Научная статья
Научная специальность
5.1.4 «Уголовно-правовые науки»

УДК 343.98
DOI https://doi.org/10.26516/2071-8136.2026.1.103

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В КРИМИНАЛИСТИЧЕСКОМ АНАЛИЗЕ: ОТДЕЛЬНЫЕ ПРОБЛЕМЫ ТЕОРИИ И ПРАКТИКИ

© Фомина И. А., 2026
Восточно-Сибирский институт МВД России, г. Иркутск, Россия

Проведен комплексный анализ трансформации криминалистической деятельности под воздействием технологий искусственного интеллекта, обусловленной цифровизацией доказательственной базы и усложнением механизмов преступной деятельности. Рассматриваются ключевые направления алгоритмической обработки криминалистически значимой информации, включая автоматизированные системы биометрической идентификации, нейросетевые модели анализа видеопотоков, методы интеллектуальной трасологии, а также инструменты выявления аномалий и латентных связей в цифровых следах. Показано, что внедрение систем искусственного интеллекта способствует повышению точности экспертных заключений, расширяет возможности комплексной реконструкции событий преступления и оптимизации аналитических процедур, требующих обработки больших массивов данных. Отдельно акцентируется внимание на формировании новых форм цифровой криминалистической компетентности, предполагающей интеграцию традиционных экспертных методик с алгоритмами статистического и вероятностного анализа. Кроме того, подчеркивается, что развитие технологий искусственного интеллекта приводит к возникновению принципиально новых типов цифровых следов, требующих методического осмысления и унификации процедур их оценки. Особое внимание уделено проблематике методологической верифицируемости алгоритмов, возникающей вследствие непрозрачности вычислительных моделей (эффект «черной коробки»), а также рискам алгоритмических смещений, проявляющихся при несбалансированности обучающих выборок. Обосновывается необходимость разработки нормативно-технических регламентов, устанавливающих требования к качеству исходных данных, формальным параметрам цифровых доказательств, процедурам интерпретации результатов автоматизированных систем и критериям допустимости их использования в уголовном судопроизводстве. Подчеркивается, что интеграция алгоритмических инструментов в криминалистический анализ требует сохранения профессионального контроля со стороны человека, который должен включать критическую оценку корректности вычислительных процедур, двойную проверку «пограничных» результатов и документирование всех этапов алгоритмической обработки. Утверждается, что устойчивое функционирование систем искусственного интеллекта в сфере раскрытия и расследования преступлений возможно лишь при сочетании технической стандартизации, междисциплинарной экспертной подготовки и правовой регламентации, обеспечивающих минимизацию рисков ложноположительных совпадений, недопущение дискриминационных ошибок и гарантирование соблюдения принципов справедливого правосудия.

Ключевые слова: цифровая криминалистика, искусственный интеллект, информационные технологии, криминалистический анализ, цифровые технологии, нейросети.

APPLICATION OF ARTIFICIAL INTELLIGENCE IN FORENSIC ANALYSIS: SELECTED THEORETICAL AND PRACTICAL CHALLENGES

© Fomina I. A., 2026
East Siberian Institute of the MIA of Russia, Irkutsk, Russian Federation

The present study offers a comprehensive analysis of the transformation of forensic activity under the influence of artificial intelligence technologies, driven by the digitalization of the evidentiary base and the growing complexity of criminal mechanisms. The work examines key directions of algorithmic processing of forensically significant information, including automated biometric identification systems, neural-network models for video stream analysis, methods of intelligent trace examination, as well as tools for detecting anomalies and latent connections within digital traces. It is demonstrated that the implementation of artificial intelligence systems enhances the accuracy of expert conclusions, expands the possibilities for comprehensive reconstruction of crime events, and optimizes analytical procedures that require the processing of large data volumes. Special emphasis is placed on the emergence of new forms of digital forensic competence, which presuppose the integration of traditional expert methodologies with algorithms of statistical

