



УДК 343.1:174(574)

**ЭТИКО-ПРАВОВЫЕ АСПЕКТЫ
ЦИФРОВОЙ КРИМИНАЛИСТИКИ
И СУДЕБНОЙ ЭКСПЕРТИЗЫ
В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ
РЕСПУБЛИКИ КАЗАХСТАН**

Сакен Жусипахметович Абдолла

Верховный Суд Республики Казахстан, Астана, Республика Казахстан,
abdolla.saken@bk.ru

Аннотация. В статье рассматриваются этико-правовые аспекты применения цифровых технологий и искусственного интеллекта в сфере криминалистики и судебной экспертизы в уголовном судопроизводстве Республики Казахстан. Анализируются действующие нормативные правовые акты, включая Уголовно-процессуальный кодекс Республики Казахстан, законы «Об искусственном интеллекте», «О судебно-экспертной деятельности», «О персональных данных и их защите», а также Цифровой кодекс Республики Казахстан (вступит в силу в июне 2026 г.). Особое внимание уделяется вопросам допустимости цифровых доказательств, обеспечения судебного контроля, защиты прав личности и минимизации рисков, связанных с предвзятостью алгоритмов и нарушением конфиденциальности. Подчеркивается необходимость разработки национального этического кодекса для экспертов, сертификации ИИ-систем и гармонизации законодательства с международным опытом на основе адаптации, а не прямого заимствования. Статья основана на анализе научных публикаций, нормативных актов и практических примеров применения цифровых методов в экспертной деятельности.

Ключевые слова: цифровая криминалистика, судебная экспертиза, искусственный интеллект, Уголовно-процессуальный кодекс Республики Казахстан

Для цитирования: Абдолла С. Ж. Этико-правовые аспекты цифровой криминалистики и судебной экспертизы в уголовном судопроизводстве Республики Казахстан // Судебная экспертиза. 2026. № 1 (85). С. 103–111.

**ETHICAL AND LEGAL ASPECTS
OF DIGITAL FORENSICS AND FORENSIC EXAMINATION
IN CRIMINAL PROCEEDINGS
IN THE REPUBLIC OF KAZAKHSTAN**

Saken Zhusipakhmetovich Abdolla

Supreme Court of the Republic of Kazakhstan, Astana, Republic of Kazakhstan,
abdolla.saken@bk.ru

© Абдолла С. Ж., 2026



Abstract. The article discusses the ethical and legal aspects of the use of digital technologies and artificial intelligence in the field of criminalistics and forensic examination in criminal proceedings in the Republic of Kazakhstan. It analyzes the current regulatory and legal acts, including the Criminal Procedure Code of the Republic of Kazakhstan, the Law "On Artificial Intelligence", the Law "On Forensic Activities", the Law "On Personal Data and Their Protection", as well as the Digital Code of the Republic of Kazakhstan (which will come into force in June 2026). Particular attention is paid to issues of the admissibility of digital evidence, ensuring judicial control, protecting individual rights, and minimizing risks associated with algorithm bias and privacy violations. The article emphasizes the need to develop a national code of ethics for experts, certify AI systems, and harmonize legislation with international experience based on adaptation rather than direct borrowing. The article is based on an analysis of scientific publications, regulatory acts, and practical examples of the application of digital methods in expert activities.

Keywords: digital forensics, forensic examination, artificial intelligence, Criminal Procedure Code of the Republic of Kazakhstan

For citation: Abdolla S. Zh. Ethical and legal aspects of digital forensics and forensic examination in criminal proceedings in the Republic of Kazakhstan. Forensic Examination, 103–111, 2026. (In Russ.).

В эпоху цифровизации общества криминалистика и судебная экспертиза претерпевают фундаментальные изменения, связанные с внедрением информационных технологий, искусственного интеллекта (далее – ИИ) и цифровых методов сбора, анализа и представления доказательств. Цифровая криминалистика, как междисциплинарная область, объединяет традиционные криминалистические подходы с современными технологиями, позволяющими работать с электронными следами, данными в сетях и виртуальными объектами.

