

КРИМИНАЛИСТИКА, СУДЕБНО-ЭКСПЕРТНАЯ ДЕЯТЕЛЬНОСТЬ, ОПЕРАТИВНО-РАЗЫСКНАЯ ДЕЯТЕЛЬНОСТЬ

CRIMINALISTICS; FORENSIC EXPERT ACTIVITY; OPERATIONAL INVESTIGATIONS

Научная статья

УДК 343.98

DOI 10.33184/vest-law-bsu-2026.31.12

Василевская Дарья Владимировна

Московский государственный юридический университет

имени О.Е. Кутафина (МГЮА), Москва, Россия,

dvvasilevskaya@msal.ru,

<https://orcid.org/0000-0003-0263-7550>

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СУДЕБНОЙ КОМПЬЮТЕРНО-ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЕ

Аннотация. Сегодня технологии искусственного интеллекта (ИИ) широко внедряются в самые разные сферы общественной жизни, включая правоохранительную деятельность. Их применение становится необходимым условием успешной борьбы с преступностью, поскольку сама преступность значительно трансформируется под влиянием возможностей ИИ как средства реализации преступного умысла. Прогрессивно растущий объём компьютерной информации делает практически невозможным расследование преступлений, совершённых с помощью информационных технологий без автоматизации процессов обработки данных и выявления в них паттернов, свидетельствующих о преступной деятельности. Такая автоматизация может быть реализована через технологии ИИ.

Цель статьи: рассмотреть мировую практику применения различных технологий искусственного интеллекта для решения задач судебной компьютерно-технической экспертизы и последующего расследования преступлений, совершённых с помощью информационных технологий. Результаты: выявлены наиболее целесообразные архитектуры нейросетей для работы с различными классами задач СКТЭ: анализом сетевого трафика, обнаружением и классификацией вредоносного ПО, анализом поведенческих паттернов пользователя, установлением последовательности событий, обработкой естественного языка, в том числе, анализом переписок, работой с видеофайлами и изображениями и др. Также определены основные ограничения применения технологий ИИ в СКТЭ и приведены наиболее перспективные направления их внедрения.

Ключевые слова: судебная компьютерно-техническая экспертиза, искусственный интеллект, нейросеть, машинное обучение, обучение нейросети, датасет, компьютерные преступления

Для цитирования: Василевская Д.В. Применение технологий искусственного интеллекта в судебной компьютерно-технической экспертизе / Д.В. Василевская. – DOI 10.33184/vest-law-bsu-2026.31.12 // Вестник Института права Башкирского государственного университета. – 2026. – № 3. – С. 155–172.

Original article

Vasilevskaya Daria Vladimirovna

Kutafin Moscow State Law University (MSAL), Moscow, Russia,
dvvasilevskaya@msal.ru, <https://orcid.org/0000-0003-0263-7550>

THE ARTIFICIAL INTELLIGENCE TECHNOLOGIES APPLICATION IN DIGITAL FORENSICS

Abstract. Today, artificial intelligence (AI) technologies are widely integrated into various spheres of public life, including law enforcement. Their use has become a prerequisite for successful crime control since crime itself is significantly transformed under the influence of AI capabilities as a means of implementing criminal intent. The progressively growing volume of computer information makes it impossible to investigate crimes committed with the use of information technologies without automating data processing and identifying patterns indicative of criminal activity. Such automation can be achieved through AI technologies. The purpose of the article is to examine global practice in applying various AI technologies to solve the tasks of forensic computer expertise and the subsequent investigation of crimes committed with the use of information technologies. Results: the most appropriate neural network architectures for working with different classes of digital forensic tasks are identified: network traffic analysis, detection and classification of malicious software, analysis of user behavioral patterns, establishing event sequences, natural language processing (including the analysis of messages), working with video files and images and others. The main limitations of applying AI technologies in digital forensics are also outlined and the most promising directions for their implementation are presented.

Keywords: digital forensics, artificial intelligence, neural network, machine learning, neural network training, dataset, computer crimes

For citation: Vasilevskaya D.V. The Artificial Intelligence Technologies Application in Digital Forensics. *Vestnik Instituta prava Bashkirskogo gosudarstvennogo universiteta* = *Bulletin of the Institute of Law of the Bashkir State University*, 2026, no. 3, pp. 155–172. (In Russian). DOI 10.33184/vest-law-bsu-2026.31.12

Введение. Одним из главных трендов современной науки является исследование искусственного интеллекта, цифровизации общества, а также возможностей и проблем, которые обусловлены природой и повсеместным внедрением новых технологий. Науки криминалистики и судебной экспертологии не являются исключением. Отечественные и зарубежные учёные рассматривают различные аспекты применения технологий искусственного интеллекта (далее «ИИ») в расследовании преступлений и судебной экспертизе [1, с. 61–62]. Успешное расследование высокотехнологичных преступлений становится невозможным без сложных судебно-экспертных исследований, подразумевающих анализ большого объёма разрозненных данных. Несмотря на то, что потенциал ИИ колоссален для большинства судебных экспертиз, особенного внимания заслуживает рассмотрение вопроса о его применении в первую очередь в рамках судебной компьютерно-технической экспертизы (далее СКТЭ).

Как отмечают ведущие специалисты в области судебной экспертизы [2, с. 77; 3, с. 7–8], возникновение и развитие различных родов и видов экспертиз, в том числе СКТЭ, неразрывно связаны с развитием отдельных отраслей науки и техники и во многом определяются ими, поскольку, с одной стороны, технический прогресс ведёт к появлению новых способов совершения преступлений, новых объектов исследования, а, значит, и общественного заказа на новые виды экспертиз, а с другой – предопределяет те инструменты и методы, которыми они будут производиться. Следовательно, закономерности развития информационных технологий непосредственно определяют закономерности развития как судебной экспертологии в целом, так и отдельных её родов и видов.

СКТЭ неразрывно связана с технологиями искусственного интеллекта по ряду причин. Прежде всего, информационные технологии во всём их многообразии, включая ИИ, выступают непосредственным объектом исследования судебной компьютерно-технической экспертизы. Во-вторых, постоянная эволюция таких технологий ведёт к качественному усложнению способов и средств совершения преступлений, росту их количества, увеличению разнообразия объектов экспертного исследования наряду с экспоненциальным ростом объёма цифровой информации. Всё это приводит, с одной стороны, к росту общественного заказа на проведение исследований в области СКТЭ [4, с. 19], а с другой – к тому, что обработка имеющегося массива данных «вручную» становится непосильной для человека. Технологии ИИ дают возможность значительно сократить временные затраты на проведение экспертизы. Так, один из протестированных инструментов ИИ сократил время работы с данными до 93 % [5, с. 4]. Кроме того, традиционные методы СКТЭ не дают надлежащего инструментария для работы со сложными массивами данных, возникающими в результате фрагментации по различным платформам, облачным хранилищам и пр. Собрать из таких данных общую картину, установить последовательность действий или скрытый паттерн без автоматизированных инструментов невозможно. При этом в условиях объективной необходимости применения ИИ в СКТЭ на

сегодняшний день отсутствуют апробированные методики и системное правовое регулирование.

