Дата поступления рукописи в редакцию: 16.04.2026 г.
Дата принятия рукописи в печать: 14.05.2026 г.
DOI: 10.24412/2224-9133-2026-4-330-339

ШАГАПОВ Исаак Равильевич,
аспирант кафедры криминалистики Института права
ФГБОУ ВО «Уфимский Университет Науки и Технологий»,
г. Уфа, Российская Федерация,
e-mail: isa.shagapow@gmail.com

К ВОПРОСУ О КРИМИНАЛИСТИЧЕСКОЙ ТАКТИКЕ ИСПОЛЬЗОВАНИЯ СПЕЦИАЛЬНЫХ ЗНАНИЙ В СУДЕБНОЙ ЭКСПЕРТИЗЕ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация. *Стремительное развитие технологий искусственного интеллекта (далее – «ИИ») обусловило появление новых способов совершения преступлений, что создает серьезные вызовы для правоохранительной системы. Преступления с использованием ИИ характеризуются высокой степенью латентности, сложностью выявления следов преступной деятельности и необходимостью применения специализированных методов расследования. В статье рассматриваются особенности криминалистической тактики использования специальных знаний при производстве судебных экспертиз по данной категории дел.*

Исследование базируется на анализе следственной практики, изучении зарубежного опыта противодействия киберпреступности с применением ИИ-технологий.

Установлено, что традиционные подходы к назначению и производству экспертиз требуют существенной модификации применительно к преступлениям, совершаемым с использованием ИИ. Выявлены специфические проблемы: сложность интерпретации алгоритмов машинного обучения, необходимость междисциплинарного взаимодействия экспертов различных специальностей, потребность в новых методиках исследования цифровых следов.

Разработаны тактические рекомендации по оптимизации взаимодействия следователя с экспертами при расследовании данной категории преступлений, предложена система критериев отбора экспертов, обладающих необходимыми компетенциями в области ИИ-технологий. Обоснована необходимость создания специализированных экспертных подразделений и разработки унифицированных методических подходов к исследованию преступлений, совершенных с использованием ИИ.

Результаты исследования имеют практическое значение для совершенствования криминалистической тактики и методики расследования преступлений в сфере высоких технологий. Предложены конкретные меры по интеграции ИИ-инструментов в процедуры экспертного исследования, включая алгоритмы автоматического анализа цифровых следов, системы распознавания искусственно генерированного контента и методы выявления паттернов машинного обучения в криминальной деятельности. Исследование демонстрирует перспективность создания гибридных экспертных систем, сочетающих возможности ИИ с профессиональным опытом судебных экспертов. Разработанные рекомендации могут быть использованы при подготовке нормативно-правовых актов, регламентирующих применение ИИ-технологий в правоохранительной деятельности, а также при создании образовательных программ повышения квалификации экспертов.

Ключевые слова: *Специальные знания; судебная экспертиза; нейронные сети; социальная инженерия; синтетический контент; цифровые следы; цифровые преступления.*

SHAGAPOV Isaac Ravilevich,
Postgraduate student at the Criminalistics
Department of the Institute of Law,
Ufa University of Science and Technology,
Ufa, Russian Federation

ON THE ISSUE OF CRIMINALISTIC TACTICS OF USING SPECIAL KNOWLEDGE IN FORENSIC EXAMINATION IN THE INVESTIGATION OF CRIMES USING ARTIFICIAL INTELLIGENCE

Annotation. *The rapid development of artificial intelligence (AI) technologies has led to the emergence of new ways of committing crimes, which poses serious challenges to the law enforcement system. Crimes involving AI are characterized by a high degree of latency, the difficulty of detecting traces of criminal activity, and the need to use specialized investigative methods. The article discusses the features of criminalistic tactics of using special knowledge in the production of forensic examinations in this category of cases.*

The research is based on the analysis of investigative practice, the study of foreign experience in countering cybercrime using AI technologies.

It has been established that traditional approaches to the appointment and production of examinations require significant modification in relation to crimes committed using AI. Specific problems have been identified: the complexity of interpreting machine learning algorithms, the need for interdisciplinary interaction between experts from various specialties, and the need for new methods for investigating digital footprints.

Tactical recommendations have been developed to optimize the investigator's interaction with experts in the investigation of this category of crimes, and a system of criteria for selecting experts with the necessary competencies in the field of AI technologies has been proposed. The necessity of creating specialized expert units and developing unified methodological approaches to the investigation of crimes committed using AI is substantiated.

The results of the study are of practical importance for improving forensic tactics and methods of investigating crimes in the field of high technology. Specific measures are proposed to integrate AI tools into expert research procedures, including algorithms for automatic analysis of digital footprints, recognition systems for artificially generated content, and methods for detecting machine learning patterns in criminal activity. The study demonstrates the promise of creating hybrid expert systems that combine AI capabilities with the professional expertise of forensic experts. The developed recommendations can be used in the preparation of regulatory legal acts regulating the use of AI technologies in law enforcement, as well as in the creation of educational programs for advanced training of experts.

