Дата поступления рукописи в редакцию: 16.06.2026 г.
Дата принятия рукописи в печать: 13.07.2026 г.
DOI: 10.24412/2782-3830-2026-7-416-420

ИСАЕВА Елена Дмитриевна,
кандидат юридических наук,
доцент кафедры криминалистики и уголовно-правовых дисциплин
Брянского филиала Орловского юридического института
МВД России имени В.В. Лукьянова,
e-mail: isaevaelena190373@yandex.ru

ТРАНСФОРМАЦИЯ СЛЕДСТВЕННОЙ ДЕЯТЕЛЬНОСТИ ПОД ВОЗДЕЙСТВИЕМ ЦИФРОВИЗАЦИИ И ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: ВОЗМОЖНОСТИ, РИСКИ И ПРАВОВЫЕ ПЕРСПЕКТИВЫ

Аннотация. *В статье исследуется процесс глубинной трансформации методики расследования преступлений под влиянием цифровизации и интеграции технологий искусственного интеллекта (ИИ). Актуальность темы обусловлена качественным изменением как самого преступного поведения (цифровизация способов совершения преступлений), так и инструментов правоохранительной деятельности. В работе анализируется смена парадигмы с реактивной на проактивную, обосновывается появление новых объектов криминалистического исследования и внедрение интеллектуальных систем анализа данных. Особое внимание уделяется проблемам правового регулирования, этическим вызовам и необходимости трансформации профессиональной подготовки следователей. Автор приходит к выводу, что формируется новый этап развития криминалистики — цифровая криминалистика, требующая синтеза процессуальных гарантий и технологических инноваций.*

Ключевые слова: *цифровизация, искусственный интеллект, методика расследования, цифровые следы, криминалистическая кибернетика, большие данные, допустимость доказательств.*

ISAEVA Elena Dmitrievna,
Candidate of Legal Sciences,
Associate Professor of the Department of Forensic Science and Criminal Law Disciplines at the Bryansk Branch of the Oryol Law Institute of the Ministry of Internal Affairs of Russia named after V.V. Lukyanov

TRANSFORMATION OF INVESTIGATION ACTIVITIES UNDER THE IMPACT OF DIGITALIZATION AND ARTIFICIAL INTELLIGENCE TECHNOLOGIES: OPPORTUNITIES, RISKS, AND LEGAL PROSPECTS

Annotation. *This article examines the profound transformation of crime investigation methods under the influence of digitalization and the integration of artificial intelligence (AI) technologies. The relevance of this topic stems from the qualitative change in both criminal behavior (the digitalization of crime methods) and law enforcement tools. The paper analyzes the paradigm shift from reactive to proactive, substantiates the emergence of new forensic investigation objects, and the implementation of intelligent data analysis systems. Particular attention is paid to legal regulation issues, ethical challenges, and the need to transform the professional training of investigators. The author concludes that a new stage in the development of forensic science is emerging—digital forensics, which requires a synthesis of procedural safeguards and technological innovations.*

Key words: *digitalization, artificial intelligence, investigative methodology, digital traces, forensic cybernetics, big data, admissibility of evidence.*

Современный этап развития общественных отношений характеризуется беспрецедентными темпами цифровой трансформации, охватившей все сферы общественной жизни, включая правоприменительную практику. Преступность не стоит на месте: киберпреступления, использование криптовалют, даркнет и технологии социальной инженерии требуют от следователей принципиально новых подходов к сбору и фиксации доказательств.

Цифровая трансформация уголовного судопроизводства является объективной реальностью современного этапа развития права. Если ранее информационные технологии использовались преимущественно как средства фиксации (фотоаппараты, диктофоны), то сегодня речь идет о внедрении когнитивных технологий, способных анализировать информацию и предлагать готовые решения. Искусственный интеллект перестает быть футуристической концепцией и начинает интегрироваться в рутинную работу правоохранительных органов.

