Проблемы применения уголовного законодательства об ответственности за мошенничество с использованием электронных средств платежа

Ембулаева Наталья Юрьевна
кандидат юридических наук, доцент, заведующий кафедрой теории и истории государства и права, Кубанский государственный аграрный университет имени И. Т. Трубилина, embulaeva.n@kubsau.ru
Окороков Виктор Иванович
Студент, Кубанский государственный аграрный университет имени И. Т. Трубилина, vitya.okorokov.06@mail.ru

В статье рассматриваются актуальные вопросы квалификации мошенничества, совершаемого с использованием электронных средств платежа (ст. 159.3 УК РФ). Анализ охватывает динамику изменений уголовного закона; одновременно исследуются проблемы разграничения смежных составов преступлений, предусмотренных статьями 159, 159.3 и 158 УК РФ. Особое внимание сосредоточено на толковании понятия «электронное средство платежа» и на определении момента окончания преступления - именно эти элементы вызывают наиболее заметные затруднения в правоприменении.
Ключевые слова: электронные средства платежа, мошенничество, информационные технологии, киберпреступность, кража, банковские карты, уголовное законодательство.

На фоне всеобщей цифровизации экономических отношений и широкого распространения удаленных финансовых сервисов традиционная преступность меняет привычные формы. Мошенничество, ответственность за которое установлена статьёй 159 Уголовного кодекса Российской Федерации, все заметнее смещается от непосредственного контакта с потерпевшим к более сложным, многоступенчатым моделям, где используются информационно-телекоммуникационные сети и электронные средства платежа.

Согласно статистическим данным правоохранительные органы фиксируют устойчивое увеличение количества зарегистрированных хищений денежных средств граждан, совершаемых посредством обмана или злоупотребления доверием в цифровой среде. Одновременно для этой категории деяний по-прежнему характерна высокая латентность, то есть часть потерпевших не обращается в правоохранительные органы, поскольку размер причиненного ущерба представляется им незначительным либо отсутствует доверие к результативности расследования. На этом фоне все острее обозначается необходимость в углубленном научном анализе вопросов квалификации деяний, связанных с использованием электронных средств платежа.

Несмотря на внесение законодателем ряда изменений в диспозиции статей главы 21 УК РФ, включая введение специальных составов (в частности, ст. 159.3 УК РФ, практика применения которой впоследствии была скорректирована Верховным Судом РФ), правоприменительная практика сталкивается с комплексом доктринальных и процессуальных противоречий. Остаются дискуссионными вопросы разграничения мошенничества с использованием платежных карт от кражи с банковского счета (п. «г» ч. 3 ст. 158 УК РФ), определения момента окончания преступления при бесконтактных транзакциях, а также установления субъективной стороны виновного при использовании методов социальной инженерии [7].

Цель настоящего исследования состоит в выявлении и систематизации проблем применения уголовного законодательства об ответственности за мошенничество с использованием электронных средств платежа, а также в разработке предложений по их устранению.

Достижение указанной цели предполагает решение ряда задач:

– необходимо исследовать изменения статьи 159.3 УК РФ и установить, в какой степени её действующая редакция соответствует криминологической реальности цифровых посягательств на собственность;

– требуется проанализировать критерии разграничения мошенничества с использованием электронных средств платежа и смежных составов преступлений, прежде всего кражи с банковского счёта и мошенничества в сфере компьютерной информации, выявив причины устойчивой конкуренции норм, именно в этой зоне наиболее заметны квалификационные затруднения;

– следует исследовать правоприменительную практику, включая как количественные параметры судимости и назначаемых наказаний, так и качественные характеристики конкретных судебных решений, с тем чтобы установить реальные, а не декларируемые законом критерии квалификации;

– необходимо определить институциональные и организационные факторы, препятствующие единообразному применению статьи 159.3 УК РФ;

– на основе полученных результатов надлежит сформулировать комплекс предложений по совершенствованию уголовного законодательства и практики его применения, в их взаимосвязи и с учетом выявленных проблем.

Научная новизна исследования определяется тем, что проблема применения статьи 159.3 УК РФ рассматривается не изолированно, а в контексте более широкого процесса трансформации уголовно-правовой охраны собственности под влиянием цифровизации. Авторский подход не сводится к фиксации противоречий судебной практики. Напротив, предпринимается попытка объяснить устойчивость этих противоречий через призму институциональных факторов и структурных особенностей самой уголовно-правовой нормы, такой ракурс позволяет выйти за пределы традиционной догматической критики и предложить решения, с учетом не только содержания закона, но и условий его применения.

