает оптимальное решение, в том числе в области профилактики). МВД России планирует внедрение систем «Клон» (позволит определять факт подделки видеоизображения) и «Конъюнктура» (призвана прогнозировать негативные события и явления и разрабатывать сценарии реакции на них), работающих на основе ИИ [2], в целях предупреждения специального рецидива и общей превенции применяются технологии в области раскрытия преступлений, например, при помощи технологии распознавания лиц.

В основе ИИ лежат исходные данные. В нашем случае – сведения о преступлениях и их совокупности, в том числе о месте и времени деяний, личности виновных и потерпевших. Дополнительной информацией, которая позволяет сделать достоверной прогноз, могут являться данные о типичном поведении для граждан в «группе риска», экономические и демографические показатели. Такой широкий охват исходной информации позволяет делать более глубокие и достоверные прогнозы по критериям, заложенным в основу «машинного мышления».

В попытке противодействия преступности государство нередко проигрывает. Суть предупреждения – в опережающем воздействии. Решающую роль играет фактор времени и ресурсов: первыми часто действуют преступники, разрабатывая новые криминальные схемы и реализуя их на практике, имея возможность за счет мощного финансового резерва привлекать к работе наиболее квалифицированные в своем роде силы и лучшие средства. Правоохранительные органы вынуждены реагировать, т. е. действовать часто в условиях, когда угроза не только назрела, но и стала весомой, уже реализована и переросла в устойчивую тенденцию в форме преступлений конкретного вида. После этого происходит выделение совокупности преступлений в виде самостоятельного криминального фактора, требующего противодействия и разрабатываются соответствующие меры. Применение ИИ – попытка сместить акценты, сделав позицию правоохранительных органов опережающей, в большей мере проактивной и направленной на сдерживание преступности.

Поскольку профилактика немыслима без достоверного прогноза, инновационный подход использования ИИ состоит в эффективном анализе глобального массива данных, на основе которых делается вывод об особенностях и направлениях профилактики. Программные алгоритмы в состоянии не только выявлять неочевидные закономерности, но и делать выводы о месте, времени совершения преступлений, возможных виновных, вредных последствиях.

С одной стороны, использование ИИ делает работу более продуктивной при меньших затратах; с другой – имеет недостатки и вызывает к жизни новые риски, связанные с качеством прогноза. Сильной стороной ИИ является учет множества факторов, связь которых в единое целое неочевидна, что должно делать качество прогноза высоким. Тем не менее, последнее вызывает вопросы. Факторы риска в использовании ИИ для предупреждения преступности, способные приводить к ошибкам, следующие:

1. *Переоценка роли ИИ и стремление полностью заместить традиционные методы профилактики.* В правовой литературе высказывается обоснованное мнение о том, что ИИ не есть самостоятельный субъект познания. Играя вспомогательную роль, он выполняет лишь функцию познания. Не смотря на способность ИИ к обучению, в качестве субъекта его деятельности выступает оператор-человек, воля которого и является побудительным мотивом [3, с. 31–38; 1, с. 24]. Тем не менее, существует риск избыточной зависимости от технологий, при которой сотрудники чрезмерно полагаются на достоверность результатов работы машинных алгоритмов, отказываясь от собственных усилий и отвергая впоследствии традиционные формы и методы профилактической деятельности.

При этом методики традиционной профилактики перестают совершенствоваться, отражать существующее положение дел, будут устаревать, а опыт будет забыт. Если приоритет в принятии решений отдается выводам ИИ, субъект перестает действовать самостоятельно. При этом не стоит исключать вероятность тех-

нического сбоя, при котором система перестает работать полностью или частично на неопределенное время. В такой ситуации в условиях утраты компетенций в области применения традиционных методов профилактики в среднесрочной перспективе эта работа может быть полностью парализована.

2. *Возможная недостоверность и необоснованность исходной информации.* Выводы, сделанные компьютерным алгоритмом, основаны на исходных данных и зависят от их точности и адекватности обстановке. Если в основе полученных выводов лежит не реальная криминальная ситуация, а информация, обусловленная объективно немотивированными факторами (например, конъюнктурные соображения, ситуативно обусловленные действия, которые, будучи заложены в качестве исходных данных, интерпретируются системой), решения, принятые на их основе будут неадекватными или даже вредными. Так, длительный и повышенный интерес правоохранительных органов в конкретной местности способен предопределять последующие меры профилактики в данном районе. Таким образом, вектор профилактической деятельности может быть необоснованно искажен по причине действия субъективных факторов личного или служебного предпочтения. И наоборот, переоценка качества правоохранительной деятельности в других районах может повлечь дефицит внимания там.

