Дата поступления рукописи в редакцию: 17.04.2026 г.
Дата принятия рукописи в печать: 27.05.2026 г.
DOI: 10.24412/2782-3849-2026-5-157-165

ШАГАПОВ Исаак Равильевич,

аспирант кафедры Криминалистики Института права ФГБОУ ВО «Уфимский Университет Науки и Технологий»,

e-mail: isa.shagapow@gmail.com

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

Аннотация. *Научная статья посвящена актуальным вопросам криминалистической методики использования специальных знаний при расследовании преступлений, совершаемых с применением технологий искусственного интеллекта. Анализируется специфика данной категории общественно-опасных деяний, характеризующихся повышенной латентностью, трансграничностью и сложностью следообразования в цифровой среде. Рассматривается эволюция понятия специальных знаний в контексте современных технологических вызовов. Автор обосновывает необходимость модернизации традиционных методов расследования и создания междисциплинарных экспертных групп. Предлагаются конкретные решения выявленных проблем, включая разработку национальных стандартов криминалистической экспертизы искусственного интеллекта, внедрение образовательных программ для подготовки специалистов и создание технологических инструментов атрибуции действий при использовании интеллектуальных систем в преступных целях.*

Ключевые слова: *искусственный интеллект, киберпреступность, специальные знания, криминалистическая экспертиза, цифровая форензика, методика расследования преступлений.*

SHAGAPOV Isaac Ravilevich,

postgraduate student of the Department Kriminalistika of the Institute of Law of the Ufa University of Science and Technology

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

Annotation. *The scientific article is devoted to topical issues of the criminalistic methodology of using special knowledge in the investigation of crimes committed using artificial intelligence technologies. The article analyzes the specifics of this category of socially dangerous acts, characterized by increased latency, cross-border nature and complexity of trace formation in the digital environment. The evolution of the concept of special knowledge in the context of modern technological challenges is considered. The author substantiates the need to modernize traditional investigative methods and create interdisciplinary expert groups. Specific solutions to the identified problems are proposed, including the development of national standards for the forensic examination of artificial intelligence, the introduction of educational programs for training specialists, and the creation of technological tools for attributing actions when using intelligent systems for criminal purposes.*

Key words: *artificial intelligence, cybercrime, special knowledge, forensic examination, digital forensics, methods of crime investigation.*

Интенсивное внедрение технологий искусственного интеллекта (далее – «ИИ») в различные области человеческой деятельности закономерно привело к их использованию в противоправных целях, что обусловило формирование качественно нового сегмента преступных проявлений. Криминальная среда традиционно демонстрирует высокую адаптивность к технологическим новациям, оперативно интегрируя возможности ИИ в механизмы совершения общественно опасных деяний, что создало принципиально иные условия для их раскрытия и расследования.

Специфика преступлений с применением

ИИ-технологий заключается в их повышенной латентности, многоэтапности подготовки и реализации, а также возможности дистанционного воздействия на объекты посягательства независимо от географических границ.

Данное обстоятельство детерминирует необходимость разработки специализированной методики расследования, учитывающей особенности следообразования в цифровой среде, специфику доказывания причастности конкретных лиц к использованию интеллектуальных систем в преступных целях, а также не только отечественный, но и международный характер взаимодействия при собирании и закреплении доказательственной информации в условиях трансграничного функционирования технологических платформ.

