# Особенности возбуждения уголовного дела по признакам совершённого мошенничества в сфере компьютерной информации

**Савкин Александр Сергеевич**
магистр, юридический факультет, Московский университет им. С.Ю. Витте, savkin.alexandr@bk.ru

Современное общество переживает беспрецедентную цифровую трансформацию, которая, наряду с очевидными преимуществами, породила новые, высокотехнологичные формы преступлений. Мошенничество в сфере компьютерной информации выделено в самостоятельный состав преступления, при этом его квалификация и возбуждение уголовного дела, как первоначальный этап уголовного процесса, сопряжен целым с комплексом криминалистических задач. В центре внимания находятся проблемы, связанные с оценкой достаточности имеющихся в наличии данных, которые могут указывать на состав преступления и его признаки, в условиях высокой латентности и трансформации способов хищения. Ежегодно наблюдается количественный рост такого рода преступлений в общей массе преступности.
В качестве объективных признаков состава выступает предмет преступления, а именно: компьютерная информация используемая, как средство хищения; способы совершения: ввод, удаление, блокировка, модификация информации, вмешательство в работу средств хранения, обработки или передачи информации. Непосредственными примерами мошенничества в сфере компьютерной информации являются такие способы, как: использование вредоносного программного обеспечения (троянская программа ZeuS, вирус Melissa, программы Search Marquis, SpyLoan и WannaCry); так называемый фишинг, при котором мошенники пытаются получить данные пользователей, являющиеся конфиденциальными; несанкционированный доступ к аккаунтам, посредством ввода паролей, логинов, реквизитов банковских счетов и карт, а также манипуляций с электронными платежами.
В отличии от посягательств на чужое имущество, совершённых в условиях относительной очевидности, которые содержат признаки составов преступлений, предусмотренных статьями 158, 161, 162 УК РФ, при разрешении вопроса о возбуждении уголовного дела по статье 159.6 УК РФ ключевое значение имеет специфика предмета доказывания, которая должна фокусироваться на таких элементах, как способы обмана или злоупотребления доверием, реализуемые исключительно через компьютерные системы, а также характер причиняемого ущерба. Особое внимание следует уделять процессуальным сложностям, возникающим при обнаружении и изъятии цифровых доказательств, для их последующего процессуального закрепления, в связи с тем, что они могут быть дистанционно уничтожены, либо видоизменены. Так, некорректное копирование или изъятие жесткого диска с компьютера, без соблюдения требований протоколов копирования может привести к потере данных и недостаточности доказательной базы на стадии досудебного следствия.
**Ключевые слова:** преступная деятельность в сфере компьютерной информации, возбуждение уголовного дела, высокотехнологичные формы преступной деятельности.

На сегодняшний день, эпоха глобальной цифровизации пронизывает все отрасли человеческой жизнедеятельности. На этом фоне, закономерно выглядит трансформация объектов посягательств в криминальной сфере. Традиционные преступления, связанные с хищением имущества, активно мигрируют в киберпространство, приобретая новые, зачастую более изощренные и масштабные формы. В этом ряду особое место занимает мошенничество в сфере компьютерной информации, предусмотренное статьей 159.6 Уголовного кодекса Российской Федерации. Данная статья была введена Федеральным законом "О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации" от 29 ноября 2012 года, как ответ на вызовы времени, однако в правоприменительной практике, особенно на критически важной – начальной стадии уголовного процесса, имеют место пробелы, вызванные сложностями, связанными с отсутствием единства алгоритмов предпринимаемых действий, при поступлении в правоохранительные органы сообщений о совершённом преступлении, с использованием вредоносного ПО или хищением конфиденциальных данных.

