Дата поступления рукописи в редакцию: 19.02.2026 г.
Дата принятия рукописи в печать: 10.03.2026 г.
DOI: 10.24412/2076-1503-2026-2-781-786

МАГОМЕДОВ Темирлан Магомед-Саидович,
К.ю.н., доцент кафедры уголовного права и криминологии Юридического института Дагестанского государственного университет,
e-mail: mail@law-books.ru

АЛИЕВ Ахмед Шамилович,
Магистрант 2 курса Юридического института Дагестанского государственного университета,
e-mail: mail@law-books.ru

ОСОБЕННОСТИ УГОЛОВНО-ПРАВОВОЙ КВАЛИФИКАЦИИ «ТЕЛЕФОННОГО МОШЕННИЧЕСТВА» В СОВРЕМЕННЫХ УСЛОВИЯХ

Аннотация. *Телефонные хищения представляют собой не отдельный «вид» преступления, а совокупность дистанционных имущественных посягательств, объединённых использованием голосовой связи (включая мессенджеры и VoIP) как канала обманного воздействия и как средства координации распределённой преступной группы. Отсутствие самостоятельного состава «телефонного мошенничества» в УК РФ закономерно поднимает проблем конкуренции и разграничения норм о мошенничестве (ст. 159, 159.3, 159.6 УК РФ) и краже (ст. 158 УК РФ, прежде всего п. «г» ч. 3), а также норм о преступлениях в сфере компьютерной информации (ст. 272–274.1 УК РФ) и неправомерном обороте средств платежей (ст. 187 УК РФ). В статье обосновывается, что «телефонный» способ воздействия сам по себе не предопределяет квалификацию по ст. 159 УК РФ; решающими являются юридический механизм изъятия (кто совершил платёжное распоряжение и в каком статусе), наличие либо отсутствие незаконного воздействия на программное обеспечение/сети (критерий ст. 159.6 УК РФ), а также использование электронных средств платежа и характер обмана (для ст. 159.3 УК РФ).*

Ключевые слова*: Уголовное право; дистанционные хищения; телефонное мошенничество; социальная инженерия; ст. 159 УК РФ; ст. 158 УК РФ; ст. 159.3 УК РФ; ст. 159.6 УК РФ; электронные доказательства.*

MAGOMEDOV Temirlan Magomed-Saidovich,
PhD in Law, Associate Professor Department of Criminal Law and Criminology Law Institute, Dagestan State University

ALIEV Ahmed Shamilovich,
Second-Year Master's Student Law Institute, Dagestan State University

FEATURES OF THE CRIMINAL LAW QUALIFICATION OF TELEPHONE FRAUD IN CONTEMPORARY CONDITIONS

Annotation. *Telephone thefts are not a separate type of crime, but a set of remote property offences unified by the use of voice communication, including messengers and VoIP, both as a channel of deceptive influence and as a means of coordinating a distributed criminal group. The absence of an independent offence of telephone fraud in the Criminal Code of the Russian Federation naturally raises issues of concurrence and differentiation between provisions on fraud, Articles 159, 159.3, 159.6 of the Criminal Code of the Russian Federation, and theft, Article 158 of the Criminal Code of the Russian Federation, primarily paragraph g of part 3, as well as provisions on crimes in*

the sphere of computer information, Articles 272 to 274.1 of the Criminal Code of the Russian Federation, and unlawful trafficking in payment instruments, Article 187 of the Criminal Code of the Russian Federation. The article argues that the telephone method of influence in itself does not predetermine qualification under Article 159 of the Criminal Code of the Russian Federation. Decisive factors are the legal mechanism of taking, who issued the payment order and in what capacity, the presence or absence of unlawful interference with software or networks, as the criterion for Article 159.6 of the Criminal Code of the Russian Federation, and the use of electronic means of payment and the nature of deception for Article 159.3 of the Criminal Code of the Russian Federation.