Как отмечал на коллегии Следственного комитета Российской Федерации (далее – «СК России») в докладе на заседании коллегии СК России от 3 марта 2023 г. [19], докладе на научно-практической конференции «Уголовно-правовое обеспечение информационной безопасности человечества» от 13 февраля 2025 г [20]. Председатель СК России А.И. Бастрыкин: «Наблюдается постоянная положительная динамика преступных деяний, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, и увеличение их доли в общей структуре преступности. Так, в Российской Федерации за 7 лет число указанных преступлений выросло в 7,5 раза, а их удельный вес - с 15% до 40%.», «…Следственный комитет активно развивает такое важное направление, как киберкриминалистика, которое повышает эффективность расследования подобных деяний.». Соглашаясь с Председателем СК России, отметим, что увеличение доли киберпреступлений с 15% до 40% в общей структуре преступности означает, что традиционные методы расследования и экспертизы требуют существенной модернизации и дополнения специальными знаниями в области цифровых технологий и искусственного интеллекта. Упоминание о развитии киберкриминалистики как приоритетного направления работы СК России подтверждает практическую востребованность научных разработок в этой сфере и создаёт контекст для обоснования необходимости совершенствования экспертно-криминалистического обеспечения расследования технологически сложных преступлений.

Кроме того, политико-правовая конъюнктура признает проблему использования ИИ-технологий при совершении преступлений, что соотносится с поручением главы российского государства, Президента России В.В. Путина: «рассмотреть вопрос о целесообразности признания в качестве обстоятельства, отягчающего ответственность или наказание, использования при совершении правонарушения (преступления) технологий искусственного интеллекта и при необходимости обеспечить внесение» [21].

В условиях глобальной эскалации преступных посягательств, совершаемых посредством использования ИИ-технологий, криминалистическая наука сталкивается с императивной потребностью модернизации инструментария их обнаружения и расследования.

Сложившаяся система организационно-тактических алгоритмов, апробированных методов документирования преступной деятельности и процессуальных механизмов доказывания демонстрирует выраженную ограниченность при работе со следственными ситуациями, возникающими в контексте применения преступниками интеллектуальных систем.

Представляется, что конвенциональные подходы к анализу цифровых следов, ориентированные на исследование структурированных массивов информации ограниченного объема, утрачивают практическую значимость в условиях необходимости процессуального осмысления гетерогенных данных колоссального масштаба.

Таким образом, методологическая проблематика расследования общественно опасных деяний, реализуемых посредством ИИ-технологий, неизбежно приобретает транснациональное измерение.

Функциональные характеристики современных нейросетевых архитектур и глобальная интеграция цифровых инфраструктур объективно создают условия для совершения противоправных действий субъектами, территориально дистанцированными от юрисдикции причинения вреда. Подобная экстерриториальность криминальной активности существенно осложняет реализацию следственных мероприятий, направленных на процессуальную идентификацию и установление лиц, использующих интеллектуальные системы в преступных целях, что обусловливает потребность в формировании скоординированных государственных и транснациональных механизмов криминалистического противодействия.

Кроме того, специфика методики расследования преступлений, совершенных с применением ИИ, систематически становится

предметом профессионального обсуждения в рамках международных институциональных площадок, включая структуры Организации Объединенных Наций [22], Совета Европы [23], а также специализированные правоохранительные органы транснационального уровня.

В данной парадигме, обоснованно отмечает Г.В. Семеко, что чрезвычайная степень общественной опасности таких форм криминальной активности заключается в нанесении огромного экономического ущерба, который затрагивает не только конкретных граждан и организации, но и финансовую систему как отдельно взятых стран, так и глобальной экономики в целом [13].

Следует подчеркнуть, что параллельно с развитием механизмов транснационального сотрудничества в сфере противодействия цифровым правонарушениям актуализируется вопрос формирования на внутригосударственном уровне концептуального аппарата, позволяющего юридически квалифицировать преступные деяния, реализуемые в киберпространстве, и разработать комплексные криминалистические методики их расследования с привлечением специализированных экспертных компетенций, что приобретает особую значимость применительно к качественно новой категории противоправных посягательств, характеризующихся использованием ИИ-технологий в качестве инструментария криминальной активности.

Рассматривая преступления, совершенные использованием ИИ, целесообразно отметить, что данный вид преступной деятельности относится к числу киберпреступлений.

В доктрине уголовного права существуют различные научные позиции относительно сущностного наполнения термина «киберпреступление».