Стадия доследственной проверки, при регистрации сообщения о преступлении, выступает своеобразным процессуальным фильтром и последующим фундаментом, заложенным в основу доказательной базы, на стадии досудебного следствия. Качество собранных доказательств, предопределяет успех или неудачу в раскрытии преступления, но применительно к мошенничеству в сфере компьютерной информации, этот этап изобилует особенностями, требующими от следователей и оперативных сотрудников не только глубоких правовых знаний, но и специфической цифровой компетенции. Нередко заявление в правоохранительные органы содержит лишь описание последствий: исчезновение денежных средств со счета, блокировка доступа к учетной записи, несанкционированное списание криптоактивов, что само по себе, без непосредственного установления факта, свидетельствующего о злоупотреблении доверием или фиксации обмана, может указывать на иные составы преступлений, предусмотренные статьями 272 - 274 УК РФ или согласно пункту 2 части 1 статьи 24 УПК РФ являться деянием, в котором отсутствует состав преступления. Довольно часто, сложности на данном этапе начинаются уже с восприятия самой сути исследуемого преступления. Мошенничество в сфере компьютерной информации, по своей юридической природе, остается хищением. Однако его «Modus operandi» коренным образом отличается от классических схем. Предметом преступления, предусмотренного ст. 159.6 УК РФ, являются не любые утраченные сведения, а исключительно компьютерная информация, под которой понимаются данные, представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи [1]. Это означает, что объектом посягательства становится не физическая вещь и не право на нее в чистом виде, а цифровая запись, изменение, блокировка или уничтожение которой позволяет злоумышленнику завладеть чужим имуществом или правом на его фактическое использование. Так, мошенник, получив через фишинг доступ к банковскому аккаунту, совершает не «классическую» кражу денег, а незаконные действия с

компьютерной информацией: её ввод, удаление или блокировку, что в итоге приводит к противоправному изъятию чужого имущества или приобретению права на его использование, что по своей природе также является хищением. Эта опосредованность через манипуляции с данными, создает первый барьер для понимания сути произошедшего как потерпевшими, так и сотрудниками правоохранительных органов, принимающими заявления.

Заявители далеко не всегда могут четко сформулировать, в чём именно выразился обман или злоупотребление доверием, особенно когда речь идет о преступлениях в сфере компьютерной информации с использованием сложных финансовых схем. Потерпевший, обращаясь в правоохранительные органы, часто описывает событие как «пропажу денег с карты» или «несанкционированный перевод». Задача лица, осуществляющего доследственную проверку – перевести этот бытовой эпизод в плоскость уголовно-правовой квалификации, вычленив из повествования обратившегося, признаки состава, предусмотренные статьёй 159.6 УК РФ. Ключевым элементом является установление способа совершения преступления: был ли обман или злоупотребление доверием, реализованы путём мошенничества именно по средствам ввода, удаления, блокировки или модификации компьютерной информации? Таким образом в зоне риска, могут оказаться не только компании, владеющие серверами, на которых хранится финансовая информация о счетах, денежных средствах и праве на их использование, а любой пользователь мобильного приложения, размещённого на принадлежащем ему мобильном устройстве. Злоумышленнику достаточно лишь на время завладеть чужим мобильным телефоном и данными банковской карты, чтобы в кратчайшие сроки изменив пароль в мобильном приложении, перевести денежные средства на подконтрольные ему лицевые счета. По факту, все личные вещи потерпевшего остаются на месте, но денежные суммы похищены и установить преступников в такой ситуации можно только при полном содействии банков или кредитных организаций, на счетах которых были размещены денежные средства потерпевшего.

Спектр возможных способов хищения невероятно широк и постоянно эволюционирует: от относительно простого взлома аккаунта до многоходовых схем с использованием социальной инженерии, вредоносного ПО, поддельных интернет-магазинов и фиктивных инвестиционных платформ. Как констатируют эксперты в области киберкриминалистики – использование социальной инженерии стало доминирующим методом при совершении мошенничества, связанного с компьютерной информацией, поскольку оно эксплуатирует «человеческий фактор», как наиболее уязвимое звено в системе безопасности [2]. В ходе проверки, подлежат детальному изучению следующие факты: какие именно действия совершал потерпевший (переход по ссылке, установка программы, ввод кода), какие данные были им непосредственно предоставлены, каким образом злоумышленнику удалось ввести его в заблуждение (имитация сайта банка, звонок от лжесотрудника службы безопасности).

Не менее важным элементом, подлежащим проверке при принятии решения о возбуждении уголовного дела, является размер причиненного ущерба. В контексте компьютерного мошенничества, его определение также имеет определённую специфику. Ущербом признаётся стоимость имущества, изъятого или приобретенного преступным путем. Однако в цифровой среде ценность может быть представлена не только в денежном эквиваленте, но и в виде криптовалют, дорогих внутриигровых предметов, NFT-токенов. Оценка такого ущерба требует привлечения специалистов, а иногда и проведения экспертизы уже на этапе доследственной проверки. Более того, учитывая трансграничный характер многих схем хищения, ущерб может быть причинён имуществу, расположенному за рубежом, что создает дополнительные процессуальные сложности. Установление размера ущерба при мошенничестве с использованием криптоактивов осложняется волатильностью их курса и отсутствием единообразных подходов к оценке на момент совершения преступления [3].