В этих условиях искусственный интеллект и цифровые технологии становятся не просто вспомогательными инструментами, а стратегическим ресурсом, определяющим эффективность следствия.

По данным Генпрокуратуры РФ за 2025 год массив преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, сократился на 11,8% (по сравнению с 2024 годом), до 675,4 тысяч. Их раскрываемость улучшилась - количество нераскрытых деяний снизилось на 13,5%, до 494,3 тысяч. IT-преступления составляют 38% в общей структуре преступности. Половину всех IT-преступлений составляют кибермошенничества - 350 тысяч. При этом число мошенничеств в России сократилось в 2025 году на 7,6%, из них около 85% приходится на кибермошенничества [7].

Это создает качественно новые вызовы для правоохранительной системы. Традиционные криминалистические методики, сформированные в эпоху доминирования материальных и идеальных следов, сталкиваются с ограничениями при работе с гигантскими массивами неструктурированных данных (Big Data), киберпространством и распределенными реестрами.

Цифровая трансформация затрагивает не только объект познания (преступность), но и сам инструментарий следователя. Современная криминалистика переживает революцию благодаря внедрению искусственного интеллекта и систем автоматизированного анализа, что значительно повышает эффективность раскрытия и расследования преступлений. Происходит фундаментальный сдвиг от традиционных, описательных подходов к кибернетической криминалистике, опирающейся на математизацию и автоматизацию работы с информацией. Этот процесс сопряжен с неизбежными противоречиями, возникающими на стыке передовых технологий, существующих правовых норм и этических принципов.

Криминальный мир претерпевает кардинальные изменения, что ставит перед нами задачу переосмысления фундаментальных основ криминалистического анализа. Во-первых, достаточное количество преступлений совершается в интернете и с помощью новых технологий. Преступники используют искусственный интеллект, чтобы создавать поддельные видео (дипфейки), автоматически рассылать мошеннические письма (фишинг) и взламывать системы защиты. Во-вторых, цифровизация проникает в «традиционные» составы преступлений (кражи, мошенничества, коррупционные деяния), придавая им гибридный характер.

Ключевым понятием современной криминалистики становится «цифровой след». В отличие от традиционных материальных следов, цифровые следы обладают специфическими свойствами: они легко тиражируемы, подвержены модификации, могут существовать как на физическом носителе, так и в «облачной» среде, и часто имеют трансграничную природу. Дискуссионным остается вопрос классификации: являются ли цифровые следы разновидностью материальных или представляют собой самостоятельный, третий вид следов (наряду с материальными и идеальными). Их двойственная природа (физический носитель + виртуальное содержание) требует разработки новых процессуальных и тактических подходов к их собиранию, фиксации и исследованию.

Электронные данные могут быть подвергнуты изменениям или уничтожены, что может вызвать сомнения в их достоверности и юридической значимости. Для использования данных с цифровых носителей в суде необходимо соблюдать стандарты цифровой криминалистики, гарантирующие подлинность и целостность информации. Важно, чтобы процесс был стандартизирован, и специалисты имели высокую квалификацию [2].

Кроме того, объектами криминалистического исследования все чаще становятся не только данные на конкретных устройствах, но и большие данные — массивы информации от операторов сотовой связи, провайдеров интернет-услуг, датчиков интернета вещей (IoT) и систем видеонаблюдения. Обработка таких массивов вручную становится физически невозможной, что создает объективную потребность в автоматизации.

Под влиянием цифровых технологий также происходит фундаментальная трансформация

всей парадигмы расследования. Традиционная модель, основанная на реакции на уже совершенное преступление (реактивная модель), уступает место проактивному подходу. Этот подход включает в себя элементы прогнозирования преступлений, раннего выявления криминальных угроз и автоматизированного горизонтного сканирования для обнаружения новых способов совершения преступлений.

Значимым компонентом процесса доминирования информационно-коммуникационных технологий в обществе становится мышление самих членов общества. Возникает вопрос, является ли сложившаяся в криминалистике ситуация кризисом познания или это лишь необходимость адаптации к изменению объективной реальности [1, С. 45].

