Научная статья
УДК 343.14
doi: 10.17223/15617793/516/25

Цифровая трансформация уголовно-процессуального доказывания: преимущества и риски

Татьяна Кимовна Рябинина[1], Дарья Олеговна Чистилина[2], Ярослава Петровна Ряполова[3]

[1, 2, 3] Юго-Западный государственный университет, Курск, Россия
[1] tatyanakimovna-r@yandex.ru
[2] darya-chistilina@yandex.ru
[3] yarosslava@mail.ru

Аннотация. Анализируются перспективные направления цифровой трансформации доказывания по уголовным делам. С учетом зарубежного опыта цифровизации доказательственной деятельности продемонстрированы различия и общность подходов в правовом регулировании стандартов «электронного доказывания» в национальных законодательствах стран – представительниц разных правовых систем. Отмечены положительное влияние введения электронного формата производства по уголовному делу на степень обеспеченности прав участников процесса, а также положительный эффект и прогнозируемые риски от использования систем искусственного интеллекта в практике доказывания в ходе расследования уголовных дел.
Ключевые слова: цифровизация, уголовно-процессуальное доказывание, цифровые технологии, правосудие, участники уголовного процесса, искусственный интеллект, риски

Источник финансирования: исследование выполнено за счет гранта Российского научного фонда № 25-28-01341, https://rscf.ru/project/25-28-01341/

Для цитирования: Рябинина Т.К., Чистилина Д.О., Ряполова Я.П. Цифровая трансформация уголовно-процессуального доказывания: преимущества и риски // Вестник Томского государственного университета. 2025. № 516. С. 223–236. doi: 10.17223/15617793/516/25

Original article
doi: 10.17223/15617793/516/25

Digital transformation of criminal procedure evidence: Advantages and risks

Tatyana K. Ryabinina[1], Darya O. Chistilina[2], Yaroslava P. Ryapolova[3]

[1, 2, 3] Southwest State University, Kursk, Russian Federation
[1] tatyanakimovna-r@yandex.ru
[2] darya-chistilina@yandex.ru
[3] yarosslava@mail.ru

Abstract. The primary objective of this research is to investigate the opportunities and risks associated with the implementation of digital technologies in the process of criminal procedural evidence. The gradual introduction of such technologies into criminal proceedings may positively impact the quality and speed of investigations, as well as the interaction between participants in criminal litigation. The authors employed a range of methods, including the dialectical, comparative legal, and systemic methods, analysis, synthesis, as well as specialized legal cognitive methods. The study involved an analysis of legislation from foreign countries where digital technologies are operational, alongside international provisions regulating this issue. Foreign experience with digitalization indicates a positive impact of this process on safeguarding the rights of participants in criminal proceedings and enhancing the efficiency of criminal procedural activities. For instance, in some countries, information technologies simplify communication between citizens and state authorities and accelerate the process of evidence collection and investigation. At the international level, the use of electronic evidence is regulated by establishing channels of interaction between countries to simplify the process of transferring electronic information. Many countries have developed an approach to defining the concept and essence of electronic evidence, as well as the requirements for it, which helps to resolve problematic aspects of its collection and storage in practice. The implementation of artificial intelligence systems also requires detailed legal regulation, since criminal procedural activity is governed not only by legal but also by ethical norms; this aspect prevents the complete replacement of a legal practitioner with an automated system. Artificial intelligence should serve as an auxiliary tool for working with large volumes of data. However, the introduction of digital technologies must account for the risks that legal practitioners may encounter. The outcome of this research will be a systematization of the risks faced by legislators and legal practitioners during the implementation of digital technologies, along with proposals for mitigating these negative trends based on an analysis of domestic and foreign criminal procedural practice. Imperfections in technology, the lack of preparedness among legal practitioners and citizens, and a lack of coordination between countries in the exchange of electronic information can all pose obstacles to the digital transformation of

criminal procedure. Overcoming these obstacles is possible through improving the technical equipment of investigative bodies and courts, raising the level of digital literacy among the population, developing a legislative framework that regulates issues of digitalization, and enhancing and adapting information technologies to meet the needs of criminal procedural activities.

Keywords: digitalization, criminal procedural evidence, information technology, justice, participants in criminal proceedings, artificial intelligence, risks of digitalization

Financial support: The study was supported by the Russian Science Foundation, Project No. 25-28-01341, https://rscf.ru/project/25-28-01341/

***For citation*:** Ryabinina, T.K., Chistilina, D.O. & Ryapolova, Ya.P. (2025) Digital transformation of criminal procedure evidence: Advantages and risks. *Vestnik Tomskogo gosudarstvennogo universiteta – Tomsk State University Journal*. 516. pp. 223–236. (In Russian). doi: 10.17223/15617793/516/25

Введение

Цифровизация является одним из основных направлений развития Российской Федерации. Указ Президента РФ от 07.05.2024 № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» [1] поставил четкие цели, заключающиеся в создании единых цифровых платформ, во внедрении систем искусственного интеллекта и цифровой трансформации большинства отраслей экономики, управления и социума в целом. Стратегия научно-технологического развития РФ, утвержденная Указом Президента РФ от 28.02.2024 № 1456 [2], призвана в условиях больших вызовов противодействовать современным угрозам, создать технологии и продукцию, отвечающие национальным интересам, обеспечить взаимосвязь образования, науки, технологического потенциала страны и взаимозависимость их развития. Положения стратегии распространяются на все сферы деятельности, в том числе на деятельность субъектов, осуществляющих уголовное преследование либо правосудие.

В рамках реализации обозначенных задач созданы системы и аппаратные комплексы по дистанционному взаимодействию граждан и госструктур (электронные обращения, электронная запись на прием и др.), введены электронные медицинские карты, созданы цифровые платформы для бизнеса («Мой Бизнес», «1С:Предприятие» и др.), широко используются системы блокчейн и т.д.

Сфера правоохранительной и судебной деятельности также стремится не отставать: успешно функционируют система автоматизированного учета статистических карточек и электронные алфавитные указатели, облегчающие поиск судебных решений в ГАС «Правосудие»; модуль АМИРС22, предназначенный для автоматизации процессов судебного делопроизводства и информационного сопровождения всех стадий судебного рассмотрения уголовного дела; система видеоконференц-связи (отечественные разработчики ВКС-решений Труконф, Винтео и др.); средства аудио- и видеофиксации; средства оповещения участников уголовного процесса; интегратор судебных решений судов (sudact.ru) и др. [3. С. 142].

Более интенсивные темпы внедрения IT-технологий в правоохранительную деятельность во многом могли бы облегчить работу правоприменителя, в то же время прогнозируемые риски, обусловленные опережающим воздействием цифровых технологий на уголовный процесс, становятся ощутимыми препятствиями на пути их внедрения. Как бы то ни было, уголовная юстиция в России является сферой, где цифровые новинки не так легко приживаются ввиду консервативности соответствующей отрасли права, непоколебимости и высокой степени защищенности на законодательном уровне процессуальных гарантий обеспечения прав личности, резкого усиления формальной определенности ключевых понятий уголовно-процессуального доказывания, ментальных, психологических и прочих особенностей российского населения, а также влияния нравственных начал на уголовно-процессуальную деятельность.

Уголовно-процессуальное доказывание – регулируемая законом деятельность, состоящая в собирании, проверке и оценке доказательств в целях установления обстоятельств, подлежащих доказыванию по делу [4. С. 321]. Именно посредством доказывания удается установить достоверные сведения относительно обстоятельств произошедшего и постановить законный, обоснованный и справедливый приговор, при этом одной из важных процессуальных гарантий выступает уголовно-процессуальная форма, ее сущность раскрывается в том числе в строго установленной законом процедуре формирования процессуальных доказательств. Однако установившаяся на рубеже веков высокая формализация стандартов доказывания нивелирует большую часть процессуальных гарантий скорого и справедливого правосудия, а также прав и свобод личности, ибо не позволяет решать стоящие перед уголовным процессом задачи с содержательных сторон, вынуждая органы и должностных лиц фокусировать внимание на выполнении массы формальных предписаний закона. В этом контексте наблюдаемый процесс цифровизации доказательственной деятельности, под которым следует понимать ее оптимизацию посредством внедрения цифровых технологий на этапах выявления, сбора и фиксации доказательств, несмотря на незавершенный и фрагментарный характер, призван отчасти снять остроту обозначенной проблемы, положительный отклик получают те немногие «цифровые новеллы» УПК РФ, которые были приняты в последнее время, в позитивном ключе отмечаются преобразования по части автоматизации делопроизводства, сокращение времени и ресурсов в ходе осуществления отдельных следственных действий в дистанционном формате [5. С. 159–160], регламентация правил изъятия электронных носителей информации и

т.д. [6. С. 195]. В то же время сохраняются трудности методологического, правового и практического плана, которые могут сопровождать использование электронных документов в доказывании, обусловленные требованиями уголовно-процессуальной формы [7. С. 31].

Цифровая трансформация – фаза, которая традиционно следует за цифровизацией любого рода деятельности. Применительно к уголовно-процессуальному доказыванию она представляет собой более глубокую и комплексную правовую реорганизацию компонентов доказывания в условиях развития цифровых технологий. Целью настоящей работы стало исследование отдельных направлений такой трансформации, а равно обобщение прогнозируемых преимуществ и существующих рисков, с ней связанных: закрепление стандартов «электронного доказывания», переход уголовного дела в электронный формат и внедрение систем искусственного интеллекта в доказательственную деятельность. Актуализирует данные вопросы возможность изучения зарубежного опыта регламентации основных подходов к оценке цифровых доказательств: подход континентальной правовой семьи, известный принципом свободы оценки доказательств, и подход семьи общего права, известный стремлением к формализации оценки доказательств [8. С. 906–915].

