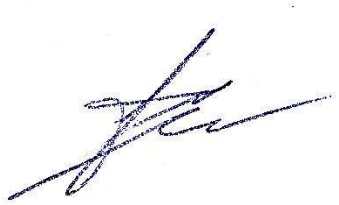
На правах рукописи



Фаниев Павел Андреевич

ИНФОРМАЦИОННЫЕ ОБЪЕКТЫ И ИХ МЕТАДАННЫЕ КАК ИСТОЧНИК КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМОЙ ИНФОРМАЦИИ ПО УГОЛОВНЫМ ДЕЛАМ

5.1.4. Уголовно-правовые науки

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата юридических наук

Краснодар – 2026

Работа выполнена в федеральном государственном казенном образовательном учреждении высшего образования «Краснодарский университет Министерства внутренних дел Российской Федерации»

Научный руководитель – кандидат юридических наук, доцент **Еремченко Владимир Игоревич**

Официальные оппоненты: **Гаврилин Юрий Викторович,** начальник кафедры управления органами расследования преступлений Академии управления МВД России, доктор юридических наук, профессор;

Мещеряков Владимир Алексеевич, профессор кафедры криминалистики юридического факультета Воронежского государственного университета, доктор юридических наук, профессор

Ведущая организация – Волгоградская академия МВД России

Защита состоится 2 октября 2026 г. в 09.00 часов на заседании диссертационного совета 03.2.005.01 при Краснодарском университете МВД России по адресу: 350005, г. Краснодар, ул. Ярославская, 128, корпус «А4», конференц-зал.

С диссертацией можно ознакомиться в библиотеке Краснодарского университета МВД России.

Полный текст диссертации, автореферат диссертации и отзыв научного руководителя размещены на официальном сайте Краснодарского университета МВД России по адресу: крду.мвд.рф

Автореферат разослан «___» июля 2026 г.

Ученый секретарь
диссертационного совета  Грибанов Евгений Викторович

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы диссертационного исследования. Современное развитие информационно-коммуникационных технологий характеризуется существенной трансформацией различных сфер жизнедеятельности, расширением возможностей коммуникации, обработки и передачи данных. В этих условиях данные, формируемые в цифровой среде, приобретают особое значение для расследования преступлений, поскольку отражают действия лиц, последовательность событий, способы коммуникации и иные обстоятельства, подлежащие доказыванию. Их выявление, фиксация, изъятие и исследование позволяют получить доказательственную информацию не только по делам о преступлениях в сфере компьютерной информации, но и при расследовании иных уголовно наказуемых деяний, когда следы в цифровой среде выступают важным источником криминалистически значимой информации. Раскрытие и расследование таких преступлений напрямую зависит от результатов изучения изымаемых цифровых следов, что обусловливает особую важность их исследования.

Анализ судебно-следственной и экспертной практики свидетельствует о наличии ряда организационно-тактических и методических проблем, возникающих как в ходе изъятия цифровых следов, так и при их последующем исследовании.

Постоянное усложнение информационно-коммуникационных технологий требует изменения сложившихся подходов к привлечению специалистов к участию в следственных действиях, связанных с изъятием и исследованием электронных носителей информации. Выбор специалистов следователем (дознавателем) зачастую осуществляется без оценки их профессиональной компетенции, учета специфики подлежащей решению задачи и сводится лишь к формальному подтверждению наличия специальных знаний в сфере информационно-коммуникационных технологий, что не позволяет получить весь объем криминалистически значимой информации.

Отдельной проблемой в процессе изъятия является несоблюдение участниками следственных действий технических требований и правил обращения с электронными носителями информации. Непонимание либо игнорирование ими особенностей функционирования отдельных видов устройств и носителей данных нередко приводит к утрате либо искажению криминалистически значимой информации.

Назначение компьютерных экспертиз часто носит шаблонный характер, задания инициаторов в основном предусматривают поиск файлов определенной категории (графических, видео и др.) без учета их криминалистической значимости по уголовному делу, упускается потенциальная возможность анализа метаданных.

Обращает на себя внимание, что многочисленные подходы к сущности и содержанию предмета и объекта судебной компьютерной экспертизы не в полной мере учитывают современное состояние информационно-коммуникационных технологий, что влечет неполное выявление и исследование цифровых следов.

Технологическая сложность современных информационных систем и многообразие форм представления цифровых данных объективно требуют конкретизации потенциальных объектов исследования, которые могут быть объединены понятием «информационный объект». Однако в настоящее время отсутствует ориентированное на следственную и экспертную практику определение данного термина, а также недостаточно разработаны подходы к типологизации таких объектов, которые могли бы использоваться как инициаторами судебной компьютерной экспертизы, так и экспертами непосредственно при ее производстве.

Кроме того, отмечается недостаточная разработанность методического обеспечения судебной компьютерной экспертизы. В экспертно-криминалистических подразделениях системы МВД России рекомендована к применению единая методика, ориентированная преимущественно на поиск компьютерной информации на внешних носителях по заданным критериям. Вместе с тем не всегда обеспечена возможность получения ориентирующей информации при исследовании данных, размещенных в сети Интернет, по причине ограничения специалиста возможностью исследования только информации, содержащейся на представленном ему электронном носителе, что препятствует получению всего объема потенциально доступных криминалистически значимых сведений. В Судебно-экспертном центре Следственного комитета Российской Федерации методическое обеспечение компьютерно-технических исследований и экспертиз также представлено ограниченным количеством методик. Отсутствует и единообразие подходов к исследованию цифровых следов в различных ведомственных экспертных учреждениях. Это позволяет констатировать незавершенность формирования научно-методической базы в данной области и необходимость ее дальнейшего развития.

Указанные проблемы приводят к снижению эффективности расследования, что подтверждается официальной статистикой ГИАЦ МВД России. В частности, анализ статистических данных за 2017–2025 гг. фиксирует семикратный рост числа преступлений, совершенных с использованием информационно-коммуникационных технологий и в сфере компьютерной информации (с 90,5 до 675,3 тыс.), при этом их раскрываемость остается стабильно низкой. Фактически раскрывается только четверть таких преступлений, что свидетельствует о наличии нерешенных проблем в деятельности правоохранительных органов как при получении доказательств совершения преступления по результатам производства отдельных следственных действий, так и при проведении экспертных исследований электронных носителей информации.

