Научная статья
Научная специальность
5.1.4 «Уголовно-правовые науки»

УДК 343.9
DOI https://doi.org/10.26516/2071-8136.2025.4.141

КРИМИНАЛИСТИЧЕСКИЕ АСПЕКТЫ РАССЛЕДОВАНИЯ МОШЕННИЧЕСТВА, СОВЕРШЕННОГО С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

© Шишмарева Е. В.[1], Исакова А. С.[2], 2025
[1] Иркутский государственный университет, г. Иркутск, Россия
[2] Межмуниципальное управление МВД России «Братское», г. Братск, Россия

Рассмотрены криминалистические и процессуальные аспекты процесса расследования мошенничества, совершенного с использованием информационно-коммуникационных технологий (ИКТ). На основе изучения статистических данных, отображающих абсолютные показатели рассматриваемого вида преступности, выявлены качественные и количественные изменения, свидетельствующие о негативных тенденциях. Рассматривается структура криминалистической характеристики мошенничества в сфере ИКТ. Представлены типичные способы совершения мошенничества в сфере ИКТ, анализируется механизм следообразования, выделены определяющие аспекты, характеризующие лиц, совершающих рассматриваемые деяния, и признаки, присущие пострадавшим. На основе анализа материалов уголовных дел определены направления расследования мошенничества, совершенного в сфере ИКТ, описаны экспертизы, типичные для данной группы деяний, и особенности процесса их назначения. По результатам исследования предложены меры, направленные на профилактику данных преступлений и борьбу с ними.

Ключевые слова: мошенничество, право, информационно-коммуникационные технологии, экспертизы, мобильные технологии, акт, закон.

CRIMINALISTIC ASPECTS OF THE INVESTIGATION OF FRAUD COMMITTED USING INFORMATION AND COMMUNICATION TECHNOLOGIES

© Shishmareva E. V.[1], Isakova A. S.[2], 2025
[1] Irkutsk State University, Irkutsk, Russian Federation
[2] Intermunicipal Directorate of the Ministry of Internal Affairs of Russia "Bratskoye", Bratsk, Russian Federation

The criminalistic and procedural aspects of the fraud investigation process committed using information and communication technologies are considered. Based on the study of statistical data reflecting the absolute indicators of the type of crime under consideration, qualitative and quantitative changes indicating negative trends have been identified. The structure of the criminalistic characteristics of fraud in the field of information and communication technologies is considered. Typical methods of committing fraud in the field of ICT are presented, the mechanism of trace formation is analyzed, the defining aspects characterizing the perpetrators of the acts in question and the characteristics inherent in the victims are highlighted. Based on the analysis of the materials of criminal cases, the directions of the investigation of fraud committed in the field of information and communication technologies are determined, the expertise typical for this group of acts and the specifics of the process of their appointment are presented. Based on the results of the research, a material has been compiled on typical problems of investigating fraud in the field of ICT, the reasons for their commission, gaps in legislation and proposals aimed at preventing these crimes.

Keywords: fraud, law, information and communication technologies, expertise, mobile technologies, act, law.

Рост использования цифровых технологий в жизни современного общества, в бизнесе, в сфере предоставления государственных услуг и деятельности государственных органов на текущем этапе неизбежен. Сегодня люди имеют множество цифровых аккаунтов и проводят в Сети больше времени, чем когда-либо прежде. Все это, с одной стороны, существенно упрощает решение многих вопросов, с другой – приводит к увеличению криминальных инцидентов в данной сфере. Особое место по распространенности преступных проявлений в сети Интернет занимает мошенничество, совершаемое с использованием информационно-коммуникационных сетей. В совершение данных преступлений вовлечен широкий круг правонару-

шителей и потерпевших, сумма причиненного ущерба зачастую поражает своими размерами, а процесс их выявления, раскрытия и расследования нуждается в выработке методических и тактических рекомендаций. Ответственность за такие действия предусмотрена ст. 159 УК РФ[1] «Мошенничество», и законодатель трактует данное преступление как хищение чужого имущества, совершенное путем обмана, или злоупотребление доверием.

