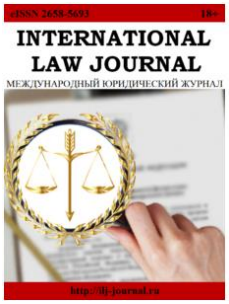
ISSN 2658-5693
https://ilj-journal.ru



Научно-исследовательский журнал «International Law Journal»
https://ilj-journal.ru
2025, Том 8, № 7 / 2025, Vol. 8, Iss. 7 https://ilj-journal.ru/archives/category/publications
Научная статья / Original article
Шифр научной специальности: 5.1.4. Уголовно-правовые науки (юридические науки)
УДК 347.77

Проблемы квалификации мошенничества с использованием электронных средств платежа: теория и правоприменительная практика

[1] Мастюкова И.И., [1] Роженцева А.П., [1] Гаврильченко К.Р., [1] Соболинская Е.М., [1] Хаджиматов В.А.,
[1] Дальневосточный федеральный университет

Аннотация: *в условиях стремительного развития цифровых технологий и их внедрения в финансовую сферу электронные средства платежа стали неотъемлемой частью экономических отношений, обеспечивая удобство операций. Однако это привело к росту преступлений, связанных с хищениями, и вызвало трудности в уголовно-правовой квалификации таких деяний. Актуальность исследования обусловлена противоречиями в разграничении мошенничества с использованием электронных средств платежа (ст. 159.3 УК РФ), кражи с банковского счета (п. «г» ч. 3 ст. 158 УК РФ) и мошенничества в сфере компьютерной информации (ст. 159.6 УК РФ). Цель работы – анализ теоретических и практических проблем квалификации, выявление причин нестабильности судебной практики и разработка рекомендаций по ее унификации. Исследование выявило ключевые проблемы конкуренции норм: нечеткие критерии разграничения обмана и тайного хищения, особенно при социальной инженерии (фишинг, вишинг). Анализ практики показал, что суды часто квалифицируют схожие деяния по-разным статьям, что нарушает принцип правовой определенности. Обнаружены типичные сценарии, такие как использование чужих карт в бесконтактных платежах или переводы под обманом, приводящие к противоречивым решениям.*

Ключевые слова: *мошенничество, электронные средства платежа, квалификация, УК РФ, судебная практика*

Для цитирования: Мастюкова И.И., Роженцева А.П., Гаврильченко К.Р., Соболинская Е.М., Хаджиматов В.А. Проблемы квалификации мошенничества с использованием электронных средств платежа: теория и правоприменительная практика // International Law Journal. 2025. Том 8. № 7. С. 6 – 11.

Поступила в редакцию: 8 июля 2025 г.; Одобрена после рецензирования: 10 сентября 2025 г.; Принята к публикации: 5 ноября 2025 г.

Problems of qualification of fraud using electronic payment means: theory and law enforcement practice

[1] Mastyukova I.I., [1] Rozhentseva A.P., [1] Gavrilchenko K.R., [1] Sobolinskaya E.M., [1] Khadzhimatov V.A.,
[1] Far East Federal University

Abstract: *with the rapid development of digital technologies and their introduction into the financial sector, electronic payment means have become an integral part of economic relations, providing convenience of transactions. However, this has led to an increase in crimes related to embezzlement and has caused difficulties in the criminal law qualification of such acts. The relevance of the study is due to contradictions in distinguishing fraud using electronic payment means (Art. 159.3 of the Criminal Code of the Russian Federation), theft from a*

bank account (subpara. "g," para. 3, Art. 158 of the Criminal Code of the Russian Federation), and fraud in the sphere of computer information (Art. 159.6 of the Criminal Code of the Russian Federation). The purpose of the work is to analyze theoretical and practical problems of qualification, to identify the causes of instability in judicial practice, and to develop recommendations for its unification. The study revealed key problems of competition between norms: vague criteria for distinguishing deception from covert theft, especially in cases of social engineering (phishing, vishing). An analysis of practice showed that courts often classify similar acts under different articles, which undermines the principle of legal certainty. Typical scenarios have been identified, such as using someone else's cards in contactless payments or transfers made under deception, leading to contradictory decisions.

