

Дата поступления рукописи в редакцию: 06.06.2026 г.
Дата принятия рукописи в печать: 11.07.2026 г.

DOI: 10.24412/2782-3849-2026-7-452-456

КУЗЬМИН С.А.,

Адъюнкт очной формы обучения ФПНПиНК Московского университета МВД России имени В.Я. Кикотя,

e-mail: mail@law-books.ru

К ВОПРОСУ ОБ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА НЕПРАВОМЕРНЫЙ ОБОРОТ СРЕДСТВ ПЛАТЕЖЕЙ ПО ЗАКОНОДАТЕЛЬСТВУ РОССИЙСКОЙ ФЕДЕРАЦИИ И РЕСПУБЛИКИ БЕЛАРУСЬ

Аннотация. В статье рассматриваются актуальные вопросы уголовной ответственности за неправомерный оборот средств платежей в Российской Федерации и Республике Беларусь (ст. 187 УК РФ и ст. 222 УК РБ). Подчеркивается высокая общественная опасность посягательств на платёжную инфраструктуру и имущественную безопасность, обусловленная массовостью ущерба, трансграничностью и латентностью. Сопоставляются тенденции преступности в двух государствах и выделяются ведущие криминальные практики, включая использование банковских карт, мобильных каналов и вовлечение «дропперов». Анализируются ключевые этапы установления и развития уголовной ответственности за обозначенные преступления, выявляются проблемные зоны существующих моделей: неполный охват цифровых и виртуальных платёжных инструментов. Предлагаются меры по модернизации ст. 222 УК РБ и дальнейшей конкретизации ст. 187 УК РФ.

Ключевые слова: неправомерный оборот средств платежей; платёжные инструменты; электронные средства платежа; цифровые кошельки; токены; криптовалюта; дропперы; инструменты преступления; гармонизация законодательства.

KUZMIN S.A.,

Adjunct full-time education FPNPiNK Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikotya

ON CRIMINAL LIABILITY FOR ILLEGAL CIRCULATION OF MEANS OF PAYMENT UNDER THE LAWS OF THE RUSSIAN FEDERATION AND THE REPUBLIC OF BELARUS

Annotation. The article considers topical issues of criminal liability for illegal circulation of means of payment in the Russian Federation and the Republic of Belarus (Article 187 of the Criminal Code of the Russian Federation and Article 222 of the Criminal Code of the Republic of Belarus). The high public danger of encroachments on payment infrastructure and property security is emphasized, due to the massive damage, cross-border and latency. Crime trends in the two states are compared and leading criminal practices are highlighted, including the use of bank cards, mobile channels and the involvement of "droppers." The key stages of establishing and developing criminal liability for the designated crimes are analyzed, problem areas of existing models are identified: incomplete coverage of digital and virtual payment instruments. Measures are proposed to modernize Art. 222 of the Criminal Code of the Republic of Belarus and further concretization of Art. 187 of the Criminal Code of the Russian Federation.

Key words: illegal circulation of means of payment; payment instruments; electronic means of payment; digital wallets; tokens; cryptocurrency; droppers; instruments of crime; harmonization of legislation.

Неправомерный оборот средств платежей обладает высокой степенью общественной опасности в силу системности посягательства на устойчивость платёжной инфраструктуры и имущественную безопасность граждан и бизнеса [1, с. 149; 3, с. 66]. Указанное выражается в подрыве доверия к безналичным расчётам и цифровой экономике в целом, в массовом характере ущерба,

в трансграничности и высокой латентности таких деяний, а также в перераспределении издержек на добросовестных участников рынка через рост комиссий, затрат на комплаенс [7] и антифрод контроль [8]. Это преступление затрагивает не только частные интересы потерпевших, но и публичные – стабильность финансовой системы и её способность обеспечивать надёжные расчёты

[4, с. 227].

Как отмечают специалисты, неправомерный оборот средств платежей представляет собой преступное деяние, совершаемое в сфере экономической деятельности, посягающее на установленный порядок функционирования платёжной системы и причиняющее ущерб имущественным интересам граждан и организаций [2, с. 226; 6, с. 140].

Развитие цифровых технологий привело к появлению новых видов платёжных инструментов [5, с. 67] и, одновременно, к эволюции способов их неправомерного использования. Соответственно, для обоих выбранных государств возникает необходимость криминализации соответствующих деяний посредством их отнесения в силу общественной опасности к числу преступных и наказуемых.

