



О некоторых сложностях формирования в уголовном судопроизводстве доказательств при использовании IT-технологий для совершения преступлений

О. С. Поликарпова

Кандидат юридических наук,
старший преподаватель кафедры административной
деятельности органов внутренних дел

Санкт-Петербургский университет МВД России
198206, Россия, г. Санкт-Петербург, ул. Летчика Пилютова, 1

E-mail: zhuravlenok_os@mail.ru

Аннотация: в статье исследуются положения Федерального закона от 20 февраля 2026 г. № 38-ФЗ, которыми дополнен Уголовно-процессуальный кодекс Российской Федерации; анализируется их значение для развития института доказывания в отечественном уголовном судопроизводстве. Вместе с тем детализируются сложности, с которыми сталкиваются правоприменители в ходе расследования преступлений, совершаемых с использованием IT-технологий. Предлагается перечень методических рекомендаций, направленных на повышение эффективности реализации в правоприменительной практике внесенных Федеральным законом № 38-ФЗ дополнений в УПК РФ и нивелирование сложностей при формировании доказательств при расследовании данного вида преступлений в условиях недостаточного нормативно-правового регулирования вопросов перевода имеющих доказательственное значение при производстве по уголовным делам цифровых финансовых активов под контроль правоохранительных органов.

© Поликарпова О. С., 2026



Эта работа распространяется по лицензии CC BY 4.0.
Чтобы просмотреть копию этой лицензии, посетите
<https://creativecommons.org/licenses/by/4.0/>

Ключевые слова: ИТ-технологии, децентрализованные цифровые финансовые активы, доказывание, криптовалюта, электронная информация, цифровые носители информации

On Some Difficulties in Forming Evidence in Criminal Proceedings When IT Technologies Are Used to Commit Crimes

O. S. Polikarpova

Saint Petersburg University
of the Ministry of Internal Affairs of Russia
1, Letchika Pilyutova st., Saint Petersburg, 198206, Russia

E-mail: zhuravlenok_os@mail.ru

Abstract: *the article examines the provisions of Federal Law No. 38-FZ of February 20, 2026, which supplemented a number of provisions of the Criminal Code and the Code of Criminal Procedure of the Russian Federation, and analyzes their significance for the development of the institution of evidence in Russian criminal proceedings. At the same time, the difficulties faced by law enforcement officers during the investigation of crimes committed and committed using IT technologies are detailed. A list of methodological recommendations is proposed aimed at improving the effectiveness of the implementation in law enforcement practice of the amendments introduced by Federal Law No. 38-FZ to the Code of Criminal Procedure of the Russian Federation and leveling the difficulties in forming evidence in the investigation of this type of crime in the context of insufficient regulatory regulation of the transfer of evidentiary value in criminal proceedings of digital financial assets under control of law enforcement agencies.*

Keywords: *IT technologies, decentralized digital financial assets, proof, cryptocurrency, electronic information, digital media*

В 2023 году нами, с приведением официальных статистических данных, акцентировалось внимание на масштабах стоящей перед государством проблемы использования ИТ-технологий в преступной деятельности¹. В качестве одного из способов пресечения преступлений или установления подлежащих доказыванию обстоятельств общественно опасных деяний, инструментом совершения которых являлись ИТ-технологии, позволяющие финансировать преступную деятельность посредством применения децентрализованных цифровых финансовых активов (далее также ЦФА,

¹ Поликарпова О. С. Использование ИТ-технологий при совершении преступлений – глобальная проблема государства // Юридический вестник Дагестанского государственного университета. 2023. Т. 47, № 3. С. 156–163.

криптовалюта)², научным сообществом³, в том числе и нами⁴, указывалась проработка на законодательном уровне возможности наложения ареста на такие активы в ходе уголовного судопроизводства, что требовало отнесения их к имуществу. В свою очередь, причина выбора для финансирования преступлений виртуальных активов в виде криптовалют детально исследована А. В. Рощупкиной⁵.

По прошествии нескольких лет предложения научного сообщества были приняты во внимание на законодательном уровне и сформировали основу для Федерального закона от 20 февраля 2026 г. № 38-ФЗ⁶.