Таким образом, тогда как для остальных родов и видов экспертиз ИИ является вспомогательным инструментом для проведения исследований, в рамках СКТЭ специфика объекта делает ИИ и объектом, и средством исследований, а кроме того, предопределяет объективную необходимость его внедрения.

Цель данного исследования – рассмотреть существующие возможности применения ИИ для решения задач СКТЭ в мировой практике. Оценить правовые и методологические риски использования таких инструментов в правоохранительной деятельности, а также определить перспективные направления их применения.

Искусственный интеллект и его применение в СКТЭ. Поскольку искусственный интеллект – сложное и развивающееся явление, затрагивающее самые разные сферы общественной жизни, на сегодняшний день мировое сообщество не пришло к его единому понятию ни с юридических, ни с технических позиций.

Зарубежные правовые порядки избегают широкого понятия ИИ и определяют его через «машинную систему»^{1,2}. Отечественный законодатель определяет искусственный интеллект шире. Так, Национальная стратегия развития искусственного интеллекта закрепляет следующее понятие: искусственный интеллект – комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека или превосходящие их. Комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (в том числе, в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений³. Более широкое понятие ИИ в данном случае обосновано тем, что Российская Федерация стремится к быстрому внедрению технологий ИИ в различные отрасли общественной жизни для обеспечения государственной безопасности и конкурентоспособности, что непосредственно нашло свое отражение в положениях Стратегии⁴. Несмотря на то, что судебно-экспертная деятельность не упоминается непосредственно в документе, мы полагаем, что по общему смыслу Стратегии это одно из приоритетных направлений внедрения технологий ИИ, поскольку количество, качество и скорость исполнения судебно-экспертных исследований непосредственно сказываются на уровне правоохранительной деятельности и национальной безопасности.

¹ National Artificial Intelligence Initiative Act of 2020 [Электронный ресурс] // URL: <https://www.govtrack.us/congress/bills/116/hr6216/text> (дата обращения: 06.05.2026).

² EU Artificial Intelligence Act [Электронный ресурс] // URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689> (дата обращения: 06.05.2026).

³ Национальная стратегия развития искусственного интеллекта на период до 2030 г.: утв. Указом Президента РФ от 10.10.2019 № 490 // Собрание законодательства РФ. – 2019. – № 41. – Ст. 5700 [Электронный ресурс] // URL: <http://www.kremlin.ru/acts/bank/44731> (дата обращения: 05.05.2026).

⁴ Там же. Подп. д, е, з п. 24.

С технической точки зрения искусственный интеллект представляет собой обширную экспериментальную междисциплинарную область знания, охватывающую математику, компьютерные науки, программирование, статистику, лингвистику, целью которой является алгоритмизация решения тех задач, которые на данном этапе научно-технического прогресса доступны только человеческому разуму [6, с. 36]. Или иными словами – создание интеллектуальных машин [7, с. 6]. Функционирование таких машин обеспечивается совокупностью технических решений и концепций. На данном этапе – это машинное обучение (и глубокое обучение), нейросети, компьютерное зрение, обработка естественного языка и др. В ходе дальнейшего развития технологий средства, с помощью которых искусственный интеллект решает поставленные перед ним задачи, продолжают эволюционировать, а общая идея – «создание интеллектуальных машин» или имитация человеческого разума – останется той же.

Сегодня выделяют три вида искусственного интеллекта: узкий (или слабый) ИИ (ANI), общий (или сильный) ИИ (AGI) и суперинтеллект (ASI).

Узкий ИИ (ANI) – это то, с чем мы непосредственно имеем дело на данном этапе развития технологий. Информационные системы⁵ этого типа фокусируются на решении конкретных задач в рамках конкретно заданных параметров. В силу большого объёма изученных данных часто такой ИИ может решать поставленную задачу гораздо быстрее и точнее человека. Однако он не обладает автономностью, не может выйти за рамки заданного алгоритма, а значит, если он был обучен на некачественных данных, то ошибки неизбежны.

Уровни общего и суперинтеллекта на сегодняшний день не достигнуты. Предполагается, что общий ИИ будет означать, что машина обладает интеллектом, неотличимым от человеческого: она будет способна к творчеству и воображению, долгосрочной памяти и самосознанию.

Суперинтеллект – это высшая форма развития ИИ. На этом этапе машинный интеллект будет превосходить человеческий по всем параметрам. Предполагается, что если человечество достигнет этой точки, то суперинтеллект сможет, среди прочего, решить глобальные проблемы и ответить на извечные философские вопросы. Однако такой уровень самосознания машины небеспопечно вызывает множество опасений и этических дебатов. Отметим, что сегодня это только гипотетические вопросы будущего и любые подобные рассуждения носят исключительно умозрительный характер. Однако уже сегодня при разработке и регулировании технологий искусственного интеллекта одним из базовых принципов выступает риск-ориентированный подход для оценки соотношения преимуществ и рисков, связанных с конкретной технологией⁶.

⁵ П. 3 ст. 2 ФЗ от 27.07.2006 № 149-ФЗ: Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств // Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 05.05.2026).

⁶ Национальная стратегия развития искусственного интеллекта на период до 2030 г.: утв. Указом Президента РФ от 10.10.2019 № 490 // Собрание законодательства РФ. – 2019. – № 41. – Ст. 5700 [Электронный ресурс] // URL: <http://www.kremlin.ru/acts/bank/44731> (дата обращения: 05.05.2026).

Итак, в том, что касается практического применения ИИ, в частности, в области СКТЭ, на данный момент речь идет исключительно о технологиях узкого ИИ. Рассмотрим подробнее его структуру и возможности.

