

УДК 004.728.3:332.407.4

Идентификация цифрового имущества должника (способы выявления цифрового имущества)

Калинчук Павел Дмитриевич

Аспирант,
Санкт-Петербургский государственный экономический университет,
191023, Российская Федерация, Санкт-Петербург,
наб. Канала Грибоедова, 30-32;
e-mail: pavel_kalinchuk@mail.ru

Аннотация

В статье рассматривается актуальная проблема идентификации цифрового имущества должника с целью повышения эффективности принудительного взыскания долгов и улучшения работы судебных органов. Раскрываются предпосылки возникновения данной проблемы в условиях стремительного развития информационных технологий и глобальной цифровизации экономики, а также указывается на необходимость разработки новых методологических подходов, позволяющих точно выявлять и оценивать цифровые активы должника. Методы исследования базируются на комплексном анализе современных информационных технологий, методов цифровой криминалистики и правового анализа. Применялись методы сравнительного правоведения, компьютерной экспертизы и анализа электронных следов. В качестве основных инструментов использовались программное обеспечение для мониторинга сетевой активности, алгоритмы поиска в базах данных, а также методики анализа метаданных, позволяющие установить происхождение и актуальное местоположение цифровых активов. Отдельное внимание уделялось интеграции результатов технического анализа с юридическими механизмами идентификации имущественных прав. Результаты исследования демонстрируют, что комплексное применение описанных методов позволяет существенно повысить точность выявления цифрового имущества должника. На основе проведенного анализа определены наиболее эффективные способы обнаружения активов в различных цифровых средах, включая облачные сервисы, мобильные приложения и блокчейн-системы. Выявлены ключевые проблемные области, связанные с недостаточным уровнем стандартизации электронных документов и сложностями верификации цифровых следов, что может негативно сказываться на результативности судебного разбирательства. Автором подчеркивается необходимость дальнейшей разработки законодательной базы, адаптированной к реалиям цифровой экономики, а также выработки общих стандартов для идентификации цифровых активов. Представленные в статье методологические подходы могут стать основой для создания специализированных инструментов, способных автоматизировать процесс выявления и оценки цифрового имущества на всех этапах судебного разбирательства. Таким образом, проведенное исследование вносит значительный вклад в развитие теоретических и практических аспектов правового регулирования цифровой экономики, открывая перспективы для дальнейших разработок в данной сфере.

Для цитирования в научных исследованиях

Калинчук П.Д. Идентификация цифрового имущества должника (способы выявления цифрового имущества) // Вопросы российского и международного права. 2025. Том 15. № 2А. С. 293-307.

Ключевые слова

Идентификация, цифровое имущество, должник, способы, выявление.

Введение

Деятельность по выявлению цифрового имущества должников становится все более актуальной в современном правовом поле, особенно с учетом растущего количества финансовых операций, проходящих онлайн. При возникновении задолженностей и необходимости принудительного взыскания важно понимать, какие виды активов могут быть скрыты в цифровом пространстве и какие методы могут использоваться для их обнаружения вовремя. Цифровое имущество включает в себя криптовалюты, токены, внутриигровые ценности и иные виртуальные объекты, имеющие определенную стоимость на рынке. Многие должники полагают, что цифровые активы сложно отследить из-за децентрализованных механизмов и шифрования, но на практике специальные органы и эксперты обладают разнообразными методиками выявления и анализа таких объектов. В судебной практике все чаще встречаются дела, в которых скрытые криптовалютные счета должников играют ключевую роль в решении финансовых споров до вынесения вердикта. При этом важно учитывать, что виртуальные активы могут находиться не только на криптобиржах, но и в децентрализованных кошельках, не требующих верификации личности их владельца. Следовательно, работа судебных приставов и других уполномоченных лиц по розыску такого имущества требует глубоких знаний в области блокчейна, аналитики транзакций и специфических технических инструментов для мониторинга. Успешная идентификация цифровых активов основывается, среди прочего, на сотрудничестве государственных структур с частными аналитическими фирмами, имеющими доступ к необходимым инструментам отслеживания. Особую роль играет изучение публичных реестров транзакций блокчейна, которые хоть и анонимизированы, но все же сохраняют жесткую структуру, позволяющую связывать различные адреса и кошельки друг с другом. Блокчейн-эксперты могут отследить движение криптовалют и вывести цепочку транзакций, дойдя тем самым до предположительной личности владельца. Методы, связанные со служебной информацией, включают анализ IP-адресов при взаимодействии с определенными узлами сети, изучение метаданных обращения к определенным адресам криптовалютных кошельков и многое другое. Ситуация усложняется, если должник использует миксеры или анонимные криптовалюты, вроде Monero, которые затрудняют отслеживание. Несмотря на все эти преграды, существуют технические сервисы, помогающие выявлять следы даже в такой ситуации, поскольку любой перевод, в конечном счете, может пересекаться с серверами и точками хранения лог-файлов [Черных, 2023]. Таким образом, идентификация цифрового имущества должника должна проводиться комплексно и аккуратно, чтобы охватить максимальный спектр возможных источников информации. Многие эксперты сходятся во мнении, что без тесного взаимодействия с крупными биржами, провайдерами кошельков и специализированными аналитическими платформами качественный и точный розыск затруднен.