Стремительное внедрение цифровых технологий в сферу имущественных отношений, наблюдаемое в последнее десятилетие, обусловило фундаментальную трансформацию не только способов распоряжения материальными благами, но и самого криминологического облика посягательств на собственность. Безналичные расчеты, дистанционное банковское обслуживание, системы мгновенных переводов и платёжные приложения стали повседневной практикой миллионы граждан; их использование перестало восприниматься как технологическая экзотика. Но обратной стороной этой технологической революции стало формирование качественно новых форм преступного поведения, в них традиционные криминальные схемы получают цифровую оболочку, а электронные средства платежа выступают инструментом завладения чужим имуществом [4].

От «классического» мошенничества, предусмотренного ст. 159 УК РФ, данный состав отличается адресатом обмана. В первой ситуации обман или злоупотребление доверием обращены непосредственно к человеку, тогда как здесь используется технический посредник - банковская карта, система дистанционного банковского обслуживания, мобильное приложение, электронный кошелёк, платёжный терминал либо иное устройство, обеспечивающее инициирование перевода денежных средств в системе безналичных расчётов. Именно электронное средство платежа, как представляется, выступает тем орудием, посредством которого виновный преодолевает защитный механизм имущественных благ и получает доступ к счетам потерпевшего.

Содержание данного преступления состоит в ином механизме воздействия: виновный вводит в заблуждение либо злоупотребляет доверием субъекта, уполномоченного санкционировать платёжную операцию. Таким субъектом может выступать работник кредитной организации, сотрудник торговой точки или сам владелец счёта - круг лиц здесь определяется характером конкретной транзакции. При этом внешне операция нередко воспринимается как правомерная, поскольку списание денежных средств производится по установленным правилам платёжной системы, а согласие на транзакцию формально наличествует; однако такое согласие получено обманным путём либо основано на ложной уверенности в законности происходящего.

Ключевая юридическая особенность состава связана с его разграничением с кражей (ст. 158 УК РФ). Если лицо скрытно использует чужую банковскую карту, не вступая во взаимодействие с уполномоченными лицами и не прибегая к обману, содеянное подлежит квалификации как кража; мошенничество же имеет место в тех случаях, когда электронное средство платежа применяется именно как инструмент обмана или злоупотребления доверием, а не как техническое средство тайного изъятия имущества. По этой причине мошенничество с использованием электронных средств платежа образует самостоятельный вид хищения. В его конструкции цифровые платежные технологии выступают не просто каналом перевода денежных средств, а обязательным элементом преступного способа - именно он придаёт деянию повышенную общественную опасность и требует специальной уголовно-правовой оценки. Российский законодатель отреагировал на эти вызовы в 2012 году, дополнив Уголовный кодекс Российской Федерации статьей 159.3. Эта норма установила ответственность за мошенничество с использованием платежных карт, а позднее – за мошенничество с использованием электронных средств платежа; однако её дальнейшая эволюция оказалась существенно более сложной. Неоднократное реформирование статьи, введение в 2018 году самостоятельной ответственности за кражу с банковского счета (пункт «г» части третьей статьи 158 УК РФ), признавшее необоснованным применение разъяснений Пленума, данных применительно к ранее действовавшей редакции статьи 159.3 УК РФ, фактически дезавуировало сложившуюся практику квалификации, но не предложило определенной альтернативы, в результате нижестоящие суды оказались перед необходимостью самостоятельно разрешать вопрос между мошенничеством и кражей, руководствуясь не столько буквой закона, сколько интуитивными представлениями о справедливости [5].

В условиях цифровой трансформации имущественных отношений российский законодатель обособил в самостоятельный состав деяния, посягающие на собственность с применением электронных платёжных инструментов. В ст. 159.3 УК РФ закреплена ответственность за хищение чужого имущества или приобретение права на него путём обмана или злоупотребления доверием, совершённое с использованием электронных средств платежа. Вместе с тем юридическая природа данного состава продолжает вызывать дискуссии: он соединяет признаки традиционного мошенничества и специфику, обусловленную технологическим способом совершения преступления - именно это сочетание затрудняет его однозначное теоретическое объяснение. Эта двойственность и определяет научную полемику вокруг нормы.

Содержание рассматриваемого деяния раскрывается через особую функцию платежного инструмента. Виновный использует электронное средство платежа не просто как канал перевода денег, а как средство воздействия на волю лица, санкционирующего платёж. Обман или злоупотребление доверием может адресоваться работнику кредитной организации, сотруднику торговой точки или самому владельцу счёта; в результате потерпевший либо уполномоченное лицо добровольно, но под влиянием заблуждения, инициирует перевод средств в пользу виновного. Именно этот волевой акт, хотя и дефектный по своему содержанию, отличает мошенничество от кражи, при которой изъятие имущества совершается помимо воли собственника.

Специфика объективной стороны проявляется в опосредованном характере взаимодействия участников. Виновный и потерпевший могут находиться на значительном расстоянии, а транзакция осуществляется автоматически, без непосредственного контакта сторон. Подобная конструкция порождает сложности при установлении момента окончания преступления, а также при его разграничении со смежными составами, прежде всего с кражей с банковского счёта (п. «г» ч. 3 ст. 158 УК РФ) и мошенничеством в сфере компьютерной информации (ст. 159.6 УК РФ). Ключевой критерий здесь, характер обмана, если он направлен на человека, санкционирующего операцию, налицо мошенничество, если же доступ к счету обеспечивается путём преодоления технической защиты, содеянное квалифицируется как кража.