В частности, согласно позиции А.С. Мирончика, киберпреступления в расширительной трактовке представляют собой противоправные общественно опасные действия, направленные первостепенно против компьютерных систем, однако, одновременно причиняющие вред и иным охраняемым законом интересам, среди которых выделяются безопасность государства и международного сообщества (проявления кибертерроризма), имущественная сфера субъектов гражданского оборота (хищения и мошеннические операции в цифровой среде), интеллектуальная собственность (незаконное использование результатов творческой деятельности и цифровое пиратство) [10].

Соглашаясь с В.Б. Клишковым, отметим, что в условиях усложняющейся геополитической обстановки киберпреступность демонстрирует непрерывную трансформацию, порождая всё более утончённые и технологически сложные методы осуществления преступных посягательств [7].

Эффективное расследование преступлений в киберпространстве немыслимо без применения специальных знаний. Содержание указанных специальных знаний охватывает непосредственно познания в области разработки программного обеспечения и функционирования сетевой инфраструктуры, практические навыки создания защитных программных решений против распространения вредоносного кода, равно как и практический опыт обнаружения и исследования цифровых следов преступной деятельности.

Киберпреступность характеризуется неуклонным совершенствованием преступных навыков правонарушителей, их высоким уровнем координации и консолидации в устойчивые криминальные формирования, а также значительной скрытностью от статистического учёта. Дополнительную специфику представляет нестандартная природа компонентов, формирующих вероятностную модель криминалистической характеристики инцидента в киберпространстве.

Преступные элементы выработали комплексную методологию противоправных действий, базирующуюся на передовых информационных технологиях, включая алгоритмы машинного обучения и системы ИИ. Цифровые технические средства применяются злоумышленниками на всех стадиях преступной деятельности - от предварительной подготовки до непосредственной реализации и согласования действий соучастников. Параллельно с этим лица, совершающие киберпреступления, демонстрируют высокую результативность в сокрытии идентификационных данных посредством технологий анонимизации IP-адресов, криптографической защиты информации, применения промежуточных серверов и аналогичных инструментов.

Необходимо подчеркнуть, что действующее уголовно-процессуальное законодательство Российской Федерации не содержит легального толкования термина «специальные знания». При этом, следует отметить, что в период дореволюционных событий, отечественный уголовный процесс (в частности, Устав уголовного судопроизводства) устанавливал конкретные сферы применения таких знаний, относя к ним компетенции научного, технического, художественного либо ремесленного характера [24].

Ю.К. Орлов отмечал, что специальными

признаются знания, находящиеся за границами базового образовательного уровня и обыденных представлений, которыми располагает ограниченный круг специалистов [11]. Вместе с тем, данная концепция вызывает дискуссии, поскольку критерии житейского опыта невозможно унифицировать - они варьируются применительно к каждой отдельной личности.

Ю.Г. Корухов интерпретировал специальные знания как комплекс сведений из конкретной сферы науки, техники либо искусства, применяемых в качестве доказательственного материала при расследовании уголовных дел [8].

Наиболее методологически выверенной, с нашей точки зрения, представляется дефиниция, сформулированная В.И. Шикановым [18]. Охватывая знания из многообразных направлений естественнонаучных и технических дисциплин, различных художественных форм и ремесленных специальностей, включая прикладной опыт и профессиональные навыки, В.И. Шиканов концентрирует внимание на функциональном предназначении их использования в уголовно-процессуальной деятельности - выявление и изучение фактических обстоятельств, составляющих предмет доказывания. Одновременно с этим, В.И. Шиканов выводит за пределы специальных те знания, которые являются общедоступными и составляют базовый образовательный минимум населения, равно как и юридические познания, связанные с квалификацией деяний по уголовному закону и принятием процессуальных решений.

Приведенные научные концепции сохраняют свою значимость и сегодня, однако в современных условиях интенсивного проникновения цифровых технологий и интеллектуальных систем в криминальную среду назрела необходимость концептуального обогащения содержательного наполнения категории «специальные знания».