Цифровое имущество может принимать самые различные формы, начиная от более известных криптовалют, таких как Bitcoin и Ethereum, и заканчивая токенами на основе умных контрактов, которые используются для привлечения инвестиций или представляют собой права собственности на цифровые предметы коллекционирования. Когда возникает вопрос об их идентификации, одной из первых мер становится обращение к публичным клиентам и проводникам блокчейна, которые позволяют просмотреть историю транзакций по определенному адресу. Однако задача усложняется, когда владелец старается замаскировать свои операции, разбивая переводы на многочисленные мелкие суммы или пользуясь децентрализованными площадками, где счет может быть открыт без прохождения процедуры KYC. При этом наличие соответствующего законодательного регулирования в разных юрисдикциях порождает различные правовые коллизии, которые могут препятствовать получению необходимых сведений [Петраков, 2024]. Например, если должник использует платформу, расположенную в государстве с недостаточно прозрачным регулированием, то юридический запрос о предоставлении данных может остаться без ответа. Управление такими рисками во многом зависит от налаженных международных каналов обмена информацией и правовой помощи, которые дают возможность получать данные о транзакциях и идентификационных деталях. На практике органы, ответственные за исполнение судебных решений, часто обращаются к узкопрофильным организациям, которые имеют доступ к коммерческим инструментам анализа блокчейна, способным не только строить графы связей между адресами, но и отслеживать транзакции, проходящие через анонимайзеры. Кроме того, когда речь идет об идентификации цифрового имущества, не следует забывать про различные веб-сервисы, играющие роль кошельков, обменных пунктов и бирж. Именно через них большинство пользователей взаимодействуют с криптовалютами, оставляя при этом определенный цифровой след, включая адреса электронной почты, IP-логирования и другую информацию [Переломова, 2024]. Детальный анализ таких данных способен пролить свет на то, кем является владелец конкретного счета и какова динамика его финансовых операций. Определенные методы сопоставления публичных данных о транзакциях с информацией об активности в социальных сетях также используются для более точного расследования и розыска. В некоторых случаях представители правосудия и специалисты по кибербезопасности создают фальшивые аккаунты или совершают пробные транзакции с целью выявления паттернов поведения должника в цифровом пространстве. Сочетание технических инструментов и традиционных методик расследования, таких как опрос свидетелей и анализ документальных доказательств, позволяет создать комплексную картину и эффективно установить, где именно может быть спрятано цифровое имущество. С учетом того, что каждый год появляются все новые криптовалюты и токены со своей спецификой, эксперты в данной области должны постоянно повышать квалификацию и изучать изменения в цифровом ландшафте, который подвержен быстрым трансформациям.

Материалы и методы исследования

Одним из наиболее типичных способов скрыть цифровые активы является использование личных кошельков на специально настроенных устройствах, не постоянно подключенных к сети, или на аппаратных кошельках, которые хранятся в защищенном месте. Так как в этом случае для аналитика остается меньше возможностей отследить активность по сетевым отпечаткам, подход к поиску такого имущества должен включать в себя не только техническое, но и физическое исследование. Иногда должники записывают фразы для восстановления

кошельков или пароли в бумажных или цифровых блокнотах, которые скрывают в разных местах, пытаясь избежать обнаружения [Павлова, 2022]. Тем не менее следователи и судебные приставы могут обратиться к ручному обыску помещений, при котором изымаются электронные носители, и уже после их изучения можно выйти на данные о кошельках и транзакциях. Если должник совершал операции с использованием криптобирж, эти биржи могут предоставлять отчет о проведенных сделках, особенно если у них есть локальные представительства и они подчиняются требованиям местного законодательства. Преимуществом такой стратегии является возможность отслеживать движения активов и сопоставлять историю транзакций с идентификационными данными, предоставленными при регистрации аккаунта. Однако сложность заключается в том, что многие современные биржи предоставляют клиентам расширенные возможности по повышению анонимности, в том числе путем торговли без прохождения полной процедуры подтверждения личности. Существует также много платформ в сегменте P2P-обмена, где пользователи могут договариваться напрямую без посредника. Несистематизированные платформы типа локальных обменов или частных чатов в мессенджерах затрудняют идентификацию сторон сделки, хотя и оставляют косвенные цифровые следы. Эксперты по расследованиям часто анализируют и такие косвенные данные: банковские переводы на счета третьих лиц, упоминания о сделках в переписках, сообщения на форумах, указания на участие в определенных торговых группах. Все эти составляющие постепенно формируют доказательную базу, которая впоследствии может лечь в основу судебного иска или исполнительного производства. Принимая во внимание активное развитие технологий шифрования и безопасность аппаратных кошельков, стоит отметить, что границы анонимности для владельцев цифровых активов все же достаточно подвижны. Должники, полагающие, что их невозможно обнаружить, рискуют столкнуться с целым набором инструментов, используемых современными следователями, которые работают на стыке IT и права.

Для выявления цифрового имущества должника активно применяются аналитические платформы, специализирующиеся на трассировке криптовалютных транзакций. Они используют различные алгоритмы, включая методы кластеризации, позволяющие объединить несколько адресов в один пул, если имеется статистически значимое сходство в их транзакционном поведении [Коновальчук, Письмарова, 2023]. Такие инструменты способны сопоставлять анонимизированные данные с известными «метками» – кошельками крупных рынков, бирж, мошеннических схем или законопослушных провайдеров. Ведущие компании также сотрудничают с правительством и правоохранительными органами, предоставляя отчеты об отмывании средств, финансировании противоправных действий и иных формах злоупотребления криптовалютами. В ситуации, когда необходимо найти цифровое имущество конкретного должника, эти платформы помогают выявить связи между адресами и понять, к каким сервисам они принадлежат. Благодаря глобальному характеру блокчейн-сети, даже если должник перемещает средства через границы, сохраняются записи о каждой транзакции, что дает следователям дополнительные возможности для отслеживания. Вместе с тем стоит отметить, что недостаточное понимание принципов работы сети может привести к пробелам в расследовании. Например, если специалисты неверно интерпретируют данные и не учитывают комиссии или специфику транзакций мультиподписей, это может затруднить определение истинного владельца адреса. Кроме того, многие криптовалюты, ориентированные на конфиденциальность, такие как Zcash или Dash, частично скрывают сумму переводов и адреса отправителей. В таких случаях требуется применение более сложных методик, включая анализ трафика и исследование сетевых узлов, которые обрабатывают те или иные транзакции

[Batsutsa, 2023]. Очевидно, что использование подобных инструментов требует не только технического оборудования, но и квалифицированных кадров, хорошо знакомых с процедурой судебного взыскания и законодательством в сфере цифровых активов. Эффективность работы зависит от того, насколько быстро и профессионально будут приняты меры по обеспечению доказательств. Пока должник не перевел средства в трудно отслеживаемые анонимные зоны, есть шанс застать активы в месте, где они еще могут быть идентифицированы.

