Право

УДК 343.7:004.056.5

О.М. КАБАНОВ
(olegkabanov06@mail.ru)
Санкт-Петербургский государственный экономический университет

ХИЩЕНИЕ КРИПТОАКТИВОВ ЧЕРЕЗ ФИШИНГ ПРИВАТНЫХ КЛЮЧЕЙ: УГОЛОВНО-ПРАВОВОЙ АНАЛИЗ*

Анализируются уголовно-правовые проблемы квалификации хищений криптоактивов, совершаемых через фишинг приватных ключей и иных данных доступа к криптовалютным кошелькам. Обосновывается, что криптоактив следует рассматривать как имущественную ценность. Проводится разграничение кражи, мошенничества, мошенничества в сфере компьютерной информации, неправомерного доступа и использования вредоносных программ. Предлагается прикладной алгоритм квалификации.

Ключевые слова: *криптоактив, цифровая валюта, фишинг, приватный ключ, хищение, неправомерный доступ, судебная практика.*

Хищение криптоактивов через фишинг приватных ключей относится к числу преступлений против собственности, совершаемых с использованием информационно-телекоммуникационных технологий. Практическая сложность таких деяний состоит в том, что внешний результат обычно выглядит одинаково: потерпевший утрачивает контроль над цифровой валютой, а актив переводится на адрес, контролируемый виновным или связанными с ним лицами. Однако юридический механизм утраты может быть различным. В одном случае потерпевший сам переводит криптовалюту под влиянием обмана, в другом – только раскрывает seed-фразу или пароль, после чего перевод выполняет преступник, в третьем – доступ к кошельку получается с помощью вредоносной программы или неправомерного доступа к устройству.

Именно поэтому при квалификации нельзя ограничиваться общим указанием на «криптомошенничество» или «киберпреступление». Для уголовного права решающее значение имеет не способ общения преступника с потерпевшим в сети Интернет, а то, каким образом произошло изъятие имущественной ценности: путем добровольного распоряжения потерпевшего, путем тайного списания актива, через вмешательство в компьютерную информацию либо с использованием вредоносного инструмента. От этого зависит выбор между ст. 158, 159, 159.6, 272, 273 и при наличии соответствующих признаков ст. 174.1 УК РФ [9].

Актуальность темы подтверждается криминальной статистикой. По данным МВД России, по итогам 2025 г. количество преступлений, совершенных с использованием информационно-телекоммуникационных технологий, снизилось на 11,8%, однако дистанционные кражи и мошенничества сохраняют значительную распространенность [2]. Следовательно, уменьшение общего числа зарегистрированных ИТ-преступлений не снимает проблемы их квалификации. Напротив, по мере усложнения схем вывода цифровых активов возрастает значение точного описания события преступления, фиксации цифровых следов и разграничения смежных составов.

Согласно Федеральному закону от 31.07.2020 № 259-ФЗ, «цифровой валютой признается совокупность электронных данных (цифрового кода или обозначения), содержащихся в информационной системе, которые предлагаются и (или) могут быть приняты в качестве средства платежа… и (или) в качестве инвестиций» [6]. Долгое время в правоприменении сохранялась неопределенность: цифровая валюта не является вещью в традиционном смысле, но имеет экономическую ценность и может выступать объектом фактического контроля. Федеральный закон от 20.02.2026 № 38-ФЗ закрепил признание цифровой валюты имуществом для целей применения уголовного и уголовно-процессуального законодательства [3].

* Работа выполнена под руководством Тиминой Т.Н., кандидата юридических наук, доцент кафедры уголовного права и уголовного процесса ФГБОУ ВО «СПбГЭУ».

© Кабанов О.М., 2026

Данная позиция согласуется с выводами Конституционного Суда РФ, который указал на необходимость судебной защиты имущественных требований, связанных с цифровой валютой, при условии подтверждения законности ее получения и использования [8]. Для уголовно-правовой квалификации это принципиально важно: если цифровая валюта признается имущественной ценностью, ее неправомерное изъятие может образовывать хищение. Следовательно, предметом преступного посягательства является не seed-фраза или приватный ключ как последовательность символов, а криптоактив, контроль над которым обеспечивается этими данными.