Машинное обучение – это область технологий, обеспечивающая функционирование искусственного интеллекта через разработку алгоритмов обучения компьютеров на больших массивах данных. Оно родилось в 1959 г. в IBM, когда Артур Сэмюел написал компьютерную программу для игры в шахматы, способную к самообучению [8, с. 3]. Такое обучение сегодня позволяет компьютерам строить прогнозы и принимать решения. Принципиальное отличие этого процесса от классической компьютерной программы состоит в том, что система следует не строго заданному алгоритму, а именно учится выявлять некие объекты или закономерности на примере представленного ей набора данных, и, следовательно, инженер машинного обучения на старте не знает, к какому именно результату придёт компьютер при решении той или иной задачи. Машинное обучение нашло самое разное применение в мировой практике СКТЭ за последние 10 лет. Оно используется для обнаружения и восстановления утраченных данных [9], триажа устройств и уязвимостей [10], для обнаружения подозрительной активности или потенциально криминальных паттернов в компьютерных сетях [11] и др.

Машинное обучение происходит с помощью нейросетей, состоящих из искусственных нейронов. Отдельно взятый нейрон – это функция, обрабатывающая входящие данные по определённой схеме⁷. Архитектуры и конфигурации⁸ современных нейросетей очень многообразны и постоянно усложняются, поскольку растёт сложность (глубина) нейросетей, а также объёмы обрабатываемых данных и вычислительные мощности. В результате очень быстро растёт и точность нейросетей. Чем больше нейронов и чем объёмнее массив данных, на которых обучается нейросеть, тем эффективнее она работает. Качество данных также непосредственно влияет на результаты работы технологий ИИ.

Для реализации машинного обучения данные в том виде, в каком они воспринимаемы человеком, должны быть переведены в абстракцию, пригодную для понимания и обработки системой. Одни и те же исходные данные, будь то текст, изображение, видео- или аудиофайл, могут быть представлены в

⁷ Описание хода обучения нейросетей рассмотрено многими отечественными и зарубежными специалистами в области информатики и машинного обучения. За более подробной информацией о ходе и математической составляющей обучения нейросетей, см. например, Вьюгин В.В. «Математические основы теории машинного обучения и прогнозирования» / В.В. Вьюгин. – М.: 2013. – 387 с.; Воронцов К.В. Машинное обучение: курс лекций [Электронный ресурс] // URL: http://www.machinelearning.ru/wiki/index.php?title=Машинное_обучение_%28курс_лекций%2C_К.В.Воронцов%29 (дата обращения: 06.05.2026); Основы машинного обучения [Электронный ресурс] // URL: <https://deepmachinelearning.ru/docs/Machine-learning/Base-concepts> (дата обращения: 06.05.2026).

⁸ Архитектура и конфигурация нейронной сети – это общие принципы её построения, а именно количество нейронов, тип связи между ними, активационные функции, количество слоев и пр.

качестве разного набора признаков: категориально, порядково или количественно. Так, например, для обработки текста с целью классификации может быть использован метод «мешок слов», который предполагает репрезентацию текста в виде модели, описывающей количество слов в нём. Тот же текст для работы со свёрточной нейронной сетью может быть представлен как изображение в виде последовательности векторов, соответствующих словам или словам. Таким образом, нет универсального способа работы с определённым видом данных, но есть архитектуры и инструменты, наилучшим образом заточенные под решение определённых задач.

Обобщённая мировая практика применения технологий ИИ в компьютерно-технической экспертизе свидетельствует о том, что они наиболее широко применяются при решении следующих классов задач:

1. Анализ сетевого трафика и обнаружение аномалий в нём, а именно выявление атак, бот-сетей, анализ поведенческих паттернов и временных рядов;
2. Обработка естественного языка, в том числе анализ переписок, выявление фишинговых писем и сгенерированных текстов;
3. Автоматическое обнаружение и классификация вредоносного ПО;
4. Анализ изображений и видео, в том числе для классификации объектов, обнаружения *deepfake* и манипуляций, установления визуальных паттернов.

Классической архитектурой для решения первых трёх классов задач являются рекуррентные нейронные сети (RNN) [12, с. 52–53], в частности нейронные сети с краткосрочной памятью (LSTM) [13, с. 2; 14].

Рекуррентные нейронные сети – это вид нейросетей, позволяющих обрабатывать серии событий во времени, их последовательности. Преимущество рекуррентных сетей состоит в том, что благодаря тому, что они содержат обратные связи между элементами, они способны сохранять информацию, то есть фактически её запоминать. LSTM – разновидность архитектуры рекуррентных нейронных сетей, способная к запоминанию информации на значительные периоды времени. Нейронные сети этого типа могут устанавливать последовательность событий во времени и работать с временными рядами, обнаруживать разного рода паттерны в сетевом потоке [15, с. 1–2], в том числе, признаки вредоносного ПО [16] и атак на информационные системы [17].

Для анализа сетевого трафика и обнаружения аномалий в нём ещё одним распространенным инструментом является автоэнкодер. Этот тип нейросетей является базовым инструментом машинного обучения. Автоэнкодеры кодируют данные в более компактный объект, чем исходный массив, а потом декодируют его в исходную форму. Смысл автоэнкодера в том, что он не просто сжимает данные, а может понять их так называемые латентные особенности – самые важные и специфичные черты – и закодировать именно их, а при восстановлении воссоздать по ним массив, максимально приближенный к исход-

ному. Автоэнкодеры могут не просто сохранять информацию, но и придавать новым представлениям исходных данных разные свойства [18, с. 278; 19].

Для обработки естественного языка (анализ переписок, выявление фишинговых писем и сгенерированных текстов), помимо рассмотренных инструментов, характерно также применение моделей трансформеров [20, с. 2–3]. Именно на базе трансформенной архитектуры создаются LLM – большие языковые модели, такие как ChatGPT. Данная архитектура нейронных сетей также, как и RNN, эффективна для обработки последовательностей данных, но в данном случае наиболее характерные последовательности для неё – упорядоченные совокупности слов.

Модели этого типа формируют векторное представление для каждого элемента последовательности, включая как его собственную семантику, так и контекстуальные взаимосвязи с другими элементами. Полученные представления могут быть переданы другим нейронным сетям для решения различных задач, например, для классификации. Благодаря созданию информативных представлений, учитывающих контекст, трансформеры способствуют более эффективному выявлению скрытых паттернов и зависимостей в исходных данных.

Стандартным инструментом для работы с обнаружением и классификацией вредоносного ПО и анализа изображений и видео выступают свёрточные нейронные сети (CNN) [21, с. 1030]. Этот тип архитектуры нейронных сетей предназначен для обработки данных с сеточной структурой, в первую очередь изображений, но они подходят и для обработки видео и текстов. Такие сети последовательно анализируют пиксели, находящиеся рядом и содержащие непрерывную визуальную информацию: яркость и оттенок. В них применяются так называемые свёрточные слои, которые извлекают пространственные признаки из входных данных, что позволяет им автоматически обнаруживать локальные паттерны, такие как текстуры, формы, и «собирать» их в более сложные признаки (например, объекты на изображениях).