Key words: *Criminal Law, Remote Property Offences, Telephone Fraud, Social Engineering, Article 159 of the Criminal Code of the Russian Federation, Article 158 of the Criminal Code of the Russian Federation, Article 159.3 of the Criminal Code of the Russian Federation, Article 159.6 of the Criminal Code of the Russian Federation, Electronic Evidence.*

В настоящее время, «телефонное мошенничество» часто описывается как единый феномен: звонок, легенда «службы безопасности», эмоциональное давление и последующий имущественный ущерб. Однако для уголовного права принципиально важно иное: «телефон» (в широком смысле — голосовой канал связи, включая мессенджеры) является прежде всего средством воздействия на психику потерпевшего и элементом криминальной технологии, но не самостоятельным юридическим признаком состава. Поэтому корректнее говорить о квалификационной модели телефонных хищений, которая строится вокруг общего состава мошенничества и смежных составов хищений и «цифровых» преступлений [4].

По данным МВД России, в 2025 году зафиксировано снижение преступлений, совершённых с использованием информационно телекоммуникационных технологий, при этом дистанционные мошенничества сохраняют высокую распространённость; отдельно отмечалось снижение дистанционных мошенничеств на 9% при сохранении значимого массива зарегистрированных деяний [12]. Банк России, в свою очередь, фиксирует масштаб предотвращённых попыток хищений и существенные потери граждан от операций без добровольного согласия: в I квартале 2025 года банки предотвратили 43,8 млн попыток хищений, однако злоумышленникам удалось совершить 296,6 тыс. операций почти на 6,9 млрд руб., причём наибольшие потери пришлись на дистанционное банковское обслуживание и переводы [11]. В обзорной отчётности за III квартал 2025 года социальная инженерия названа наиболее распространённым типом атак, а также отражены данные о выявлении мошеннических номеров и взаимодействии с операторами связи [8].

В нормативном плане отсутствие статьи УК РФ о «телефонном мошенничестве» объективно означает, что правоприменитель вынужден выбирать среди нескольких конкурирующих конструкций. Базовый блок составляют ст. 159 УК РФ (мошенничество), ст. 159.3 УК РФ (мошенничество с использованием электронных средств платежа), ст. 159.6 УК РФ (мошенничество в сфере компьютерной информации) и ст. 158 УК РФ (кража), включая п. «г» ч. 3 (кража с банковского счёта, а равно в отношении электронных денежных средств — при отсутствии признаков ст. 159.3 УК РФ) [1]. «Смежный» блок охватывает преступления в сфере компьютерной информации (ст. 272–274.1 УК РФ) и неправомерный оборот средств платежей (ст. 187 УК РФ), которые в реальных кейсах нередко образуют совокупность с хищениями либо выступают формой подготовки к ним [1].

Ключевое методологическое значение для квалификации имеют разъяснения Пленума Верховного Суда РФ. Постановление № 48 (2017, с последующими редакциями) закрепляет подходы к пониманию обмана и злоупотребления доверием, даёт критерии разграничения мошенничества и кражи в ситуациях, когда обман используется лишь для облегчения доступа, формулирует техническое толкование «вмешательства» применительно к ст. 159.6 УК РФ и, что особенно важно для телефонных сценариев, указывает: использование учётных данных и конфиденциальной информации (в том числе переданных потерпевшим под воздействием обмана) для списания безналичных средств при отсутствии незаконного воздействия на программное обеспечение/сети образует кражу, а не мошенничество [2]. Тем самым Верховный Суд фактически развёл «обман человека» как способ завладения имуществом и «обман как способ получения доступа», после которого изъятие происходит тайно.

Однако, главная практическая трудность уголовно правовой оценки телефонных хищений состоит в высокой вариативности механизма изъятия имущества при внешне одинаковой «легенде» звонка. Сценарий «безопасный счёт», «взлом Госуслуг», «следователь», «родственник в беде» может завершаться принципиально разными юридически значимыми действиями: потерпевший сам переводит деньги; потерпевший сообщает код/пароль, а перевод совершает виновный; потерпевший устанавливает ПО удалённого

доступа; оформляется кредит на потерпевшего и деньги выводятся на третьих лиц; наличные передаются курьеру. Следовательно, квалификацию нельзя строить по сюжету «звонка», она должна строиться по конструкции изъятия: кто совершил распоряжение имуществом, каким способом обеспечен доступ, было ли техническое вмешательство, как устроено соучастие и организованность [5].

