Научная статья
УДК 343.98

КОНЦЕПЦИЯ ГЛОБАЛЬНОГО НЕЙРОСЕТЕВОГО КРИМИНАЛИСТИЧЕСКОГО КЛАСТЕРА ДАННЫХ В ОБЛАСТИ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Зарина Ирековна Харисова
Уфимский юридический институт МВД России, Уфа, Россия
zarinaid@mail.ru, ORCID: 0000-0002-3902-3459

Аннотация. Процесс накопления, обработки, поиска и хранения криминалистически значимой информации, объединенной общими видовыми характеристиками, позволяет формировать информационно-поисковые системы, способствующие решению диагностических, классификационных и идентификационных задач в криминалистике. В статье описывается концепция нового криминалистического учета, который может выступить кластером обучающих данных для информационной системы, используемой в целях систематизации (классификации) криминалистически значимой компьютерной информации. Сделан вывод, что в основу криминалистического кластера электронных доказательств необходимо заложить гибридную модель анализа разнородных данных с интеграцией методов цифровой криминалистики, машинного обучения и объяснимого искусственного интеллекта. Указанный подход позволит сформировать базу данных для построения принципиально нового интеллектуального технико-криминалистического средства. В совокупности с применением облачных технологий, средств визуализации и анализа больших данных предлагаемая концепция может представлять собой современный инструмент противодействия преступлениям в сфере компьютерной информации.

Ключевые слова: цифровые доказательства, криминалистический кластер данных, криминалистический учет, нейросетевой кластер данных, цифровая криминалистика, компьютерная криминалистика, расследование преступлений, преступления в сфере компьютерной информации, технико-криминалистическое средство.

Для цитирования: Харисова З. И. Концепция глобального нейросетевого криминалистического кластера данных в области противодействия преступлениям в сфере компьютерной информации // Вестник Уфимского юридического института МВД России. 2025. № 3 (109). С. 116–125.

Original article

THE CONCEPT OF A GLOBAL NEURAL NETWORK FORENSIC DATA CLUSTER IN THE FIELD OF COUNTERING COMPUTER INFORMATION CRIMES

Zarina I. Kharisova
Ufa Law Institute of the Ministry of Internal Affairs of Russia, Ufa, Russia
zarinaid@mail.ru, ORCID: 0000-0002-3902-3459

Abstract. The process of accumulation, processing, search and storage of forensically significant information, combined by common specific characteristics, makes it possible to form information and search systems that contribute to the solution of diagnostic, classification and identification tasks in forensics. The article describes the concept of a new forensic accounting, which can act as a cluster of training data for an information system used to systematize (classify) forensically significant computer information. It is concluded that the basis of the forensic cluster of electronic evidence should be a hybrid model for analyzing

heterogeneous data with the integration of digital forensics methods, machine learning and explainable artificial intelligence. This approach will make it possible to form a database for building a fundamentally new intellectual technical and forensic tool. Together with the use of cloud technologies, visualization tools and analysis of big data, the proposed concept can represent a modern tool for countering computer information crimes.

Keywords: digital evidence, forensic data cluster, forensic accounting system, neural network data cluster, digital forensics, computer forensics, crime investigation, computer crimes, forensic technology tool.

For citation: Kharisova Z. I. The concept of a global neural network forensic data cluster in the field of countering computer information crimes // Bulletin of Ufa Law Institute of the Ministry of Internal Affairs of Russia. 2025. No. 3 (109). P. 116–125. (In Russ.)