and probabilistic analysis. Furthermore, it is noted that the development of artificial intelligence technologies leads to the formation of fundamentally new types of digital traces, which require methodological conceptualization and the unification of evaluation procedures. Particular attention is devoted to the problem of methodological verifiability of algorithms, arising from the opacity of computational models (the "black box" effect), as well as to the risks of algorithmic bias resulting from imbalanced training datasets. The study substantiates the need for the development of regulatory and technical frameworks establishing requirements for the quality of input data, formal parameters of digital evidence, procedures for the interpretation of automated system outputs, and criteria for their admissibility in criminal proceedings. It is emphasized that the integration of algorithmic tools into forensic analysis requires the preservation of professional human oversight, which must include a critical assessment of computational procedures, double-checking of borderline results, and thorough documentation of all stages of algorithmic processing. The study asserts that the stable functioning of artificial intelligence systems in the field of crime detection and investigation is possible only through a combination of technical standardization, interdisciplinary expert training, and legal regulation, ensuring the minimization of false positives, the prevention of discriminatory errors, and the safeguarding of the principles of fair justice.

Keywords: digital forensics, artificial intelligence, information technologies, forensic analysis, digital technologies, neural networks.

Введение

Современная криминалистика переживает качественный этап трансформации под влиянием цифровых технологий и систем искусственного интеллекта (далее – ИИ). Развитие вычислительных мощностей, алгоритмов машинного обучения и методов анализа больших данных (АБД) создает новые возможности для обработки доказательств, идентификации лиц, сопоставления следов и моделирования событий преступлений. Важно подчеркнуть, что необходимость внедрения современных технологий была обозначена для системы органов внутренних дел сразу после утверждения указом Президента РФ[1] Национальной стратегии развития искусственного интеллекта до 2030 года. В данном акте среди ключевых направлений выделены ускоренное развитие отечественных ИИ-систем, активизация научных исследований в этой области, а также подготовка специалистов, способных эффективно работать с технологиями искусственного интеллекта.

ИИ-технологии используются в различных сферах криминалистики, включая автоматизированное распознавание лиц, биометрических данных, почерка и отпечатков, анализ видеозаписей с мест происшествий, компьютерную трасологию и цифровую криминалистику. Алгоритмы машинного обучения способны выявлять скрытые закономерности в больших массивах данных, прогнозировать вероятные сценария развития событий, при этом их использование в экспертной деятельности может способствовать повышению объективности и воспроизводимости выводов экспертов, не подменяя собой процесс экспертного исследования. Так, «посредством использования ИИ при расследовании преступлений коррупционной направленности возможно создание действенного и прозрачного механизма криминалистической профилактики, а также повысить уровень доверия населения к органам государственной власти и местного самоуправления» [5, с. 34]. Вместе с тем такие системы требуют контроля и понимания их возможностей и ограничений, так как автоматизация отдельных процессов не исключает необходимости профессиональной оценки и интерпретации результатов. Особое значение имеют вопросы взаимодействия ИИ с традиционными методами криминалистического анализа. Совмещение автоматизированных инструментов с экспертной оценкой позволит достигать более высокой достоверности и обоснованности выводов.

Однако интеграция ИИ в криминалистическую практику также порождает новые вызовы и задачи, связанные с проверкой корректности работы алгоритмов, предупреждением ошибок и минимизацией возможного влияния алгоритмических предубеждений на результаты расследования.

Нельзя не согласиться, что «качественное совершенствование средств преступлений, использующих методы, получаемые при разработке технологий искусственного интеллекта, приводит к серьезному усложнению расследования и предупреждения высокотехнологичных преступных деяний» [2, с. 23]. Соответственно, исследование различных аспектов использования ИИ в криминалистическом анализе предполагает рассмотрение не только возможностей данных технологий и их ограничений, а также разработку подходов, обеспечивающих безопас-

[1] О развитии искусственного интеллекта в Российской Федерации : указ Президента РФ от 10 окт. 2019 г. № 490 // Президент России : офиц. сайт. URL: http://www.kremlin.ru/acts/bank/44731 (дата обращения: 11.11.2025).

ное и рациональное применение рассматриваемых инструментов. В данном контексте задача исследования заключается в систематизации существующих методов, анализе потенциальных проблем и выработке рекомендаций по эффективной интеграции ИИ в практику раскрытия, расследования и предупреждения преступлений, с учетом необходимости сохранения профессионального контроля и соблюдения правовых и этических норм.

