

Оригинальная статья / Original article

УДК 343.3/.7:004.056

<https://doi.org/10.21869/2223-1501-2026-16-1-104-114>**Цифровая анонимность как элемент способа совершения мошенничества****А.В. Василенко¹**✉

¹ Межрайонная инспекция Федеральной налоговой службы №13 по Московской области
ул. Панфилова, д. 31, г. Химки 141407, Российская Федерация

✉ e-mail: vas.art7728@gmail.com

Резюме

Актуальность. Быстрый переход мошенничества в цифровую среду изменил характер преступного поведения и способы реализации обманных схем. Использование анонимизирующих инструментов: виртуальных номеров, антидетект-браузеров, криптовалютных транзитных сервисов, инфраструктуры дропов, VPN и Tor – формирует распределённую технологическую модель, позволяющую скрывать личность, усложнять установление причинно-следственных связей и затруднять квалификацию по статьям 159, 159.3 и 159.6 Уголовного кодекса Российской Федерации. Изучение роли этих средств становится значимым как для теории, так и для практики расследования.

Цель – определить значение цифровой анонимизации как элемента способа совершения мошенничества и её влияние на квалификацию и доказательственную базу.

Задачи включают характеристику используемых анонимизирующих инструментов, выявление их функциональной роли, анализ последствий для квалификации действий участников распределённых схем, а также определение ключевых проблем доказывания.

Методология. В статье использованы методы системного анализа, функционального подхода, сравнительно-правового исследования и криминалистического изучения цифровых следов.

Результаты. Установлено, что анонимизирующая инфраструктура является устойчивым компонентом механизма цифрового мошенничества и влияет на распределение ролей между участниками. Традиционные критерии соучастия не обеспечивают адекватной оценки технических действий – регистрации реквизитов, подготовки цифровых профилей, обеспечения транзита средств. Существенные доказательственные трудности возникают из-за временной природы цифровых идентификаторов и отсутствия единообразия в их фиксации. Комплексный анализ подтверждает необходимость пересмотра подходов к определению роли технических участников и стандартизации работы с цифровыми следами.

Вывод. Цифровая анонимизация выступает самостоятельным элементом способа мошенничества, требующим учёта при квалификации и доказывании. Унификация методик фиксации digital-следов и оценки функционального участия в распределённых схемах позволит повысить качество расследования и обеспечить стабильность практики при неизменности статьи 159 Уголовного кодекса Российской Федерации.

Ключевые слова: цифровая анонимизация; мошенничество; виртуальные номера; антидетект-браузеры; криптовалюта; цифровые следы; преступление.

Конфликт интересов: Автор декларирует отсутствие явных и потенциальных конфликтов интересов, связанных с публикацией настоящей статьи.

Для цитирования: Василенко А.В. Цифровая анонимность как элемент способа совершения мошенничества // Известия Юго-Западного государственного университета. Серия: История и право. 2026. Т. 16, № 1. С. 104–114. <https://doi.org/10.21869/2223-1501-2026-16-1-104-114>.

Поступила в редакцию 18.11.2025

Принята к публикации 20.01.2026

Опубликована 25.02.2026

Digital anonymity as an element of the method of committing fraud

Artem V. Vasilenko¹✉

¹ Interdistrict Inspectorate of the Federal Tax Service No. 13 for the Moscow Region
31 Panfilova Str., Khimki 141407, Russian Federation

✉ e-mail: vas.art7728@gmail.com

Abstract

Relevance. The rapid shift of fraud into the digital environment has fundamentally transformed the nature of criminal conduct and the methods used to implement deceptive schemes. The use of anonymizing tools—virtual numbers, anti-detect browsers, cryptocurrency transit services, drop infrastructures, VPNs and Tor—creates a distributed technological model that conceals the offender's identity, complicates the establishment of causal links, and hinders qualification under Articles 159, 159.3, and 159.6 of the Criminal Code of the Russian Federation. The examination of the role of such tools is increasingly significant for both legal doctrine and law enforcement practice.

Purpose – is to determine the significance of digital anonymization as an element of the method of committing fraud and to identify its impact on qualification and evidentiary standards.

Objectives include characterizing anonymization tools used in digital fraud schemes, identifying their functional role, assessing their implications for the qualification of participants in distributed schemes, and determining key evidentiary challenges.

Methodology. The article employs methods of systemic analysis, functional assessment, comparative legal research, and forensic examination of digital traces.