Анализ официальных статистических данных, отображающих уровень и состояние всех преступлений, предусмотренных ст. 159 УК РФ, на территории России за 2019–2025 гг., демонстрирует стойкую тенденцию к их увеличению с 219 021 до 432 912 преступлений, т. е. более чем в 2 раза (табл.). При этом мошенничество, совершенное с использованием информационно-телекоммуникационных технологий (ИКТ), является одним из видов мошенничества. Однако, если в 2019 г. его доля в структуре всех деяний, предусмотренных ст. 159 УК РФ, составляла 54,7 %, то по результатам 2024 г. этот показатель достиг 87,7 %, что однозначно свидетельствует об актуальности данной проблемы [5, с. 401]. Абсолютное количество таких преступлений с 2019 г. увеличилось более чем в 3 раза к 2024 г., с 119 903 до 379 762 преступлений (см. табл.).

Таблица

Количество зарегистрированных преступлений, предусмотренных ст. 159 УК РФ, на территории России за 2019–2025 гг.[2]

Год	Количество преступлений, предусмотренных ст. 159 УК РФ	Количество преступлений, предусмотренных ст. 159 УК РФ, совершенных с использованием информационно-телекоммуникационных технологий
2019	219 021	119 903
2020	291 233	210 493
2021	311 211	238 560
2022	319 674	249 984
2023	415 138	353 201
2024	432 912	379 762
Январь – август 2025	278 684	240 967

Кроме того, важно учитывать, что по рассматриваемой категории деяний очень высок уровень латентности, соответственно, анализируемые показатели не в полной мере отображают реальный уровень мошенничества, совершенного в сфере ИКТ. Так, по результатам опроса практических работников ОВД, реальные показатели по рассматриваемой группе деяний превосходят данные официальной статистики в 3–4 раза[3]. Данное обстоятельство обусловлено многими аспектами, в числе которых: нежелание потерпевших сообщать о преступлении в правоохранительные органы при относительно небольшом размере похищенного, отсутствие веры в результативность работы правоохранительных органов, чувство стыда и вины за отсутствие достаточной критичности к действиям преступников, потеря доверия к себе и т. д. [9, с. 65]

Анализ рассматриваемых криминальных деяний выявляет не только негативные количественные показатели, но свидетельствует и об изменении их качественных характеристик [3, с. 310]. К их числу следует отнести: увеличивающийся размер материального ущерба по данной группе преступлений [4, с. 218], постоянно трансформирующиеся способы совершения, вовлечение в совершение криминальных актов группы лиц, а также граждан, находящихся на территории иных государств и т. д.

Все это служит наглядной иллюстрацией общей проблемы: современные информационно-коммуникационные технологии и интернет-пространство становятся все более привлекательной площадкой для криминальной активности. Соответственно, представляется необходимым формирование современной методики расследования рассматриваемой группы деяний, которая могла бы стать основой методологической поддержки для работников следствия и дознания.

Формирование криминалистических методик расследования возможно через различные подходы [3, с. 310]. Однако все эти подходы базируются на анализе криминалистической характеристики преступления. Согласно определению, предложенному Р. С. Белкиным, криминалистическая характеристика отображает модель криминальной ситуации со всеми сопутствующими обстоятельствами, включая материальные и идеальные следы преступных действий, механизм противоправного поведения, способ совершения преступления и объект посягательства. По сути, это взаимосвязанный комплекс информативных данных о криминальном деянии определенной категории, которые позволяют систематизировать подход к их расследованию.

Важным элементом криминалистической характеристики является механизм следообразования. Мошеннические действия, реализуемые

[1] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // Собр. законодательства РФ. 1996. № 25. Ст. 2954.

[2] Официальный сайт МВД России. URL: https://мвд.рф/reports/1/ (дата обращения: 12.10.2025).

[3] В ходе исследования было опрошено 20 дознавателей отделов полиции г. Иркутска и Иркутской области.

через ИКТ, оставляют после себя следующие группы характерных следов.

Группу *материальных следов* составляют те изменения в объективном мире, которые образовались в результате действий преступников. К их числу следует отнести: биологический материал (потожировое вещество) и следы пальцев рук, обнаруживаемые на технических средствах; поддельные документы; средства и приспособления подделки документов; письма, записи, номера телефонов; предметы и вещи, оставленные на месте происшествия; следы ног, транспортных средств; микрочастицы и запаховые следы и т. д.