Наиболее остро проблема проявляется в разграничении мошенничества и кражи при «социальной инженерии». Мошенничество по ст. 159 УК РФ предполагает завладение имуществом или приобретение права на него путём обмана либо злоупотребления доверием, то есть обман должен быть именно способом завладения, а не просто «фоном» события[6]. Между тем в телефонных делах обман часто используется для получения конфиденциальных данных (одноразовых кодов, паролей, реквизитов карты) или доступа к устройству, а само изъятие средств затем осуществляется виновным без участия потерпевшего, посредством списания/перевода через дистанционный банковский сервис. Пленум Верховного Суда РФ сформулировал для правоприменения принципиальную позицию: если безналичные денежные средства похищены посредством использования конфиденциальной информации, переданной держателем карты под воздействием обмана, содеянное квалифицируется как кража (при отсутствии незаконного воздействия на программное обеспечение/сети) [2]. Эта логика означает, что значительная часть того, что в обыденной речи именуется «телефонным мошенничеством», в строгом уголовно правовом смысле тяготеет к п. «г» ч. 3 ст. 158 УК РФ (кража с банковского счёта), а телефонный контакт — лишь способ получения доступа.

Однако такая конструкция порождает несколько проблем правоприменения. Во-первых, следствию и суду требуется достоверно установить субъект платёжного распоряжения: кто фактически «нажал кнопку» перевода, кто был авторизован, чьим устройством и учётной записью пользовались, какие действия совершал потерпевший и какие — виновный. В практике это осложняется тем, что злоумышленники нередко действуют через удалённый доступ: потерпевший устанавливает программу, затем оператор фактически управляет смартфоном и выполняет операции «руками потерпевшего» (через его устройство), а жертва лишь подтверждает отдельные этапы, не понимая их смысла. Возникает вопрос: считать ли это «добровольной передачей» под влиянием обмана (что тяготеет к мошенничеству) или тайным списанием с использованием доступа к устройству и учётным данным (что тяготеет к краже). Сама по себе социальная инженерия здесь не отвечает на вопрос квалификации; ответ зависит от того, сохранял ли потерпевший реальный контроль над распоряжением и понимал ли юридическую значимость совершённых действий, а также от того, имело ли место техническое вмешательство, выходящее за рамки обычной авторизации [7].

Во-вторых, «переквалификационный эффект» позиции Пленума усиливает требования к доказыванию причинной связи. Для мошенничества важно показать, что именно обман обусловил передачу имущества или совершение перевода, а не просто сопровождал событие [9]. Для кражи, напротив, решающим становится доказательство тайного характера изъятия и способа доступа к платёжной инфраструктуре. На практике, особенно при отсутствии аудиозаписей и мессенджер логов, следствие вынуждено опираться на показания потерпевшего, которые нередко эмоциональны и неполны. Это повышает риск квалификационной неопределённости и расхождения оценок между следствием и судом.

Отдельный пласт проблем связан с конкуренцией ст. 159.3 УК РФ и п. «г» ч. 3 ст. 158 УК РФ. Законодатель специально предусмотрел оговорку «при отсутствии признаков преступления, предусмотренного ст. 159.3» в п. «г» ч. 3 ст. 158 УК РФ, тем самым задав приоритет специальной нормы при наличии её признаков [10]. Но в дистанционных схемах нередко переплетаются несколько способов: у потерпевшего выманивают реквизиты, затем совершают операции через СБП, токенизированные инструменты, электронные кошельки, иногда с введением в заблуждение третьих лиц (например, работников организаций или служб поддержки). В таких случаях разграничение «обманного использования платёжного инструмента» (159.3) и «тайного списания» (158) может быть неочевидным и требует оценки роли обмана именно в момент совершения операции: направлен ли он на уполномоченное лицо/инфраструктуру совершения платежа или лишь на потерпевшего для получения доступа. Практическая значимость разграничения велика, поскольку влияет на структуру обвинения и на пределы доказывания.

