Научная статья
УДК 343.985:004.896

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

ОПТИМИЗАЦИЯ ПРОЦЕССА ПОИСКА, АНАЛИЗА И ИНТЕРПРЕТАЦИИ ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ С ИСПОЛЬЗОВАНИЕМ АЛГОРИТМОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация. 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. В статье представлена возможность оптимизации процесса поиска, анализа и интерпретации цифровых доказательств с использованием подхода алгоритмизации, что предусматривает разработку новых программных технико-криминалистических средств. На примере преступлений в сфере компьютерной информации показана целесообразность внедрения интеллектуальных систем в криминалистику, что обусловлено необходимостью выявления закономерных связей между элементами криминалистической характеристики преступных деяний, анализа больших массивов данных в цифровом виде, выявления шаблонов преступной активности и оперативного принятия решений в условиях неопределенности.

Ключевые слова: цифровые доказательства, криминалистический алгоритм, расследование преступлений, алгоритмы расследования, цифровая криминалистика, искусственный интеллект, технико-криминалистическое средство, преступления в сфере компьютерной информации, киберпреступления, криминалистика 5.0

Для цитирования: Харисова З. И. Оптимизация процесса поиска, анализа и интерпретации цифровых доказательств с использованием алгоритмов искусственного интеллекта // Общество, право, государственность: ретроспектива и перспектива. 2025. № 3 (23). С. 60–69.

Original article

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

OPTIMIZATION OF THE SEARCH, ANALYSIS AND INTERPRETATION PROCESSES OF DIGITAL EVIDENCE BASED ON ARTIFICIAL INTELLIGENCE ALGORITHMS

Abstract. Criminalistics as a science that studies the mechanism of crime and the emergence of information about it, in the context of universal digitalization and intellectualization, acquires new research and practice-oriented opportunities. At the same time, artificial intelligence technologies are an additional tool integrated into the system of forensic means. The article presents the possibility of optimizing the process of searching, analyzing and interpreting digital evidence using an algorithmic approach, which leads to the development of software technical and forensic tools. The example of crimes in the field of computer information shows the feasibility of introducing intelligent systems into criminalistics, which is due to the need to identi-

fy natural relationships between elements of the criminalistics characteristics of criminal acts, analyze large amounts of data in digital form, identify patterns of criminal activity and prompt decision-making in conditions of uncertainty.

Keywords: digital evidence, criminalistics algorithm, crime investigation, investigation algorithms, digital forensics, artificial intelligence, forensic technology, computer crime, cybercrime, forensics 5.0

For citation: Kharisova Z. I. Optimization of the search, analysis and interpretation processes of digital evidence based on artificial intelligence algorithms // Society, law, statehood: retrospective and perspective. 2025. No. 3 (23). P. 60–69. (In Russ.)

Введение

Четвертый этап развития криминалистики (криминалистика 4.0)[1] тесно связан с интеграцией информационных технологий и подразумевает цифровизацию технико-криминалистических средств (далее − ТКС) в целях раскрытия и расследования преступлений, в частности, совершаемых с использованием технических средств в цифровой среде [1, с. 52], что соответствует довольно значимым на сегодняшний день научно-исследовательским приоритетам в области уголовно-правовых наук. Формирование информации о противоправном деянии, в частности о следах преступной активности, выступает системообразующим элементом, опосредующим взаимосвязь между криминальной и процессуально-познавательной деятельностью. Деятельность по раскрытию и расследованию преступлений рассматривается криминалистикой как процесс трансформации криминальной информации в доказательственную посредством поиска доказательств, их исследования и дальнейшей оценки, что часто возможно унифицировать путем разработки различных алгоритмов действий. Проведенный библиографический поиск с учетом морфологии слов свидетельствует о широкой распространенности подхода алгоритмизации процесса расследования преступлений. Так, расширенный поиск с использованием ключевых слов, операторов поиска и ранжирования результатов в международной библиографической базе данных Google Scholar, индексирующей научные работы из различных источников, включая академические издательства, репозитории и прочие источники, по фразе «алгоритм* расслед* преступлен*» выдает более 16 тыс. наименований научных изданий на русском языке и более 21 тыс. результатов по фразе crim* investigat* algorithm* на английском. Поиск с учетом морфологии в российской научной электронной библиотеке, интегрированной с Российским индексом научного цитирования eLibrary, по вышеуказанным фразам предоставляет более 29 тыс. результатов на русском языке и более 2 тыс. источников на английском языке соответственно, при этом унификация процессуальных действий в большей степени ориентирована на работу с доказательствами.