Keywords: *fraud, electronic payment means, qualification, Criminal Code of the Russian Federation, judicial practice*

For citation: Mastyukova I.I., Rozhentseva A.P., Gavrilchenko K.R., Sobolinskaya E.M., Khadzhimatov V.A. Problems of qualification of fraud using electronic payment means: theory and law enforcement practice. International Law Journal. 2025. 8 (7). P. 6 – 11.

The article was submitted: July 8, 2025; Approved after reviewing: September 10, 2025; Accepted for publication: November 5, 2025.

Введение

Стремительное развитие цифровых технологий и их повсеместное внедрение во все сферы общественной жизни, включая финансовую, кардинальным образом изменили парадигму экономических отношений. Электронные средства платежа, от классических банковских карт до систем быстрых платежей и электронных кошельков, стали неотъемлемой частью повседневности, обеспечивая удобство, скорость и доступность финансовых операций. Однако эта технологическая трансформация имеет и оборотную сторону, порождая новые вызовы для системы уголовной юстиции. Рост числа преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, опережает темпы адаптации законодательства и правоприменительной практики, что создает серьезные проблемы в области защиты прав граждан и организаций от преступных посягательств [12]. Особую остроту приобретает вопрос правильной уголовно-правовой квалификации хищений, совершаемых с использованием электронных средств платежа, поскольку от этого напрямую зависит справедливость наказания, эффективность расследования и возможность возмещения причиненного ущерба.

Актуальность настоящего исследования обусловлена наличием системных трудностей, с которыми сталкиваются правоприменители при разграничении смежных составов преступлений, в частности, мошенничества с использованием электронных средств платежа (ст. 159.3 УК РФ), кражи, совершенной с банковского счета (п. «г» ч. 3 ст. 158 УК РФ), и мошенничества в сфере компьютерной информации (ст. 159.6 УК РФ). Сложность заключается в многообразии способов совершения таких преступлений, которые часто сочетают в себе элементы обмана, тайного хищения и неправомерного воздействия на компьютерную информацию. Развитие методов социальной инженерии, таких как фишинг и вишинг, когда потерпевший под влиянием обмана сам совершает действия по переводу денежных средств, еще более усложняет определение объективной стороны преступления и направленности умысла виновного [3]. Отсутствие единых и четких критериев квалификации в судебной практике приводит к вынесению противоречивых решений, нарушению принципа законности и формированию у преступников чувства безнаказанности, что требует глубокого теоретического анализа и выработки практических рекомендаций.

Материалы и методы исследований

Теоретическую и нормативную основу исследования составили положения Конституции Российской Федерации, нормы уголовного и уголовно-процессуального законодательства, в частности, Уголовный кодекс Российской Федерации (далее – УК РФ) и Уголовно-процессуальный кодекс Российской Федерации. Особое внимание было уделено анализу федеральных законов, регулирующих правоотношения в финансовой сфере, таких как Федеральный закон «О национальной платежной системе» [9]. Важнейшим источником для понимания правоприменительных тенденций послужили разъяснения высших судебных инстанций, прежде всего Постановления Пленума Верховного Суда Российской Федерации, в том числе Постановление от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате». Кроме того, в работе использованы научные труды, монографии и публикации ведущих отечественных ученых-юристов в области уголовного права и криминологии, посвященные проблемам

ISSN 2658-5693
https://ilj-journal.ru

квалификации киберпреступлений и хищений в цифровой среде [5]. В качестве материалов исследования также были использованы обезличенные судебные акты (приговоры, апелляционные и кассационные определения) судов общей юрисдикции различных регионов Российской Федерации, опубликованные в открытых источниках и справочно-правовых системах.

Результаты и обсуждения

Центральной проблемой правоприменения является конкуренция уголовно-правовых норм, предусмотренных ст. 159.3 УК РФ и п. «г» ч. 3 ст. 158 УК РФ. Изначально, в своей первой редакции, статья 159.3 УК РФ была ориентирована на ситуации, когда виновный использовал чужую или поддельную банковскую карту для оплаты товаров или услуг, вводя в заблуждение уполномоченного работника торговой точки относительно своей правомочности на совершение операции. В данном случае обман был очевиден и направлен на конкретное физическое лицо [1]. Однако с распространением бесконтактных платежей и онлайн-операций, где прямое взаимодействие с человеком отсутствует, возник вопрос о природе такого хищения.