Results. The study establishes that anonymizing infrastructure is a stable component of digital fraud mechanisms and shapes the distribution of roles among participants. Traditional criteria of complicity do not adequately reflect technical actions such as registering credentials, preparing digital profiles, or ensuring the transit of funds. Significant evidentiary difficulties arise from the ephemeral nature of digital identifiers and the lack of unified standards for their collection. A comprehensive assessment confirms the need to revise approaches to determining the role of technical participants and to standardize procedures for handling digital traces.

Conclusion. Digital anonymization constitutes an independent element of the method of committing fraud and must be considered in both qualification and proof. The unification of methodologies for handling digital traces and assessing functional participation in distributed schemes will improve investigative quality and stabilize judicial practice without amending Article 159 of the Criminal Code.

Keywords: digital anonymization; fraud; virtual numbers; antidetector browsers; cryptocurrency; digital traces; crime.

Conflict of interest: The Author declare the absence of obvious and potential conflicts of interest related to the publication of this article.

For citation: Vasilenko A.V. Digital anonymity as an element of the method of committing fraud. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Istoriya i pravo* = *Proceedings of the Southwest State University. Series: History and Law*. 2026;16(1):104–114. (In Russ.) <https://doi.org/10.21869/2223-1501-2026-16-1-104-114>.

Received 18.11.2025

Accepted 20.01.2026

Published 25.02.2026

Введение

Стремительное развитие цифровой коммуникационной среды радикально изменило модель реализации мошеннических схем. Например, в 2024 г. каждый третий из десяти респондентов сталкивался с кибермошенничеством; 9% таких

пострадавших лишились денег¹. Если для классических форм мошенничества определяющим элементом оставалось непосредственное взаимодействие преступни-

¹ Кибермошенничество: портрет пострадавшего // Банк России: сайт. 2025. URL: https://www.cbr.ru/statistics/information_security/cyber_portrait/2024/ (дата обращения: 06.11.2025).

ка и потерпевшего, то при дистанционных цифровых посягательствах центральным инструментом становится инфраструктура анонимизации, позволяющая скрывать субъект, распределять исполнение преступных действий и затруднять установление причинно-следственных связей. Практика расследования преступлений, квалифицируемых по ст. 159, 159.3 и 159.6 Уголовного кодекса Российской Федерации¹ (далее – УК РФ), показывает, что именно средства сокрытия цифрового следа во многих случаях определяют особенности способа совершения деяния, придавая ему устойчивый организованный характер.

Анонимизация в цифровой криминальной среде не ограничивается использованием VPN или сетей Tor. Современные преступные схемы включают многоуровневую цифровую инфраструктуру: виртуальные мобильные номера, сервисы одноразовой связи, дропы (3-е лица), а также дроп-аккаунты и дроп-карты, антидетект-браузеры, криптовалютные микшеры, транзитные биржи и специализированные бот-сервисы. Каждое из этих средств формирует отдельный технологический модуль, а их совокупность позволяет фрагментировать преступную деятельность на этапы, исполнение которых невозможно напрямую связать с конкретным лицом. В результате следствию приходится взаимодействовать не с традиционной моделью «исполнитель – потерпевший», а с распределённым цифровым механизмом, в котором человеческое участие сведено к минимуму, что усложняет установление причинно-следственной связи и роли каждого соучастника. Так, в апреле–июне 2025 г. банки отразили 38,7 млн попыток мошеннических операций – в 1,5 раза больше, чем средний показатель за

предыдущие четыре квартала; предотвращено хищение средств на сумму 3,4 трлн руб.²

Для анализа выявленных проблем и правовой оценки цифровых мошеннических схем в исследовании использована комплексная нормативно-правовая база, включающая положения уголовного, процессуального законодательства, а также разъяснения Верховного Суда РФ, регулирующие вопросы киберпреступности³.

² Противодействие мошенническим операциям: итоги II квартала 2025 // Банк России: сайт. URL: <https://www.cbr.ru/press/event/?id=26832> (дата обращения: 06.11.2025).

³ Уголовный кодекс Российской Федерации; Уголовно-процессуальный кодекс Российской Федерации; Федеральный закон от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации» № 149-ФЗ; Федеральный закон от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности»; Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи»; Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»; Федеральный закон от 27 июня 2011 г. № 161-ФЗ; Указ Президента РФ от 12 апреля 2021 г. № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности»; Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»; Постановление Правительства РФ от 27 августа 2005 г. № 538 «Об утверждении Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-разыскную деятельность»; Приказ Минкомсвязи России от 16 апреля 2014 г. № 83 «Об утверждении Правил применения оборудования систем коммутации, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий»; Постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате».