Не менее дискуссионна конкуренция ст. 159 УК РФ и ст. 159.6 УК РФ. Пленум Верховного Суда РФ дал узкое техническое толкование «вмешательства» для ст. 159.6 УК РФ как целенаправленного воздействия программных и (или) программно аппаратных средств на серверы, компьютеры, сети, нарушающего установленный процесс обработки, хранения или передачи информации и позволяющего незаконно завладеть имуществом [2]. Разъяснено также, что распространение заведомо ложных сведений в сети

(например, поддельные сайты) само по себе образует состав мошенничества (ст. 159), а не «компьютерного мошенничества» (ст. 159.6). Если звонок лишь «подводит» потерпевшего к фишинговой странице или к передаче данных, но не доказано незаконное техническое вмешательство в функционирование средств/сетей, то применение ст. 159.6 будет необоснованным. Вместе с тем в современных схемах установка вредоносного ПО, перехват кодов, подмена реквизитов, вмешательство в работу приложения банка или систем аутентификации встречаются всё чаще, и тогда возможна квалификация по ст. 159.6, причём при неправомерном доступе или использовании вредоносных программ требуется дополнительная квалификация по ст. 272, 273 или 274.1 УК РФ [13]. Практическая трудность здесь состоит в доказательстве именно «технического» компонента: нужно установить характер программного воздействия, его связь с имущественным результатом, а также разграничить «обычное изменение баланса вследствие авторизации» и вмешательство в установленный процесс обработки информации.

Научная дискуссия вокруг ст. 159.6 УК РФ усиливает неопределённость. В доктрине подчёркивается, что конструкция нормы имеет «остаточный» характер: реальный массив дел уходит либо в мошенничество, либо в кражу, а «чистая» 159.6 применяется сравнительно редко, что провоцирует либо расширительное толкование, либо отказ от нормы там, где она могла бы быть уместна [4]. Потребность в законодательном уточнении «мошеннического блока» 159–159.6 с учётом правоприменения отмечалась и в публичных материалах Конституционного Суда РФ [7]. Для телефонных кейсов это выражается в том, что схожие фактические ситуации могут получать различную квалификацию в зависимости от того, как следствие и суд интерпретируют роль «цифрового инструмента» в механизме хищения.

Проблемы квалификации усугубляются организованным характером телефонных посягательств. Современные схемы типологически предполагают распределение ролей: «оператор» (коммуникатор), «куратор» (контроль и распределение задач), «технарь» (инфраструктура, вредоносное ПО, подмена номеров), «дроп» (получатель и обналичиватель), «курьер» (получение наличных). Пленум Верховного Суда РФ указал, что при признании преступления совершённым организованной группой действия всех участников квалифицируются по соответствующей части статьи без ссылки на ст. 33 УК РФ, независимо от фактической роли, а размер при групповом хищении определяется по общей сумме похищенного [1]. Тем не менее на практике установление организованной группы требует доказательства устойчивости, распределения ролей и единого умысла, что сложно при трансграничности инфраструктуры и при «многоэтажности» денежных потоков через «дропов». Особенно проблематичны «дропы», которые нередко утверждают о своей неосведомлённости; тогда требуется тонкая доказательственная работа по установлению субъективной стороны и момента формирования умысла.

Серьёзный массив вопросов связан с определением момента окончания преступления и стадийности (покушение/оконченное). Для дистанционных хищений критично установить, когда виновный получил реальную возможность распоряжаться средствами, и когда ущерб причинён владельцу. Позиции Верховного Суда ориентируют на момент изъятия средств, повлекшего ущерб, что важно для разграничения покушения и оконченного состава при прерванных переводах [9]. При этом развитие банковского антифрода и механизмов приостановления переводов добавляет «процессуальную динамику»: если банк остановил операцию по признакам перевода без добровольного согласия, правовая оценка чаще смещается к покушению, а своевременное наложение ареста на средства повышает шанс возмещения ущерба. Обновлённые процедуры, включая двухдневный «период охлаждения» и новые признаки переводов без добровольного согласия, вступающие в силу с 1 января 2026 года и учитывающие телефонные коммуникации и данные от операторов связи/мессенджеров, усиливают эту тенденцию [3]. Следовательно, квалификация и доказывание становятся тесно зависимыми от скорости межведомственного реагирования.

С учётом обозначенных проблем, совершенствование квалификации телефонных хищений в России целесообразно рассматривать не как поиск «новой статьи» о телефонном мошенничестве, а как комплекс согласованных мер в толковании, доказывании, организационном взаимодействии и, при необходимости, точечной корректировке норм. Такой подход отвечает природе феномена: телефонный канал — лишь «вход» в разные юридические механизмы хищения, и уголовный закон уже содержит инструменты для их охвата при корректном разграничении составов.