Алгоритмы прогнозирования опираются на факты, характеризующие ретроспективные данные о преступности и методах борьбы с ней и формируют на их основе выводы, используемые в дальнейшем в рамках профилактической работы. Поэтому еще один фактор риска здесь – вероятность изменения актуальной обстановки, подлежащей учету для принятия обоснованного решения, не эволюционным путем, что, как правило, учитывается программой, а радикально, в кратчайший срок. В этом случае ИИ будет действовать в условиях нехватки информации. В результате повышается риск перерасхода ресурсов и необоснованного ограничения прав и свобод граждан, непричастных к преступлению.

3. Обратной стороной использования недостоверной информации в ходе профилактических действий являются *риски нарушения прав человека.* Поскольку в основе алгоритмов ИИ, работающих в целях профилактики преступности, заложена конкретная информация (о фактах преступлений и смежных с ними правонарушений, количестве задержаний на конкретной территории (в организации), фактах потребления запрещенных средств и т. п.), то и в фокусе последующих прогнозов будет она же, интерпретированная в соответствии с логикой действия модели ИИ. Например, в определенном районе массово наблюдались случаи хищений. Если к настоящему моменту реальность изменилась, появилась устойчивая тенденция количественного сокращения данных преступлений и (или) существенного качественного снижения их тяжести, такая динамика должна найти отражение в определении форм и методов профилактической работы. Необходимость радикального сокращения преступности в конкретном районе и применение сравнительно жестких методов часто основаны на стремлении погасить возникшее социальное напряжение. При этом такое же самое напряжение может возникать в связи с налагаемыми ограничениями в ситуации, которая того не требует: права граждан существенно ограничиваются, при этом, качественный эффект в борьбе с преступностью не достигается (например, сегодня на Крымском мосту для его сохранения и безопасности граждан принимаются беспрецедентные меры, связанные с остановкой, осмотром транспорта, досмотровыми мероприятиями (при необходимости). Эти меры перестанут быть уместными, станут несоразмерными потенциальной угрозе в условиях существенного снижения опасности). Неверные выводы ИИ при этом могут быть обусловлены инертностью, вызванной тем, что предложения по профилактике преступности будут основаны на всей совокупности заложенной информации. Поэтому так важна способность ИИ к выбору для анализа актуальных данных.

4. *Традиционно-негативные факторы* – влияют вне зависимости от применяемого механизма анализа информации для подготовки мер профилактики. Поскольку в расчет оценки преступности берется, в первую очередь, информация о зарегистрированных деяниях, очень важно в программные алгоритмы закладывать поправку на искажение данных при регистрации преступлений. Традиционно выраженным фактором здесь является объективная и субъективная латентность. Неполная информация о преступности, которая используется в работе ИИ, не только приводит к ошибочным выводам, но и усугубляет проблему, поскольку программные алгоритмы являются самообучающимися. В этом смысле неправдивые данные, заложенные в систему оценки, приводят к последующим искаженным выводам, усиливая разрыв с реальностью с каждым последующим завершенным «циклом». Неверная количественная и качественная оценка преступности способна приводить к дисбалансу в правоохранительной деятельности (в силу диспропорции в применении сил и средств, в конкретных районах по разным причинам преступлений выявляется все больше, больше затрачивается ресурсов, в то время как проблемы преступности в иных районах будут нарастать).

5. *Непрозрачность программных алгоритмов.* Закрытый характер ключевых параметров ИИ, лежащих в основе выводов системы в области профилактики, вызывает обоснованное недоверие к результатам и опасение со стороны общества. Этот факт признается официально [4, п. 8]. Опасение может вызывать возможная предвзятость применения ограничительных мер. В англоязычной литературе данная проблема известна как «проблема черного ящика» [5]. Например, в качестве объекта влияния в связи с возможным совершением коррупционных преступлений ИИ избирается общность граждан, выделенная по признакам занимаемой долж-