¹ Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // КонсультантПлюс: сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_10482 (дата обращения: 10.09.2025).

Методология

Методологическая основа исследования определяется характером анализируемых отношений и опирается на сочетание общенаучных и специальных юридических методов. Системный подход позволил рассмотреть цифровое мошенничество как комплексное явление, включающее технические, правовые и криминалистические компоненты. Функциональный анализ применён для оценки роли отдельных участников распределённых схем с учётом специфики их технических действий. Сравнительно-правовой метод использовался для сопоставления различных моделей квалификации, встречающихся в следственной и судебной практике. Криминалистический метод обеспечил исследование особенностей фиксации, сохранения и анализа цифровых следов [1, с. 154], возникающих при использовании анонимизирующих инструментов. Эмпирическую основу составили материалы уголовных дел о мошенничествах, совершаемых с применением цифровых технологий, а также анализ научных работ, посвящённых квалификации и доказыванию таких преступлений.

Результаты и их обсуждение

При определении квалификации ключевым ориентиром должна выступать конечная направленность деяния – незаконное безвозмездное изъятие чужого имущества, предусмотренное ст. 159 УК РФ. Соответственно, действия, связанные с использованием информационно-телекоммуникационных технологий и средствами обеспечения цифровой безопасности, подлежат оценке не как самостоятельные преступления, а как способ реализации мошеннического умысла, при условии отсутствия конкуренции специальных норм иного состава [2, с. 45]. Поэтому в практическом плане требуется не изменение диспозиций уголовного закона, а развитие доктринального подхода к оценке способа и роли технических

средств как составообразующих компонентов.

Особенность складывающейся практики состоит в том, что анонимизирующая инфраструктура становится не второстепенным прикрытием, а самостоятельной частью преступного метода. Например, использование виртуальных номеров и дроп-аккаунтов не только скрывает личность злоумышленника, но и структурирует схему, позволяя вовлекать третьих лиц, не осознающих реального характера совершаемых операций. В уголовно-правовом аспекте это создаёт проблему квалификации: формально лицо, зарегистрировавшее на себя банковскую карту и передавшее доступ к ней, может не совершать изъятия имущества, однако обеспечивает ключевое звено преступной конструкции. Вопрос о разграничении роли таких лиц значительно осложняется отсутствием прямого контакта между исполнителем и потерпевшим и заменой межличностного взаимодействия цифровым посредничеством.

Анализ материалов расследований показывает, что в делах о цифровом мошенничестве традиционные критерии соучастия оказываются недостаточными. Поспособничество и организаторская деятельность нередко выражаются не в передаче информации или участии в обмане потерпевшего, а в техническом обеспечении схемы: предоставлении анонимизирующих сервисов, создании и продаже «чистых» аккаунтов, выведении средств через криптовалютные транзитные кошельки. Правовая оценка таких действий требует функционального подхода: объектом анализа становится не только участие в хищении, но и вклад в реализацию преступного замысла через технологические инструменты. Данная тенденция прослеживается в научной литературе, где обращается внимание на необходимость учитывать техническую роль в механизме посягательства как элемент объективной стороны способа совершения преступления, а не только

как обстоятельство, затрудняющее расследование.

Сложности доказывания усугубляются масштабом цифровых посредников. Большая часть коммуникации осуществляется через зарубежные сервисы, криптовалютные транзакции проходят через юрисдикции [3, с. 95], не взаимодействующие с российскими правоохранительными органами, а цифровые идентификаторы обладают временной природой и не сохраняются в зафиксированном виде. Следствию приходится работать с ситуацией, когда значительная часть следовой информации носит цифровой, эфемерный характер (лог-записи, метаданные) [4 с. 22], что требует специализированной фиксации и верификации.

Уголовно-правовые проблемы квалификации

При традиционном мошенничестве психическое воздействие на потерпевшего являлось ключевым элементом объективной стороны; при цифровых схемах воздействию подвергается не человек, а инфраструктура его цифровой репрезентации – мобильный банк, электронная почта, личный кабинет, платёжный шлюз. Это смещает акцент с межличностного обмана на подмену доверенных механизмов аутентификации и идентификации [5, с. 128].

Тем самым формируется новая криминологическая реальность: способ совершения преступления превращается в совокупность цифровых действий, а анонимизирующая инфраструктура – в центральный элемент преступного замысла. Именно это обстоятельство создаёт методологическую проблему уголовно-правовой квалификации. При отсутствии прямого взаимодействия субъекта с потерпевшим значение получает характер цифрового инструментария, а границы между обманом и неправомерным доступом к информационной системе становятся размытыми [6, с. 53].