Key words: *Specialized knowledge; forensic science; neural networks; social engineering; synthetic content; digital footprints; digital crimes*.

Согласно статистике МВД России о преступности за последние пять лет, значительная часть преступлений в России совершается с использованием информационно-телекоммуникационных технологий (далее – «ИКТ») – более трети (40%) от общего числа зарегистрированных в России преступлений, что является максимумом удельного веса преступлений в период с 2020 года по настоящее время [23]. Как отмечалось Генеральным прокурором России на координационном совещании по вопросам противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей, цифровой валюты и компьютерной информации от 10 октября 2024 г., в основном, криминальные посягательства совершаются с помощью Интернета (526,8 тыс. в 2023 г. и 417,1 тыс. в 2024 г.) и средств мобильной связи (302,9 тыс. в 2023 г. и 231,9 тыс. в 2024 г.) [24].

Преступления, совершенные с использованием ИКТ или в сфере компьютерной информации представляют серьезную угрозу государственной и общественной безопасности, поскольку выражаются в нарушении целостности информационных систем, компрометации персональных данных граждан, дестабилизации работы критически важных объектов инфраструктуры, распространении недостоверной информации через цифровые каналы, а также в создании условий для совершения традиционных преступлений с использованием новых технологических возможностей. Особую опасность представляет использование искусственного интеллекта (далее – «ИИ») для автоматизации противоправных действий, создания поддельного контента высокого качества и обхода существующих систем защиты, что требует разработки адекватных правовых механизмов противодействия и соответствующего методического обеспечения правоохранительной деятельности.

Общим трендом в развитии российской преступности в сфере IT-технологий в период 2017 гг. – 2024 гг. стало заметное увеличение числа преступлений, совершенных с использованием ИКТ или в сфере компьютерной информации. Так, в 2024 г. по сравнению с 2017 г. общее количество зарегистрированных преступлений показало рост в 643% (с 90 587 в 2017 г. до 765 365 в 2024 г.) (*рис. 1*) [25].