Мошенничество с использованием электронных средств платежа представляет собой сложный по своей юридической конструкции состав. В нём технологический способ совершения преступления неразрывно связан с традиционными признаками обмана или злоупотребления доверием, что исключает упрощённое понимание данной формы хищения. По нашему мнению, уяснение его сущности требует одновременного учёта классических положений о хищении и специфики цифровых платёжных отношений, по этой причине сохраняется необходимость дальнейшего совершенствования как законодательной регламентации, так и практики применения соответствующей нормы. Такая связь определяет и дальнейшее развитие правоприменения.

При применении ст. 159.3 УК РФ ключевое значение имеет понятие «электронное средство платежа». Уголовный кодекс РФ не содержит его легального определения, перенаправляя правоприменителя к Федеральному закону «О национальной платежной системе». Под данное понятие подпадают не только банковские карты, но также системы интернет-банкинга, мобильные приложения, электронные кошельки и даже NFC-модули. На практике, как представляется, это влечет неодинаковую квалификацию внешне сходных деяний, то есть одинаковые по фактическому рисунку действия получают различную уголовно-правовую оценку в зависимости от того, какое техническое решение было использовано [7].

Проблема заключается в отсутствии четких критериев отнесения конкретного технического устройства или программного обеспечения к электронным средствам платежа. При таком положении возникает риск расширительного толкования, по этой причине затрагивается и принцип правовой определенности. Отсюда, при квалификации по ст. 159.3 УК РФ сохраняется неопределенность, способная повлечь нарушение принципа правовой определенности при оценке того, охватывается ли соответствующее средство понятием электронного средства платежа.

В 2025 году общее число зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий, составило 675,4 тыс., что на 11,8 % меньше, чем годом ранее. Их доля в структуре всей преступности достигла 38 %, причем указанное сокращение количества не устраняет масштаб самой проблемы. С другой стороны, ущерб от телефонного и интернет-мошенничества в 2024 – 2025 гг. достиг рекордных значений, по оценкам экспертов, от 275 млрд до 295 млрд рублей, тем самым количественное снижение зарегистрированных деяний сочетается с сохранением исключительно значительных имущественных потерь.

По тяжким и особо тяжким составам в сфере IT-мошенничества показатель раскрываемости не превышает 23,2 %, а в отдельные периоды – снижался до 10,1 %. В 2025 году нераскрытыми остались 494,3 тыс. таких преступлений, что составило 73,2 % от числа зарегистрированных, что указывает на сохраняющийся разрыв между масштабом выявления соответствующих деяний и результативностью их последующего расследования. В судебной практике наиболее остро стоит вопрос разграничения ст. 159.3 и ст. 158 УК РФ, предусматривающей кражу. Именно способ совершения преступления выступает здесь определяющим критерием. Отсюда, центральное значение приобретает установление того, каким именно образом виновный получает возможность непосредственно распорядиться чужими денежными средствами, а именно через обман либо посредством их фактического тайного изъятия [6].

Кража по ст. 158 УК РФ, напротив, предполагает тайное хищение. Иная квалификация требуется, когда доступ к счету потерпевшего получают без его ведома и вопреки его воле. Если затем виновный переводит денежные средства, используя вредоносное программное обеспечение, скимминг или подглядывание PIN-кода, содеянное квалифицируется как кража, а не мошенничество, поскольку изъятие происходит тайно, без участия владельца [7].

Показательной коллизией выступает хищение денежных средств с банковского счета с использованием найденной банковской карты. Когда лицо оплачивает покупки в магазине через бесконтактную технологию, не требующую ввода ПИН-кода, суды на протяжении длительного времени квалифицировали такие действия как кражу (п. «г» ч. 3 ст. 158 УК РФ). Основание было следующим, доступ к счету осуществлялся без обмана уполномоченного лица, то есть кассира, и потому рассматривался как тайный способ изъятия денежных средств, при отсутствии непосредственного введения кого-либо в заблуждение.

Пленум Верховного Суда РФ в Постановлении от 30.11.2017 № 48 дал по этому вопросу специальное разъяснение. Если виновный использовал чужую банковскую карту для хищения денежных средств, но не вводил в заблуждение уполномоченных лиц (например, при оплате через терминал или в интернете), содеянное надлежит квалифицировать как кражу. Иная оценка возникает при наличии обмана, мошенничество имеет место тогда, когда виновный вводит в заблуждение уполномоченного работника (кассира, продавца), либо самого потерпевшего [10].

