

Дата поступления рукописи в редакцию: 06.02.2026 г.
Дата принятия рукописи в печать: 18.03.2026 г.

DOI: 10.24412/2782-3830-2026-2-301-308

ПОСАШКОВ Антон Сергеевич,
заместитель командира взвода
факультета подготовки дознавателей
Белгородского юридического института
МВД России имени И.Д. Путилина,
e-mail: posashkov04@internet.ru

НОВИКОВА Екатерина Анатольевна,
кандидат юридических наук, доцент,
начальник кафедры информационно-компьютерных
технологий в деятельности органов внутренних дел
Белгородского юридического института
МВД России имени И.Д. Путилина,
e-mail: tomchik1980@mail.ru

ЖИТИНЕВА Оксана Александровна,
старший научный сотрудник
отделения организации научно-исследовательской
работы научно-исследовательского отдела
Белгородского юридического института
МВД России имени И.Д. Путилина,
e-mail: oksana.kls80@mail.ru

НОВИКОВА Яна Олеговна,
курсант 4 «С»-1 курса 3205 взвода
института-факультета подготовки сотрудников
для органов предварительного расследования
Московского ордена почета университета
МВД России имени В.Я. Кикотя,
e-mail: annanovikovaol3004@gmail.com

ОСОБЕННОСТИ ДОКАЗЫВАНИЯ ПРЕСТУПЛЕНИЙ ЭКОНОМИЧЕСКОЙ НАПРАВЛЕННОСТИ, СВЯЗАННЫХ С ЦИФРОВЫМИ ФИНАНСОВЫМИ ИНСТРУМЕНТАМИ

Аннотация. В научной статье уделяется особое внимание проблемным аспектам, возникающим в процессе собирания доказательственной информации с использованием цифровых материалов при расследовании преступлений экономической направленности. Авторами анализируется специфика расследования компьютерных атак на финансовые предприятия и хищений цифровых активов, выделяются основные проблемы в данной области: трансграничный характер преступлений, трудности фиксации и оценки цифровых активов, отсутствие единых методик определения размера ущерба и правовая неопределенность криптовалюты (имущество или средство платежа).

Подчеркивается исключительная роль специалистов, обладающих специальными познаниями в области информационных технологий, финансового анализа, бухгалтерского учета для формирования достоверной и допустимой доказательственной базы. Особое значение придается соблюдению строгого процессуального порядка при осмотре, изъятии и фиксации цифровых следов, сохранении их неизменности и, как следствие, дальнейшем использовании в доказывании преступлений экономической направленности.

Авторами формулируются предложения, нацеленные на комплексную реформу отдельных отраслей законодательства, конкретизацию понятий и критериев, а также разработку специальных методик и механизмов взыскания цифровых активов. Необходимость системно-

го правового регулирования в указанном вопросе обусловлена механизмом мер, направленных на противодействие преступлениям экономической направленности и киберпреступлениям.

Ключевые слова: преступления экономической направленности, цифровые доказательства, криптовалюта, цифровые активы, электронные следы, доказывание.

POSASHKOV Anton Sergeevich,

Deputy Platoon Commander,

Investigator Training Department Belgorod Law Institute

The Ministry of Internal Affairs of Russia named after I.D. Putilin

NOVIKOVA Ekaterina Anatolyevna,

Candidate of Law, Associate Professor,

Head of the Department ICT in Law Enforcement Agencies

Belgorod Law Institute The Ministry of Internal

Affairs of Russia named after I.D. Putilin

ZHITINEVA Oksana Alexandrovna,

Senior Researcher at the Department of Organization

of Scientific Research Work of the Scientific Research Department

Belgorod Law Institute The Ministry of Internal

Affairs of Russia named after I.D. Putilin

NOVIKOVA Yana Olegovna,

Cadet of the 4th «C»-1st year,

3205th platoon of the Institute-Faculty of Training Employees

for Preliminary Investigation Bodies Moscow Order

of Honor University V.Ya. Kikot' Ministry of Internal Affairs of Russia

FEATURES OF PROVING CRIMES OF AN ECONOMIC NATURE, RELATED TO DIGITAL FINANCIAL INSTRUMENTS

Annotation. *The scientific article focuses on the problematic aspects that arise during the collection of evidence using digital materials in the investigation of economic crimes. The authors analyze the specifics of investigating computer attacks on financial institutions and the theft of digital assets, highlighting the main challenges in this area: the cross-border nature of crimes, difficulties in capturing and evaluating digital assets, the lack of unified methods for determining the amount of damage, and the legal uncertainty surrounding cryptocurrency (as property or as a means of payment).*