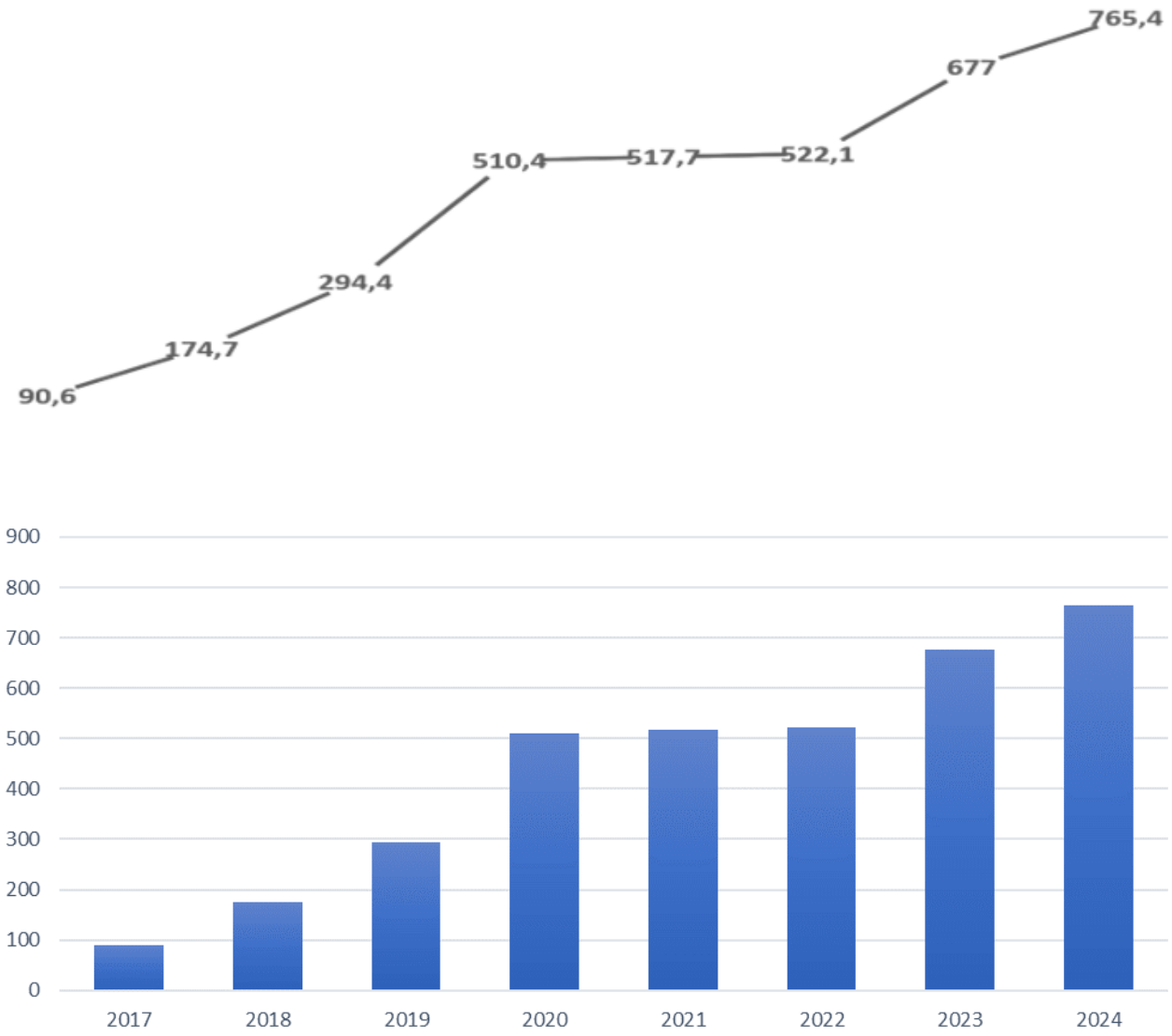


Рис. 1. Динамика преступлений, совершенных с использованием ИКТ или в сфере компьютерной информации

Fig. 1. Dynamics of crimes committed using ICT or in the field of computer information

Резюмируя вышеизложенное, рост преступлений, совершенных с использованием ИКТ, и сложность их предупреждения, выявления, расследования и раскрытия свидетельствуют о необходимости совершенствования системы противодействия киберпреступлениям. Противодействие преступлениям, совершаемым с использованием ИКТ представляет собой комплексную деятельность, что требует тесного взаимодействия государственных органов с общественностью и юридическими лицами, так или иначе связанными с вопросами обеспечения кибербезопасности [4, с. 58].

В рамках отечественной научной доктрины Л.В. Санина и В.В. Коломинов подмечают, что ИИ является не только новым инструментом цифровизации для просвещения граждан России и помощи в их деятельности, но и «оружием» злоумышленников для совершения киберпреступлений [16, с. 355]. Преступления с использованием ИИ представляют собой качественно новую подкатегорию в структуре преступлений, совершаемых с использованием ИКТ. ИИ являлся главной темой исследований в 2022–2023 гг., а также в период появления новых терминов, таких как большие языковые модели, дипфейки, виртуальная и дополненная реальность и иных [21, с. 453].

Согласно отчету Исследовательского центра «Аналитика. Бизнес. Право» (ABL) от 17 марта 2025 г. о результатах анализа судебной практики

в России за период 2021 гг. – 2024 гг., в части споров, где фигурирует ИИ, установлено, что количество дел, связанных с ИИ, стабильно растет год к году [26]. В 2021 г. число случаев правонарушений с использованием ИИ составляло 112 случаев, в 2024 г. их количество выросло до 292. Рост на 39% за 4 года связан с ростом киберпреступности, а также ростом нарушений закона в области интеллектуальной собственности и прав потребителей.

Отметим, что законодательное регулирование ИИ только формируется, поэтому многие споры могут просто не называть ИИ как способ совершения преступлений. Таким образом, актуальная статистика, вероятно, показывает лишь часть дел, так как многие случаи использования ИИ в противоправных целях могут оставаться невыявленными или квалифицироваться без упоминания его роли. Анализируя тенденции ИИ-преступлений, возможно выделить следующие (*рис. 2*) [27].



Рис. 2. Виды ИИ-преступлений: анализ тенденций (категории часто пересекаются)

Fig. 2. Types of AI crimes: trend analysis (categories often overlap)

Рассматривая указанную деятельность как дефиницию, определим, что под преступлением, совершенным с использованием ИИ, следует понимать применение алгоритмов машинного обучения, нейронных сетей и других технологий ИИ для совершения преступных деяний в сфере ИКТ. В современных реалиях обострения криминогенной обстановки, характеризующейся активизацией организованных преступных групп и возрастающими угрозами экстремистского и террористического характера, особую важность приобретает не только расследование уже совершенных преступлений, но и их профилактика с применением криминалистического инструментария. Соглашаясь с М.А. Иващенко, отметим, что сочетание ИИ с глобальной сетью открывает беспрецедентные перспективы для криминальных элементов [11, с. 22].

Как отмечают Ф.Г. Аминев, А.В. Чемерис и С.В. Хомутов, в последние годы значительно усовершенствованы методологические подходы к предупреждению противоправных деяний на основе специальных знаний [1, с. 506]. Параллельно с этим, цифровая трансформация судебно-экспертной сферы диктует необходимость пересмотра стандартов профессиональной подготовки экспертов-криминалистов в РФ, делая акцент на освоении современных ИКТ [2, с. 9].

Вместе с тем, государственные структуры, несмотря на традиционно более консервативный подход к технологическим инновациям, постепенно признают потенциал ИИ в решении застарелых проблем бюрократической эффективности и активно исследуют перспективы его внедрения [5, с. 6].

