УГОЛОВНОЕ ПРАВО, ПРОЦЕСС И КРИМИНАЛИСТИКА

Статья поступила в редакцию: 16.07.2026
Статья принята к публикации: 21.07.2026
Статья опубликована: 01.08.2026

УДК 343.98:004.8

DOI: 10.32743/UniLaw.2026.142.8.23216

КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Радионов Никита Евгеньевич
студент
Юридический институт, Северо-Кавказский федеральный университет
РФ, г. Ставрополь
E-mail: Nikita-4.nik@yandex.ru

Щербалев Андрей Андреевич
ассистент
кафедры уголовного права и процесса, Юридический институт, Северо-Кавказский федеральный университет
РФ, г. Ставрополь
E-mail: ug_pravo11a@mail.ru

CRIMINALISTIC CHARACTERISTICS OF CRIMES COMMITTED USING ARTIFICIAL INTELLIGENCE TECHNOLOGIES

Radionov Nikita Evgenievich
student
Law Institute
North-Caucasus Federal University
Russia, Stavropol

Shcherbalev Andrey Andreevich
Assistant
Department of Criminal Law and Procedure
Law Institute
North-Caucasus Federal University
Russia, Stavropol

Библиографическое описание: Радионов Н.Е., Щербалев А.А. Криминалистическая характеристика преступлений, совершаемых с использованием технологий искусственного интеллекта // Universum: экономика и юриспруденция : электрон. научн. журн. 2026. 8(142). URL: https://7universum.com/ru/economy/archive/item/23216

Аннотация

Цель исследования состоит в формировании криминалистической характеристики преступлений, совершаемых с использованием технологий искусственного интеллекта, и определении организационно-правовых условий применения интеллектуальных систем в расследовании в условиях цифровизации уголовного судопроизводства. Методологическую основу составили формально-юридический и сравнительно-правовой методы, анализ научной литературы и нормативных актов, систематизация цифровых следов, а также моделирование межведомственного взаимодействия. Установлено, что искусственный интеллект изменяет способ подготовки, совершения и сокрытия преступлений: автоматизирует социальную инженерию, создает синтетические аудио- и видеоматериалы, масштабирует фишинговые и мошеннические схемы, затрудняет атрибуцию действий. К криминалистически значимым признакам отнесены дистанционный и трансграничный характер деяний, высокая скорость воспроизводства, распределенная инфраструктура, использование облачных платформ и наличие специфической следовой картины, включающей журналы событий, метаданные, историю запросов к моделям, сетевые и платежные следы. Предложен пятиэтапный механизм внедрения искусственного интеллекта в правоохранительную деятельность: создание единой правовой базы, обеспечение объяснимости и аудита алгоритмов, минимизация злоупотреблений, повышение цифровой грамотности и организация общественного контроля. Сделан вывод о необходимости сохранения решающей роли человека при оценке доказательств и принятии процессуальных решений.

Abstract

The purpose of the study is to develop a criminalistic profile of crimes committed using artificial intelligence technologies and to determine the organizational and legal conditions for the use of intelligent systems in investigations. The methodology combines formal legal and comparative legal methods, analysis of academic literature and regulations, systematization of digital traces, and modeling of interagency cooperation. The study establishes that artificial intelligence changes the preparation, commission, and concealment of crimes by automating social engineering, generating synthetic audio and video, scaling phishing and fraud schemes, and complicating attribution. Criminalistically significant features include the remote and cross-border nature of offences, high replication speed, distributed infrastructure, reliance on cloud platforms, and a specific trace pattern comprising event logs, metadata, model interaction histories, network traces, and payment records. A five-stage mechanism for introducing artificial intelligence into law-enforcement practice is proposed: establishing a unified legal framework, ensuring explainability and independent audit, reducing risks of abuse, improving digital literacy, and organizing public oversight. The study concludes that human decision-making must remain decisive in the evaluation of evidence and in procedural decisions, while artificial intelligence should perform an auxiliary analytical function.

Ключевые слова: искусственный интеллект, криминалистика, цифровые следы, расследование преступлений, объяснимый ИИ, межведомственное взаимодействие, права человека.

Keywords: artificial intelligence, criminalistics, digital traces, crime investigation, explainable AI, interagency cooperation, human rights.