По этой причине важно выявить перспективные методы поиска, анализа и интерпретации одних из наиболее типичных на сегодняшний день и трудно обнаруживаемых следов преступлений в виде цифровых доказательств, интегрируя в эти процессы подход алгоритмизации.

Методы

В процессе исследования использовалась совокупность общих методов научного познания (описание, обобщение и сравнение), общенаучных (анализ, синтез), частнонаучных и специальных методов (кибернетический, формально-юридический, сравнительно-правовой), что позволило выявить направление оптимизации процесса поиска, анализа и интерпретации цифровых доказательств на основе алгоритмов искусственного интеллекта.

Результаты

Одним из важнейших элементов механизма совершения преступления является способ, значимость выявления которого об-

[1] Нестеров А. В. Виртуальные следы в криминалистике : учеб. М. : КноРус, 2024. С. 52.

условлена необходимостью установления следовой картины. Данный элемент криминалистической характеристики преступного деяния весьма специфичен, поскольку в условиях повсеместной цифровизации, помимо традиционных криминалистических следов, все чаще необходимо выявлять цифровые (электронные) следы. Свойство отражения, присущее всем видам и формам материи, заключается в том, что каждый объект материального мира в процессе взаимодействия с окружающей средой подвергается воздействию внешних факторов. Известно, что отражение присутствует всегда, когда происходит взаимодействие двух и более материальных объектов − объектов следообразования. Поэтому основой для распознавания способа совершения преступления часто служит следовая картина в виде материальных цифровых следов [2, с. 2], механизм следообразования которых является электронным или электромагнитным. Указанные цифровые следы возможно идентифицировать исключительно с использованием ТКС, специально разработанных, приспособленных или заимствованных из смежных криминалистике наук, с целью обнаружения, фиксации, изъятия или исследования доказательств либо для предотвращения преступлений.

Применение того или иного ТКС определяет технико-криминалистический и тактико-криминалистический (тактический) приемы. Криминалистическая методика, в свою очередь, объединяет положения криминалистической техники и криминалистической тактики применительно к конкретным условиям или задачам расследования определенного вида преступления и содержит систему научных положений и разрабатываемых на их основе рекомендаций по организации и осуществлению расследования и предотвращения преступлений [3, с. 6]. ТКС в совокупности с приемами криминалистических техники и тактики аккумулируются в криминалистической методике в соответствии с особенностями расследования конкретного вида преступного деяния. Соответственно, для решения той или иной криминалистической задачи выбирается наиболее эффективное ТКС [4, с. 360], позволяющее достигнуть наилучших результатов расследования в оптимальные сроки, что соотносимо с основными специальными задачами науки криминалистики. К числу ее дополнительных специальных задач также относят: привлечение данных естественных и технических наук в целях оптимизации научно-технического обеспечения раскрытия и расследования преступлений; совершенствование имеющихся ТКС и применяемых тактических приемов, методических рекомендаций; анализ практики с целью выявления потребностей в новых ТКС, а также установления степени надежности и перспективности тех, которые были ранее рекомендованы к внедрению.