Следующую группу следов, характерных именно для мошенничества, совершенного в сфере ИКТ, составляют *цифровые (виртуальные) следы*, или, по определению ряда криминалистов, «*нетрадиционные» следы* [7, с. 104], которые образуются при взаимодействии с интернет-ресурсами и создании различного контента в информационной среде.

Типология таких следов напрямую зависит от методов осуществления мошеннических операций в технологической сфере[1]. Эти следы принято делить на пассивные (IP-адреса) и активные (публикации в социальных сетях, письма и т. д.). Эти следы могут быть обнаружены в памяти персонального компьютера, смартфона или в облачном хранилище файлов в интернете и т. д.[2]

Идеальные следы – это те изменения психики, которые сформировались у людей, причастных к преступлению. В группу таких следов входят показания потерпевшего, свидетелей и лиц, совершивших криминальные деяния.

Современное мошенничество, совершенное с использованием информационно-коммуникационных технологий, осуществляются различными способами. К их числу можно отнести атаки с применением социальной инженерии, в сочетании с вредоносными программами они представляют серьезную угрозу. Наиболее распространенным примером такой тактики является фишинг: жертву манипулятивно побуждают совершить определенные действия (например, перейти по ссылке в электронном сообщении или посетить подозрительный веб-ресурс), что приводит к компрометации системы.

Другой распространенный метод – распределенные атаки типа «отказ в обслуживании» (DDOS). При таком подходе злоумышленники используют сетевые протоколы для генерации массированного потока запросов к целевому серверу или сервису с единственной целью – нарушить его нормальное функционирование. Злонамеренное программное обеспечение также широко применяется в киберпреступлениях. Данная стратегия основана на неправомерном использовании компьютерных систем и сетевой инфраструктуры. Компьютерные устройства могут быть инфицированы вредоносным ПО для различных целей: повреждения оборудования, прерывания работы систем, а также кражи или уничтожения информации. При этом для сокрытия своей личности преступники активно используют технологии анонимизации, создают фальшивые профили и применяют шифрование при обмене сообщениями[3] .

Другой способ, когда мошенники представляются сотрудниками операторов сотовой связи и под предлогом окончания срока действия договора или необходимости обновления услуг убеждают жертву перейти по ссылке из мессенджера и скачать поддельное приложение. Такие приложения дают злоумышленникам полный доступ к данным на смартфоне, включая коды из СМС-сообщений, логины и пароли к онлайн-банкингу.

Следующий способ, когда преступники создают поддельные голосовые сообщения и видео (дипфейки) с использованием голоса или изображения родственников и знакомых жертвы. Затем такие фальшивые сообщения рассылаются контактам жертвы с просьбами о материальной помощи на лечение или другие нужды, часто с указанием реквизитов банковской карты или просьбой передать деньги через «знакомого»[4] .

Другим примером совершения рассматриваемых преступлений выступает схема, сформировавшаяся в 2021 г., когда мошенники размещают объявления о продаже объектов недвижимости, автомобилей и медицинских масок на популярных интернет-площадках. Перед заключением «сделки» они просят подтвердить платежеспособность, для чего требуют перевести небольшую сумму денег знакомым или родственникам через специальные платежные системы и предъявить квитанцию об оплате. Таким образом они выманивают персональные данные получателей переводов и изготавливают на их имена под-

[1] Актуальные способы совершения киберпреступлений. URL: https://school39mog.by/?page_id=10590 (дата обращения: 13.09.2025).

[2] Актуальные проблемы онлайн-платежей: от взломов до социальной инженерии. URL: https://new-retail.ru/tehnologii/aktualnye_problemy_onlayn_platezhey_ot_vzlomov_do_sotsialnoy_inzhenerii2264/ (дата обращения: 13.09.2025)

[3] Способы совершения киберпреступлений. URL: https://epp.genproc.gov.ru/web/proc_09/activity/legal-education/explain?item=74387457 (дата обращения: 13.09.2025)

[4] Актуальные способы совершения киберпреступлений. URL: https://school39mog.by/?page_id=10590 (дата обращения: 13.09.2025)

дельные паспорта, после чего посещают отделения банков и похищают деньги со счетов[1].