На современном этапе значительная часть преступных посягательств связана с мошенничествами посредством мобильной связи и банковских карт. Вовлечение в незаконные схемы так называемых «дропперов» [9] приобрело массовый характер и существенно затрудняет раскрытие хищений, совершенных онлайн. Эти тенденции демонстрируют высокую степень общественной опасности преступлений, связанных с оборотом средств платежей, и требуют адекватной реакции со стороны законодателя.

В Российской Федерации в 2015 г. была модернизирована норма об ответственности за неправомерный оборот средств платежей (ст. 187 УК РФ), благодаря чему преступление было описано более широко, взамен ранее применяемой узкой конструкции о подделке расчётных карт и иных платёжных документов. Спустя десятилетие, в июне 2025 г., федеральным законом от 24 июня 2025 г. №176-ФЗ «О внесении изменений в статью 187 Уголовного кодекса Российской Федерации», были выполнены существенные преобразования в ст. 187 УК РФ, а также введены примечания к этой статье.

В Республике Беларусь уголовная ответственность за незаконный оборот платёжных инструментов, средств платежа и их реквизитов предусмотрена ст. 222 УК РБ. Несмотря на наработанную практику по применению ст. 222 УК РБ, на сегодняшний момент существует ряд проблем: отсутствуют легальные определения ключевых понятий («средства платежа», «электронные средства» и т.п.); не регламентируется уголовная ответственность дропперов; отдельные современные объекты преступлений не охватываются действующими нормами белорусского уголовного закона в анализируемой сфере. В отношении указанного, для Республики Беларусь ценным можно считать

опыт Российской Федерации, предпринявшей шаги для предусмотрения ответственности дропперов посредством модернизации ст. 187 УК РФ в июне 2025 г.

Кроме того, для Российской Федерации и Республики Беларусь с учётом транснационального характера многих преступлений в платёжной сфере и разнообразия платёжных инструментов, возникает задача гармонизации подходов для совместной выработки государствами мер, направленных на противодействие неправомерному обороту средств платежей.

Уголовно-правовое регулирование в экономической сфере в Российской Федерации и Республике Беларусь связано с рядом проблем.

Пробелы в охвате новых технологий. Стремительная цифровизация платежей создала новые способы совершения преступлений, не полностью учтённые уголовным законом. Например, классические составы не охватывали фишинговые атаки [10] с хищением реквизитов для удалённого доступа к счетам, скимминговые устройства [11] для копирования данных карт, незаконное использование токенов [12], а также операции с крипто-активами [13]. До недавнего времени в Российской Федерации и Республике Беларусь не было прямых норм, инкриминирующих использование чужих электронных платёжных аккаунтов (кошельков) без согласия владельца – такие деяния приходилось квалифицировать через общие нормы о мошенничестве или краже данных, что не всегда полностью соответствовало специфике посягательства. Обозначенная ситуация сохранила актуальность для Республики Беларусь, а в Российской Федерации с учетом законодательных новелл 2025 г. ответственность за дропперство теперь осуществляется по ч. 3 ст. 187 УК РФ.

На предыдущем этапе отсутствие легального определения электронного платёжного инструмента затрудняло единообразное правоприменение в разных юрисдикциях, что потребовало существенной детализации нормативных правовых положений ст. 187 УК РФ и ст. 222 УК РБ. Разрешению обозначенной проблемы может способствовать закрепление современных понятий и расширение предмета преступления. Прежде всего, в законодательство Республики Беларусь рекомендуется по аналогии с российской практикой закрепить в примечании к ст. 222 УК РБ понятия незаконного оборота, платёжных инструментов, средств платежа, их реквизитов.

Помимо указанного, для обоих государств представляется целесообразной трансформация законодательства о банках и банковской деятельности с включением в число средств

платежей также цифровых и виртуальных средств, к числу которых будут отнесены электронные деньги, токены, криптовалюты, используемые как платёжное средство, цифровые (в т.ч. мобильные) кошельки и реквизиты доступа к ним. Это устранил неопределённость статуса таких объектов и обеспечит единообразное применение закона в условиях появления новых технологий.

Недостаточная охватываемость роли «посредников-дропперов». Лица, занимающиеся приобретением, переводом или обналичиванием незаконно полученных чужих средств платежей по поручению организаторов преступлений, нередко привлекаются к ответственности лишь как пособники либо наказываются за отмыwanie доходов. Однако специальные составы, отражающие их роль в качестве звена платёжной цепочки, долгое время отсутствовали. Российская Федерация посредством трансформации ст. 187 УК РФ реализовала соответствующие изменения, предусмотрев уголовную ответственность для лиц, предоставляющих свой банковский счёт, карту, цифровые кошельки для транзита или обналичивания похищенных средств, тем самым содействуя сокрытию их происхождения.