Одна из групп закономерностей, составляющих предмет криминалистики, связана с собиранием, исследованием, оценкой и использованием доказательств. Собирание доказательств осуществляется с применением тех или иных методов и способов их обнаружения, фиксации, изъятия и сохранения, что является серьезной проблемой, особенно при расследовании преступлений в сфере компьютерной информации. Обнаружение представляет процесс отыскания криминалистически значимой информации, имеющей отношение к расследованию конкретного преступления. Фиксация предполагает процесс закрепления в установленном Уголовно-процессуальным кодексом Российской Федерации порядке обнаружения сведений и подразделяется на основные (в виде протоколирования или, например, создания скриншотов, видеозаписей) и факультативные (в виде составления схем, изготовления копий, слепков и пр.) способы. Изъятие доказательств связано с извлечением носителей информации, при этом под ее сохранением понимают процесс принятия мер по обеспечению целостности и последующей доступности собранных доказательств в первоначальном виде, например, для повторного исследования. Исследование и оценка (анализ) доказательств подразумевают их проверку

с целью выяснения их относимости, допустимости, достоверности и достаточности. Наконец, использование полученных доказательств предполагает процесс проверки изначально выдвинутых версий по расследуемому делу и применения всех собранных фактов.

Не менее важной частью предмета криминалистики являются непосредственно методы и средства раскрытия и расследования преступлений, исследования доказательств по делам, а также вопросы профилактики преступных деяний. Для криминалистического исследования технических средств, информационных систем и компьютерной информации необходим комплекс знаний, сформированный на базе теории информационно-компьютерного обеспечения криминалистической деятельности [5, с. 35]. Предметом входящего в указанную теорию учения о криминалистическом исследовании компьютерных средств и систем является система закономерностей собирания криминалистически значимой компьютерной информации, анализ которой предполагает разработку технико-криминалистических методов и средств, а также методик и приемов обнаружения, фиксации, изъятия и сохранения цифровых доказательств. Следует отметить, что криминалистическая техника, как раздел науки, представлена прежде всего системой знаний о закономерностях объективной действительности, составляющих научную основу разработки ТКС, приемов и методов, предназначенных для использования в раскрытии и расследовании преступлений[1]. Развитие информационных технологий постоянно опережает развитие правовых рамок, создавая разрыв между возможностями преступников и инструментами, доступными правоохранительным органам. Этот диссонанс подчеркивает необходимость адаптации правовых механизмов к динамической природе киберугроз [6, с. 208], а сложность идентификации преступников и собирания доказательственной базы требует совершенствования криминалистических методов и средств расследования, что, в свою очередь, сонаправлено наиболее актуальным на сегодняшний день научно-исследовательским приоритетам в области криминалистики[2], а именно:

1) разработке и своевременной модернизации ТКС, тактических приемов и методологических алгоритмов поиска, фиксации и анализа криминалистически значимой информации;

2) оптимизации ТКС, соответствующих новым методам расследования и предотвращения преступной деятельности;

3) развитию общих и частных криминалистических теорий как теоретико-методологической базы формирования системы ТКС и методов судебного исследования.

Таким образом, можно сделать вывод о том, что рассмотренные выше категории составляют ключевые элементы упрощенной модели последовательности этапов расследования преступления, которую можно идентифицировать как каскадную модель жизненного цикла программного обеспечения [7, с. 14], заимствованную из методологии создания информационных систем, включающей их планирование, разработку, тестирование и развертку (от англ. software development life cycle [8, с. 356] − жизненный цикл разработки программного обеспечения) (рис.).

Так, в рассматриваемой модели способ совершения преступления, как исходный вектор, влияет на тип оставляемых цифровых следов. Цифровые следы, в свою очередь, обнаруживаются использованием ТКС, которые определяют методику расследования, алгоритм действий для поиска и собирания доказательств и их дальнейшей юридической интерпретации. Модель представленного вида является динамичной, элементы ее находятся в тесной взаимосвязи. Изменение исходного вектора в виде спосо-

[1] Зеленский В. Д., Меретуков Г. М. Криминалистика : учеб. СПб. : Юридический центр-Пресс, 2015. С. 115.

[2] Криминалистика : учеб. / Т. В. Аверьянова, Е. Р. Россинская, Р. С. Белкин, Е. Г. Корухов. М. : Норма, 2023. С. 66.

Рис. Упрощенная модель последовательности этапов расследования преступления (на примере преступления в сфере компьютерной информации)

ба совершения преступления должно закономерно влиять на все последующие этапы, обеспечивая их непрерывное совершенствование.