Проанализировав представленные трактовки специальных знаний, предложенные Р.С. Белкиным [1], К.А. Букаловым [2], В.И. Гончаренко [3], Г.И. Грамовичем [4], А.М. Зининым и Н.П. Майлис [6], В.К. Лисиченко и В.В. Циркалем [9], О.В. Евстигнеевой [5], Е.Р. Россинской и А.И. Усовым [12], Н.И. Трапезниковой [15], Д.А. Харченко [16], Д.П. Чипуром [17] и другими научными деятелями, возможно констатировать, что преобладающая часть правоведов придерживается концепции структурирования специальных знаний через систему познаний и практического опыта, аккумулирующего профессиональные компетенции и навыки.

Анализ научных дефиниций специальных знаний позволяет выявить ключевые характеристики, определяющие природу такого знания как специального, при этом некоторые из них остаются предметом научных дискуссий. К таким характеристикам относится представление о специальных знаниях как о комплексе познаний, практических навыков и профессионального опыта конкретного субъекта - эксперта или специалиста. Существенным признаком выступает относимость знания к предмету исследования. Также, традиционно подчеркивается, что специальные знания формируются в определенных сферах именно человеческой активности - научной, технической, художественной или ремесленной.

Представляется, что использование ИИ и самообучающихся алгоритмов как новой формы специального знания качественно отличается от человеческой деятельности. Устоявшимся является исключение юридических познаний в сфере уголовно-правовых наук из категории специальных. Наконец, специальные знания определяются как профессиональные познания, приобретенные посредством целенаправленной подготовки или в ходе профессиональной практики, при этом не учитываются профессиональные знания должностного лица, осуществляющего производство по уголовному делу.

В контексте данного аспекта специальных знаний необходимо признать их динамическую природу и непрерывное видоизменение. Исследователи обоснованно указывают на двунаправленный процесс эволюции этих знаний [14].

С одной стороны, познания, которые прежде составляли исключительную прерогативу компетентных специалистов, постепенно становятся достоянием широкой общественности и утрачивают статус специальных - показательным примером служат элементарные навыки работы с компьютерными технологиями.

С другой стороны, наблюдается обратная тенденция: юридические познания, традиционно считавшиеся неотъемлемой частью профессионального арсенала следователя, прокурорского работника и судьи, все активнее признаются в качестве специальных знаний. Указанное обусловлено колоссальным расширением правовой системы и её углубленной специализацией, вследствие чего практически невозможно обнаружить профессионала, обладающего универсальными познаниями во всех без исключения правовых сферах и механизмах, что особенно актуально при расследовании правонарушений.

Анализируя методологию применения специальных знаний в криминалистической практике, следует отметить, что речь идёт о целостной совокупности научно-обоснованных

методов и инструментов использования знаний из разнообразных научных дисциплин, технических отраслей, творческих направлений и прикладных ремёсел для эффективного решения задач по выявлению и расследованию противоправных деяний.

В контексте расследования преступной деятельности, осуществляемой посредством ИИ-технологий, целесообразно использовать интегрированную методологию, предполагающую вовлечение специалистов по информационным системам, разработке программного обеспечения, алгоритмам самообучения и компьютерной форензике.

На первоначальной стадии следственных мероприятий профильные эксперты должны осуществлять обнаружение и идентификацию признаков задействования систем ИИ путём изучения журналов событий, алгоритмических конструкций, массивов данных для обучения и характерных особенностей функционирования программных решений, что позволит зафиксировать применение интеллектуальных технологий в преступном механизме.