Центральное место при проведении доследственной проверки, по факту компьютерного мошенничества, занимает работа с цифровыми источниками, которые впоследствии играют ключевую роль в процессе доказывания на стадии судебного следствия. Именно их своевременное обнаружение, изъятие и процессуальное закрепление – решают судьбу будущего уголовного дела. Речь идет о самом широком круге носителей: логи интернет-трафика, история браузера, переписка в мессенджерах и соцсетях, электронные письма, метаданные файлов, дампы оперативной памяти, записи с камер видеонаблюдения, если преступление совершалось через публичный Wi-Fi. Проблема в том, что такая информация не всегда имеет долгосрочную фиксацию на мобильных носителях и может быть удалена автоматически (кеш, временные файлы) или зашифрована и храниться на серверах, расположенных в других странах.

Эксперты в области цифровых технологий, специализирующиеся на сборе цифровых доказательств, подчёркивают, что на стадии возбуждения уголовного дела, критически важно обеспечить сохранность источников компьютерной информации, применив в случае необходимости меры, предусмотренные ст. 164.1 УПК РФ, в частности, изъятие электронных носителей или получение трафика от провайдера [4]. На практике это требует от сотрудника, осуществляющего проверку, комплекса оперативных действий: немедленного направления запроса интернет-провайдеру о блокировке IP-адреса и сохранении логов, запроса в банк о приостановке операций и предоставлении детализации, а также квалифицированного осмотра устройства потерпевшего с участием специалиста в области информационно-коммуникационных технологий. Любая задержка может привести к безвозвратной утрате ключевых доказательств и потере средств.

Взаимодействие с потерпевшим на этой стадии также требует особого подхода. Потерпевшие в делах о компьютерном мошенничестве зачастую испытывают не только материальные потери, но и стресс, чувство растерянности. Их первичный опрос должен быть детализированным и технически грамотным. Подлежат выяснению не только обстоятельства и события, но и специфические детали: тип устройства и операционной системы, используемое антивирусное ПО, адреса посещаемых сайтов, точный текст сообщений, который был получен при взаимодействии с предполагаемыми мошенниками. Важно получить согласие на добровольную передачу устройства для дальнейшего исследования. Эффективный первичный опрос жертвы кибермошенничества является основой для построения модели инцидента и определения вектора дальнейшего расследования [5]. При этом важно разъяснить потерпевшему необходимость сохранения всех возможных следов на устройстве, до момента его первичного осмотра.

Одной из наиболее острых проблем остается трансграничность киберпреступлений. Серверы, домены, электронные кошельки для вывода средств часто находятся под юрисдикцией иностранных государств, что создает значительные препятствия оперативного получения информации не только на стадии проверки, но и при досудебном следствии. Время, необходимое для направления международного правового запроса через Генеральную прокуратуру РФ, может исчисляться месяцами, в то время

как данные на зарубежных сервисах могут храниться ограниченное количество времени. В этом контексте возрастает значение профессионального и непосредственного взаимодействия с администраторами крупных международных платформ (таких как Google и Telegram), которые в рамках своих внутренних политик могут оперативно предоставлять информацию по запросу правоохранительных органов, особенно в случаях, не терпящих отлагательств. Современные реалии требуют развития механизмов оперативного международного полицейского сотрудничества, в том числе для быстрого обмена криминалистически значимой информацией [6].

Как правило, ошибки, допускаемые на этапе возбуждения уголовного дела, носят системный характер. К наиболее типичным из них относятся: формальный отказ в возбуждении дела из-за «отсутствия состава преступления» при поверхностном анализе способа хищения; неистребование и неприобщение к материалам проверки ключевых цифровых доказательств (логов, скриншотов, ответов от банков); некорректная квалификация, в случаях когда действия, подпадающие под статью 159.6 УК РФ, ошибочно пытаются квалифицировать согласно статье 159 УК РФ, игнорируя компьютерную составляющую способа хищения. Верховный Суд РФ указывает, что разграничение составов преступлений, предусмотренных ст. 159 и ст. 159.6 УК РФ, должно проводиться в зависимости от способа совершения хищения: если обман или злоупотребление доверием были направлены непосредственно на владельца имущества, присутствует состав мошенничества в соответствии со ст. 159 УК РФ); если же эти действия были осуществлены путем воздействия на компьютерную информацию, содеянное надлежит квалифицировать по ст. 159.6 УК РФ