Необходимо развить эту практику для Республики Беларусь, дополнив ст. 222 УК РБ положениями о дропперах. Это закроет канал безнаказанного вывода денег и упростит привлечение к ответственности организованных сетей обналичивания, действующих и через границы.

Выводы

Сравнительная обзорная характеристика показывает, что уголовное законодательство Российской Федерации и Республики Беларусь выработало комплексный подход к противодействию неправомерному обороту средств платежей. К общим чертам можно отнести унификацию ответственности за неправомерный оборот различных видов средств платежей (платёжные карты, электронные средства платежа и т.д.), а также установление ответственности за максимально широкий круг действий: от изготовления поддельных средств платежа до их использования и распространения, включая хранение, перевозку, пересылку, импорт, экспорт и иные пособнические действия. Вводятся специальные нормы (ч.5, ч. 6 ст. 187 УК РФ) за неправомерное использование чужого платёжного инструмента. Эти решения позволяют устранить пробелы, которые преступники могли бы использовать, и которые заслуживают внимания при совершенствовании российского и белорусского уголовных законов.

Совершенствование уголовной ответственности за незаконный оборот

средств платежей – необходимое условие для адекватного ответа на новые вызовы цифровой экономики. Динамика развития платёжных технологий требует постоянного обновления уголовных законов обоих выбранных государств и сближения их опыта установления уголовно-правовых запретов. В конечном счёте, унифицированный и технологически актуальный подход к противодействию этим преступлениям поможет обеспечить надёжность безналичных расчётов, снизить ущерб от кибер-преступлений и укрепить доверие граждан и бизнеса к цифровым финансовым инструментам.

Список литературы:

- [1] Боженко С. А. Уголовно-правовая защита оборота средств платежей // Вестник Университета имени О. Е. Кутафина. 2018. № 12 (52). С. 148-154.
- [2] Иванова Е. А. Уголовная ответственность за неправомерный оборот средств платежей по законодательству некоторых зарубежных стран // Государственная служба и кадры. 2021. № 5. С. 226-229.
- [3] Клыков Д. А. Вопросы квалификации преступлений, связанных с неправомерным оборотом средств платежей // Вестник БелЮИ МВД России. 2025. № 2. С. 65-71.
- [4] Меженский А. А. Об общественной опасности неправомерного оборота средств платежей // Вестник ВГУ. Серия: Право. 2020. № 1 (40). С. 222-227.
- [5] Погосян А. М. Инновационные платёжные инструменты в цифровой экономике // Научные записки молодых исследователей. 2017. № 3. С. 63-67.
- [6] Хисамова З. И. Неправомерный оборот средств платежей в контексте норм об ответственности за преступления, совершаемые в отношении информационно-коммуникационных технологий // Общество и право. 2015. № 4 (54). С. 139-144.
- [7] Комплаенс – это система мер, направленных на обеспечение соответствия деятельности компании законодательству, этическим нормам и внутренним правилам, чтобы снизить юридические, финансовые и репутационные риски / См. также: <https://www.fedsfm.ru/kfo/compliance/questions> (дата обращения: 09.04.2026).
- [8] Антифрод-контроль – это система мер и инструментов для выявления и предотвращения мошеннических действий / См. также: <https://www.cfo-russia.ru/glossary/92/79496/> (дата обращения: 09.04.2026).
- [9] Дроппер (дроп, money mule) – лицо, предоставляющее свой банковский счёт/ карту/цифровые кошельки для транзита или

обналичивания похищенных средств, тем самым содействуя сокрытию их происхождения (типичная «прослойка» в схемах хищения и отмыкания). В международной практике соответствует понятию money mule – посредник, который получает деньги от третьих лиц и переводит их далее за вознаграждение / См. также: <https://www.sberbank.ru/ru/person/kibrary/vocabulary/drop> (дата обращения: 09.04.2026).

[10] Фишинг, фишинговая атака – способ социальной инженерии: введение в заблуждение (письма/сайты/сообщения), побуждающее жертву раскрыть учётные данные, платежные реквизиты или совершить перевод. Это способ совершения преступления, а не самостоятельный состав / См. также: <https://www.sberbank.ru/ru/person/kibrary/vocabulary/fishing> (дата обращения: 09.04.2026).

[11] Скимминг – тайное копирование данных платёжной карты и/или PIN при помощи накладок/врезных модулей на банкоматах, POS-терминалах или топливных колонках; затем данные используют для изготовления дубликатов карт и несанкционированных списаний; скиммер, скимминговое устройство – устройство, предназначенное для такого считывания / См. также: <https://www.sberbank.ru/ru/> (дата обращения: 09.04.2026).