Введение

Цифровая трансформация преступной деятельности обусловила появление способов совершения общественно опасных деяний, в которых алгоритмы машинного обучения используются не только как вспомогательный инструмент, но и как средство автоматизации подготовки, исполнения и сокрытия противоправных действий. Национальная стратегия развития искусственного интеллекта закрепляет необходимость ускоренного развития соответствующих технологий при одновременном обеспечении безопасности, защиты прав и свобод человека [7]. В системе государственного стратегического планирования внедрение искусственного интеллекта связано с постановкой измеримых целей, координацией участников и контролем результатов [5, с.32 – 44].

Актуальность исследования определяется двойственной природой искусственного интеллекта. С одной стороны, интеллектуальные системы повышают результативность анализа больших массивов информации, распознавания объектов, сопоставления цифровых следов и выдвижения следственных версий. С другой стороны, те же инструменты применяются для создания дипфейков, клонирования голоса, автоматизированной социальной инженерии, генерации вредоносного кода и масштабирования мошеннических коммуникаций. В сфере правосудия особое значение приобретают вопросы допустимых пределов автоматизации, прозрачности моделей и сохранения персональной ответственности должностного лица [8, с.91 – 107].

Современная криминалистика рассматривает цифровизацию не как простую замену аналоговых носителей электронными, а как изменение механизмов образования, обнаружения и исследования следов преступления [3,с.35 – 39]. Практические исследования показывают возможность использования алгоритмов для построения цифровых моделей серийной преступной деятельности и выявления устойчивых взаимосвязей между эпизодами [1, с.45 – 53]. Вместе с тем криминалистическая характеристика преступлений, совершаемых с использованием искусственного интеллекта, пока не получила устойчивой структуры, пригодной для планирования расследования.

Цель исследования — определить основные элементы криминалистической характеристики преступлений, совершаемых с использованием технологий искусственного интеллекта, выявить типичные цифровые следы и предложить организационную модель безопасного применения интеллектуальных систем правоохранительными органами.

Материалы и методы

Эмпирическую и нормативную основу исследования составили положения Национальной стратегии развития искусственного интеллекта, российские научные публикации по цифровизации криминалистики и уголовно-процессуального доказывания, а также зарубежные документы риск-ориентированного регулирования искусственного интеллекта. При анализе учитывались результаты применения алгоритмов к моделированию серийных преступлений [1, с.45 – 53], предложения о задачах внедрения искусственного

интеллекта в криминалистическую деятельность [2, с.25 – 33], особенности использования интеллектуальных технологий в доказывании [6, с.481 – 497] и возможности исследования данных из открытых источников [4, с.95 – 103].

Использованы формально-юридический метод для анализа нормативных требований, сравнительно-правовой метод для сопоставления российских подходов с европейской моделью регулирования высокорисковых систем [9], системно-структурный метод для выделения элементов криминалистической характеристики, а также методы анализа, синтеза и моделирования. Риск-ориентированная оценка строилась с учетом принципов управления рисками, закрепленных в NIST AI RMF 1.0: управляемости, измеримости, прозрачности и постоянного мониторинга жизненного цикла системы [10].

Исследование проводилось последовательно. На первом этапе были выделены типовые способы использования искусственного интеллекта в преступной деятельности. На втором этапе систематизированы объекты посягательства, обстановка и цифровая следовая картина. На третьем этапе определены требования к сбору, фиксации, проверке и интерпретации алгоритмически обработанной информации. На четвертом этапе сформирована пятиэтапная модель межведомственного взаимодействия, направленная на сочетание технологической эффективности и процессуальных гарантий.

Результаты и обсуждения

Проведенный анализ позволяет определить преступления, совершаемые с использованием технологий искусственного интеллекта, как неоднородную группу деяний, в механизме которых интеллектуальная система выполняет одну или несколько функций: генерирует противоправный контент, классифицирует цели, персонализирует воздействие, автоматизирует коммуникацию, управляет технической инфраструктурой либо скрывает цифровые следы. Искусственный интеллект не образует самостоятельный универсальный способ преступления, однако существенно повышает скорость, масштабируемость и адаптивность традиционных криминальных схем.