Фишинг представляет собой форму обмана, направленного на получение данных доступа к криптовалютному кошельку. На практике он выражается в создании поддельных сайтов бирж и кошельков, рассылке сообщений от имени службы безопасности, имитации уведомлений о блокировке аккаунта, предложении «подтвердить» кошелек, подключить его к фальшивому сервису или пройти повторную авторизацию. Потерпевший, доверяя внешнему сходству сайта или сообщения с официальным сервисом, вводит seed-фразу, приватный ключ, пароль, одноразовый код либо подписывает транзакцию, смысла которой фактически не понимает.

Необходимо различать два близких, но юридически разных варианта. Первый вариант: потерпевший сам переводит криптовалюту на адрес виновного, полагая, что оплачивает услугу, участвует в инвестиционном проекте, защищает активы от блокировки или выполняет иное законное действие. Здесь волевое распоряжение имуществом исходит от потерпевшего, хотя оно сформировано обманом. Такой механизм ближе к мошенничеству, предусмотренному ст. 159 УК РФ. Второй вариант: потерпевший только сообщает данные доступа или вводит их на фишинговом ресурсе, а списание цифровой валюты происходит без его осознанного распоряжения. В этом случае обман используется не как способ получения имущества от потерпевшего, а как способ облегчения тайного доступа к нему; поэтому основной квалификационный вариант связан с кражей по ст. 158 УК РФ.

Такой подход соответствует разъяснениям Пленума Верховного Суда РФ. Постановление от 30.11.2017 № 48 разграничивает обычное мошенничество и мошенничество в сфере компьютерной информации, подчеркивая, что для применения ст. 159.6 УК РФ необходимо воздействие на компьютерную информацию либо вмешательство в функционирование средств ее хранения, обработки или передачи [3]. Само использование сайта, мессенджера, электронной почты или криптовалютного приложения еще не делает деяние мошенничеством в сфере компьютерной информации. Интернет в таком случае может быть только средой общения с потерпевшим, а не самостоятельным способом воздействия на компьютерную информацию.

Постановление Пленума Верховного Суда РФ от 16.06.2026 № 19 также имеет непосредственное значение для рассматриваемой темы. В нем указано, что к предмету кражи, грабежа, разбоя и иного хищения относится не только вещь, но и иное имущество, включая цифровую валюту [4]. В отношении криптоактивов моментом окончания хищения обычно следует считать фактическое выбытие цифровой валюты из-под контроля потерпевшего, если после этого виновный получает реальную возможность перевести, обменять, раздробить или скрыть актив.

Отдельного внимания требует ст. 159.6 УК РФ. Ее применение возможно, когда хищение осуществляется путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации. Например, если виновный не просто убеждает потерпевшего передать данные доступа, а изменяет программную логику сервиса, подменяет реквизиты транзакции, вмешивается в работу учетной записи или автоматически инициирует перевод через вредоносный скрипт, вопрос о ст. 159.6 УК РФ становится более обоснованным. Если же потерпевший добровольно вводит данные на поддельной странице, а затем преступник вручную использует их для вывода средств, квалификация по ст. 159.6 УК РФ не должна применяться автоматически.

Ст. 272 и 273 УК РФ применяются не вместо составов хищения, а при наличии самостоятельных признаков неправомерного доступа к компьютерной информации или использования вредоносных программ [9]. Так, если виновный получает доступ к устройству потерпевшего, облачному храни-

© Кабанов О.М., 2026

лищу, электронной почте, аккаунту биржи или файлу с seed-фразой без согласия владельца, содеянное может дополнительно содержать признаки ст. 272 УК РФ. Если же для похищения ключей используется программа, специально предназначенная для копирования данных, подмены адреса кошелька, перехвата буфера обмена или удаленного управления устройством, возможна квалификация по ст. 273 УК РФ. В таких случаях хищение криптоактива и преступления в сфере компьютерной информации образуют совокупность.