Таким образом, несмотря на то, что в цифровой среде информационные объекты и их метаданные выступают важным источником криминалистически значимой информации, позволяющим устанавливать обстоятельства совершения преступлений, существующие научно-методические и организационные подходы к обнаружению, фиксации, изъятию и исследованию таких объектов не позволяют в полной мере раскрыть их доказательственный потенциал. Это свидетельствует о необходимости дальнейшего научного осмысления сущности информационных объектов в цифровой среде, определения криминалистически значимых особенностей их метаданных, а также совершенствования организационно-тактических и методических основ их обнаружения, фиксации, изъятия и исследования в ходе расследования преступлений для формирования исчерпывающей совокупности доказательств.

Указанные проблемы требуют решения и обусловливают актуальность и практическую значимость данного диссертационного исследования.

Степень научной разработанности темы диссертационного исследования. Вопросы, связанные с классификацией цифровых следов, исследовались в научных трудах Н.Н. Безрукова, В.Б. Вехова, С.И. Гонгало, К.Е. Демина, А.В. Комова, В.А. Милашева, В.А. Мещерякова, А.Л. Осипенко, Е.С. Переверзева, Е.Р. Россинской, И.А. Рядовского, А.Б. Смушкина, А.И. Усова, А.Н. Яковлева и др.

Перспективы развития судебной компьютерной экспертизы и особенности исследования массивов информации в сети Интернет освещались в работах А.А. Васильева, В.Б. Вехова, К.Е. Демина,

О.Б. Дроновой, Д.В. Завьяловой, В.Ю. Иванова, А.В. Ким, М.М. Льянова, Ю.С. Руденковой, А.Б. Смушкина, А.И. Усова, Ш.Н. Хазиева, А.Н. Яковлева и некоторых других ученых.

Отдельные вопросы изъятия электронных носителей информации нашли отражение в исследованиях А.А. Балашовой, В.Ф. Васюкова, В.Б. Вехова, А.И. Гайдина, Ю.В. Гаврилина, В.В. Клевцова, П.В. Козловского, А.В. Комова, А.А. Кузнецова, Д.В. Муленкова, А.Л. Осипенко, С.В. Пропастина, А.Г. Себякина, П.В. Седельникова, А.Б. Смушкина, А.Б. Соколова и других авторов.

Работы указанных ученых внесли значительный вклад в разработку и решение широкого спектра научных проблем, связанных с использованием цифровых доказательств в уголовном судопроизводстве, заложили фундамент для понимания значимости цифровых доказательств, особенностей их использования в процессе доказывания. Вместе с тем до настоящего времени не получили должного научного осмысления вопросы, связанные с определением и систематизацией непосредственных объектов исследования судебной компьютерной экспертизы – информационных объектов и их метаданных, являющихся источником криминалистически значимой информации по уголовным делам. Остаются малоизученными вопросы комплексного подхода к их исследованию – от теоретико-правового обоснования и разработки организационно-тактических положений собирания до особенностей экспертного анализа в зависимости от типа носителя и среды размещения.

Изложенное указывает на необходимость изучения и последующего разрешения комплекса проблем, возникающих при изъятии и исследовании информационных объектов и их метаданных в ходе расследования преступлений

Объектом диссертационного исследования является правоприменительная практика обнаружения, фиксации, изъятия и исследования информационных объектов и их метаданных как носителей криминалистически значимой информации при расследовании преступлений.

Предметом диссертационного исследования выступают закономерности формирования теоретических, организационно-правовых, тактико-криминалистических и судебно-экспертных основ обнаружения, фиксации, изъятия и исследования информационных объектов и их метаданных, содержащих криминалистически значимую информацию, при расследовании преступлений.

Целью диссертационного исследования является формирование комплекса научных знаний о процессах получения криминалистически значимой информации из информационных объектов и их метаданных в уголовном судопроизводстве и разработка на его основе целостной системы мер по совершенствованию механизмов их обнаружения, фиксации, изъятия и исследования.

Достижение данной цели обусловливает последовательное решение следующих **задач**:

сформировать криминалистическое понятие информационных объектов как вещественных доказательств – потенциальных объектов судебной компьютерной экспертизы;

определить криминалистически значимые особенности метаданных информационных объектов;

разработать научно обоснованную типологию информационных объектов, направленную на оптимизацию процессов их обнаружения, фиксации, изъятия и последующего экспертного исследования;

предложить типологию данных, выявляемых в процессе доэкспертной оценки информационных объектов, обеспечивающую результативность экспертного исследования;

разработать предложения по совершенствованию нормативного правового регулирования организации производства судебной компьютерной экспертизы, а также расширению перечня экспертно-криминалистических учетов;

предложить организационно-тактические рекомендации по производству отдельных следственных действий, направленные на повышение результативности обнаружения, фиксации и изъятия информационных объектов и их метаданных;

разработать технологию получения ориентирующей информации при работе с информационными объектами и их метаданными, размещенными в общедоступных ресурсах информационно-телекоммуникационной сети Интернет;

разработать предложения по совершенствованию отдельных элементов экспертной технологии проведения судебной компьютерной экспертизы (исследование компьютерной информации).

Методологическую основу исследования составили общенаучные, частнонаучные и специально-юридические методы познания. Для раскрытия сущности информационных объектов и их метаданных как источника криминалистически значимой информации по уголовным делам использованы диалектический и системный подхо-

ды, а также общелогические приемы: анализ, синтез, индукция и дедукция.

Исследование криминалистически значимых особенностей метаданных информационных объектов, а также систематизация самих информационных объектов (с учетом возможностей их оптимального использования в экспертной практике) проводились с опорой на системно-структурный, формально-логический методы, а также методы классификации и обобщения.

Использование формально-юридического метода позволило осуществить предметный анализ правового регулирования обнаружения, фиксации, изъятия и исследования информационных объектов и их метаданных в уголовном судопроизводстве.

Деятельность правоохранительных органов по раскрытию и расследованию преступлений изучалась с применением конкретно-социологических методов, включая изучение форм статистической отчетности, материалов правоприменительной практики, результатов интервьюирования.

Совокупность использованных методов, а также междисциплинарный подход позволили сформировать целостное восприятие предметной области проведенного диссертационного исследования.

Нормативно-правовую базу исследования составляют Конституция Российской Федерации, Уголовный кодекс Российской Федерации, Уголовно-процессуальный кодекс Российской Федерации, Гражданский кодекс Российской Федерации, федеральные законы (в том числе от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 31.05.2001 № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации»), ведомственные и межведомственные нормативные правовые акты, регламентирующие процесс предварительного расследования преступлений, производства судебных экспертиз и ведения экспертно-криминалистических учетов.