Следующий способ, когда преступник звонит по объявлению потерпевшего, размещенному на известных сайтах, таких как «Авито», «Юла», «Циан» и др., с целью приобретения его товара [8, с. 60]. После этого предлагает внести задаток, для чего просит продиктовать контрольные данные по банковской карте и поступивший код. Получив данные сведения, осуществляют перевод через онлайн-сервисы или просят подойти к банкомату и выполнить ряд комбинаций, подключая мобильный банк и в последующем похищая денежные средства.

Большое количество рассматриваемых преступлений совершается путем оформления кредитов и микрозаймов с использованием чужих документов, номеров телефонов и т. д. Так, гражданин Н. оформил кредит на сумму 16 тыс. руб. в кредитной организации, подав заявку через подтверждение портала «Госуслуги» и телефонного номера, который получил в связи со сменой номера сотового телефона оператора.

Следующий распространенный способ, когда преступник приобретает в интернете взлом страницы социальной сети, например «ВКонтакте», «Одноклассники», «ДругВокруг» и др., или осуществляет его самостоятельно. После этого мошенник связывается с контактами из списка с просьбой занять денежные средства под различными предлогами (заболел родственник, не хватает на срочную покупку и т. д.).

Следует отметить, что данные примеры составляют лишь часть мошеннических схем и свидетельствуют об изобретательности преступников и постоянной трансформации их методов работы. Именно данные факторы определяют сложность профилактической работы, которая ведется с целью предотвращения виктимизации граждан, поскольку невозможно информировать общество обо всех мошеннических способах.

Характеризуя потерпевших от рассматриваемой группы деяний, следует отметить, что это совершенно разные по возрасту, образованию и социальному статусу люди. При этом стоит не согласиться с мнением некоторых исследователей, которые выделяют такие отличительные свойства жертв, как алчность либо доверчивость [10, с. 88]. По нашим наблюдениям, отличительной чертой пострадавших от рассматриваемых деяний является отсутствие критичности мышления и невнимательность. Вместе с тем следует отметить, что лица, совершающие мошенничество в сфере ИКТ, используют психологические ловушки, манипуляции, строят диалог таким образом, что потерпевшие впоследствии сравнивают свое состояние в механизме преступления с воздействием гипноза. В результате в числе жертв оказываются совершенно разные люди, не обладающие какими-либо виктимными качествами или поведением, в том числе юристы, сотрудники правоохранительных органов и т. д.

Важной особенностью рассматриваемых деяний также является то, что ряд из них выступает лишь частью способа совершения более серьезных преступных деяний, таких как ч. 2 ст. 167, ст. 213, 205 или 281 УК РФ. В таком случае совершение мошеннических действий, в результате которых жертва теряет определенную сумму денег, дает возможность преступникам оказывать на потерпевшего воздействие, предлагая вернуть похищенное в обмен на совершение рассматриваемых выше преступных действий, чаще всего таких, как поджог военкоматов и иных административных объектов.

Таким образом, злоумышленники, специализирующиеся на рассматриваемых деяниях, представляют серьезную угрозу для всех пользователей сети Интернет, различных устройств с возможностью выхода в сеть и платежных систем. Действия преступников сложно предсказуемы в том плане, что невозможно предупредить совершение криминальных деяний в отношении всех потенциальных потерпевших (по причине их слишком большой численности), спрогнозировать новые формы мошеннических действий и т. д. [1, с. 4] К тому же личность типичного преступника, совершающего рассматриваемые деяния, неоднородна и включает в себя возрастные группы от 18 до 45 лет, преимущественно мужского пола, с разным уровнем образования (данный фактор более других коррелирует с выбранным способом совершения преступления), отличается изобретательностью, стойкой антиобщественной направленностью и высокой степенью адаптивности к изменяющимся внешним факторам. Данные свойства существенно усложняют возможности предупредительной работы, поскольку круг объектов профилактики представляется необъятным.