В данной связи, проанализируем характеристику применения специальных знаний в судебной экспертизе при исследовании некоторых преступлений, совершаемых с использованием ИИ в табличной форме (*таблица 1*).

Таблица 1. Применение специальных знаний в судебной экспертизе преступлений с использованием ИИ

Tab. 1. The use of specialized knowledge in the forensic examination of crimes using AI

№	Вид преступления с ИИ	Необходимые специальные знания	Методы экспертного исследования	Объекты исследования	Квалификация эксперта
1	Генерация дипфейков для мошенничества	Компьютерно-техническая экспертиза, анализ алгоритмов машинного обучения, цифровая криминалистика	Анализ метаданных, исследование артефактов генерации, сравнительный анализ с оригиналом	Видеофайлы, аудиозаписи, исходный код, модели ИИ	Специалист по компьютерной безопасности, эксперт в области цифровой обработки медиафайлов, эксперт по ИИ
2	Автоматизированные кибератаки с применением ИИ	Сетевая безопасность, анализ вредоносного ПО, архитектура ИИ-систем	Обратная инженерия кода, анализ сетевого трафика, поведенческий анализ алгоритмов	Логи, вредоносное ПО, сетевой трафик, алгоритмы	Эксперт по информационной безопасности, специалист по компьютерно-технической экспертизе
3	Использование ИИ для обхода систем защиты	Криптография, архитектура защитных систем, методы машинного обучения	Моделирование атак, анализ уязвимостей, исследование алгоритмов	Системы защиты, исходный код, алгоритмы ИИ	Криптоаналитик, специалист по защите информации, эксперт по машинному обучению
4	Фальсификация доказательств с помощью ИИ	Лингвистическая экспертиза, экспертиза документов, анализ генеративных моделей	Стилометрический анализ, проверка подлинности, сравнение с эталонами	Текстовые документы, изображения, синтезированные файлы	Лингвист, документовед, специалист по генеративным моделям ИИ
5	Манипуляция рынком с помощью алгоритмов ИИ	Финансовый анализ, экономическая экспертиза, анализ данных	Исследование торговых алгоритмов, анализ паттернов сделок, статистический анализ	Торговые алгоритмы, финансовые данные, журналы транзакций	Финансовый аналитик, экономист, специалист по алгоритмической торговле
6	Создание вредоносных ботов и ИИ-агентов	Поведенческий анализ, программирование, сетевые технологии	Анализ поведенческих паттернов, реверс-инжиниринг, сетевой анализ	Исходный код ботов, сетевой трафик, алгоритмы	Программист, сетевой аналитик, эксперт по искусственному интеллекту

Анализируя тенденции, нельзя не отметить укрепление феномена дипфейков, которые представляют собой созданные с помощью компьютерных алгоритмов аудиовизуальные материалы, достоверно имитирующие несуществующие в реальности события и процессы на основе подлинных образцов голоса и внешности человека. Современный уровень технологий затрудняет идентификацию подлинности видеоматериалов с изображением человека без экспертной оценки специалистов [13, с. 391].

Распространение нейротехнологий в преступной среде видоизменяет характер социоинженерных манипуляций, придавая им одновременно масштабность и индивидуальную направленность, а уязвимости робототехнических комплексов, особенно при использовании программ с открытым кодом, становятся плодородной почвой для кибернетических вторжений [10 с. 25, 12 с. 246, 14 с. 193]. В связи с этим, следственным органам необходимо привлекать междисциплинарные команды экспертов (специалистов по ИИ, кибербезопасности), разрабатывать методики идентификации цифровых следов в нейросетевых структурах, а также создавать правовые механизмы получения доступа к закрытым алгоритмам коммерческих систем, что существенно расширяет арсенал специальных знаний, необходимых для эффективного расследования высокотехнологичных преступлений.

Вполне обоснованно, что злоупотребление технологиями дипфейка квалифицируется как противозаконное деяние и подлежит уголовно-правовому преследованию. Иллюстрацией правового механизма противодействия служит ст. 272.1 УК РФ [28], устанавливающая наказание за неправомерные манипуляции с персональными данными и создание инфраструктуры для их нелегального распространения [3, с. 27].

Зарубежные исследователи отмечают, что особую тревогу вызывает применение дипфейк-технологий для создания обнаженных изображений, что представляет собой новую, технологически продвинутую форму сексуальной агрессии с использованием цифровых материалов [6, с. 1349, 22 с. 651]. Цифровые и компьютерные достижения сегодня превращаются в инструментарий преступной деятельности, формируя своеобразный симбиоз криминальных намерений человека и технологических возможностей.

Применение компьютерных технологий в данной категории деяний следует рассматривать как неотъемлемый элемент объективной стороны преступления, непосредственно связанного с использованием технологических средств [15, с. 109]. Полагаем, достаточно дискуссионным остаётся вопрос определения субъекта ответственности при совершении противоправных действий с применением ИИ.