Первое направление — развитие и актуализация разъяснений Верховного Суда РФ по типовым «матрицам» телефонных сценариев. Позиции Постановления Пленума № 48 уже заложили базовую конструкцию разграничения 159/158/159.6, однако технологическая эволюция требует детализации на уровне примеров и критериев применительно к удалённому управлению устройством, перехвату одноразовых кодов, подмене реквизитов и использованию синтеза голоса (дипфейков). Практически значимым было бы

закрепление в разъяснениях алгоритма квалификации, ориентированного на три вопроса: кто совершил платёжное распоряжение (потерпевший или виновный), было ли незаконное техническое вмешательство в функционирование средств/сетей, и какой ролью обладало электронное средство платежа в момент совершения операции. Такая детализация не требует изменения закона, но снижает разнотолкование и «плавающую» практику, особенно на границе кражи с банковского счёта и мошенничества с использованием электронных средств платежа.

Второе направление — стандартизация доказывания причинной связи между обманом и имущественным результатом с учётом природы социальной инженерии. Потерпевший рассказ должен оставаться важным, но недостаточным источником: описание «обмана» необходимо привязывать к объективным данным — аудиозаписям, детализации соединений, логам мессенджеров, фишинговым доменам, следам установки и работы приложений, цифровым артефактам удалённого доступа. В научных работах социальная инженерия описывается через повторяемые приёмы («претекст», «фишинг»), что позволяет выстраивать криминалистические модели и проверяемые версии. Для уголовного процесса это означает возможность унифицировать набор «минимально необходимых» доказательств для типовых схем и тем самым повысить устойчивость квалификации в суде, а также облегчить разграничение мошенничества и кражи в тех случаях, когда коммуникация одинакова, а механизм изъятия различен.

Третье направление — точечное нормативное уточнение и «бережная» корректировка спорных зон, прежде всего связанных со ст. 159.6 УК РФ и разграничением её с кражей и мошенничеством. Учитывая научную критику «остаточного» характера 159.6 и риск расширительного толкования понятия «вмешательство», оправданным является не «переписывание» всей конструкции, а уточнение критериев через разъяснения и, при необходимости, через корректировку диспозиции либо примечаний, чтобы повысить предсказуемость применения. Например, целесообразно нормативно и/или интерпретационно подчеркнуть, что удалённый доступ сам по себе ещё не равен «вмешательству», если он не нарушает установленный процесс обработки/передачи информации, но использование вредоносных механизмов подмены реквизитов, перехвата кодов, вмешательства в сетевое взаимодействие и модификации данных должно уверенно подпадать под 159.6 при одновременной оценке совокупности со ст. 272–273 УК РФ, когда признаки этих составов доказаны[13]. Такой подход сохраняет системность «преступлений против собственности» (как её понимает доктрина) и одновременно уменьшает квалификационные коллизии.

В целом предлагаемые меры ориентированы на достижение двух взаимосвязанных целей. Первая — обеспечить предсказуемость квалификации через ясные критерии разграничения 159/159.3/158/159.6 и корректное выявление совокупности со «смежными» составами. Вторая — повысить качество доказывания за счёт раннего закрепления телеком и финтех следов, использования антифрод инфраструктуры и стандартизированных криминалистических подходов к социальной инженерии. Именно эти направления представляются наиболее реалистичными и применимыми в российских условиях, поскольку они опираются на уже существующие правовые инструменты и актуальные регуляторные механизмы.

Список литературы:

[1] Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 № 63-ФЗ (ред. от 29.12.2025) // Собрание законодательства Российской Федерации. — 1996. — № 25. — Ст. 2954. — URL: https://pravo.gov.ru/proxy/ips/?docbody=&nd=102041891 (дата обращения: 13.02.2026).

[2] 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) [Электронный ресурс] // КонсультантПлюс: справ.-правовая система. — URL: https://www.consultant.ru/document/cons_doc_LAW_283918/ (дата обращения: 13.02.2026).

[3] Об установлении признаков осуществления перевода денежных средств без добровольного согласия клиента и отмене приказа Банка России от 27 июня 2024 года № ОД-1027 : Приказ Банка России от 05.11.2025 № ОД-2506 [Электронный ресурс]. — Официальный сайт Банка России. — URL: https://cbr.ru/Crosscut/LawActs/File/10123 (дата обращения: 13.02.2026).