Теоретической основой исследования послужили труды в области криминалистики, судебной экспертологии, уголовно-процессуального права, информатики и оперативно-розыскной деятельности. В диссертации использованы положения, изложенные в работах отечественных ученых В.Ю. Агибалова, В.Б. Вехова, К.Е. Демина, С.В. Зуева, В.Ю. Иванова, А.В. Комова, М.М. Льянова, В.А. Мещерякова, В.А. Милашева, А.Л. Осипенко, Н.О. Павленко, Е.С. Переверзева, Д.Л. Петрянина, Е.Р. Россинской, И.А. Рядовского,

Г.В. Саенко, А.И. Семикаленовой, А.Б. Смушкина, О.В. Тушкановой, А.И. Усова, И.Г. Чекунова, Н.К. Юркова, А.Н. Яковлева и др., а также зарубежных авторов (B. Carrier, Raphael A. Finkel, Greg Gagne, Peter Baer Galvin, Jenn Riley, Abraham Silberschatz, Andrew S. Tanenbaum и пр.).

Интеграция результатов отечественных и зарубежных исследований позволила всесторонне проанализировать предмет диссертационного исследования, решить поставленные задачи с учетом современных тенденций развития цифровых технологий.

Эмпирическую базу исследования составили:

результаты анализа официальных статистических данных ГИАЦ МВД России об уровне, динамике и структуре преступлений, совершенных с использованием информационно-коммуникационных технологий и в сфере компьютерной информации, на территории Российской Федерации в 2017–2025 гг., а также статистической отчетности экспертно-криминалистических подразделений системы МВД России (форма 1-НТП[1]) за 2018–2025 гг.;

результаты изучения, анализа и обобщения 530 заключений судебной компьютерной экспертизы;

результаты изучения и обобщения материалов следственной и судебной практики по производству отдельных следственных действий, направленных на изъятие объектов исследования судебной компьютерной экспертизы (проанализировано 127 материалов уголовных дел, отражающих производство осмотров и обысков, в части выявления, фиксации, изъятия и упаковки объектов, подлежащих исследованию в рамках судебной компьютерной экспертизы);

результаты интервьюирования 103 сотрудников, осуществляющих деятельность, связанную с раскрытием и расследованием рассматриваемой категории преступлений, из них: 40 – оперуполномоченные уголовного розыска, 40 – следователи следственных отделов территориальных органов МВД России, 23 – сотрудники иных подразделений (бюро специальных технических мероприятий, подразделения по организации борьбы с противоправным использованием информационно-коммуникационных технологий), а также 35 сотрудников экспертно-криминалистических подразделений системы МВД России, осуществляющих производство судебных компьютерных экспертиз.

[1] Утверждена приказом МВД России от 1 ноября 2008 г. № 952 «Об утверждении формы статистической отчетности “1-НТП”».

Научная новизна диссертационного исследования состоит в формировании комплекса научных знаний о процессах получения криминалистически значимой информации из информационных объектов и их метаданных в уголовном судопроизводстве и разработке на его основе целостной системы мер по совершенствованию механизмов их обнаружения, фиксации, изъятия и исследования.

Сформировано и научно обосновано понятие информационных объектов как вещественных доказательств – потенциальных объектов исследования судебной компьютерной экспертизы, уточняющее их содержание применительно к решению экспертных задач; определены криминалистически значимые особенности метаданных информационных объектов. Предложены криминалистическая типология информационных объектов, а также типология данных, получаемых в ходе их доэкспертной оценки.

В рамках организационно-правового совершенствования процесса изъятия и исследования информационных объектов и их метаданных обоснована необходимость выделения новых самостоятельных направлений исследований при производстве судебной компьютерной экспертизы, определены требования к компетентности специалиста и эксперта, необходимой для их производства, с учетом особенностей объектов исследования, используемых технологий и типовых экспертных задач. Разработан порядок создания в системе МВД России экспертно-криминалистического учета устойчивых цифровых следов, обеспечивающего расширение аналитических возможностей по выявлению связей между отдельными эпизодами преступления.

Предложены организационно-тактические рекомендации по работе с информационными объектами и их метаданными при производстве отдельных следственных действий, направленные на повышение результативности их выявления, фиксации, изъятия и обеспечение последующей сохранности.

Разработана технология получения ориентирующей информации при работе с информационными объектами и их метаданными, размещенными в общедоступных ресурсах информационно-телекоммуникационной сети Интернет, включающая цели, объекты, этапы исследования и требования к фиксации результатов. Предложено совершенствование отдельных элементов экспертной технологии проведения судебной компьютерной экспертизы (исследование компьютерной информации), способствующее повышению достовер-

ности, объективности, полноты и проверяемости результатов экспертного исследования.

Научную новизну диссертационного исследования подтверждают **основные положения, выносимые на защиту**:

1. При работе с цифровыми данными с целью получения криминалистически значимой информации целесообразно оперировать термином «информационный объект», под которым предлагается понимать логически целостную и идентифицируемую совокупность компьютерной информации, потенциально содержащую криминалистически значимые сведения и подлежащую исследованию с учетом взаимосвязи содержательной части (контента), метаданных (в том числе системных и прикладных – при их наличии и/или восстановимой форме) и контекстных связей (происхождение, среда формирования и использования, связи с иными информационными объектами, событиями и субъектами).

Предложенное определение ориентирует участников уголовного судопроизводства на собирание и исследование составных элементов информационных объектов не изолированно, а с учетом их взаимосвязей, что повышает криминалистическое значение получаемой доказательственной информации по уголовному делу.

2. Криминалистически значимыми особенностями метаданных информационного объекта являются: автоматизированность и системная обусловленность формирования и регистрации метаданных в цифровой среде; структурированность и машиночитаемость, обеспечивающие извлечение, проверяемость и сопоставимость сведений; связующая и диагностическая способность метаданных, позволяющая устанавливать происхождение, временные и иные атрибутивные характеристики информационных объектов, а также их связи с другими объектами и событиями. Совокупность указанных особенностей позволяет рассматривать метаданные в качестве самостоятельного источника криминалистически значимых сведений и объекта исследования судебной компьютерной экспертизы.