В профессиональном сообществе отсутствует консенсус относительно того, должен ли владелец прав на нейросеть нести ответственность за созданный с её помощью контент. Проблема разграничения юридической ответственности между создателями и пользователями подобных технологий находится на стыке правовых и этических аспектов современной юриспруденции [7, с. 373].

В данном свете, заслуживает внимания инициатива А.В. Степановой о дополнении ст. 63 УК РФ положением об использовании ИИ как обстоятельстве, усиливающем наказание за совершённое деяние [17, с. 352].

Рассматривая некоторые вопросы криминалистической тактики использования специальных знаний при расследовании преступлений с использованием ИИ, в том числе, для целей судебной экспертизы, усматриваются следующие недостатки (*таблица 2*).

Таблица 2. Вопросы криминалистической тактики использования специальных знаний в судебной экспертизе при расследовании преступлений с использованием ИИ

Tab. 2. Issues of criminalistic tactics of using special knowledge in forensic examination in the investigation of crimes using AI

№	Вопрос	Сущность
1	Сложность интерпретации алгоритмов машинного обучения	Проблема оценки надежности и точности алгоритмов ИИ, используемых преступниками или при сборе экспертом цифровых доказательств. Отсутствие четких методологических подходов к оценке достоверности результатов работы моделей машинного обучения осложняет процесс доказывания. Эксперты не всегда обладают инструментарием для определения, был ли контент создан ИИ, модифицирован с его помощью или является подлинным.

2	Потребность в новых методиках исследования цифровых следов	Преступления с использованием ИИ формируют принципиально новые виды цифровых следов, которые традиционные криминалистические методики не способны эффективно выявлять и исследовать. Например, генеративные модели ИИ оставляют специфические артефакты, алгоритмические «отпечатки», которые требуют разработки особых инструментов и методов обнаружения. Цифровые следы, связанные с использованием ИИ, часто характеризуются повышенной изменчивостью, многослойностью и распределенностью. Указанные следы могут существовать одновременно на устройствах пользователей, серверах, в облачных сервисах, что требует комплексного подхода к их фиксации и изъятию.
3	Необходимость междисциплинарного взаимодействия экспертов различных специальностей	Эффективное расследование преступлений с использованием ИИ требует интеграции знаний из различных областей: информатики, криминалистики, лингвистики, психологии и других специальностей. Однако, существующая система подготовки судебных экспертов и организация экспертных учреждений часто не позволяют оперативно формировать междисциплинарные группы. Высокотехнологичная природа преступлений, совершаемых с использованием ИИ, требует от всех участников судопроизводства базового понимания принципов работы таких систем. Данное обстоятельство создает необходимость в новых образовательных программах, методических материалах и форматах взаимодействия между экспертами и правоприменителями, которые позволили бы эффективно транслировать сложные технические знания в юридический контекст.

Современные нейросети и алгоритмы глубокого обучения могут включать миллионы параметров, работающих одновременно, что делает практически невозможным восстановление цепочки логических решений, приведших к конкретному результату. Это создает серьезные препятствия для использования таких доказательств в суде, поскольку не соблюдается принцип проверяемости.

Для решения проблемы сложности интерпретации алгоритмов машинного обучения, предлагаем рассмотреть возможность развития направления «объяснимого ИИ», включая специализированные инструменты криминалистического аудита алгоритмов и создание стандартов документирования работы ИИ-систем. Важно обеспечить привлечение экспертов, специализирующихся на интерпретации моделей машинного обучения, способных объяснить суду в доступной форме принципы работы конкретного алгоритма и достоверность полученных с его помощью доказательств.

Вместе с тем, традиционные методы криминалистического исследования оказываются недостаточными при анализе цифровых следов, связанных с использованием ИИ. Изучение технических принципов и механизмов создания дипфейков позволит обнаружить уязвимости в этой технологии, что повысит эффективность выявления и расследования соответствующих преступлений [19, с. 238]. Модели генерации дипфейков непрерывно совершенствуются при одновременном повышении качества синтезируемого контента. Потребность правоохранительных структур в методах идентификации подобных технологий обуславливает необходимость разработки специальных методик противодействия неправомерному использованию этих достижений ИИ.

Современная эпоха развития ИИ и нейросетевых технологий характеризуется не только появлением принципиально новых методов мошенничества, но и трансформацией традиционных способов неправомерного доступа к информации и материальным ценностям [8, с. 290]. Текущие тенденции в сфере создания «фейковых новостей», ведения информационных войн в онлайн-пространстве, а также расширяющееся применение ботов и ИИ в криминальной среде требуют разработки аналитических инструментов, способных эффективно выявлять пропагандистские методики и идентифицировать связанные с ними идеологические конструкты [9, с. 563].