Наиболее характерными способами являются создание синтетических аудио- и видеоматериалов для обмана потерпевших; автоматическая генерация сообщений и сценариев социальной инженерии; подбор уязвимых адресатов по данным из открытых источников; модификация вредоносного программного обеспечения; интеллектуальный анализ похищенных массивов данных; обход средств идентификации; автоматизированное управление множеством учетных записей. В отличие от обычной цифровой преступности, такие деяния способны быстро изменять тактику в зависимости от реакции пользователя или средств защиты.

К объектам посягательства относятся денежные средства, учетные записи, персональные и биометрические данные, деловая репутация, информационные ресурсы и нормальная работа цифровой инфраструктуры. Потерпевшими могут выступать граждане, организации и публичные органы. Обстановка совершения преступления обычно характеризуется дистанционностью, использованием облачных сервисов и зарубежных платформ, распределением ролей между участниками, применением анонимизирующих средств и кратким жизненным циклом технических ресурсов.

Следовая картина включает традиционные цифровые следы — сетевые адреса, журналы авторизации, идентификаторы устройств, данные браузера, сведения операторов связи и платежные записи, — а также специфические следы взаимодействия с интеллектуальными моделями: историю запросов и ответов, параметры генерации, версии модели, идентификаторы API, метаданные синтетических файлов, артефакты обработки и сведения о вычислительной среде. Данные из открытых источников могут использоваться для установления связей между псевдонимами, доменами, учетными записями и цифровой инфраструктурой, однако требуют процессуально корректной фиксации и экспертной верификации [4].

Личность преступника не сводится к образу высококвалифицированного разработчика. В преступной группе могут участвовать оператор готового сервиса, специалист по социальной инженерии, поставщик данных, разработчик или арендатор инфраструктуры, посредник по обналичиванию средств. Такая ролевая специализация затрудняет доказывание субъективной стороны и требует восстановления всей цепочки распределенных действий. Результаты алгоритмического анализа серийных эпизодов могут содействовать выявлению повторяющихся признаков, однако выводы системы должны проверяться следователем и специалистом [1].

Таблица 1.

Основные элементы криминалистической характеристики преступлений, совершаемых с использованием искусственного интеллекта

Элемент	Типичное содержание	Значение для расследования
Способ совершения	Генерация дипфейков, клонирование голоса, автоматизированный фишинг, подбор целей, модификация вредоносного кода.	Определяет круг технических объектов, экспертиз и неотложных следственных действий.
Предмет и потерпевший	Денежные средства, учетные записи, персональные и биометрические данные, информационные ресурсы, репутация.	Позволяет установить механизм причинения вреда и источники доказательственной информации.
Следовая картина	Логи, метаданные, API-запросы, история взаимодействия с моделью, сетевые, платежные и файловые артефакты.	Обеспечивает атрибуцию действий, связь эпизодов и проверку версии о применении конкретного сервиса.
Личность и роли	Оператор сервиса, разработчик, поставщик данных, специалист по социальной инженерии, финансовый посредник.	Требует доказывания распределенного умысла и вклада каждого участника.
Обстановка	Дистанционность, трансграничность, облачная инфраструктура, анонимизация, высокая скорость смены ресурсов.	Обусловливает международное и межведомственное взаимодействие, оперативность фиксации данных.

Использование искусственного интеллекта правоохранительными органами создает самостоятельную группу рисков. Автоматизированное сопоставление лиц, прогнозирование поведения и ранжирование объектов могут приводить к ложным срабатываниям, дискриминационным эффектам и некритичному переносу статистических закономерностей на конкретного человека. Европейский акт об искусственном интеллекте относит ряд

правоохранительных применений к высокорисковым и устанавливает требования к качеству данных, документированию, человеческому контролю и оценке соответствия [9]. Аналогичный риск-ориентированный подход предполагает непрерывное управление рисками, а не разовую проверку системы перед вводом в эксплуатацию [10].

Первый этап предлагаемой модели межведомственного взаимодействия состоит в создании единой правовой базы. Необходимо определить допустимые цели применения искусственного интеллекта, порядок доступа к данным, правила хранения исходной и производной информации, требования к воспроизводимости результатов и распределение ответственности между разработчиком, оператором и должностным лицом. Процессуальное решение не должно основываться на выводе системы, который невозможно проверить и объяснить.