Результаты и обсуждение

Еще одним методом обнаружения цифрового имущества должников становится анализ их интернет-активности. Современные браузеры и мобильные устройства оставляют значительный объем информации о посещенных сайтах, загруженных приложениях, использовании VPN или Tor. Если должник входит в свой криптовалютный кошелек через браузер, то сведения об этом могут сохраниться в истории посещений, куках или кэше. Аналогичным образом, мобильные приложения для работы с криптовалютами, трейдинговые платформы и кошельки могут оставлять следы в логах операционной системы, особенно если пользователь не предпринимает специальных мер для удаления шифрования этих данных [Трофимов, 2022]. При проведении судебных расследований нередко проводится экспертиза личных компьютеров и телефонов должника. В рамках такой экспертизы может быть обнаружен не только сам факт использования конкретного приложения, но и сведения об идентификационных цепочках, используемых для авторизации. Иногда пользователь использует один и тот же адрес электронной почты, аккаунт в соцсетях или пароль для множества сервисов, что позволяет сопоставить различную информацию и вывести на поверхность наличие цифровых активов. Впрочем, должники, обладающие определенными техническими знаниями, могут применять инструменты шифрования и стирания данных, что усложняет процесс поиска. Однако и для таких случаев существуют специальные программные комплексы, способные восстанавливать удаленную информацию или проводить глубокое исследование диска на предмет фрагментов ранее существовавших файлов. Отдельное внимание эксперты уделяют социальным сетям, где пользователи часто публично или в частных сообщениях обсуждают особенности своих финансовых инвестиций, делятся успехами на биржах или говорят о новых проектах, в которые они вкладывают средства [Мороз, 2024]. При определенном стечении обстоятельств такие разговоры могут оказаться основанием для дальнейшего детального расследования, поскольку раскрывают дополнительные детали о количестве и типе цифровых активов.

Сложность в определении принадлежности цифрового имущества нередко связана с тем, что многие криптовалюты не требуют реальной привязки к личности пользователя. Теоретически любой человек может создать неограниченное количество кошельков и адресов без дополнительных затрат, затрудняя задачу определения, какой из них контролирует должник [Брагинец, 2023]. Однако практика показывает, что если пользователь регулярно взаимодействует с сервисами обмена или выводит криптовалюту в фиатные деньги, то на каком-то этапе он оставляет цифровой отпечаток. Ведь переводы на банковские счета уже проходят через традиционную финансовую систему, которая регулируется нормами противодействия легализации доходов, полученных преступным путем. Когда судебные органы получают санкцию на проверку таких переводов, они могут проследить всю цепочку операций, от пользователя к бирже и обратно, что нередко ведет к обнаружению скрытых активов. Помимо этого, важно учитывать и человеческий фактор: некоторые должники, уверенные в своей анонимности, публично афишируют свои криптовалютные успехи, не задумываясь о

последствиях. Посты в соцсетях, участие в публичных мероприятиях, интервью в СМИ – все это может включать намеки на наличие значительных цифровых средств, что впоследствии стимулирует судебных приставов обратить пристальное внимание на данного человека. Другая ситуация может касаться тех, кто привлекает инвестиции через собственные проекты на блокчейне, выпускает токены или NFT. В таких случаях информация о кошельках, на которые поступают средства от инвесторов, обычно находится в открытых источниках, и остается только сопоставить ее с личностью эмитента или организатора. Специализированные форумы и каналы в мессенджерах могут также раскрыть определенные детали о деятельности должника, особенно если речь идет об обвинениях со стороны недовольных партнеров или клиентов. Любые упоминания о неисполнении обязательств или жалобы на мошенничество могут служить дополнительным поводом для детального расследования, в ходе которого всплывает реальный объем цифровых активов и пути их движения. Регулярно публикуемые в интернете обзоры и отчеты о деятельности крупных торговых площадок фиксируют статистику существенных транзакций, и в сочетании с добровольно или случайно обнародованными сведениями о ключах и кошельках должника эта статистика может раскрыть всю схему.

Чтобы эффективно выявлять цифровое имущество, юристы и правоохранительные органы нередко сотрудничают со специалистами в области компьютерной криминалистики. Эти эксперты проводят системный анализ электронных устройств, восстанавливая переписки, журналы активности и другие артефакты, которые могут указывать на использование конкретных кошельков. Важную роль играет анализ установленных приложений, а также поиски резервных копий ключей и файлов с конфиденциальными данными. Существует практика, когда при обыске у должника изымаются не только ноутбуки и смартфоны, но и любые носители информации: флешки, жесткие диски, облачные аккаунты. После соответствующего судебного разрешения эксперты могут расшифровать часть найденных данных и выявить следы использования криптовалют, особенно если должник использует стандартные программы или интерфейсы без дополнительного шифрования [Андреева, 2022]. В рамках развернутой экспертизы может также анализироваться сетевой трафик, если имеются логи о подключении к определенным узлам блокчейна. Отмечается, что в некоторых случаях для сокрытия цифровых активов должники пользуются виртуальными приватными серверами (VPS), расположенными за границей, а также всеми возможными методами анонимизации. Тем не менее даже эти действия не освобождают их от риска быть разоблаченными, поскольку любая операция в блокчейне так или иначе оставляет след. Свести его на нет крайне сложно, разве что прибегнуть к продвинутым методам микширования и использовать анонимные сети, но такой путь подразумевает значительные денежные и временные затраты. Кроме того, наличие подобных действий может само по себе служить косвенным доказательством, что должник пытается скрыть активы. В конечном счете, сотрудничество различных экспертов, от киберинженеров до традиционных сыщиков, позволяет сформировать комплекс мер, направленных на розыск цифровых активов и их последующую конфискацию или арест в интересах взыскателя. Также важно помнить о том, что методы и технологии не стоят на месте, и преступники постоянно ищут новые способы уйти от ответственности, создавая уникальные схемы перевода и хранения криптовалют. Поэтому развитие юридической практики и криминалистики в данной сфере является непрерывным процессом.