Преступления в сфере компьютерной информации, в отличие от традиционных форм преступных деяний, совершаются с использованием технических средств и различных информационно-телекоммуникационных технологий, что формирует трудно поддающуюся для криминалистического исследования цифровую среду. По этой причине расследование рассматриваемых в качестве примера преступлений (совершаемых в сфере компьютерной информации) в большей степени требует применения методов и средств, сформированных на базе информационных технологий (аналогичных по своей природе инструментам, используемым злоумышленниками).

Как подотрасль криминалистической науки (условно – род судебных экспертиз), цифровая криминалистика базируется на поиске, фиксации, собирании, анализе и интерпретации цифровых доказательств, которые осуществляются с использованием ТКС в виде программного обеспечения, что позволяет сохранить целостность следовой картины, точность и воспроизводимость результатов исследований криминалистически значимой информации. По этой причине целесообразно дальнейшее рассмотрение особенностей расследования преступлений с использованием программного обеспечения, что позволит в дальнейшем сформировать концептуальные основы криминалистического исследования цифровой информации, способствующие решению имеющихся в настоящее время проблем в деятельности по поиску цифровых доказательств.

Рассмотрение теоретических и методологических основ создания и использования типовых моделей преступной деятельности, выявление присущих ей закономерностей, а также практика ее типизации и моделирования послужили импульсом для новых криминалистических разработок, объектом изучения которых стал метод моделирования, что создало предпосылки формирования и развития метода ситуационного подхода к расследованию преступлений (теории криминалистической ситуалогии) [9, с. 18]. Однако отказ от универсализации схем расследования для всех категорий преступлений обусловливает необходимость разработки частных криминалистических методик, ориентированных на типовые следственные ситуации, характерные для конкретных видов и моделей преступных деяний, и предусматривающих дифференцированные подходы к организации их расследования. Соответственно, любая частная криминали-

стическая методика может быть представлена набором криминалистических алгоритмов (программ) расследования [10, с. 164] и моделей, формализованных на основе современных подходов к обработке данных.

Несмотря на то, что работа по систематизации и типологизации следственных ситуаций проводится давно, на сегодняшний день отчетливо прослеживается их принципиальная значимость для построения эффективных программных ТКС, однако в полной мере ресурс их не воплощен. Обусловлено это необходимостью реализации сложных динамичных (самообучающихся) алгоритмов расследования, что возможно лишь на основе технологий искусственного интеллекта (машинного обучения), в основу которых заложены математические методы (математический анализ, линейная алгебра и матричные вычисления, теория вероятностей и математической статистики, численные методы оптимизации, теория графов, логика и алгоритмы и пр.).

В настоящее время при расследовании различных преступлений могут применяться алгоритмы с жестко детерминированными предписаниями[1] в виде методик расследования (методических рекомендаций), однако в условиях неочевидности следственной версии или принимаемого решения целесообразнее применять криминалистические алгоритмы эвристического типа, которые допускают в рамках системы предписаний автоматизированный или автоматический поиск оптимальных путей[2], в частности на основе искусственного интеллекта[3], оценку предпринятых действий и их корректировку при необходимости[4].

Комплекс алгоритмических решений на основе интеллектуальных технологий включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение, использующее методы машинного обучения, а также процессы и сервисы, обеспечивающие обработку данных и выбор оптимальных решений. Следует отметить, что к искусственному интеллекту в широком понимании относят технологии компьютерного зрения, обработки естественного языка, распознавания и синтеза речи, возможности интеллектуальной поддержки принятия решений, а также иные перспективные методы.

Одним из наиболее значимых направлений использования искусственного интеллекта в криминалистике является установление закономерных связей между элементами криминалистической характеристики преступления, что позволяет выявлять причинно-следственные и вероятностные связи между обстоятельствами преступных деяний, формулировать частные криминалистические версии, в том числе версии о распространенности (серийности) преступлений, идентифицировать лиц, потенциально причастных к преступной деятельности, и пр.

[1] Свидетельство о государственной регистрации программы для ЭВМ № 2020610510 Российская Федерация. БАЗИС – базовый анализ защищенности информационных систем : № 2019666679 : заявл. 17.12.2019 : опубл. 15.01.2020 / З. И. Харисова ; заявитель ФГКОУ ВО «Уфимский юридический институт Министерства внутренних дел Российской Федерации».