The article emphasizes the exceptional role of specialists and experts with special knowledge in the field of information technology, financial analysis, and accounting in forming a reliable and admissible evidence base. Special attention is given to the strict adherence to procedural rules during the examination, seizure, and fixation of digital traces, ensuring their preservation and, as a result, their further use in proving economic crimes.

The authors formulate proposals aimed at a comprehensive reform of certain branches of legislation, the specification of concepts and criteria, as well as the development of special methods and mechanisms for recovering digital assets. The need for systemic legal regulation in this area is due to the mechanism of measures aimed at countering economic crimes and cybercrimes.

Key words: *digital evidence, cryptocurrencies, digital assets, criminal procedure, fixation, electronic traces, damage, evidence, Criminal Procedure Code of the Russian Federation, proving.*

В уголовном судопроизводстве доказательства представляют собой любые сведения, на основе которых органы предварительного расследования и суд устанавливают обстоятельства, имеющие значение для уголов-

ного дела. Законодатель закрепляет перечень видов доказательств в части 2 статьи 74 УПК РФ, при этом указанные сведения должны отвечать требованиям относимости, допустимости и достоверности, а их собирание, проверка и

оценка осуществляться в строгом соответствии с уголовно-процессуальным законодательством.

Комплексный подход к установлению истины в уголовном судопроизводстве предполагает всестороннее исследование всех имеющихся сведений, где каждое собранное доказательство – от показаний свидетелей до цифровых следов – вносит существенный вклад в формирование всей доказательственной базы. Определяющим критерием допустимости сведений является их относимость и законность получения. Это означает, что различного вида доказательства по конкретному уголовному делу должны указывать на обстоятельства, подлежащие доказыванию, и соответствовать установленным процессуальным нормам.

Российское законодательство не выделяет электронные доказательства или цифровые следы как отдельную категорию, однако цифровые материалы могут быть представлены в рамках уже существующих видов источников. Согласно статье 81 УПК РФ, к вещественным доказательствам относятся любые материальные предметы, которые сохранили следы преступления, являлись орудиями преступления или выступали объектами преступного посягательства.

В соответствии с частью 2 статьи 84 УПК РФ, «документы могут содержать сведения, зафиксированные в различных формах (фото- и киносъемки, аудио- и видеозаписи, иные носители информации, полученные в соответствии со статьей 86 УПК РФ)» [1].

Цифровые следы или цифровые материалы – файлы документов, электронная переписка, данные блокчейна, осмотры аккаунтов и личных кабинетов – обычно приобщаются к уголовному делу посредством протокола осмотра оперативно-розыскных или процессуальных мероприятий, иными видами протоколов, а также документами или предоставленной информацией по запросу уполномоченных органов.

Например, Князков А.А. рассматривает цифровые финансовые активы как предмет преступления и отмечает, что к ним относятся криптовалюта, цифровые права, токены и другие формы виртуальных ценностей. Автор подчеркивает, что данные активы могут быть децентрализованными, что усложняет их регулирование и доказывание преступления в уголовном процессе [2].

Основополагающими условиями является соблюдение процедуры собирания и соблюдение критериев оценки относимости, достаточности, допустимости и достоверности доказательств.

Нарушение установленного порядка влечет признание доказательств недопустимыми (часть 1 статьи 75 УПК РФ).

Специфика деятельности сотрудников органов предварительного расследования и специалистов при работе с электронными доказательствами предполагает необходимость четкой законодательной регламентации порядка их осмотра, изъятия и фиксации, а также предварительное изучение методических рекомендаций, нацеленных на следование четкому алгоритму действий, направленному на неизменность доказательств с момента их обнаружения и изъятия.