С принятием данного федерального закона децентрализованные цифровые финансовые активы были признаны имуществом для целей уголовного судопроизводства. Это исключило правовую неопределенность, обусловленную признанием цифровых валют имуществом для целей Федерального закона от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» и Федерального закона от 25 декабря 2008 г. № 273-ФЗ «О противодействии коррупции» и одновременно отсутствием возможности пресечь преступную деятельность путем наложения ареста на ЦФА в уголовном судопроизводстве и использования их в качестве средства, которое после принятия итогового решения в виде обвинительного приговора в отношении подвергнутого уголовному преследованию лица (лиц) могло подлежать конфискации либо быть применено для обеспечения заявленных стороной обвинения исковых требований. Принятием Федерального закона № 38-ФЗ законодатель расширил способы пресечения связанных с применением IT-технологий преступлений и диапазон доказывания при их расследовании.

Позволим себе высказать убежденность в том, что предусмотренные Федеральным законом № 38-ФЗ дополнения положений Уголовно-процессуального кодекса Российской Федерации⁷ (далее – УПК РФ) позволят с высокой степенью эффективности обеспечивать изъятие цифровых валют при их обнаружении в ходе производства следственных действий, предусмотренных статьями 182 и 183 УПК РФ, с последующим обращением в суд в целях наложения ареста на имущество в виде цифровых

² О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: Федер. закон от 31 июля 2020 г. № 259-ФЗ (ред. от 15.12.2025).

³ Кайгородова О. С. Решение вопроса о возможности наложения ареста на цифровые финансовые активы, цифровую валюту // Сибирские уголовно-процессуальные и криминалистические чтения. 2022. № 1 (35). С. 43–52.

⁴ Поликарпова О. С. Указ. соч. С. 161–162.

⁵ Рощупкина А. В. Роль криптовалют в финансировании терроризма // Российско-азиатский правовой журнал. 2024. № 4. С. 79–83.

⁶ О внесении изменений в статью 104.1 Уголовного кодекса Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации: Федер. закон от 20 февр. 2026 г. № 38-ФЗ. Далее по тексту – Федеральный закон № 38-ФЗ, Федеральный закон № 38-ФЗ от 20 февраля 2026 г.

⁷ Уголовно-процессуальный кодекс Российской Федерации: Федер. закон от 18 дек. 2001 г. № 174-ФЗ: принят Гос. Думой 22 нояб. 2001 г.: одобрен Советом Федерации 5 дек. 2001 г. (ред. от 09.04.2026).

финансовых активов. Однако для более оперативного внедрения в правоприменительную практику внесенных дополнений представляется необходимым разработать методические рекомендации, предусматривающие как разъяснение основных понятий, так и последовательный алгоритм действий правоприменителей из числа дознавателей (следователей) либо сотрудников органа дознания, действующих по поручению органов предварительного расследования в соответствии с пунктом 4 части 2 статьи 38 и пунктом 1.1 части 3 статьи 41 УПК РФ, в отношении цифровых активов, функционирующих на базе IT-технологий.

Следует отметить, что сложности формирования доказательств в уголовном судопроизводстве при расследовании такого вида преступлений обусловлены прежде всего спецификой децентрализованных цифровых финансовых активов, транзакция которых реализуется без участия финансово-кредитных организаций и неподконтрольна им. В этой связи при выявлении выступающих средством совершения преступления или его обнаружения криптовалют в местах их хранения, что преимущественно происходит посредством оперативно-розыскных мероприятий⁸, но может быть выявлено и при производстве ряда следственных действий, от следователя или дознавателя либо по поручению последних должностного лица органа дознания требуется оперативная реакция, вплоть до производства следственных действий в условиях неотложности, поскольку необходимо своевременно обеспечить фиксацию и надлежащую сохранность цифровых активов.

В частности, сложности вызывают технические особенности средств и способов хранения цифровых активов, что требует детального разъяснения этих особенностей правоприменителям и дифференцированного подхода в процессе документирования при расследовании преступления.