Введение

В настоящее время насчитываются десятки различных учетов, которые в зависимости от особенностей учитываемых объектов и характеризующих их признаков подразделяются на оперативно-справочные, криминалистические и справочно-вспомогательные учеты. Криминалистическая регистрация является систематизированным научно обоснованным учетом и основой информационного обеспечения органов внутренних дел сведениями об объектах и лицах в сфере уголовного судопроизводства и оперативно-розыскной деятельности. В виду того, что криминалистическая регистрация определяется перечнем учетных объектов, набор которых диктуется существующим уровнем технического развития, одним из вариантов решения проблем, связанных с поиском, анализом и исследованием цифровых следов, является введение новой системы регистрации цифровых доказательств в виде нейросетевого кластера криминалистически значимой цифровой информации. Формами криминалистических учетов, входящих в указанную систему регистрации цифровых доказательств, могут являться документированная информация, структурированные базы данных со сведениями о технических средствах и их сетевой активности, программное обеспечение, в том числе вредоносное, веб-ресурсы, аудио- и видеозаписи, а также их смешанные варианты, что позволит сформировать глобальную платформу анализа разнородных данных.

Предложенная система криминалистического учета цифровых доказательств сможет послужить в дальнейшем основой для реализации программного технико-криминалистического средства с возможностью формирования типовых следственных версий и планов расследования преступлений в сфере компьютерной информации.

Методы

В процессе исследования использовалась совокупность общих методов научного познания (описание, обобщение и сравнение), общенаучных (анализ, синтез, системный), частнонаучных и специальных методов (кибернетический, формально-юридический, сравнительно-правовой). Использование указанных приемов позволило выявить возможность систематизации криминалистически значимой компьютерной информации и реализации интеллектуального программного обеспечения в области противодействия преступлениям в сфере компьютерной информации.

Результаты

Быстрый темп технологического прогресса, переход к цифровой экономике и, как следствие, обработка значительных массивов данных в электронном виде объясняют недостаточность применения традиционных методов собирания и исследования доказательств при расследовании ряда наиболее распространенных в настоящее время преступных деяний. В этой связи в криминалистической теории наблюдается тенденция изучения так называемых цифровых следов преступной деятельности [1, с. 3], что в большей степени обусловлено ежегодным приростом преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, в совокупности составивших за 2024 год более 40 % от

числа всех зарегистрированных преступных деяний[1].

Несмотря на широкое применение термина «цифровое доказательство» в зарубежной и отечественной научной литературе, в Уголовно-процессуальном кодексе Российской Федерации в настоящее время отсутствует его законодательное определение. Но на международном уровне под цифровым (электронным) доказательством, как правило, понимают любую информацию, обладающую доказательной силой и хранимую (передаваемую) в цифровой форме[2].

Анализ способов совершения преступных деяний позволяет сделать заключение о наиболее вероятном расположении следов, оставляемых при том или ином используемом преступником методе [2, с. 117]. Криминалистическое изучение особенностей совершения преступлений и, в частности, их способов дает исходные положения для разработки технико-криминалистических средств, при помощи которых следы преступления окажутся зафиксированными наиболее полно и будут пригодными для дальнейшего исследования.

Доказывание в понимании познавательной деятельности – это оперирование доказательствами [3, с. 76], поэтому процесс доказывания складывается из четырех элементов – поиска (обнаружения, собирания, фиксации), исследования, оценки и использования доказательств, грамотность проведения и правильность процессуального оформления которых способствуют оперативному изобличению участников преступного события и обеспечению надежной доказательственной базы для органов следствия [4, с. 44]. Обнаружение цифровых следов преступлений является поисковой деятельностью следователя, которая направлена на собирание доказательственной и ориентирующей криминалистически значимой информации, что возможно с использованием различных технических устройств (компьютерных, мобильных и пр.), а также программных технико-криминалистических средств. Несмотря на динамичное развитие общей теории криминалистики, например, путем ее дополнения частными криминалистическими теориями (исследования компьютерной информации [5, с. 11], информационно-компьютерного обеспечения криминалистической деятельности [6, с. 13] и пр.), релевантные на сегодняшний день обзоры, посвященные выявлению проблем в области расследования преступлений [7, с. 176; 8, с. 3; 9, с. 25483; 10, с. 81; 11, с. 2], позволяют сделать вывод о значимости собирания цифровых доказательств и необходимости автоматизации процесса их исследования, что обусловлено сложностями анализа больших массивов данных в электронном виде.