В современных реалиях особенности расследования преступлений в сфере экономической направленности и информационно - коммуникационных технологий требуют привлечения специалистов, обладающих специальными знаниями и компетенциями. Это обусловлено комплексным характером правонарушений, требующих междисциплинарного подхода к их расследованию.

Согласно положениям УПК РФ заключение и показания специалиста или эксперта являются самостоятельными видами доказательств. Данная норма позволяет органам предварительного расследования активно привлекать специалистов различных областей – от финансового анализа и цифровых активов до информационной безопасности, для формирования доказательственной базы и преодоления угрозы потери доказательственной информации или факта совершения иных преступлений. При проверке сообщений о преступлении и его дальнейшем расследовании эксперты проводят всестороннюю оценку собранных материалов, которые оформляются в виде заключений и приобщаются к материалам проверки или уголовного дела. Особую роль играет компетентность специалистов и экспертов, способных работать на стыке различных наук и профессиональных отраслей. Данные заключения и показания способствуют подтверждению факта наличия состава преступления.

Нельзя не согласиться с Тимченко В.А. в том, что «расследование и судебное разбирательство дел о преступлениях, совершенных с использованием цифровых финансовых активов, цифровой валюты, криптовалюты, практически невозможно без использования специальных знаний судебного эксперта или специалиста» [3].

Таким образом, привлечение специалистов или экспертов является неотъемлемым элементом современного уголовного судопроизводства, особенно при расследовании преступлений, связанных с экономическими преступлениями и цифровыми активами.

Преступления, связанные с компьютерными атаками на финансовые учреждения, отличаются особой технической и процессуальной сложностью и международным характером формирования доказательственной базы.

Основу доказательственной информации по данному виду преступлений составляют цифровые следы [4]:

- системные журналы серверов и сетевого оборудования;
- данные системы безопасности;
- информация с электронных материальных носителей информации (жесткие диски, флеш-накопители, сервера и т.д.);
- вредоносные программы и сопутствующие файлы;
- материалы компьютерно-технических экспертиз.

Все изъятые материалы требуют правильного процессуального оформления и фиксации в протоколе осмотра места происшествия, выемки или обыска. Процессуальные документы заверяются подписями участвующих лиц и, согласно статье 83 УПК РФ, правильно оформленные протоколы следственных действий являются доказательством по уголовному делу. К ним могут прилагаться электронные носители информации, фототаблицы, скриншоты, протоколы осмотра и распечатки цифровых данных.

В случае, если электронные данные поступают не в результате производства следственных или процессуальных действий, а от иных источников получения информации (предоставление службой собственной безопасности, представителем банка, интернет-провайдера, сотрудниками информационной безопасности или иного должностного лица и др.) они приобщаются к уголовному делу как «иные документы» в соответствии со статьей 84 УПК РФ.

Данные преступления зачастую носят трансграничный характер и как отмечает Клевцов К.К. «киберпреступления как правило носят международный характер, поскольку имеют негативные последствия на территории других суверенов» [5].

Расследование компьютерных атак на финансовые учреждения представляет особую сложность из-за их международного характера и специфики хранения доказательств. Подозреваемые зачастую используют зарубежные сервера для размещения данных, а их местонахождение может быть за пределами юрисдикции российских органов предварительного расследования.

В целях преодоления данных трудностей правоохранительные органы используют различные механизмы международного сотрудничества:

двусторонние договоры о правовой помощи, каналы связи через Интерпол, запросы о правовой помощи через Генпрокуратуру РФ, механизм сотрудничества через международное объединение или организации (СНГ, БРИКС, ШОС, ЕС и иные).

Экспертному анализу может подвергаться различный вид носителей информации: компьютеры, мобильные устройства, средства связи, SIM- карты, флеш-накопители, кассовые машины, электронные подписи, программные продукты, сервера и т.д. При этом эксперт должен грамотно подобрать инструменты и методы исследования, чтобы обеспечить допустимость и достоверность получаемых результатов в соответствии с процессуальными требованиями.

При необходимости предоставления суду части электронного массива данных, например, переписка между подозреваемым и соучастником в заданный следователем период, применяются специальные процедуры:

- оформление заверенных копий;
- хеширование исходного объекта и готовой копии;
- документация ключевых фрагментов, имеющих значение для уголовного дела, посредством фотографирования и создания фототаблиц;
- протоколирование основополагающих деталей и процессов.