3. При обнаружении, фиксации и изъятии информационных объектов в рамках производства следственных действий, а также их последующем экспертном исследовании целесообразно использовать типологию информационных объектов по следующим основаниям: локализация, происхождение, защищенность от исследования, степень устойчивости, среда формирования. С учетом указанных оснований выделяются следующие типы информационных объектов:

а) по локализации: локальные; удаленно размещенные; синхронизируемые;

б) по происхождению: системные; пользовательские; прикладные; сетевые;

в) по защищенности от исследования[1]: защищенные; незащищенные;

г) по степени устойчивости: волатильные; динамически изменяемые; устойчиво сохраняемые;

д) по среде формирования: сформированные в стационарных вычислительных системах; мобильных устройствах; встроенных и специализированных устройствах; виртуализированных и облачных средах.

Предложенная типология позволяет определять последовательность действий и выбор необходимых инструментов и методов при собирании и последующем исследовании информационных объектов.

4. Для повышения результативности экспертного исследования целесообразно использовать в качестве основания для типологизации данных, выявляемых в процессе доэкспертной оценки информационных объектов, их роль в установлении обстоятельств преступления. Типология включает следующие типы данных: идентификационные; хронологические; контентные; контекстные; интегративные (комплексные).

Предложенный подход позволит инициатору назначения судебной экспертизы ставить перед экспертом вопросы, ориентированные на получение криминалистически значимых результатов, определять приоритетность направлений исследования, исходя из ценности различных типов данных, получать результаты экспертного исследования в структурированном виде, демонстрирующем искомые связи по делу, что облегчит их последующее восприятие участниками уголовного судопроизводства.

5. Для обеспечения всесторонности и полноты исследования информационных объектов необходимо дополнить перечень родов (видов) судебных экспертиз, проводимых в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации, утвержденный приказом МВД России от

[1] Под защищенностью от исследования в настоящей работе понимается наличие технических или программных средств, препятствующих легальному доступу к содержимому информационного объекта в ходе экспертного исследования (например, шифрование, парольная защита).

29.06.2005 № 511, новыми направлениями исследований, проводимых в рамках судебной компьютерной экспертизы:

«Исследование компьютерной информации, размещенной в общедоступных ресурсах информационно-телекоммуникационной сети Интернет»;

«Исследование информационной системы на предмет выявления признаков компрометации (несанкционированного доступа) и установления способа ее реализации»;

«Исследование компьютерной информации, содержащейся в мобильных устройствах и цифровых системах транспортных средств».

6. В целях реализации возможностей экспертно-криминалистических учетов для решения задач, возникающих при раскрытии и расследовании преступлений, совершенных с использованием информационно-коммуникационных технологий, необходимо дополнить перечень действующих экспертно-криминалистических учетов органов внутренних дел, регламентированный приказом МВД России от 10.02.2006 № 70, учетом устойчивых цифровых следов.

Целями формирования, ведения и использования учета устойчивых цифровых следов выступают расширение аналитической возможности по выявлению связей между отдельными эпизодами преступления, а также своевременный обмен сведениям между экспертно-криминалистическими и оперативными подразделениями, необходимыми для решения задач раскрытия и расследования преступлений.

Основными объектами предлагаемого информационного массива должны стать цифровые идентификаторы и связанные с ними технические атрибуты, полученные при проведении процессуальных действий, оперативно-розыскных мероприятий, в результате производства судебной компьютерной экспертизы:

а) сетевые идентификаторы и технические параметры сетевого взаимодействия (статические IP-адреса по протоколам IPv4/IPv6, аппаратные адреса сетевых интерфейсов (MAC), иные устойчивые сетевые идентификаторы при их наличии);

б) идентификаторы интернет-ресурсов и инфраструктуры (доменные имена и связанные с ними регистрационные сведения (WHOIS-данные и история изменений), сведения о TLS/SSL-сертификатах, используемых ресурсом);

в) пользовательские идентификаторы (адреса электронной почты, используемые для регистрации и длительной авторизации в сер-

висах; абонентские номера и связанные с ними учетные записи/идентификаторы в мессенджерах при наличии признаков устойчивой привязки и подтверждаемой истории использования).

Ведение учета необходимо осуществлять в форме электронной базы данных, размещенной в единой системе информационно-аналитического обеспечения деятельности Министерства внутренних дел Российской Федерации[1], с разграничением доступа пользователей к производимым операциям: внесение и верификация данных осуществляются сотрудниками экспертно-криминалистических подразделений системы МВД России; просмотр – сотрудниками оперативных подразделений системы МВД России без права внесения изменений, с ежемесячным аудитом обращений со стороны региональных курирующих подразделений. Ведение учета необходимо осуществлять на региональном и федеральном уровнях.

7. Организационно-тактические рекомендации по обнаружению, фиксации и изъятию информационных объектов и их метаданных, при производстве отдельных следственных действий, направленные на сохранение неизменности цифровых данных, полноту их фиксации, минимизацию рисков утраты или искажения, а также повышение качества последующей судебной компьютерной экспертизы и обоснованности экспертных выводов.

Предложенные организационно-тактические рекомендации включают: привлечение специалиста в области информационно-коммуникационных технологий для корректной фиксации и минимизации изменений цифровых данных; первоочередное извлечение энергозависимой информации при наличии признаков релевантных данных с минимальным вмешательством; определение границ исследуемой цифровой среды на основе логических, временных и юрисдикционных факторов; изоляцию устройства от сети и предотвращение удаленного воздействия с применением минимально изменяющих состояние цифровой среды способов анализа; видеофиксацию действий специалиста для их детализации и возможности последующего удостоверения; расчет и документирование хэш-значений цифровых копий и извлеченных файлов с указанием используемого программного обеспечения; детализированное отражение в протоколе временных меток, перечня объектов, параметров хэширования и очередности изъятия; фиксацию топологии подключений оконечных

[1] Далее – ИСОД МВД России.

устройств и схем хранения данных путем фотосъемки с маркировкой соединений и составлением плана-схемы.

8. Для получения ориентирующей информации при работе с информационными объектами и их метаданными, размещенными в общедоступных ресурсах информационно-телекоммуникационной сети Интернет, целесообразно использовать авторскую технологию проведения исследований, включающую цели, объекты и поэтапный порядок действий по получению, фиксации, анализу и систематизации сведений, содержащихся в общедоступных интернет-источниках, включая контент, технические и пользовательские метаданные, а также идентификаторы пользователя.

Разработанная технология предусматривает проведение исследования в зависимости от формы представления исследуемого объекта:

а) по предоставленным инициатором исследования электронным образам/снимкам интернет-ресурсов, выгрузкам и иным документированным копиям, записанным на внешние электронные носители информации либо размещенным в информационных системах, к которым обеспечен доступ специалисту;

б) по размещенным в сети Интернет информационным объектам (при невозможности их натурного предоставления) с использованием представленных инициатором назначения экспертизы исходных установочных сведений, обязательной фиксацией полученных данных и параметров доступа.