Одним из вариантов обеспечения быстрой и эффективной обработки собранной криминалистически значимой компьютерной информации является внедрение в алгоритмы функционирования программных технико-криминалистических средств технологий искусственного интеллекта, основанных на математических моделях и реализованных по принципу организации сетей нервных клеток человека. Таким образом, автоматизировать процессы собирания и исследования цифровых доказательств с минимальными трудозатратами позволит специализированное программное обеспечение, разработанное на базе машинного обучения, при этом точность и прозрачность анализа данных смогут обеспечить, например, XAI-системы (от англ. «explainable artificial intelligence» (XAI) – объяснимый искусственный интеллект) [12, с. 7] и модели, способные объяснять принимаемые нейросетью решения адаптированным для человека языком, что особенно важно для исключения проблем предвзятости алгоритмов.

---

[1] Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2024 года // МВД России. URL: https://media.mvd.ru/files/application/9209203 (дата обращения: 25.06.2025).

[2] Практическое руководство по истребованию электронных доказательств // УНП ООН. URL: https://sherloc.unodc.org/cld/ru/st/evidence/practical-guide.html (дата обращения: 25.06.2025).

Наиболее перспективными направлениями применения методов обработки данных на основе технологий искусственного интеллекта в области расследования преступлений являются проведение криминалистических исследований и выдача заключений по вопросам, разрешение которых требует специальных знаний в области цифровой криминалистики. При этом необходимо соблюдать этичное использование указанных технологий, а также обеспечивать строгую регламентацию обучения и переобучения разрабатываемых на его основе систем, что возможно только при соблюдении единых стандартов управления процессами для анализа данных. Таким образом, на сегодняшний день важно принять факт неотвратимости задействования нейросетевых технологий в процесс расследования преступлений. Однако на стадии зарождения и реализации основного функционала рассмотренных систем необходимо заблаговременно определить базовые требования к разработкам и возможности их использования в области противодействия преступлениям с учетом применимости принципов справедливости, подотчетности, прозрачности и объяснимости всех осуществляемых искусственным интеллектом действий и принимаемых решений.

Активное внедрение современных информационных технологий в деятельность правоохранительных органов способствует расширению использования аналитических методов, что значительно влияет на организацию расследования преступлений. Автоматизация процессов сбора, хранения, систематизации и анализа криминалистически значимой информации повышает эффективность следственной, оперативно-розыскной, экспертной и судебной деятельности, способствует научной организации труда и оптимизации процессов расследования [13, с. 704]. Эффективность раскрытия и расследования преступлений в большинстве случаев зависит от качества и количества криминалистически значимой информации, источниками которой могут быть как материальные и идеальные следы, так и следообразующие объекты [14, с. 382]. К такого рода информации относят находящиеся в причинно-следственной связи с преступлением данные или сведения, которые, например, могут характеризовать способ и средства его совершения, объект, субъект или предмет преступного посягательства и пр. Системы объектов в виде баз данных или хранилищ информации представляют собой криминалистическую регистрацию, которая складывается из подсистем (криминалистических учетов), отличающихся друг от друга учитываемыми данными, способами или формами их систематизации. В связи с этим предлагается ввести новый криминалистический учет, который выступит кластером обучающих данных для информационной системы, используемой в целях систематизации криминалистически значимой компьютерной информации.

Основными источниками информационного обеспечения следственной деятельности в настоящее время являются криминалистические регистрационные системы правоохранительных ведомств, ведомственные учеты правоохранительных органов, не затрагивающие преступную деятельность, различные информационные системы государственных органов власти и управления, учреждений, организаций и предприятий различных форм собственности, информационные ресурсы научно-методического и справочного содержания, а также сведения, размещенные в киберсреде.

Перечисленные ресурсы довольно широко используются следователями, но зачастую бессистемно, эпизодически либо не в полном объеме. Для повышения эффективности их использования необходима систематизация имеющихся данных, обеспечивающая организацию информационных потоков и удобный к ним доступ. Увеличение объема регистрируемых данных и доступных информационных ресурсов, а также создание новых и совершенствование уже существующих криминалистических учетов является перспективным направлением развития информационного обеспечения следственной деятельности.