ности, прохождения службы на конкретной территории, возраста и т. п. Возникает ситуация, при которой профилактические меры, связанные с ограничением прав и законных интересов, вопреки объективной необходимости и разумности будут действовать лишь в отношении определенных лиц, не затрагивая и давая свободу действий второй половине граждан в «зоне риска». Оспаривание такого положения дел затруднено в связи с тем, что меры профилактики и объект воздействия избраны «непредвзятым» ИИ, проверить обоснованность работы которого крайне тяжело, поскольку конструирование и работа машинных алгоритмов имеет закрытый характер. По этой причине в некоторых государствах (регионах) алгоритмы ИИ, которые планируются к внедрению в правоохранительную деятельность, подлежат размещению в публичном доступе (например, по законодательству штата Айдахо, США) [6, с. 94]. В России правовое регулирование иное: программы на основе ИИ подлежат охране в силу норм об авторском праве на программы для ЭВМ (ст. 1261 ГК РФ) и о коммерческой тайне, поскольку механизм работы ИИ имеет действительную или потенциальную экономическую ценность и не составляет сведения, которые не могут быть отнесены к коммерческой тайне (ст. 5 ФЗ от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне») [7]. В то же время на страницах специальной литературы подчеркивается наличие проблемы предоставления авторско-правовой защиты алгоритму ИИ, которая связана с нестабильностью его содержания, перманентным изменением, «дописыванием» в ходе самообучения и автономной работы [8, с. 348]. В практическом плане требование о выведении алгоритмов, затрагивающих интересы граждан, за рамки законодательства об их охране реализовано с октября 2023 г. в отношении рекомендательных алгоритмов социальных сетей [9].

Применение в работе алгоритмов ИИ вероятностных оценок для принятия решений и невозможность полного объяснения сделанных выводов названа Концепцией развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 г. проблемой алгоритмической прозрачности систем ИИ и отнесена к проблемам, не имеющим однозначного решения [10]. Несмотря на то, что одним из принципов развития и использования ИИ является прозрачность (п. 19 Национальной стратегии развития искусственного интеллекта на период до 2030 года), проблема открытости и подотчетности систем прогнозирования правоохранительных органов актуальна по-прежнему.

6. *Трудности правового регулирования конструирования и использования алгоритмов ИИ.* Выбор модели регулирования строится на необходимости сочетания двух противоположных требований: по соблюдению прав человека и обеспечению ускоренного развития инноваций [11, с. 211].

В вопросе правового регулирования профилактики преступности с использованием ИИ можно идти двояким путем: от практики к ее нормативному регулированию и от концептуальной модели к необходимости соблюдения последней на практике. Ни один из этих подходов сегодня не является доминирующим, оба обоснованно используются во взаимном дополнении.

Существует проблема несоответствия между практикой применения ИИ и регулированием данной сферы, что часто объясняется пробелами законодательства и влечет за собой риск необоснованного ограничения прав граждан. В известной мере это следствие чрезвычайно быстрого развития технологий и внедрения их в правоохранительную практику. В России приняты основы регулирования отношений в сфере технологий ИИ. Значительную часть вопросов еще предстоит формализовать. Отсутствие правовых норм, оптимально регулирующих применение технологий ИИ, в тексте Концепции объясняется наличием проблем, не имеющих однозначного решения. В их числе: необходимость соблюдения баланса между защитой персональных данных и потребностью их использования в целях обучения алгоритмов ИИ; пределы «делегирования» решений системам ИИ; ответственность за причинение вреда с применением ИИ и др. С принятием ФЗ от 31 июля 2020 г. № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых и технологических инноваций в Российской Федерации» [12] законодатель постарался заложить основу решения некоторых из них, в частности, вопроса о причинении вреда при исполнении решений, разработанных с применением технологий ИИ (ст. 18.1).

Поскольку законотворчество в этой сфере происходит в условиях отсутствия соответствующего опыта, дальнейший процесс предполагает изучение практики правоприменения с последующими выводами и внесением изменений в нормативный инструментарий.

7. *Избыточный охват сбора данных.* Поскольку прогнозирование в профилактической деятельности базируется на сборе данных, ключевое значение имеет обоснованность круга лиц, интересы которых будут затронуты, а также содержание информации, подлежащей сбору. Вследствие непрозрачности работы алгоритмов ИИ опасения строятся на том, что «сети» могут забрасываться слишком широко, не только в отношении подозреваемых. Не ясны источники данных, которые могут быть как открытыми, так и с ограниченным доступом, включая активность интернете (в том числе в социальных сетях), отслеживание местоположения, интересов, предпочтений гражданина и т. п. Такой подход порождает опасения в возможности накопления гигантского объема личной информации без согласия собственника, что входит в противоречие с соображениями защиты личной и семейной тайн. По мнению критиков, такая практика влечет недоверие со стороны граждан, ставя их в один ряд с подозреваемыми [13]. В связи с галопирующими темпами развития технологий, возможности сбора информации в будущем будут расширяться, и проблема усугубляться.