Правовое регулирование электронных доказательств в России и за рубежом

«Электронное доказывание» сейчас находится в стадии осмысления и теоретического обоснования, притом что проблематика работ, вызывающих острые дискуссии среди практиков и ученых-процессуалистов, демонстрирует первостепенное значение определения статуса электронных доказательств (к ним относят электронные сообщения и документы, цифровые аудио- и видеозаписи, фотоизображения, сообщения в мессенджерах, информацию из различных интернет-порталов и др.) [9. С. 75].

Современное уголовно-процессуальное законодательство не дает четкого определения электронным доказательствам, поэтому правоприменителю приходится вписывать их в уже существующую систему доказательств, что не позволяет в полной мере учитывать их особенности, связанные с изъятием, хранением проверкой и оценкой подобных доказательств. Специфику доказательств рассматриваемого вида определяет то обстоятельство, что электронную информацию можно уничтожить путем проведения нескольких манипуляций на компьютере, в том числе удаленно, поэтому важно своевременно и оперативно зафиксировать ее и защитить от ликвидации иными лицами [10. С. 110–112]. Ключевым признаком электронного документа А.С. Пастухов, А.А. Дмитриева называют способность человека его воспринимать с использованием электронных вычислительных машин [11. С. 274], возможность его свободной передачи по информационно-телекоммуникационным каналам связи, копирования, размещения и обработки в информационных системах.

Отсутствие официальной дефиниции в действующем уголовно-процессуальном законодательстве как самого понятия электронных доказательств, так и смежных, связанных с ним понятий, приводит в тому, что к ним применяются общие требования, предъявляемые к доказательствам, что зачастую не соответствует определению их сущности, форме фиксации, способам передачи, хранения, обработки и воспроизведения электронной информации. В вопросах целесообразности дополнения перечня доказательств в тексте УПК РФ новым видом доказательств нет единства мнений и консолидированной позиции среди ученых. Отмеченное демонстрирует противоречие между «традиционной консервативной следственной моделью и более современными, а поэтому эффективными методами работы с доказательственной информацией» [11. С. 276], очевидно, что при нерегулируемом применении существующих и вновь появляющихся информационных технологий и систем повышается риск нарушения прав и свобод личности [12. С. 125], что нельзя расценивать как положительное явление.

К.В. Обидин основную проблему видит в том, что российский законодатель в основном концентрируется не на поиске оптимальных путей регулирования использования электронной информации и определении ее как самостоятельного объекта познания, а на физических хранилищах информации (электронных носителях) [13. С. 231–236], что не менее важно, однако не имеет смысла без решения первой части вопроса.

Во многих странах вопросы использования электронных доказательств регламентированы на уровне законодательных положений либо предопределены судебно-прецедентной практикой. Для восприятия зарубежного опыта правовой регламентации использования электронных доказательств рассмотрим некоторые примеры подобного регулирования.

В США рассматриваемое судопроизводственное явление возникло раньше и сопровождается динамичным развитием прецедентного права и доктрины. Американскими исследователями цифровые доказательства определяются как информация, хранимая или передаваемая в двоичной форме, которую сторона уголовного процесса может использовать в качестве доказательств в судебном разбирательстве [14]. Федеральные правила доказывания [15] в Правиле 101 (6) содержат указание, что ссылка на любой вид письменного материала или любого другого носителя включает информацию, хранящуюся в электронном виде; правило 1001 (d), разграничивающее доказательственную ценность копии и оригинала применительно к электронным данным, определяет, что для информации, хранящейся в электронном виде, «оригинал» означает любую распечатку или другой вывод, читаемый визуально, если он точно отражает информацию. Однако в остальном Правила доказывания применяются к электронным доказательствам аналогично традиционным документам без каких-либо специальных уточнений. Американские законодатели не стали выделять «электронные» доказательства из числа обычных, но все же отметили их специфику [16. С. 185].

Суд сам определяет, являются ли доказательства относимыми и подлинными, не являются ли они «слухами» (hearing) и достаточно ли будет копии электронного документа либо потребуется оригинал,

ввиду следования прецедентному праву в практических примерах американской судебной практики отражены различные трактовки надежности цифровых доказательств исходя из их аутентификации, «правил наилучших доказательств» и т.д. [17. С. 281].

При этом действует единый подход, закрепляющий необходимость получения судебного решения (ордера) для получения информации, содержащейся в цифровом устройстве, когда эта информация представляет интерес и имеет значение для уголовного дела, т.е. является источником цифровой информации либо средством совершения преступления. Критерий аутентичности в сборе цифровых доказательств заключается в том, чтобы гарантировать, что доказательства на цифровых объектах, собранные на месте преступления, являются точными доказательствами и исходят из правильного источника после сохранения [18. P. 1–8].

Более предметно алгоритм использования цифровых доказательств по уголовному делу отражен в Руководстве по поиску и собиранию электронных доказательств, указания имеют рекомендательный характер для правоприменителей [19]. В этом документе обобщены подходы судейского корпуса к доктрине «разумного ожидания конфиденциальности» в делах, связанных с компьютерной информацией, перечислены исключения из требования получения ордера в делах, связанных с изъятием электронной информации, сформулированы рекомендации по производству «компьютерного обыска», раскрыты условия, когда необходимо получить несколько ордеров для сетевого обыска и т.д. В Правиле 41 Федеральных правил уголовного судопроизводства США [15] отмечено, что ордер предусматривает изъятие электронных носителей информации либо изъятие или копирование информации, хранящейся в электронном виде. Ордер санкционирует более поздний просмотр носителя или содержащейся в нем информации, тем самым копирование или изъятие информации (без физического истребования ее носителя) представляет собой самостоятельные следственные действия в американском уголовном процессе.

Два громких дела иллюстрируют как ценность и правдоподобность представления цифровых доказательств, так и ограниченный вес (weight) этих доказательств (оценка этого свойства доказательства относится к исключительной прерогативе коллегии присяжных) в отсутствие ясности и достоверности методов компьютерной судебной экспертизы, примененных для их получения.

Показательным примером стал случай, когда электронная информация имела решающее значение при установлении обстоятельств совершения преступления. Так, по делу об убийстве в 2014 г. своего малолетнего сына Купера и жестоком обращении с детьми Джастином Россом Харрисом судебная экспертиза его компьютера, мобильного устройства, флеш-накопителя, внешнего жесткого диска, SD-карты и DVD-диска обвиняемого помогла выявить, чем он занимался в то время, когда на семь часов оставил своего сына одного в раскаленном автомобиле с закрытыми окнами. Выяснилось, что в момент гибели сына он вел переписку с несколькими женщинами, кроме этого, с помощью извлеченных доказательств удалось уличить его в сексуальной связи с несовершеннолетней. Впоследствии, спустя девять лет после смерти Купера, в 2023 г., вследствие череды пересмотров вынесенного обвинительного приговора Верховный суд Джорджии прекратил преследование Харриса ввиду отсутствия мотива преднамеренности убийства, поддержав версию защиты о том, что отец забыл про оставленного ребенка в машине, вместе с тем Харрис до сих пор остается осужденным на двенадцатилетний срок по другим обвинениям, связанным с его сексуальной деятельностью, включая преступную попытку сексуальной эксплуатации детей и распространение запрещенных порнографических материалов среди несовершеннолетних [20].

По другому делу большое жюри округа Орандж, штат Флорида, предъявило Кейси Энтони обвинение в убийстве его дочери Кейли. Эксперт, проводя экспертизу данных, содержащихся на компьютере, дал показания в пользу обвинения, заявив, что кто-то просматривал слова «хлороформ» в общей сложности 84 раза на компьютере, изъятом из дома обвиняемого, что свидетельствовало о его преднамеренности, при этом у присяжных возникли сомнения в надежности таких выводов вследствие того, что временные метки, которые указывают, когда был сделан конкретный поиск, не согласовывались с используемыми экспертом инструментами поиска по ключевым словам. Энтони была признана невиновной из-за недопустимости представленных цифровых доказательств [21].

На территории Великобритании Управлением полиции принято Руководство по передовой практике в области цифровых доказательств (ACPO) [22], которое является комплексным актом, содержащим нормы и правила извлечения информации с электронных носителей, данные рекомендации предназначены для использования в работе правоохранительными органами. Руководство закрепляет четыре принципа, которые могут быть восприняты если не законодателем, то ведомственными структурами, а именно: недопустимость изменения электронных данных, которые впоследствии могут быть использованы в суде; компетентность и ответственность лица, имеющего доступ к исходным данным, проверяемость всех манипуляций с электронной информацией, поступившей в распоряжение органа расследования (создание и сохранение контрольных записей всех процессов, применяемых к цифровым доказательствам), независимая третья сторона должна иметь возможность изучить эти процессы и достичь того же результата; лицо, ответственное за расследование, несет общую ответственность за обеспечение соблюдения закона и вышеуказанных принципов.

Законодательство стран Германии и Франции отличает своеобразное единство нормативных подходов в использовании цифровых технологий при сборе доказательств, при этом легального определения понятия электронных доказательств, а также принципов работы с ними в законах не содержится.

Особенностью института доказывания во Франции является его четкая направленность на научно-техническую сторону, в УПК Франции достаточно подробно

урегулированы вопросы перехвата корреспонденции, отправленной посредством электронных средств связи, использование программного обеспечения, условия анализа, обработки, хранения и передачи персональных данных, а также использования технологии обработки больших данных, порядок получения данных геолокации, целые главы посвящены использованию национальной платформы судебных перехватов (или прослушиваний) (глава 6, ст. 230-45 УПК Франции), съемке и фиксации и использованию в расследовании изображений, полученных в общественных местах с помощью воздушных средств (глава 8, ст. 230-47–230-53 УПК Франции) [23]. Ст. 706-96 УПК Франции разрешает следователю использовать технические средства получения цифровой информации, размещаемой, хранящейся и передаваемой посредством телекоммуникационных сетей. При этом такие средства могут работать не только посредством удаленного доступа, но и внедряться на компьютеры или иные цифровые устройства подозреваемых лиц без их согласия.