Второй этап направлен на обеспечение прозрачности и достоверности алгоритмов. Для систем, влияющих на ход расследования, необходимы описание назначения и ограничений, сведения о версии модели, протоколирование запросов, тестирование на релевантных данных и независимый аудит. Технологии объяснимого искусственного интеллекта могут облегчить интерпретацию результата, однако объяснение должно быть содержательным для следователя, специалиста, суда и стороны защиты, а не ограничиваться техническими показателями.

Третий этап связан с минимизацией злоупотреблений. Все операции с использованием интеллектуальной системы подлежат обязательному логированию; доступ предоставляется по ролевой модели; результаты должны храниться вместе с исходными данными и параметрами обработки. Необходимо предусмотреть механизмы обжалования, повторной проверки и исключения информации, полученной с нарушением установленной процедуры. Такой подход соответствует требованию о сохранении персональной ответственности должностного лица за процессуальное решение [8].

Четвертый этап предполагает повышение цифровой грамотности сотрудников. Следователь должен понимать происхождение алгоритмического результата, различать корреляцию и доказанную причинную связь, оценивать вероятность ошибки и правильно формулировать задания специалисту или эксперту. Эффективное внедрение невозможно без межведомственных учений, единых методических рекомендаций и обмена практикой. Решение прикладных, а не только теоретических задач является обязательным условием полезности искусственного интеллекта для криминалистики [2].

Пятый этап предусматривает общественный и профессиональный диалог. Публикация обезличенных отчетов об эффективности и ошибках систем, участие научного сообщества, адвокатуры и специалистов по защите данных повышают легитимность технологий. При этом раскрытие информации не должно создавать новые уязвимости или препятствовать расследованию. Баланс достигается разграничением сведений о принципах, гарантиях и статистике работы системы и информации ограниченного доступа.

В совокупности предложенная модель позволяет рассматривать искусственный интеллект как контролируемый аналитический инструмент. Он способен ускорить поиск связей, кластеризацию эпизодов, анализ видео и документов, но не заменяет доказывание. Алгоритмический результат приобретает значение только после проверки его

происхождения, относимости, достоверности и соответствия процессуальной форме. В уголовно-процессуальном доказывании особое значение имеют сохранность исходных данных и возможность воспроизведения преобразований [6].

Заключение

Преступления, совершаемые с использованием технологий искусственного интеллекта, характеризуются сочетанием традиционного противоправного замысла и новых средств его реализации. Их ключевыми признаками являются автоматизация и персонализация воздействия, высокая масштабируемость, дистанционный и трансграничный характер, распределение ролей, использование облачной инфраструктуры и формирование специфических цифровых следов.

Для эффективного расследования необходимо фиксировать не только конечный файл или сообщение, но и всю цепочку его создания и распространения: данные об учетной записи, устройстве, сети, запросах к модели, параметрах генерации, платежах и взаимодействии участников. Криминалистическая характеристика должна использоваться как ориентир для выдвижения версий и планирования действий, а не как основание для автоматического вывода о виновности.

Внедрение искусственного интеллекта в правоохранительную деятельность целесообразно осуществлять поэтапно: нормативно закрепить цели и ограничения, обеспечить объяснимость и аудит, создать механизмы предотвращения злоупотреблений, повысить цифровую компетентность сотрудников и организовать общественный контроль. Окончательная оценка доказательств и принятие процессуальных решений должны оставаться за человеком, несущим персональную юридическую ответственность.

Список литературы

1. Бессонов, А.А. Использование алгоритмов искусственного интеллекта в криминалистическом изучении преступной деятельности (на примере серийных преступлений) / А.А. Бессонов // Вестник Университета имени О.Е. Кутафина (МГЮА). – 2021. – № 2. – С. 45–53. – DOI: 10.17803/2311–5998.2021.78.2.045–053.
2. Головин, А.Ю. Технологии искусственного интеллекта в криминалистике: задачи, которые необходимо решить / А.Ю. Головин // Сибирские уголовно-процессуальные и криминалистические чтения. – 2024. – № 2. – С. 25–33. – DOI: 10.17150/2411–6122.2024.2.25–33.
3. Карагодин, В.Н. Цифровизация и криминалистика / В.Н. Карагодин // Вестник Белгородского юридического института МВД России имени И.Д. Путилина. – 2021. – № 3. – С. 35–39.
4. Себякин, А.Г. Данные, находящиеся в открытых источниках информации, как объект судебной информационно-аналитической экспертизы / А.Г. Себякин // Сибирские уголовно-процессуальные и криминалистические чтения. – 2024. – № 2. – С. 95–103. – DOI: 10.17150/2411–6122.2024.2.95–103.

