



УДК 343.9

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В КРИМИНАЛИСТИЧЕСКОМ ИССЛЕДОВАНИИ ЦИФРОВЫХ СЛЕДОВ

Коновалова Алина Олеговна

студентка 4 курса

научный руководитель: **Саюшкина Е. В.**

кандидат юридических наук, доцент кафедры уголовно-правовых наук,

Оренбургский институт (филиал) Московского государственного юридического университета

имени О. Е. Кутафина (МГЮА) (ОИ МГЮА).

Россия, г. Оренбург

Аннотация. В статье рассматривается применение технологий искусственного интеллекта (ИИ) в криминалистическом исследовании цифровых следов. Актуальность темы обусловлена цифровой трансформацией общества, приводящей к экспоненциальному росту объема и сложности цифровой информации, связанной с преступной деятельностью. Автор анализирует возможности ИИ для автоматизации анализа данных, распознавания паттернов, идентификации лиц и обработки биологических следов, особое внимание уделяется правовым и процессуальным аспектам использования результатов ИИ-анализа в качестве доказательств в соответствии с требованиями УПК РФ, а также вопросам обеспечения защиты персональных данных и конфиденциальности.

Ключевые слова: криминалистика, искусственный интеллект, цифровые следы, цифровые доказательства, защита персональных данных.

THE USE OF ARTIFICIAL INTELLIGENCE IN FORENSIC ANALYSIS OF DIGITAL TRACES

Konovalova Alina Olegovna

student

scientific supervisor: **Sayushkina E. V.**

candidate of Legal Sciences, Associate Professor of the Department of Criminal Law Sciences
of the Orenburg Institute (branch) O.E. Kutafin University.

Russia, Orenburg

Abstract. The article discusses the application of artificial intelligence (AI) technologies in the forensic examination of digital traces. The relevance of this topic is due to the digital transformation of society, which leads to an exponential increase in the volume and complexity of digital information related to



criminal activities. The author analyzes the capabilities of AI for automating data analysis, pattern recognition, facial identification, and the processing of biological traces, with a focus on the legal and procedural aspects of using AI analysis results as evidence in accordance with the requirements of the Criminal Procedure Code of the Russian Federation, as well as the issues of ensuring the protection of personal data and confidentiality.

Key words: forensics, artificial intelligence, digital traces, digital evidence, and personal data protection.

Современное общество переживает цифровую трансформацию, в рамках которой практически каждый аспект человеческой деятельности, включая противоправную, оставляет многочисленные и сложные цифровые следы. Количество и многогранность представленных сведений, охватывающих переписку в программах обмена сообщениями, действия в социальных медиа, техническую информацию о файлах и записи системных журналов сетевой инфраструктуры, разрослись до такой степени, что классические подходы к проведению экспертного анализа в цифровой сфере утрачивают свою продуктивность. Любое преступное событие сопровождается материальными следами, под которыми понимаются следы, образованные в результате отображения хода преступного деяния и его результатов на объектах материального мира [4]. В этом контексте искусственный интеллект (далее - ИИ) становится не просто инновационным инструментом, а критически необходимой технологией для поддержки и усиления возможностей эксперта-криминалиста.

ИИ в расследовании преступлений используется для автоматизированного анализа, распознавания закономерностей и прогнозирования возможных связей между участниками противоправных действий [4]. Так, применение искусственного интеллекта в криминалистике также способствует оптимизации процесса идентификации подозреваемых, которые оставляют различные цифровые следы. Цифровой след в юридической литературе определяется как совокупность данных, оставляемых человеком при взаимодействии с цифровыми устройствами и сетевой инфраструктурой; к ним относятся IP-адреса, логи подключений, файлы, фото, геолокационные данные и т. д. Системы распознавания лиц, основанные на нейронных сетях, позволяют сопоставлять изображения с базами данных правоохранительных органов, значительно сокращая время, затрачиваемое на установление личности преступника. Алгоритмы анализа ДНК, использующие методы машинного обучения, повышают точность идентификации биологических следов, обнаруженных на месте преступления. Однако, несмотря на высокий потенциал, использование ИИ в этой сфере сопряжено с риском ошибок распознавания и требует обязательной верификации результатов специалистом. Для криминалистики это открывает



возможности к более быстрому и тщательному анализу цифровых следов преступления и данных о причастных к нему лицах.