Отличительной особенностью УПК Франции является обширный перечень гарантий прав и свобод личности при применении цифровых технологий в ходе судебного расследования: прокурорский и судебный надзор; практика обжалования гражданами своих прав в связи с применением специальных средств и обязанность должностных лиц принять соответствующие меры с информированием заявителей в установленный срок; ограничительный перечень сотрудников правоохранительных органов, имеющих право применять специальные средства; запрет использования специальных средств в административных или иных целях; установление сроков хранения информации, полученной в ходе применения специальных средств; установление запретов на хранение информации о частной жизни, если это не связано с целями применения специальных средств; указание на этические стандарты применения специальных средств и т.д. [24. С. 71]. В качестве доказательств по уголовному делу может использоваться не только оригинал цифровой информации, изъятый вместе с его носителем, но и копия такой информации (ст. 56, 97 УПК Франции).

В немецком законодательстве строго регламентированы правила обнаружения и фиксации электронной информации (поиск с помощью сети, наблюдение за телекоммуникациями, онлайн-поиск, сбор данных об использовании цифровых услуг и т.д.) [25], при этом, как отмечают немецкие процессуалисты, оценка цифровых доказательств, исследуемых в порядке строгого доказывания, является свободной, т.е. не привязанной к формальным правилам оценки [26. С. 13]. Согласно §249 УПК ФРГ суду разрешается зачитывать электронные документы без их распечатки на традиционных бумажных носителях: причем вне зависимости от того, был ли документ первоначально создан в цифровой форме или представляет собой электронную копию бумажного документа. Уголовно-процессуальное законодательство ФРГ содержит положения относительно защиты данных в ходе расследования уголовного дела, применимых к электронным доказательствам, подробно регламентируются правила об обязательном уничтожении электронных данных, не относящихся к делу (§ 101 УПК ФРГ). § 110 УПК ФРГ был дополнен ч. 3, предусматривающей возможность получения цифровых доказательств посредством удаленного доступа к электронным носителям как составной части обыска компьютерных устройств. Тем не менее посредством удаленного доступа следствие не может получить информацию с тех устройств, которые находятся за пределами Германии, в связи с отсутствием у них юрисдикционных полномочий действовать на территории иностранных государств.

Согласно закону о доказательствах Индии 1872 г., раздел 65B действующей редакции данного нормативного акта закрепляет следующие условия, которым должны соответствовать электронные доказательства:

1) электронная запись должна быть создана с помощью компьютера, который регулярно использовался для хранения или обработки информации в целях любой регулярно осуществляемой деятельности лицом, имеющим контроль над использованием компьютера на основании закона;

2) информация, содержащаяся в электронной записи, регулярно вводилась в компьютер в ходе обычной деятельности;

3) компьютер работал должным образом;

4) копия должна быть воспроизведением оригинальной электронной записи [27].

Кроме того, допускается установление подлинности электронных доказательств путем допроса свидетеля, если невозможно предоставить сертификат подлинности, однако такие документы должны быть доступны для воспроизведения в оригинальном виде, сохраняя целостность формата без изменений. Информация, содержащаяся в электронной записи, считается оригинальным документом, даже если она напечатана на бумаге, сохранена, записана или скопирована на носитель, созданный компьютером, при условии соблюдения установленных требований [28. P. 55]. Таким образом, в Индии, которая имеет смешанную правовую систему, на законодательном уровне не только закреплено понятие электронных доказательств, но и определен алгоритм их использования при осуществлении доказывания.

Знаковым событием в китайской юрисдикции стали дополнения ст. 48 УПК КНР, в соответствии с которыми в 2012 г. перечень видов доказательств был расширен новым видом – «электронные данные», в 2016 г. Верховным Народным Судом КНР совместно с Верховной Народной прокуратурой КНР и Министерством общественной безопасности КНР были приняты положения по ряду вопросов, касающихся сбора, обработки, изучения и вынесения решения по электронным данным при рассмотрении уголовных дел. Точное значение электронных данных было определено как «данные, которые формируются в процессе расследования дела, хранятся, обрабатываются и передаются в цифровой форме и могут подтверждать факты по делу» [29]. В ст. 2 Положения «О решении некоторых вопросов, касающихся собирания, получения и анализа электронных данных по уголовным делам» [30] Китая приведена классификация электронных доказательств. К ним относятся:

веб-сайты, блоги (онлайн-дневники), микроблоги, страницы в социальных сетях, идентификаторы приложения (например, WeChat), форумы, онлайн-диски (онлайновые хранилища). Безусловно, наличие подобной классификации значительно облегчает процесс их изъятия и использования. Также обращается внимание, что достаточно четко должен быть определен их источник (лицо, от которого исходила данная информация; зарегистрированный пользователь на сайте и др.).

Развитие высокотехнологичной транснациональной преступности в киберпространстве, появление новых видов преступлений в сфере электронной торговли и цифровой экономики обусловили разработку межгосударственных мер, направленных на совершенствование правового режима использования электронных доказательств в уголовном судопроизводстве.

Интерполом принято руководство по обращению с электронными доказательствами, в котором указано, что при проведении обыска и выемки, их идентификации с помощью методов, гарантирующих их целостность, рекомендуется обращаться с ними так же, как и со всеми другими традиционными доказательствами. Особого внимание заслуживает их хранение и транспортировка с учетом того, что они могут быть подвержены негативному воздействию электромагнитных полей, вследствие чего данные, содержащиеся на электронных носителях информации, могут быть повреждены или безвозвратно утрачены [31].

В практике Международного уголовного суда электронные доказательства также достаточно давно используются при осуществлении правосудия: суд в качестве доказательств исследовал спутниковые снимки в деле о насильственной кампании правительства против повстанцев. Прокурор подробно ссылался на доклад Комиссии по расследованию, опирающийся на спутниковые снимки, предоставленные правозащитными организациями, которые использовали их для выявления разрушений и поджогов деревень, а также перемещения беженцев. В деле Аль-Махди прокурором также было представлено значительное количество доказательств из открытых источников, включая спутниковые снимки. Однако для установления достоверности подобных доказательств требуется, чтобы к ним прилагались метаданные, включая информацию о цепочке поставок в хронологическом порядке, личность источника, первоначального автора и получателя информации [32. P. 13–16]. Отмечается, что во всех странах следует установить единые правила для использования электронных доказательств, что должно привести к единообразию правоприменительной практики. Данный аспект важен ввиду того, что преступность, особенно киберпреступность, носит транснациональный характер, поэтому единые стандарты использования электронных доказательств могут помочь в обмене данными между странами.

Европейским агентством по сетевой и информационной безопасности (ENISA) в 2014 г. принято руководство для работы с электронными доказательствами, которое содержит рекомендации о том, как обращаться с доказательствами и собирать их. Положения данного документа определяют пять международно признанных практических принципов: целостность данных, контроль, поддержка специалистов, соответствующее обучение и законность.

Сбор электронных доказательств должен проходить в несколько этапов: подготовка, выезд на место, изъятие, осмотр, оценка и представление. Однако в Руководстве отсутствует информация, касающаяся обмена электронными доказательствами, нет указаний на регламент защиты данных и др. Кроме того, электронные доказательства должны отвечать правилам приемлемости – установлением того, что доказательства получены законным путем и являются подлинными, т.е. прошли проверку и аутентификацию. Обращается внимание и на то, что доказательства необходимо хранить безопасным способом для защиты от изменений. При сборе и обработке электронных доказательств целостность, подлинность и неизменность таких доказательств должны быть гарантированы на протяжении всей цепочки хранения – от изъятия до судебного разбирательства. Таким образом, цепочка хранения должна регистрироваться, а доступ к доказательствам должен быть ограничен лицами, уполномоченными обрабатывать доказательства [33].

Глобальной проблемой в фиксации электронных следов преступления является то, что провайдерами интернет-услуг зачастую являются частные компании, которые находятся в других странах, поэтому каждый раз для получения информации необходимо направлять запрос в другое государство и ждать его обработки. Причем запрос направляется в страну, где находится провайдер, через государственные органы, которые и передают его в частную компанию. Вся эта процедура занимает много времени, по истечении которого повышается риск того, что цифровые следы могут быть скорректированы либо вовсе удалены. И это при условии, что с соответствующим государством установлено соглашение о взаимной правовой помощи. В противном случае, эту информацию никак не удастся получить [34. P. 230–235].

На эту проблему внимание обращается и в Регламенте (ЕС) 2023/1543 о производстве и хранении электронных доказательств в уголовных процессах и об исполнении приговоров к лишению свободы, вынесенных в рамках уголовного процесса. В нем указано, что не существует гармонизированной структуры сотрудничества с поставщиками услуг, как следствие, государства-члены все больше полагаются на добровольные каналы прямого сотрудничества с поставщиками услуг, если таковые имеются, и применяют различные национальные инструменты, условия и процедуры. При этом отмечается, что применение Регламента не должно зависеть от фактического местонахождения учреждения поставщика услуг или объекта обработки или хранения данных. Кроме того, поставщики услуг должны обеспечить, чтобы назначенные ими учреждения или законные представители могли использовать децентрализованную IT-систему через соответствующую национальную IT-систему для получения сертификата Европейского постановления о предоставлении или сохранении данных (EPOC, EPOC-PR), отправки запрашиваемых данных в выдающий орган и любого

другого взаимодействия с выдающим органом и правоприменительным органом [35]. В Директиве (ЕС) 2023/1544, устанавливающей правила определения уполномоченных учреждений и назначения законных представителей для целей сбора электронных доказательств в уголовном судопроизводстве, отмечается, что сетевые услуги могут предоставляться из любой точки мира и не требуют физической инфраструктуры, помещений или персонала в стране, где предлагается соответствующая услуга, или на самом внутреннем рынке [36]. Поэтому система взаимодействия между странами по данному вопросу требует значительного упрощения.