Верховный Суд Российской Федерации в Постановлении Пленума от 30 ноября 2017 г. № 48 попытался разрешить эту коллизию, указав, что хищение денежных средств путем использования похищенной или поддельной кредитной, расчетной или иной платежной карты для оплаты товаров или услуг в торговых точках следует квалифицировать как мошенничество. Если же карта используется для снятия наличных через банкомат, то деяние квалифицируется как кража. Эта позиция основывалась на том, что в первом случае виновный обманывает сотрудника магазина, а во втором – тайно похищает деньги у банка, поскольку банкомат не может быть введен в заблуждение [8]. Однако данное разъяснение быстро устарело ввиду технологического прогресса.

Ситуация кардинально изменилась с введением в действие Федерального закона от 23 апреля 2018 г. № 111-ФЗ, который изложил ст. 159.3 УК РФ в новой редакции и ввел квалифицирующий признак кражи – с банковского счета, а равно в отношении электронных денежных средств (п. «г» ч. 3 ст. 158 УК РФ). Ключевым моментом стало то, что из диспозиции ст. 159.3 УК РФ было исключено указание на обман уполномоченного работника. Теперь состав преступления охватывает мошенничество с использованием электронных средств платежа в целом [15]. Это породило новую волну дискуссий. Например, как квалифицировать оплату покупки в магазине чужой картой с функцией бесконтактной оплаты на сумму, не требующую ввода ПИН-кода? С одной стороны, виновный использует чужое электронное средство платежа, что подпадает под признаки ст. 159.3 УК РФ. С другой стороны, хищение происходит тайно от потерпевшего, а работник магазина или система самообслуживания не обманываются в юридически значимом смысле, а лишь обрабатывают технический сигнал от карты. Судебная практика пошла по пути квалификации таких действий как кражи по п. «г» ч. 3 ст. 158 УК РФ, мотивируя это тайным характером изъятия денежных средств со счета потерпевшего [6].

Еще более сложной является конкуренция между ст. 159.3 УК РФ и ст. 159.6 УК РФ (мошенничество в сфере компьютерной информации). Основной водораздел между этими составами, по замыслу законодателя, проходит по способу совершения преступления. Для ст. 159.6 УК РФ характерен ввод, удаление, блокирование, модификация компьютерной информации либо иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. В свою очередь, ст. 159.3 УК РФ предполагает использование уже существующего, легитимного по своей форме электронного средства платежа, но неправомочным лицом [11].

На практике это разграничение оказывается крайне размытым. Классическим примером являются преступления, совершаемые с использованием методов социальной инженерии. Когда мошенник, представляясь сотрудником банка, убеждает потерпевшего сообщить ему реквизиты карты, коды из СМС-сообщений, а затем с их помощью переводит денежные средства на свои счета через онлайн-банк, возникает вопрос о квалификации. С одной стороны, виновный использует электронное средство платежа (реквизиты карты и доступ к онлайн-банку), что указывает на ст. 159.3 УК РФ. С другой стороны, он вводит в систему аутентификационные данные (коды), которые по своей сути являются компьютерной информацией, и тем самым осуществляет неправомерный доступ и воздействие на информационную систему банка. Многие суды квалифицируют такие действия как кражу по п. «г» ч. 3 ст. 158 УК РФ, считая, что обман используется лишь как способ получения доступа к счету, а само хищение является тайным. Другие же видят в этом признаки мошенничества в сфере компьютерной информации (ст. 159.6 УК РФ), поскольку виновный вводит в систему банка информацию (коды подтверждения), легитимирующую операцию в глазах автоматизированной системы [4].