Процедура расследования мошенничества, совершенного в сфере ИКТ, включает в себя комплекс следующих действий: осмотр места происшествия, опрос заявителя и очевидцев, а

[1] Актуальные проблемы онлайн-платежей: от взломов до социальной инженерии. URL: https://new-retail.ru/tehnologii/aktualnye_problemy_onlayn_platezhey_ot_vzlomov_do_sotsialnoy_inzhenerii2264/ (дата обращения: 13.09.2025)

после возбуждения уголовного дела допрос потерпевшего и свидетелей, а также допрос лиц, находящихся под подозрением (при их идентификации), осмотр предметов и документов (например, выписки по движению денежных средств на банковских счетах, с которых были похищены денежные средства, а также детализации телефонных соединений потерпевшего), проведение обысков на территории проживания и работы подозреваемых субъектов, а также инициирование различных экспертных исследований [2, с. 81].

Важно подчеркнуть, что работа следственных органов независимо от характера действий, будь то поисковые или познавательные операции, проверка гипотез или анализ имеющихся сведений, сбор доказательств, неизменно проходит три последовательные фазы. Сначала следователь ориентируется в ситуации, затем осуществляет взаимодействие с объектами интереса (прямое или опосредованное) и, наконец, проводит оценку полученной информации, обеспечивает сохранность изъятых предметов и завершает документальное оформление процесса [4, с. 218].

Необходимым элементом процесса расследования мошенничества, совершенного в сфере ИКТ, выступает процесс применения специальных знаний, в частности назначение и производство экспертиз [6, с. 23].

При расследовании рассматриваемого вида мошенничества могут назначаться следующие экспертизы: дактилоскопическая, компьютерно-техническая, фоноскопическая, судебно-экономическая, почерковедческая, технико-криминалистическая экспертиза документов и т. д. [11, с. 277]

Особую роль в механизме расследования мошенничества в сфере информационно-коммуникационных технологий играет компьютерно-техническая экспертиза. Цель данного исследования – выявить факты использования компьютерной техники и средств связи в совершении преступлений, установить элементы способа совершения преступления и т. д.

Вопросы, на которые отвечает экспертиза:

– Имеется ли на представленном устройстве программное обеспечение, считывающее IP-адреса и иные персональные данные, и если да, то каковы название и версия этого программного обеспечения?

– Какая операционная система установлена на представленном устройстве?

– Возможна ли установка программного обеспечения, являющегося орудием совершения преступления, на данную операционную систему?

– Имеются ли на представленном устройстве программы, позволяющие работать с электронными системами платежей и проводить денежные транзакции?

– Имеются ли на представленном устройстве программы, позволяющие подключаться к локальным сетям или самостоятельно подключаться к сети Интернет?

– Имеются ли на представленном устройстве вредоносные программы, приводящие к модификации, копированию или уничтожению информации заведомо для пользователя и т. д.?

В качестве материалов, предоставляемых экспертам, выступают компьютерные данные, программное обеспечение, электронная почта, файлы и другие цифровые объекты, которые могут содержать доказательства преступных действий [6, с. 23].

Процесс расследования мошенничества, совершенного в сфере ИКТ, включает в себя комплекс действий, направленных на сбор доказательств путем запросов в банки, кредитные учреждения, провайдерам, предоставляющим услуги связи, владельцам интернет-магазинов и т. д.

Таким образом, представляется необходимой реализация комплексного подхода к противодействию мошенничеству в сфере ИКТ, который должен включать в себя как правовые, так и технические меры. Важно развивать международное сотрудничество и адаптировать законодательство к стремительно меняющимся технологиям. Особое внимание следует уделять повышению киберграмотности населения и усилению подготовки специалистов в данной области. Вместе эти шаги помогут создать более безопасную цифровую среду и минимизировать риски, связанные с рассматриваемым видом мошенничества. Также важным элементом эффективного расследования данных деяний выступает уровень подготовки следователя к такой работе, его степень владения специальными знаниями в IT-сфере.

СПИСОК ЛИТЕРАТУРЫ

1. Акопджанова М. О. Особенности оперативно-розыскной деятельности на современном этапе // Актуальные проблемы теории и практики оперативно-розыскной деятельности : материалы IV Всерос. науч.-практ. конф. Краснодар : Краснодар. ун-т МВД России, 2016. С. 3–5.

2. Васюков В. Ф. Некоторые вопросы назначения компьютерно-технической экспертизы мобильных телефонов при расследовании преступлений // Вестник Академии Генеральной прокуратуры РФ. 2015. № 2. С. 81–84.