Таким образом, для повышения эффективности проверки на стадии возбуждения уголовного дела о мошенничестве в сфере компьютерной информации стоит применять комплексный подход, при использовании которого, необходимо постоянно повышать уровень цифровой грамотности сотрудников правоохранительных органов, системно разрабатывать и внедрять специализированные алгоритмы действий, создавать мобильные группы быстрого реагирования с участием IT-специалистов, укреплять каналы оперативного взаимодействия с финансовыми институтами и интернет-компаниями. Необходима стандартизация процедур первоначальных проверочных действий при обращениях, связанных с кибермошенничеством, что позволит минимизировать риски утраты доказательств и обеспечить единообразие правоприменительной практики [7].

В конечном счете, качество решений, принимаемых на этапе возбуждения уголовного дела, определяет не только судьбу конкретного уголовного преследования, но и уровень доверия граждан к способности государства защищать их права при взаимодействии в цифровой среде. Сложность и динамика кибермошенничества делают эту задачу чрезвычайно трудной, ввиду крайне стремительного развития пользовательских систем и повсеместно внедряемого программного обеспечения с использованием искусственного интеллекта [8]. Современные нейросети, обученные на гигантских массивах аудиоданных, способны генерировать человеческую речь с пугающим реализмом. Они могут имитировать не просто голос, а эмоции – страх, спешку, боль, раскаяние, тем самым снимая барьеры недоверия. Сценарии обычно разворачиваются в два этапа: первый – звонок «от государственных органов». Звонящий, представляясь сотрудником банка, правоохранительных органов или службы технической поддержки портала «Госуслуги», сообщает жертве о имевшей место подозрительной активности: попытке взлома, незаконном оформлении кредита, начислении огромного штрафа, причастности к финансовому преступлению. Голос может быть как живым, так и уже сгенерированным ИИ, копирующим официальный, спокойный тон сотрудника ведомства. Основная цель на данном этапе – вызвать максимальный стресс и чувство опасности, парализовать критическое мышление. Человеку сообщают, что его «счета находятся под угрозой». Естественным желанием становится, как можно быстрее решить проблему и вот здесь начинается второй - технический этап. Чтобы «защитить деньги», «заблокировать мошенников» или «провести проверку», «сотрудник» просит предоставить данные для «идентификации» или «удалённого доступа». Под предлогом «восстановления безопасности» у жертвы выманивают одноразовые пароли из СМС, коды доступа к порталу государственных услуг, паспортные данные, логины и пароли от онлайн-банка. Как правило мошенники сообщают, что: «Для подтверждения личности было направлено СМС с кодом». На экран телефона действительно приходит код доступа к учётной записи на Gosuslugi.ru, но инициировал данный запрос сам преступник, который в этот момент находится на странице восстановления пароля. Узнав код, он мгновенно получает полный контроль над аккаунтом жертвы. А в аккаунте «Gosuslugi.ru» в современных условиях, зачастую содержится кладезь информации: паспортные данные, СНИЛС, ИНН, сведения об имуществе, налоговые задолженности. Получив доступ к личному кабинету, мошенники действуют молниеносно.

Как отмечает современный криминолог, противодействие мошенничеству в сфере компьютерной информации должно начинаться с процессуально грамотной, технически оснащенной и оперативно проводимой стадии возбуждения уголовного дела, которая выступает в роли «умного фильтра» всего последующего расследования [9]. От квалифицированности принимаемых решений напрямую зависит эффективность всего механизма противодействия данному виду преступности.

Только осознание уникальности этой стадии, при расследовании цифровых преступлений и адаптация к ней процессуальных и тактических инструментов позволит правоохранительной системе адекватно отвечать на вызовы цифровой эпохи.