В Республике Казахстан (далее – РК) эти процессы регулируются Уголовно-процессуальным кодексом РК (далее – УПК РК), где судебная экспертиза выступает ключевым средством установления обстоятельств дела (ст. 270–287 УПК РК). Однако внедрение цифровых технологий поднимает актуальные этические и правовые вопросы: от обеспечения конфиденциальности персональных данных до минимизации рисков предвзятости ИИ и этических нарушений в экспертной деятельности. Стоит отметить, уже вступил в силу Закон РК «Об искусственном интеллекте»¹, в июне 2026 г. вступит в силу Цифровой кодекс РК² (далее – ЦК РК), которые распределили роли между разработчиками и пользователями.

Актуальность темы обусловлена глобальной цифровизацией правоохранительных органов, включая РК. В рамках государственной программы «Концепция цифровой трансформации, развития отрасли информационно-коммуникационных

¹ Об искусственном интеллекте: закон Республики Казахстан от 17 ноября 2025 г. № 230-VIII ЗПК. URL: <https://adilet.zan.kz/rus/docs/Z2500000230> (дата обращения: 23.01.2026).

² Цифровой кодекс Республики Казахстан от 9 января 2026 года № 255-VIII ЗПК. URL: <https://adilet.zan.kz/rus/docs/K2600000255#z756> (дата обращения: 23.01.2026).



технологий и кибербезопасности на 2023–2029 годы»¹ предусмотрены стратегические цели:

- развитие отрасли информационно-коммуникационных технологий (далее – ИКТ);
- усиление мер кибербезопасности;
- внедрение новых технологий, включая ИИ;
- повышение цифрового потенциала государственных структур.

Несмотря на преимущества – ускорение расследований, повышение точности доказывания, – возникают риски: нарушение прав человека, этические дилеммы при использовании ИИ и пробелы в правовом регулировании. Это требует переосмысления правовых и этических оснований цифровой криминалистики в условиях национальной правовой системы.

Цель статьи – проанализировать этико-правовые аспекты цифровой криминалистики и судебной экспертизы в уголовном судопроизводстве РК. Задачи: определить ключевые понятия, выявить действующие правовые нормы, обсудить этические риски и предложить рекомендации. Методология включает анализ нормативных актов РК, сравнительный подход и обобщение научных источников.

Понятие и роль цифровой криминалистики в судебной экспертизе.

Цифровая криминалистика представляет собой раздел криминалистики, ориентированный на выявление, фиксацию и анализ цифровых следов преступлений с использованием информационных технологий. Как отмечает А. А. Бульбачева, в условиях цифровой трансформации такие технологии включают автоматизированные системы поиска и анализа данных, что актуально для экспертно-криминалистической деятельности [1].

В РК цифровая криминалистика интегрируется в судебную экспертизу через Закон РК «О судебно-экспертной деятельности» от 10 февраля 2017 г.², где подчеркивается необходимость применения современных методов для обеспечения объективности (ст. 4–6).

Судебная экспертиза в уголовном судопроизводстве РК (ст. 270–287 УПК РК) предполагает применение специальных знаний для разрешения вопросов, требующих научного подхода. Цифровые технологии расширяют ее возможности: от анализа цифровой фотографии на местах происшествий [2] до использования ИИ в почерковедческой экспертизе [3] и виртуальной аутопсии [4; 5].

Например, В. А. Клевно и Ю. В. Чумакова описывают виртуальную аутопсию (виртопсию) как метод предсекционного КТ-исследования, повышающий объективность [4]. В казахстанском контексте такие данные могут признаваться доказательствами при соблюдении требований ст. 115–125 УПК РК, где подчеркивается, что цифровые изображения признаются документами, приложенными к материалам дела, при условии их аутентичности и допустимости.

¹ Постановление Правительства РК № 269 от 28 марта 2023 г. URL: <https://adilet.zan.kz/rus/docs/P2300000269> (дата обращения: 23.01.2026).

² О судебно-экспертной деятельности: закон Республики Казахстан от 10 февраля 2017 г. № 44-VI ЗПК. URL: https://adilet.zan.kz/rus/docs/Z1700000044/z44_1.htm (дата обращения: 23.01.2026).