3. Гайдин А. И., Морин А. В. Проблемы формирования частной криминалистической методики расследования вы-

могательства, совершаемого с использованием информационно-телекоммуникационных технологий // Право и государство: теория и практика. 2023. № 7 (223). С. 310–313.

4. Григорьева А. Е. Особенности криминалистической характеристики мошенничеств, совершенных с использованием информационных технологий // Аграрное и земельное право. 2022. № 12 (216). С. 218–219.

5. Катаев С. А. Анализ актуального состояния и тенденций киберпреступности в России // Молодой ученый. 2025. № 4 (555). С. 400–402.

6. Крючков М. А. Производство судебных экспертиз при расследовании мошенничества с использованием информационно-коммуникационных технологий // Научный аспект. 2023. Т. 1, № 5. С. 22–29.

7. Мещеряков В. А. Основы методики расследования преступлений в сфере компьютерной информации : дис. … д-ра юрид. наук. Воронеж, 2001. 387 с.

8. Никулина О. А. Расследование мошенничества с использованием мобильной связи // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. 2019. № 1(5). С. 57–61.

9. Петрякова Л. А. Социально-правовая и информационно-технологическая обусловленность криминализации и проблемы квалификации мошенничества в сфере компьютерной информации // Сибирский юридический вестник. 2023. № 3(102). С. 63–69.

10. Ревенко Н. И. Криминалистическая характеристика мошенничества с использованием информационно-телекоммуникационных технологий // Вестник Омского университета. Серия «Право». 2024. Т. 21, № 2. С. 87–90.

11. Телигисова С. С. К вопросу о видах экспертиз при расследовании преступлений, совершенных с использованием цифровых и информационно-телекоммуникационных технологий // Государственная служба и кадры. 2024. № 1. С. 276–279.

REFERENCES

1. Akopdzhanova M.O. Osobennosti operativno-rozysknoi deyatelnosti na sovremennom etape [Features of Operative-Investigative Activities at the Present Stage]. *Aktualnye problemy teorii i praktiki operativno-rozysknoi deyatelnosti* [Topical Issues of Theory and Practice of Operative-Investigative Activities]. Materials of the 4th All-Russian Scientific and Practical Conference. Krasnodar, Krasnodar Univ. MVD Rossii, 2016, pp. 3-5. (in Russian)

2. Vasyukov V.F. Nekotorye voprosy naznacheniya kompyuterno-tekhnicheskoy ekspertizy mobil'nykh telefonov pri rassledovanii prestupleniy [Some Issues of Appointment of Computer-Technical Examination of Mobile Phones in the Investigation of Crimes]. *Vestnik Akademii Generalnoy prokuratury RF* [Bulletin of the Academy of the General Prosecutor's Office of the Russian Federation], 2015, no. 2, pp. 81-84. (in Russian)

3. Gaidin A.I., Morin A.V. Problemy formirovaniya chastnoy kriminalisticheskoy metodiki rassledovaniya vymogatelstva, sovershayemogo s ispolzovaniem informatsionno-telekommunikatsionnykh tekhnologiy [Problems of Forming Private Criminalistic Methodology for Investigating Extortion Committed Using Information and Telecommunication Technologies]. *Pravo i gosudarstvo: teoriya i praktika* [Law and State: Theory and Practice], 2023, no. 7 (223), pp. 310-313. (in Russian)

4. Grigoryeva A.E. Osobennosti kriminalisticheskoy kharakteristiki moshennichestv, sovershennykh s ispolzovaniem informatsionnykh tekhnologiy [Features of Criminalistic Characterization of Frauds Committed Using Information Technologies]. *Agrarnoe i zemelnoe pravo* [Agrarian and Land Law], 2022, no. 12 (216), pp. 218-219. (in Russian)

5. Kataev S. A. Analiz aktualnogo sostoyaniya i tendentsiy kiberprestupnosti v Rossii [Analysis of the Current State and Trends of Cybercrime in Russia]. *Molodoy uchenyy* [Young Scientist], 2025, no. 4(555), pp. 400-402. (in Russian)

6. Kryuchkov M. A. Proizvodstvo sudebnykh ekspertiz pri rassledovanii moshennichestva s ispolzovaniem informatsionno-kommunikatsionnykh tekhnologiy [Conducting Forensic Examinations in the Investigation of Frauds Using ICT]. *Nauchnyy aspekt* [Scientific Aspect], 2023, vol. 1, no. 5, pp. 22-29. (in Russian)