В реальной практике искусственный интеллект широко используется в ходе расследования преступлений, относящихся к кибермошенничеству, организованной преступности в сфере наркотиков, торговле людьми и террористической деятельности. Согласно статистике Министерства внутренних дел Российской Федерации, в 2024 году с применением систем, предназначенных для анализа цифровых улик, было успешно раскрыто приблизительно 63% противоправных деяний, связанных с мошенничеством в сети Интернет. Кроме того, отмечается, что среднее время, затрачиваемое на обработку цифровых данных, сократилось в среднем на 40% [7]. Примеры из реальной следственно-судебной работы заслуживают особого внимания. Так, в 2023 году в Санкт-Петербурге было инициировано расследование по факту масштабной фишинговой аферы. В ходе данного расследования была задействована система искусственного интеллекта, предназначенная для анализа метаданных сетевой активности, получившая название «СЦИОН». Данная система позволила установить прямую связь между двадцатью семью эпизодами противоправной деятельности и одной преступной группировкой. Основанием для этой связи послужили выявление идентичных паттернов в переписке участников и схожей структуры фишинговых веб-ресурсов. Следует отметить, что заключение, составленное по результатам машинного анализа, было принято в качестве допустимого доказательства. Это стало возможным благодаря тому, что оно было подкреплено заключением эксперта-криминалиста, а также протоколом, подтверждающим корректность работы примененного алгоритма [2].

Можно обратиться к Методическим рекомендациям МВД РФ по применению технологий искусственного интеллекта при анализе цифровых доказательств, которые включают рекомендации по использованию законодательных норм, методов, программного обеспечения и экспертизы. В данном документе указано, что специалисты, работающие с цифровыми доказательствами, должны владеть навыками идентификации цифровых следов, понимать принципы работы алгоритмов анализа и уметь интерпретировать результаты автоматической обработки данных [5]. Важно учитывать, что ИИ следует рассматривать в криминалистике как вспомогательный аналитический инструмент, т.е. его алгоритмы расширяют возможности экспертов, но без участия специалиста не могут самостоятельно квалифицировать доказательства. Принятие решения всегда должно оставаться за человеком, это основа, базовый принцип использования технологий ИИ. Однако необходимо обеспечить подготовку специалистов, способных максимально эффективно владеть и использовать эти технологии, интерпретировать результаты и критически оценивать выводы, сохраняя при этом и другие традиционные криминалистические навыки [8].

Активное внедрение искусственного интеллекта сопряжено с рядом этических рисков. Применение алгоритмов, анализирующих цифровые данные, обязано быть прозрачным и поддаваться проверке. Недопустимо выносить судебные или следственные вердикты, опираясь только на результаты работы машин, исключая человека из процесса принятия решения. В противном случае может быть нарушен один из базовых принципов уголовного судопроизводства – принцип личной ответственности за принимаемые решения [3]. Кроме того, в соответствии со статьей 75 УПК РФ, доказательства, полученные с нарушением закона, являются недопустимыми [9]. Это означает, что результаты работы ИИ должны быть не только технически корректны, но и получены в строгом соответствии с процессуальными требованиями, иначе они не могут быть положены в основу обвинения.

Усиление опасений по поводу конфиденциальности данных обусловлено способностью искусственного интеллекта собирать, анализировать и интерпретировать огромные массивы информации, включая личные сведения, финансовые отчеты и данные о перемещениях. Несанкционированный доступ к таким данным или их утечка могут привести к серьезным последствиям для частных лиц и организаций, включая кражу личных данных, финансовые потери и нанесение ущерба репутации. В связи с этим необходимо разработать строгие нормативные рамки и этические принципы, регулирующие применение искусственного интеллекта в криминалистике, с особым акцентом на защиту частной жизни и конфиденциальности. Согласно Национальной стратегии развития искусственного интеллекта на период до 2030 г. [6], ИИ представляет собой систему технологий, способную воспроизводить познавательные процессы человека (такие как обучение и поиск решений) и достигать результатов, не уступающих человеческим. Указанный комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (в том числе то, в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений.