Преступления с применением ИИ генерируют особый тип цифровых артефактов: уникальные паттерны вычислений, специфические метаданные обработки информации, следы взаимодействия различных алгоритмов. Существующие методики не позволяют эффективно идентифи-

цировать, фиксировать и исследовать такие следы, что снижает эффективность расследования. Решение данной проблемы требует разработки новой методологической базы, включающей алгоритмы обнаружения признаков применения ИИ в цифровых данных, методы анализа информационных потоков в нейросетевых структурах и специализированные программные инструменты для визуализации скрытых взаимосвязей. Особое внимание следует уделить методикам идентификации дипфейков, синтезированных текстов и изображений, а также выявлению следов модификации данных с помощью генеративных алгоритмов.

Рассматривая вопрос обеспечения междисциплинарного взаимодействия экспертов различных специальностей, представляется перспективным внедрение междисциплинарных экспертных групп, работающих по специально разработанным протоколам взаимодействия. Иными словами, формирование новой экспертной специализации – криминалиста-аналитика в сфере ИИ, обладающего компетенциями на стыке различных наук. Важным элементом является также разработка специализированных образовательных программ и курсов повышения квалификации для следователей, экспертов и судей, позволяющих понимать специфику преступлений с использованием ИИ и эффективно применять специальные знания при их расследовании.

Криминалистическая наука изначально формировалась как дисциплина, интегрирующая достижения различных областей знания – математики, физики, химии, биологии, медицины и информатики, в целях противодействия преступности. Следовательно, представляется целесообразным интегрировать технологии ИИ в арсенал средств криминалистики для борьбы с правонарушениями. Системы ИИ способны значительно повысить эффективность работы правоохранительных органов, выступая в качестве вспомогательного инструмента, но не замены человеческого фактора.

Потенциал нейросетевых архитектур в анализе криминалистических ситуаций и формировании обоснованных следственных версий также весьма закономерен, однако, нормативные рамки их применения в расследовании преступлений пока не определены. Критически важным представляется обеспечение качественного обучения нейросетей использованию современного криминалистического инструментария, предшествующего внедрению ИИ в практическую деятельность следственных органов [18, с. 28].

В структуре риск-менеджмента экспертных лабораторий целесообразно сформировать отдельное направление исследования рисков применения технологий ИИ в экспертной работе [20, с. 19]. Указанное потребует выявления специфических угроз, обусловленных несовершенством алгоритмов машинного обучения и недостатками информационных массивов, используемых системами ИИ. Целесообразным представляется первоначальное внедрение исключительно алгоритмов контролируемого обучения (с учителем) как способ минимизации рисков.

Таким образом, настоящее исследование подтверждает, что преступления, совершаемые с использованием ИКТ, представляют значительную угрозу национальной безопасности России. В рамках данной категории преступлений выделяется новая подкатегория – противоправные деяния с использованием ИИ, которые демонстрируют стабильный рост. Представляется, что сложность выявления, фиксации и исследования цифровых следов преступлений с использованием ИИ обусловлена тремя ключевыми факторами: проблемой интерпретации алгоритмов машинного обучения, недостаточностью методик исследования специфических цифровых следов и отсутствием эффективного междисциплинарного взаимодействия экспертов различных специальностей, в связи с чем, автором были предложены соответствующие пути решения.

Список литературы:

[1] Аминев Ф.Г., Чемерис А.В., Хомутов С.В. «О потенциале всеобщей геномной регистрации в предупреждении преступлений» // Всероссийский криминологический журнал. 2022. № 4. С. 505-511.

[2] Аминев Ф.Г. О проблемах формирования компетентности судебного эксперта в условиях цифровизации // Криминологический журнал. 2024. № 1. С. 9-12.

[3] Архиереев Н.В. Правовое регулирование создания и использования дипфейков // Правовое государство: теория и практика. 2025. № 2 (80). С. 22-30.

[4] Астахова Е.А. Перспективы противодействия использованию информационно-коммуникационных технологий в преступных целях // Правовая политика и правовая жизнь. 2025. № 1. С. 56–64.

[5] Adams I.T., Barter M., McLean K. et al. No man's hand: artificial intelligence does not improve police report writing speed. J. Exp. Criminol. 2024. pp. 1-18.

[6] Asher Flynn, Anastasia Powell, Adrian J. Scott, Elena Cama, Deepfakes and Digitally Altered Imagery Abuse: A Cross-Country Exploration of an Emerging form of Image-Based Sexual Abuse, The British Journal of Criminology. 2022. Volume 62. pp. 1341–1358.

[7] Вашеняк Н.Е. Сложные правовые аспекты, связанные с использованием искусственного интеллекта // Вестник науки. 2023. № 12 (69). С. 371-377.

[8] Гладких И.Н., Фомичев Д.С. К вопросу об особенностях применения искусственного интеллекта при раскрытии мошеннических преступлений // Право и управление. 2024. № 4. С. 289-292.

[9] Deborah H. Drake, Reece Walters, Mark Wood, Greg Koumouris, Criminology and Propaganda Studies: Charting New Horizons in Criminological Thought, The British Journal of Criminology, Volume 64, Issue 3, May 2024, pp. 558–575.

[10] Зотина Е.В. Мошенничество с использованием информационно-телекоммуникационных технологий и приемов социальной инженерии: криминологическое исследование : автореф. дис. ... канд. юрид. наук. М., 2024. 33 с.