В качестве выводов отметим, что использование ИИ в интересах профилактики преступности необходимо, несмотря на возможные отрицательные последствия. Отказ от его использования существенно уменьшит возможности правоохранительных органов. В целях минимизации выявленных рисков предлагаем следующее:

1. Использование ИИ для предупреждения преступности крайне важно и необходимо. При этом особое внимание должно уделяться сохранению широких возможности государства по контролю над сферой ИИ в сочетании с широким и обоснованным внедрением ИИ в публичную сферу. При разработке отечественных систем следует учитывать положительный и отрицательный отечественный и зарубежный опыт законотворчества и практики его применения.

2. Прогностические суждения на основе ИИ необходимо строить исходя из данных, свободных от мотивов личной и корпоративной выгоды, статистических искажений, взятых за актуальный для текущей обстановки исторический период. Для этого требуется своевременное обновление сведений, блокирование устаревшей, неадекватной информации, использование которой может привести к выводам и рекомендациям, не отвечающим современным реалиям, способным повлечь социальную напряженность и иные отрицательные последствия.

3. ИИ должен действовать только под контролем человека. Конкретные решения на основании выводов специальных программ в области профилактики преступности, тем более на стратегическом уровне, должны приниматься только после их анализа и оценки специалистами. Требуется неуклонное соблюдение этического постулата, закрепленного Концепцией, о подконтрольности ИИ человеку и минимизации заложенной возможности автономного его функционирования и только в условиях необходимости.

4. В принятии решения о внедрении ИИ в дело профилактики преступности необходимо отталкиваться от необходимости такового. Грань между обоснованным использованием ИИ и злоупотреблением весьма тонкая. Применение ИИ не самоцель, а лишь средство. Оптимальным решением является сочетание новейших с консервативными, но прогрессирующими методами профилактической работы, при которых происходит взаимное их дополнение и обогащение.

5. Профилактические рекомендации ИИ должны строиться на основе программных алгоритмов, которые давали бы эффективные прогнозы преступности с поправкой на статистические и др. искажения.

6. Для программных алгоритмов ИИ в области профилактики преступности, на которых строятся решения, влияющие на широкий, индивидуально неопределенный круг лиц, следует предусмотреть понятный механизм доступа к информации о применяемых в программных продуктах алгоритмах работы ИИ. Должна быть прописана процедура подотчетности, которая, возможно, «приоткроет завесу» коммерческой тайны компаний-разработчиков, раскрывая работу алгоритмов ИИ как условие для приемки и широкого использования в интересах государства.

7. В вопросе правового регулирования применения ИИ в сфере профилактики преступности происходит комбинирование моделей «от практики к нормативному регулированию» и «от концептуальной модели к ее внедрению на практике», их взаимное дополнение. Сегодня в стране приняты лишь основополагающие документы. Требуется их дальнейшая апробация с последующими выводами и формированием законодательства «широкого» действия.

Список источников

1. Смирнов В. Е. К вопросу о допустимости в уголовном судопроизводстве информации, генерируемой системами с элементами машинного обучения (на примере США) // Международное уголовное право и международная юстиция. 2025. № 1.

2. Кинякина Е., Устинова А. МВД привлекает нейросети к поиску нарушителей // URL: https://www.vedomosti.ru/technology/articles/2024/01/11/1014513-mvd-privlechet-neiroseti-k-poisku-pravonarushitelei?from=popular_search_1&utm_source=Securitylab.ru/

3. Архипов С. И. Субъект права : теоретическое исследование. СПб., 2004.

4. Национальная стратегия развития искусственного интеллекта на период до 2030 года (утв. Указом Президента РФ от 10 октября 2019 г. № 490) // URL: http://www.kremlin.ru/acts/bank/44731?clckid=2427a1c8/

5. Roth A. L. Trial by Machine // Georgetown Law Journal. 2016. Vol. 104. Iss. 5. P. 20–21.

6. Ермакова Е. П., Фролова Е. Е. Искусственный интеллект в гражданском судопроизводстве и арбитраже : опыт США и КНР. М. : Юрлитинформ, 2021.

7. Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» // Собрание законодательства Российской Федерации. 2004. № 32. Ст. 3283.

8. Харитонова Ю. С. Правовые средства обеспечения принципа прозрачности искусственного интеллекта // Journal of Digital Technologies and Law. 2023. № 1 (2).

9. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации. 2006. № 31. Ст. 3448.