9. В целях повышения достоверности, объективности, полноты и проверяемости результатов экспертного исследования в отдельные элементы экспертной технологии проведения судебной компьютерной экспертизы (исследование компьютерной информации) следует включить:

применение при анализе объектов экспертного исследования типологии информационного объекта;

решение задач, связанных с исследованием журналов и артефактов программного обеспечения, выявлением следов подключения внешних носителей, а также исследованием стегоконтейнеров;

использование для решения частных экспертных задач, выходящих за пределы возможностей имеющихся в распоряжении экспертно-криминалистического подразделения аппаратно-программных комплексов, в качестве вспомогательного инструментария самостоятельно разработанного (авторского) программного обеспечения в порядке экспертной инициативы с обязательным отражением в исследова-

тельской части заключения эксперта корректности его функционирования.

Теоретическая значимость исследования заключается в развитии понятийного аппарата и методологических основ судебной компьютерной экспертизы. Полученные результаты уточняют научные представления об информационных объектах как объектах исследования, о роли и криминалистически значимых особенностях их метаданных, а также предлагают научно обоснованные подходы к исследованию цифровых данных. Сформулированные теоретические положения могут служить основой для дальнейших исследований и обоснования направлений совершенствования судебной компьютерной экспертизы и тактики производства отдельных следственных действий, связанных с обнаружением, фиксацией и изъятием цифровых следов.

Практическая значимость исследования заключается в возможности использования результатов диссертационного исследования и разработанных методических рекомендаций:

в следственной и экспертной практике – при участии специалиста в процессуальных действиях, связанных с обнаружением, фиксацией и изъятием цифровых следов, при назначении и производстве судебной компьютерной экспертизы, а также при разработке и актуализации методических материалов и действующей методики проведения судебной компьютерной экспертизы;

в образовательном процессе профильных образовательных организаций системы МВД России – при подготовке обучающихся по направлениям (специальностям), связанным с оперативно-розыскной деятельностью, расследованием преступлений, совершаемых с использованием информационно-коммуникационных технологий, и производством судебной экспертизы, в том числе по программам 40.03.02 Обеспечение законности и правопорядка (оперативно-розыскная деятельность, включая профиль, ориентированный на противодействие IT-преступлениям), 10.05.05 Безопасность информационных технологий в правоохранительной сфере (специализация «Компьютерная экспертиза»), 40.05.01 Правовое обеспечение национальной безопасности (уголовно-правовая специализация, направленность – расследование преступлений, совершаемых с использованием информационно-телекоммуникационных технологий), 40.05.03 Судебная экспертиза.

Достоверность результатов исследования обеспечена его проведением с учетом современных положений уголовно-процессуальной, уголовно-правовой и криминалистической науки, действующих нормативных правовых актов, а также с опорой на эмпирический материал, сформированный на основе анализа практики деятельности экспертно-криминалистических подразделений системы МВД России. При подготовке диссертационного исследования использован многолетний опыт работы соискателя экспертом в экспертно-криминалистических подразделениях системы МВД России. Достоверность и практическая применимость результатов подтверждены их апробацией в деятельности экспертно-криминалистических подразделений системы МВД России и в образовательных организациях, осуществляющих подготовку судебно-экспертных кадров для нужд МВД России.

Апробация результатов исследования. Результаты диссертационного исследования отражены в 11 научных статьях общим объемом 5,4 п. л., 7 из которых опубликованы в изданиях, рекомендованных Высшей аттестационной комиссией при Министерстве науки и высшего образования Российской Федерации, и в 2 учебно-методических рекомендациях общим объемом 6,8 п. л. В диссертации использованы результаты научных работ, ранее выполненных соискателем ученой степени лично.

Основные положения, выводы, предложения и рекомендации, разработанные по результатам диссертационного исследования, докладывались и обсуждались на заседаниях кафедры судебно-экспертной деятельности Краснодарского университета МВД России, а также на всероссийских и международных научно-практических мероприятиях: «Судебная экспертиза: российский и международный опыт» (Волгоград, 2024), «Цифровые технологии современной криминалистики, использование специальных знаний» (Москва, 2024), «Технико-криминалистическое обеспечение раскрытия и расследования преступлений» (Москва, 2024), «Информационные и телекоммуникационные технологии в противодействии экстремизму и терроризму» (Краснодар, 2025).

Результаты диссертационного исследования используются в учебном процессе Краснодарского университета МВД России и Московского ордена Почета университета МВД России имени В.Я. Кикотя, а также в практической деятельности УБК ГУ МВД России по Краснодарскому краю, экспертно-криминалистических под-

разделений: ЭКЦ ГУ МВД России по Краснодарскому краю, ЭКЦ ГУ МВД России по г. Санкт-Петербургу и Ленинградской области, ЭКЦ УМВД России по Астраханской области, ЭКЦ УМВД России по Брянской области, ЭКЦ ГУ МВД России по Новосибирской области и ЭКЦ УМВД России по Ханты-Мансийскому автономному округу – ЮГРЕ, что подтверждается соответствующими актами внедрения.

Структура диссертации включает введение, две главы, содержащие шесть параграфов, заключение, список литературы и приложения. Диссертационное исследование оформлено в соответствии с требованиями Высшей аттестационной комиссии при Министерстве науки и высшего образования Российской Федерации.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обосновывается актуальность темы диссертационного исследования, определяются его объект, предмет, цель и задачи, характеризуются методологическая основа, нормативная база и научная новизна работы, формулируются основные положения, выносимые на защиту, освещаются используемый эмпирический материал, теоретическая и практическая значимость, приводятся сведения об апробации полученных результатов.

Первая глава **«Теоретические и организационно-правовые основы криминалистического исследования информационных объектов и их метаданных»**, состоящая из трех параграфов, посвящена изучению существующих подходов к пониманию информационных объектов и криминалистически значимых особенностей их метаданных. Автором анализируются существующие типологии информационных объектов и получаемых при их изучении данных, а также основные проблемы организационного и правового характера, возникающие при исследовании информационных объектов, их метаданных, и подходы к выработке возможных путей их разрешения.