Для анализа изображений и видео используется классическая архитектура свёрточных сетей. Работа с обнаружением и классификацией вредоносного ПО предполагает как использование вариаций CNN [22], так и интеграции с другими типами нейросетей, в первую очередь – с трансформерами, упомянутыми выше. Такая комбинация архитектур позволяет обрабатывать многомодальные данные: из разных источников или разных типов.

Работа с обнаружением и классификацией вредоносного ПО осложнена тем, что постоянно создаются его новые модификации, что требует непрерывного обновления баз признаков, по которым его распознает та или иная нейросеть. Избежать этого позволяет визуализация вредоносных программ и последующее применение CNN как инструмента работы с изображениями. Так, например, ещё в 2008 г. был предложен метод преобразования бинарного кода вредоносного ПО в изображение в градациях серого, применение которого продемонстрировало, что визуальный анализ позволяет дифференцировать

различные области данных в таком представлении [23, с. 2]. Сегодня этот подход к анализу вредоносного ПО продолжает развиваться.

Необходимо отметить, что рассмотренные нами инструменты для каждого класса задач – это примеры наиболее стандартных подходов, а не исчерпывающий список. Сегодня наблюдается тенденция построения гибридных моделей, которые сочетают в себе преимущества различных типов архитектур, что позволяет ещё больше повысить точность конечного инструмента, сделать его более индивидуализированным в соответствии с конкретным запросом, а также всё большее распространение получает использование генеративного искусственного интеллекта⁹ для решения различных задач СКТЭ¹⁰. Кроме того, все коммерческие комплексы для компьютерных судебно-экспертных исследований, такие как Belkasoft¹¹, Magnet Forensics¹², Cellebrite¹³ и др. активно разрабатывают собственные ИИ-инструменты на базе различных архитектур и их сочетаний, которые интегрируются в уже существующие продукты этих компаний и предоставляются сразу пакетом для решения рассмотренных групп задач, что значительно облегчает доступ к ИИ технологиям, так как снимает необходимость разработки собственных моделей. Полагаем, что подобный подход будет применён и при отечественной разработке экспертного ПО.

ИИ в СКТЭ: проблемы и перспективы. Машинное обучение демонстрирует довольно высокую точность при решении задач СКТЭ – в среднем около 80 % [24, с. 136]. Некоторые модели демонстрируют невероятную точность – до 99,87 % [25, с. 13]. Однако при разработке таких инструментов необходимо учитывать потенциальные сложности.

Среди проблем использования технологий ИИ в судебно-экспертной деятельности, оказывающих наибольшее влияние на их внедрение, можно выделить две основные группы: проблемы, связанные с качеством данных для обучения нейросетей, и проблемы правового регулирования использования технологий ИИ в судебно-экспертной деятельности. Эти две группы неразрывно связаны друг с другом и непосредственно влияют на соответствие результатов работы ИИ требованиям допустимости и достоверности и, следовательно, на возможность его применения в уголовном процессе.

Качество данных и их достаточность имеют первостепенное значение для работы нейросетей. Наборы данных для обучения должны отвечать следующим требованиям: быть заданного формата (текстовые файлы, видео, изобра-

⁹ Генеративный ИИ – тип искусственного интеллекта, который в отличие от других видов ИИ может не просто анализировать и классифицировать данные, а способен самостоятельно создавать оригинальный контент на основе закономерностей, выявленных им в больших наборах данных.

¹⁰ Robert J., Al-Salmi N., Al-Sinani H. GenAI in Digital Forensics: Enhancing Timeline Reconstruction and Anomaly Attribution [Электронный ресурс] // URL: https://www.researchgate.net/publication/389128934_GenAI_in_Digital_Forensics_Enhancing_Timeline_Reconstruction_and_Anomaly_Attribution (дата обращения: 08.05.2026).

¹¹ Belkasoft [Электронный ресурс] // URL: <https://belkasoft.com/belkagpt> (дата обращения: 06.05.2026).

¹² Magnet Forensics [Электронный ресурс] // URL: <https://www.magnetforensics.com/resources/magnet-ai-a-minute-with-magnet/> (дата обращения: 06.05.2026).

¹³ Cellebrite [Электронный ресурс] // URL: <https://cellebrite.com/en/ai-center/> (дата обращения: 06.05.2026).

жения и пр.), быть актуальными, представленными в достаточном количестве, верно размеченными¹⁴, полученными законным путём, а также их правовой режим должен допускать использование этих наборов для целей обучения ИИ. Недостаточность данных – это одна из самых острых проблем при создании моделей ИИ. В контексте судебно-экспертной деятельности она особенно актуальна, поскольку:

1. Отдельные судебно-экспертные учреждения не создают объёма данных, достаточного для систематического создания и переобучения нейросетей;
2. Исходные данные – материалы судебно-экспертных исследований – нуждаются в дополнительной правовой защите (анонимизации, обеспечении дополнительных мер охраны при хранении и обработке).

Таким образом, для обеспечения достаточности данных для разработки и переобучения специализированных ИИ инструментов необходимо:

- а) разработать ГОСТ, содержащий требования к сбору, хранению, обработке, передаче и защите данных для систем искусственного интеллекта¹⁵;
- б) разработать систему сотрудничества между судебно-экспертными учреждениями различных подразделений в вопросах создания и использования экспертных моделей ИИ;
- в) обеспечить в структуре судебно-экспертных учреждений материально-техническую базу, позволяющую безопасно работать с большими объёмами чувствительных данных.

Только при условии создания единых наборов данных и репозиторий, а также общей установленной процедуры сбора и подготовки данных возможны будут апробация и верификация моделей для экспертной практики, что обеспечит допустимость и достоверность доказательств, полученных с применением технологий ИИ.