Но даже после этих разъяснений судебная практика сохраняет противоречивый характер. Использование технологий бесконтактной оплаты размывает границу между «тайным» и «обманным» способом, поскольку физический контакт с потерпевшим или его представителем отсутствует. По этой причине в ситуациях, когда лицо выдает себя за законного держателя карты, возникает конкуренция с мошенничеством, при этом отсутствие прямого взаимодействия осложняет установление того, имел ли место именно обман как способ завладения чужим имуществом.

Ниже, на основе анализа судебных актов, научных публикаций и материалов правоприменительной практики, приведены конкретные примеры, иллюстрирующие ключевые проблемы применения ст. 159.3 УК РФ. Первый из них - переквалификация с кражи на мошенничество и обратно в уголовном деле в отношении Кактан Ю. Ю., судебным актом по нему выступает Определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 29 сентября 2020 года № 12-УДП20-5-К6 [2].

В этом эпизоде предметом оценки стали действия по оплате товаров, при том, что доступ к денежным средствам был пресечен вследствие блокировки карты.

Хронология квалификации в данном деле последовательно менялась, причем каждое процессуальное решение по-разному определяло уголовно-правовую природу содеянного. Суд первой инстанции осудил Кактан Ю. Ю. по ч. 3 ст. 30, п. «г» ч. 3 ст. 158 УК РФ (покушение на кражу с банковского счёта). Шестой кассационный суд общей юрисдикции 13 мая 2020 года переквалифицировал действия на ч. 3 ст. 30, ч. 1 ст. 159.3 УК РФ (покушение на мошенничество с использованием электронных средств платежа). Затем Верховный Суд РФ отменил кассационное определение и направил дело на новое рассмотрение.

Позиция Верховного Суда строилась на разграничении признаков хищения и мошенничества применительно к действующей редакции уголовного закона. Судебная коллегия указала, что ссылка кассационной инстанции на п. 17 постановления Пленума Верховного Суда РФ от 30 ноября 2017 года № 48 является необоснованной, поскольку разъяснения были даны применительно к ранее действовавшей редакции ст. 159.3 УК РФ.

Именно эта правовая позиция, по нашему мнению, имеющая принципиальное значение для квалификации, создала основу для переквалификации многих аналогичных деяний.

Другой показательный пример связан с использованием чужой карты в супермаркете и с вопросом об обмане сотрудника. Источником выступает научная статья Тюнина В.И., Чабукиани О.А. (Санкт-Петербургский университет МВД России), в которой анализируется ситуация, выявляющая спорность признаков мошенничества при оплате товаров чужой банковской картой [1].

Ситуация состояла в следующем, гражданин Г. передал работнику торгового центра чужую банковскую карту в целях оплаты товаров. Суд первой инстанции, оценивая содеянное, указал:, что хотя Г. и не раскрыл свою личность, само по себе это обстоятельство не образует обмана либо введения в заблуждение сотрудника торговой организации, поскольку при нем отсутствовал документ, способный удостоверить его личность. Ключевое значение в данном деле приобрёл характер поведения лица, требовалось установить, достаточно ли одного лишь предъявления карты, не сопровождаемого какими-либо иными действиями, для признания наличия обмана.

В толковании норм уголовного права представлен и альтернативный подход к оценке указанных обстоятельств. По мнению ряда авторов, судебный орган не учел, что для применения ст. 159.3 УК РФ, то есть для констатации факта мошенничества, достаточно самого несообщения о незаконном владении банковской картой; данное умолчание рассматривается как юридически значимое обстоятельство. Уже одно это, как полагают сторонники такой позиции, образует введение в заблуждение работников супермаркета, даже при отсутствии иных действий со стороны лица. Иначе говоря, Тюнин В.И. и Чабукиани О.А. связывают наличие обмана с пассивным сокрытием существенного обстоятельства, а не только с активным сообщением ложных сведений.

Следующий пример касается мошенничества с использованием платежной карты, сопряженного с причинением значительного ущерба. Источником выступает приговор Саровского городского суда Нижегородской области по делу № 1-74/14 в отношении Рыжовой А.Н., он позволяет проследить, как в судебной практике применяется ч. 2 ст. 159.3 УК РФ при наличии квалифицирующего признака [8]. По фабуле дела Рыжова А.Н. признана виновной в совершении преступления, предусмотренного ч. 2 ст. 159.3 УК РФ. Тем самым в квалификации были одновременно отражены способ совершения деяния и последствие в виде значительного ущерба. Суд учел ряд смягчающих обстоятельств, а именно наличие на иждивении малолетнего ребенка (п. «г» ч. 1 ст. 61 УК РФ), добровольное возмещение имущественного ущерба (п. «к» ч. 1 ст. 61 УК РФ), состояние здоровья (наличие хронических заболеваний), а также признание вины и раскаяние в содеянном. Но наряду с этим было установлено и отягчающее обстоятельство, рецидив преступлений (п. «а» ч. 1 ст. 18 УК РФ). Подсудимая ранее была судима за мошенничество (ч. 1 ст. 159 УК РФ) и кражу (п. «в» ч. 3 ст. 158 УК РФ).