5. Сильвестров, С.Н. Определение и реализация национальных целей развития в российском стратегическом планировании / С.Н. Сильвестров, Ю.А. Крупнов, В.Г. Старовойтов // Российский экономический журнал. – 2021. – № 1. – С. 32–44.
6. Спиридонов, М.С. Технологии искусственного интеллекта в уголовно-процессуальном доказывании / М.С. Спиридонов // Journal of Digital Technologies and Law. – 2023. – Т. 1, № 2. – С. 481–497. – DOI: 10.21202/jdtl.2023.20.
7. Указ Президента Российской Федерации от 10.10.2019 № 490 (ред. от 15.02.2024) «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») // Собрание законодательства Российской Федерации. – 2019. – № 41. – Ст. 5700.
8. Цветков, Ю.А. Искусственный интеллект в правосудии / Ю.А. Цветков // Закон. – 2021. – № 4. – С. 91–107.
9. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [Электронный ресурс]. // Official Journal of the European Union. URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj (дата обращения: 17.07.2026).
10. Tabassi, E. Artificial Intelligence Risk Management Framework (AI RMF 1.0) / E. Tabassi. – Gaithersburg, MD: National Institute of Standards and Technology, 2023. – NIST AI 100–1. – DOI [Электронный ресурс]. URL: https://doi.org/10.6028/NIST.AI.100–1 (дата обращения: 17.07.2026).

References

1. [The use of artificial intelligence algorithms in the criminalistic study of criminal activity (on the example of serial crimes)] // Vestnik Universiteta imeni O.E. Kutafina (MGYuA). – 2021. – № 2. – P. 45–53. – DOI: 10.17803/2311–5998.2021.78.2.045–053.
2. [Artificial intelligence technologies in criminalistics: tasks to be solved] // Sibirskie ugolovno-protsessualnye i kriminalisticheskie chteniya. – 2024. – № 2. – P. 25–33. – DOI: 10.17150/2411–6122.2024.2.25–33.
3. [Digitalization and criminalistics] // Vestnik Belgorodskogo yuridicheskogo instituta MVD Rossii imeni I.D. Putilina. – 2021. – № 3. – P. 35–39.
4. [Data from open sources as an object of forensic information and analytical examination] // Sibirskie ugolovno-protsessualnye i kriminalisticheskie chteniya. – 2024. – № 2. – P. 95–103. – DOI: 10.17150/2411–6122.2024.2.95–103.
5. Silvestrov S.N., Krupnov Yu. A., Starovoitov V.G. [Definition and implementation of national development goals in Russian strategic planning] // Rossiiskii ekonomicheskii zhurnal. – 2021. – № 1. – P. 32–44.
6. [Artificial intelligence technologies in criminal procedural proof] // Journal of Digital Technologies and Law. – 2023. – № 2. – P. 481–497. – DOI: 10.21202/jdtl.2023.20.

7. Ukaz Prezidenta Rossiiskoi Federatsii ot 10.10.2019 No. 490 (red. ot 15.02.2024) [Decree of the President of the Russian Federation No. 490 of October 10, 2019 (as amended on February 15, 2024) “On the Development of Artificial Intelligence in the Russian Federation”]. Sobranie zakonodatelstva Rossiiskoi Federatsii. – 2019. – No. 41. – Art. 5700. (In Russ.)
8. [Artificial intelligence in justice] // Zakon. – 2021. – № 4. – P. 91–107.
9. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) // Official Journal of the European Union. – URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj (accessed 31.07.2026) (дата обращения: 17.07.2026).
10. Tabassi E. Artificial Intelligence Risk Management Framework (AI RMF 1.0). – Gaithersburg, MD: National Institute of Standards and Technology, 2023. – NIST AI 100–1 – URL: https://doi.org/10.6028/NIST.AI.100–1 (accessed 31.07.2026) (дата обращения: 17.07.2026).