Таким образом, регулирование электронного доказывания имеет неоднородную правовую основу в национальных законодательствах различных стран. Законодательные тренды указывают на потенциальную возможность цифровых доказательств выступать пригодным и надежным источником сведений об обстоятельствах, имеющих значение для уголовного дела. Если в одних государствах традиционные правила доказывания распространяются в полном объеме на цифровые доказательства, то в других эти вопросы регламентируются специальными правовыми нормами и институтами. При этом общность подходов законодателей и представителей юридической доктрины разных стран заключается в признании и необходимости учета неординарных свойств информации, содержащейся в электронном виде и могущей стать основой для формирования доказательства; необходимости соблюдения специальных требований по ее хранению, копированию, расшифровке и т.д. При этом подчеркивается неизменность гарантий прав личности при собирании конфиденциальных электронных данных в уголовном судопроизводстве, необходимость обеспечения требований их аутентификации, надежности, полноты и целостности в ходе оценки таких доказательств судом. Также можно сделать вывод о том, что имеющиеся различия в правилах оценки традиционных видов доказательств, существующие в правовых системах англо-американского и континентального права, также проявляются и в работе с разновидностью «диджитал» доказательств.

Электронный формат производства по уголовному делу

Упорядочивание работы с электронными доказательствами требует перехода на цифровой формат уголовного дела.

На страницах юридической печати давно и регулярно звучат призывы к переходу на систему электронных уголовных дел [37. С. 83–94], что позволило бы всем участникам уголовного процесса в более короткие сроки получать доступ к материалам уголовного дела, создавать, редактировать и подписывать бланки уголовно-процессуальных актов, не затрачивая на это чрезмерно много усилий и ресурсов. Очевидное преимущество состоит также в том, что внедрение электронного документооборота по уголовным делам способствует обеспечению транспарентности правосудия в целом, усилению мер контроля и надзора со стороны прокуратуры и суда. Субъекты ведомственного контроля могли бы в условиях перманентного мониторинга и режима реального времени проводить своевременную проверку законности и обоснованности действий и принимаемых решений, что в своей совокупности обусловливает в том числе усиление гарантий прав личности.

Во многих странах подобный переход уже осуществлен. В Казахстане предусмотрена возможность использования в качестве протоколов следственных и иных процессуальных действий, постановлений и приговоров электронных документов, удостоверенных электронной подписью. Более того, защитник также может использовать электронные средства фиксации при опросе лиц с их согласия. В 2018 г. в этой стране было впервые рассмотрено «электронное» уголовное дело [38. С. 75]. Бельгия запустила проект системы электронного правосудия «Phenix» одной из первых стран, еще в 2001 г., в результате доступ к цифровому профилю (с помощью электронного паспорта) и размещенных в ней электронных файлов получили участники судопроизводства: судьи, сотрудники полиции, адвокаты [39]. Согласно УПК ФРГ по каждому уголовному делу формируется электронное досье, в котором содержатся все материалы дела в оцифрованном виде. Защитник может получить электронные версии документов на свой специальный ящик, однако это не мешает ему произвести сверку полученных материалов с бумажными носителями в случае возникновения сомнений в их подлинности [40]. Примером успешного перехода к электронному уголовному делу является опыт Саудовской Аравии, где с 2008 г. все материалы хранятся в цифровом формате, что позволяет довольно быстро и без лишних формальностей за несколько дней завершить производство по ним. Практика судопроизводства в электронном формате распространена также в рамках судебных систем Австрии, Дания, Италии, Канады, Швеции, Южной Кореи и др. [41. С. 11].

Изложенное свидетельствует о том, что многие страны либо уже перешли на электронный формат ведения уголовного дела, либо делают большие шаги в этом направлении. Стоит отметить, что в России на теоретическом уровне имеются разработки и предложения о переходе на электронный формат хранения материалов уголовного дела. О.В. Качалова, Ю.А. Цветков выдвигают предложения о создании единого информационного портала, содержащего всю информацию по уголовному делу. Каждый участник судопроизводства будет иметь специальный доступ к материалам дела, с которыми он может знакомиться. Причем документы будут классифицироваться по группам (участникам, стадиям, должностным лицам) [42. С. 95–101]. Подобная система позволит ускорить процесс доступа к информации и обеспечить оперативный контроль законности со стороны прокуратуры и суда. Если добавить возможности использования искусственного интеллекта, то он будет анализировать загруженные материалы и давать подсказки следователю относительно полноты доказательств и корректности оформления процессуальных актов.

Переход в электронный формат будет способствовать большему обеспечению прав участников уголовного процесса, так как позволит оперативно получать доступ к материалам дела и будет содействовать улучшению коммуникации между представителями государственных органов и гражданами. Более того, это позволит без лишних задержек разрешать ходатайства и жалобы, что также усилит уголовно-процессуальные гарантии.

Однако в краткосрочной перспективе прогнозируемые изменения сопряжены с разрешением ряда трудностей, связанных с низкой степенью подготовленности как самих правоприменителей, так и граждан к полному переходу в цифровой формат. Внедрение возможностей ведения дела в электронном формате не означает полной замены бумажного документооборота, на первых порах сохранится необходимость изготовления документа в двух форматах, что обусловливает определенные сложности в случае необходимости подписании такого документа несколькими должностными лицами. К тому же оцифровка материалов дела на бумажных носителях будет занимать определенное время и требовать затраты ресурсов (каждый отдел должен быть оснащен достаточным количеством оргтехники и помощниками, которые будут оцифровывать данные). Закономерно требует решения вопрос о едином стандарте «цифровой зрелости» следственной деятельности в целостном информационном пространстве системы уголовной юстиции [43. С. 4].

Также необходимо будет решить вопросы информационной безопасности и контроля доступа к материалам уголовного дела, а также повышения квалификации сотрудников правоохранительных органов. Следователь должен знать IT-процесс, чтобы понимать, как размещать в сети электронные документы, обеспечить их сохранность и неизменность, оформить электронное поручение органу дознания для производства процессуальных действий, оформить и направить в суд ходатайство о производстве следственного действия или об избрании меры пресечения и т.д. [44. С. 82–88].

Сохраняются риски несанкционированного искажения, передачи или распространения электронных данных, а значит, нарушения конфиденциальности и тайны предварительного расследования, если вся информация по уголовному делу будет храниться в электронном формате и обрабатываться на недостаточно защищенных ресурсах. Новый формат ставит вызовы перед решением проблемы сохранности электронных данных при системном сбое, заражении вредоносной программой, хакерских атаках и т.д. Кратно усиливает риск утраты конфиденциальности и то обстоятельство, что специалисты сторонних организаций, обеспечивающие техническую поддержку и контроль работы систем и аппаратных комплексов, отвечающих за электронный документооборот, получают доступ к охраняемой законом информации.

С позиции соотношения частных и публичных начал актуализируется проблема «цифрового неравенства», когда для отдельных лиц все еще остаются недоступными для понимания или использования достижения электронных технологий.

Каждое вводимое законодателем технологическое решение не должно выступать каким-либо ограничением или препятствием для реализации заинтересованными субъектами своих законных интересов.

В условиях ведения электронного уголовного дела присутствует постоянная угроза конфликта при взаимодействии пользователей, заказчиков и разработчиков специализированного программного обеспечения, используемого для работы с электронными материалами уголовного дела, риск технической несовместимости новых интеграций и существующих программных продуктов; необходимость дополнительных расходов на обновление программного обеспечения ввиду изменения законодательства, «моральное» устаревание аппаратных комплексов и т.п.

Наконец, существует риск, что любая информация в электронном формате по уголовному делу будет ошибочно восприниматься как доказательство, поэтому может возникнуть опасность неправильной оценки материалов расследования.

Внедрение систем искусственного интеллекта в доказательственную деятельность по уголовным делам: преимущества и риски

Еще одним направлением интеграции цифровых технологий в доказательственную деятельность следует признать внедрение систем искусственного интеллекта (далее – ИИ). Одним из основных преимуществ данных систем является то, что за короткий срок они могут обработать значительный объем информации, что ввиду когнитивных ограничений недоступно простому человеку.

Американские исследователи выделяют пять основных областей правоприменения, на которые системы искусственного интеллекта окажут наибольшее влияние в ближайшем будущем: поиск информации по обстоятельствам дела; поиск прецедентов; составление документов; подготовка материалов дела; прогнозирование исхода дела [45. С. 1230–1250]. На основе выводных знаний ИИ можно сформировать и автоматизировать базы данных, что повысит информационно-аналитические возможности криминалистической регистрации, учетов органов внутренних дел, иных правоохранительных органов.

В некоторых странах уже используются системы на основе искусственного интеллекта, значительно облегчающие работу правоприменителям. Так, в США функционируют системы Judicata, BriefMine, LawDepot, которые могут структурировать судебные прецеденты, систематизировать и анализировать судебных иски, формировать пакет юридических документов и т.д. [45. С. 1230–1250]. В странах Латинской Америки также начали активно использовать генеративные модели в области правосудия и государственных услуг [46. С. 37].

Зарубежный опыт использования систем искусственного интеллекта позволяет констатировать его позитивное влияние на правоприменительную практику правоохранительных органов. Так, в Ханчжоу (Китай) с 2017 г. функционирует интернет-суд, в рамках которого взаимодействие между участниками судопроизводства происходит полностью дистанционно,

что значительно сокращает время, затрачиваемое на формальные моменты. Причем система сама подсказывает участникам, каких документов не хватает и какие ошибки были допущены при заполнении форм [47. С. 705–710]. В Японии на законодательном уровне установлены четкие правила в отношении защиты частной информации и определены границы применения систем искусственного интеллекта при расследовании уголовных дел. Законодательство Великобритании уделяет внимание практическим аспектам применения искусственного интеллекта в правоохранительной деятельности, в частности для анализа больших массивов данных и создания профилей преступников. Такой подход позволяет эффективно использовать потенциал искусственного интеллекта для оптимизации процессов расследования при сохранении надлежащих гарантий защиты прав личности [48. P. 818–824].

Подобные системы могут быть применены и в отечественном доказывании. Если с помощью специальных программ удастся выявить устойчивые, повторяющиеся связи между доказательствами, средствами доказывания, обстоятельствами, подлежащими доказыванию, и объектом доказывания, то можно выявить некоторые закономерности, которые в последующем станут основой для создания целых систем, оказывающих помощь следователю при расследовании. Безусловно, это потребует значительных усилий для проведения анализа большого массива эмпирических данных в виде судебно-следственной практики [49. С. 89–95], что по силам искусственному интеллекту.