Значительную трудность составляет установление носителя юридической ответственности, так как возникает необходимость чёткого разделения функционирования непосредственно интеллектуальной системы, действий её создателей, администраторов и непосредственных пользователей, что обуславливает необходимость проведения многоаспектных программно-аппаратных исследований для выявления причинно-следственных механизмов между человеческими действиями и итогами функционирования алгоритмических процессов. Специалисты подвергают анализу программный код, структуру искусственных нейронных сетей, тренировочные наборы данных и механизмы формирования решений

интеллектуальными системами с целью обнаружения намеренных искажений, встроенных недостатков безопасности или злоумышленного применения технологических возможностей при осуществлении обманных действий, компьютерных правонарушений, фальсификации информационного контента или производства поддельных медиа-материалов. Экспертное криминалистическое изучение охватывает исследование цифровых следов, сопутствующих информационных данных, потоков сетевого обмена и процессов взаимодействия ИИ-систем с внешними информационными источниками, при этом, специалистам следует задействовать технологии реконструктивного анализа программных решений, методики обработки массивных информационных массивов и профильный инструментарий для получения и истолкования электронных улик.

Вместе с тем, центральным направлением работы становится выявление преднамеренности и виновности человека, осуществляющего применение ИИ-технологий, что предполагает экспертное изучение конфигурационных параметров системы, процессов её обучающей подготовки, внесённых алгоритмических изменений и документальных свидетельств, удостоверяющих намеренное задействование ИИ для реализации противоправных замыслов, что обусловливает потребность в фундаментальной междисциплинарной компетентности, объединяющей юридическую, технологическую и криминалистическую сферы.

Анализируя современные проблематики методологии применения специализированных экспертных компетенций в криминалистической практике при производстве расследований противоправных деяний с задействованием искусственного интеллекта, целесообразно отметить нижеследующее.

Актуальные вопросы методики использования специальных знаний в криминалистике при расследовании преступлений с использованием искусственного интеллекта			
№	**Проблематика**	**Сущность**	**Предлагаемые пути решения**
1.	Недостаток квалифицированных специалистов	Отсутствие экспертов, обладающих одновременно знаниями в области криминалистики, искусственного интеллекта, машинного обучения и программирования	Создание специализированных образовательных программ и курсов повышения квалификации; формирование междисциплинарных экспертных групп; привлечение IT-специалистов в качестве консультантов
2.	Отсутствие унифицированных методик экспертизы	Нет стандартизированных процедур исследования ИИ-систем, что приводит к разночтениям в экспертных заключениях	Разработка национальных и международных стандартов криминалистической экспертизы ИИ-технологий; создание методических рекомендаций и протоколов исследования
3.	Сложность атрибуции действий	Трудность установления, кто несет ответственность: разработчик алгоритма, пользователь системы или сама ИИ-система	Создание технических методов трассировки действий пользователей; анализ логов и истории взаимодействия; разработка правовых критериев определения субъекта ответственности
4.	Проблема «черного ящика»	Непрозрачность работы нейронных сетей и невозможность объяснить логику принятия решений алгоритмом	Внедрение требований о применении объяснимого ИИ (XAI); разработка методов визуализации работы нейросетей; использование методов обратного инжиниринга

Таблица 1. Актуальные вопросы методики использования специальных знаний в криминалистике при расследовании преступлений с использованием искусственного интеллекта

Рассмотрим решение вышеуказанных актуальных вопросов в сфере методики расследования преступлений, совершенных с использованием искусственного интеллекта, более предметно.

Решение проблемы недостатка квалифицированных специалистов требует комплексного подхода к образованию и организации экспертной деятельности. В первую очередь необходимо внедрить программу «Цифровой криминалист» в ведущих юридических ВУЗах страны, рассчитанную на двухгодичную магистратуру с углубленным изучением алгоритмов машинного обучения, языков программирования Python, а также методов цифровой форензики (компьютерной криминалистики). Параллельно следует запустить краткосрочные курсы повышения квалификации «ИИ-следователь» для действующих экспертов-криминалистов продолжительностью ориентировочно шесть месяцев, где основной акцент делается на практическое освоение инструментов анализа искусственного интеллекта. Одновременно требуется формирование межведомственных центров компетенций, объединяющих криминалистов,

программистов и специалистов по машинному обучению в единые рабочие группы. Привлечение IT-консультантов из технологических компаний через механизм экспертных советов позволит обеспечить постоянный доступ к актуальным знаниям в облас ти искусственного интеллекта.