В этих условиях всё более актуальным становится вопрос о том, какие при-

знаки должны определять правовую природу деяния, когда внешне нейтральные технические манипуляции обеспечивают достижение преступного результата. Технические действия: настройка каналов связи, имитация легитимных сервисов, интеграция анонимизирующих инструментов – формируют самостоятельный пласт поведения, требующий включения в правовую оценку не только как обстоятельств, затрудняющих раскрытие, но и как элементов объективной стороны преступления. Трансформация механизма посяательства приводит к тому, что традиционный критерий «воздействия на волю потерпевшего» утрачивает универсальный характер, и на первый план выходит анализ того, каким образом злоумышленник воздействует на информационные процессы, заменяющие межличностное взаимодействие в цифровой среде.

Эта тенденция подчёркивает необходимость более тонкого методологического разграничения составов, в которых цифровая среда становится не просто фоном преступления, а его структурообразующим компонентом. Правоприменителю требуется учитывать не только факт вмешательства в информационные системы, но и то, что использование анонимизирующих технологий позволяет искусственно создавать видимость автономности действий различных участников и маскировать их вклад в достижение общего результата. В совокупности это формирует новую отраслевую проблему – определение границ уголовно-правового значения технических цифровых операций, которые в ряде случаев становятся ключевыми маркерами преступного умысла и функционального участия.

Комплексный анализ проблем квалификации и доказывания в условиях цифровой анонимизации

Развитие цифровых коммуникаций объективно изменило структуру мошенничества: из межличностного преступле-

ния, основанного на обмане потерпевшего, оно трансформируется в распределённую технологическую модель, где ключевую роль играет не столько психологическое воздействие, сколько скрытая инфраструктура, обеспечивающая маскировку личности и цифрового следа исполнителя. Современные схемы всё чаще строятся вокруг анонимизирующих инструментов, позволяющих злоумышленнику действовать вне зоны прямой идентификации: виртуальные мобильные номера, антидетект-браузеры, прокси-сети, VPN и TOR, криптовалютные транзакции с использованием миксеров, а также инфраструктура дропов – подставных лиц, карт и аккаунтов. В научной литературе подчеркивается, что именно технологическая среда создаёт условия для существования «преступного безличия», при котором связь между субъектом и хищением становится неочевидной [7, с. 4]. С правовой точки зрения это требует корректировки подхода к анализу объективной и субъективной сторон состава преступления: использование анонимизирующей инфраструктуры нередко имеет самостоятельное доказательственное значение, т. к. демонстрирует преднамеренность сокрытия следов и сформированный преступный умысел.

Особую сложность создаёт феномен распределённости действий. Зачастую исполнитель не взаимодействует с потерпевшим и даже не совершает хищение напрямую [8, с. 178]: техническое обеспечение операции (регистрация домена для фишингового сайта, покупка виртуальных номеров, подготовка антидетект-браузера, создание криптокошельков, привязка дроп-карты) [9, с. 166] передаётся отдельным лицам, которые не вступают в контакт с деньгами, но обеспечивают ключевое условие – невозможность идентификации. Вследствие этого субъективная сторона оказывается фрагментированной: разные участники выполняют автономные функции, и задача следствия состоит в том, чтобы доказать их

осознанное участие в общем умысле. С методологической точки зрения правоприменение фактически сталкивается с новой формой соучастия, в которой решающее значение имеет не физическое действие, а техническое обеспечение схемы. В научных публикациях указывается, что криминалистическая фиксация таких действий требует специальной подготовки следователя и стандартизированного подхода к сбору цифровых артефактов [10, с. 431].

В уголовно-правовом аспекте основной проблемой становится квалификация. Большинство цифровых мошенничеств по-прежнему квалифицируется по ст. 159 УК РФ, включая случаи, когда техническая часть составляет значительную долю способа совершения преступления. В научной литературе отмечается, что нередко встречаются ситуации, когда следствие пытается квалифицировать эпизоды как неправомерный доступ к компьютерной информации (ст. 272 УК РФ) [11, с. 14], создание вредоносных программ (ст. 273 УК РФ) или вмешательство в работу информационной системы (ст. 274.1 УК РФ) [12, с. 445]. Однако если конечной целью остается незаконное безвозмездное изъятие денежных средств или иного имущества, конструкция мошенничества должна сохранять приоритет, а технические действия рассматриваться как способ его совершения. Подобный подход обоснован позицией, высказанной рядом исследователей, отмечающих, что подмена криминалистической сложности юридической переквалификацией разрушает системность квалификации и создаёт разнотолкование в судебной практике [13, с. 129].