Значение данного примера состоит в том, что он демонстрирует применение квалифицированного состава ст. 159.3 УК РФ при наличии признака «значительный ущерб гражданину». Одновременно этот материал показывает, каким образом суд учитывает смягчающие обстоятельства при назначении наказания, даже в ситуации, когда в деле присутствует рецидив.

Приговор по делу № 1-40/34/2020 Джанкойского судебного района Республики Крым в отношении гражданина Сулько С.А. Фабула дела сводилась к следующим обстоятельствам, С.А. Сулько обнаружил мужской кошелек с двумя банковскими картами ПАО «РНКБ Банк». Реализуя внезапно возникший умысел на завладение чужим имуществом мошенническим путем, он умышленно ввел в заблуждение уполномоченных сотрудников нескольких магазинов, умолчав об отсутствии права на использование указанных выше найденных им средств электронного платежа, и расплатился за товар безналичным расчетом. В результате потерпевшему был причинен материальный ущерб - 4 800 рублей 90 копеек [9]. Содеянное было квалифицировано по ч. 1 ст. 159.3 УК РФ, как мошенничество с использованием электронных средств платежа. Именно такая уголовно-правовая оценка легла в основу итогового судебного решения. При назначении наказания суд учел ряд смягчающих обстоятельств, а именно явка с повинной, активное способствование раскрытию и

расследованию преступления, частичное добровольное возмещение имущественного вреда, раскаяние в содеянном, признание вины. Их совокупность характеризовала поведение виновного после совершения преступления и, как представляется, имела значение для индивидуализации ответственности. Одновременно суд установил отягчающее обстоятельство, а именно рецидив преступлений (п. «а» ч. 1 ст. 63 УК РФ), ранее лицо было судимо по п. «г» ч. 2 ст. 161 УК РФ. Наличие этого обстоятельства прямо повлияло на итоговую меру ответственности. Наказание было назначено в виде лишения свободы с учетом рецидива. Этот элемент приговора отражает повышенное значение данных о личности виновного при определении санкции.

Значение данного приговора состоит в том, что он иллюстрирует традиционный подход к квалификации оплаты чужой банковской картой в магазине. Согласно этому подходу, умолчание о незаконном владении картой перед сотрудником торговой организации расценивается как введение в заблуждение, то есть обман. Но после определения Верховного Суда РФ № 12-УДП20-5-К6 подобная квалификация, при сохранении прежней логики оценки фактов, вступила в противоречие с формирующейся единообразной практикой.

Дело, рассмотренное в отношении гражданина Курбанова А.С. Батайским городским судом Ростовской области является важным примером как судебно-практический эпизод с четко обозначенными квалификацией деяния и итогом рассмотрения. Согласно обстоятельствам уголовного дела, гражданину, проживающему в Батайске, инкриминировалось деяние, квалифицированное по ч. 2 ст. 159.3 УК РФ. Речь шла о мошенничестве, совершенном с применением электронных платежных инструментов и повлекшем значительный ущерб для потерпевшего, именно такая квалификация, и это принципиально, была положена в основу предъявленного обвинения. Иных составов преступлений в вину данному лицу не вменялось.

По нашему мнению, именно такой подход и воспроизводится в данном случае. Для соответствующей категории дел этот материал показателен, как пример наказания сравнительно небольшой тяжести при установленной виновности судом.

В российском правовом поле отсутствует единство мнений относительно момента окончания мошенничества с использованием электронных средств платежа. Дискуссия сосредоточена вокруг нескольких возможных юридически значимых моментов, а именно введения виновным данных карты в устройство, то есть составления распоряжения; списания денежных средств с банковского счета потерпевшего; их зачисления на счет виновного; получения виновным реальной возможности распорядиться похищенным, например путем снятия наличных. Отсюда, ключевое значение приобретает ответ на вопрос о том, какой именно этап следует признавать моментом завершения преступного посягательства.

Нечеткость в определении момента окончания прямо влияет на квалификацию неоконченных преступлений. Речь идет о разграничении приготовления и покушения, причем ошибка на этом этапе меняет пределы уголовной ответственности. Если лицо ввело данные карты, но транзакция была заблокирована службой безопасности банка, содеянное должно квалифицироваться как покушение, поскольку исполнение объективной стороны уже началось, однако преступный результат не наступил по независящим от виновного обстоятельствам.

На практике, однако, такие действия иногда ошибочно оцениваются как оконченное преступление. В иных случаях им, напротив, придается значение лишь приготовления; подобное расхождение, как представляется, влечет необоснованное смягчение или ужесточение ответственности. По этой причине отсутствие четкого подхода к моменту окончания мошенничества с использованием электронных средств платежа сохраняет не только теоретическую, но и прикладную значимость.