Для устранения отсутствия унифицированных методик экспертизы необходима разработка национального стандарта «ГОСТ Р «Криминалистическая экспертиза систем искусственного интеллекта», который должен установить единые требования к процедурам исследования. Данный стандарт должен включать четкие протоколы сбора цифровых доказательств, методы анализа алгоритмов и форматы представления результатов.

Решение проблемы атрибуции действий начинается с внедрения технологии «ИИ-след» - программного комплекса, позволяющего отслеживать все операции пользователей с системой искусственного интеллекта через создание неизменяемых записей в распределенном реестре. Каждое взаимодействие фиксируется с указанием времени, учетных данных пользователя и характера выполненных действий. На правовом уровне необходимо принятие методических рекомендаций «Критерии субъектной ответственности в ИИ-преступлениях», устанавливающих градацию ответственности в зависимости от степени контроля каждого участника над функционированием системы.

Преодоление проблемы непрозрачности нейронных сетей достигается через обязательное применение технологии методики локальной интерпретации моделей, которая показывает, какие входные параметры оказали наибольшее влияние на конкретное решение алгоритма. Метод обратного инжиниринга целесообразно реализовать через технологию, которая систематически подает на вход системы специально подготовленные данные и анализирует реакции алгоритма для восстановления внутренней логики его работы. Создание национального репозитория «Регистр ИИ-моделей» позволит хранить эталонные версии алгоритмов вместе с документацией об их архитектуре и принципах функционирования, что облегчит последующую экспертизу.

Таким образом, формирование специализированной криминалистической методики расследования преступлений с использованием ИИ представляет собой императивную необходимость современной правоохранительной системы, обусловленную качественной трансформацией криминальной среды и возрастанием технологической сложности противоправных деяний. Решение обозначенных проблем требует комплексного междисциплинарного подхода, включающего создание специализированных образовательных программ для подготовки экспертов-криминалистов с компетенциями в ИИ-области, разработку унифицированных национальных стандартов криминалистической экспертизы ИИ-систем, внедрение технологий трассировки действий пользователей для установления субъектов ответственности, а также применение методов объяснимого ИИ для преодоления проблемы непрозрачности алгоритмических решений. Эффективность противодействия преступлениям данной категории зависит от способности правоохранительных органов адаптировать традиционные криминалистические методы к специфике цифровой среды, обеспечить координацию между различными ведомствами и профильными специалистами, что в совокупности позволит создать надежную систему документирования, расследования и доказывания противоправной деятельности с применением интеллектуальных технологий.

Список литературы:

[1] Белкин Р.С. Криминалистическая энциклопедия / М. : Мегатрон-XXI, 2000. 333 с.

[2] Букалов К.А. Применение товароведческих познаний при проведении комплексной ревизии по требованию следователя // Теория и практика криминалистики и судебной экспертизы. Саратов, 1982. Вып. 4. С. 90.

[3] Гончаренко В.И. Использование данных естественных и технических наук в уголовном судопроизводстве: (методологические вопросы) / В.И. Гончаренко. Киев, 1980. 157 с.

[4] Грамович Г.И. Тактика использования специальных знаний в раскрытии и расследовании преступлений : учеб. пособ. / Минск, 1987. 66 с.

[5] Евстигнеева О.В. Использование специальных познаний в доказывании на предварительном следствии в российском уголовном процессе : дисс. канд. юрид. наук : Саратов, 1998. 194 с.

[6] Зинин А.М. Судебная экспертиза : учебник / А.М. Зинин, Н.П. Майлис. М. : Юрайт, 2002. 318 с.

[7] Клишков В.Б. Киберпреступность: понятие, признаки, основные направления противодействия // Вестник Нижегородского университета им. Н.И. Лобачевского. 2022. № 4. С. 106–114.