Таким образом, для более эффективного использования экспертно-криминалистических учетов в раскрытии и расследовании преступлений целесообразно интегрировать различные виды учетов в единую систему, что позволит установить корреляционные связи между объектами разных видов учетов [15, с. 155]. В такого рода системе должен быть предусмотрен функционал для определения связей между следами, оставленными преступником в информационных системах и технических средствах, изъятыми в рамках одного преступного деяния, с другим комплексом следов, изъятым с иного объекта.

Повысить эффективность расследования преступлений в сфере компьютерной информации за счет систематизации, классификации и автоматизированного анализа цифровых следов позволит интегрированная система учета цифровых доказательств, структурными элементами при реализации которой могут выступить подсистемы сбора и агрегации данных, их классификации и структурирования, анализа и оценки, хранения и обмена данными, а также генерации отчетов и визуализации (рисунок 1).

Так, подсистема сбора и агрегации данных обеспечит оперативный сбор разнородных цифровых доказательств из множества источников, например, с локальных носителей данных, серверов, облачных хранилищ, технических средств, а также элементов (датчиков) интернета вещей, сетевых маршрутизаторов, журналов криптовалютных транзакций, адресов электронных кошельков, межсетевых экранов, прокси-серверов, систем обнаружения вторжений и пр.

Подсистема классификации и структурирования доказательств в зависимости от заданных критериев и способов стандартизации данных обеспечит их систематизацию и разделение по типу, например, на текстовые файлы, бинарные данные, лог-файлы, метаданные, графические данные, аудио- или видеозаписи, а также классификацию по временным меткам и корреляцию событий (создание временных шкал, выявление закономерностей взаимодействия между событиями (например, совпадение времени доступа к информационным системам и осуществление несанкционированного доступа к компьютерной информации).

Подсистема анализа и оценки доказательств позволит осуществить аналитическую обработку собранных данных, выявить скрытые взаимосвязи между событиями на основе методов машинного обучения, кластеризации, предсказания сценария развития преступления, оценки достоверности цифровых доказательств и их весомости.

Подсистема хранения и обмена данными обеспечит их централизованную сохранность в виде баз данных, обеспеченных функциями индексирования, шифрования и контроля доступа, интеграцию с национальными и международными реестрами криминалистически значимых данных с возможностью обмена информацией для оперативного реагирования, а также аудит и протоколирование для фиксации изменений и доступа к данным.

Подсистема генерации отчетов и визуализации послужит гибким инструментом для построения отчетов в наглядной форме (дашбордов (от англ. «dashboard» – панель

Рисунок 1. Структура системы криминалистической регистрации цифровых доказательств по преступлениям в сфере компьютерной информации

управления), диаграмм, временных линий, графов связей между событиями, а также статистических сводок с возможностью формирования выводов на основе пользовательских запросов и анализа шаблонов на базе обученных ранее данных).

В систему криминалистического учета по преступлениям в сфере компьютерной информации целесообразно включить:

1) подсистему учета зарегистрированных преступлений для сбора и систематизации информации о каждом зарегистрированном преступном деянии, включая дату, время, место, способ совершения преступления, используемые средства, предмет преступного посягательства, размер ущерба;

2) подсистему учета лиц, совершивших преступления, для систематизации информации о подозреваемых или обвиняемых лицах, включая анкетные данные, сведения о судимостях, используемые учетные данные, IP-адреса и MAC-идентификаторы принадлежащих им устройств, адреса электронной почты, аккаунты в социальных сетях и мессенджерах, профессиональные навыки и умения;

3) подсистему учета средств совершения преступлений для сбора информации о задействованных технических средствах и программном обеспечении, включая их характеристики, происхождение, способы задействования;

4) подсистему учета цифровых следов преступлений и мест их расположения для систематизации информации о цифровых следах, оставляемых различными средствами совершения преступлений (например, лог-файлы, дампы памяти, особенности прохождения сетевого трафика), а также о местах их наиболее вероятного расположения (например, журналы серверов, файлы операционной системы, базы данных и пр.);

5) подсистему учета криминалистически значимой информации об обстановке совершения преступлений для выявления и систематизации факторов, способствовавших совершению преступления.