К применяемым на сегодняшний день способам хранения децентрализованных цифровых финансовых активов следует отнести:

1) онлайн-хранение – использование подключенных к информационно-телекоммуникационной сети «Интернет» специальных мобильных приложений, веб-кошельков, компьютерных программ или приложений, именуемых «браузерный кошелек», «десктопный кошелек», а равно предоставляемый при открытии счета криптовалютными биржами «биржевой кошелек». Такие способы хранения именуют еще «горячие кошельки»⁹;

2) офлайн-хранение, то есть хранение с применением холодных кошельков – аппаратных кошельков или (реже) бумажных носителей информации.

Приведенные понятия требуют разъяснения в части ключевых различий, влияющих на способ хранения и, соответственно, изъятия децентрализованных ЦФА в ходе производства по уголовным делам.

Так, во взаимосвязи с децентрализованными финансовыми активами, кошельком именуют «приложение для хранения криптовалюты», позволяющее «пользователям получать доступ к цифровым активам, переводить их на другие адреса,

⁸ Михайленко Н. В., Рудин А. В. Арест криптовалют и цифровых финансовых активов: вызовы правового регулирования // Вестник Московского университета МВД России. 2024. № 5. С. 112.

⁹ Там же. С. 111.

использовать для оплаты и иных целей»¹⁰. Коллективом авторов учебного пособия «Работа с цифровыми виртуальными активами» выделяются аппаратные кошельки, представляющие отдельные устройства, конструктивно сходные с флеш-накопителем и наиболее безопасные, в силу того что доступ к ним возможен исключительно при осведомленности о пароле доступа и физическом наличии самого материального носителя информации. К браузерным кошелькам ученые относят встроенные в браузер программы в виде расширения. Desktopные кошельки формируются в виде устанавливаемого на компьютер (ноутбук) специального приложения, а отнесенный к наименее надежным способам хранения криптовалют биржевой кошелек выдается пользователям при открытии счета на биржах торговли децентрализованными ЦФА¹¹.

Кроме того, важно знать, что криптовалюта может быть зафиксирована в виде совокупности электронных данных, содержащихся не в информационной системе, а на материальном носителе, таком как персональный компьютер, ноутбук, сервер. Аппаратные кошельки могут быть сохранены и как сами финансовые активы в виде совокупности электронных данных, и как коды доступа к базам IT-технологий с функционирующими децентрализованными цифровыми активами, обмен которых либо их перевод производятся с материального носителя.

Очевидно, что такая вариативность способов хранения криптовалют требует для их обнаружения специальных знаний.

Вместе с тем необходимо учитывать, что в целях эффективного производства обыска (выемки) для достижения результата в виде сформированного допустимого доказательства в ходе расследования уголовного дела, а также в целях недопущения сокрытия цифровых активов подвергнутым уголовному преследованию лицом или третьими лицами следователь (дознатель), а равно должностное лицо органа дознания, уполномоченное соответствующим поручением на производство указанных следственных действий, могут не только изъять материальный носитель, содержащий ЦФА в виде совокупности электронных данных либо коды доступа к таким активам, но и перевести эти активы на адрес-идентификатор либо аппаратный кошелек правоохранительных органов, позволяющие обеспечить их сохранность¹². Иными словами, следователь (дознатель) или уполномоченное должностное лицо органа дознания вправе по результатам произведенного следственного действия, предусмотренного статьями 182 или 183 УПК РФ, прибегнуть к одной из указанных мер либо реализовать обе для обеспечения сохранности криптовалют в целях их последующего признания вещественными доказательствами по уголовному делу с возможностью наложения ареста на имущество в качестве меры процессуального принуждения для обеспечения на перспективу исполнения приговора в части исковых требований.

¹⁰ Работа с цифровыми виртуальными активами: учеб. пособие / [С. Е. Волков, И. В. Гайдашко, В. А. Голобоков и др.]. М.: Спутник+, 2022. С. 40.

¹¹ Там же.

¹² О внесении изменений в статью 104-1 Уголовного кодекса Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации: законопроект № 902782-8. URL: <https://sozd.duma.gov.ru/bill/902782-8>.