Ещё одной значимой проблемой в контексте сбора и подготовки данных для обучения нейросетей, отмечаемой и отечественными [26, с. 29; 27, с. 34], и зарубежными специалистами [28, с. 2], выступает алгоритмическая предвзятость. Она является результатом неверной работы с наборами данных, на которых будет обучаться нейросеть. Суть алгоритмической предвзятости состоит в том, что, если исходный набор содержит какую-либо дискриминационную тенденцию или каким-либо образом выдаёт некие субъективные и оценочные суждения за объективные факты, нейросеть «унаследует» эту предвзятость и будет выдавать закономерности и решения с её учетом. Так, например, широко известен случай американской системы COMPAS, которая предсказывала вероятность рецидива среди американских преступников. В ходе проверки результатов работы ИИ-инструмента было установлено, что результаты были очень

¹⁴ Разметка данных – это процесс добавления к необработанным данным (текстам, фото, видео и пр.) меток (тэгов) для того, чтобы модель машинного обучения смогла их воспринять и проанализировать.

¹⁵ ГОСТы такого рода уже существуют для других отраслей, например ГОСТ Р 59897–2021 «Данные для систем искусственного интеллекта в образовании».

расово неоднородны. Нейросеть почти в два раза чаще предсказывала, что афроамериканцы представляют более высокий риск рецидива, чем белые, и наоборот – необоснованно утверждала, что риск повторных преступлений среди белых заключенных меньше¹⁶.

Избежать алгоритмической предвзятости и повысить уровень надёжности работы нейросети можно только путём скрупулёзной работы со стартовыми наборами данных. Для составления таких датасетов необходима междисциплинарная работа, включающая, помимо архитекторов и инженеров машинного обучения, юристов и специалистов в области этики.

Допустимость использования результатов работы ИИ в процессе принятия экспертных решений также осложнена принципом работы нейросетей, известным как «black box» – чёрный ящик. Ранее мы упоминали, что инженер машинного обучения не знает, к какому выводу придёт нейросеть в процессе обучения. В этом и заключается принцип чёрного ящика – в невозможности для человека проследить внутреннюю логику вычислений, произведённых моделью ИИ. В таком случае обеспечить достоверность и законность доказательств представляется невозможным. Одним из способов решения этой проблемы является разработка так называемого объяснимого ИИ (XAI, Explainable AI)¹⁷ [29].

Что касается перспектив развития технологий ИИ в СКТЭ, то всё более широкое применение в различных отраслях находит агентный ИИ. Он представляет собой систему специализированных моделей-агентов, каждая из которых решает свою задачу. Так, например, при работе с сетевым трафиком одна из моделей-агентов будет анализировать трафик на предмет аномалий, другая – классифицировать их, третья – готовить проект заключения эксперта. Такие системы могут не только решать задачи в рамках заданного алгоритма, но и самостоятельно генерировать контент, осуществлять целеполагание, работать с крупными процессами, разбивая их на этапы и задачи, адаптируя изначальные цели. Система собирает сведения от каждого агента, автономно самообучается, имеет долгосрочную память и способна координировать действия агентов, из которых состоит.

Такая система в рамках СКТЭ сможет не только решать конкретную задачу, например, по поиску аномалий в сетевом трафике, но и выстраивать план экспертного исследования, приоритезировать задачи, выстраивая наиболее эффективный порядок действий, менять этот план в соответствии с изменяющимися или установленными обстоятельствами и пр.

В контексте агентного ИИ речь фактически идёт уже не столько об инструменте сокращения времени работы над конкретной экспертизой или облегчения рутинных задач эксперта, сколько о качественно новом уровне инте-

¹⁶ AI bias: 10 real-world failures and what they reveal about training data [Электронный ресурс] // URL: <https://www.prolific.com/resources/shocking-ai-bias> (дата обращения: 05.05.2026).

¹⁷ Объяснимый ИИ (XAI) – это такие модели искусственного интеллекта, которые могут предоставить понятные человеку обоснования своих выводов и решений.

грации ИИ технологии в экспертный процесс, что безусловно порождает и дополнительные этические и правовые риски [30, с. 4].

Наиболее перспективными направлениями для внедрения систем ИИ выступают те, где имеется наибольший поток данных, требующих оперативной обработки и выявления неочевидных закономерностей. В первую очередь, это дешифрование и подбор паролей и ключей доступа, поиск по ключевым словам заданного объекта в большом массиве данных, установление последовательности событий (особенно с анализом данных разного типа и из различных источников).

Среди перспектив применения технологий ИИ мы не рассматриваем ситуацию, когда ИИ заменяет эксперта полностью или в какой-то части. Технологии ИИ – это вспомогательный инструмент, призванный сократить нагрузку на эксперта и время проведения экспертиз. Пока не решён вопрос о субъектности ИИ, именно эксперт несёт полную юридическую и этическую ответственность за вынесенное заключение. Использование моделей ИИ налагает дополнительную этическую и профессиональную задачу: проверку результатов деятельности нейросетей, выявление ошибок, галлюцинаций¹⁸, проверку адекватности и валидности самой модели.

Подводя итоги, отметим, что несмотря на разнообразие и высокую эффективность технологий ИИ при решении задач судебной компьютерно-технической экспертизы, необходимо провести много технической и юридической подготовительной работы, обеспечивающий возможность минимизации рисков и ошибок, апробации методик, гарантий достаточного уровня достоверности доказательств, прежде чем можно будет широко внедрить этот инструмент в отечественную практику.

Заключение. Итак, использование технологий ИИ в рамках СКТЭ продиктовано объективной необходимостью и закономерностями развития информационного общества и информационных технологий. Решение задач СКТЭ и адекватное удовлетворение общественного запроса на такие экспертизы уже сейчас невозможно с использованием только классических методов исследования.

Технологии ИИ позволяют с помощью различных архитектур нейросетей и их сочетаний создавать профильные инструменты, наиболее эффективные для решения конкретных классов задач.

Однако несмотря на высокую эффективность и большой потенциал, внедрять ИИ в судебно-экспертную деятельность необходимо с большой осторожностью и соблюдением правовых гарантий, поскольку имеющиеся ограничения технологии часто не позволяют обеспечить надлежащий уровень допустимости и достоверности получаемых доказательств. Среди таких ограничений мы особенно отметили недостаточность данных для обучения нейросетей, отсутствие единых требований и процедуры сбора, обмена, обработки и хранения таких данных, отсутствие методик разработки и обучения нейросетей для целей судебно-экспертной деятельности, апробации и верификации моде-

¹⁸ Галлюцинации ИИ – ситуация, когда модель ИИ выдаёт правдоподобную, но неверную или несуществующую информацию.

лей ИИ, алгоритмическую предвзятость, принцип «чёрного ящика», этические ограничения, связанные с принятием экспертных решений.

Таким образом, технологии ИИ являются неотъемлемой частью развития СКТЭ, но должны применяться с осторожностью. Как инструмент облегчения рутинных задач, сокращения потоковой нагрузки на экспертов и времени проведения конкретного исследования, но не как основной инструмент исследования, единственное основание для вынесения экспертных решений или замена эксперта.