[12] Токен платежный (EMV-token) – суррогат реквизита карты (PAN), генерируемый токенизатором и ограниченный условиями использования (устройство/мерчант/сценарий). Применяется для снижения риска компрометации реквизитов. Это элемент инфраструктуры платежа, а не самостоятельное «средство платежа» / См. также: <https://www.sberbank.ru/ru/person/kibrary/vocabulary/token> (дата обращения: 09.04.2026).

[13] Крипто-активы – обобщающий международный термин: цифровое представление ценности/прав, которое может передаваться и храниться электронно с использованием DLT/аналогичных технологий. В стандартах ФАТФ это «виртуальные активы»; в ЕС MiCA закрепляет определение и вводит подвиды (utility-tokens, asset-referenced tokens, e-money tokens) / См. также: <https://www.sberbank.ru/ru/person/kibrary/vocabulary/kriptoalyuta> (дата обращения: 09.04.2026).

References:

[1] S. A. Bozhenok Criminal law protection of the circulation of means of payment//Bulletin of the O. E. Kutafin University. 2018. № 12 (52). S. 148-154.

[2] E.A. Ivanova Criminal liability for illegal circulation of means of payment under the legislation of some foreign countries//Public service and personnel. 2021. № 5. S. 226-229.

[3] D.A. Klykov Issues of qualification of

crimes related to illegal circulation of funds of payments//Bulletin of BelYul of the Ministry of Internal Affairs of Russia. 2025. № 2. S. 65-71.

[4] A. A. Mezhenyky On the public danger of illegal circulation of means of payment//Vestnik VSU. Series: Right. 2020. № 1 (40). S. 222-227.

[5] A. Poghosyan Innovative payment tools in the digital economy//Scientific notes of young researchers. 2017. № 3. S. 63-67.

[6] Z. Khisamova Illegal circulation of means of payment in the context of norms on responsibility for crimes committed in relation to information and communication technologies//Society and law. 2015. № 4 (54). S. 139-144.

[7] Compliance is a system of measures aimed at ensuring compliance of the company's activities with legislation, ethical standards and internal rules in order to reduce legal, financial and reputational risks/See also: <https://www.fedsfm.ru/kfo/compliance/questions> (date of appeal: 09.04.2026).

[8] Antifraud control is a system of measures and tools to identify and prevent fraud/See also: <https://www.cfo-russia.ru/glossariy/92/79496/> (contact date: 09.04.2026).

[9] Dropper (drop, money mule) - a person who provides his bank account/card/digital wallets for the transit or cashing of stolen funds, thereby helping to conceal their origin (a typical "layer" in theft and laundering schemes). In international practice, it corresponds to the concept of money mule - an intermediary who receives money from third parties and transfers it further for a fee/See also: <https://www.sberbank.ru/ru/person/kibrary/vocabulary/drop> (date of appeal: 09.04.2026).

[10] Phishing, phishing attack - a method of social engineering: misleading (letters/sites/messages), prompting the victim to disclose credentials, payment details or make a transfer. This is a method of committing a crime, not an independent composition/See also: <https://www.sberbank.ru/ru/person/kibrary/vocabulary/fishing> (date of appeal: 09.04.2026).

[11] Skimming - secretly copying payment card and/or PIN data using overlays/IDMs at ATMs, POS terminals or fuel columns; the data is then used to make duplicate cards and unauthorized write-offs; skimmer, skimming device - a device designed for such reading/See also: <https://www.sberbank.ru/ru/> (access date: 09.04.2026).

[12] Payment token (EMV-token) - a surrogate for card details (PAN) generated by the tokenizer and limited by the terms of use (device/merchant/script). It is used to reduce the risk of compromising details. This is an element of the payment infrastructure, not a standalone "means of payment" /See also: <https://www.sberbank.ru/ru/person/kibrary/vocabulary/token> (circulation date: 09.04.2026).

[13] Crypto assets are a generalizing international term: a digital representation of value/rights that can be transmitted and stored electronically using DLT/similar technologies. In FATF standards, these are “virtual assets”; in the

EU, MiCA establishes the definition and introduces subspecies (utility-tokens, asset-referenced tokens, e-money tokens)/See also: <https://www.sberbank.ru/ru/person/kibrary/vocabulary/kriptovalyuta> (access date: 09.04.2026).



**ЮРИДИЧЕСКОЕ ИЗДАТЕЛЬСТВО
«ЮРКОМПАНИ»**

Издание учебников,
учебных и методических
пособий, монографий,
научных статей.

Профессионально.

В максимально
короткие сроки.

Размещаем
в РИНЦ, E-Library.

ЮРКОМПАНИ

www.law-books.ru