При этом оригинальный носитель информации сохраняется в неизменном виде для повторной проверки, чтобы обеспечить прозрачность и законность при верификации данных цифровых следов в доказательства.

Особую значимость также приобретает оценка не только подлинности электронных данных, но и их юридической значимости. В процессе судебного разбирательства цифровые доказательства рассматриваются в комплексе с традиционными видами. Например, совпадение показаний свидетелей с данными камер видеонаблюдения, что в свою очередь взаимоусиливает предоставленные суду доказательства.

Доктор юридических наук, профессор Зуев С.В. подчеркивает, что электронные доказательства не являются «особой категорией». Они подлежат тем же критериям оценки, что и традиционные, однако специфика их формирования и сохранения требует специальных процессуальных гарантий [6].

Современная тенденция правоприменения характеризуется постепенным стиранием границ между электронными и традиционными доказательствами. Практически любой вид доказательств также может иметь цифровую природу

или отражение. В международной и отечественной практике формируется единый подход к анализу представленных материалов, который характеризуется комплексным анализом всех предоставленных данных, обеспечением строгих процессуальных гарантий, предусмотренных законодательством, и отсутствием предвзятого отношения к цифровым следам или доказательствам.

При расследовании хищений криптовалют органы предварительного расследования сталкиваются со следующими ключевыми и взаимосвязанными проблемами: фиксации наличия актива, определения его точного объема и правомерной оценки в стоимостном выражении для точного определения размера ущерба. Каждый этап сопряжен со специфическими правовыми и техническими рисками, способными поставить под сомнение всю доказательственную базу.

Первостепенной задачей является документальное подтверждение того, что у потерпевшего на определенный момент времени действительно находилось во владении конкретное количество криптоактива. Источники данных в данном случае делятся на два основных типа:

- офчейн-данные с централизованных бирж и сервисов. Их получение требует направления официальных запросов, в том числе через механизмы международной правовой помощи, а успех зависит от юрисдикции и принципов иностранной компании;
- ончейн-данные из публичного блокчейна. Следовательно, специалист или оперативный сотрудник анализирует историю транзакций через обозреватели blockchain.com или etherscan.io.

Доказательственное значение в данном случае будет иметь не распечатка баланса, а составленный протокол осмотра интернет-ресурса (статья 164, 166, 180 УПК РФ). Указанный протокол должен содержать детальное описание действий: точное время и дату осмотра, использование программного обеспечения, фиксацию IP-адресов и хеш-сумм страниц, данные баланса и истории транзакций, оформленные скриншотом или фототаблицей и приобщенные к протоколу осмотра, по возможности заверенные электронной подписью следователя.

В приговоре Находкинского городского суда Приморского края от 17.07.2025 хеш-суммы файлов использовались как средство подтверждения неизменности цифровых доказательств при доказывании деяний, предусмотренных статьей 272 и 159 УК РФ [7].

Отдельной сложностью в рамках данного вопроса является проблема обеспечения доступа

к личному кабинету, когда приватные ключи не записаны на материальном носителе, а хранятся в памяти или уничтожены. В данном случае установить исходный объем можно лишь по косвенным данным, которые не всегда будут отражать объективную реальность: переписки о переводе средств, показаниям возможных свидетелей, истории выводов с бирж на конкретный адрес, что в последствии существенно ослабляет позицию обвинения.

Определение размера материального ущерба – наиболее оспариваемый аспект при расследовании преступлений стороной защиты, поскольку отсутствует единая утвержденная методика, а курс активов исключительно изменчив. Данный критерий порождает два вопроса: выбор момента оценки и выбор источника курса.

Как верно отмечает Филатова М.А. «отсутствие четких критериев определения размера ущерба при хищении криптовалюты порождает споры в судебной практике. Ключевыми проблемами являются выбор даты оценки и источника курса, так как эти параметры напрямую влияют на сумму ущерба и квалификацию деяния» [8]. Сумма ущерба напрямую зависит от даты оценки, что влияет на квалификацию преступления. Типичные моменты: период совершения преступления, момент обнаружения, дата возбуждения уголовного дела, дата проведения экспертизы или время транзакции. Каждый вариант может быть обоснован с различных точек зрения, исходя из реального ущерба или фактических данных.