Ключевым драйвером этих изменений выступает интеграция инструментов искусственного интеллекта в деятельность следственных и оперативных подразделений. Анализ зарубежного опыта, в частности результатов европейского проекта ROXANNE, демонстрирует создание платформ (Autocrime), способных в автоматическом режиме анализировать перехваченные телефонные переговоры, текстовые сообщения и видеоданные (включая распознавание речи и идентификацию дикторов на нескольких языках), извлекать из них значимую информацию (имена, локации, даты) и строить графы связей преступных сетей.

Использование таких систем позволяет сократить долю рутинной работы по первичному анализу данных с 50–80% до существенно более низких показателей, высвобождая время следователей для содержательной аналитики и принятия стратегических решений.

Процесс автоматизации охватывает все стадии расследования. Например, сбор информации с применением дронов для осмотра места происшествия, использование технологий 3D-моделирования и фотограмметрии для создания неразрушающих и максимально точных виртуальных копий обстановки.

На базе искусственного интеллекта (ИИ) используются системы для обработки и анализа видеоизображений (распознавание лиц, номерных знаков, выявление подозрительного поведения), обработки текстов (анализ переписки в мессенджерах и социальных сетях) и структурирования больших данных.

Для организации более эффективного расследования необходимо внедрять автоматизированные информационные системы, интегрирующие базы данных различных ведомств и обеспечивающие электронное взаимодействие между следователями, экспертами и судами (по информации на декабрь 2025 года МВД России и его территориальные подразделения на региональном уровне имеют возможность отправлять документы в систему ГосЭДО — государственную платформу для обмена электронными документами между организациями и ведомствами, она дополняет обмен сведениями через систему межведомственного электронного взаимодействия (СМЭВ) и открывает путь к переводу документооборота с организациями из бумажного в электронный формат; сервис «Сфера Госзапросы» позволяет получать запросы от органов, осуществляющих оперативно-розыскную деятельность или обеспечение безопасности (МВД, ФСБ, Следственный комитет), в режиме онлайн и направлять актуальные сведения в ответ на них без участия сотрудников организации).

Принципиальное значение для раскрытия и расследования преступлений имеет информация, содержащаяся в системах обеспечения безопасности дорожного движения «Поток»; аппаратно-программном комплексе «Безопасный город» [4]; данные, регистрируемые в автоматическом режиме по сетям мобильной связи, а также в системах позиционирования ГЛОНАСС, GPS, «Android» и «AppleIOS» [6, С. 145].

Председатель Следственного комитета России А.И. Бастрыкин отметил, что для раскрытия IT-преступлений следователи задействуют различные технологические инструменты. В частности, используется программное обеспечение Росфинмониторинга, которое позволяет отслеживать операции с криптовалютами. Кроме того, налажено взаимодействие с крупнейшими российскими IT-компаниями для решения сложных технических задач, возникающих в ходе расследований [4].

Внедрение искусственного интеллекта в расследование преступлений порождает также и сложнейший комплекс правовых проблем — от трудностей правового регулирования до обеспечения допустимости доказательств. Центральное место занимает противоречие между динамикой технологического развития и статичностью уголовно-процессуального законодательства. Применение «умных» алгоритмов в доказывании сталкивается с требованием законности, которое подразумевает ясность, проверяемость и воспроизводимость процедур.

Ключевым вызовом внедрения цифровизации и технологий искусственного интеллекта в судопроизводство является проблема «черного ящика» (black box) — непрозрачности процессов принятия решений многими моделями машинного обучения, особенно глубокими нейросетями, то есть видна только взаимосвязь между входными и выходными данными, а все этапы обработки информации, принимаемые решения и вычисления происходят внутри системы незаметно, их

нельзя проверить напрямую или объяснить простым способом. Таким образом, если следователь, прокурор или суд не могут понять, на каком основании алгоритм выдал ту или иную информацию (например, указал на конкретное лицо как на вероятного преступника), использование такой информации в качестве доказательства становится проблематичным. Это требует разработки механизмов «объяснимого ИИ» (Explainable AI — XAI) - создание систем и моделей, способных объяснять свои действия и принимать решения понятным для людей образом. В центре внимания — логика рассуждений, лежащая в основе решений и предсказаний систем ИИ, адаптированных для нужд уголовного судопроизводства.