ISSN 2658-5693
https://ilj-journal.ru

Проблема усугубляется, когда потерпевший под влиянием обмана самостоятельно совершает перевод денежных средств через мобильное приложение. В этом случае отсутствует тайность хищения (потерпевший видит, что делает) и формально отсутствует неправомерный ввод информации самим преступником. Воля потерпевшего при совершении транзакции порочна, так как сформировалась под влиянием обмана. В таких ситуациях правоприменитель часто обращается к общей норме о мошенничестве (ст. 159 УК РФ), что, однако, не в полной мере отражает специфику использования высоких технологий при совершении преступления [10]. Отсутствие единого подхода приводит к тому, что одно и то же деяние в разных регионах может быть квалифицировано по трем, а то и четырем разным статьям УК РФ, что недопустимо с точки зрения принципа правовой определенности.

Анализ судебной практики показывает, что суды при выборе нормы часто ориентируются не столько на тонкости объективной стороны, сколько на сложившиеся в регионе «традиции» квалификации и степень очевидности того или иного признака. Если доминирующим элементом является использование вредоносного программного обеспечения, взлом аккаунта, то деяние с большей вероятностью будет квалифицировано по ст. 159.6 УК РФ. Если же акцент делается на обмане конкретного лица с целью получения данных его карты, суды могут склоняться к квалификации по ст. 159 или ст. 159.3 УК РФ.

Особую сложность представляет доказывание умысла и определение субъекта преступления в организованных группах, которые специализируются на данном виде хищений. Часто такие группы имеют сложную иерархическую структуру: одни участники («прозвонщики») осуществляют звонки и обманывают потерпевших, другие («технари») обеспечивают техническую сторону (подмена номеров, создание фишинговых сайтов), третьи («обнальщики» или «дропы») занимаются выводом и легализацией похищенных средств через цепочку подставных счетов и лиц [7]. Привлечение к ответственности организаторов и всех звеньев такой цепи требует значительных усилий от правоохранительных органов и глубокого понимания технологий, используемых преступниками.

Законодатель, пытаясь решить проблему, периодически вносит изменения в уголовный закон, однако эти изменения зачастую носят «точечный» характер и не решают системных проблем конкуренции норм. Представляется, что наличие в УК РФ нескольких специальных составов мошенничества (ст. 159.1-159.6) излишне усложняет правоприменение [2]. Возможно, более эффективным был бы возврат к единой статье о мошенничестве, в которой использование информационных технологий, электронных средств платежа или причинение значительного ущерба рассматривались бы как квалифицирующие признаки.

Судебная практика также нуждается в дополнительных, более детализированных разъяснениях со стороны Верховного Суда РФ. Необходимо выработать четкие критерии разграничения кражи с банковского счета и различных видов мошенничества в цифровой среде. Ключевым критерием должно стать не то, кто является «обманутым» (человек или машина), а то, каким образом виновный получает доступ к денежным средствам потерпевшего. Если доступ получен тайно (например, путем несанкционированного копирования данных карты) и хищение происходит без ведома владельца, это кража. Если же виновный путем обмана или злоупотребления доверием побуждает самого потерпевшего совершить перевод либо получает от него аутентификационные данные, которые затем использует для имитации законной операции, деяние должно рассматриваться как мошенничество [13].

Дальнейшее разграничение между видами мошенничества должно строиться на специфике способа. Если обман направлен исключительно на получение реквизитов и их последующее использование в стандартных платежных процедурах, это должно охватываться составом ст. 159.3 УК РФ. Если же способ хищения включает в себя активное вмешательство в работу программного обеспечения, модификацию компьютерной информации (например, создание фишингового сайта, который перехватывает данные, или использование вредоносных программ), то применению подлежит ст. 159.6 УК РФ. Такой подход позволил бы унифицировать практику и обеспечить более точную и справедливую квалификацию содеянного.

Выводы

Проведенное исследование демонстрирует наличие серьезных системных проблем в сфере уголовно-правовой квалификации хищений, совершаемых с использованием электронных средств платежа. Основная сложность заключается в объективной трудности разграничения смежных составов преступлений, предусмотренных статьями 158, 159.3 и 159.6 Уголовного кодекса Российской Федерации. Существующие диспозиции этих норм имеют пересекающиеся признаки, а многообразие и постоянная трансформация способов совершения преступлений, особенно с применением социальной инженерии, создают ситуации, не имеющие однозначного толкования ни в доктрине, ни в судебной практике. Отсутствие четких и универсальных критериев разграничения приводит к формированию противоречивой и нестабильной

правоприменительной практики, что нарушает принцип правовой определенности и снижает эффективность уголовно-правовой защиты имущественных прав граждан.