Выбор источника курса является определяющей задачей следователя в рамках квалификации преступного деяния. Именно он должен решать какой конкретной биржи использовать курс, где хранил активы потерпевший, данные агрегаторов или даже информацию с децентрализованных бирж. В условиях отсутствия официального курсообразования в России это решение носит дискреционный характер.

В целях преодоления данной неопределенности органы предварительного расследования в обязательном порядке назначают финансово-экономическую экспертизу. В постановлении о назначении экспертизы формулируется вопрос: «Определите рыночную стоимость ... единиц криптовалюты (наименование) в рублях на момент (указание необходимой даты и времени до минут по часовому поясу ...) с использованием данных (сайт Binance). Таким образом, следователь фактически делегирует эксперту техническое вычисление, при заданных необходимых параметрах.

Решение следователя об определении даты и источника курса должно быть подробно мотивировано в соответствующих процессуальных

документах, так как с высокой долей вероятности будет оспариваться защитой, которая может настаивать на другой дате или источнике, кардинально меняющем сумму ущерба. Экспертиза в данном случае выполняет не только расчетную, но и стабилизирующую функцию, придавая выработанной методике научную обоснованность, объективность и независимость. Однако суд и сторона защиты вправе оценить как заключение экспертизы, так и обоснованность заданных вопросов и критерии исходных параметров, что делает данный этап доказывания наиболее сложным и спорным в рамках дел о цифровых активах.

Правовая квалификация цифровых активов как иного имущества или как средства платежа является не теоретико-законодательным выбором, а практикой применения, предопределяющей предмет доказывания, способ оценки ущерба и механизм его возмещения. Данный выбор создает различные процессуальные пути и направления расследования.

В рамках подхода к определению криптовалюты как иного имущества предметом доказывания становится факт законного владения в результате преступных действий. Доказывание владения выходит за рамки простой констатации знания ключей. Прежде необходимо установить легальность приобретения актива (добыча, покупка, обмен, майнинг удаленно и иное), возможность технически распоряжаться им и отсутствие правовых препятствий для такого владения. Правовой базой служит преимущественно сложившаяся судебная практика по статьям 159 УК РФ и иных преступлений экономической направленности. Кроме того, федеральный закон «О цифровых финансовых активах» оставляет вне прямого регулирования многие популярные криптоактивы или криптобиржи, создавая правовой вакуум для их квалификации. Правовым последствием для потерпевшего является тот факт, что ущерб подлежит возмещению в рублевом эквиваленте, рассчитанном по методике, описанной ранее. Возврат именно той же криптовалюты в рамках исполнительного производства практически нереализуем из-за отсутствия механизма принудительного взыскания и передачи цифровых ключей, что ставит потерпевшего в зависимость от изменчивости рынка и выбранной даты оценки.

Подход, который определяет криптовалюту как средство платежа, смещает фокус доказывания с факта владения имуществом на функциональное назначение актива и направленность умысла виновного. Требуется доказать, что криптовалюта использовалась или предназнача-

лась для использования именно в качестве расчетного инструмента, а целью посягательства было завладение именно этим универсальным финансовым ресурсом. Это может влиять на квалификацию. Несмотря на позицию Банка России, отрицающую законный статус криптовалют как платежного средства, суды могут признавать их фактическим средством платежа в контексте конкретного преступного деяния. На практике, однако, это также приводит к взысканию ущерба в рублях, поскольку российская судебная система оперирует национальной валютой.