[8] Корухов Ю.Г. Правовые основы применения научно-технических средств при расследовании преступлений / М., 1974. 29 с.

[9] Лисиченко В.К. Использование специальных знаний в следственной и судебной

практике : учеб. пособ. / В.К. Лисиченко, В.В. Циркаль. Киев : Киев. гос. ун-т им. Т.Г. Шевченко, 1987. 100 с.

[10] Мирончик А.С. Хищения в электронной среде как разновидность информационных преступлений: проблемы разграничения и квалификации // Юридические исследования. 2019. № 9. С. 17–30.

[11] Орлов Ю.К. Заключение эксперта и его оценка по уголовным делам / М. : Юрист, 1995. 64 с.

[12] Россинская Е.Р. Судебная компьютерно-техническая экспертиза / Е.Р. Россинская, А.И. Усов. М. : Право и закон, 2001. 416 с.

[13] Семеко Г.В. Информационная безопасность в финансовом секторе: киберпреступность и стратегия // Социальные новации и социальные науки. 2020. № 1 С. 77–96.

[14] Специальные знания в уголовном судопроизводстве : хрестоматия / Е.В. Елагина, Т.Г. Николаева, Н.А. Данилова. СПб, 2022. 204 с.

[15] Трапезникова И.И. Специальные знания в уголовном процессе России: понятие, признаки, структура : автореф. дисс. канд. юрид. наук : Челябинск, 2004. 22 с.

[16] Харченко Д.А. Судебная экспертиза в российском уголовном судопроизводстве : автореф. дисс. канд. юрид. наук : Иркутск, 2006. 22 с.

[17] Чипура Д.П. Использование специальных экономических знаний при расследовании преступлений : автореф. дисс. канд. юрид. наук : Волгоград, 2005. 20 с.

[18] Шиканов В.И. Использование специальных познаний при расследовании убийств : учеб. пособие / Иркутск, 1976. 88 с.

[19] В Следственном комитете России состоялось заседание коллегии, на котором подведены итоги работы за 2022 год // Официальный сайт Следственного комитета Российской Федерации [Электронный ресурс]. URL:https://sledcom.ru/press/events/item/1771051/ (дата обращения: 17.10.2025).

[20] В Российской Федерации за семь лет число IT-преступлений выросло в 7,5 раза // Государственное информационное агентство России «ТАСС» [Электронный ресурс]. URL:https://tass.ru/obschestvo/23128087 (дата обращения: 17.10.2025).

[21] Перечень поручений по итогам совещания с членами Правительства от 5 марта 2025 г. // Официальный сайт Президента России [Электронный ресурс]. URL:http://www.kremlin.ru/acts/assignments/orders/76615 (дата обращения: 17.10.2025).

[22] В ООН обеспокоились темпами роста использования ИИ преступниками // Российское информационное агентство «РИА Новости» [Электронный ресурс]. URL:https://ria.ru/20250417/oon-2011848430.html (дата обращения: 17.10.2025).

[23] Европарламент одобрил первый в мире закон о запрете неприемлемого использования ИИ // Информационное агентство «Интерфакс» [Электронный ресурс]. URL:https://www.interfax.ru/digital/950209 (дата обращения: 17.10.2025).

[24] Устав уголовного судопроизводства от 20 ноября 1864 г. // Информационно-правовое обеспечение «Гарант» [Электронный ресурс]. URL:https://constitution.garant.ru/history/act1600-1918/3137/ (дата обращения: 17.10.2025).

References:

[1] Belkin R.S. Forensic Encyclopedia/M.: Megatron-XXI, 2000. 333 pp.

[2] Bukalov K.A. Application of commodity knowledge in a comprehensive audit at the request of the investigator//Theory and practice of criminalistics and forensic examination. Saratov, 1982. No. 4. S. 90.

[3] V.I. Goncharenko. Use of natural and technical sciences in criminal proceedings: (methodological issues)/V.I. Goncharenko. Kyiv, 1980. 157 pp.