Ввиду изложенного, при производстве в ходе обыска (выемки) изъятия материальных носителей, содержащих ЦФА или коды доступа к ним, а равно переводе таких активов на адрес-идентификатор требование части 2 статьи 164.1 УПК РФ об участии специалиста является обязательным и нашло свое отражение в положениях новой статьи УПК РФ – 164.2. Именно специалист, чью компетентность, согласно части 2 статьи 168 УПК РФ и с учетом части 1 статьи 223 УПК РФ, устанавливает следователь (дознатель) или уполномоченное соответствующим поручением должностное лицо органа дознания, не только производит непосредственные действия, направленные на соблюдение правильного и последовательного копирования, отключения и прочих технических мероприятий в целях изъятия электронных носителей информации, но и определяет выбор необходимых мер для обеспечения сохранности электронных средств платежа с учетом особенностей примененных при совершении конкретного преступления IT-технологий и децентрализованных цифровых финансовых активов. Детальнее роль специалиста для повышения эффективности деятельности по изъятию и наложению ареста на криптовалюту раскрыта Г. П. Осиповым¹³. Соответственно, при производстве следственного действия с участием специалиста компетенции последнего надо подтверждать, например, приложением к протоколу копии диплома об образовании или свидетельства о повышении квалификации.

Кроме того, не следует забывать и о правильном выборе фактического доказательства по уголовному делу при признании его вещественным путем вынесения постановления (ч. 2 ст. 81, ч. 1 ст. 81.1 УПК РФ), поскольку материальный носитель не всегда может являться средством обнаружения преступления или установления подлежащих доказыванию обстоятельств. В ряде случаев именно цифровая информация несет в себе доказательственное значение, что нами аргументировалось ранее¹⁴.

Необходимость ареста цифровой валюты может возникнуть также в ситуации, когда до этого в рамках следственных действий она не изымалась, а в ходе допроса участника уголовного судопроизводства выяснилось, что хранение цифровой валюты организовано на горячем кошельке криптобиржи. Соответственно, при получении значимых для расследуемого уголовного дела данных о способе и месте хранения цифровых финансовых активов следователю (дознателю) необходимо не только ходатайствовать перед судом о наложении в порядке, предусмотренном положениями статьи 115 УПК РФ, ареста на имущество в виде ЦФА, включая материальные носители с наличием таких активов или кодов доступа к базам IT-технологий, на которых имеющие доказательственное значение активы функционируют, но и учитывать при разработке плана следственных и процессуальных действий по уголовному делу возможное наличие кодов доступа к цифровым финансовым активам у третьих лиц

¹³ Осипов Г. П. Изъятие и арест криптовалюты: роль и участие специалиста // Вестник Университета прокуратуры Российской Федерации. 2025. № 3 (107). С. 93–100.

¹⁴ Андреева Е. Ю., Поликарпова О. С. К вопросу о процессуальной форме закрепления информации на электронных носителях в качестве доказательства по уголовному делу // Уголовное судопроизводство России и зарубежных государств: проблемы и перспективы развития: материалы Междунар. науч.-практ. конф. (Санкт-Петербург, 2 декабря 2022 г.). СПб.: СПбУ МВД России, 2022. С. 23–28.

или резервного способа восстановления прав на эти активы при условии владения информацией об открытых или частных ключах доступа к месту их хранения. Поэтому наиболее эффективным способом обеспечить сохранность децентрализованных цифровых финансовых активов до завершения производства по уголовному делу, в том числе и на судебных стадиях, является их перевод на адрес-идентификатор либо аппаратный кошелек правоохранительных органов, что с момента фактического расширения полномочий должностных лиц органов предварительного расследования, обусловленного введением в УПК РФ статьи 164.2, представляется возможным.