Материалы и методы исследования

Материалами исследования выступают публикации и нормативные документы, регулирующие использование технологий искусственного интеллекта в криминалистической практике, а также работы по криминалистике и судебной экспертизе. С практической стороны изучены примеры применения ИИ в анализе видеозаписей, биометрических данных, трасологических следов и других видов доказательств, включая открытые датасеты и опубликованные кейсы ошибок и ограничений алгоритмов.

Результаты исследования

В современном криминалистическом анализе технологии искусственного интеллекта находят свое применение в нескольких ключевых направлениях, обеспечивая автоматизацию процессов идентификации и сопоставления доказательств, повышение точности экспертиз, ускорение обработки больших массивов информации и формирование более обоснованных версий событий преступления.

Одним из наиболее распространенных направлений использования ИИ-технологий является автоматизированное распознавание лиц, следов и видеозаписей с мест происшествия. Использование алгоритмов машинного обучения позволяет систематизировать и сопоставлять большие массивы визуальной информации, выявлять характерные признаки объектов и проводить идентификацию участников событий. Так, системы распознавания лиц интегрируются в процесс идентификации подозреваемых и свидетелей, обеспечивая быстрый поиск совпадений по массивам изображений, полученных с камер наблюдения и больших биометрических баз. Технологии анализа следов позволяют алгоритмически выделять микроскопические особенности и сравнивать их с образцами, ранее внесенными в экспертные коллекции и АБД.

Видеоконтент, поступающий с камер наблюдения или дорожно-транспортных систем, обрабатывается нейросетями, способными фиксировать движения объектов, распознавать действия людей, отслеживать траектории и идентифицировать аномалии поведения. Примером может служить практика применения информационно-поисковой системы АПК «Безопасный город», которая обеспечивает эффективное управление безопасностью при массовых мероприятиях, поддержание общественного порядка, а также выявление, предупреждение и расследование преступлений и правонарушений. По состоянию на март 2024 г. в России каждая третья камера видеонаблюдения из более 1 млн установленных в рамках «Безопасного города» подключена к системе распознавания лиц, а все камеры, которые установлены на дорогах, автоматически распознают номера транспортных средств[1]. По данным сайта Департамента информационных технологий Москвы, система городского видеонаблюдения используется при раскрытии 70 % преступлений[2]. Применение указанных технологий позволяет идентифицировать участников преступлений и инцидентов, ускоряя расследование. Система постепенно интегрирует модули ИИ, аналитические платформы, автоматическое распознавание – что делает ее не просто наблюдательной, но и предиктивной, способной анализировать поведение объектов в реальном времени, выявлять аномалии, прогнозировать потенциальные инциденты и заранее сигнализировать о ситуациях, требующих вмешательства правоохранительных органов. Развитие этих технологий существенно ускоряет процесс криминалистического анализа, снижает нагрузку на правоохранительные органы и экспертные подразделения и обеспечивает более высокую степень детализации по сравнению с традиционными методами ручного просмотра.

Кроме того, автоматизированное распознавание способствует выявлению сведений и доказательственной информации, которые могли бы остаться не замеченными при визуальной оценке. Однако эффективность таких систем зависит:

– *от качества исходных данных.* Так, ухудшение качества изображения (размытость, слабое освещение, низкое разрешение, нестандартный угол съемки) сильно снижает точность алгоритмов распознавания лиц – при этом риски лож-

[1] АПК «Безопасный город» // Tadviser. Государство. Бизнес. Технологии : сайт. URL: https://www.tadviser.ru/index.php (дата обращения: 12.10.2025).

[2] Москва раскрыла бюджет на безопасность в 2024 году // РБК : сайт. URL: https://www.rbc.ru/economics/20/10/2023/652e7f7e9a794735bd3aa2a4 (дата обращения: 06.11.2025).

ных совпадений остаются особенно высокими для женщин и представителей этнических меньшинств[1];

– *точности обучающих выборок и корректности алгоритмических моделей*. Так, недостаточно сбалансированные обучающие данные (например, несбалансированность по демографическим признакам (раса, пол, возраст) или представленность только «идеальных» условий) могут вести к искажению итоговых результатов, снижению точности распознавания для других групп.