Китайские исследователи предлагают для решения этой проблемы концепцию «тройственных правил»: сбор — использование — проверка. Данная модель подразумевает:

– внедрение систем иерархической авторизации доступа к данным — иерархическая авторизация предотвращает утечки и нецелевое использование данных на этапе сбора;
– создание механизмов состязательной проверки результатов работы алгоритмов (по принципу «ИИ против ИИ» или независимый аудит) — состязательная проверка выявляет баги и логические провалы в процессе использования;
– введение института технических заседателей или экспертов, способных дать квалифицированную оценку корректности применения ИИ-технологий — технические заседатели обеспечивают человеческий контроль на этапе проверки, переводя сложные технические решения на язык права и этики.

Отдельную группу составляют вопросы защиты персональных данных и приватности. Сбор и анализ огромных массивов данных о законопослушных гражданах в рамках профилактики преступлений создает риски тотального контроля и нарушения фундаментальных прав человека. Принцип пропорциональности (необходимость и соразмерность ограничения прав) должен стать краеугольным камнем правового регулирования.

Наконец, существует риск алгоритмической предвзятости (algorithmic bias). Проблема заключается в том, что данные, на которых обучаются системы искусственного интеллекта, могут отражать существующие в обществе предубеждения. Это может привести к тому, что ИИ будет принимать дискриминационные решения. Яркий пример – когда усиленное патрулирование в районах с определенным этническим составом происходит не из-за реального роста преступности, а из-за того, что в данных присутствуют статистические искажения, которые модель интерпретирует как сигнал к действию. Такое явление происходит, когда модель машинного обучения систематически выдает предвзятые результаты, касающиеся, например, определенных демографических групп или типичных ситуаций.

Важно также учитывать этические аспекты и то, как это повлияет на профессиональные навыки. Внедрение ИИ в криминалистику ставит перед нами не только юридические, но и глубокие моральные вопросы. Особую сложность представляет определение того, кто несет ответственность за ошибки, совершенные на основе рекомендаций ИИ. Если следователь, следуя указаниям алгоритма, нарушает права человека, возникает вопрос: кто должен отвечать – создатель программы, сотрудник, который ею воспользовался, или руководитель, который разрешил ее применение? Действующее законодательство пока не дает четкого ответа.

Кроме того, меняется сама профессиональная культура следователя. Современный сотрудник правоохранительных органов должен обладать компетенциями, выходящими далеко за рамки традиционного юридического образования. Необходим синтез юридических знаний и понимания основ информационных технологий, принципов работы нейросетей и методов анализа данных.

Система подготовки кадров стоит перед необходимостью кардинального обновления. Требуется внедрение междисциплинарных образовательных программ, формирующих специалистов «цифрового профиля», способных не только нажимать кнопки в программном обеспечении, но и критически оценивать качество исходных данных и корректность работы алгоритмов. Необходимо изменение образовательных стандартов для юристов и следователей, включение в программу обучения дисциплин по цифровой грамотности, кибербезопасности и работе с аналитическими системами на базе ИИ. Речь идет о воспитании «цифрового юриста», который понимает как догму права, так и математическую статистику.

Кроме вышеперечисленного, необходима разработка этического кодекса использования ИИ в правоохранительной деятельности, который закрепит принцип, что окончательное решение о мере пресечения, квалификации деяния и виновности остается прерогативой человека (следователя, прокурора, судьи).