Правоприменение демонстрирует и вторую проблему: отсутствие устойчивых методик доказывания участия лиц, обеспечивающих инфраструктуру анонимизации. Дроп, который зарегистрировал SIM-карту или банковский счёт и передал их организатору схемы, формально не присутствует в момент хищения, од-

нако без его участия совершение преступления было невозможно. В ряде дел суды квалифицируют таких лиц как пособников, но в других – как неведущих участников, что порождает правовую неопределённость. При этом даже недавнее обновление ст. 187 УК РФ (ред. 2025 г.), расширившее ответственность за неправомерный оборот электронных средств платежа и доступов к ним, не устраняет указанной неопределённости, поскольку охватывает иные по своей природе деяния и не решает вопрос квалификации лиц, обеспечивающих инфраструктуру анонимизации. Научная доктрина указывает, что роль лица в распределённой цифровой схеме определяется не физическим присутствием при операции, а его функциональной значимостью в механизме хищения. Эта позиция представляется логически выверенной: если лицо сознательно предоставляет реквизиты для анонимизации, понимая, что они будут использованы в преступных целях, его действия образуют интеллектуальное или техническое пособничество, а в некоторых случаях – элементы организации. Отсутствие единых методических критериев приводит к тому, что в одинаковых, по сути, схемах участники получают разную уголовно-правовую оценку. Это обусловлено недостаточной методической унификацией фиксации технических функций участника (например, регистрация SIM, настройка антитрассинга, создание кошельков) и их привязки к общему умыслу.

Не менее значимой является доказательственная сторона. Цифровые следы: логи VPN-подключений, данные о входах в аккаунты, сведения о транзакциях через криптовалютные кошельки, переписка об аренде виртуальных номеров – обладают высоким криминалистическим потенциалом, однако их собираемость и применимость в суде зависят от того, насколько корректно они были зафиксированы с точки зрения процессуального закона [14, с. 180]. Отсутствие единых методик при-

водит к тому, что доказательства нередко признаются недопустимыми из-за ошибок при фиксации или изъятии. В научной дискуссии подчёркивается необходимость развития цифровой криминалистики [15, с. 565] как самостоятельного инструмента доказывания [16, с. 130]. Реализация этой задачи возможна не только посредством законодательных изменений, но и на уровне ведомственных методик следственных органов, устанавливающих порядок работы с лог-файлами, хеш-суммами, криптовалютными отчётами и экспертными заключениями по анализу транзакций.

С практической точки зрения целесообразным представляется формирование единых методических рекомендаций МВД России и Генеральной прокуратуры Российской Федерации, посвящённых фиксации и оценке средств анонимизации как элемента способа совершения преступления [17, с. 166]. В подобных рекомендациях можно закрепить перечень цифровых артефактов, подлежащих обязательному сбору, правила взаимодействия следствия с операторами связи, банками и криптовалютными платформами, а также требования к экспертизам, анализирующим структуру цифрового следа [18, с. 125]. При наличии таких инструкций правоприменитель получил бы устойчивый алгоритм работы [19, с. 55], сокращающий вероятность процессуальных ошибок и повышающий доказательственную силу цифровых материалов.

Аналогичной стандартизации требует и вопрос квалификации участия дропов [20, с. 178]. Криминально-правовая оценка подобных лиц по-прежнему определяется не формальным статусом операции, а их функциональной значимостью в реализации преступного умысла.

На доктринальном уровне оправдан подход, при котором их роль устанавливается с учётом функциональной значимости для исполнения преступного умысла: если лицо регулярно предостав-

ляет реквизиты, получает вознаграждение и понимает предназначение своих действий, его участие должно рассматриваться не как случайное содействие, а как осознанный элемент схемы. Это позволило бы устранить неоднородность судебных решений и сформировать более предсказуемую практику. Реализация названных подходов не предполагает коренной перестройки уголовного законодательства. Речь идет о развитии правоприменительных механизмов – совершенствовании криминалистических методик, процессуальной грамотности и межведомственного взаимодействия. Практика показывает, что многие эпизоды цифрового мошенничества остаются нераскрытыми не из-за технологической «непобедимости» преступников, а из-за отсутствия формализованного подхода к сбору и оценке цифровых следов. Методическая унификация позволила бы не только повысить качество расследования, но и снизить вероятность оправдательных приговоров, основанных на признании доказательств недопустимыми.