Существенное значение для поиска цифрового имущества имеет законодательная база, регулирующая деятельность криптобирж и других посредников. В странах, где существует четкое правовое поле для обращения криптовалют, компании обязаны проводить идентификацию клиентов и предоставлять информацию по запросу компетентных органов.

Такая практика упрощает процедуру розыска и изъятия активов, поскольку достаточно просто предоставить судебное решение и запросить у биржи данные счета и историю транзакций [Хромов, 2024]. Однако в ряде государств криптовалюта остается серой зоной, без четкой регуляции, что создает дополнительный барьер для международного сотрудничества. В подобных случаях судебные приставы могут использовать механизмы международного права, конвенции и договоры о правовой помощи, но успех операции во многом зависит от степени вовлеченности конкретной страны в глобальные процессы противодействия финансовым преступлениям. Более того, некоторые площадки работают на основе децентрализованных смарт-контрактов и совсем не хранят информацию о пользователях в централизованном виде. Это означает, что формально никто не контролирует кошельки участников кроме самих участников, а значит, законодательно воздействовать на такие платформы затруднительно. Тем не менее судебная практика постепенно развивается, и появляются случаи, когда суды признают юридическую силу тех или иных смарт-контрактов, а также накладывают санкции на разработчиков, которые способствовали отмыванию средств или содействовали уклонению от уплаты долгов. В долговых спорах усиливается тенденция к расширительному толкованию понятия имущества, включающему и цифровые активы, что дает судебным органам дополнительные основания для их розыска. При этом параллельно появляется все больше инструментов, позволяющих должникам скрывать свою активность, например использование одноразовых адресов, мультиподписей, atomic swap-площадок, где обмен криптовалютами происходит напрямую между кошельками сторон без посредников. Но, опять же, любая ошибка или невнимательность должника могут дать основание для последующего его разоблачения.

Инструментарий для обнаружения цифровых активов непрерывно совершенствуется. Появляются новые сервисы, способные автоматически анализировать огромные объемы данных о транзакциях в разных блокчейнах, выявляя подозрительные или связанные между собой адреса [Цветкова, 2023]. Дополнительно развиваются системы машинного обучения, которые по паттернам поведения могут определить принадлежность адресов одному человеку или группе лиц, даже если те пытаются маскироваться. В то же время, грамотные участники цифровой среды могут прибегать к комбинированным методам сокрытия, используя не только криптовалюты, но и токены, привязанные к реальным активам, либо переводя средства в закрытые экосистемы игровых платформ, где внутриигровая валюта или предметы могут иметь значительную стоимость. Подобные механизмы заметно усложняют работу правоохранительных органов, поскольку приходится исследовать новые ниши виртуальных экономик, где нет четкого регулирования или прозрачности. Аналогично, использование NFT, привязанных к цифровым объектам искусства или коллекционным предметам, может создавать путаницу в определении реальной стоимости и принадлежности. Определить владельца NFT можно через блокчейн, но сопоставить его с реальным человеком проблематично, если он не афишировал себя публично. Однако многие NFT-площадки все же требуют авторизации через социальные аккаунты или электронную почту, что дает надежду на возможность розыска, в случае если органы правопорядка получают доступ к соответствующим регистрационным данным. Технологические инновации идут рука об руку с усовершенствованием технического арсенала следователей, поэтому можно ожидать, что дальнейшие разработки будут еще эффективнее в идентификации даже самых сложных схем. Одновременно совершенствующиеся методы шифрования и появление новых протоколов приватности снова создают замкнутый круг, в котором стороны – следователи и должники – пытаются переиграть друг друга, используя достижения современных технологий.

Не менее важным фактором в поиске цифрового имущества остается человеческая ошибка.

Даже самый продвинутый специалист по криптовалютам может случайно оставить зацепку: быть геолокированным при доступе к кошельку, сохранить некорректно зашифрованный файл, случайно переслать приватный ключ или семя фразы в мессенджере. Такие проколы часто становятся решающими, когда дело доходит до судебных споров. Следователи изучают личную переписку в популярных приложениях для коммуникаций, обращают внимание на метаданные онлайн-файлообменников, где могут храниться резервные копии ключей, а также опрашивают родственников и знакомых должника для выяснения дополнительных деталей [Терсенов, 2024]. Сложность процесса заключается в том, что при выявлении цифровых активов необходимо доказать суду их принадлежность именно человеку, в отношении которого ведется производство. Недостаточно просто найти адрес в блокчейне и показать историю транзакций – требуется продемонстрировать связь между владельцем ключей и должником. В этом контексте часто применяются методы технологической экспертизы, допросы свидетелей, анализ переписки и банковских выписок, указывающих на факт пополнения или вывода средств с конкретного криптокошелька. Одновременно возникает проблема оценки стоимости цифровых активов, так как курс криптовалют может значительно колебаться. Для целей взыскания зачастую применяется средневзвешенный курс за определенный период, чтобы избежать претензий о том, что заемщик понес убытки из-за конвертации в неподходящий момент. Несмотря на все трудности, удачные примеры взыскания с помощью обнаружения криптоактивов уже есть в судебной практике. Эти прецеденты вносят ясность в правовое поле и подчеркивают, что скрыть цифровые активы на 100% крайне проблематично, если затрагиваются интересы правосудия и задействованы все доступные методы расследования.