[2] Свидетельство о государственной регистрации программы для ЭВМ № 2024661188 Российская Федерация. Blockchain analytics [аналитика блокчейна] – расследование преступлений, связанных с использованием криптовалют и сети блокчейн : № 2024619990 : заявл. 06.05.2024 : опубл. 16.05.2024 / З. И. Харисова, Э. Д. Нугаева, А. С. Ишмеева ; заявитель ФГКОУ ВО «Уфимский юридический институт Министерства внутренних дел Российской Федерации».

[3] Свидетельство о государственной регистрации программы для ЭВМ № 2023667481 Российская Федерация. BIOSCAN – Интеллектуальная система распознавания биометрических данных на основе машинного обучения (ML), компьютерного зрения (CV) и искусственного интеллекта (AI) : № 2023666662: заявл. 08.08.2023 : опубл. 15.08.2023 / З. И. Харисова, Э. Д. Нугаева ; заявитель ФГКОУ ВО «Уфимский юридический институт Министерства внутренних дел Российской Федерации».

[4] Свидетельство о государственной регистрации программы для ЭВМ № 2022611631 Российская Федерация. Система мониторинга киберинцидентов Local SIEM : № 2022610610 : заявл. 19.01.2022 : опубл. 28.01.2022 / З. И. Харисова, В. В. Антонов, А. И. Рафиков ; заявитель ФГБОУ ВО «Уфимский государственный авиационный технический университет».

Наиболее перспективными в этой сфере представляются анализ и интерпретация цифровых доказательств. Следует также отметить наличие структурных и технических ограничений, связанных с фрагментацией существующих информационных ресурсов. На текущий момент базы данных различных ведомств являются несогласованными, разобщенными, что затрудняет доступ следователей и оперативных сотрудников к информации. Это закономерно приводит к мысли о необходимости разработки единой криминалистической информационной платформы с унифицированными протоколами доступа и возможностью интеллектуального анализа цифровых данных.

В качестве подтверждения важности применения искусственного интеллекта в криминалистике необходимо отметить исследование, проведенное Научно-исследовательским институтом криминалистики Следственного комитета Российской Федерации. Интеллектуальный анализ более 1000 уголовных дел о серийных преступлениях сексуального характера, совершенных 186 преступниками, позволил построить цифровые криминалистические модели серийных преступников, включающие 27 личностных признаков, географические координаты мест совершения преступлений, жительства преступника и потерпевшего, время совершения преступления, используемые средства совершения преступления и возраст потерпевших [11, с. 98]. Применение методов математической статистики и анализа данных на основе нейросетевых алгоритмов обеспечило точность прогнозирования на уровне 92–98 %, что свидетельствует о высокой криминалистической значимости примененных подходов.

При рассмотрении направлений повышения эффективности расследования преступлений с задействованием технологий искусственного интеллекта, в частности, для обработки цифровых доказательств представляется вполне целесообразным выделение видовых криминалистических характеристик. Именно методы искусственного интеллекта могут позволить провести тщательный корреляционный анализ цифровых данных, обеспечивая устранение ложных корреляций и составление корреляционных таблиц, отображающих коэффициенты взаимосвязанности между различными переменными анализа (элементами криминалистической характеристики преступления). Основой большинства выводов, формируемых искусственным интеллектом, могут являться закономерные связи, выявляемые между элементами криминалистической характеристики преступления. Однако в рамках этих закономерностей могут встречаться исключения и отклонения от типичных случаев. Преимуществом интеллектуальных систем является способность обрабатывать и учитывать такого рода отклонения, обучаясь на них, что позволяет выходить за рамки стереотипных представлений о взаимосвязях между элементами криминалистической характеристики и формировать новые структуры криминалистического знания, опираясь на вероятность, а не только на повторяемость.