Для преодоления сложившейся ситуации требуется комплексный подход, включающий как совершенствование законодательства, так и выработку единых правоприменительных стандартов. Представляется целесообразным пересмотреть действующую конструкцию уголовного закона в части множественности специальных составов мошенничества, рассмотрев возможность их унификации в рамках единой статьи с развернутой системой квалифицирующих признаков. Наряду с этим, назрела острая необходимость в подготовке нового, детализированного постановления Пленума Верховного Суда Российской Федерации, которое бы дало исчерпывающие разъяснения по вопросам квалификации киберхищений с учетом современных технологий и преступных схем. Только системная работа по гармонизации законодательства и судебной практики позволит обеспечить адекватную реакцию государства на новые криминальные угрозы в цифровой эпохе и повысить уровень защищенности граждан от мошеннических посягательств.

Список источников

1. Диденко К.В., Бочарникова Л.Н. К вопросу о квалификации мошенничества с использованием электронных средств платежа // Вопросы российского и международного права. 2020. Т. 10. № 4-1. С. 76 – 82.

2. Абызова Е.Р. Проблемы квалификации мошенничества, совершаемые с использованием электронных средств платежа // Евразийский юридический журнал. 2024. № 8 (195). С. 260 – 262.

3. Куликов А.В., Гуц Е.А. Проблема квалификации мошенничества с использованием электронных средств платежа // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2020. № 1 (59). С. 21 – 25.

4. Кулумбегова М.В. Отграничение мошенничества с использованием электронных средств платежа от кражи с банковского счета, а равно в отношении электронных денежных средств // Юридическая наука: история и современность. 2022. № 3. С. 140 – 146.

5. Думанская Е.И., Меньшикова А.Г. Мошенничество с использованием электронных средств платежа: трансформация в законе и практике // Правопорядок: история, теория, практика. 2022. № 3 (34). С. 50 – 57.

6. Перетолчин А.П. Отдельные аспекты квалификации мошенничества с использованием электронных средств платежа в контексте обновленной позиции Верховного Суда Российской Федерации // Российский следователь. 2021. № 7. С. 56 – 60.

7. Суслова А.Е., Яковлева Ю.С., Качурова Е.С. Проблемы квалификации мошенничества с использованием электронных средств платежа // Человек. Социум. Общество. 2024. № 10. С. 138 – 142.

8. Лещенко В.П. Квалификация мошенничества с использованием электронного средства платежа и его отграничение от смежных составов преступлений // Ius Publicum et Privatum. 2024. № 3 (27). С. 88 – 94.

9. Григорьева Н.В., Саморока В.А., Угольникова Н.В. Ситуативная квалификация мошенничества с использованием электронных средств платежа // Криминологический журнал. 2023. № 3. С. 57 – 60.

10. Аминов И.Р., Трусов С.В. Проблемы квалификации мошенничества с использованием электронных средств платежа // Право и управление. 2024. № 8. С. 379 – 382.

11. Найденов Д.В., Фоменко И.В. Использование электронных платёжных средств как способ совершения мошенничества: проблемы толкования и правоприменения // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. 2022. № 11 (150). С. 137 – 141.

12. Христюк А.А., Асатрян Х.А. Проблемы уголовно-правовой регламентации и квалификации деяний, совершаемых с использованием электронных средств платежа // Академический юридический журнал. 2023. Т. 24. № 1 (91). С. 71 – 79.

13. Беляков А.В., Бондаренко С.В. Проблемы квалификации хищений с использованием электронных средств платежа // Наука XXI века: актуальные направления развития. 2022. № 2-2. С. 97 – 101.