Однако конструкция нормы – статьи 164.2 УПК РФ – не конкретная, поскольку ее содержанием не детализирован фактический порядок перевода цифровых финансовых активов на адрес-идентификатор, что неизбежно создаст сложности для правоприменителей. Неопределенность обусловлена прежде всего тем обстоятельством, что на сегодняшний день проработка на законодательном уровне порядка перевода криптовалют под контроль правоохранительных органов не завершена, в связи с чем доступ к информации о поступившей на адрес-идентификатор криптовалюты имеет ограниченный круг субъектов правоохранительных органов. В частности, такой доступ организован для налоговых органов¹⁵. Поэтому усилия по проработке на законодательном уровне непосредственного порядка перевода цифровой валюты на адрес-идентификатор, обеспечивающий учет и хранение изъятых цифровых финансовых активов, на которые решением суда, вынесенным с учетом требований статей 115 и 165 УПК РФ, наложен арест, должны быть продолжены и в основу разрабатываемых нормативных правовых актов Правительства РФ должны быть заложены рекомендации Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ)¹⁶, направленные на расширение контроля над операторами информационных систем, в которых происходит обращение децентрализованных цифровых финансовых активов.

До завершения указанной работы на законодательном уровне, которая, нужно надеяться, нивелирует для правоприменителей сохранившиеся сложности в фактической реализации следственных и процессуальных действий с учетом внесенных Федеральным законом № 38-ФЗ в положения УПК РФ дополнений, правоприменителям из числа следователей (дознавателей), в целях обеспечения сохранности кодов доступа к базам IT-технологий, на которых децентрализованные цифровые активы функционируют, или данных о месте и способах их хранения, до обращения в суд с ходатайством о наложении ареста на имущество следует принять дополнительные меры для надежной защиты цифровой информации. Помещением изъятого в ходе обыска (выемки) цифрового оборудования – системных блоков (моноблоков) персональных компьютеров, ноутбуков, смартфонов и/или прочего оборудования с функци-

¹⁵ Об обязанности лица, осуществляющего майнинг цифровой валюты (в том числе участника майнинг-пула), по предоставлению информации о получении цифровой валюты в случае выпуска (получения) цифровой валюты в результате майнинга цифровой валюты, а также об адресе-идентификаторе, включая адрес-идентификатор майнинг-пула: постановление Правительства Рос. Федерации от 1 нояб. 2024 г. № 1466.

¹⁶ Рекомендации ФАТФ: Международные стандарты по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения. URL: www.fatf-gafi.org/recommendations.html.

ональной возможностью приема сигналов передачи данных – в камеру хранения вещественных доказательств обеспечить сохранность значимой для расследования преступления информации не всегда возможно. Современные IT-технологии, при наличии у третьих лиц доступа к аккаунту подвергнутого уголовному преследованию лица, позволяют заблокировать либо стереть все данные с телефона, компьютера, ноутбука, прочих технических устройств уже после их фактического изъятия в ходе производства обыска (выемки) у подозреваемого (обвиняемого) по уголовному делу. Для предупреждения таких ситуаций и реального наложения ареста на ЦФА, хранение кодов доступа к которым обеспечено в памяти персональных компьютеров, ноутбуков, смартфонов и прочего оборудования с возможностью приема сигналов передачи данных, необходимо применять средства, исключающие возможность эти цифровые данные удаленно заблокировать или стереть.

Еще в 1836 году ученым-физиком Майклом Фарадеем было изобретено простое устройство с широким спектром применения, позволяющее блокировать проникновение электромагнитных волн и препятствующее в том числе прохождению цифровых сигналов, которое сам ученый назвал «клетка Фарадея». Детально сущность и функциональное предназначение этого устройства разъяснены О. Ю. Быковой и Э. В. Мухметзяновым¹⁷. Данное изобретение широко применяется современной наукой и адаптировано под решение разных задач по защите от электромагнитных волн. Изменились и формы «клетки»: сегодня изготавливаются кейсы, коробки разных форматов, чехлы, помещение цифровых устройств в которые влечет блокировку направляемых на них электромагнитных сигналов, что, в свою очередь, исключает возможность блокировки или удаления цифровых данных, содержащихся в памяти этих устройств.