Также, в соответствии со статьей 74 Уголовно-процессуального кодекса Российской Федерации, доказательствами по уголовному делу признаются любые фактические данные, полученные в установленном законом порядке [9]. Это означает, что результаты анализа, проведенного с применением ИИ, могут быть признаны доказательствами только при условии документирования всех этапов их получения и возможности их последующей экспертной проверки.

В перспективе планируется формирование единого государственного реестра сертифицированных систем анализа цифровых следов, что обеспечит унификацию процедур и минимизирует риски использования некорректных алгоритмов [1]. Такая стандартизация позволит гарантировать, что алгоритмы, используемые для сбора и обработки информации,



соответствуют установленным законом критериям, исключая тем самым возможность применения непроверенных или некорректных методов, способных исказить реальную картину событий. Разработка четких регламентов, определяющих, каким образом эти данные должны храниться, кто имеет к ним доступ, и в каких случаях они подлежат уничтожению, является первостепенной необходимостью. Это позволит предотвратить несанкционированный доступ, злоупотребление информацией и гарантировать соблюдение права граждан на конфиденциальность и защиту персональных данных.

Проведенный анализ демонстрирует, что искусственный интеллект стал неотъемлемым и важным инструментом в криминалистическом исследовании цифровых следов, что обусловлено цифровой трансформацией общества и показательным ростом объема и сложности данных. Использование ИИ позволяет преодолеть ограничения классических экспертных методов, обеспечивая автоматизированный анализ, выявление скрытых паттернов и установление связей в таких сферах, как кибермошенничество, организованная преступность и терроризм. Таким образом, для полноценного внедрения ИИ в уголовное судопроизводство требуется дальнейшее совершенствование нормативной базы, обеспечивающей баланс между эффективностью расследования и защитой прав граждан.

Список литературы:

1. Баранов П.П. Искусственный интеллект и цифровые доказательства в уголовном судопроизводстве / П. П. Баранов. — М.: Проспект, 2024. — 248 с.
2. Быстров А.П. Информационные технологии в доказательственном праве / А. П. Быстров. — М.: Юрлитинформ, 2024. — 212 с.
3. Дело о фишинговом мошенничестве в Санкт-Петербурге // Архив Следственного комитета РФ. — 2023. — № 4. — С. 14–17.
4. Криминалистика. Полный курс: учебник для вузов / под общей редакцией В. В. Агафонова, А. Г. Филиппова. — 6-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2025. 778 с.
5. Методические рекомендации по применению технологий искусственного интеллекта при анализе цифровых доказательств / МВД РФ. — М.: 2024. — 46 с.
6. О развитии искусственного интеллекта в Российской Федерации: Указ Президента РФ от 10.10.2019 № 490 (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») Электронный ресурс. (10 октября 2019 г. // Собрание законодательства. — 2019. — № 41. — Ст. 5700.) (дата обращения: 22.02.2026 г.)
7. Отчёт МВД РФ о состоянии преступности в сфере информационных технологий за 2024 год/ Электронный ресурс. — Режим доступа: <https://мвд.рф> (дата обращения: 22.02.2026)



8. Тюнис И. О., Анисимова А.М. Искусственный интеллект и цифровые технологии в криминалистике // Закон и право. 2025. № 3. С. 246–251. <https://doi.org/10.24412/2073-3313-2025-3-246-251> EDN: <https://elibrary.ru/YEEVXC> (дата обращения: 22.02.2026 г.)
9. Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 18 декабря 2001 г. № 174-ФЗ (в ред. от 30 декабря 2025 г.) // Собрание законодательства. — 2001. — № 52. — Ст. 4921. (дата обращения: 22.02.2026 г.)