14. Меньшикова А.Г., Кочкурова Е.А. К вопросу о характеристике предмета мошенничества с использованием электронных средств платежа // Правопорядок: история, теория, практика. 2023. № 2 (37). С. 73 – 80.

15. Гурина К.А. Электронные средства платежа как предмет мошенничества в уголовном праве // Всероссийский научный журнал "Вопросы права". 2025. № 3. С. 92 – 94.

References

1. Didenko K.V., Bocharnikova L.N. On the issue of qualification of fraud using electronic means of payment. Issues of Russian and International Law. 2020. Vol. 10. No. 4-1. P. 76 – 82.
2. Abyzova E.R. Problems of qualification of fraud committed using electronic means of payment. Eurasian Law Journal. 2024. No. 8 (195). P. 260 – 262.
3. Kulikov A.V., Guts E.A. Problems of qualification of fraud using electronic means of payment. Bulletin of the Kaliningrad branch of the St. Petersburg University of the Ministry of Internal Affairs of Russia. 2020. No. 1 (59). P. 21 – 25.
4. Kulumbegova M.V. Distinction between fraud using electronic means of payment and theft from a bank account, as well as in relation to electronic money Legal science: history and modernity. 2022. No. 3. P. 140 – 146.
5. Dumanskaya E.I., Menshikova A.G. Fraud using electronic means of payment: transformation in law and practice. Law and order: history, theory, practice. 2022. No. 3 (34). P. 50 – 57.
6. Peretolchin A.P. Certain aspects of qualification of fraud using electronic means of payment in the context of the updated position of the Supreme Court of the Russian Federation. Russian investigator. 2021. No. 7. P. 56 – 60.
7. Suslova A.E., Yakovleva Yu.S., Kachurova E.S. Problems of qualification of fraud using electronic means of payment. Man. Society. Society. 2024. No. 10. P. 138 – 142.
8. Leshchenko V.P. Qualification of fraud using an electronic means of payment and its distinction from related crimes. Ius Publicum et Privatum. 2024. No. 3 (27). P. 88 – 94.
9. Grigorieva N.V., Samoroka V.A., Ugolnikova N.V. Situational qualification of fraud using electronic means of payment. Criminological journal. 2023. No. 3. P. 57 – 60.
10. Aminov I.R., Trusov S.V. Problems of qualification of fraud using electronic means of payment. Law and Management. 2024. No. 8. P. 379 – 382.
11. Naidenov D.V., Fomenko I.V. Use of electronic payment instruments as a method of committing fraud: problems of interpretation and law enforcement. Science and education: economy and economics; entrepreneurship; law and management. 2022. No. 11 (150). P. 137 – 141.
12. Khrystyuk A.A., Asatryan H.A. Problems of criminal-legal regulation and qualification of acts committed with the use of electronic means of payment. Academic Law Journal. 2023. Vol. 24. No. 1 (91). P. 71 – 79.
13. Belyakov A.V., Bondarenko S.V. Problems of qualification of thefts using electronic means of payment. Science of the XXI century: current directions of development. 2022. No. 2-2. P. 97 – 101.
14. Menshikova A.G., Kochkurova E.A. On the Characteristics of the Subject of Fraud Using Electronic Means of Payment. Law and Order: History, Theory, Practice. 2023. No. 2 (37). P. 73 – 80.
15. Gurina K.A. Electronic Means of Payment as a Subject of Fraud in Criminal Law. All-Russian Scientific Journal "Questions of Law". 2025. No. 3. P. 92 – 94.

Информация об авторах

Мастюкова И.И., специалист-эксперт, Дальневосточный федеральный университет, mastuykova.ii@students.dvfu.ru

Роженцева А.П., специалист-эксперт, Дальневосточный федеральный университет, rozhentceva.ap@students.dvfu.ru

Гаврильченко К.Р., специалист-эксперт, Дальневосточный федеральный университет, Gavrilchenko @dvfu.ru

Соболинская Е.М., специалист-эксперт, Дальневосточный федеральный университет, sobolinskaya.em@dvfu.ru

Хаджиматов В.А., преподаватель, Юридическая школа, Дальневосточный федеральный университет, Khadzhimatov@dvfu.ru