Систему искусственного интеллекта следует рассматривать как вспомогательную технологию в следственной и судебной работе. Например, использование GPT-4 дает возможность одновременно обрабатывать текст и графические изображения. Возможности компьютерного моделирования могут помочь создать модель объекта в виде конечно-элементной схемы, что позволит не только увеличить наглядность представленных материалов дела, но и более четко представить обстоятельства произошедшего [50. С. 273–279].

В контексте использования технологии искусственного интеллекта в уголовно-процессуальном доказывании перспективным видится создание цифрового профиля лица, учение о котором разрабатывают О.А. Зайцев и П.С. Пастухов. Они предлагают фиксировать идентификационные признаки криминальных следов и вещественных доказательств, а также характеристик человека, чтобы в последующем использовать данную информацию для раскрытия не только конкретного уголовного дела, по которому она была изъята, но и всех других преступлений, связанных с подозреваемым (обвиняемым). Причем предлагается систематизировать сведения, полученные из различных источников. Данная информация поможет раскрыть конкретное преступление, а также идентифицировать неизвестное лицо по другому делу. Цифровой профиль авторы определяют как совокупность сведений о физическом лице, включает четыре групп идентификаторов: анкетных персональных данных; регистрационных данных субъектов и объектов в информационной инфраструктуре и системе цифровых правоотношений; биометрических персональных данных в цифровой инфраструктуре; цифровых идентификаторов оконечного оборудования, информационных систем и компьютерных сетей [51. С. 294]. Важность выявления индивидуальных психологических качеств личности, осуществляющей преступную деятельность в сфере информационных технологий, отмечена в исследовании Д.В. Алымова, К.Г. Балашова, А.Ю. Дериглазовой. С помощью детализации признаков подобной преступной деятельности повышается шанс нейтрализации механизмов, посредством которых она осуществляется [52. С. 190–192].

Актуальной задачей для субъектов законодательной инициативы является разработка вопроса о закреплении дополнительных прав и обязанностей у субъектов уголовного судопроизводства ввиду внедрения информационных технологий в уголовный процесс. А.Н. Першин, в частности, полагает, что следователь должен получить такое «цифровое право», как возможность осуществления поиска, изучения, фиксации криминалистически значимой информации в информационно-телекоммуникационных системах, а также подтверждать правомерность ее получения и использования в качестве доказательств. При этом для реализации данного права должны быть созданы соответствующие базы данных, к которым у него должен быть доступ [53. С. 108–115].

На данном этапе в условиях законодательной неопределенности использование подобных систем может приводить к нарушению прав граждан, так как отсутствует четкий алгоритм работы с системами ИИ, отсюда неопределенность на практике и разный уровень гарантий прав, фактически зависящий от усмотрения правоприменителя.

Несмотря на то, что технологии искусственного интеллекта включают в себя множество программ и систем, каждая из которых отличается по составу и сложности, разнообразием методов и моделей, к общим, применимым ко всем системам ИИ рискам следует отнести следующие:

1) искусственный интеллект функционирует на основе данных, сформированных до этого в большинстве случаев человеком, который не свободен от различного рода предубеждений и субъективизма, в связи с чем даже самая совершенная система будет подвержена влиянию человека и его взглядов, кроме того, обрабатываемые данные могут содержать эпизоды судебных и следственных ошибок, которые при их систематическом проявлении будут имитироваться и воспроизводиться программой (эффект «усиления» человеческой ошибки);

2) несовершенства алгоритма машинного обучения и введенных в систему критериев, что влечет ошибки в отраженном результате и ведет к несправедливому решению. Так, американская система COMPAS, в задачи которой входит прогнозирование рисков повторного совершения преступлений лицами, претендующими на освобождение под залог или условно-досрочное освобождение, функционирует с рядом недостат-

ков. В ней прослеживается некоторая предубежденность относительно расовой и половой принадлежности обвиняемых. Фактически в системе нашли отражение установки писавших ее лиц [54. С. 65–68];

3) сложность определения субъекта ответственности в ходе поддержки принятия решений с использованием ИИ, в том числе в случаях обнаружения ошибок и нарушений в его работе, в настоящее время отсутствуют предпосылки для наделения искусственного интеллекта «субъектностью в процессе доказывания» [55. С. 481];

4) несовершенство систем искусственного интеллекта, которые не могут распознать и учесть некоторые нравственные понятия. Так, нельзя заложить в систему возможность оценки таких нравственных понятий, как «примерный семьянин», «чувство долга», «добропорядочность», «честность» и др., не используя при этом различную степень глубины данных категорий [56. С. 81–90];

5) ограниченные возможности для проверки и оспаривания решения, вынесенного с помощью искусственного интеллекта, ввиду непрозрачности и сложности для понимания используемых алгоритмов или их закрытости со стороны разработчиков (эффект «черного ящика»), современные ИИ-модели способны скрывать собственные алгоритмы, источник своей логики;

6) неумелое обращение правоприменителя и иных участников уголовного процесса с подобными системами (неточное формирование промптов, излишнее доверие, неприятие, саботирование, злоупотребления, когда вектор доказывания и вся доказательственная база строится в фарватере результатов запроса ИИ; ярким примером этого является нашумевшее уголовное дело в отношении ученого-гидролога Александра Цветкова, который был задержан по делу об убийствах 20-летней давности: система распознавания лиц, установленная в аэропорту, определила сходство изображения ученого на 55% с ранее составленным фотороботом предполагаемого убийцы) [12. С. 152–153];

7) юридические галлюцинации («непреднамеренные искажения»): при подготовке проектов процессуальных документов ИИ-системы генерируют ответы на основе статистических закономерностей, полученных из больших наборов данных, а не путем проверки фактов в этих наборах, иными словами, создают несуществующие факты, отличающиеся своей убедительностью. Много таких негативных примеров демонстрирует судебная практика стран прецедентного права;

8) негативные свойства авторегрессивности ИИ-моделей (алгоритма оценки значений ряда по прошлым значениям этого же ряда), когда языковая модель принятого решения по поставленному запросу опирается на наиболее часто упоминаемые в прошлом языковые цепочки, их совпадение и распределение, система не учитывает изменения обстановки, формирующейся региональной практики и новейшие разъяснения высшей судебной инстанции и прочее.

Как мы видим, многие страны уже перешли на уровень законодательного регулирования проблемных аспектов, возникающих при функционировании систем искусственного интеллекта, тогда как в России только обсуждается вопрос их внедрения. В связи с этим необходимо проанализировать и понять, где искусственный интеллект может реально помочь, чтобы осуществлять постепенное его внедрение в российскую уголовно-процессуальную систему. Для этого необходимо разработать эффективную правовую базу, обеспечить доступ к современным инструментам расследования и методам, организовать обучение правоприменителей и гарантировать технические возможности, сбалансировать соотношение участия человека и систем ИИ в ходе рассмотрения и разрешения уголовных дел без ущерба принципам уголовно-процессуальной деятельности.

Выводы

Таким образом, в результате обобщения и анализа опыта зарубежных стран относительно использования цифровых технологий в доказательственной деятельности по уголовным делам продемонстрированы различия и общность подходов в правовом регулировании стандартов электронного доказывания в национальных законодательствах стран – представительниц различных правовых систем, проанализированы прогрессивные нормативные подходы в регламентации правил работы с электронными доказательствами, которые в последующем могут быть учтены российским законодателем, также показана и обратная сторона процесса интеграции цифровых технологий в компоненты доказывания, что может значительно повлиять на степень гарантированности прав участников процесса и в целом на достижение назначения уголовного судопроизводства.

Россия находится только на первоначальном этапе цифровизации доказательственной деятельности, в силу чего ей предстоит взвешенно подходить к передовой практике использования электронной информации в качестве доказательственной, прогнозировать риски функционирования информационных технологий и систем в ходе доказывания с учетом существующей правовой системы и факторов неправового характера – технических возможностей и «цифровой зрелости» различных правоохранительных органов, степени подготовленности граждан и т.д. Данный процесс потребует много времени, в связи с чем поэтапная цифровая трансформация уголовно-процессуального доказывания будет являться наилучшим выходом в данной ситуации.

Список источников

1. Указ Президента РФ от 07.05.2024 № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» // Президент России. URL: http://www.kremlin.ru/acts/bank/50542 (дата обращения: 02.04.2025).
2. Указ Президента РФ от 28.02.2024 № 145 «О Стратегии научно-технологического развития Российской Федерации» // Президент России. URL: http://www.kremlin.ru/acts/bank/50358 (дата обращения: 02.04.2025).