В первом параграфе ***«Понятие информационных объектов и криминалистически значимые особенности их метаданных»*** проведен анализ существующих нормативных и научных подходов к пониманию информационного объекта в различных областях знания. Установлено, что на этапах обнаружения, фиксации, изъятия и исследования цифровые данные традиционно объединяются категорией «компьютерная информация», которая, несмотря на техническую

точность, не отражает логическую целостность массивов данных, не позволяет отграничить один цифровой феномен от другого и игнорирует структурную неоднородность информации, в частности различие между содержательной частью, служебными сведениями и контекстными связями. Автор указывает, что категория «информационный объект» не получила должной теоретической разработки и практического применения, что в совокупности негативно сказывается на качестве процессов их обнаружения, фиксации, изъятия и исследования.

Проведенным анализом 530 постановлений о назначении судебных компьютерных экспертиз установлено, что более чем в 70% случаев инициатор проведения экспертизы формулирует запрос только в части наличия данных определенной категории, не конкретизируя его с учетом обстоятельств дела. При этом задачи по установлению источника, способов формирования и выявлению взаимосвязей обнаруженной информации перед экспертом, как правило, не ставятся. Кроме того, при формировании вопросов, выносимых на экспертное разрешение, метаданные как доказательственный ресурс либо полностью упускаются, либо сам термин используется поверхностно, без разъяснения его сути. Сложившийся подход, ориентированный на обнаружение «контента», без учета контекста и метаданных, не обеспечивает получение всех возможных сведений, значимых для дела, тем самым снижая весь доказательственный потенциал экспертного исследования.

С учетом изложенного автором обосновывается необходимость использования понятия «информационный объект» в качестве базовой категории для решения задач, связанных с обнаружением, фиксацией, изъятием и последующим исследованием цифровых данных. Сформулировано криминалистически ориентированное определение информационного объекта, учитывающее взаимосвязь содержательной части, метаданных и контекстных связей.

Рассмотрены источники формирования метаданных, особенности их автоматизированного создания программными средствами и операционными системами, а также их роль в структуре информационных объектов. Отмечено, что метаданные могут образовываться на различных уровнях функционирования информационных систем, формируясь в результате: работы операционной системы и прикладных программ; генерирования сетевой инфраструктурой и интернет-ресурсами; функционирования специализированных информационных систем, включая базы данных, облачные сервисы и системы журналирования. При этом автор обращает внимание, что, несмотря

на то, что большинство метаданных формируется автоматически, некоторые из них могут изменяться пользователем целенаправленно, что, в свою очередь, может свидетельствовать о попытках модификации следовой информации в случаях установления расхождений между автоматическими и пользовательскими метаданными. Отмечено, что метаданные способны фиксировать сведения о времени создания и изменения файлов, параметрах программной среды, характеристиках используемых устройств и иных обстоятельствах функционирования информационных систем.

На основе проведенного анализа определяются криминалистически значимые особенности метаданных информационных объектов. Сделан вывод о высокой криминалистической значимости метаданных, позволяющих устанавливать происхождение информационных объектов, выявлять факты их изменения или удаления, а также реконструировать последовательность действий пользователей в информационных системах.

Во втором параграфе ***«Типология информационных объектов и данных, получаемых при их исследовании»*** проведен анализ существующих подходов к систематизации информационных объектов. Установлено, что используемые в различных областях научного знания классификации не позволяют облегчить процессы систематизации информационных объектов, определения приоритетных направлений их изучения и выбора инструментов для их обнаружения, фиксации, извлечения и исследования при проведении следственных действий и экспертиз.

Разработана криминалистическая типология информационных объектов, учитывающая их локализацию, происхождение, защищенность от исследования, степень устойчивости и среду формирования.

Проведен анализ этапов осуществления кибератак, в результате которого выделены приоритетные направления поиска и анализа информационных объектов при расследовании преступлений с учетом текущего этапа совершения противоправного деяния. Предложена типология данных, выявляемых при исследовании информационных объектов на этапе доэкспертной оценки, которая включает в себя идентификационные, хронологические, контентные, контекстные и интегративные данные.

Сделан вывод о том, что использование разработанных типологий позволит оптимизировать процессы обнаружения, фиксации, изъятия и экспертного исследования информационных объектов; опре-

делить приоритетные направления исследования на этапе доэкспертной оценки и упорядочить получаемые результаты с учетом криминалистической значимости получаемых данных.

В третьем параграфе ***«Организационные и правовые аспекты работы с информационными объектами и их метаданными»*** на основе анализа действующей нормативно-правовой базы и эмпирического материала определен круг основных проблем в исследуемой сфере, требующих научного разрешения. Предложены пути их преодоления.

Изучение ведомственных нормативных правовых актов позволило обобщить подходы к определению уровня компетенции эксперта, осуществляющего производство судебных компьютерных экспертиз. Отмечено, что наиболее значимым недостатком существующего подхода является недостаточный учет постоянно усложняющихся объектов экспертного исследования, вызванный развитием информационных технологий. Предложено развитие трех новых направлений исследований в рамках судебной компьютерной экспертизы, основанных на различиях объектов исследования: «Исследование компьютерной информации, размещенной в общедоступных ресурсах информационно-телекоммуникационной сети Интернет», «Исследование информационной системы на предмет выявления признаков компрометации (несанкционированного доступа) и установления способа ее реализации», «Исследование компьютерной информации, содержащейся в мобильных устройствах и цифровых системах транспортных средств», которые в совокупности с уже существующими направлениями позволят осуществлять комплексное исследование цифровых следов. Предусмотрено внесение соответствующих дополнений в перечень родов (видов) судебных экспертиз, проводимых в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации, утвержденный приказом МВД России от 29.06.2005 № 511 «Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации».

Проанализированы существующие подходы и мнения ученых по вопросу формирования экспертно-криминалистических учетов цифровых следов. Установлено, что, несмотря на ввод в эксплуатацию специального программного обеспечения подсистемы интегрированного банка данных коллективного пользования федерального уровня (ИБД-Ф) «Дистанционное мошенничество», номенклатура учитываемой инфор-

мации остается недостаточной для решения частных задач расследования. В целях реализации потенциала криминалистической регистрации при раскрытии преступлений, совершаемых с использованием информационно-коммуникационных технологий, обоснована необходимость создания в системе МВД России специализированного экспертно-криминалистического учета устойчивых цифровых следов с внесением соответствующих изменений в перечень действующих экспертно-криминалистических учетов органов внутренних дел, регламентированный приказом МВД России от 10.02.2006 № 70 «Об организации использования экспертно-криминалистических учетов органов внутренних дел Российской Федерации». Формирование и ведение указанного вида учета позволит в полной мере проводить сопоставление изымаемых цифровых следов, а их разделение на устойчивые и временные позволит четко отграничить следы, которые могут быть использованы в качестве объектов экспертно-криминалистического учета, от тех, которые целесообразно учитывать только для решения вопроса об объединении нескольких уголовных дел в одно производство в рамках ИБД-Ф «Дистанционное мошенничество».