Интеграция технологий требует учета процессуальных особенностей. Д. В. Бахтеев связывает частные криминалистические теории с разработкой ИИ-систем, подчеркивая их нелинейность и обучаемость [6]. В РК аналогичные подходы могут применяться в рамках Инструкции о ведении уголовного судопроизводства в электронном формате¹.

Кроме того, А. В. Отогочев классифицирует цифровые следы преступлений на финансовом рынке, подчеркивая необходимость их оперативной фиксации во избежание уничтожения [7]. Рассматривая цифровой портрет человека как объект исследования, И. Н. Подволоцкий расширяет возможности идентификации с использованием биометрических методов [8]. В судебно-медицинской практике С. В. Ерофеев и другие предлагают 2D- и 3D-моделирование для повышения достоверности экспертиз [9]. А. А. Бессонов отмечает применение ИИ при расследовании серийных преступлений для построения поискового портрета [10].

Правовые аспекты применения цифровых технологий в уголовном судопроизводстве РК

Правовую основу применения цифровых технологий в РК составляют:

- ЦК РК;
- УПК РК;
- Закон РК «Об искусственном интеллекте»;
- Закон РК «О персональных данных и их защите».

Эти акты регулируют сбор, обработку и использование цифровых доказательств с соблюдением принципов законности, пропорциональности и судебного контроля.

Нам необходимо остановиться на ЦК РК, который поясняет, что электронный документ, удостоверенный электронной цифровой подписью (далее – ЭЦП), «равнозначен подписанному документу на бумажном носителе». Это положение является краеугольным камнем для процессуального права, поскольку оно делает цифровые файлы допустимыми доказательствами в суде (п. 2 ст. 62 ЦК РК). А ЭЦП (ст. 49 ЦК РК) определяется как инструмент, «подтверждающий достоверность электронного документа, его принадлежность и неизменность содержания», что соответствует п. 5 ст. 125 УПК РК.

Кроме того, законодатель закрепил нормы о цифровой аутентификации (ст. 46 ЦК РК) и цифровом подтверждении (ст. 47 ЦК РК). Пункт 5 статьи 46 ЦК РК прямо указывает, что такие записи «не могут быть признаны не имеющими юридической силы только на основании того, что они представлены в виде цифровых данных». Это означает, что логи входа в систему, записи об использовании двухфакторной аутентификации или биометрического подтверждения могут служить в суде доказательством совершения юридически значимых действий конкретным лицом.

Кроме того, ЦК РК закрепил норму о цифровом событии (ст. 76 ЦК РК). Это понятие охватывает любые зафиксированные в цифровой форме обстоятель-

¹ Инструкции о ведении уголовного судопроизводства в электронном формате: приказ Генпрокурора РК от 3 января 2018 г. № 2. URL: <https://adilet.zan.kz/rus/docs/V1800016268> (дата обращения: 23.01.2026).



ства, возникающие при работе цифровых объектов (например, журналы операций, логи серверов). Данные о таких событиях могут служить бесценным источником объективной информации для проведения компьютерно-технической экспертизы (forensic-анализа) и восстановления точной хронологии событий в рамках расследования.

В итоге формируется четкая иерархия: ЦК РК выступает в роли «материального» закона, который придает юридический статус цифровым объектам, действиям и событиям. УПК РК является «процессуальным» законом, который определяет порядок и правила использования этих легитимизированных объектов в качестве доказательств и их исследования экспертами в ходе судебного разбирательства.

Судебная экспертиза, в свою очередь, назначается в порядке ст. 270 УПК РК, но только если возникают вопросы, требующие специальных знаний. Само по себе использование ИИ не влечет обязательного назначения экспертизы – экспертиза необходима лишь для проверки результатов, если их достоверность оспаривается или требует научного обоснования.

В РК отсутствует специализированный кодекс этики для цифровой экспертизы, хотя ст. 283 УПК РК требует от эксперта объективности и беспристрастности. А. Д. Горбунова описывает применение цифровых технологий в гистологическом анализе, что может быть интегрировано в практику судебно-медицинских учреждений РК [11].