Список источников

1. Чеснокова Е.В., Усов А.И., Омелянюк Г.Г., Никулина М.В. Искусственный интеллект в судебной экспертологии / Е.В. Чеснокова, А.И. Усов, Г.Г. Омелянюк, М.В. Никулина // Теория и практика судебной экспертизы. – 2023. – Т. 18, № 3. – С. 60–77. – DOI: 10.30764/1819-2785-2023-3-60-77.
2. Руденкова Ю.С., Хазиев Ш.Н., Усов А.И. Искусственный интеллект и судебная компьютерно-техническая экспертиза / Ю.С. Руденкова, Ш.Н. Хазиев, А.И. Усов // Теория и практика судебной экспертизы. – 2024. – Т. 19, № 2. – С. 76–87. – DOI: 10.30764/1819-2785-2024-2-76-87.
3. Россинская Е.Р., Неретина Н.С., Чубина Е.А., Семикаленова А.И., Шамаев Г.П., Чернявская М.С. Современное состояние и перспективы развития машинного обучения и искусственного интеллекта для решения задач судебно-экспертной деятельности: аналитический доклад [Электронный ресурс] // URL: https://consortium.msal.ru/wp-content/uploads/2024/07/K_5-Sovremennoe-sostoyanie-i-perspektivy-razvitiya-mashinnogo-obucheniya-i-iskusstvennogo-intellekta-dlya-resheniya-zadach-sudebno-eksper.pdf (дата обращения: 06.05.2026).
4. Хатунцев Н.А. Судебная компьютерно-техническая экспертиза в свете цифровизации общества / Н.А. Хатунцев // Эксперт-криминалист. – 2020. – № 2. – С. 18–20.
5. RizwanBasha A., Annamalai R. Transforming crime scene investigations through the integration of artificial intelligence in digital forensics / A. RizwanBasha, R. Annamalai // 2024 IEEE International Conference on Communication, Computing and Signal Processing (IICCCS). – P. 1–6.
6. Мищук В.А. Соотношение понятий «искусственный интеллект» и «искусственная нейронная сеть» в судебной экспертологии / В.А. Мищук // Теория и практика судебной экспертизы. – 2024. – Т. 19, № 3. – С. 33–46. – DOI: 10.30764/1819-2785-2024-3-33-46.
7. Баланов А.Н. Машинное обучение и искусственный интеллект: учебное пособие для вузов. 2-е изд., стер. / А.Н. Баланов. – СПб.: Лань, 2025. – 172 с. — ISBN 978-5-507-52891-2.
8. Brink H., Richards J.W., Fetherolf M. Real-World Machine Learning / H. Brink, J.W. Richards, M. Fetherolf. – Manning Publications, 2016. – 264 p. – ISBN 9781617291920.

9. Vulinović K., Ivković L., Petrović J., Skračić K., Pale P. Neural Networks for File Fragment Classification / K. Vulinović, L. Ivković, J. Petrović, K. Skračić, P. Pale // 2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). – P. 1194–1198.
10. Marturana F., Tacconi S. A Machine Learning-based Triage methodology for automated categorization of digital media / F. Marturana, S. Tacconi // Digital Investigation. – 2013. – Vol. 10, iss. 2. – P. 193–204. – DOI: 10.1016/j.diin.2013.01.001.
11. Moustafa N., Hu J., Slay J. A holistic review of Network Anomaly Detection Systems: A comprehensive survey / N. Moustafa, J. Hu, J. Slay // Journal of Network and Computer Applications. – 2019. – Vol. 128. – P. 33–55. – DOI: 10.1016/j.jnca.2018.12.006.
12. Pfautch R., Dagli C., Ashiku L. Cyber Forensics with Deep Learning Recurrent Neural Networks / R. Pfautch, C. Dagli, L. Ashiku // Procedia Computer Science. – 2025. – Vol. 268. – P. 51–60. – DOI: 10.1016/j.procs.2025.08.181.
13. Chourasiya L., Khatri S., Lilhore U.K. et al. Advanced system log analyzer for anomaly detection and cyber forensic investigations using LSTM and transformer networks / L. Chourasiya, S. Khatri, U.K. Lilhore [et al.] // Journal of Cloud Computing. – 2025. – Vol. 14, art. no. 60. – DOI: 10.1186/s13677-025-00789-y.
14. Jamshidi S. et al. Effective text classification using BERT, MTM LSTM, and DT / S. Jamshidi [et al.] // Data & Knowledge Engineering. – 2024. – Vol. 151, art. no. 102306. – DOI: 10.1016/j.datak.2024.102306.
15. Mahmoudi A. Investigating LSTM-based time series prediction using dynamic systems measures / A. Mahmoudi // Evolving Systems. – 2025. – Vol. 16, art. no. 71. – DOI: 10.1007/s12530-025-09703-y.
16. Jha S., Prashar D., Long H.V., Taniar D. Recurrent neural network for detecting malware / S. Jha, D. Prashar, H.V. Long, D. Taniar // Computers & Security. – 2020. – Vol. 99, art. no. 102037. – DOI: 10.1016/j.cose.2020.102037.
17. Ibrahim M., Elhafiz R. Modelling an intrusion detection using recurrent neural networks / M. Ibrahim, R. Elhafiz // Journal of Engineering Research. – 2023. – Vol. 11, iss. 1, art. no. 100013. – DOI: 10.1016/j.jer.2023.100013.
18. Wei Y., Chow K.P., Yiu S.M. Insider Threat Detection Using Multi-autoencoder Filtering and Unsupervised Learning / Y. Wei, K.P. Chow, S.M. Yiu // Advances in Digital Forensics XVI / ed. by G. Peterson, S. Shenoi. – Cham: Springer, 2020. – P. 273–290. – (IFIP Advances in Information and Communication Technology; vol. 589). – DOI: 10.1007/978-3-030-56223-6_15.
19. Studiawan H., Sohel F. Anomaly detection in a forensic timeline with deep autoencoders / H. Studiawan, F. Sohel // Journal of Information Security and Applications. – 2021. – Vol. 63, art. no. 103002. – DOI: 10.1016/j.jisa.2021.103002.
20. Rodrigues F.B., Giozza W., Albuquerque R., Villalba L.J.G. Natural Language Processing Applied to Forensics Information Extraction With Transformers and Graph Visualization / F.B. Rodrigues, W. Giozza, R. Albuquerque, L.J.G. Villalba // IEEE Transactions on Computational Social Systems. – 2024. – Vol. 11, no. 4. – P. 4727–4743. – DOI: 10.1109/TCSS.2022.3159677.