[4] Gramovich G.I. Tactics of using special knowledge in solving and investigating crimes: tutory. method ./Minsk, 1987. 66 c.

[5] Evstigneeva O.V. Use of special knowledge in proving at the preliminary investigation in the Russian criminal trial: diss. cand. jurid. Sciences: Saratov, 1998. 194 pp.

[6] Zinin A.M. Forensic examination: textbook/A.M. Zinin, N.P. Mailis. M.: Yurayt, 2002. 318 p.

[7] Klishkov V.B. Cybercrime: concept, signs, main directions of counteraction//Bulletin of Nizhny Novgorod University named after N.I. Lobachevsky. 2022. № 4. S. 106-114.

[8] Korukhov Yu.G. Legal basis for the use of scientific and technical means in the investigation of crimes/M., 1974. 29 pp.

[9] Lisichenko V.K. Use of special knowledge in investigative and judicial practice: study. method ./V.K. Lisichenko, V.V. Circus. Kyiv: Kyiv. state. un-t them. T.G. Shevchenko, 1987. 100 s.

[10] Mironchik A.S. Theft in the electronic environment as a type of information crime: problems of distinction and qualification//Legal research. 2019. № 9. C. 17–30.

[11] Orlov Yu.K. Expert opinion and his assessment in criminal cases/M.: Lawyer, 1995. 64 pp.

[12] Rossinskaya E.R. Forensic computer-technical expertise/E.R. Rossinskaya, A.I. Usov. M.:

Law and Law, 2001. 416 p.

[13] Semeko G.V. Information Security in the Financial Sector: Cybercrime and Strategy//Social Innovation and Social Sciences. 2020. NO. 1 S. 77-96.

[14] Special knowledge in criminal proceedings: anthology/E.V. Elagina, T.G. Nikolaeva, N.A. Danilova. St. Petersburg, 2022. 204 pp.

[15] Trapeznikova I.I. Special knowledge in the criminal process of Russia: concept, signs, structure: author. diss. cand. jurid. Sciences: Chelyabinsk, 2004. 22 pp.

[16] D.A. Kharchenko. Forensic examination in Russian criminal proceedings: abstract. diss. cand. jurid. Sciences: Irkutsk, 2006. 22 pp.

[17] Chipura D.P. Use of special economic knowledge in crime investigation: ref. diss. cand. jurid. Sciences: Volgograd, 2005. 20 s.

[18] Shikanov V.I. The use of special knowledge in the investigation of murders: study. manual/Irkutsk, 1976. 88 pp.

[19] A board meeting was held at the Investigative Committee of Russia, at which the results of work for 2022 were summed up//Official website of the Investigative Committee of the Russian Federation [Electronic Resource]. URL: https://sledcom.ru/press/events/item/1771051/ (access date: 17.10.2025).

[20] In the Russian Federation, the number of IT crimes has increased 7.5 times in seven years//Russian State News Agency "TASS" [Electronic Resource]. URL: https://tass.ru/obschestvo/23128087 (access date: 17.10.2025).

[21] List of instructions following a meeting with members of the Government dated March 5, 2025//Official website of the President of Russia [Electronic resource]. URL: http://www.kremlin.ru/acts/assignments/orders/76615 (access date: 17.10.2025).

[22] The UN was concerned about the growth rate of AI use by criminals//Russian news agency RIA Novosti [Electronic Resource]. URL: https://ria.ru/20250417/oon-2011848430.html (access date: 17.10.2025).

[23] The European Parliament approved the world's first law banning the unacceptable use of AI// Interfax News Agency [Electronic Resource]. URL: https://www.interfax.ru/digital/950209 (access date: 17.10.2025).

[24] Charter of criminal proceedings of November 20, 1864//Information and legal support "Guarantor" [Electronic resource]. URL: https://constitution.garant.ru/history/act1600-1918/3137/ (access date: 17.10.2025).