Выводы

Проведённый анализ позволяет утверждать, что цифровая среда не просто модифицирует отдельные элементы мошенничества, а формирует иную модель преступного поведения, в которой анонимизирующие технологии выступают системообразующим компонентом. Их использование меняет характер взаимодействия участников, трансформирует структуру преступной деятельности и существенно усложняет процесс установления криминально значимых связей. Тем самым цифровая анонимизация приобретает самостоятельное правовое значение и должна рассматриваться как фактор, влияющий на содержание как объективной, так и субъективной сторон состава преступления.

Результаты исследования свидетельствуют, что развитие технических средств сокрытия личности приводит к

снижению роли межличностного обмана и усилению значимости цифровых механизмов воздействия на информационную инфраструктуру потерпевшего. В этих условиях центральным становится не способ введения в заблуждение, а способ организации цифрового пространства, обеспечивающего возможность хищения. Такое смещение акцента требует корректного включения технических операций в систему доказательственных признаков и переосмысления критериев участия в распределённых схемах.

Правоприменительная практика демонстрирует, что существенная часть возникающих сложностей обусловлена не особенностями законодательной конструкции, а несформированностью единых методических подходов. Отсутствие стандартизированных процедур фиксации и оценки цифровых следов приводит к неоднородности квалификации и снижает надёжность доказательственной базы. Последовательная выработка единых правил получения, закрепления и анализа цифровых данных представляется необходимым условием для повышения качества расследования.

Актуализируется и проблема определения степени участия лиц, выполняющих технические функции в составе цифровых схем. Практика показала, что именно функциональная роль, а не формальный статус действий позволяет отразить реальный вклад лица в достижение преступного результата. Формирование устойчивых критериев такой оценки является одним из наиболее перспективных направлений совершенствования правоприменения.

В свете полученных результатов можно заключить, что повышение эффективности противодействия цифровым мошенничествам должно базироваться на институциональных и методических изменениях, а не на корректировке состава ст. 159 УК РФ. Развитие цифровой криминалистики, создание межведомственных методических стандартов и укрепле-

ние экспертного потенциала способны обеспечить стабильную и предсказуемую

практику в условиях дальнейшей цифровизации преступной деятельности.

Список литературы

1. Бадиков Д.А., Елисеева К.А. Алгоритм действий следователя при расследовании мошенничества с использованием электронных средств платежа // Закон и право. 2023. № 4. С. 153-155.
2. Егоров В.А. Особенности квалификации мошенничества, совершенного с использованием компьютерных средств и телекоммуникационных технологий // Концепт. 2018. №1. С. 43–49.
3. Харисова З.И. Актуальные проблемы деятельности правоохранительных органов по противодействию преступности в глобальной сети «Интернет» // Вестник Уфимского юридического института МВД России. 2019. № 3 (85). С. 92-98.
4. Давыдов В.О., Тишутина И.В. Цифровые следы в расследовании дистанционного мошенничества // Известия Тульского государственного университета. Экономические и юридические науки. 2020. № 3. С. 22.
5. Тропынина Н.Е. Цифровизация и обеспечение безопасности финансовых операций // Экономика и бизнес: теория и практика. 2021. № 2-2 (72). С. 128-130.
6. Потапова А.В. Мошенничество в сети интернет: криминологическая характеристика и проблемы квалификации // StudNet. 2020. Т. 3, № 6. С. 52-57.
7. Головин А.Ю., Головина Е.В. Социальная инженерия в механизме преступной деятельности в сфере информационно-телекоммуникационных технологий // Известия Тульского государственного университета. Экономические и юридические науки. 2021. Вып. 2. С. 3-13.
8. Коновалова К.В., Ермакова Т.Н. Мошенничество в сфере компьютерных технологий и сети интернет – современная угроза // Актуальные направления научных исследований: от теории к практике. 2016. № 3 (9). С. 177-179.
9. Мартыненко Н.Н., Овчаренко А.В. Мошенничество в сфере дистанционного банковского обслуживания и методы борьбы с ним в период пандемии // Инновации и инвестиции. 2020. № 12. С. 164-167.
10. Гаужаева В.А., Прокофьева Е.В. Особенности фиксации и изъятия цифровых следов // Право и государство: теория и практика. 2024. № 3 (231). С. 430-433.
11. Вестов Ф.А., Шамьенов Н.Р. Актуальность проблем DoS и DDoS-атак в уголовном праве в сфере компьютерной информации // Базис. 2020. № 1 (7). С. 13-16.
12. Шамшин А.А. Мошенничество в сфере компьютерной информации // Человек в мире природы и культуры. Трибуна молодых: сборник материалов Международной научно-практической конференции. Хабаровск: Дальневост. гос. ун-т путей сообщения, 2018. С. 443–447.
13. Барчуков В.К. К вопросу о квалификации мошенничества в сфере компьютерной информации // Пробелы в российском законодательстве. 2017. № 2. С. 128-130.
14. Денисов Е.А. Скриншоты в системе уголовно-процессуальных доказательств: вопросы теории и практики // Скиф. Вопросы студенческой науки. 2017. № 15(15). С. 179-183.
15. Овчинникова Ю.С., Милова И.Е. К вопросу о криминализации киберпреступлений // Наука XXI века: актуальные направления развития. 2020. № 1-2. С. 565.
16. Климова Я.А. Цифровая криминалистика: перспективы развития // Вестник Волгоградской академии МВД России. 2020. № 4 (55). С. 128-133.
17. Завьялов Д.А. Трансформация способов совершения мошенничества в современных условиях // Вопросы совершенствования правоохранительной деятельности: взаимодействие науки, нормотворчества и практики. IV Всероссийская научно-практическая конференция молодых ученых: сборник научных трудов. М.: Моск. ун-т МВД России им. В.Я. Кикотя, 2021. С. 165-168.
18. Озеров И.Н., Озеров К.И., Сергиенко В.В. Современные способы киберпреступлений // Противодействие незаконному обороту наркотиков в условиях цифровизации общества: сборник материалов Международной научно-практической конференции. Белгород: Белгород. юрид. ин-т МВД РФ им. И.Д. Путилина, 2024. С. 124-128.