Финансовые учреждения и банки тоже постепенно подключаются к механизму идентификации цифровых активов. Когда на счете у должника появляются регулярные зачисления с криптобирж, специалисты по комплаенсу могут начать внутреннее расследование, пытаясь выяснить природу таких транзакций. Если возникает подозрение на несоответствие поступающих средств декларируемой деятельности, банк может запросить дополнительные документы или даже временно заморозить счет до выяснения обстоятельств. Безусловно, это формирует дополнительный канал для органов, занимающихся взысканием долгов. Крупные банки внедряют инструменты мониторинга блокчейн-транзакций и анализаторов криптокошельков, которые автоматически сверяют данные о финансовой активности клиентов с базами находящихся в розыске адресов [Османова, 2023]. При выявлении нарушения или несоответствия банковские организации незамедлительно сигнализируют компетентным органам, что упрощает процесс розыска. Такое взаимодействие позволяет формировать более полную картину о реальном финансовом положении должника, учитывая его активы в цифровой сфере. В то же время законодатели разных стран пытаются разработать более четкие правила и требования к банкам и другим финансовым посредникам, обязывая их передавать данные о подозрительных транзакциях. Хотя конфиденциальность клиентов до определенной степени защищена законом о банковской тайне, она не является абсолютной и в случае судебных разбирательств банк обязан предоставить всю необходимую информацию. Однако это не означает, что сами банки без прямого запроса суда будут активно заниматься розыском цифровых активов. Роль банков скорее вспомогательная: они помогают фиксировать денежные потоки, связывая их с потенциальными криптовалютными операциями, что существенно облегчает задачу правоохранительных органов и судебных приставов.

Еще одним актуальным направлением является использование искусственного интеллекта для анализа пользовательской активности в сети. Алгоритмы могут изучать социальные медиаплатформы, публичные форумы, блоги, каналы мессенджеров и сопоставлять найденные

сведения с официальными данными о должнике. Если человек заявляет о своем финансовом положении одно, а в сети рассказывает или демонстрирует совсем другое, это может послужить поводом для дополнительной проверки [Нигматзянова, 2024]. Искусственный интеллект способен обрабатывать огромные объемы информации, включая тексты, изображения и даже видеоматериалы, пытаясь обнаружить намеки на использование криптовалют и иные формы цифровых активов. Иногда пользователи выкладывают скриншоты своих кошельков или транзакций, хвастаются приобретенными NFT или вступают в открытые дискуссии о новых инвестиционных возможностях. Все это может стать важным элементом доказательной базы, свидетельствующим о наличии у лица скрытых активов. Но, как и любой другой способ, анализ данных с помощью искусственного интеллекта требует правильной интерпретации итогов. Алгоритм может ошибаться, неверно сопоставлять разные аккаунты или выдавать ложноположительные результаты. Поэтому окончательные выводы в любом случае делает человек-эксперт, оценивая контекст и сопоставляя результаты с другими доказательствами. Параллельно улучшаются технологии приватности, позволяющие пользователям создавать анонимные профили, скрывать свой реальный IP-адрес и маскировать свою активность. Несмотря на это, органы правопорядка активно сотрудничают с провайдерами интернет-услуг, чтобы отслеживать подозрительные действия, связанные с криптовалютными переводами. В некоторых случаях устанавливаются фишинговые сайты или специальные ловушки, призванные побудить должника использовать свой кошелек, тем самым раскрывая его идентификационные данные.

Развитие рынка криптовалют и цифровых активов стимулирует рост количества консалтинговых компаний, специализирующихся на расследованиях, связанных с блокчейном. Они предлагают услуги комплексной проверки личности, проведение технической аналитики, оценку стоимости виртуальных активов и представительство в суде [Османова, 2023]. При этом каждая ситуация индивидуальна: в одних случаях достаточно проследить один-два перевода, чтобы выйти на главный кошелек должника, в других – приходится разворачивать масштабное расследование с привлечением экспертов из разных областей. Важно отметить, что сам по себе факт владения цифровым активом не является противозаконным; преследуются в первую очередь незаконные действия, такие как уклонение от уплаты долгов, укрывательство имущества или попытки отмыwania денег. Судебные органы, принимая решение об обращении взыскания на цифровые активы, должны учитывать специфику их хранения и обращения, а также возможность конвертации в национальную валюту. Если удастся выявить кошельки должника и подтвердить, что они действительно принадлежат ему, суд может распорядиться о блокировке транзакций, передаче прав доступа кредитору или продаже активов с торгов. Иногда возникают ситуации, когда надо учесть интересы третьих лиц, если активы хранятся на совместном кошельке или если ими управляет доверенное лицо. Все эти юридические тонкости делают процесс взыскания цифровых активов более сложным, чем традиционных средств, но при этом порождают и новые возможности, ведь скорость операций в блокчейне и их международный характер также могут сыграть на руку взыскателю, если процесс организован грамотно. Многое зависит от уровня осведомленности и подготовки всех участников процесса, включая юристов, судебных приставов, технических специалистов и самих должников.

Строгие меры, такие как арест цифровых активов, тоже находят применение на практике. Принимается судебное постановление, в рамках которого приставы пытаются ограничить должника в возможности распоряжаться найденными счетами и кошельками. Тем не менее, в отличие от традиционных банковских счетов, арестовать криптокошелек намного сложнее. Фактически, если у должника есть приватный ключ, то даже при наличии запрета он может

перевести средства в другое место, и никто не сможет это отменить, если только у суда или приставов не окажется доступа к самому ключу. Поэтому в реальности часто применяется тактика обеспечения мер: попытаться как можно раньше обнаружить и заблокировать активы, пока должник не принял контрмеры. Некоторые биржи и сервисы охотно сотрудничают с органами правопорядка и выполняют судебные постановления, замораживая активы на счетах подозреваемого или должника. Но если речь идет о децентрализованных кошельках, то процедура лишается смысла, поскольку не существует центрального органа, который мог бы принудительно заморозить средства. Именно поэтому в рамках поисковых мероприятий особый упор делается на ранний этап, когда должник еще не успел скрыть или перевести активы. Бывают и ситуации, когда цифровой актив передается в качестве залога или используется для расчета с кредиторами по взаимному соглашению, что формально может упростить процедуру взыскания. Однако каждый такой случай требует тщательного правового анализа, чтобы не нарушить интересы других кредиторов и не выйти за рамки закона. В конечном итоге арест цифровых активов – это наиболее сложный вид исполнительных действий, требующий от судебных органов глубокого понимания технической среды и тесного взаимодействия с профессионалами.