Практически важным является вопрос о легализации похищенной цифровой валюты. После вывода криптоактивов виновные часто переводят их через цепочку адресов, используют обменники, P2P-сделки, биржи, миксеры, дробление сумм и перевод через третьих лиц. Однако не каждое последующее перемещение похищенного актива образует состав ст. 174.1 УК РФ. Для квалификации легализации необходимо доказать не просто распоряжение похищенным, а цель придания правомерного вида владению, пользованию или распоряжению имуществом, приобретенным преступным путем. Таким образом, обычный перевод с одного адреса на другой для сокрытия следов хищения сам по себе не всегда достаточен; значение имеют фиктивные сделки, вывод в легальный оборот, оформление через подставных лиц и обмен на фиатные денежные средства с созданием видимости законного происхождения [9].

В судебной практике уже встречаются дела, подтверждающие имущественный характер криптовалюты. Показательным является дело о хищении Ethereum в Санкт-Петербурге: потерпевший приобрел 7000 ETH и хранил их на криптокошельке, а расследование велось по статьям о краже и неправомерном доступе к компьютерной информации. Суд допустил арест криптовалюты, что свидетельствует о возможности применения уголовно-процессуальных мер к цифровым активам [10]. Такие дела демонстрируют общий вектор: криптоактив рассматривается как имущественная ценность, а действия виновных оцениваются через конкретный механизм изъятия.

Для прикладной квалификации фишингового хищения криптоактивов целесообразно использовать последовательный алгоритм. На первом этапе устанавливается принадлежность цифровой валюты потерпевшему: история приобретения актива, биржевые выписки, сведения о переводах, скриншоты личного кабинета, данные кошелька, переписка, документы об оплате и иные подтверждения законного владения.

На втором этапе фиксируется событие выбытия: адрес отправителя, адрес получателя, хеш транзакции, время, сумма, сеть, комиссия и последующее движение средств.

На третьем этапе определяется роль потерпевшего: совершал ли он перевод сам, подписывал ли транзакцию, передавал ли только данные доступа и понимал ли фактический смысл совершаемого действия.

На четвертом этапе анализируется способ действий виновного. Если основной способ состоял в обмане потерпевшего и получении от него добровольного имущественного распоряжения, базовой является квалификация по ст. 159 УК РФ. Если обман использовался только для получения доступа, а цифровая валюта списана без осознанного распоряжения потерпевшего, более обоснованной является квалификация по ст. 158 УК РФ. Если хищение совершено посредством воздействия на компьютерную информацию, рассматривается ст. 159.6 УК РФ. Если дополнительно имел место неправомерный доступ к охраняемой компьютерной информации либо использование вредоносной программы, оценивается вопрос о совокупности со ст. 272 или 273 УК РФ.

На пятом этапе определяется размер ущерба. В делах о цифровой валюте это особенно важно, поскольку стоимость актива может существенно меняться. Для целей квалификации целесообразно устанавливать стоимость на момент фактического выбытия имущества из владения потерпевшего, используя данные бирж, специализированных сервисов, заключение специалиста или эксперта. При этом необходимо указывать не только количество криптовалюты, но и ее рублевый эквивалент, метод расчета, источник курса и дату определения стоимости. Без этого затрудняется оценка размера ущерба и применение квалифицирующих признаков.

Доказывание по таким делам имеет специфику. Блокчейн-адрес сам по себе не содержит персональных данных владельца, поэтому принадлежность адреса конкретному лицу устанавливается по совокупности доказательств. Значение имеют данные централизованных бирж, сведения о прохож-

© Кабанов О.М., 2026

дении идентификации, IP-адреса, устройства входа, номера телефонов, электронная почта, банковские карты, переписка с потерпевшим, логи сайтов, доменные данные фишингового ресурса, сведения хостинг-провайдера и результаты осмотра электронных носителей. Чем раньше зафиксированы цифровые следы, тем выше вероятность установить связь между фишинговой страницей, получением данных доступа и последующим выводом актива.