19. Озеров К.И. Современные цифровые технологии, используемые в противодействии IT мошенничествам в призме обеспечения национальной безопасности // Вестник криминалистики. 2022. № 4 (84). С. 54-58.

20. Кобец П.Н., Краснова К.А. Проблемы классификации преступлений, совершаемых с использованием информационно-телекоммуникационных технологий // Правоохранительная деятельность органов внутренних дел в контексте современных научных исследований: материалы Международной научно-практической конференции. СПб.: С.-Петерб. ун-т МВД России, 2018. С. 178-181.

References

1. Badikov D.A., Eliseeva K.A. Algorithm of actions for investigators in cases of fraud involving electronic payment instruments. *Zakon i pravo = Law and Order*. 2023;(4):153-155. (In Russ.)
2. Egorov V.A. Specifics of qualification of fraud committed with the use of computer and telecommunication technologies. *Kontsept = Concept*. 2018;(1):43-49. (In Russ.)
3. Kharisova Z.I. Current issues in the activities of law enforcement agencies in counteracting crime on the global internet network. *Vestnik Ufimskogo yuridicheskogo instituta MVD Rossii = Bulletin of the Ufa Law Institute of the Ministry of Internal Affairs of Russia*. 2019;(3):92-98. (In Russ.)
4. Davydov V.O., Tishutina I.V. Digital traces in the investigation of remote fraud. *Izvestiya Tul'skogo gosudarstvennogo universiteta. Ekonomicheskie i yuridicheskie nauki = Izvestiya of Tula State University. Economic and Legal Sciences*. 2020;(3):22. (In Russ.)
5. Tropynina N.E. Digitalization and ensuring the security of financial transactions. *Ekonomika i biznes: teoriya i praktika = Economics and Business: Theory and Practice*. 2021;(2-2):128-130. (In Russ.)
6. Potapova A.V. Internet fraud: criminological characteristics and issues of qualification. *StudNet*. 2020;3(6):52-57. (In Russ.)
7. Golovin A.Yu., Golovina E.V. Social engineering in the mechanism of criminal activity in the sphere of information and telecommunication technologies. *Izvestiya Tul'skogo gosudarstvennogo universiteta. Ekonomicheskie i yuridicheskie nauki = Izvestiya Tula State University. Economic and Legal Sciences*. 2021;(2):3-13. (In Russ.)
8. Konovalova K.V., Ermakova T.N. Fraud in the sphere of computer technologies and the internet as a modern threat. *Aktual'nye napravleniya nauchnykh issledovaniy: ot teorii k praktike = Actual Directions of Scientific Research: From Theory to Practice*. 2016;(3):177-179. (In Russ.)
9. Martynenko N.N., Ovcharenko A.V. Fraud in remote banking services and methods of counteraction during the pandemic. *Innovatsii i investitsii = Innovations and Investments*. 2020;(12):164-167. (In Russ.)
10. Gauzhaeva V.A., Prokofieva E.V. Specifics of seizure and preservation of digital evidence. *Pravo i gosudarstvo: teoriya i praktika = Law and State: Theory and Practice*. 2024;(3):430-433. (In Russ.)
11. Vestov F.A., Shamyenov N.R. Relevance of issues of DoS and DDoS attacks under criminal law in the sphere of computer information. *Bazis = Basis*. 2020;(1):13-16. (In Russ.)
12. Shamshin A.A. Fraud in the sphere of computer information. In: *Chelovek v mire prirody i kul'tury. Tribuna molodykh: sbornik materialov Mezhdunarodnoi nauchno-prakticheskoi konferentsii = Man in the world of nature and culture. Tribune of young scholars: proceedings of the International scientific and practical conference*. Khabarovsk: Dal'nevost. gos. un-t putei soobshcheniya; 2018. P. 443-447. (In Russ.)
13. Barchukov V.K. On the issue of qualification of fraud in the sphere of computer information. *Probely v rossiiskom zakonodatel'stve = Gaps in Russian Legislation*. 2017;(2):128-130. (In Russ.)
14. Denisov E.A. Screenshots in the system of criminal procedure evidence: theoretical and practical issues. *Skif. Voprosy studentcheskoi nauki = Scythian: Questions of Student Science*. 2017;(15):179-183. (In Russ.)