**Заключение**

Резюмируя сказанное, можно сформулировать ряд выводов, характеризующих специфику и определяющие векторы совершенствования процедуры возбуждения уголовного дела по признакам мошенничества в сфере компьютерной информации. Ключевая особенность данной стадии процесса заключается в необходимости двойной компетенции правоприменя: глубокого понимания конструкции состава преступления предусмотренной статьёй 159.6 УК РФ и практических навыков работы с цифровыми доказательствами. Наличие признаков преступления определяется не через физические следы, а путём исследования данных, требующих немедленного и профессионального реагирования, для их последующего сохранения. Объективность подхода состоит в комплексном рассмотрении стадии возбуждения дела как единой системы, интегрирующей уголовно-правовую квалификацию, криминалистическую тактику и информационно-технологическую составляющую, в то время как в правоприменительной практике, эти аспекты часто рассматривают изолированно. Результаты анализа демонстрируют, что типичные ошибки на этом этапе (неверное разграничение составов, пассивная позиция при истребовании информации) коренятся в устаревших, ориентированных на «материальные» преступления, подходах исследования поступивших материалов, при проведении доследственной проверки. Необходимо применение специализированных познаний,

начиная с первых минут поступления сообщения о преступлении и детализированный опрос потерпевшего с акцентом на технические нюансы, имевших место событий. Требуется взаимодействие в сфере межведомственного и международного сотрудничества для выстраивания более эффективных каналов быстрого обмена информацией с частными компаниями (банками, IT-гигантами) и зарубежными коллегами в целях преодоления трансграничной киберпреступности и более полного представления о возможных связях на всей территории криминального ландшафта. Оптимизация стадии возбуждения уголовного дела является не техническим усовершенствованием, а стратегической задачей в борьбе с мошенничеством в компьютерной сфере. Ее успешное решение позволит не только увеличить раскрываемость данного рода преступлений и обеспечить возмещение ущерба потерпевшим, но и создать действенный барьер на пути криминализации цифрового пространства, укрепляя правопорядок и доверие к государственным институтам в условиях цифровой трансформации общества.

**Литература**


1. Куликов А.В. Проблемные вопросы хищения безналичных денежных средств путем мошенничества с использованием компьютерных технологий (п. «в» ч. 3 ст. 159.6 УК РФ)// Криминалист. 2025. № 4(53) С. 63 – 71.
2. Цифровая криминалистика: учебник для вузов / под редакцией В. Б. Вехова, С. В. Зуева. – 2-е изд., перераб. и доп. – Москва: Юрайт, 2024. – С. 201 – 207.
3. Е. П. Данилова, Е. М. Портняга Финансовое мошенничество в современном мире // Siberian Socium. 2023. Том 7. No 2 (24). С. 67 – 97.
4. Бадзгарадзе Г. Д. Особенности возбуждения уголовного дела о мошенничестве, совершенном с использованием информационных технологий// Криминалист. 2023. № 3(44) – С. 3 – 11.
5. Гусева, И.И., Коробова, И.В. К вопросу об использовании цифровых доказательств в уголовном процессе // Гуманитарные, социально-экономические и общественные науки. – 2022. – No 11-2. – С. 64.
6. Цифровая криминалистика: учебник для вузов / под редакцией В. Б. Вехова, С. В. Зуева. – 2-е изд., перераб. и доп. – Москва: Юрайт, 2024. – С. 132 – 137.
7. Васюков В. Ф., Стражинская А. Н. К вопросу об организационных и процессуальных особенностях получения электронных данных при расследовании преступлений // Вестник Московского университета МВД России. 2024 № 6 С. 20-25.
8. Арзамасцев М.В. Цифровая валюта как легализуемое имущество// Журнал российского права. 2025. № 5. С. 122-135.
9. Жижина, М. В. Личность субъекта преступлений в сфере компьютерной информации как системообразующий элемент криминалистической характеристики (по материалам российских и зарубежных источников) / М. В. Жижина, Д. В. Завьялова // Актуальные проблемы российского права. – 2022. – Т. 17, № 5 (138). – С. 149 – 158.


**Features of initiation of criminal cases based on signs of committed fraud in the sphere of computer information**


**Savkin A.S.**

Moscow Witte University



Modern society is experiencing an unprecedented digital transformation, which, along with its obvious advantages, has given rise to new, high-tech forms of criminal activity. Computer information fraud has been designated as a separate crime, but its classification and initiation of a criminal case, as the initial stage of the criminal process, presents a complex set of forensic challenges. The focus is on assessing the sufficiency of available data that may indicate the elements of a crime and its characteristics, given the high level of latency and the transformation of methods of theft. Every year, there is an increase in the number of such crimes in the overall crime rate.