Проведенный анализ позволяет утверждать, что цифровизация и внедрение искусственного интеллекта знаменуют собой начало нового этапа в развитии криминалистики. Трансформация методики расследования преступлений носит системный характер, затрагивая все элементы

криминалистической науки: от ее теоретических основ (учение о следах, криминалистическая характеристика) до прикладных аспектов (тактика отдельных действий, методика расследования конкретных видов преступлений).

Ключевыми векторами этой трансформации на сегодняшний день выступают:

– смена объекта познания - расширение понятия следа, признание цифровых и гибридных следов полноценными источниками информации;
– автоматизация процессов, т.е. переход от ручной обработки информации к человеко-машинным процедурам сбора и анализа больших объемов данных;
– инициирование действий, предвидение проблем и возможностей, а также дополнение реактивной модели элементами прогнозирования и раннего выявления угроз;
– технологизация доказывания — необходимость процессуального осмысления результатов работы «черных ящиков» и обеспечения их проверяемости.

Успешность дальнейшего развития криминалистики в цифровую эпоху будет зависеть от решения триединой задачи: совершенствования правовой базы (обеспечение баланса между эффективностью и правами человека), разработки стандартизированных и валидированных технологических решений, а также подготовки нового поколения юридических кадров, в том числе и в следственных подразделениях правоохранительных органов, владеющих компетенциями на стыке права и высоких технологий. Только в этом случае технологии искусственного интеллекта станут надежным союзником правосудия, а не источником неконтролируемых рисков.

Список литературы:

[1] Абаканова В.А. Современное развитие криминалистики: цифровое измерение // Вестник МГПУ. Серия: Юридические науки. - 2025. № 3 (59). С. 40-51.

[2] Байчорова А.Т. Современные технологии в криминалистике: цифровая криминалистика и искусственный интеллект в расследованиях // Молодой ученый. - 2025. № 14 (565). С. 247-248.

[3] Бастрыкин А.И. Цифровые технологии современной криминалистики // Вестник московской академии Следственного комитета Российской Федерации. - 2021. № 2 (28). С. 11-17.

[4] Бастрыкин А.И. О цифровых технологиях в работе Следственного комитета РФ // https://www.gazeta.ru (15.01.2026).

[5] Жамова В.А. Интеграция цифровых технологий в традиционные криминалистические методы // Молодой ученый. - 2025. № 49 (600). С. 305-310.

[6] Калюжный А.Н. Векторы реализации потенциала информационных технологий в деятельности оперативных и следственных подразделений // Вестник Восточно-Сибирского института МВД России. - 2025. № 2 (113). С. 140-149.

[7] Число IT-преступлений в России в 2025 году сократилось до 675 тысяч (по данным Генпрокуратуры РФ) // https://tass.ru (09.02.2026).

References:

[1] Abakanova V.A. Modern development of forensic science: digital dimension//Bulletin of Moscow State Pedagogical University. Series: Legal Sciences. - 2025. № 3 (59). S. 40-51.

[2] Baichorova A.T. Modern technologies in forensics: digital forensics and artificial intelligence in investigations//Young scientist. - 2025. № 14 (565). S. 247-248.

[3] Bastrykin A.I. Digital technologies of modern forensics//Bulletin of the Moscow Academy of the Investigative Committee of the Russian Federation. - 2021. № 2 (28). S. 11-17.

[4] Bastrykin A.I. On digital technologies in the work of the Investigative Committee of the Russian Federation// https://www.gazeta.ru (15.01.2026).

[5] Zhamova V.A. Integration of digital technologies into traditional forensic methods//Young scientist. - 2025. № 49 (600). S. 305-310.

[6] Kalyuzhny A.N. Vectors for realizing the potential of information technologies in the activities of operational and investigative units//Bulletin of the East Siberian Institute of the Ministry of Internal Affairs of Russia. - 2025. № 2 (113). S. 140-149.

[7] The number of IT crimes in Russia in 2025 decreased to 675 thousand (according to the Prosecutor General's Office of the Russian Federation) // https://tass.ru (09.02.2026).