15. Ovchinnikova Yu.S., Milova I.E. On the issue of criminalization of cybercrimes. *Nauka XXI veka: aktual'nye napravleniya razvitiya = Science of the 21st Century: Current Development Trends*. 2020;(1–2):565. (In Russ.)
16. Klimova Ya.A. Digital forensics: prospects for development. *Vestnik Volgogradskoi akademii MVD Rossii = Bulletin of the Volgograd Academy of the Ministry of Internal Affairs of Russia*. 2020;(4):128-133. (In Russ.)
17. Zavyalov D.A. Transformation of fraud methods under modern conditions. In: *Voprosy sovershenstvovaniya pravookhranitel'noi deyatel'nosti: vzaimodeistvie nauki, normotvorchestva i praktiki. IV Vserossiiskaya nauchno-prakticheskaya konferentsiya molodykh uchenykh: sbornik nauchnykh trudov = Issues of improving law enforcement activities: interaction of science, lawmaking, and practice: proceedings of the IV All-Russian scientific and practical conference of young scholars*. Moscow: Mosk. un-t MVD Rossii im. V.YA. Kikotya; 2021. P. 165-168. (In Russ.)
18. Ozerov I.N., Ozerov K.I., Sergienko V.V. Modern methods of cybercrime. In: *Protivodeistvie nezakonnomu oborotu narkotikov v usloviyakh tsifrovizatsii obshchestva: sbornik materialov Mezhdunarodnoi nauchno-prakticheskoi konferentsii. = Counteracting illegal drug trafficking in the context of society's digitalization: proceedings of the International scientific and practical conference*. Belgorod: Belgorod. yurid. in-t MVD RF im. I.D. Putilina; 2024. P. 124-128. (In Russ.)
19. Ozerov K.I. Modern digital technologies used in counteracting it fraud from the perspective of national security. *Vestnik kriminalistiki = Bulletin of Criminalistics*. 2022;(4):54-58. (In Russ.)
20. Kobets P.N., Krasnova K.A. Problems of classification of crimes committed using information and telecommunication technologies. In: *Pravookhranitel'naya deyatel'nost' organov vnutrennikh del v kontekste sovremennykh nauchnykh issledovaniy: materialy Mezhdunarodnoi nauchno-prakticheskoi konferentsii = Proceedings of the International scientific and practical conference*. St. Petersburg: S.-Peterb. un-t MVD Rossii; 2018. P. 178-181. (In Russ.)

Информация об авторе / Information about the Author

Василенко Артем Витальевич, Главный государственный налоговый инспектор отдела камеральных проверок 1, Межрайонная инспекция Федеральной налоговой службы № 13 по Московской области, г. Химки, Российская Федерация,
e-mail: vas.art7728@gmail.com,
ORCID: 0009-0003-6113-3122

Artem V. Vasilenko, Chief State Tax Inspector, Desk Audit Department No. 1, Interdistrict Inspectorate of the Federal Tax Service No. 13 for the Moscow Region, Khimki, Russian Federation,
e-mail: vas.art7728@gmail.com,
ORCID: 0009-0003-6113-3122