21. Tundis A., Cauteruccio F. On Machine Learning for Digital Forensics Investigation in Network Traffic / A. Tundis, F. Cauteruccio // 2025 21st International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT). – P. 1027–1033. – DOI: 10.1109/DCOSS-IoT65416.2025.00155.
22. Vasan D., Alazab M., Wassan S., Safaei B., Zheng Q. Image-Based malware classification using ensemble of CNN architectures (IMCEC) / D. Vasan, M. Alazab, S. Wassan, B. Safaei, Q. Zheng // Computers & Security. – 2020. – Vol. 92, art. no. 101748. – DOI: 10.1016/j.cose.2020.101748.
23. Nataraj L., Karthikeyan S., Jacob G., Manjunath B.S. Malware images: visualization and automatic classification / L. Nataraj, S. Karthikeyan, G. Jacob, B.S. Manjunath // Proceedings of the 8th International Symposium on Visualization for Cyber Security (VizSec '11). – New York: Association for Computing Machinery, 2011. – P. 1–7. – DOI: 10.1145/2016904.2016908.
24. Dhabliya D., Gujar S.N., Dhabliya R., Chavan G.T., Kalnawat A., Bendale S.P. Temporal Intelligence in AI-Enhanced Cyber Forensics using Time-Based Analysis for Proactive Threat Detection / D. Dhabliya, S.N. Gujar, R. Dhabliya [et al.] // Journal of Electrical Systems. – 2023. – Vol. 19, № 3. – P. 126–146. – DOI: 10.52783/jes.659.
25. Islam U., Alwageed H.S., Farooq M.M.U., Khan I., Awwad F.A., Ali I., Abonazel M.R. Investigating the Effectiveness of Novel Support Vector Neural Network for Anomaly Detection in Digital Forensics Data / U. Islam, H.S. Alwageed, M.M.U. Farooq [et al.] // Sensors. – 2023. – Vol. 23, iss. 12, art. no. 5626. – DOI: 10.3390/s23125626.
26. Россинская Е.Р. Нейросети в судебной экспертологии и экспертной практике: проблемы и перспективы / Е.Р. Россинская // Вестник Университета имени О.Е. Кутафина (МГЮА). – 2024. – № 3 (115). – С. 21–33. – DOI: 10.17803/2311-5998.2024.115.3.021-033.
27. Кокин А.В., Денисов Ю.Д. Искусственный интеллект в криминалистике и судебной экспертизе: вопросы правосубъектности и алгоритмической предвзятости / А.В. Кокин, Ю.Д. Денисов // Теория и практика судебной экспертизы. – 2023. – Т. 18, № 2. – С. 30–37. – DOI: 10.30764/1819-2785-2023-2-30-37.
28. Kartal E. A Comprehensive Study on Bias in Artificial Intelligence Systems: Biased or Unbiased AI, That's the Question! / E. Kartal // International Journal of Intelligent Information Technologies. – 2022. – Vol. 18, no. 1. – P. 1–23. – DOI: 10.4018/IJIT.309582.
29. Billah M. Explainable AI for Digital Forensics: Ensuring Transparency in Legal Evidence Analysis / M. Billah // Journal of Forensic Science and Research. – 2025. – Vol. 9, iss. 2. – P. 109–116. – DOI: 10.29328/journal.jfsr.1001089.
30. Wickramasekara A., Scanlon M. A Framework for Integrated Digital Forensic Investigation Employing AutoGen AI Agents / A. Wickramasekara, M. Scanlon // Conference: 2024 12th International Symposium on Digital Forensics and Security (ISDFS). – DOI: 10.1109/ISDFS60797.2024.10527235.

References

1. Chesnokova E.V., Usov A.I., Omelyanyuk G.G. et al. Artificial Intelligence in Forensic Expertology. *Theory and Practice of Forensic Science*, 2023, vol. 18, no. 3, pp. 60–77. DOI: 10.30764/1819-2785-2023-3-60-77. (In Russian).
2. Rudenkova Yu.S., Khaziev Sh.N., Usov A.I. Artificial Intelligence and Computer Forensics. *Theory and Practice of Forensic Science*, 2024, vol. 19, no. 2, pp. 76–87. DOI: 10.30764/1819-2785-2024-2-76-87. (In Russian).
3. Rossinskaya E.R., Neretina N.S., Chubina E.A. et al. Current State and Prospects of Development of Machine Learning and Artificial Intelligence for Solving Problems of Forensic Expert Activity: Analytical Report. Available at: https://consortium.msal.ru/wp-content/uploads/2024/07/K_5-Sovremennoe-sostoyanie-i-perspektivy-razvitiya-mashinnogo-obucheniya-i-iskusstvennogo-intellekta-dlya-resheniya-zadach-sudebno-eksper.pdf. (In Russian).
4. Khatuntsev N.A. Computer Forensic Examination against the Background of Society Digitalization. *Expert–Criminalist*, 2020, no. 2, pp. 18–20. (In Russian).
5. Rizwan Basha A., Annamalai R. Transforming Crime Scene Investigations Through the Integration of Artificial Intelligence in Digital Forensics. *Materials of IEEE International Conference on Communication, Computing and Signal Processing (IICCCS). India, 19-20 September 2024*. India, IEEE, 2024, pp. 1–6. (In English).
6. Mishchuk V.A. The Relationship between the Concepts of “Artificial Intelligence” and “Artificial Neural Network” in Forensic Expertology. *Theory and Practice of Forensic Science*, 2024, vol. 19, no. 3, pp. 33–46. DOI: 10.30764/1819-2785-2024-3-33-46. (In Russian).
7. Balanov A.N. Machine Learning and Artificial Intelligence: Textbook for Universities. St. Petersburg, Lan’, 2025. 172 p. (In Russian).
8. Brink H., Richards J.W., Fetherolf M. Real-World Machine Learning. Manning Publications, 2016. 264 p. (In English).
9. Vulinović K., Ivković L., Petrović J. et al. Neural Networks for File Fragment Classification. *Materials of the 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). Opatija, Croatia, 20-24 May 2019*. IEEE, 2019, pp. 1194–1198. (In English).
10. Marturana F., Tacconi S.A Machine Learning-Based Triage Methodology for Automated Categorization of Digital Media. *Digital Investigation*, 2013, vol. 10, no. 2, pp. 193–204. DOI: 10.1016/j.diin.2013.01.001. (In English).
11. Moustafa N., Hu J., Slay J. A holistic review of Network Anomaly Detection Systems: A comprehensive survey. *Journal of Network and Computer Applications*, 2019, vol. 128, pp. 33–55. DOI: 10.1016/j.jnca.2018.12.006. (In English).
12. Pfautch R., Dagli C., Ashiku L. Cyber Forensics with Deep Learning Recurrent Neural Networks. *Procedia Computer Science*, 2025, vol. 268, pp. 51–60. DOI: 10.1016/j.procs.2025.08.181. (In English).