7. Meshcheryakov V.A. *Osnovy metodiki rassledovaniya prestupleniy v sfere komp'yuternoy informatsii* [Fundamentals of Investigating Crimes in the Field of Computer Information]. Dr. sci. diss. Voronezh, 2001, 387 p. (in Russian)

8. Nikulina O.A. Rassledovanie moshennichestva s ispolzovaniem mobilnoy svyazi [Investigation of Fraud Using Mobile Communication]. *Prestupnost' v sfere informatsionnykh i telekommunikatsionnykh tekhnologiy: problemy preduprezhdeniya, raskrytiya i rassledovaniya prestupleniy* [Crime in the Field of Information and Telecommunication Technologies: Problems of Prevention, Disclosure and Investigation of Crimes], 2019, no. 1(5), pp. 57-61. (in Russian)

9. Petryakova L.A. Sotsialno-pravovaya i informatsionno-tekhnologicheskaya obuslovlennost kriminalizatsii i problemy kvalifikatsii moshennichestva v sfere kompyuternoy informatsii [Socio-Legal and Information-Technological Conditioning of Criminalization and Problems of Qualification of Fraud in the Field of Computer Information]. *Sibirskiy yuridskiy vestnik* [Siberian Legal Bulletin], 2023, no. 3(102), pp. 63-69. (in Russian)

10. Revenko N.I. Kriminalisticheskaya kharakteristika moshennichestva s ispolzovaniem informatsionno-telekommunikatsionnykh tekhnologiy [Criminalistic Characteristics of Fraud Using Information and Telecommunication Technologies]. *Vestnik Omskogo universiteta. Seriya "Pravo"* [Bulletin of Omsk University. Law Series], 2024, vol. 21, no. 2, pp. 87-90. (in Russian)

11. Teligisova S.S. *K voprosu o vidakh ekspertiz pri rassledovanii prestupleniy, sovershennykh s ispolzovaniem tsifrovykh i informatsionno-telekommunikatsionnykh tekhnologiy* [On the Types of Examinations in the Investigation of Crimes Committed Using Digital and Information and Telecommunication Technologies]. *Gosudarstvennaya sluzhba i kadry* [Public Service and Personnel], 2024, no. 1, pp. 276-279. (in Russian)

Статья поступила в редакцию 28.08.2025; одобрена после рецензирования 18.10.2025; принята к публикации 19.11.2025

Received on 28.08.2025; approved on 18.10.2025; accepted for publication on 19.11.2025

Шишмарева Екатерина Владимировна – доцент кафедры судебного права, Юридический институт, Иркутский государственный университет (Россия, 664003, г. Иркутск, ул. К. Маркса, 1), ORCID: 0000-0002-2925-4472, РИНЦ Author ID: 692051, e-mail: chalv@bk.ru

Shishmareva Ekaterina Vladimirovna – Candidate of Juridical Sciences, Associate Professor, Associate Professor of the Department of Judicial Law, Law Institute, Irkutsk State University (1, K. Marx st., Irkutsk, 664003, Russian Federation), ORCID: 0000-0002-2925-4472, RSCI Author ID: 692051, e-mail: chalv@bk.ru

Исакова Алиса Сергеевна – дознаватель ОД ОП № 5, Межмуниципальное управление МВД России «Братское» (Россия, 665700, г. Братск, проезд Индустриальный, 9а), e-mail: alisaisakova1988@mail.ru

Isakova Alisa Sergeevna – investigator of OD OP N 5, Intermunicipal Directorate of the Ministry of Internal Affairs of Russia "Bratskoye" (9a, passage Industrial, Bratsk, 665700, Russian Federation), e-mail: alisaisakova1988@mail.ru

Вклад авторов

Шишмарева Екатерина Владимировна – концепция исследования (формирование идеи), сбор и обработка теоретического и эмпирического материала, написание основных результатов исследования, оформление и утверждение окончательного варианта статьи.

Исакова Алиса Сергеевна – сбор эмпирического материала, описание материалов и метода исследования, написание текста введения и отдельных результатов исследования.