Параллельно с правоприменительными органами важную роль в выявлении цифровых активов играют посредники, такие как адвокаты и частные детективы, специализирующиеся на финансовых расследованиях. Они могут в интересах кредитора проводить негласные проверки, анализировать публичные и полупубличные реестры, вступать в контакт со свидетелями и техническими специалистами. Как правило, такие действия осуществляются на ранних стадиях, до того как дело официально попадет в суд или к приставам. Цель – собрать максимальный объем информации о финансовом положении должника, в том числе о наличии у него криптовалют и иных цифровых активов. Результаты подобных частных расследований могут затем лечь в основу судебного иска. Адвокаты, знакомые со спецификой блокчейна, помогают грамотно оформить ходатайства и запросы в суд [Черных, 2023], хотя ключевой вызов – это необходимость доказать связь между цифровым адресом и реальным человеком. В ходе судебного процесса могут быть задействованы киберэксперты в качестве специалистов, дающих заключения о том, какие операции совершались с конкретного адреса, сколько там осталось средств, может ли владелец адреса являться должником. Важным инструментом становятся показания свидетелей, которые могут рассказать о разговорах, транзакциях, инвестиционных планах должника. Все это складывается в судебный пазл, результатом которого чаще всего становится либо добровольное погашение долга должником, осознавшим неотвратимость обнаружения своих активов, либо судебное постановление о взыскании. Конечно, в юридической практике бывают случаи, когда должник все же ускользает, если ему удастся грамотно и вовремя перевести криптоактивы в анонимные сети. Но подобное требует больших усилий и рисков, поэтому не каждый готов идти на такие крайние меры, которые к тому же могут привести и к уголовной ответственности.

Особое внимание исследователей привлекает взаимодействие цифровых и традиционных активов. К примеру, если должник одновременно ведет бизнес, в котором принимает оплату в криптовалюте, есть шанс отследить соответствующие счета или транзакции через бухгалтерские документы или отчеты. Кроме того, в некоторых юрисдикциях уже существуют требования декларировать владение криптовалютами и включать их в налоговые отчеты. Невыполнение подобных правил может быть расценено как налоговое преступление, дающее дополнительное основание для производства следственных действий. Когда долг серьезна, судебные исполнители могут исследовать не только личные счета человека, но

и счета компаний, связанных с ним, подозревая, что активы выводились через юридические лица. Если в ходе проверки выяснится, что компании, контролируемые должником, имеют криптокошельки, то они тоже могут стать объектом взыскания, если будет доказано, что средства фактически принадлежат должнику, а не самой компании. В конечном счете, современные технологии усложняют процесс сокрытия активов, так как оставляют множество следов, даже если кажутся анонимными. Интеллектуальные системы анализа данных, глобальная сеть обмена информацией между финансовыми учреждениями и доступность блокчейн-экспертиз выводят на новый уровень возможности по розыску имущества. В то же время практика показывает, что при должном уровне подготовки и изобретательности некоторые должники могут весьма эффективно замести следы, поэтому каждое дело требует индивидуального подхода. Сложность процесса не отменяет того факта, что количество успешных кейсов по идентификации цифрового имущества неуклонно растет, формируя правовую базу и повышая осведомленность всех сторон о возможностях и ограничениях новых технологий.

Практика применения инструментов допроса и сбора свидетельских показаний тоже оказывается эффективной. Часто близкое окружение должника обладает какими-то знаниями о его инвестициях, пусть и поверхностными. Родственники, друзья или партнеры могут упоминать о том, что человек когда-то рассказывал о своих криптовалютных вкладах, обсуждал курсовые колебания или делился планами купить недвижимость за биткоины. Эти сведения, даже если не дают прямых доказательств, становятся отправной точкой для технического анализа. Сам должник, особенно неподготовленный, может допустить оговорки в показаниях или документах, случайно раскрывающие детали владения цифровыми кошельками. Некоторые должники пытаются хранить криптоактивы через доверенных лиц или номинальных владельцев, однако и это не гарантирует полной безопасности. Любая финансовая операция оставляет следы в виде электронных переписок, договоров, упоминаний в социальных сетях, а иногда и в офлайн документах, если, к примеру, речь идет о заключении инвестиционных соглашений. Так или иначе, комбинируя методы классической оперативной работы с техническим анализом блокчейна, следователи могут добраться до истины. Значительной поддержкой в этом вопросе становятся новые образовательные программы и тренинги для сотрудников правоохранительных органов, где они получают базовые знания о криптовалютах, о механизмах транзакций и способах сокрытия. Без такого обучения даже самый способный следователь может не распознать косвенные признаки, указывающие на наличие цифровых активов. Поэтому в последние годы наблюдается тенденция к активному повышению компетенций судебных приставов и полицейских в области IT и блокчейна, что постепенно сокращает число нераскрытых случаев.

Интерес представляет и вопрос психологического воздействия на должника. Иногда, когда подозреваемый осознает, что следствие обладает достаточным набором инструментов и сведений, он сам решает пойти на соглашение и предоставить информацию о своих активах, чтобы избежать более серьезных последствий. Открытый диалог с уполномоченными органами, заключение мирового соглашения или соглашение о реструктуризации долга могут стать для должника привлекательными вариантами, если он понимает, что все равно будет найден. С другой стороны, судебная система стремится стимулировать такую открытость, иногда предлагая льготные условия или снижая штрафные санкции за добровольную выдачу информации. Однако это применимо не во всех случаях и зависит от тяжести нарушений и общей правовой политики государства. В любом случае методы выявления цифрового имущества должника продолжают развиваться, и автоматизация ряда процессов снижает

временные затраты на проведение расследований. Когда-то поиск криптобогатств казался неразрешимой задачей, но сегодня существуют компании и государственные службы, проходящие сертификацию и обучение и могущие за короткий срок проследить целую сеть транзакций. Конечно, чем более компетентен должник в вопросах кибербезопасности, тем труднее его найти, но абсолютной анонимности достичь трудно в условиях тотальной цифровизации. Практика показывает, что любые действия в интернете оставляют какую-то зацепку, будь то IP-адрес, устройство, социальные связи или финансовые транзакции. Кроме того, судебные органы активно осваивают новые методы давления, в том числе *freezing injunctions*, которые запрещают должнику совершать какие-либо действия с активами под угрозой уголовного наказания. Это повышает шансы на то, что активы будут сохранены до момента исполнения судебного решения или внесудебного урегулирования.