Правовые риски включают несанкционированный доступ к персональным данным. И. Б. Воробьева отмечает нарушения прозрачности и достоверности при использовании ИИ [12].

В РК до принятия в ноябре 2025 г. закона РК «Об искусственном интеллекте» это регулировалось главой 7 «Уголовные правонарушения в сфере информатизации и связи» Уголовного кодекса РК (ст. 205–207), а также Законом РК «О персональных данных и их защите», который устанавливает правила обработки персональных данных.

На данный момент ст. 7 «Прозрачность и объяснимость» Закона РК «Об искусственном интеллекте» закрепляет право пользователя на получение полной информации о характеристиках и ограничениях системы ИИ. Более того, п. 2 ст. 7 Закона РК «Об искусственном интеллекте» наделяет пользователя, в отношении которого ИИ принимает решения, правом быть «информированным о порядке автоматизированной обработки и ее последствиях, о возможности заявить возражение против автоматизированной обработки, а также о порядке защиты своих прав».

Таким образом, стратегическим ядром нового законодательства является ст. 4 Закона РК «Об искусственном интеллекте», закладывающая фундамент для всего государственного регулирования в сфере ИИ. Перечисленные в ней принципы (1) законности; 2) справедливости и равенства; 3) прозрачности и объяснимости; 4) ответственности и подконтрольности; 5) приоритета благополучия человека, свободы воли в принятии им решений; 6) защиты данных и конфиденциальности; 7) безопасности и защищенности) представляют собой прямое юридическое выражение ключевых этических требований, предъявляемых к современным технологиям. Они служат основой для всех



последующих норм, определяя вектор развития и применения искусственного интеллекта в Казахстане.

В. А. Клевно и Ю. В. Чумакова демонстрируют возможности виртуальной аутопсии при огнестрельной травме [5]. Однако для признания таких данных допустимыми доказательствами необходимо соблюдение ст. 117 УПК РК «Недопустимые доказательства» и ст. 120 УПК РК «Фиксация доказательств».

Международный опыт также представляет интерес. Отчет Стэнфордского центра уголовного правосудия (2024 г.) обсуждает влияние ИИ на правосудие, делая акцент на прозрачности и минимизации предвзятости [13]. Н. Л. Каравасос подчеркивает риски предвзятости в системах типа COMPAS [14]. Опыт зарубежных юрисдикций может служить ориентиром при совершенствовании национального законодательства РК, но не заменяет его.

Этические аспекты и риски цифровой криминалистики

Этические проблемы возникают на всех этапах – от разработки до применения технологий. М. Х. Бадмаева применяет принцип ответственности Ганса Йонаса к этике ИИ, подчеркивая необходимость минимизации экзистенциальных рисков [15]. В контексте РК это означает учет этических норм при использовании ИИ для предотвращения алгоритмической предвзятости, что может нарушать ст. 14 Конституции РК «Равенство всех перед законом».

И. О. Перепечина фокусируется на этических рисках генетических технологий, требуя прогнозирования нежелательных последствий [16]. В РК это актуально для генетической экспертизы (ст. 270–287 УПК РК), где риски включают нарушение приватности.

С. М. Бобовкин, Я. А. Климова и В. П. Полунин описывают кибернетические методы в почерковедческой экспертизе (например, CEDAR-FOX), отмечая их вспомогательную роль [3]. Этически это требует прозрачности алгоритмов, чтобы избежать ошибок, влияющих на права обвиняемых (ст. 13 УПК РК «Недопустимость доказательств, полученных с нарушением закона»).

Применение компьютерных программ для диагностики повреждений при сексуальном насилии поднимает вопросы конфиденциальности жертв [17]. Стэнфордский отчет и Н. Л. Каравасос рекомендуют аудит ИИ-систем и обязательный человеческий надзор [13; 14]. В РК эти риски усугубляются отсутствием специальных этических норм, что требует разработки профессиональных стандартов.

В практике РК цифровые технологии уже применяются:

- в судебно-медицинских экспертизах (гистологический анализ с цифровыми изображениями [11]);
- фотографической фиксации следов [2];
- виртуальной аутопсии при огнестрельной травме [5];
- расследовании финансовых преступлений (анализ цифровых следов на крипторынках [7]).