[11] Иващенко М.А. Новые формы организованной преступности : автореф. дис. ... канд. юрид. наук. М., 2022. 35 с.

[12] Кийко Д.С. Автономные роботы как угроза и инструмент защиты жертв преступлений // Виктимология. 2025. № 2. С. 243-249.

[13] Морозова И.Г. К вопросу о необходимости правового регулирования дипфейков // Право и государство: теория и практика. 2025. № 2. С. 390-392.

[14] Мочалкина И.С. Криминологическое противодействие экономическим преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий // Вестник Университета имени О.Е. Кутафина. 2025. № 5 (129). С. 189-196.

[15] Перина А.С. «Цифровые преступления»: понятие, типология, признаки // Юридический вестник Самарского университета. 2023. № 3. С. 106-115.

[16] Санина Л.В., Коломинов В.В. Особенности расследования мошенничества, совершенные с помощью искусственного интеллекта // Право и государство: теория и практика. 2024. № 8 (236). С. 355-359.

[17] Степанова А. В. Взаимосвязь искусственного интеллекта как средства совершения преступления и иных субъективных признаков состава преступления // Образование и право. 2021. № 5. С. 349-355.

[18] Хамидуллин Р.С. Криминалистическое обеспечение использования технологии искусственного интеллекта в раскрытии и расследовании преступлений // Электронное приложение к Российскому юридическому журналу. 2024. № 2. С. 19-29.

[19] Шепель Н.В., Янгаева М.О. Использование возможностей искусственного интеллекта при создании дипфейков // Вестник Сибирского юридического института МВД России. 2024. № 4 (57). С. 233-239.

[20] Шихалиева С.З. Судебные экспертизы объектов в цифровой форме: прогнозирование и профилактика экспертных ошибок : автореф. дис. ... канд. юрид. наук. Москва, 2025. 32 с.

[21] Dunaeva, Y. Digital Evolution of Universities: Neural Networks in Education. In: Bolgov, R., et al. Proceedings of Topical Issues in International Political Geography (TIPG 2023). TIPG 2022. Springer Geography. Springer, Cham. pp. 453-463.

[22] Sidsel Kirstine Harder, Re-faced and Pornified— A Visual, Narrative Analysis of Sexual Scripts in Police Cases of Image-based Abuse, The British Journal of Criminology, Volume 63, Issue 3, May 2023, pp. 651–667.

[23] Состояние преступности в России за период 2020-2025 гг.// Министерство внутренних дел Российской Федерации. URL: https://мвд.рф/reports (дата обращения: 24.09.2025).

[24] Координационное совещание по вопросам противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей, цифровой валюты и компьютерной информации от 10 октября 2024 г. // Официальный сайт Генеральной прокуратуры Российской Федерации. URL: https://epp.genproc.gov.ru/web/gprf/mass-media/news?item=98418092 (дата обращения: 24.09.2025).

[25] Состояние преступности в России за период 2017-2024 гг.// Министерство внутренних дел Российской Федерации. URL: https://мвд.рф/reports (дата обращения: 24.09.2025).

[26] Публикация Исследовательского центра «АБП» (ABL) от 17 марта 2025 г. о количестве судебных дел, связанных с искусственным интеллектом // Информационное агентство «РБК». URL: https://companies.rbc.ru/news/XpHsgaQhNg/kolichestvo-sudebnyih-del-svyazannyih-s-ii-vyiroslo-na-39-za-4-goda/ (дата обращения: 24.09.2025).

[27] Уголовная ответственность за новые преступления, совершаемые с использованием информационно-телекоммуникационных технологий // Официальный сайт прокуратуры Республики Коми. URL: https://epp.genproc.gov.ru/web/gprf/mass-media/news?item=98418092 (дата обращения: 24.09.2025).

[28] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63 (с посл. изм. и доп. от 31 июля 2025 г. № 282-ФЗ) // Официальный интернет-портал правовой информации [Электронный ресурс]. Режим доступа: http://www.pravo.gov.ru/ (дата обращения: 16.09.2025).

References:

[1] Aminev FG, Chemeris A.V., Khomutov S.V. “On the potential of universal genomic registration in crime prevention “//All-Russian Criminological Journal. 2022. № 4. S. 505-511.

[2] Aminev F.G. On the problems of forming the competence of a forensic expert in the context of digitalization//Criminological Journal. 2024. № 1. S. 9-12.

[3] Bishop N.V. Legal regulation of the creation and use of deepfakes//Legal state: theory and practice. 2025. № 2 (80). S. 22-30.

[4] Astakhova E.A. Prospects for countering the use of information and communication technologies for criminal purposes//Legal policy and legal life. 2025. № 1. S. 56-64.

[5] Adams I.T., Barter M., McLean K. et al. No man's hand: artificial intelligence does not improve police report writing speed. J. Exp. Criminol. 2024. pp. 1-18.