10. Распоряжение Правительства Российской Федерации от 19 августа 2020 г. № 2129-р // Собрание законодательства Российской Федерации. 2020. № 35. Ст. 5593.

11. Кутейников Д. Л., Ижаев О. А., Зенин С. С., Лебедев В. А. Ключевые подходы к правовому регулированию использования систем искусственного интеллекта // Вестник Тюменского государственного универ-

ситета. Социально-экономические и правовые исследования. 2022. Т. 8. № 1 (29).

12. Федеральный закон от 31 июля 2020 г. № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых и технологических инноваций в Российской Федерации» // Собрание законодательства Российской Федерации. 2020. № 31 (часть I). Ст. 5017.

13. Regan P. M. Privacy, Data Protection and the Law // Journal of Information Law and Technology. 2015.

References

1. Smirnov V. E. On the issue of the admissibility in criminal proceedings of information generated by systems with elements of machine learning (using the example of the USA) // International criminal law and international justice. 2025. № 1.

2. Kinyakina E., Ustinova A. M. First of all attracts the attention of readers // URL: https://www.vedomosti.ru/technology/articles/2024/01/11/1014513-mvd-privlechet-neiroseti-k-poisku-pravonarushitelei?from=popular_search_1&utm_source=Securitylab.ru/

3. Arkhipov S. I. The subject of law : theoretical study. SPb., 2004.

4. National Strategy for the development of Public Administration for the period up to 2030 (Decree of the President of the Russian Federation dated October 10, 2019 № 490) // URL: http://www.kremlin.ru/acts / bank/44731?clckid=2427a1c8/

5. Roth A. L. Judicial process using a machine // Georgetown Law Journal. 2016. Vol. 104. Iss. 5. P. 20–21.

6. Ermakova E. P., Frolova E. E. Artificial intelligence in civil proceedings and arbitration : the experience of the USA and China. M. : Yurlitinform, 2021.

7. Federal Law of July 29, 2004 № 98-FZ «On commercial secrets» // Collection of legislation of the Russian Federation. 2004. № 32. Art. 3283.

8. Kharitonova Yu. S. Basic tools for monitoring the use of the Internet // Journal of Digital Technologies and Law. 2023. № 1 (2).

9. Federal Law of July 27, 2006 № 149-FZ «On Information, information technologies and information protection» // Collection of Legislation of the Russian Federation. 2006. № 31. Art. 3448.

10. Decree of the Government of the Russian Federation dated August 19, 2020 № 2129-r // Collection of legislation of the Russian Federation. 2020. № 35. Art. 5593.

11. Kuteynikov D. L., Izhaev O. A., Zenin S. S., Lebedev V. A. Key approaches to the legal regulation of the use of artificial intelligence systems // Bulletin of the Tyumen State University. Socio-economic and legal studies. 2022. V. 8. № 1 (29).

12. Federal Law № 258-FZ dated July 31, 2020 «On Experimental Legal Regimes in the Field of Digital and Technological Innovations in the Russian Federation» // Collection of legislation of the Russian Federation. 2020. № 31 (part I). Art. 5017.

13. Regan P. M. Confidentiality, data protection and the law // Journal of Information Law and Technology. 2015.

Информация об авторах

М. Д. Давитадзе – профессор кафедры криминологии и уголовно-исполнительного права имени В.Е. Эминова Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), профессор кафедры теории и истории государства и права Московского университета имени С.Ю. Витте, доктор юридических наук, профессор;

А. А. Середин – доцент кафедры уголовного права и процесса Открытого гуманитарно-экономического университета, кандидат юридических наук, доцент.

Information about the author

M. D. Davitadze – Professor of the V.E. Eminov Department of Criminology and Penal Enforcement Law of the Kutafin Moscow State Law University (MSAL), Professor of the Department of Theory and History of State and Law of the Moscow University named after S.Yu. Witte, Doctor of Legal Sciences, Professor;

A. A. Seredin – Associate Professor of the Department of Criminal Law and Procedure of the Open University of Humanities and Economics, Candidate of Legal Sciences, Associate Professor.

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации. Авторы заявляют об отсутствии конфликта интересов.

Contribution of the authors: the authors contributed equally to this article. The authors declare no conflicts of interests.

Статья поступила в редакцию 11.11.2025; одобрена после рецензирования 10.12.2025; принята к публикации 13.01.2026.

The article was submitted 11.11.2025; approved after reviewing 10.12.2025; accepted for publication 13.01.2026.