Сохраняются, однако, и вопросы квалификации, имеющие принципиальное значение. Первый из них связан со случаями, когда хищение с использованием электронных систем платежа сопряжено с неправомерным доступом к компьютерной информации, предусмотренным ст. 272 УК РФ. Возникает вопрос, следует ли рассматривать содеянное по совокупности преступлений или имеет место поглощение одного состава другим, в зависимости от уголовно-правового значения неправомерного доступа для механизма хищения.

Не менее сложным остается разграничение ст. 159.3 и ст. 159.6 УК РФ, предусматривающей мошенничество в сфере компьютерной информации. Граница между этими составами проводится по способу совершения деяния, а именно в ст. 159.6 таким способом выступает модификация компьютерной информации, тогда как в ст. 159.3 электронное средство платежа используется как инструмент завладения чужими денежными средствами. По этой причине отсутствие четких критериев разграничения создает ситуацию, при которой одно и то же, по существу, деяние, может получить квалификацию по статье с более мягкой или более строгой санкцией, а это затрагивает принцип справедливости.

Проведенный анализ позволяет выделить несколько ключевых проблем применения уголовного законодательства об ответственности за мошенничество с использованием электронных средств платежа. Первая из них – терминологическая неопределенность, отсутствие легального определения электронных средств платежа в УК РФ при широкой трактовке в смежном законодательстве создает предпосылки для противоречивого толкования. Далее обнаруживается сложность разграничения со смежными составами, поскольку критерии отграничения от кражи (ст. 158 УК РФ) и мошенничества в сфере компьютерной информации (ст. 159.6 УК РФ) нуждаются в дальнейшем уточнении, особенно с учетом развития бесконтактных технологий. К числу существенных относится и неопределенность момента окончания преступления, виртуальный характер изъятия имущества порождает споры о моменте окончания, а это непосредственно влияет на квалификацию неоконченной преступной деятельности. Наконец, сохраняется конкуренция норм, то есть необходимым остается четкое разграничение совокупности преступлений при неправомерном доступе к компьютерной информации и использовании электронных средств платежа.

В целях совершенствования правоприменительной практики, как представляется, целесообразно предпринять следующие меры.

Во-первых, следует дополнить Постановление Пленума Верховного Суда РФ № 48 от 30.11.2017 разъяснениями относительно квалификации действий с использованием бесконтактных технологий оплаты.

Обоснование данного подхода связано с разграничением функциональной роли электронного средства платежа в механизме хищения. Это позволит исключить квалификацию по ст. 159.3 УК РФ случаев, когда электронное средство платежа используется лишь как технический канал передачи денег, а обман направлен на потерпевшего, а не на платёжную систему. Отсюда следует вывод, предлагаемое уточнение через легальное определение и прямое указание способа совершения деяния, ориентировано на устранение коллизий в правоприменении.

Вопрос об ужесточении санкций и устранении несоразмерности наказаний обусловлен различием в законодательной оценке близких по содержанию деяний. Проблема состоит в том, что часть первая ст. 159.3 УК РФ относится к категории преступлений небольшой тяжести, в то время как аналогичное по общественной опасности деяние, предусмотренное п. «г» ч. 3 ст. 158 УК РФ (кража с банковского счёта), является тяжким преступлением. Здесь обнаруживается нормативный дисбаланс, при сопоставимой общественной опасности законодатель закрепляет различный уровень уголовно-правовых последствий.

В качестве предложения выдвигается ужесточение санкций каждой части ст. 159.3 УК РФ с приведением их в соответствие с санкциями п. «г» ч. 3 ст. 158 УК РФ. В частности, предлагается предусмотреть в части первой наказание в виде лишения свободы на срок до четырех лет, в части второй – до шести лет, в части третьей – до восьми лет. Подобная корректировка, как представляется, направлена не на формальное повышение репрессивности, а на устранение расхождения между сходными составами преступлений.

Обоснование данной позиции исследователи связывают с содержательным сходством рассматриваемых посягательств, отмечается, что схожее деяние, закрепленное в ч. 3 ст. 158 УК РФ, является тяжким преступлением, хотя обладает практически одинаковой общественной опасностью. По этой причине несоразмерность санкций нарушает принцип справедливости и создает стимулы для защиты, выбирающих менее наказуемую форму посягательства. Предлагаемое изменение, при сохранении структуры статьи, должно устранить указанное противоречие.

Дифференциация ответственности в зависимости от типа преступного поведения обусловлена неоднородностью деяний, охватываемых ст. 159.3 УК РФ. Проблема заключается в том, что статья 159.3 УК РФ не различает «массовое» телефонное мошенничество и «целевое» высокотехнологичное мошенничество, различающиеся по степени организованности и общественной опасности. При таком

подходе единая норма, несмотря на различие способов совершения, охватывает качественно неодинаковые формы преступной активности.