Рассмотрены пределы допустимости признания цифровых следов в качестве источника доказательств, в том числе при невозможности их повторного воспроизведения в рамках экспертизы. Сделан вывод о целесообразности внесения в ч. 1 ст. 307 УК РФ изменения, предусматривающего ответственность за дачу заведомо ложного заключения или показаний специалиста.

В результате анализа эмпирического материала выявлены отдельные проблемы, возникающие при обнаружении, фиксации и изъятии информационных объектов и их метаданных, связанные: с применением ненадлежащих способов работы с цифровыми следами и их носителями; недостаточными познаниями участников следственных действий в области информационных технологий; формализмом при определении компетенций лица, привлекаемого в качестве специалиста. Выработаны наиболее оптимальные пути их решения, включающие в себя: привлечение специалиста, обладающего специальными знаниями в области информационно-коммуникационных технологий; принятие мер по предотвращению удаленного воздействия на исследуемое устройство и данные; приоритетную фиксацию энергозависимых данных; дополнительную видеофиксацию действий специалиста с цифровыми устройствами; детализированную фиксацию в протоколе действий специалиста.

Вторая глава **«Тактико-криминалистическое и судебно-экспертное обеспечение работы с информационными объектами и их метаданными»** состоит из трех параграфов, в которых рассмотрены особенности проведения отдельных процессуальных действий по преступлениям, совершенным с использованием информационно-коммуникационных технологий и в сфере компьютерной информации, разработанная диссертантом технология получения ориентирующей информации при работе с информационными объектами и их метаданными, размещенными в общедоступных ресурсах информационно-телекоммуникационной сети Интернет, а также предложения по совершенствованию существующей технологии проведения судебной компьютерной экспертизы.

В первом параграфе ***«Тактико-криминалистические особенности производства отдельных следственных действий, предусматривающих обнаружение, фиксацию и изъятие информационных объектов и их метаданных»*** разработаны криминалистические рекомендации по проведению качественного сбора первоначальной следовой информации в цифровом пространстве.

Сформулированы организационно-тактические рекомендации по проведению подготовительного, рабочего и заключительного этапов осмотра места происшествия, учитывающие особенности работы с информационно-коммуникационными устройствами. Определен круг цифровых следов и сведений, поиск и установление которых наиболее целесообразны в зависимости от категории потерпевшего: для физических лиц – URL-адреса, полученные от злоумышленника, экземпляры устанавливаемого на устройство потерпевшего программного обеспечения, файлы, поступившие от преступника, номера телефонов, банковских счетов и карт, используемых злоумышленниками, характер контента, рассылаемого с похищенной учетной записи потерпевшего; для юридических лиц – все вышеперечисленные данные, а также характер похищенной информации, статус и уровень доступа скомпрометированных учетных записей организации, журналы работы программ удаленного доступа, параметры локальной сети и выявленные признаки несанкционированного перемещения данных внутри инфраструктуры, факты привлечения внешних подрядчиков, в том числе и для аудита информационной безопасности. Предложен порядок определения границ исследуемой цифровой среды на основании логических, временных и юрисдикционных факторов.

С учетом специфики преступлений, совершаемых с использованием информационно-коммуникационных технологий, предложены рекомендации по производству обысковых мероприятий, направленные не только на обнаружение, фиксацию и изъятие цифровых следов, но и на недопущение фактов их уничтожения, как умышленного (обыскиваемым лицом либо его сообщниками), так и неумышленного (в результате действий со стороны сотрудников, осуществляющих проведение обыска либо выемки). Подробно описаны рекомендуемые тактические приемы, в том числе связанные с использованием носимых видеорегистраторов и расчетом хэш-сумм для изымаемых цифровых следов, а также порядком их отражения в протоколе следственного действия.

Во втором параграфе ***«Современные возможности получения ориентирующей информации при работе с информационными объектами и их метаданными, размещенными в общедоступных ресурсах информационно-телекоммуникационной сети Интернет»*** представлен анализ опыта подразделений УБК и БСТМ МВД России, а также Следственного комитета Российской Федерации в части исследования цифрового пространства и получения криминалистически значимых сведений из открытых источников сети Интернет. Выявлен ряд проблем, связанных с использованием полученных в интернет-пространстве сведений, наиболее значимыми из которых являются: проблемы использования в качестве доказательств информации, полученной из сети Интернет в рамках оперативно-розыскных мероприятий; отсутствие единых методологических основ получения подобных сведений. На основании проведенного анализа автор приходит к выводу о целесообразности формирования направления предварительного исследования, ориентированного на поиск и анализ информационных объектов и их метаданных, размещенных в общедоступных ресурсах информационно-телекоммуникационной сети Интернет, проводимого в системе МВД России.

С учетом полученных результатов сформирована технология получения ориентирующей информации при работе с информационными объектами и их метаданными, размещенными в общедоступных ресурсах информационно-телекоммуникационной сети Интернет. Определены: задача, объекты и предмет исследования, круг разрешаемых вопросов, рекомендуемое оборудование и технические характеристики используемых в рамках исследования персональных электронных вычислительных машин, последовательность и границы допустимости дей-

ствий специалиста, возможные формулировки выводов, а также требования к поручению на проведение исследования.

Представлен подход к оформлению результатов исследования в части иллюстративного материала как с использованием неориентированной граф-модели (вершины – интернет-ресурсы и выявленные данные; ребра – совпадающие сведения), так и с созданием информационных карт в случаях анализа пользовательской активности.

Отмечается, что полученные в ходе исследования идентификаторы и метаданные могут использоваться как поисковые параметры при производстве судебной компьютерной экспертизы (исследование компьютерной информации), в том числе при назначении комплексного исследования, расширяя и оптимизируя область поиска на изъятых электронных носителях информации и повышая обоснованность последующего экспертного анализа.