Отдельно стоит сказать, что само понятие цифрового имущества расширяется по мере появления новых технологий. Если ранее это в основном относилось к криптовалютам, сегодня под это определение можно подвести токены, различные права на цифровые объекты, внутриигровые ценности многопользовательских проектов и даже уникальные идентификаторы в блокчейн-приложениях. Для должников это открывает новые возможности скрыть свои активы, однако и инструменты розыска не отстают. Некоторые государственные органы инициируют создание собственных аналитических отделов, которые будут специализироваться на отслеживании движений в различных цифровых экосистемах. Эти отделы занимаются сбором больших данных, их обработкой и выявлением аномалий, которые могут свидетельствовать о попытках укрытия имущества. Не исключено, что в будущем мы увидим специализированные международные агентства или консорциумы, работающие именно в сфере отслеживания цифровых активов, поскольку трансграничная природа блокчейна требует глобальных ответов на вызовы. Вопрос стандартизации форматов отчетности и обмена данными между странами тоже встает на повестку дня, ведь эффективный розыск возможен только при условии оперативного взаимодействия всех заинтересованных сторон. Вместе с тем не нужно забывать об этической стороне вопроса: избыточное вторжение в цифровую жизнь человека может нарушать его права на приватность, особенно если дело касается только предполагаемого долга. Поэтому правовая система должна стремиться к балансу, обеспечивая защиту интересов кредиторов и общества в целом, но при этом не ущемляя без оснований личные свободы граждан. Только комплексный, сбалансированный подход позволит развивать цивилизованную практику поиска и идентификации цифровых активов, не скатываясь в беспредел или тотальную слежку.

Заключение

Таким образом, на сегодняшний день существуют многочисленные способы выявления цифрового имущества должника, опирающиеся как на технические, так и на правовые и психологические инструменты. Исследуются блокчейн-транзакции, проводятся обыски и экспертизы электронных устройств, анализируется интернет-активность и банковская история, а в ряде случаев прибегают к помощи свидетелей или потенциальных соучастников. Хотя цифровая природа активов создает иллюзию анонимности, современные технологии вкупе с традиционными методами следственных действий показывают, что абсолютной невидимости достичь непросто. Развитие аналитических платформ, совершенствование международного правового сотрудничества и растущая компетенция правоохранителей делают процедуру розыска цифровых активов все более эффективной и целенаправленной. При должных усилиях

и знаниях со стороны юристов и приставов даже тщательные попытки скрыть криптовалюту и другие цифровые ценности могут быть раскрыты, а непрерывное совершенствование инструментов позволяет сохранять актуальность в условиях, когда технологический ландшафт постоянно меняется и адаптируется к новым вызовам. В конечном счете, кто владеет информацией – тот владеет ситуацией, и это правило как никогда верно в контексте идентификации цифрового имущества должника.

Библиография

1. Андреева Е.М. Правовая природа цифрового свидетельства // Право и экономика. 2022. № 11 (417). С. 34-38.
2. Брагинец А.Ю. Информационные объекты как имущество: опыт юрисдикций общего права и перспективы его имплементации в России // Закон. 2023. № 9. С. 111-123.
3. Коновальчук М.В., Письмарова М.А. О возможности правовой регламентации порядка изъятия и хранения цифровых прав как имущества, используемого в преступной деятельности // Вестник Самарского юридического института. 2023. № 2 (53). С. 128-133.
4. Мороз С.П. Цифровые активы как объект гражданских прав // Вестник Карагандинского университета. Серия Право. 2024. Т. 113. № 1. С. 94-105.
5. Нигматзянова Д.А. Некоторые аспекты универсального правопреемства цифровых финансовых активов в России // Нотариальный вестник. 2024. № 5. С. 27-33.
6. Османова Д.О. Цифровые активы в конкурсной массе должника // Право и цифровая экономика. 2023. № 2 (20). С. 34-42.
7. Павлова Д.А. Особенности правовой природы цифровых свидетельств // Юристы Правоведь. 2022. № 4 (103). С. 211-215.
8. Переломова О.С. Возможность и специфика раздела цифровых активов супругов и бывших супругов в некоторых зарубежных странах // Вестник Академии управления и производства. 2024. № 1. С. 311-320.
9. Петраков Н.А. Концепция цифрового имущества как объекта гражданских прав // Цивилист. 2024. № 1 (47). С. 62-69.
10. Терсенов М. А. Актуальные вопросы уголовно правовой оценки цифровых прав как предмета хищения чужого имущества // Право и управление. 2024. № 3. С. 359-363.
11. Трофимов А.А. Идентификация представителей в гражданском праве в цифровой среде // Власть Закона. 2022. № 3 (51). С. 229-236.
12. Хромов Е.В., Зябликов В.Ю. Хищение бестелесного имущества // Уголовное право. 2024. № 8 (168). С. 46-67.
13. Цветкова Е.С. Особенности оформления наследственных прав на цифровые активы // Наследственное право. 2023. № 3. С. 33-36.
14. Черных А.В. К вопросу о проблеме наследования, раздела и принудительной реализации цифровых прав // Наследственное право. 2023. № 3. С. 19-21.
15. Batsutsa V. On the question of the features of the acquisition and disposal of property rights to digital assets // Law herald. 2023. № 6. С. 153-162.