В качестве предложения рассматривается дополнение ст. 159.3 УК РФ квалифицирующим признаком, совершение деяния «с использованием специальных технических средств, предназначенных для неправомерного доступа к электронным средствам платежа, либо с использованием вредоносных компьютерных программ». Одновременно предлагается установить за данное деяние наказание в виде лишения свободы на срок до восьми лет со штрафом. Подобная конструкция, при прямом указании на специальные средства и вредоносные программы, позволяет выделить более опасный способ посягательства в самостоятельный квалифицированный случай.

Введение квалифицирующего признака для защиты социально уязвимых категорий граждан обусловлено составом потерпевших по делам о данном посягательстве. Проблема состоит в том, что лица предпенсионного и пенсионного возраста образуют одну из наиболее уязвимых категорий потерпевших.

В качестве предложения может быть рассмотрено дополнение ст. 159.3 УК РФ квалифицирующим признаком – совершение деяния «в отношении лица, заведомо для виновного, находящегося в беспомощном состоянии либо в материальной или иной зависимости от виновного, а равно в отношении лица предпенсионного или пенсионного возраста». Такая формула, объединяя несколько вариантов повышенной виктимности, прямо указывает на особые свойства потерпевшего как на обстоятельство, влияющее на уголовно-правовую оценку. И тем самым диспозиция получает более точный ориентир для дифференциации ответственности. Такой подход, при сохранении общей логики уголовно-правовой охраны, позволяет адресно усилить защиту наиболее уязвимых категорий граждан.

Анализ статьи 159.3 Уголовного кодекса Российской Федерации показывает, что с момента введения в 2012 году законодательная конструкция данной нормы существенно изменилась. При этом необходимой степени определенности она до настоящего времени не приобрела, именно в этом состоит одна из базовых проблем её применения. Первоначальная редакция статьи, ориентированная на хищение денежных средств с использованием платежных карт, после введения в 2018 году ответственности за кражу с банковского счета (пункт «г» части третьей статьи 158 УК РФ) утратила значительную часть собственного предмета регулирования, а возникшее вследствие этого «пересечение» смежных составов породило устойчивую конкуренцию норм, её разрешение в правоприменительной практике осуществляется непоследовательно.

Центральный вывод исследования состоит в констатации следующего положения. Ключевой критерий разграничения мошенничества и кражи, то есть наличие обмана, направленного на уполномоченное лицо, в условиях цифровизации платежных отношений утрачивает эвристическую ценность. Показательно, что определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 29 сентября 2020 года № 12-УДП20-5-К6 обозначило принципиальный поворот в судебной практике, в нем высшая судебная инстанция указала на необоснованность применения разъяснений Пленума, данных применительно к ранее действовавшей редакции статьи. Однако этот поворот не сопровождался своевременной актуализацией разъяснений Пленума Верховного Суда Российской Федерации, вследствие чего возникло состояние нормативной неопределенности - в нем нижестоящие суды вынуждены самостоятельно выбирать между конкурирующими подходами.

Выявленная гетерогенность имеет принципиальное уголовно-политическое значение. За единой нормой статьи 159.3 УК РФ скрываются как минимум два качественно различных криминологических типа: массовое дистанционное мошенничество, характеризующееся случайным выбором жертвы и относительно невысоким средним ущербом, и целевое высокотехнологичное мошенничество, отличающееся предварительной подготовкой, организационной структурой и планируемым крупным ущербом. Действующая редакция нормы не позволяет дифференцировать ответственность в зависимости от этих различий, что противоречит принципу справедливости и снижает эффективность уголовно-правового воздействия. Отсюда следует практический вывод, существующая модель нуждается в более тонкой нормативной настройке.

Исследование позволяет констатировать и наличие институциональных деформаций, выходящих за рамки собственно уголовно-правового регулирования. Высокий уровень нераскрытых преступлений рассматриваемой категории, достигающий, по отдельным оценкам, трех четвертей от числа зарегистрированных, свидетельствует о том, что проблемы применения статьи 159.3 УК РФ не могут быть решены исключительно средствами законодательной техники. Существенное значение имеют технологическая компетентность правоприменителей, качество работы с цифровыми доказательствами, а также система оценки деятельности правоохранительных органов, которая в ряде случаев создаёт стимулы к искусственному сокращению регистрации заявлений, именно поэтому институциональный контекст в данном случае не менее значим, чем формальная конструкция уголовно-правовой нормы.