В третьем параграфе «***Судебно-экспертное исследование информационных объектов и их метаданных, содержащихся на физических носителях информации***» проведен анализ эмпирического материала и ведомственной статистической отчетности, отражающей количество и результативность проводимых в экспертно-криминалистических подразделениях системы МВД России судебных компьютерных экспертиз. Выявлен недостаток ведомственной статистической отчетности, обусловленный учетом компьютерных экспертиз в качестве результативных без соотнесения обнаруженных данных с обстоятельствами уголовного дела и оценки криминалистической значимости полученной информации. Изучение нормативных правовых актов позволило выявить условие, препятствующее обеспечению межведомственного единообразия экспертной практики, выразившееся в невозможности использования экспертно-криминалистическими подразделениями системы МВД России методик, не рекомендованных ЭКЦ МВД России, но применяемых в иных государственных экспертно-криминалистических ведомствах.

Проанализирована действующая методика проведения судебной компьютерной экспертизы (исследование компьютерной информации) на предмет ее соответствия современному уровню технического развития и реальным экспертным возможностям. Обоснована необходимость совершенствования отдельных элементов экспертной технологии проведения данного вида экспертиз, в рамках которого предложено использование типологии информационных объектов при анализе объектов экспертного исследования и расширение перечня вопросов, которые могут разрешаться экспертом при производстве судебной компью-

терной экспертизы. В частности, рассмотрена возможность решения задач, связанных с установлением тождества файлов посредством сопоставления значений рассчитанных к ним хэш-сумм, выявлением фактов подключения внешних устройств хранения данных и определением их идентификационных характеристик, обнаружением журналов функционирования отдельных программных продуктов, установлением признаков удаленного доступа к компьютерным системам, а также выявлением и анализом объектов, используемых для скрытого размещения информации (стегоконтейнеров). Предложены возможные варианты формулировок выводов.

Также в параграфе дана оценка возможности использования в качестве вспомогательного инструментария самостоятельно разработанного в порядке экспертной инициативы программного обеспечения. Отмечено, что применение указанных программ для решения частных экспертных задач, выходящих за пределы возможностей аппаратно-программных комплексов, имеющихся в распоряжении экспертно-криминалистического подразделения, допустимо при условии обязательной валидации работоспособности и корректности получаемых с ее помощью результатов. Предлагается подход к проведению и описанию процедуры валидации.

В **заключении** подведены общие итоги исследования, сформулированы основные выводы и положения.

В **приложениях** приведены сводные таблицы, отражающие результаты эмпирического исследования, технология получения ориентирующей информации при работе с информационными объектами и их метаданными, размещенными в общедоступных ресурсах информационно-телекоммуникационной сети Интернет, а также словарь терминов, сокращений и условных обозначений.

Основные научные результаты диссертации опубликованы в следующих работах автора:

Научные статьи, опубликованные в изданиях, рекомендованных Высшей аттестационной комиссией при Министерстве науки и высшего образования Российской Федерации:

1. Фаниев П.А. Защита цифровых документов: понятие, виды и классификация элементов цифровой защиты документов в рамках криминалистической науки // Научный портал МВД России. – 2022. – № 3. – С. 86–90. – 0,6 п. л.

2. Фаниев П.А. Тихая разведка OSINT как способ получения криминалистически значимой информации // Научный портал МВД России. – 2023. – № 2. – С. 82–87. – 0,7 п. л.

3. Фаниев П.А. О некоторых способах обнаружения стегосообщений с использованием языка программирования Python // Вестник Краснодарского университета МВД России. – 2024. – № 1 (63). – С. 76–79. – 0,5 п. л.

4. Фаниев П.А. Использование расширенных возможностей поисковой строки Google для сбора криминалистически значимой информации в сети Интернет // Вестник Краснодарского университета МВД России. – 2024. – № 2 (64). – С. 81–84. – 0,5 п. л.

5. Фаниев П.А. Использование артефактов Linux для получения криминалистически значимой информации // Вестник Краснодарского университета МВД России. – 2024. – № 3 (65). – С. 72–75. – 0,5 п. л.

6. Фаниев П.А. Использование языка программирования Python для установления идентичности файлов, при проведении компьютерной экспертизы // Судебная экспертиза и исследования. – 2024. – № 4. – С. 170–173. – 0,5 п. л.

7. Фаниев П.А. Понятие информационного объекта в судебной компьютерной экспертизе и его значение для расследования преступлений // Судебная экспертиза и исследования. – 2026. – № 1. – С. 150–153. – 0,5 п. л.

Научные статьи, опубликованные в иных изданиях:

8. Фаниев П.А. Определение истинного расширения файла при проведении компьютерной экспертизы // Судебная экспертиза: российский и международный опыт: материалы VII Междунар. науч.-практ. конф. – Волгоград: Волгоград. акад. МВД России, 2024. – С. 232–236. – 0,3 п. л.

9. Фаниев П.А. Теоретические и практические вопросы использования программ удаленного доступа rat для проведения оперативно-разыскных мероприятий // Цифровые технологии современной криминалистики, использование специальных знаний: сб. науч. тр. Всерос. науч.-практ. конф., проводимой в рамках деловой программы Международной выставки «Интерполитех-2024». – М.: Следственный комитет Российской Федерации Главное управление криминалистики, 2025. – С. 165–181. – 0,9 п. л.

10. Фаниев П.А. К вопросу необходимости предварительного исследования цифровых следов при проведении процессуальных действий и оперативно-разыскных мероприятий // Технико-криминалистическое обеспечение раскрытия и расследования преступлений: сб. науч. тр. Всерос. науч.-практ. конф., проводимой в рамках деловой программы Международной выставки «Интерполитех-2024». – М.: Моск. ун-т МВД России им. В.Я. Кикотя, 2024. – С. 302–304. – 0,2 п. л.

11. Фаниев П.А. О некоторых способах сбора криминалистически значимой информации в сети интернет // Информационные и телекоммуникационные технологии в противодействии экстремизму и терроризму: сб. мат. Всеросс. науч.-практ. конф. – Краснодар: Краснодар. ун-т. МВД России, 2025. – С. 59–62. – 0,2 п. л.

Иные издания:

12. Фаниев П.А. Исследование файлов и метаданных при производстве компьютерной экспертизы: учеб.-метод. рекомендации. – Москва: Перо, 2024. – 48 с. – 2,8 п. л.

13. Фаниев П.А., Омельченко В.А. Использование программного обеспечения категории Open Source, для создания анонимной рабочей среды и проведения разведки OSINT: учеб.-метод. рекомендации. – Москва: Перо, 2024. – 69 с. – 4,0 п. л.

Подписано в печать __.__.2026. Печ. л. 1,5.
Тираж 120 экз. Заказ ___.

Краснодарский университет МВД России.
350005, Краснодар, ул. Ярославская, 128.