Identification of the debtor's digital assets (methods for detecting digital property)

Pavel D. Kalinchuk

Postgraduate Student,
Saint Petersburg State University of Economics,
191023, 30-32 Kanala Griboedova emb.,
Saint Petersburg, Russian Federation;
e-mail: pavel_kalinchuk@mail.ru

Abstract

The article addresses the pressing issue of identifying the debtor's digital assets in order to enhance the effectiveness of enforced debt recovery and improve the functioning of judicial authorities. The introduction reveals the prerequisites for the emergence of this problem in the context of the rapid development of information technologies and the global digitalization of the economy, while also emphasizing the need for new methodological approaches that enable the precise identification and valuation of the debtor's digital assets. The research methods are based on a comprehensive analysis of modern information technologies, digital forensic methods, and legal analysis. Comparative law, computer forensics, and electronic trace analysis methods were applied. Key tools included software for monitoring network activity, database search algorithms, and metadata analysis techniques that allow for establishing the origin and current location of digital assets. Special attention was paid to integrating the results of technical analysis with legal mechanisms for identifying property rights. The research findings demonstrate that the comprehensive application of the described methods significantly enhances the accuracy of detecting the debtor's digital assets. Based on the analysis conducted, the most effective methods for discovering assets in various digital environments—including cloud services, mobile applications, and blockchain systems—have been identified. Moreover, key problem areas were detected, such as the insufficient standardization of electronic documents and difficulties in verifying digital traces, which may negatively affect the outcomes of judicial proceedings. In the discussion, the author emphasizes the need for further development of a legislative framework adapted to the realities of the digital economy, as well as the formulation of common standards for the identification of digital assets. The methodological approaches presented in the article may serve as the basis for creating specialized tools capable of automating the process of identifying and evaluating digital property at all stages of judicial proceedings. Thus, the research makes a significant contribution to the development of both the theoretical and practical aspects of legal regulation of the digital economy, opening up prospects for further developments in this field.

For citation

Kalinchuk P.D. (2025) Identifikatsiya tsifrovogo imushchestva dolzhnika (sposoby vyyavleniya tsifrovogo imushchestva) [Identification of the debtor's digital assets (methods for detecting digital property)]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 15 (2A), pp. 293-307.

Keywords

Identification, digital property, debtor, methods, detection.

References

1. Andreeva E.M. (2022) Pravovaia priroda tsifrovogo svidetel'stva [Legal nature of digital certificates]. *Pravo i ekonomika* [Law and Economics], 11 (417), pp. 34-38.
2. Braginets A.Iu. (2023) Informatsionnye ob"ekty kak imushchestvo: opyt iurisdiktsii obshchego prava i perspektivy ego implementatsii v Rossii [Information objects as property: experience of common law jurisdictions and prospects for its implementation in Russia]. *Zakon* [Law], 9, pp. 111-123.
3. Konoval'chuk M.V., Pis'marova M.A. (2023) O vozmozhnosti pravovoi reglamentatsii poriadka iz"iatiia i khraneniia tsifrovyykh prav kak imushchestva, ispol'zuemogo v prestupnoi deiatel'nosti [On the possibility of legal regulation of the procedure for seizure and storage of digital rights as property used in criminal activities]. *Vestnik Samarskogo iuridicheskogo instituta* [Bulletin of the Samara Law Institute], 2 (53), pp. 128-133.
4. Moroz S.P. (2024) Tsifrovye aktivy kak ob"ekt grazhdanskikh prav [Digital assets as objects of civil rights]. *Vestnik*

-
- Karagandinskogo universiteta. Seriya Pravo [Bulletin of Karaganda University. Law Series], 113 (1), pp. 94-105.
5. Nigmatzianova D.A. (2024) Nekotorye aspekty universal'nogo pravopreemstva tsifrovyykh finansovykh aktivov v Rossii [Some aspects of universal succession of digital financial assets in Russia]. Notarial'nyi vĕstnik [Notarial Herald], 5, pp. 27-33.
 6. Osmanova D.O. (2023) Tsifrovye aktivy v konkursnoi masse dolzhnika [Digital assets in the debtor's bankruptcy estate]. Pravo i tsifrovaia ekonomika [Law and Digital Economy], 2 (20), pp. 34-42.
 7. Pavlova D.A. (2022) Osobennosti pravovoi prirody tsifrovyykh svidetel'stv [Features of the legal nature of digital certificates]. Iurist Pravoedĕ [Jurist Pravoved], 4 (103), pp. 211-215.
 8. Perelomova O.S. (2024) Vozmozhnost' i spetsifika razdela tsifrovyykh aktivov suprugov i byvshikh suprugov v nekotorykh zarubezhnykh stranakh [Possibility and specifics of the division of spouses' and former spouses' digital assets in some foreign countries]. Vestnik Akademii upravleniia i proizvodstva [Bulletin of the Academy of Management and Production], 1, pp. 311-320.
 9. Petrakov N.A. (2024) Kontseptsii tsifrovogo imushchestva kak ob'ekta grazhdanskikh prav [The concept of digital property as an object of civil rights]. Tsivilist [Civilist], 1 (47), pp. 62-69.
 10. Tersenov M.A. (2024) Aktual'nye voprosy ugovorno pravovoi otsenki tsifrovyykh prav kak predmeta khishcheniia chuzhogo imushchestva [Topical issues of criminal law assessment of digital rights as the subject of theft of another's property]. Pravo i upravlenie [Law and Governance], 3, pp. 359-363.
 11. Trofimov A.A. (2022) Identifikatsiia predstavitelei v grazhdanskom prave v tsifrovoi srede [Identification of representatives in civil law in the digital environment]. Vlast' Zakona [Power of Law], 3 (51), pp. 229-236.
 12. Khromov E.V., Ziablikov V.Iu. (2024) Khishchenie bestelesnogo imushchestva [Theft of intangible property]. Ugolovnoe pravo [Criminal Law], 8 (168), pp. 46-67.
 13. Tsvetkova E.S. (2023) Osobennosti oformleniia nasledstvennykh prav na tsifrovye aktivy [Features of formalizing inheritance rights to digital assets]. Nasledstvennoe pravo [Inheritance Law], 3, pp. 33-36.
 14. Chemykh A.V. (2023) K voprosu o probleme nasledovaniia, razdela i prinuditel'noi realizatsii tsifrovyykh prav [On the issue of inheritance, division and forced realization of digital rights]. Nasledstvennoe pravo [Inheritance Law], 3, pp. 19-21.
 15. Batsutsa V. (2023) On the question of the features of the acquisition and disposal of property rights to digital assets. Law herald, 6, pp. 153-162.
-