Криминалистический учет по преступлениям в сфере компьютерной информации может осуществляться по следующим основаниям:

– по способу совершения преступления и использованным при этом техническим средствам и программному обеспечению (MAC-идентификаторы, IP-адреса, серийные номера, IMEI-коды, лицензии и пр.);

– по способу сокрытия следов преступления и используемым при этом техническим средствам и программному обеспечению;

– по месту и времени задействования технических средств при совершении преступления;

– по лог-файлам и журналам событий в информационных системах и программном обеспечении;

– по сетевому трафику, сетевым артефактам;

– по сигнатурам распространяемого вредоносного кода и паттернам аномального поведения (коллекции вредоносного программного обеспечения);

– по учетным записям и идентификаторам в сети Интернет;

– по цифровым аватарам в метасреде;

– по идентификаторам в сетях Tor и I2P;

– по хэш-суммам используемых при совершении преступления файлов и программного обеспечения;

– по поддельным электронным документам, цифровым подписям и сертификатам;

– по используемым при совершении преступления веб-ресурсам;

– по биометрическим данным;

– по метаданным мультимедиаконтента;

– по скомпрометированным данным;

– по синтетически сгенерированному контенту (дипфейк-контент);

– по идентификаторам криптовалютных транзакций и прочим финансовым операциям.

Таким образом, формирование нового криминалистического учета в виде нейросетевого кластера данных, в частности по преступлениям в сфере компьютерной информации, является важным шагом на пути к повышению эффективности противодействия им. Система учета должна учитывать

специфику цифровой среды, обеспечивать сбор, систематизацию и анализ информации о различных аспектах преступных деяний, а также соответствовать требованиям законодательства о персональных данных и информационной безопасности.

Предложенная интегрированная система учета цифровых доказательств сможет послужить в дальнейшем основой для формирования модульной и масштабируемой платформы поддержки принятия решений (подбор методики расследования), позволяющей собирать, классифицировать и анализировать цифровые доказательства в режиме реального времени, использовать современные методы анализа на основе искусственного интеллекта для выявления закономерностей и оценки вероятности развития событий, обеспечить безопасное хранение и обмен данными с возможностью интеграции с существующими национальными и международными системами, а также реализовать комплексное программное технико-криминалистическое средство с возможностью формирования типовых следственных версий и планов расследования преступлений в сфере компьютерной информации (рисунок 2) с учетом сведений, составляющих базовые элементы криминалистической характеристики преступного деяния (способ совершения преступления, обстановка, личность преступника и потерпевшего и пр.).

Предлагаемый подход к анализу данных, нахождению закономерностей, идентификации связей и корреляций между переменными и построению моделей с использованием инструментов визуализации по своей сути представляет собой технику EDA-анализа [16, с. 18] (от англ. «exploratory data analysis» – разведочный анализ данных) в виде комплекса методик, позволяющих исследовать, нормализовать и стандартизовать данные, определять их качество, структуру и характеристики, а также выявлять аномалии среди них. Таким образом, в эпоху цифровизации и растущего объема данных необходимо применение EDA-техник в криминалистике, которые обладают существенным потенциалом, являясь перспективой в области совершенствования всех имеющихся экспертных систем и криминалистических учетов.

Оптимизация процесса поиска, анализа и интерпретации цифровых доказательств возможна с применением алгоритмов искусственного интеллекта не только в отношении

Рисунок 2. Упрощенная модель оптимизации процесса поиска, анализа и интерпретации цифровых доказательств с использованием алгоритмов искусственного интеллекта (на рисунке буквами обозначены технологии: AI – искусственный интеллект, ML – машинное обучение, CV – компьютерное зрение)

реализации программного технико-криминалистического средства, но и в совокупности с формируемыми цифровой моделью преступления, кластером цифровых доказательств в виде криминалистических учетов и системой поддержки принятия решений.