Применение искусственного интеллекта также способствует развитию частных криминалистических теорий. Интеграция интеллектуальных технологий в указанные теории способствует расширению методологической базы криминалистики, трансформации ее понятийного аппарата и практических методик. Отсюда следует, что интеграция искусственного интеллекта в криминалистическую практику становится не просто желательной, но и объективно необходимой.

В связи с ростом объемов данных, связанных с киберпреступлениями, важным аспектом становится использование методов машинного обучения для анализа больших данных, выявления шаблонов преступной активности и оперативного принятия решений в условиях неопределенности. На сегодняшний день при расследовании преступлений традиционных средств и методов управления данными для реализации полноценного анализа формируемых больших массивов цифровых доказательств явно недостаточно.

Для решения указанной проблемы также возможно использование технологий искусственного интеллекта. Поскольку методы и способы совершения преступлений постоянно меняются, анализ, основанный на жестких алгоритмах, становится неприменим. Интеллектуальные технологии и машинное обучение, напротив, позволяют анализировать цифровые данные в режиме реального времени с возможностью выдачи решения по поставленной задаче с гибкой адаптацией к систематически изменяющимся характеристикам массивов информации.

Однако, наравне с преимуществами, существуют риски использования искусственного интеллекта в противодействии киберпреступности, связанные с предвзятым принятием решений. По этой причине в обязательном порядке необходимо использование технологий объяснимого искусственного интеллекта, то есть XAI-систем (от англ. explainable artificial intelligence (XAI) – объяснимый искусственный интеллект) [12, с. 13], обеспечивающих создание систем, способных объяснять свои действия и принимать решения понятным для человека образом. Обеспечить анализ больших массивов разнородных цифровых данных также можно лишь с применением методов искусственного интеллекта. Например, известны методы семантического анализа больших языковых моделей (от англ. large language model – большая языковая модель) для интерпретации смысла текста, учета контекста и генерации контекстно-адекватных ответов; разработаны алгоритмы мультимодальных нейросетей и XAI-систем для обработки естественного языка и распознавания контекстуальных связей и пр.

Заключение

Таким образом, использование технологий искусственного интеллекта в целях поиска, анализа и интерпретации цифровых доказательств представляет собой перспективное направление, способствующее развитию криминалистической науки и совершенствованию правоохранительной деятельности в целом. Оно отражает переход к новой парадигме криминалистического мышления, основанной на цифровом моделировании и интеллектуальном анализе данных.

Предлагаемый подход интеллектуализации криминалистических исследований соответствует направлению развития Индустрии 5.0 [13, с. 2] в свете формирования цифровых моделей объектов, явлений или процессов, прогнозирования и принятия решений на основе искусственного интеллекта, создания коллаборативных интеллектуальных роботизированных решений, способствующих взаимодействию человека с техникой, на основе технологий компьютерного зрения, машинного обучения и интеграции больших языковых моделей. По этой причине подход к направлениям противодействия современной преступности можно по аналогии именовать подходом «Криминалистика 5.0».

СПИСОК ИСТОЧНИКОВ

1. Волчецкая Т. С. Развитие языка криминалистики в условиях цифровизации // Высокотехнологичное право: современные вызовы : сб. материалов IV Междунар. науч.-практ. конф. (Москва – Красноярск, 17–20 февр. 2023 г.). Красноярск : КГАУ, 2023. С. 51–56.

2. Россинская Е. Р. Особенности оценки и использования в доказывании результатов судебных экспертиз в условиях цифровизации // Законы России: опыт, анализ, практика. 2021. № 3. С. 3–8.

3. Баев О. Я. Избранные работы. Воронеж : Изд-во ВГУ, 2011. Т. 2. 432 с.

4. Josang A. Cyber organizational structures and regulation // Cybersecurity. Cham : Springer, 2025. P. 355–375. https://doi.org/10.1007/978-3-031-68483-8_17.

5. Россинская Е. Р. Теория информационно-компьютерного обеспечения судебно-экспертной деятельности как новая частная теория судебной экспертологии // Вестник Университета имени О. Е. Кутафина. 2022. № 2 (90). С. 27–40.

6. Amoo O. O., Atadoga A., Abrahams T. O. The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system // World journal of advanced research and reviews. 2024. V. 21. P. 205–217.