3. Миронова Е.Ю. Нравственные начала уголовного процесса в условиях цифровизации: принципиальная незыблемость или неизбежная трансформация // Актуальные проблемы российского права. 2023. № 1 (146). С. 136–149.
4. Лупинская П.А. Уголовно-процессуальное право Российской Федерации : учебник / отв. ред. П.А. Лупинская, Л.А. Воскобитова. 4-е изд., перераб. и доп. М. : Норма; ИНФРА-М, 2024. 1008 с.
5. Химичева О.В., Панфилов П.О. Изменение уголовно-процессуальной формы в условиях цифровизации: новые риски и возможности // Вестник Московского университета МВД России. 2024. № 1. С. 158–164.
6. Зуев С.В., Черкасов В.С. Новые правила изъятия электронных носителей и копирования информации (статья 164.1 УПК РФ): преимущества и недостатки новеллы // Сибирское юридическое обозрение. 2019. Т. 16, № 2. С. 193–197.
7. Гришина Е.П. К вопросу об использовании электронных доказательств в уголовном судопроизводстве // Администратор суда. 2020. № 3. С. 31–34.
8. Абдулкарим Ф.А., Семеновский А.И. Оценка цифровых доказательств в уголовном судопроизводстве: романо-германский и англосаксонский подходы // Журнал Сибирского федерального университета. Гуманитарные науки. 2025. Т. 18, № 5. С. 906–915.
9. Воронин М.И. Электронные доказательства в УПК: быть или не быть? // Lex russica. 2019. № 7 (152). С. 74–84.
10. Нечаев В.В., Прысь Е.В., Теренков И.Е. Организационно-правовые основы использования цифровых технологий в уголовно-процессуальном доказывании (вопросы теории и правоприменительной практики) // Криминологический журнал. 2023. № 4. С. 108–113.
11. Дмитриева А.А., Пастухов П.С. Концепция электронного доказательства в уголовном судопроизводстве // Journal of Digital Technologies and Law. 2023. № 1 (1). С. 270–295.
12. Чурикова А.Ю. Использование информационных технологий и систем в уголовном судопроизводстве: возможности, риски, правовое регулирование : дис. … д-ра юрид. наук. Саратов, 2024. 498 с.
13. Обидин К.В. О роли электронной информации в уголовном судопроизводстве в условиях цифровизации // Вестник Университета имени О.Е. Кутафина. 2020. № 10 (74). С. 231–236.
14. Novak M. Digital Evidence in Criminal Cases Before the U.S. Courts of Appeal: Trends and Issues for Consideration // Journal of Digital Forensics, Security and Law. 2020. Vol. 14, № 4. Article 3. doi: 10.15394/jdfsl.2019.1609
15. Federal Rules of Criminal Procedure on December 26, 1944 (As amended to December 1, 2024) // Cornell Law School. URL: https://www.law.cornell.edu/rules/fre (дата обращения: 23.06.2025).
16. Карташов И.И., Лесников О.А. Особенности получения и использования цифровой информации в уголовном судопроизводстве некоторых зарубежных стран // Вестник Воронежского института МВД России. 2020. № 4. С. 184–191.
17. Бирюков П.Н. О цифровых доказательствах в зарубежном уголовном процессе // Вестник Воронежского государственного университета. Серия: Право. 2022. № 1 (48). С. 275–286.
18. Yeboah-Ofori A., Brown A.D. Digital forensics investigation jurisprudence: issues of admissibility of digital evidence // Journal of Forensic, Legal & Investigative Sciences. 2020. № 6 (1). P. 1–8.
19. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. URL: https://www.justice.gov/d9/criminal-ccips/legacy/2015/01/14/ssmanual2009_002.pdf (дата обращения: 23.06.2025).
20. Prosecutors Won't Retry Father Whose Son Died in Hot Car // New York Times. URL: https://www.nytimes.com/2023/05/25/us/georgia-hot-car-child-death-charges-dropped.html (дата обращения: 02.04.2025).
21. Casey Anthony Trial: Did Cindy Anthony Really Search for Chloroform? // ABC News. URL: https://abcnews.go.com/US/casey_anthony_trial/casey-anthony-trial-cindy-anthony-search-chloroform/story?id=13981375 (дата обращения: 02.04.2025).
22. The Good Practice Guide for Computer Based Electronic Evidence [ACPO]. URL: https://www.7safe.com/docs/default-source/default-document-library/acpo_guidelines_comp uter_evidence_v4_web.pdf (дата обращения: 23.06.2025).
23. Code de procédure pénale (Dernière mise à jour des données de ce code: 15 juin 2025). URL: https://www.legifrance.gouv.fr (дата обращения: 23.06.2025).
24. Белоносов В.О. Доказательства и доказывание по УПК Франции // Юридический вестник Самарского университета. 2023. Т. 9, № 4. С. 62–73.
25. Strafprozeßordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 2 Absatz 1 des Gesetzes vom 7. November 2024 (BGBl. 2024 I Nr. 351) geändert worden ist. URL: https://www.gesetze-im-internet.de/stpo/BJNR006290950.html (дата обращения: 22.06.2025).
26. Доминик Б., Маттиас Я. Цифровые доказательства в немецком уголовном процессе на стадиях предварительного расследования, рассмотрения дела по существу и ревизии // Российское право: образование, практика, наука. 2020. № 3. С. 4–18.
27. Indian Evidence Act, 1872. IEA India, Act No. 1 OF 1872. URL: https://devgan.in/iea/ (дата обращения: 16.06.2025).
28. Popova E.I. Impact of Digital Technologies on Criminal Procedure in Russia and India: Comparative Legal Aspect // International Journal «Law in Changing World». 2023. Vol. 2, № 1. P. 52–65.
29. Provisions on Several Issues concerning the Collection, Taking, Examination, and Judgment of Electronic Data in the Handling of Criminal Cases (2016). URL: https://www.chinalawtranslate.com/en/provision-on-collection-and-review-of-digital-information-in-criminal-cases/ (дата обращения: 02.04.2025).
30. Rules of Obtainment of Electronic Data as Evidence by Public Security Authorities in Handling Criminal Cases (2019). URL: https://www.chinalawtranslate.com/en/Public-Security-Organs-for-Collecting-Electronic-Evidence-in-Criminal-Cases/ (дата обращения: 02.04.2025).
31. Guidelines for digital forensics first responder. Best practices for search and seizure of electronic and digital evidence. (2021). URL: https://www.interpol.int/content/download/16243/file/Guidelines to Digital Forensics First Responders_V7.pdf (дата обращения: 02.04.2025).
32. Collecting Electronic Evidence in Criminal Cases in Russia and Foreign Countries: Experiences and Problems: Monograph / editors S.P. Shcherba (Russian ed.) and P.A. Litvishko (English ed.). Moscow : Publishing House «Gorodets», 2024. 224 p.
33. ENISA. Electronic evidence – a basic guide for First Responders. URL https://syntheticdrugs.unodc.org/uploads/syntheticdrugs/res/library/cybercrime_html/Electronic_Evidence_A_Basic_Guide_for_First_Responders_ENISA.pdf (дата обращения: 02.04.2025).
34. Mifsud Bonnici J.P., Tudorica M., Cannataci J.A. The European Legal Framework on Electronic Evidence: Complex and in Need of Reform // Handling and Exchanging Electronic Evidence Across Europe. Law, Governance and Technology Series. 2018. Vol. 39. P. 189–235.
35. Regulation (EU) 2023/1543 on European Production and Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum:4682020 (дата обращения: 02.04.2025).
36. Directive (EU) 2023/1544 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum:4682020 (дата обращения: 02.04.2025).
37. Зуев С.В., Моругина Н.А. Электронное уголовное дело: теоретическая модель // Вестник Казанского юридического института МВД России. 2024. Т. 15, № 3 (57). С. 83–94.
38. Задорожная В.А. Производство по уголовному делу в электронном формате по законодательству Республики Казахстан // Правопорядок: история, теория, практика. 2018. № 4 (19). С. 71–75.
39. Bruno de Vuyst and Alea Fairchild. 2006. The Phenix project: a case study of e-justice in Belgium // Proceedings of the 8th international conference on Electronic commerce: The new e-commerce: innovations for conquering current barriers, obstacles and limitations to conducting successful business on the internet (ICEC '06). Association for Computing Machinery, New York, USA. P. 327–333.

40. German Criminal Code (Strafgesetzbuch – StGB) on 13 November 1998. URL: https://www.gesetze-im-internet.de/englisch_stgb/index.html (дата обращения: 16.06.2025).
41. Степанов О.А., Печегин Д.А., Дьяконова М.О. К вопросу о цифровизации судебной деятельности // Право. Журнал Высшей школы экономики. 2021. Т. 14, № 5. С. 4–22.
42. Качалова О.В., Цветков Ю.А. Электронное уголовное дело – инструмент модернизации уголовного судопроизводства // Российское правосудие. 2015. № 2. С. 95–101.
43. Валов С.В. Ресурсное обеспечение цифровой трансформации следственной деятельности // Российский следователь. 2023. № 3. С. 2–6.
44. Малышева О.А. Особенности доказывания, осуществляемого следователем, в условиях цифровизации уголовного судопроизводства // Вестник Университета имени О.Е. Кутафина. 2020. № 10 (74). С. 82–88.
45. МакГиннис Д.О., Пирс Р.Дж. Великий подрыв: как искусственный интеллект меняет роль юристов в оказании юридических услуг // Актуальные проблемы экономики и права. 2019. Т. 13, № 2. С. 1230–1250.
46. Виноградова Е.А. Технологии искусственного интеллекта и нарастающие киберугрозы в Латинской Америке // Латинская Америка. 2023. № 3. С. 34–48.
47. Чистилина Д.О. Использование возможностей искусственного интеллекта в уголовном процессе // Вестник Удмуртского университета. Серия: экономика и право. 2021. Т. 31, № 4. С. 705–710.
48. Byelov D., Bielova M., Rushchak I. Artificial Intelligence in Pre-Trial Investigation of Criminal Cases: Some Issues of International Practice // Analytical and Comparative Jurisprudence. 2025. № 1. P. 818–824.
49. Афанасьев А.Ю. Системы искусственного интеллекта в механизме уголовно-процессуального доказывания // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2020. № 1 (49). С. 89–95.
50. Рамалданов Х.Х. Влияние информационных технологий на процесс доказывания в уголовном судопроизводстве // Пробелы в российском законодательстве. 2023. № 7. С. 273–279.
51. Зайцев О.А., Пастухов П.С. Цифровой профиль лица как элемент информационно-технологической стратегии расследования преступлений // Вестник Пермского университета. Юридические науки. 2022. № 56. С. 281–308.
52. Алымов Д.В., Балашов К.Г., Дериглазова А.Ю. Криминалистическая характеристика типовых следов преступника, осуществляющего криминальную деятельность в виртуальном пространстве (на примере дроповодов) // Вестник Томского государственного университета. 2024. № 506. С. 185–192. doi: 10.17223/15617793/506/23
53. Першин А.Н. Цифровые права лиц, осуществляющих предварительное расследование // Вестник Университета имени О.Е. Кутафина. 2021. № 2 (78). С. 108–115.
54. Мичурина О.В. Искусственный интеллект против внутреннего убеждения: взгляд в будущее уголовного судопроизводства // Вестник Московского университета МВД России. 2020. № 3. С. 65–68.
55. Спиридонов М.С. Технологии искусственного интеллекта в уголовно-процессуальном доказывании // Journal of Digital Technologies and Law. 2023. Т. 1. № 2. С. 481–497.
56. Спесивов Н.В. От фантастических теорий к объективной реальности: есть ли будущее у искусственного интеллекта и предиктивных технологи при отправлении правосудия по уголовным делам? // Lex Russica. 2023. № 2 (195). С. 81–90.