Решение указанных проблем видится, в частности, в использовании камер с высоким разрешением и улучшенной светочувствительностью, а также внедрении методов интеллектуальной стабилизации и коррекции изображения, включая шумоподавление, адаптивное повышение резкости и динамическую коррекцию освещенности для повышения качества исходных данных. Значимое влияние на точность распознавания оказывают процедуры нормализации изображений, такие как выравнивание лица, коррекция угла поворота и реконструкция трехмерной модели при отклонениях от фронтального ракурса.

Наряду с техническими мерами необходимо разработать требования к качеству видеозаписи (разрешение и детализация изображения, частота кадров, цветопередача, контраст, длительность и полнота записи, требования к хранению и другое) и проводить регулярное техническое обслуживание оборудования.

Повышение точности работы алгоритмов также требует тщательной работы с обучающими выборками. Полные и сбалансированные по возрасту, полу и другим характеристикам наборы данных, включающие изображения, сделанные в «неидеальных» условиях, а также использование приема увеличения данных для имитации различных условий съемки помогают улучшить качество распознавания. Важное значение имеет применение методов обучения, учитывающих принципы справедливости, а также объединение нескольких моделей и приемов самоконтролируемого обучения, которые делают алгоритмы более устойчивыми к реальным условиям.

Другим значимым направлением использования ИИ-технологий является анализ цифрового пространства на выявление потенциально скрытых угроз. Современные криминалистические задачи требуют обработки огромных массивов данных, включая журналы активности пользователей, метаданные файлов, сетевую переписку, данные систем видеонаблюдения и другие цифровые следы. Внедрение технологий ИИ позволяет правоохранительным органам не просто собирать такие данные, но систематизировать их, выявлять скрытые закономерности, типичные паттерны поведения, устанавливать связи между участниками событий и прогнозировать возможные действия подозреваемых. Так, из исследования, проведенного З. И. Харисовой, следует, что применение алгоритмов машинного обучения позволяет выделять естественные связи между элементами криминалистической характеристики (на примере коррупционных составов), распознавать модели преступного поведения и на основе анализа этих данных обеспечивать оперативное принятие решений даже в условиях неопределенности [6]. Использование ИИ в данном ключе особенно эффективно при расследовании киберпреступлений, мошенничества, несанкционированного доступа к информационным системам, распространения вредоносного программного обеспечения и иных правонарушений, связанных с информационными технологиями, где алгоритмы машинного обучения позволяют выявлять аномалии в поведении пользователей, сопоставлять повторяющиеся схемы действий и прогнозировать потенциальные угрозы на основе анализа больших данных, что было бы крайне трудозатратно при ручной обработке.

Между тем следует отметить и здесь ряд проблемных аспектов. Во-первых, качество результатов ИИ-анализа цифрового пространства напрямую зависит от полноты и достоверности исходных данных и доступа к ним: неполные журналы активности, поврежденные файлы или недостаточно точные метаданные могут приводить к ложноположительным или ложноотрицательным выводам. Во-вторых, алгоритмическая «черная коробка» часто ограничивает возможность эксперта интерпретировать процесс принятия решений заданной системой, что создает риски ошибочной оценки доказательств в судебной практике. В-третьих, существующие модели могут демонстрировать смещения, обусловленные несбалансированностью обучающих выборок или недостаточным учетом контекста, что особенно критично при анализе данных, связанных с различными демографическими или социальными группами.

[1] Cuellar M., To Hon Kiu, Mehrotra A. Accuracy and Fairness of Facial RecognitionTechnology in Low-Quality Police Images: AnExperiment with Synthetic Faces. URL: https://arxiv.org/pdf/2505.14320 (дата обращения: 12.10.2025).

Для решения обозначенных проблем, прежде всего, необходима стандартизация процедур сбора и ведения исходных материалов, включающая установление единых требований к полноте журналов активности, качеству метаданных и форматам хранения. Дополнение таких мер автоматизированными средствами проверки целостности и достоверности данных, а также механизмами их перекрестной верификации позволяет существенно снизить риск появления ложных выводов, обусловленных дефектами входной информации. Для случаев, когда повреждения или пробелы в данных неизбежны, должны применяться методы восстановительной обработки с обязательной фиксацией факта вмешательства и степени влияния на конечный результат.