Наиболее простым и доступным «инструментом» создания клетки Фарадея является пищевая фольга, которой достаточно в несколько слоев надежно обернуть подлежащий защите от электромагнитных волн и высокочастотных цифровых сигналов предмет. Следует лишь исключить наличие щелей в созданной из фольги упаковке и непосредственное соприкосновение изолируемой цифровой техники с фольгой, что может быть обеспечено бумажной или тканевой прослойкой. Важно отметить, что при извлечении цифрового устройства из защитного поля, обеспечиваемого применением клетки Фарадея либо приспособления, близкого по функциональному предназначению, даже на непродолжительный период времени содержащаяся на цифровом носителе информация может быть дистанционно заблокирована или удалена. Именно для сохранения данных на изъятых цифровых устройствах их осмотр необходимо осуществлять в помещении, где обеспечена защита от электромагнитных волн и высокочастотных цифровых сигналов, предварительно закрыв входную дверь в это помещение и исключив ее открытие до завершения осмотра. По окончании следственного действия, произведенного в описанном частью 3 статьи 177 УПК РФ порядке, нужно вновь обеспечить надежную изоляцию осмотренного цифрового устройства от электромагнитных волн.

Такой способ защиты данных от блокировки или удаления из памяти цифрового оборудования – системных блоков (моноблоков) персональных компьютеров,

¹⁷ Быкова О. Ю., Мухаметзянов Э. В. Майкл Фарадей. Клетка Фарадея. Принцип действия и применение // NovaUm.Ru. 2018. № 12. С. 3–5.

ноутбуков, смартфонов и прочего оборудования с возможностью приема сигналов передачи данных – позволит следователю (дознавателю) обеспечить исполнение решения суда о наложении ареста на цифровые финансовые активы и эффективно использовать их в процессе доказывания по уголовному делу, а на перспективу – для обеспечения решения суда в части исковых требований.

Библиографический список

Андреева Е. Ю., Поликарпова О. С. К вопросу о процессуальной форме закрепления информации на электронных носителях в качестве доказательства по уголовному делу // Уголовное судопроизводство России и зарубежных государств: проблемы и перспективы развития: материалы Междунар. науч.-практ. конф. (Санкт-Петербург, 2 декабря 2022 г.). СПб.: СПбУ МВД России, 2022. С. 23–28.

Быкова О. Ю., Мухаметзянов Э. В. Майкл Фарадей. Клетка Фарадея. Принцип действия и применение // NovaUm.Ru. 2018. № 12. С. 3–5.

Кайгородова О. С. Решение вопроса о возможности наложения ареста на цифровые финансовые активы, цифровую валюту // Сибирские уголовно-процессуальные и криминалистические чтения. 2022. № 1 (35). С. 43–52. DOI: 10.17150/2411-6122.2022.1.43-52.

Михайленко Н. В., Рудин А. В. Арест криптовалют и цифровых финансовых активов: вызовы правового регулирования // Вестник Московского университета МВД России. 2024. № 5. С. 109–114. DOI: 10.24412/2073-0454-2024-5-109-114.

Осипов Г. П. Изъятие и арест криптовалюты: роль и участие специалиста // Вестник Университета прокуратуры Российской Федерации. 2025. № 3 (107). С. 93–100.

Поликарпова О. С. Использование IT-технологий при совершении преступлений – глобальная проблема государства // Юридический вестник Дагестанского государственного университета. 2023. Т. 47, № 3. С. 156–163. DOI: 10.21779/2224-0241-2023-47-3-156-163.

Работа с цифровыми виртуальными активами: учеб. пособие / [В. А. Голобоков, И. В. Гайдамашко, С. Е. Волков и др.]. М.: Спутник+, 2022.

Рощупкина А. В. Роль криптовалют в финансировании терроризма // Российско-азиатский правовой журнал. 2024. № 4. С. 79–83. DOI: 10.14258/ralj(2024)4.12.

Информация для цитирования

Ex jure

Поликарпова О. С. О некоторых сложностях формирования в уголовном судопроизводстве доказательств при использовании IT-технологий для совершения преступлений // Ex jure. 2026. № 3. С. 141–149. DOI: 10.17072/2619-0648-2026-3-141-149. EDN SSPLZG

Polikarpova O. S. On Some Difficulties in Forming Evidence in Criminal Proceedings When IT Technologies Are Used to Commit Crimes. *Ex jure*. 2026. № 3. Pp. 141–149. DOI: 10.17072/2619-0648-2026-3-141-149. EDN SSPLZG