The objective elements of the crime include the subject of the crime, namely, computer information used as a means of theft, and the methods of committing the crime, such as entering, deleting, blocking, or modifying information, or interfering with the storage, processing, or transmission of information. Direct examples of computer information fraud include: the use of malicious software (such as the ZeuS Trojan, Melissa virus, Search Marquis, SpyLoan, and WannaCry programs); so-called phishing, where fraudsters attempt to obtain sensitive user data; and unauthorized access to accounts through the use of passwords, usernames, bank account and card details, and electronic payment manipulation.

Unlike encroachments on someone else's property committed under conditions of relative clarity, which contain elements of crimes under Articles 158, 161, and 162 of the Criminal Code of the Russian Federation, the key factor in deciding whether to initiate a criminal case under Article 159.6 of the Criminal Code of the Russian Federation is the specific nature of the subject matter, which should focus on elements such as the methods of deception or abuse of trust implemented exclusively through computer systems, as well as the nature of the damage caused. Special attention should be paid to the procedural difficulties that arise when digital evidence is discovered and seized, as it may be remotely destroyed or modified. For example, improper copying or removal of a hard drive from a computer without following the required copying protocols can result in data loss and insufficient evidence during the pre-trial investigation phase. It is also important to distinguish the specific features of this crime from related offenses, such as unauthorized access to computer information (Article 272 of the Criminal Code of the Russian Federation) or the creation and use of malicious software (Article 273 of the Criminal Code of the Russian Federation), as well as the violation of rules for the use of means of storage, processing, or transmission of computer information (Article 274 of the Criminal Code of the Russian Federation), which directly affects the correct classification of a crime report. To assess and analyze the information provided by the victim, it is necessary to involve IT security specialists at an early stage. It is necessary to develop tactics and methods that are relevant to the current time, aimed at effective interaction with victims, obtaining primary information from Internet providers and financial organizations, as well as overcoming the cross-border nature of these crimes. Decisions on initiating or refusing to initiate criminal cases should be based on modern scientific doctrine, relevant judicial practice, and recent changes in legislation, which in turn will allow for more precise formulation of practical-oriented recommendations for optimizing pre-investigation checks and making legal and reasonable procedural decisions.



Keywords: criminal activity in the field of computer information, initiation of a criminal case, high-tech forms of criminal activity.


**References**


1. Kulikov A.V. Problematic issues of theft of non-cash funds by fraud using computer technologies (p. "v" of Part 3 of Article 159.6 of the Criminal Code of the Russian Federation)// Kriminalist. 2025. No. 4(53) Pp. 63 – 71.
2. Digital Forensics: Textbook for Universities / edited by V. B. Vekhov, S. V. Zuev. – 2nd edition, revised. and add. – Moscow: Yurayt, 2024. – Pp. 201 – 207.
3. E. P. Danilova, E. M. Portnyaga Financial Fraud in the Modern World // Siberian Socium. 2023. Vol. 7. No. 2 (24). Pp. 67-97.
4. Badzgaradze G. D. Features of Initiating a Criminal Case on Fraud Committed Using Information Technologies// Criminalist. 2023. No. 3(44). Pp. 3-11
5. Guseva, I.I., Korobova, I.V. On the Use of Digital Evidence in Criminal Proceedings // Humanities, Social Sciences, Economics, and Law. – 2022. – No. 11-2. – P. 64.
6. Digital Forensics: A Textbook for Universities / Edited by V. B. Vekhov and S. V. Zuev. – 2nd edition, revised. and add. – Moscow: Yurayt, 2024. – P. 132 – 137
7. Vasyukov V. F., Strazhinskaya A. N. On the issue of organizational and procedural features of obtaining electronic data in the investigation of crimes // Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia. 2024 No. 6 P. 20-25.
8. Arzamasov M.V. Digital currency as legalized property// Journal of Russian Law. 2025. No. 5. Pp. 122-135.
9. Zhizhina, M. V. The Personality of the Subject of Computer Information Crimes as a System-Forming Element of the Criminalistic Characteristics (Based on Russian and Foreign Sources) / M. V. Zhizhina, D. V. Zavyalova // Actual Problems of Russian Law. – 2022. – Vol. 17, No. 5 (138). – Pp. 149–158.