Далее, для преодоления ограничений, связанных с эффектом «черной коробки», требуется широкое внедрение моделей, допускающих объяснение хода принятия решений и предоставляющих возможность экспертного анализа их внутренних механизмов. Это предполагает ведение подробных журналов вычислительных процедур, формирование методических рекомендаций по интерпретации результатов ИИ-систем, а также повышение квалификации специалистов, осуществляющих судебно-экспертную деятельность в сфере цифровой аналитики. Такой подход обеспечивает возможность проследить логику формирования выводов и снижает риск ошибочной оценки доказательственного материала.

Наконец, для устранения смещений, возникающих вследствие несбалансированности обучающих выборок или недостаточного учета контекста, требуется формирование репрезентативных наборов данных, отражающих разнообразие демографических и социальных характеристик, а также условий получения цифровой информации. Систематическая оценка моделей на предмет неравномерности ошибок, применение методов увеличения данных и организация независимого тестирования позволяют выявлять скрытые перекосы и корректировать алгоритмы до достижения приемлемого уровня устойчивости.

Дополнительной общей проблемой является комплекс правовых и этических рисков, возникающих при применении систем с внедренными ИИ-технологиями в сфере расследования, раскрытия и профилактики преступной деятельности, в рамках уголовного судопроизводства. Прежде всего, алгоритмически сформированные выводы, используемые без участия квалифицированного специалиста, могут вступать в противоречие с принципами справедливого правосудия. Как обоснованно отмечает С. С. Ржанникова, «внедрение возможностей искусственного интеллекта в различные сферы жизни общества обусловливает необходимость разработки и утверждения нормативно-технической документации в соответствующих отраслях» [3, с. 163].

С этической стороны особое значение имеет проблема алгоритмической предвзятости и достоверности выводов. Алгоритмы машинного обучения могут демонстрировать различную точность при работе с разными группами объектов и участников событий, что связано с особенностями обучающих данных и методами аннотации. Это создает риск получения ошибочных результатов, которые в дальнейшем могут повлиять на выводы эксперта и решения следственных органов.

С тактической точки зрения внедрение ИИ изменяет подходы к сбору и обработке доказательств. Использование автоматизированных систем позволяет ускорять анализ больших массивов данных и формировать вероятные сценарии событий, однако существует риск излишней зависимости от алгоритмических выводов. Следственные действия, включая осмотр места происшествия, допросы и реконструкцию событий, требуют сохранения профессионального контроля со стороны человека, который оценивает результаты работы ИИ и принимает решения с учетом всей совокупности доказательств. Как обоснованно был отмечено Д. В. Бахтеевым, «искусственные нейронные сети можно рассматривать как программные или аппаратные комплексы простых обработчиков данных, способных обмениваться друг с другом сигналами и при достаточно развитой структуре и настроенной логике взаимодействия решать сложные задачи» [1, с. 44].

Дополнительным тактическим аспектом является необходимость адаптации традиционных методов криминалистического анализа к новым условиям. Модернизация подходов к идентификации лиц, анализу цифровых следов и трасологических данных требует разработки регламентов и протоколов взаимодействия ИИ и эксперта, а также выработки процедур проверки корректности и воспроизводимости выводов автоматизированных систем. При этом особое внимание уделяется вопросам этической и правовой допустимости использования таких

технологий в расследовании, включая обеспечение защиты прав участников процесса и минимизацию возможных негативных последствий ошибок алгоритмов.

Системы искусственного интеллекта используют формально-логические структуры, что говорит об их неспецифичности для человеческого мышления [4, с. 7]. Соответственно, в условиях, когда логика работы алгоритма остается частично или полностью недоступной для проверки, существенно затрудняется возможность стороны защиты оспорить достоверность и корректность полученных результатов. Возникает риск замещения профессионального экспертного суждения автоматически сгенерированными заключениями, притом что алгоритм может содержать скрытые ошибки, смещения или ограничения, неочевидные для участников процесса. Такая ситуация подрывает один из фундаментальных принципов судебной деятельности – проверяемость и обоснованность доказательств. Следовательно, необходимо сочетание алгоритмического анализа и экспертной оценки: использование ИИ-технологий должно выступать лишь как инструмент фильтрации и структурирования информации, с предложением вероятностных алгоритмов решения, а окончательные выводы должны формироваться с участием человеческого фактора. Для этого необходимо разработать стандарты взаимодействия эксперта и алгоритма, включая правила двойной проверки результатов, протоколы верификации «подозрительных находок» и процедуры документирования алгоритмической обработки данных. Применение ИИ без корректной интерпретации со стороны человека усиливает риск неправильного понимания цифровых следов и может исказить общую картину расследования.