Литература

1. Тюнин В. И., Чабукиани О. А. Мошенничество с использованием электронных средств платежа (вопросы правоприменения) // Криминалист. 2023. № 4 (45). С. 92-98.
2. Определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 29.09.2020 № 12-УДП20-5-К6 // Электронный ресурс / Режим доступа: https://sudact.ru/vsrf/doc/ZN8J7fkPouZC/ (дата обращения 08.10.2026)
3. Судебная статистика // Официальный сайт Судебного департамента при Верховном Суде Российской Федерации. URL: http://www.cdep.ru/index.php?id=79 (дата обращения: 15.09.2026).
4. Сафина Э. Л. Особенности и проблемы применения уголовного законодательства об ответственности за мошенничество с использованием электронных средств платежа / Э. Л. Сафина // Вестник науки. – 2024. – Т. 4, № 5(74). – С. 611-614.
5. Ржевский Н. П. Мошенничество с использованием электронных средств платежа: зарубежный опыт правового регулирования / Н. П. Ржевский // Вестник Дальневосточного юридического института МВД России. – 2025. – № 2(71). – С. 48-52.
6. Кипкеев И. М. Актуальные проблемы применения уголовного закона об ответственности за мошенничество с использованием электронных средств платежа / И. М. Кипкеев // Евразийский юридический журнал. – 2024. – № 11(198). – С. 324-326.
7. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 20.02.2026) // Собрание законодательства РФ. 1996. № 25. Ст. 2954.
8. Приговор Саровского городского суда Нижегородской области от 09.07.2014 № 1-74/14 // Электронный ресурс / Режим доступа: https://sarovsky.nnov.sudrf.ru/ (дата обращения 08.10.2026)
9. Приговор Джанкойского судебного района Республики Крым от 03.11.2020 № 1-40/34/2020 // Электронный ресурс / Режим доступа: https://dzhankoi.krm.sudrf.ru/ (дата обращения 08.10.2026)
10. Постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // Бюллетень Верховного Суда РФ. - 2018. - № 2.

Problems in applying criminal legislation on liability for fraud using electronic payment methods

Embulaeva N.Yu., Okorokov V.I.

Kuban State Agrarian University named after I. T. Trublin

The article examines current issues related to the qualification of fraud committed using electronic payment means (Article 159.3 of the Criminal Code of the Russian Federation). The analysis covers the dynamics of changes in criminal law; at the same time, it examines the problems of distinguishing between related crime elements provided for in Articles 159, 159.3, and 158 of the Criminal Code of the Russian Federation. Special attention is focused on the interpretation of the concept of "electronic payment means" and on determining the moment when the crime ends — it is these elements that cause the most noticeable difficulties in law enforcement. The author concludes that it is necessary to further differentiate criminal liability and clarify the conceptual framework in order to avoid errors in law enforcement practice.

Keywords: Electronic payment methods, fraud, information technology, cybercrime, theft, bank cards, criminal law.

References

1. Tyunin V. I., Chabukiani O. A. Fraud Using Electronic Means of Payment (Issues of Law Enforcement) // Kriminalist. 2023. No. 4 (45). Pp. 92–98.
2. Ruling of the Judicial Collegium for Criminal Cases of the Supreme Court of the Russian Federation of 29.09.2020 No. 12-UDП20-5-K6 // Electronic resource / Access mode: https://sudact.ru/vsrf/doc/ZN8J7fkPouZC/ (date of access 08.10.2026)
3. Judicial Statistics // Official website of the Judicial Department at the Supreme Court of the Russian Federation. URL: http://www.cdep.ru/index.php?id=79 (date of access: 15.09.2026).
4. Safina E. L. Features and Problems of Applying Criminal Legislation on Liability for Fraud Using Electronic Means of Payment / E. L. Safina // Vestnik Nauki. – 2024. – Vol. 4, No. 5(74). – Pp. 611–614.

5. Rzhevsky N. P. Fraud Using Electronic Means of Payment: Foreign Experience of Legal Regulation / N. P. Rzhevsky // Bulletin of the Far Eastern Law Institute of the Ministry of Internal Affairs of Russia. – 2025. – No. 2(71). – Pp. 48–52.
6. Kipkeev I. M. Current Problems of Applying the Criminal Law on Liability for Fraud Using Electronic Means of Payment / I. M. Kipkeev // Eurasian Law Journal. – 2024. – No. 11(198). – Pp. 324–326.
7. Criminal Code of the Russian Federation of June 13, 1996 No. 63-FZ (as amended on 20.02.2026) // Collection of Legislation of the Russian Federation. 1996. No. 25. Art. 2954.
8. Verdict of the Sarov City Court of the Nizhny Novgorod Region of 09.07.2014 No. 1-74/14 // Electronic resource / Access mode: https://sarovsky.nnov.sudrf.ru/ (date of access 08.10.2026)
9. Verdict of the Dzhankoy Judicial District of the Republic of Crimea of 03.11.2020 No. 1-40/34/2020 // Electronic resource / Access mode: https://dzhankoi.krm.sudrf.ru/ (date of access 08.10.2026)
10. Resolution of the Plenum of the Supreme Court of the Russian Federation of November 30, 2017 No. 48 "On Judicial Practice in Cases of Fraud, Embezzlement and Misappropriation" // Bulletin of the Supreme Court of the Russian Federation. – 2018. – No. 2.