[6] Asher Flynn, Anastasia Powell, Adrian J. Scott, Elena Cama, Deepfakes and Digitally Altered Imagery Abuse: A Cross-Country Exploration of an Emerging form of Image-Based Sexual Abuse, The British Journal of Criminology. 2022. Volume 62. pp. 1341–1358.

[7] Washeniak N.E. Complex legal aspects related to the use of artificial intelligence//Bulletin of Science. 2023. № 12 (69). PP. 371-377.

[8] Gladkikh I.N., Fomichev D.S. On the peculiarities of the use of artificial intelligence in solving fraudulent crimes//Law and management. 2024. № 4. S. 289-292.

[9] Deborah H. Drake, Reece Walters, Mark Wood, Greg Koumouris, Criminology and Propaganda Studies: Charting New Horizons in Criminological Thought, The British Journal of Criminology, Volume 64, Issue 3, May 2024, pp. 558–575.

[10] Zotina E.V. Fraud using information and telecommunication technologies and social engineering techniques: criminological research: author's abstract. dis.... cand. jurid. sciences. M., 2024. 33 pp.

[11] Ivaschenko M.A. New forms of organized crime: author's review. dis.... cand. jurid. sciences. M., 2022. 35 p.

[12] Kiyko D.S. Autonomous robots as a threat and tool to protect victims of crime//Victimology. 2025. № 2. S. 243-249.

[13] Morozova I.G. On the need for legal regulation of deepfakes//Law and state: theory and practice. 2025. № 2. S. 390-392.

[14] Mochalkina I.S. Criminological counteraction to economic crimes committed using information and telecommunication technologies// Bulletin of the University named after O.E. Kutafin. 2025. № 5 (129). S. 189-196.

[15] Perina A.S. "Digital crimes": concept, typology, signs//Legal Bulletin of Samara University. 2023. № 3. S. 106-115.

[16] Sanina L.V., Kolominov V.V. Features of the investigation of fraud committed using artificial intelligence//Law and State: Theory and Practice. 2024. № 8 (236). S. 355-359.

[17] Stepanova A. V. Relationship of artificial intelligence as a means of committing a crime and other subjective signs of corpus delicti//Education and law. 2021. № 5. S. 349-355.

[18] Khamidullin R.S. Forensic support for the use of artificial intelligence technology in the disclosure and investigation of crimes//Electronic Appendix to the Russian Legal Journal. 2024. № 2. S. 19-29.

[19] Shepel N.V., Yangaeva M.O. Using the capabilities of artificial intelligence when creating deepfakes//Bulletin of the Siberian Law Institute of the Ministry of Internal Affairs of Russia. 2024. № 4 (57). S. 233-239.

[20] Shikhalieva S.Z. Forensic examinations of objects in digital form: forecasting and prevention of expert errors: author's review. dis.... cand. jurid. sciences. Moscow, 2025. 32 pp.

[21] Dunaeva, Y. Digital Evolution of Universities: Neural Networks in Education. In: Bolgov, R., et al. Proceedings of Topical Issues in International Political Geography (TIPG 2023). TIPG 2022. Springer Geography. Springer, Cham. pp. 453-463.

[22] Sidsel Kirstine Harder, Re-faced and Pornified— A Visual, Narrative Analysis of Sexual Scripts in Police Cases of Image-based Abuse, The British Journal of Criminology, Volume 63, Issue 3, May 2023, pp. 651–667.

[23] The state of crime in Russia for the period 2020-2025//Ministry of Internal Affairs of the Russian Federation. URL: https://мвд.рф/reports (access date: 24.09.2025).

[24] Coordination meeting on countering crimes committed using information and telecommunication networks, digital currency and computer information dated October 10, 2024//Official website of the Prosecutor General's Office of the Russian Federation. URL: https://epp.genproc.gov.ru/web/gprf/mass-media/news?item=98418092 (access date: 24.09.2025).

[25] The state of crime in Russia for the period 2017-2024//Ministry of Internal Affairs of the Russian Federation. URL: https://мвд.рф/reports (access date: 24.09.2025).

[26] Publication of the ABP Research Center (ABL) dated March 17, 2025 on the number of court cases related to artificial intelligence//RBC News Agency. URL: https://companies.rbc.ru/news/XpHsegaQhNg/kolichestvo-sudebnyih-del-svyazannyih-s-ii-vyiroslo-na-39-za-4-goda/ (дата обращения: 24.09.2025).

[27] Criminal liability for new crimes committed using information and telecommunication technologies//Official website of the Prosecutor's Office of the Komi Republic. URL: https://epp.genproc.gov.ru/web/gprf/mass-media/news?item=98418092 (access date: 24.09.2025).

[28] Criminal Code of the Russian Federation of June 13, 1996 No. 63 (from the last rev. and add. dated July 31, 2025 No. 282-FZ)//Official Internet portal of legal information [Electronic resource]. Access mode: http://www.pravo.gov.ru/ (access date: 16.09.2025).