7. Зараменских Е. П. Управление жизненным циклом информационных систем : моногр. Новосибирск : Изд-во ЦРНС, 2014. 270 с.

8. Benington H. D. Production of large computer programs // Annals of the history of computing. 1983. V. 5 (4). P. 350–361.

9. Волчецкая Т. С. Криминалистическая ситуалогия : моногр. М. ; Калининград : Калинингр. ун-т, 1997. 248 с.

10. Шаталов А. С. Алгоритмизация и программирование расследования преступлений в системе криминалистической методики // Право. Журнал Высшей школы экономики. 2017. № 2. С. 155–172.

11. Бессонов А. А. Современные информационные технологии на службе следствия // Сибирские уголовно-процессуальные и криминалистические чтения. 2022. № 1. С. 94–100. https://doi.org/10.17150/2411-6122.2022.1.94-100.

12. Sarker I. H. AI-Driven cybersecurity and threat intelligence: cyber automation, intelligent decision-making and explainability. Perth : Edith Cowan University (Springer Nature), 2024. 207 p.

13. Industry 5.0 : Towards a sustainable, human-centric and resilient European industry : an analytical review. Luxembourg : European Commission, 2021. 48 p.

REFERENCES

1. Volchetskaya T. S. Development of the language of criminalistics in conditions of digitalization // High-tech law: modern challenges: collection of materials of the 4th International scientific and practical conference (Moscow – Krasnoyarsk, February 17–20, 2023). Krasnoyarsk : Krasnoyarsk State Agrarian University, 2023. P. 51–56. (In Russ.)

2. Rossinskaya E. R. Features of evaluation and use in proving the results of forensic examinations in the context of digitalization // Laws of Russia: experience, analysis, practice. 2021. No. 3. P. 3–8. (In Russ.)

3. Baev O. Ya. Selected works. Voronezh : Voronezh State University Publishing House, 2011. Vol. 2. 432 p.

4. Josang A. Cyber organizational structures and regulation // Cybersecurity. Cham : Springer, 2025. P. 355–375. https://doi.org/10.1007/978-3-031-68483-8_17.

5. Rossinskaya E. R. Theory of information and computer support for forensic expert activities as a new private theory of forensic expertology // Courier of Kutafin Moscow State Law University. 2022. No. 2 (90). P. 27–40. (In Russ.)

6. Amoo O. O., Atadoga A., Abrahams T. O. The legal landscape of cybercrime: a review of contemporary issues in the criminal justice system // World journal of advanced research and reviews. 2024. Vol. 21. P. 205–217.

7. Zaramenskikh E. P. Information systems life cycle management : monograph. Novosibirsk : Center for the Development of Scientific Cooperation, 2014. 270 p. (In Russ.)

8. Benington H. D. Production of large computer programs // Annals of the history of computing. 1983. Vol. 5 (4). P. 350–361. (In Eng.)

9. Volchetskaya T. S. Forensic situationology : monograph. Moscow : Kaliningrad University, 1997. 248 p. (In Russ.)

10. Shatalov A. S. Algorithmization and programming of investigation in the criminalistics methodology // Law Journal of the Higher School of Economics. 2017. No. 2. P. 155–172. (In Russ.)

11. Bessonov A. A. Modern information technologies in the service of investigation // Siberian criminal procedure and criminalistic readings. 2022. No. 1. P. 94–100. https://doi.org/10.17150/2411-6122.2022.1.94-100 (In Russ.)

12. Sarker I. H. AI-Driven cybersecurity and threat intelligence: cyber automation, intelligent decision-making and explainability. Perth : Edith Cowan University (Springer Nature), 2024. 207 p.

13. Industry 5.0 : Towards a sustainable, human-centric and resilient European industry : an analytical review. Luxembourg : European Commission, 2021. 48 p.

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

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

Статья поступила в редакцию 26.06.2025; одобрена после рецензирования 30.06.2025; принята к публикации 26.09.2025.

The article was submitted 26.06.2025; approved after reviewing 30.06.2025; accepted for publication 26.09.2025.