Подводя итог вышеуказанному, отметим, что криминалистика как наука, изучающая закономерности механизма преступления и возникновения информации о нем, в условиях всеобщей цифровизации и интеллектуализации приобретает новые исследовательские и практико-ориентированные возможности. Технологии искусственного интеллекта при этом представляют собой дополнительный инструмент, интегрируемый в систему криминалистических средств.

Заключение

Проведенный анализ наиболее значимых исследований в области цифровой криминалистики за последние несколько лет определил возможность реализации гибридной модели анализа электронных доказательств, в основе которой лежит интеграция традиционных методов цифровой криминалистики, машинного обучения и объяснимого искусственного интеллекта, что значительно повысит эффективность расследования преступлений в сфере компьютерной информации. Так, существующие методы цифровой криминалистики можно усовершенствовать использованием комбинации современных технологических подходов, основанных на технологиях искусственного интеллекта (машинном обучении) и распределенных вычислений, облачных технологиях и технологиях анализа данных, что позволит сформировать полноценный инструмент в целях противодействия преступлениям в сфере компьютерной информации.

Таким образом, развитие распространенных в настоящее время методов анализа электронных доказательств по принципу глобального нейросетевого кластера цифровых доказательств представляет собой одно из перспективных направлений эволюции цифровой криминалистики и позволяет объединить преимущества отдельно взятых подходов, компенсируя недостатки при их использовании в отдельности.

СПИСОК ИСТОЧНИКОВ

1. Цифровые следы преступлений: монография / А. М. Багмет, В. В. Бычков, С. Ю. Скобелин, Н. Н. Ильин. Москва: Проспект, 2023. 168 с.

2. Выявление причин преступности и предупреждение преступлений. Общие положения / Гришанин П. Ф., Зуйков Г. Г., Кривошеев А. С., Ратинов А. Р. и др. Москва: НИиРИО МВШ МООП СССР, 1967. 179 с.

3. Белкин Р. С. Криминалистика: проблемы, тенденции, перспективы. Общая и частные теории. Москва: Юридическая литература, 1987. 270 с.

4. Скобелин С. Ю. Цифровая криминалистика: объект и направления развития // Российский следователь. 2020. № 4. С. 42–44.

5. Цифровая криминалистика / под редакцией В. Б. Вехова, С. В. Зуева. Москва: Юрайт, 2025. 490 с.

6. Теория информационно-компьютерного обеспечения криминалистической деятельности: монография / под. ред. Е. Р. Россинской Москва: Проспект, 2022. 254 с.

7. Horsman G., Sunde N. Unboxing the digital forensic investigation process // Science and Justice. 2022. No. 62. P. 171–180.

8. Dunsin D., Ghanem M., Ouazzane K. A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response // Digital Investigation. 2024. No. 48. P. 1–22.

9. Casino F., Dasaklis T., Research trends, challenges, and emerging topics in digital forensics: A review of reviews // IEEE Access. 2022. No. 10. V. P. 25464–25493.

10. Машков С. А. Большие данные и криминалистика: возможности и перспективы // Сибирские уголовно-процессуальные и криминалистические чтения. 2024. № 2. С. 78–86.

11. Jian X., Siegel M. Towards a joint semantic analysis in mobile forensics environments // Digital Investigation. 2025. No. 52. P. 1–26.

12. Lundberg E., Mozelius P. The potential effects of deepfakes on news media and entertainment // AI & Society. No. 11. 2024. P. 1–12.

13. Зеленский В. Д., Меретуков Г. М. Криминалистика. Санкт-Петербург: Юридический центр-Пресс, 2015. 755 с.

14. Курс криминалистики / Т. В. Аверьянова, Р. С. Белкин, Ю. Г. Корухов, Е. Р. Россинская. Москва: Норма: ИНФРА-М, 2023. 928 с.

15. Аминев Ф. Г. Актуальные проблемы формирования и использования экспертно-криминалистических учетов в расследовании и раскрытии преступлений: монография. Уфа: РИО БашГУ, 2004. 182 с.