Также необходимо внедрять механизмы контроля качества и оценки возможных рисков, включая независимое тестирование моделей для разных групп населения, проверку показателей ложных срабатываний и пропусков, проведение стресс-тестов, а также внутренние и внешние аудиты алгоритмов. Применение автоматизированного распознавания должно сопровождаться обязательной проверкой результатов человеком, установкой порогов достоверности совпадений и разработкой процедур оспаривания решений системы. Ведение понятных журналов работы алгоритмов и использование методов, позволяющих объяснять действия системы, повышают прозрачность и доверие к ней.

Не менее значимой является проблема соблюдения прав человека в процессе автоматизированного анализа цифровых следов. Системы ИИ, предназначенные для выявления подозрительных действий, нередко требуют обработки больших массивов личных данных, что неизбежно затрагивает право на неприкосновенность частной жизни. Риски усиливаются в случаях, когда сбор и обработка информации осуществляются без информированного согласия субъектов, без достаточного нормативного регулирования или с применением технологий скрытого наблюдения. Возможность ошибочного отнесения лица к группе повышенного риска или неверной классификации его поведения как подозрительного может приводить к неоправданному вмешательству государства в частную жизнь, а в более серьезных случаях – к ограничениям правового статуса человека.

Кроме того, автоматизация процессов анализа несет угрозу «нормализации» постоянного мониторинга, когда расширение технических возможностей приводит к постепенному размыванию границ допустимого вмешательства в личную сферу. В отсутствие четких правовых гарантий возникает риск необоснованного расширения полномочий органов, использующих такие технологии, а также проблемы с последующим контролем использования собранных данных, их хранением и доступом к ним.

Кроме технических и методологических мер, требуется нормативное регулирование. Оно должно предусматривать допустимость и критерии использования ИИ-аналитики, требования к качеству данных, стандарты хранения цифровых доказательств, а также гарантии защиты персональных данных. Отдельного внимания заслуживает разработка процессуальных критериев допустимости доказательств, полученных с использованием ИИ: суды должны иметь ясные ориентиры для оценки надежности и валидности таких выводов.

Необходимым направлением является повышение квалификации специалистов. Эксперты должны обладать навыками работы с алгоритмическими инструментами, понимать сильные и слабые стороны используемых моделей, а также уметь критически анализировать представленные им результаты. Разработка образовательных программ и методических рекомендаций способствует более корректному применению ИИ в уголовно-правовой и криминалистической деятельности.

Обсуждения и заключения

Подводя итог, следует отметить, что именно комплексный подход к решению рассматриваемых проблем является оптимальным и предполагает сочетание технических, организационных и правовых мер, включая обучение операторов, создание междисциплинарных экспертных групп, установление нормативов недискриминационности алгоритмов и ответственности за качество данных и моделей. Только интеграция этих направлений позволяет минимизировать риски ложноположительных совпадений и дискриминационных ошибок, особенно в отношении уязвимых групп населения, обеспечивая тем самым более надежное и справедливое применение технологий автоматизированного распознавания.

СПИСОК ЛИТЕРАТУРЫ

1. Бахтеев Д. В. Искусственный интеллект в криминалистике: состояние и перспективы использования // Российское право: образование, практика, наука. 2018. № 2 (104). С. 43–49.

2. Поляков В. В. К проблеме использования понятия «искусственный интеллект» в криминалистике // Юрислингвистика. 2022. № 25 (36). С. 21–28.

3. Ржанникова С. С. Стандартизация процесса использования искусственного интеллекта в судебно-экспертной деятельности // Криминалистика: вчера, сегодня, завтра. 2023. № 4. С. 163–171. DOI: 10.55001/2587-9820.2023.46.66.016

4. Степаненко А. С., Степаненко Д. А. Перспективы развития искусственного интеллекта в научном освоении мира // Baikal Research Journal. 2019. Т. 10, № 4. С. 1–10.