На основании изложенного считаем целесообразным предложить следующие рекомендации:

- 1) внести дополнения в национальный Кодекс этики судебного эксперта в части цифровых технологий и ИИ, интегрируя принципы ответственности [15] и международные рекомендации [13];



2) ввести обязательную сертификацию ИИ-систем, применяемых в правоохранительной деятельности;

3) внедрить обязательное обучение экспертов этике ИИ.

Цифровая криминалистика и судебная экспертиза в уголовном судопроизводстве РК открывают новые возможности, но сопровождаются серьезными этико-правовыми рисками. Анализ показывает: необходимо гармонизировать инновации с защитой прав человека, опираясь не на прямое заимствование иностранных норм, а на адаптацию лучших практик к национальной правовой системе. Внесение поправок в этический кодекс, усиление судебного контроля и развитие законодательства позволят обеспечить справедливость, прозрачность и доверие к правосудию в цифровую эпоху.

Список источников

1. Бульбачева А. А. О перспективах применения информационных технологий в экспертно-криминалистической деятельности в контексте цифровой трансформации системы МВД России // Полицейская деятельность. 2024. № 6. С. 149–164.
2. Telyatitskaya T. Digital photography of crime scenes in the production in forensic examinations // Technology and Language. 2021. Vol. 2 (2). P. 68–76.
3. Бобовкин С. М., Климова Я. А., Полунин В. П. Использование возможностей цифровой криминалистики (на примере судебно-почерковедческой экспертизы) // Вестник Волгоградской Академии МВД России. 2022. № 3 (62). С. 109–117.
4. Клевно В. А., Чумакова Ю. В. Виртопсия – новый метод исследования в практике отечественной судебной медицины // Судебная медицина. 2019. Т. 5, № 2. С. 27–31.
5. Возможности виртуальной аутопсии при огнестрельной травме / В. А. Клевно, Ю. В. Чумакова, Д. П. Павлик, С. Э. Дуброва // Судебная медицина. 2019. Т. 5, № 3. С. 33–38.
6. Бахтеев Д. В. Частные криминалистические теории как источник для разработки прикладных систем искусственного интеллекта в следственной деятельности // Вестник Томского государственного университета. Право. 2020. № 37. С. 32–43.
7. Отогочев А. В. Виды цифровых следов преступлений на финансовом рынке // Актуальные проблемы российского права. 2025. Т. 20, № 2. С. 111–124.
8. Подволоцкий И. Н. Цифровой портрет человека как объект комплексного исследования // Вестник криминалистики. 2024. № 3. С. 90–98.
9. Ерофеев С. В., Шишкин Ю. Ю., Федорова А. С. О технологиях анализа изображений как средствах повышения объективности и достоверности судебно-медицинских экспертиз // Судебная медицина. 2017. Т. 3, № 2. С. 17–23.
10. Бессонов А. А. Современные информационные технологии на службе следствия // Сибирские уголовно-процессуальные и криминалистические чтения. 2022. № 1. С. 94–100.
11. Горбунова А. Д. Использование цифровых технологий при проведении судебно-медицинских экспертиз // International Journal of Humanities and Natural Sciences. 2020. Vol. 11-4 (50). P. 60–62.



12. Воробьева И. Б. Этические аспекты использования систем искусственного интеллекта при расследовании преступлений // Вестник Саратовской государственной юридической академии. 2022. № 4 (147). С. 162–172.

13. The Implications of AI for criminal justice: key takeaways from a convening of leading stakeholders // Stanford Criminal Justice Center. 2024. Oct.

14. Karavasos N. L. artificial intelligence in criminal law: benefits, risks, ethical issues // NiaLena Blog. 2025. 11 May.

15. Бадмаева М. Х. Этика искусственного интеллекта: принцип ответственности Ганса Йонаса // Вестник Бурятского государственного университета. Философия. 2022. Вып. 1. С. 67–79.

16. Перепечина И. О. Этические риски современных судебно-экспертных и криминалистических технологий // Вестник экономической безопасности. 2023. № 1. С. 153–157.