16. Тьюки Дж. Анализ результатов наблюдений. Разведочный анализ. М.: Мир, 1981. 696 с.

17. Бахтеев Д. В. Частные криминалистические теории как источник для разработки прикладных систем искусственного интеллекта в следственной деятельности // Сибирские уголовно-процессуальные и криминалистические чтения. 2020. № 2 (28). С. 32–43.

REFERENCES

1. Digital traces of crimes: monograph / A. M. Bagmet, V. V. Bychkov, S. Yu. Skobelin, N. N. Ilyin. Moscow: Prospect, 2023. 168 p. (In Russ.)

2. Identification of the causes of crime and crime prevention. General provisions / Grishanin P. F., Zuikov G. G., Krivosheev A. S., Ratinov A. R., et al. Moscow: Research Institute of Criminal Procedure of the Moscow Higher School of the Ministry of Public Protection of the USSR, 1967. 179 p. (In Russ.)

3. Belkin R. S. Forensic science: problems, trends, prospects. General and specific theories. Moscow: Legal Literature, 1987. 270 p. (In Russ.)

4. Skobelin S. Yu. Digital forensics: object and directions of development // Russian investigator. 2020. No. 4. P. 42–44. (In Russ.)

5. Digital forensics / edited by V. B. Vekhov, S. V. Zuev. Moscow: Yurait, 2025. 490 p. (In Russ.)

6. Theory of information and computer support for forensic activities: monograph / edited by E. R. Rossinskaya. Moscow: Prospect, 2022. 254 p. (In Russ.)

7. Horsman G., Sunde N. Unboxing the digital forensic investigation process // Science and Justice. 2022. No. 62. P. 171–180. (In Eng.)

8. Dunsin D., Ghanem M., Ouazzane K. A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response // Digital Investigation. 2024. No. 48. P. 1–22. (In Eng.)

9. Casino F., Dasaklis T. Research trends, challenges, and emerging topics in digital forensics: A review of reviews // IEEE Access. 2022. No. 10. V. P. 25464–25493. (In Eng.)

10. Mashkov S. A. Big data and forensics: opportunities and prospects // Siberian criminal procedure and forensic readings. 2024. No. 2. P. 78–86. (In Russ.)

11. Jian X., Siegel M., Towards a joint semantic analysis in mobile forensics environments // Digital Investigation. 2025. No. 52. P. 1–26. (In Eng.)

12. Lundberg E., Mozelius P. The potential effects of deepfakes on news media and entertainment // AI & Society. No. 11. 2024. P. 1–12. (In Eng.)

13. Zelensky V. D., Meretukov G. M. Forensic Science / V. D. Zelensky, . St. Petersburg: Legal Center-Press, 2015. 755 p. (In Russ.)

14. Course in Forensic Science / T. V. Averianova, R. S. Belkin, Yu. G. Korukhov, E. R. Rossinskaya. Moscow: Norma: INFRA-M, 2023. 928 p. (In Russ.)

15. Aminev F. G. Actual Problems of Formation and Use of Forensic Accounts in Investigation and Solving Crimes: Monograph. Ufa: RIO BashSU, 2004. 182 p. (In Russ.)

16. Tukey J. Analysis of Observation Results. Intelligence Analysis. Moscow: Mir, 1981. 696 p. (In Russ.)

17. Bakhteyev D. V. Private forensic theories as a source for the development of applied artificial intelligence systems in investigative activities // Siberian criminal procedural and forensic readings. 2020. No. 2 (28). P. 32–43. (In Russ.)

Информация об авторе:
З. И. Харисова, кандидат технических наук, доцент.

Information about the author:
Z. I. Kharisova, Candidate of Technology, Associate Professor.

Статья поступила в редакцию 25.06.2025; одобрена после рецензирования 30.06.2025; принята к публикации 26.09.2025.

The article was submitted 25.06.2025; approved after reviewing 30.06.2025; accepted for publication 26.09.2025.