5. Усенко А. С. Криминалистические аспекты использования искусственного интеллекта для мониторинга доходов и расходов лиц, подверженных коррупции, и членов их семей // Актуальные проблемы правоведения. 2024. № 4 (84). С. 32–36.

6. Харисова З. И. Оптимизация процесса поиска, анализа и интерпретации цифровых доказательств с использованием алгоритмов искусственного интеллекта // Общество, право, государственность: ретроспектива и перспектива. 2025. № 3. С. 60–69.

REFERENCES

1. Bakhteev D.V. Iskusstvennyi intellekt v kriminalistike: sostoyanie i perspektivy ispol'zovaniya [Artificial Intelligence in Criminalistics: State and Prospects of Use]. *Rossiiskoe pravo: obrazovanie, praktika, nauka* [Russian Law: Education, Practice, Science], 2018, no. 2(104), pp. 43-49. (in Russian)

2. Polyakov V.V. K probleme ispolzovaniya ponyatiya "iskusstvennyi intellect" v kriminalistike [On the Problem of Using the Concept of "Artificial Intelligence" in Criminalistics]. *Yurislingvistika* [Legal Linguistics], 2022, no. 25(36), pp. 21-28. (in Russian)

3. Rzhannikova S.S. Standartizatsiya protsessa ispolzovaniya iskusstvennogo intellekta v sudebno-ekspertnoi deyatelnosti [Standardization of the Process of Using Artificial Intelligence in Forensic Expert Activity]. *Kriminalistika: vchera, segodnya, zavtra* [Criminalistics: Yesterday, Today, Tomorrow], 2023, no. 4, pp. 163-171. DOI: 10.55001/2587-9820.2023.46.66.016 (in Russian)

4. Stepanenko A.S., Stepanenko D.A. Perspektivy razvitiya iskusstvennogo intellekta v nauchnom osvoenii mira [Prospects for the Development of Artificial Intelligence in the Scientific Exploration of the World]. *Baikal Research Journal*, 2019, vol. 10, no. 4, pp. 1-10. (in Russian)

5. Usenko A.S. Kriminalisticheskie aspekty ispol'zovaniya iskusstvennogo intellekta dlya monitoringa dokhodov i raskhodov lits, podverzhennykh korruptsii, i chlenov ikh semei [Forensic Aspects of Using Artificial Intelligence for Monitoring Income and Expenses of Persons Subject to Corruption and Their Family Members]. *Aktual'nye problemy pravovedeniya* [Current Problems of Jurisprudence], 2024, no. 4(84), pp. 32-36. (in Russian)

6. Kharisova Z.I. Optimizatsiya protsessa poiska, analiza i interpretatsii tsifrovykh dokazatel'stv s ispol'zovaniem algoritmov iskusstvennogo intellekta [Optimization of the Process of Searching, Analyzing and Interpreting Digital Evidence Using Artificial Intelligence Algorithms]. *Obshchestvo, pravo, gosudarstvennost': retrospektiva i perspektiva* [Society, Law, Statehood: Retrospective and Perspective], 2025, no. 3, pp. 60-69. (in Russian)

Статья поступила в редакцию 08.12.2025; одобрена после рецензирования 28.12.2025; принята к публикации 11.02.2026

Received on 08.12.2025; approved on 28.12.2025; accepted for publication on 11.02.2026

Фомина Инна Анатольевна – кандидат юридических наук, доцент, доцент кафедры уголовного права и криминологии, Восточно-Сибирский институт МВД России (Россия, 664071, г. Иркутск, ул. Лермонтова, 110), ORCID: 0000-0002-4088-7182, Researcher ID: ACC-5222-2022, e-mail: iafomina@mail.ru

Fomina Inna Anatolievna – Candidate of Juridical Sciences, Associate Professor, Associate Professor at the Department of Criminal Law and Criminology, East-Siberian Institute of the Ministry of Internal Affairs of Russia (110, Lermontov st., Irkutsk, 664071, Russia Federation), ORCID: 0000-0002-4088-7182, Researcher ID: ACC-5222-2022, e-mail: iafomina@mail.ru