References

1. President of the Russian Federation. (2024) *Decree No. 309 dated May 07, 2024 "On the National Development Goals of the Russian Federation for the Period until 2030 and for the Future until 2036"*. [Online] Available from: http://www.kremlin.ru/acts/bank/50542 (Accessed: 02.04.2025). (In Russian).
2. President of the Russian Federation. (2024) *Decree No. 145 dated February 28, 2024 "On the Strategy for Scientific and Technological Development of the Russian Federation"*. [Online] Available from: http://www.kremlin.ru/acts/bank/50358 (Accessed: 02.04.2025). (In Russian).
3. Mironova, E.Yu. (2023) Nravstvennye nachala ugolovnogo protsessa v usloviyakh tsifrovizatsii: printsipial'naya nezyblemost' ili neizbezhnaya transformatsiya [Moral Foundations of Criminal Procedure in the Context of Digitalization: Fundamental Immutability or Inevitable Transformation?]. *Aktual'nye problemy rossiyskogo prava*. 1 (146). pp. 136–149.
4. Lupinskaya, P.A. & Voskobitova, L.A. (eds) (2024) *Ugolovno-protsessual'noe pravo Rossiyskoy Federatsii: uchebnik* [Criminal Procedure Law of the Russian Federation: Textbook]. 4th ed. Moscow: Norma; INFRA-M.
5. Khimicheva, O.V. & Panfilov, P.O. (2024) Izmenenie ugolovno-protsessual'noy formy v usloviyakh tsifrovizatsii: novye riski i vozmozhnosti [Changes in the Criminal Procedure Form in the Context of Digitalization: New Risks and Opportunities]. *Vestnik Moskovskogo universiteta MVD Rossii*. 1. pp. 158–164.
6. Zuev, S.V. & Cherkasov, V.S. (2019) Novye pravila iz"yatiya elektronnykh nositeley i kopirovaniya informatsii (stat'ya 164.1 UPK RF): preimushchestva i nedostatki novelly [New Rules for the Seizure of Electronic Media and Copying of Information (Article 164.1 of the Code of Criminal Procedure of the Russian Federation): Advantages and Disadvantages of the Novelty]. *Sibirskoe yuridicheskoe obozrenie*. 16 (2). pp. 193–197.
7. Grishina, E.P. (2020) K voprosu ob ispol'zovanii elektronnykh dokazatel'stv v ugolovnom sudoproizvodstve [On the Use of Electronic Evidence in Criminal Proceedings]. *Administrator suda*. 3. pp. 31–34.
8. Abdulkari, F.A. & Semenovsky, A.I. (2025) Otsenka tsifrovykh dokazatel'stv v ugolovnom sudoproizvodstve: romano-germanskiy i anglosaksonskiy podkhody [Evaluation of Digital Evidence in Criminal Proceedings: Romano-Germanic and Anglo-Saxon Approaches]. *Zhurnal Sibirskogo federal'nogo universiteta. Gumanitarnye nauki*. 18 (5). pp. 906–915.
9. Voronin, M.I. (2019) Elektronnye dokazatel'stva v UPK: byt' ili ne byt'? [Electronic Evidence in the Code of Criminal Procedure: To Be or Not to Be?]. *Lex russica*. 7 (152). pp. 74–84.
10. Nechaev, V.V., Prys', E.V. & Terenkov, I.E. (2023) Organizatsionno-pravovye osnovy ispol'zovaniya tsifrovykh tekhnologiy v ugolovno-protsessual'nom dokazyvanii (voprosy teorii i pravoprimenitel'noy praktiki) [Organizational and Legal Foundations for the Use of Digital Technologies in Criminal Procedural Proof (Theoretical and Practical Issues)]. *Kriminologicheskiy zhurnal*. 4. pp. 108–113.
11. Dmitrieva, A.A. & Pastukhov, P.S. (2023) Kontseptsiya elektronnogo dokazatel'stva v ugolovnom sudoproizvodstve [The Concept of Electronic Evidence in Criminal Proceedings]. *Journal of Digital Technologies and Law*. 1 (1). pp. 270–295.
12. Churikova, A.Yu. (2024) *Ispol'zovanie informatsionnykh tekhnologiy i sistem v ugolovnom sudoproizvodstve: vozmozhnosti, riski, pravovoe regulirovanie* [The Use of Information Technologies and Systems in Criminal Proceedings: Opportunities, Risks, Legal Regulation]. Law Dr. Diss. Saratov.
13. Obidin, K.V. (2020) O roli elektronnoy informatsii v ugolovnom sudoproizvodstve v usloviyakh tsifrovizatsii [On the Role of Electronic Information in Criminal Proceedings in the Context of Digitalization]. *Vestnik Universiteta imeni O.E. Kutafina*. 10 (74). pp. 231–236.
14. Novak, M. (2020) Digital Evidence in Criminal Cases Before the U.S. Courts of Appeal: Trends and Issues for Consideration. *Journal of Digital Forensics, Security and Law*. 14 (4): 3. doi: 10.15394/jdfsl.2019.1609
15. Law.cornell.edu. (2024) *Federal Rules of Criminal Procedure on December 26, 1944 (As amended to December 1, 2024*). [Online] Available from: https://www.law.cornell.edu/rules/fre (Accessed: 23.06.2025).