В условиях правовой неопределенности органы предварительного расследования должны действовать по принципу двойной квалификации в теории, ввиду того, что единого и максимально широкого подхода в доказывании на практике нет. Это означает, что при формулировке обвинения возможно использование таких терминов как: денежные средства в форме криптовалюты; цифровые активы, являющиеся иным имуществом, однако собирать доказательственную базу необходимо с учетом указанных возможных трактовок. В этой связи предполагается фиксация всего комплекса обстоятельств: факта и способа владения (носители ключей, пароли); функционального использования актива (переписка о расчетах, история транзакций, оплата товаров и услуг); преступного умысла и последующих действий лица подозреваемого (намерение обналичить, вывести в иные криптобиржи, конвертировать или использовать для легализации). Основную роль играет финансовый анализ, выходящий за рамки простой технической экспертизы. Специалист в этой области должен не только изъять данные, но и произвести оперативный анализ цепочки транзакций, осуществлять кластеризацию адресов для идентификации ассоциированных кошельков, проследить движение средств до точек обналичивания (фиатных бирж) и подготовить понятные для суда графики и схемы, наглядно демонстрирующие механизм осуществления преступления и умысел. Также важно процессуально грамотно закрепить субъективное отношение потерпевшего к активу в его показаниях (инвестиция, средство сбережения, инструмент для расчетов), так как это может служить дополнительным аргументом при выборе квалификации и методов оценки ущерба.

В приговоре № 1-39/2025 1-402/2024 от 9 марта 2025 г. по делу № 1-39/2025 Московского районного суда города Казани следователь определил, что сумма ущерба будет равна денежной сумме вносимых денежных средств на счет организации для покупки криптовалюты [9].

Таким образом, следователь фактически выстраивает правовую и экономическую модель

конкретного дела. Он вынужден в условиях законодательного вакуума своими решениями закладывать основы для будущей судебной оценки и, как следствие, формировать определенную судебную практику. Поскольку от действий следователя по избранию даты, времени и метода оценки, а также от количества собранных доказательств напрямую зависит не только верная квалификация деяния и назначение судом наказания, но и реальная возможность полноценного возмещения вреда потерпевшему.

Авторами на основании обстоятельного изучения данной проблематики были сформулированы следующие выводы и предложения:

- о внесении изменений в положения УК РФ, предполагающие конкретизацию понятия «цифровой актив» в примечаниях к соответствующим статьям (мошенничество, кража и другие), и установив единые критерии определения размера ущерба. Видится целесообразным законодательное закрепление предписаний о том, что стоимость похищенного цифрового актива определяется на момент совершения преступного деяния по средневзвешенному курсу на крупнейших мировых биржах, доступных для резидентов Российской Федерации, что снизит дискреционные полномочия органов предварительного расследования и оспаривание методов расчета ущерба стороной защиты;
- о внесении изменений в УПК РФ, предполагающие введение новой статьи, регламентирующей специальный порядок изъятия, хранения и процессуального исследования цифровых и финансовых активов. В указанной норме должны быть закреплены правила доступа к приватным ключам, порядок наложения ареста на активы в блокчейн-адресах, механизм взаимодействия с операторами обмена и валютными биржами, а также объем полномочий специалиста;
- о дополнении содержательной части постановления Пленума Верховного Суда РФ от 21.12.2010 № 28 (ред. от 29.06.2021) «О судебной экспертизе по уголовным делам» положениями, предусматривающими особенности проведения судебных финансово-технических экспертиз по делам, связанным с цифровыми финансовыми активами, детализировав процедуру изъятия и фиксации цифровых следов, методы отслеживания транзакций (ончейн-анализ), алгоритмы определения стоимости и перечни признаваемых источников курсообразования;
- о внесении изменений в законодательство об исполнительном производстве, предусмотрев механизм принудительного взыскания и передачи цифровых финансовых активов в пользу потерпевшего. Указанные изменения потребуют создания специальных регулируемых инструментов (например, при ФССП России) для безопасного хранения и передачи цифровых приватных ключей, что кардинально скажется на степени защиты прав потерпевших.

Список литературы:

- [1] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 29.12.2025) (с изм. и доп., вступ. в силу с 20.01.2026).
- [2] Князьков А.А., Пухов А.А. Цифровые финансовые активы как предмет преступления: понятие, виды, особенности незаконного оборота // Аграрное и земельное право. — 2025. — № 3. — С. 352–355.
- [3] Тимченко В.А. Применение специальных экономических знаний при расследовании преступлений с использованием цифровых финансовых активов, цифровой валюты, криптовалюты // Вестник Нижегородского университета им. Н.И. Лобачевского. № 2. 2025. С. 153–158.
- [4] Приговор Ковровского городского суда (Владимирская область) от 25 октября 2023 г. по делу № 1 36/2023 (№ 1 463/2022) // Судебная практика. URL: <https://sudact.ru/regular/doc/yKACyWLbR9Zb/> (дата обращения: 01.02.2026).
- [5] Клевцов К.К. Международное сотрудничество в борьбе с киберпреступностью в контексте противодействия новым вызовам и угрозам // Вестник Санкт-Петербургского университета. Право. 2022. Т. 13. Вып. 3. С. 678–695.
- [6] Зуев С.В. Цифровые доказательства в уголовном процессе: проблемы интеграции // Закон. 2023. № 4. С. 102–108.
- [7] Приговор Находкинского городского суда Приморского края от 17 июля 2025 г. по делу № 1 349/2025 (25RS0010 01 2025 002835 89) // ГАС «Правосудие». URL: <https://sudact.ru/regular/doc/gUC30STLL1ov/> (дата обращения: 01.02.2026).
- [8] Филатова М.А. Проблемы установления размера и ущерба при квалификации посягательства на цифровую валюту // Уголовное право. — 2022. — № 1. — С. 65–70.
- [9] Приговор суда по делу № 1 39/2025 (1 402/2024) от 9 марта 2025 г. // Официальный ресурс судебной системы. URL: <https://sudact.ru/regular/doc/lrAFdF7Rk5Jr/?page=2®ular-txt=-биткоин> (дата обращения: 01.02.2026).

References:

[1] Code of Criminal Procedure of the Russian Federation of 18.12.2001 No. 174-FZ (as amended 29.12.2025) (with amendments and additions, entry by virtue of 20.01.2026).

[2] Knyazkov A.A., Pukhov A.A. Digital financial assets as a subject of crime: concept, types, features of illegal trafficking//Agrarian and land law. — 2025. — № 3. - S. 352-355.

[3] Timchenko V.A. Application of special economic knowledge in the investigation of crimes using digital financial assets, digital currency, cryptocurrency//Bulletin of Nizhny Novgorod University named after N.I. Lobachevsky. № 2. 2025. S. 153-158.

[4] Verdict of the Kovrov City Court (Vladimir Region) of October 25, 2023 in case No. 1 36/2023 (No. 1 463/2022)//Judicial practice. URL: <https://sudact.ru/regular/doc/yKACyWLbR9Zb/> (access date: 01.02.2026).

[5] K.K. Klevtsov. International cooperation in the fight against cybercrime in the context of coun-

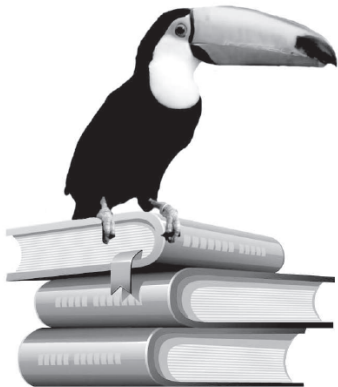
tering new challenges and threats//Bulletin of St. Petersburg University. Right. 2022. T. 13. No. 3. S. 678-695.

[6] Zuev S.V. Digital evidence in criminal proceedings: integration problems//Law. 2023. № 4. S. 102-108.

[7] Verdict of the Nakhodka City Court of Primorsky Krai dated July 17, 2025 in case No. 1 349/2025 (25RS0010 01 2025 002835 89) //GAS "Justice." URL: <https://sudact.ru/regular/doc/gUC-30STLL1ov/> (access date: 01.02.2026).

[8] Filatova M.A. Problems of establishing the amount and damage in the qualification of encroachment on digital currency//Criminal law. — 2022. — № 1. - S. 65-70.

[9] Court verdict in case No. 1 39/2025 (1 402/2024) of March 9, 2025//Official resource of the judicial system. URL: <https://sudact.ru/regular/doc/lrAFdF7Rk5Jr/?page=2®ular-txt=биткоин> (access date: 01.02.2026).



Юридическое издательство
«ЮРКОМПАНИ»

Издание учебников,
учебных и методических
пособий, монографий,
научных статей.

Профессионально.

В максимально
короткие сроки.

Размещаем
в РИНЦ, E-Library.

ЮРКОМПАНИ

www.law-books.ru