13. Chourasiya L., Khatri S., Lilhore U.K. et al. Advanced System Log Analyzer for Anomaly Detection and Cyber Forensic Investigations Using LSTM and Transformer Networks. *Journal of Cloud Computing*, 2025, vol. 14, art. no. 60. DOI: 10.1186/s13677-025-00789-y. (In English).
14. Jamshidi A., Mohammadi M., Bagheri S. et al. Effective Text Classification Using BERT, MTM, LSTM, and DT. *Data & Knowledge Engineering*, 2024, vol. 151, art. no. 102306. DOI: 10.1016/j.datak.2024.102306. (In English).
15. Mahmoudi A. Investigating LSTM-Based Time Series Prediction Using Dynamic Systems. *Evolving Systems*, 2025, vol. 16, art. no. 71. DOI: 10.1007/s12530-025-09703-y. (In English).
16. Jha S., Prashar D., Long H.V. et al. Recurrent Neural Network for Detecting. *Computers & Security*, 2020, vol. 99, art. no. 102037. DOI: 10.1016/j.cose.2020.102037. (In English).
17. Ibrahim M., Elhafiz R. Modelling an Intrusion Detection Using Recurrent Neural Networks. *Journal of Engineering Research*, 2023, vol. 11, iss. 1, art. no. 100013. DOI: 10.1016/j.jer.2023.100013. (In English).
18. Wei Y., Chow K.P., Yiu S.M. Insider Threat Detection Using Multi-autoencoder Filtering and Unsupervised Learning. *Advances in Digital Forensics XVI*. Cham, Springer, 2020, pp. 273–290. DOI: 10.1007/978-3-030-56223-6_15. (In English).
19. Studiawan H., Sohel F. Anomaly Detection in a Forensic Timeline with Deep Autoencoders. *Journal of Information Security and Applications*, 2021, Vol. 63, art. no. 103002. DOI: 10.1016/j.jisa.2021.103002. (In English).
20. Rodrigues F.B., Giazza W., Albuquerque R., Villalba L.J.G. Natural Language Processing Applied to Forensics Information Extraction with Transformers and Graph Visualization. *IEEE Transactions on Computational Social Systems*, 2024, vol. 11, no. 4, pp. 4727–4743. DOI: 10.1109/TCSS.2022.3159677. (In English).
21. Tundis A., Cauteruccio F. On Machine Learning for Digital Forensics Investigation in Network Traffic. *Materials of the 21st International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT), Italy, Lucca, June, 6–9, 2025*. Italy, IEEE, pp. 1027–1033. DOI: 10.1109/DCOSS-IoT65416.2025.00155. (In English).
22. Vasan D., Alazab M., Wassan S. et al. Image-Based Malware Classification Using Ensemble of CNN Architectures (IMCEC). *Computers & Security*, 2020, vol. 92, art. no. 101748. DOI: 10.1016/j.cose.2020.101748. (In English).
23. Nataraj L., Karthikeyan S., Jacob G., Manjunath B.S. Malware Images: Visualization and Automatic Classification. *Materials of the 8th International Symposium on Visualization for Cyber Security (VizSec '11)*. New York, Association for Computing Machinery, 2011, pp. 1–7. DOI: 10.1145/2016904.2016908. (In English).
24. Dhabliya D., Gujar S.N., Dhabliya R. et al. Temporal Intelligence in AI-Enhanced Cyber Forensics using Time-Based Analysis for Proactive Threat Detection. *Journal of Electrical Systems*, 2023, vol. 19, no. 3, pp. 126–146. DOI: 10.52783/jes.659. (In English).

25. Islam U., Alwageed H.S., Farooq M.M.U. et al. Investigating the Effectiveness of Novel Support Vector Neural Network for Anomaly Detection in Digital Forensics Data. *Sensors*, 2023, vol. 23, iss. 12, art. no. 5626. DOI: 10.3390/s23125626. (In English).

26. Rossinskaya E.R. Neural Networks in Forensic Expertology and Expert Practice: Problems and Prospects. *Courier of Kutafin Moscow State Law University (MSAL)*, 2024, no. 3 (115), pp. 21–33. DOI: 10.17803/2311-5998.2024.115.3.021-033. (In Russian).

27. Kokin A.V., Denisov Yu.D. Artificial Intelligence in Criminalistics and Forensic Examination: Issues of Legal Personality and Algorithmic Bias. *Theory and Practice of Forensic Science*, 2023, vol. 18, no. 2, pp. 30–37. DOI: 10.30764/1819-2785-2023-2-30-37. (In Russian).

28. Kartal E. A Comprehensive Study on Bias in Artificial Intelligence Systems: Biased or Unbiased AI, That's the Question! *International Journal of Intelligent Information Technologies*, 2022, vol. 18, no. 1, pp. 1–23. DOI: 10.4018/IJIT.309582. (In English).

29. Billah M. Explainable AI for Digital Forensics: Ensuring Transparency in Legal Evidence Analysis. *Journal of Forensic Science and Research*, 2025, vol. 9, iss. 2, pp. 109–116. DOI: 10.29328/journal.jfsr.1001089. (In English).

30. Wickramasekara A., Scanlon M. A Framework for Integrated Digital Forensic Investigation Employing AutoGen AI Agents. *Materials of the 12th International Symposium on Digital Forensics and Security (ISDFS), Dublin, April, 29–30, 2024*. Dublin, IEEE. DOI: 10.1109/ISDFS60797.2024.10527235.

Информация об авторе

Василевская Дарья Владимировна – кандидат юридических наук, старший преподаватель кафедры криминалистики

Information about the Author

Vasilevskaya Daria Vladimirovna – Candidate of Sciences (Law), Senior Lecturer of the Department of Criminalistics

Статья поступила в редакцию 04.05.2026 г.; одобрена после рецензирования 28.05.2026 г.; принята к публикации 05.06.2026 г.

The article was submitted 04.05.2026; approved after reviewing 28.05.2026; accepted for publication 04.05.2026.