17. Применение компьютерных программ для судебно-медицинской диагностики повреждений при сексуальном насилии / С. В. Ерофеев, Ю. Ю. Шишкин, М. В. Молоков, О. Ортодоксу // Судебная медицина. 2024. Т. 10, № 1. С. 35–39.

References

1. Bulbacheva A. A. On the prospects for the application of information technologies in forensic and criminalistic activities in the context of digital transformation of the system of the Ministry of Internal Affairs of Russia. *Police Activity*, 149–164, 2024. (In Russ.).

2. Telyatitskaya T. Digital photography of crime scenes in the production of forensic examinations. *Technology and Language*, 68–76, 2021. (In Eng.).

3. Bobovkin S. M., Klimova Ya. A., Polunin V. P. Use of digital forensic capabilities (on the example of forensic handwriting examination). *Journal of the Volgograd Academy of the Ministry of the Interior of Russia*, 109–117, 2022. (In Russ.).

4. Klevno V. A., Chumakova Yu. V. Virtopsy as a new research method in the practice of domestic forensic medicine. *Forensic Medicine*, 27–31, 2019. (In Russ.).

5. Klevno V. A., Chumakova Yu. V., Pavlik D. P., Dubrova S. E. Possibilities of virtual autopsy in cases of gunshot injury. *Forensic Medicine*, 33–38, 2019. (In Russ.).

6. Bakhteev D. V. Particular criminalistic theories as a source for the development of applied artificial intelligence systems in investigative activities. *Tomsk State University Journal of Law*, 32–43, 2020. (In Russ.).

7. Otogochev A. V. Types of digital traces of crimes in the financial market. *Actual Problems of Russian Law*, 111–124, 2025. (In Russ.).

8. Podvolotskiy I. N. Digital portrait of a person as an object of comprehensive research. *Bulletin of Criminalistics*, 90–98, 2024. (In Russ.).

9. Erofeev S. V., Shishkin Yu. Yu., Fedorova A. S. On image analysis technologies as means of increasing the objectivity and reliability of forensic medical examinations. *Forensic Medicine*, 17–23, 2017. (In Russ.).

10. Bessonov A. A. Modern information technologies in the service of investigation. *Siberian Criminal Procedure and Criminalistics Readings*, 94–100, 2022. (In Russ.).

11. Gorbunova A. D. The use of digital technologies in conducting forensic medical examinations. *International Journal of Humanities and Natural Sciences*, 60–62, 2020. (In Russ.).



12. Vorobieva I. B. Ethical aspects of the use of artificial intelligence systems in crime investigation. Bulletin of the Saratov State Law Academy, 162–172, 2022. (In Russ.).

13. The Implications of AI for criminal justice: key takeaways from a convening of leading stakeholders. Stanford Criminal Justice Center, October, 2024. (In Eng.).

14. Karavasos N. L. Artificial intelligence in criminal law: benefits, risks, ethical issues. NiaLena Blog, May 11, 2025. (In Eng.).

15. Badmaeva M. Kh. Ethics of artificial intelligence: Hans Jonas's principle of responsibility. Bulletin of Buryat State University. Philosophy, 67–79, 2022. (In Russ.).

16. Perepechina I. O. Ethical risks of modern forensic expert and criminalistic technologies. Bulletin of Economic Security, 153–157, 2023. (In Russ.).

17. Erofeev S. V., Shishkin Yu. Yu., Molokov M. V., Ortodoksu O. Application of computer programs for forensic medical diagnostics of injuries in cases of sexual violence. Forensic Medicine, 35–39, 2024. (In Russ.).

Абдолла Сакен Жусипахметович,

судья Верховного Суда Республики Казахстан,
кандидат юридических наук;
abdolla.saken@bk.ru

Abdolla Saken Zhusipakhmetovich,

judge of the Supreme Court of the Republic of Kazakhstan,
candidate of juridical sciences;
abdolla.saken@bk.ru

Статья поступила в редакцию 28.01.2026; одобрена после рецензирования 02.03.2026; принята к публикации 02.03.2026.

The article was submitted 28.01.2026; approved after reviewing 02.03.2026; accepted for publication 02.03.2026.

* * *