16. Kartashov, I.I. & Lesnikov, O.A. (2020) Osobennosti polucheniya i ispol'zovaniya tsifrovoy informatsii v ugolovnom sudoproizvodstve nekotorykh zarubezhnykh stran [Peculiarities of Obtaining and Using Digital Information in Criminal Proceedings in Some Foreign Countries]. *Vestnik Voronezhskogo instituta MVD Rossii*. 4. pp. 184–191.
17. Biryukov, P.N. (2022) O tsifrovykh dokazatel'stvakh v zarubezhnom ugolovnom protsesse [On Digital Evidence in Foreign Criminal Procedure]. *Vestnik Voronezhskogo gosudarstvennogo universiteta. Seriya: Pravo*. 1 (48). pp. 275–286.
18. Yeboah-Ofori, A. & Brown, A.D. (2020) Digital forensics investigation jurisprudence: issues of admissibility of digital evidence. *Journal of Forensic, Legal & Investigative Sciences*. 6 (1). pp. 1–8.
19. Justice.gov. (2015) *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*. [Online] Available from: https://www.justice.gov/d9/criminal-ccips/legacy/2015/01/14/ssmanual2009_002.pdf (Accessed: 23.06.2025).
20. NYT. (2023) *Prosecutors Won't Retry Father Whose Son Died in Hot Car*. [Online] Available from: https://www.nytimes.com/2023/05/25/us/georgia-hot-car-child-death-charges-dropped.html (Accessed: 02.04.2025).
21. ABC News. (2-25) *Casey Anthony Trial: Did Cindy Anthony Really Search for Chloroform?* [Online] Available from: https://abcnews.go.com/US/casey_anthory_trial/casey-anthony-trial-cindy-anthony-search-chloroform/story?id=13981375 (Accessed: 02.04.2025).
22. 7safe.com. (2025) *The Good Practice Guide for Computer Based Electronic Evidence [ACPO]*. [Online] Available from: https://www.7safe.com/docs/default-source/default-document-library/acpo_guidelines_computer_evidence_v4_web.pdf (Accessed: 23.06.2025).
23. Legifrance.gouv.fr. (2025) *Code de procédure pénale (Dernière mise à jour des données de ce code: 15 juin 2025)*. [Online] Available from: https://www.legifrance.gouv.fr (Accessed: 23.06.2025).
24. Belonosov, V.O. (2023) Dokazatel'stva i dokazyvanie po UPK Frantsii [Evidence and Proof under the French Code of Criminal Procedure]. *Yuridicheskiy vestnik Samarskogo universiteta*. 9 (4). pp. 62–73.
25. Gesetze-im-internet.de. (2025) *Strafprozeßordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 2 Absatz 1 des Gesetzes vom 7. November 2024 (BGBl. 2024 I Nr. 351) geändert worden ist*. [Online] Available from: https://www.gesetze-im-internet.de/stpo/BJNR006290950.html (Accessed: 22.06.2025).
26. Dominik, B. & Mattias, Ya. (2020) Tsifrovye dokazatel'stva v nemetskom ugolovnom protsesse na stadiyakh predvaritel'nogo rassledovaniya, rassmotreniya dela po sushchestvu i revizii [Digital Evidence in German Criminal Procedure at the Stages of Preliminary Investigation, Trial and Appeal]. *Rossiyskoe pravo: obrazovanie, praktika, nauka*. 3. pp. 4–18.
27. Devgan.in. (2025) *Indian Evidence Act, 1872. IEA India, Act No. 1 OF 1872*. [Online] Available from: https://devgan.in/iea/ (Accessed: 16.06.2025).
28. Popova, E.I. (2023) Impact of Digital Technologies on Criminal Procedure in Russia and India: Comparative Legal Aspect. *International Journal "Law in Changing World"*. 2 (1). pp. 52–65.
29. China Law Translate. (2016) *Provisions on Several Issues concerning the Collection, Taking, Examination, and Judgment of Electronic Data in the Handling of Criminal Cases*. [Online] Available from: https://www.chinalawtranslate.com/en/provision-on-collection-and-review-of-digital-information-in-criminal-cases/ (Accessed: 02.04.2025).
30. China Law Translate. (2019) *Rules of Obtainment of Electronic Data as Evidence by Public Security Authorities in Handling Criminal Cases*. [Online] Available from: https://www.chinalawtranslate.com/en/Public-Security-Organs-for-Collecting-Electronic-Evidence-in-Criminal-Cases/ (Accessed: 02.04.2025).
31. Interpol. (2021) *Guidelines for digital forensics first responder. Best practices for search and seizure of electronic and digital evidence.* [Online] Available from: https://www.interpol.int/content/download/16243/file/Guidelines to Digital Forensics First Responders_V7.pdf (Accessed: 02.04.2025).
32. Shcherba, S.P. & Litvishko, P.A. (eds) (2024) *Collecting Electronic Evidence in Criminal Cases in Russia and Foreign Countries: Experiences and Problems: Monograph*. Moscow: Publishing House "Gorodets".
33. UNODC. (2025) *ENISA. Electronic evidence – a basic guide for First Responders*. [Online] Available from: https://syntheticdrugs.unodc.org/uploads/syntheticdrugs/res/library/cybercrime_html/Electronic_Evidence_A_Basic_Guide_for_First_Responders_ENISA.pdf (Accessed: 02.04.2025).
34. Mifsud Bonnici, J.P., Tudorica, M. & Cannataci, J.A. (2018) The European Legal Framework on Electronic Evidence: Complex and in Need of Reform. In: *Handling and Exchanging Electronic Evidence Across Europe. Law, Governance and Technology Series*. 39. pp. 189–235.
35. EU. (2023) *Regulation (EU) 2023/1543 on European Production and Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings*. [Online] Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum:4682020 (Accessed: 02.04.2025).
36. EU. (2023) *Directive (EU) 2023/1544 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings.* [Online] Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum:4682020 (Accessed: 02.04.2025).
37. Zuev, S.V. & Morugina, N.A. (2024) Elektronnoe ugolovnoe delo: teoreticheskaya model' [Electronic Criminal Case: A Theoretical Model]. *Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii*. 15 (57). pp. 83–94.
38. Zadorozhnaya, V.A. (2018) Proizvodstvo po ugolovnomu delu v elektronnom formate po zakonodatel'stvu Respubliki Kazakhstan [Criminal Proceedings in Electronic Format under the Legislation of the Republic of Kazakhstan]. *Pravoporyadok: istoriya, teoriya, praktika*. 4 (19). pp. 71–75.
39. de Vuyst, B. & Fairchild, A. (2006) The Phenix project: a case study of e-justice in Belgium. *Proceedings of the 8th International Conference on Electronic Commerce: The new e-commerce: innovations for conquering current barriers, obstacles and limitations to conducting successful business on the internet (ICEC '06)*. Association for Computing Machinery, New York, USA. pp. 327–333.
40. Gesetze-im-internet.de. (2025) *German Criminal Code (Strafgesetzbuch – StGB) on 13 November 1998*. [Online] Available from: https://www.gesetze-im-internet.de/englisch_stgb/index.html (Accessed: 16.06.2025).
41. Stepanov, O.A., Pechegin, D.A. & D'yakonova, M.O. (2021) K voprosu o tsifrovizatsii sudebnoy deyatel'nosti [On the Digitalization of Judicial Activities]. *Pravo. Zhurnal Vysshey shkoly ekonomiki*. 14 (5). pp. 4–22.
42. Kachalova, O.V. & Tsvetkov, Yu.A. (2015) Elektronnoe ugolovnoe delo – instrument modernizatsii ugolovnogo sudoproizvodstva [Electronic Criminal Case - A Tool for Modernizing Criminal Proceedings]. *Rossiyskoe pravosudie*. 2. pp. 95–101.
43. Valov, S.V. (2023) Resursnoe obespechenie tsifrovoy transformatsii sledstvennoy deyatel'nosti [Resource Support for the Digital Transformation of Investigative Activities]. *Rossiyskiy sledovatel'*. 3. pp. 2–6.
44. Malysheva, O.A. (2020) Osobennosti dokazyvaniya, osushchestvlyaemogo sledovatelem, v usloviyakh tsifrovizatsii ugolovnogo sudoproizvodstva [Peculiarities of Proof Carried Out by an Investigator in the Context of Digitalization of Criminal Proceedings]. *Vestnik Universiteta imeni O.E. Kutafina*. 10 (74). pp. 82–88.
45. McGinnis, D.O. & Pirs, R.D. (2019) Velikiy podryv: kak iskusstvennyy intellekt menyaet rol' yuristov v okazanii yuridicheskikh uslug [The Great Disruption: How Artificial Intelligence is Changing the Role of Lawyers in Providing Legal Services]. *Aktual'nye problemy ekonomiki i prava*. 13 (2). pp. 1230–1250.
46. Vinogradova, E.A. (2023) Tekhnologii iskusstvennogo intellekta i narastayushchie kiberugrozy v Latinskoy Amerike [Artificial Intelligence Technologies and Growing Cyber Threats in Latin America]. *Latinskaya Amerika*. 3. pp. 34–48.

47. Chistilina, D.O. (2021) Ispol'zovanie vozmozhnostey iskusstvennogo intellekta v ugolovnom protsesse [Using the Capabilities of Artificial Intelligence in Criminal Proceedings]. *Vestnik Udmurtskogo universiteta. Seriya: ekonomika i pravo*. 31 (4). pp. 705–710.
48. Byelov, D., Bielova, M. & Rushchak, I. (2025) Artificial Intelligence in Pre-Trial Investigation of Criminal Cases: Some Issues of International Practice. *Analytical and Comparative Jurisprudence*. 1. pp. 818–824.
49. Afanas'ev, A.Yu. (2020) Sistemy iskusstvennogo intellekta v mekhanizme ugolovno-protsessual'nogo dokazyvaniya [Artificial Intelligence Systems in the Mechanism of Criminal Procedural Proof]. *Yuridicheskaya nauka i praktika: Vestnik Nizhegorodskoy akademii MVD Rossii*. 1 (49). pp. 89–95.
50. Ramaldanov, Kh.Kh. (2023) Vliyanie informatsionnykh tekhnologiy na protsess dokazyvaniya v ugolovnom sudoproizvodstve [The Influence of Information Technologies on the Process of Proof in Criminal Proceedings]. *Problemy v rossiyskom zakonodatel'stve*. 7. pp. 273–279.
51. Zaytsev, O.A. & Pastukhov, P.S. (2022) Tsifrovoy profil' litsa kak element informatsionno-tekhnologicheskoy strategii rassledovaniya prestupleniy [Digital Profile of an Individual as an Element of the Information Technology Strategy for Crime Investigation]. *Vestnik Permskogo universiteta. Yuridicheskie nauki*. 56. pp. 281–308.
52. Alymov, D.V., Balashov, K.G. & Deriglazova, A.Yu. (2024) Criminalistic Characterization of Typical Traces Left by an Offender Engaged in Criminal Activities in the Virtual Space (Using the Example of Dropper Operators). *Vestnik Tomskogo gosudarstvennogo universiteta – Tomsk State University Journal*. 506. pp. 185–192. (In Russian). doi: 10.17223/15617793/506/23
53. Pershin, A.N. (2021) Tsifrovye prava lits, osushchestvlyayushchikh predvaritel'noe rassledovanie [Digital Rights of Persons Conducting Preliminary Investigation]. *Vestnik Universiteta imeni O.E. Kutafina*. 2 (78). pp. 108–115.
54. Michurina, O.V. (2020) Iskusstvennyy intellekt protiv vnutrennego ubezhdeniya: vzglyad v budushchee ugolovnogo sudoproizvodstva [Artificial Intelligence vs. Inner Conviction: A Look into the Future of Criminal Proceedings]. *Vestnik Moskovskogo universiteta MVD Rossii*. 3. pp. 65–68.
55. Spiridonov, M.S. (2023) Tekhnologii iskusstvennogo intellekta v ugolovno-protsessual'nom dokazyvanii [Artificial Intelligence Technologies in Criminal Procedural Proof]. *Journal of Digital Technologies and Law*. 1 (2). pp. 481–497.
56. Spesivov, N.V. (2023) Ot fantasticheskikh teoriy k ob"ektivnoy real'nosti: est' li budushchee u iskusstvennogo intellekta i prediktivnykh tekhnologiy pri otpravlenii pravosudiya po ugolovnym delam? [From Fantastic Theories to Objective Reality: Is There a Future for Artificial Intelligence and Predictive Technologies in the Administration of Criminal Justice?]. *Lex Russica*. 2 (195). pp. 81–90.

Информация об авторах:
Рябинина Т.К. – д-р юрид. наук, зав. кафедрой уголовного процесса и криминалистики Юго-Западного государственного университета (Курск, Россия). E-mail: tatyanakimovna-r@yandex.ru
Чистилина Д.О. – канд. юрид. наук, доцент кафедры уголовного процесса и криминалистики Юго-Западного государственного университета (Курск, Россия). E-mail: darya-chistilina@yandex.ru
Ряполова Я.П. – канд. юрид. наук, доцент кафедры уголовного процесса и криминалистики Юго-Западного государственного университета (Курск, Россия). E-mail: yarosslava@mail.ru

Авторы заявляют об отсутствии конфликта интересов.

Information about the authors:
T.K. Ryabinina, Dr. Sci. (Law), head of the Department of Criminal Procedure and Criminalistics, Southwest State University (Kursk, Russian Federation). E-mail: tatyanakimovna-r@yandex.ru
D.O. Chistilina, Cand. Sci. (Law), associate professor, Southwest State University (Kursk, Russian Federation). E-mail: darya-chistilina@yandex.ru
Ya.P. Ryapolova, Cand. Sci. (Law), associate professor, Southwest State University (Kursk, Russian Federation). E-mail: yarosslava@mail.ru

The authors declare no conflicts of interests.

Статья поступила в редакцию 17.04.2025;
одобрена после рецензирования 11.07.2025; принята к публикации 31.07.2025.

The article was submitted 17.04.2025;
approved after reviewing 11.07.2025; accepted for publication 31.07.2025.