Таким образом, квалификация хищений криптоактивов через фишинг приватных ключей определяется не самим фактом использования сети Интернет, а конкретным механизмом утраты контроля над цифровой валютой. Если потерпевший сам распоряжается активом под влиянием обмана, применяются правила о мошенничестве. Если он лишь раскрывает данные доступа, а списание осуществляется тайно и без его осознанного распоряжения, содеянное ближе к краже. При воздействии на компьютерную информацию, неправомерном доступе или применении вредоносного программного обеспечения возникает вопрос о ст. 159.6, 272 и 273 УК РФ. Основные трудности сохраняются не столько в признании цифровой валюты имуществом, сколько в доказывании принадлежности актива, способа его изъятия, размера ущерба и связи между действиями виновного и наступившими последствиями.

Литература

1. Долгиева М.М. Противодействие криптопреступности уголовно-правовыми средствами // Актуальные проблемы российского права. 2023. Т. 18. № 2(147). С. 171–177.

2. МВД России. Статистические сведения о состоянии преступности в 2025 году // МВД Медиа. 2026. 29 янв. [Электронный ресурс]. URL: https://mvdmedia.ru/news/official/statisticheskie-svedeniya-o-sostoyanii-prestupnosti-v-2025-godu/ (дата обращения: 23.06.2026).

3. О внесении изменений в статью 104.1 Уголовного кодекса Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 20.02.2026 № 38-ФЗ // Официальный интернет-портал правовой информации. 2026. [Электронный ресурс]. URL: http://publication.pravo.gov.ru/document/0001202602200059 (дата обращения: 23.06.2026).

4. О судебной практике по делам о краже, грабеже и разбое: Постановление Пленума Верховного Суда РФ от 27.12.2002 № 29 (ред. от 16.06.2026) // Российская газета. 2026. 23 июня. № 134.

5. О судебной практике по делам о мошенничестве, присвоении и растрате: Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 (ред. от 15.12.2022) // Российская газета. 2017. № 280.

6. О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 31.07.2020 № 259-ФЗ // Собрание законодательства РФ. 2020. № 31. Ст. 5018.

7. Перов В.А. Квалификация преступлений, совершаемых с использованием криптовалюты: дисс. ... канд. юрид. наук. М., 2023.

8. Постановление Конституционного Суда Российской Федерации от 20.01.2026 № 2-П по делу о проверке конституционности части 6 статьи 14 Федерального закона «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» // Официальный интернет-портал правовой информации. 2026. [Электронный ресурс]. URL: http://publication.pravo.gov.ru/document/0001202601210002 (дата обращения: 23.06.2026).

9. Российская Федерация. Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 № 63-ФЗ // Собрание законодательства РФ. 1996. № 25. Ст. 2954.

10. Суд наложил арест на украденную с чужого кошелька криптовалюту // Российское агентство правовой и судебной информации. 2022. 5 апр. [Электронный ресурс]. URL: https://rapsinews.ru/judicial_news/20220405/307855115.html (дата обращения: 23.06.2026).

OLEG KABANOV
Saint-Petersburg State Economic University

PLUNDERING OF CRYPTOASSETS BY PHISING OF PRIVATE KEYS: CRIMINAL LAW ANALYSIS

The criminal and law issues of qualification of plundering of cryptoassets, committed by phishing of private keys and other access data to cryptocurrency wallet, are analyzed. It is substantiated that cryptoasset should be considered as the property value. The distinction between theft; fraud; fraud, involving computer information; the unauthorized access and the use of malicious programs is examined. The applied algorithm of qualification is suggested.

Keywords: *cryptoasset, digital currency, phishing, private key, plundering, unauthorized access, legal precedents.*

© Кабанов О.М., 2026