[4] Волженкин Б. В. Мошенничество. — СПб.: Изд-во СПб ЮИ, 1998. — 101 с.

[5] Гавриленко Н. В. Методика расследования хищений, совершенных с использованием информационно-телекоммуникационной сети «Интернет» [Электронный ресурс]. — 2025. — URL: https://vital.lib.tsu.ru/vital/access/services/Download/vital%3A22580/SOURCE01 (дата обращения: 13.02.2026).

[6] Когда банк обязан приостановить перевод на два дня, даже несмотря на согласие клиента? [Электронный ресурс] / Банк России. — URL: https://www.cbr.ru/Reception/TopicalMessage/Page/9627 (дата обращения: 13.02.2026).

[7] Лопашенко Н. А. Преступления против собственности: авторский курс: монография: в 4 кн. Кн. 1: Общетеоретическое исследование посягательств на собственность. — М.: Юрлитинформ, 2019. — 294 с.

[8] Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств. III квартал 2025 года [Электронный ресурс] / Банк России. — 13.11.2025. — URL: https://www.cbr.ru/statistics/ib/review_3q_2025/ (дата обращения: 13.02.2026).

[9] Обзор судебной практики Верховного Суда Российской Федерации № 3 (2021) (п. 49) : утв. Президиумом Верховного Суда РФ 10.11.2021 [Электронный ресурс] // КонсультантПлюс: справ.-правовая система. — URL: https://www.consultant.ru/document/cons_doc_LAW_400312/ (дата обращения: 13.02.2026).

[10] Овсюков Д. А. Корыстные преступления против собственности с использованием информационно-телекоммуникационных сетей: вопросы квалификации: монография / под науч. ред. С. М. Кочои. — М.: Проспект, 2023.

[11] Операции без добровольного согласия клиентов: итоги I квартала [Электронный ресурс] / Банк России. — 16.05.2025. — URL: https://cbr.ru/press/event/?id=24608 (дата обращения: 13.02.2026).

[12] Статистические сведения о состоянии преступности в 2025 году [Электронный ресурс] / Пресс-центр МВД России // МВД МЕДИА. — 29.01.2026. — URL: https://mvdmedia.ru/news/official/statisticheskie-svedeniya-o-sostoyanii-prestupnosti-v-2025-godu/ (дата обращения: 13.02.2026).

[13] Уголовное право России. Части общая и особенная: учебник для бакалавров / под ред. А. И. Рарога. — М.: Проспект, 2022. — 1345 с.

References:

[1] Criminal Code of the Russian Federation: Federal Law No. 13.06.1996 dated 63-FZ (as amended on 29.12.2025) //Collection of Legislation of the Russian Federation. — 1996. — № 25. - Art. 2954. - URL: https://pravo.gov.ru/proxy/ips/?docbody=&nd=102041891 (access date: 13.02.2026).

[2] On judicial practice in cases of fraud, misappropriation and embezzlement: decision of the Plenum of the Supreme Court of the Russian Federation of 30.11.2017 No. 48 (ed. 15.12.2022) [Electronic resource]//ConsultantPlus: legal system. - URL: https://www.consultant.ru/document/cons_doc_LAW_283918/ (access date: 13.02.2026).

[3] On establishing signs of funds transfer without the client's voluntary consent and canceling Bank of Russia Order No. OD-1027 dated June 27, 2024: Bank of Russia Order No. OD-2506 dated 05.11.2025 [Electronic Resource]. - Bank of Russia website. - URL: https://cbr.ru/Crosscut/LawActs/File/10123 (access date: 13.02.2026).

[4] Volzhenkin B.V. Fraud. - St. Petersburg: Publishing House of St. Petersburg YuI, 1998. - 101 s.

[5] Gavrilenko N.V. Methodology for investigating thefts committed using the information and telecommunication network "Internet" [Electronic resource]. — 2025. — URL: https://vital.lib.tsu.ru/vital/access/services/Download/vital%3A22580/SOURCE01 (дата обращения: 13.02.2026).

[6] When is the bank obliged to suspend the transfer for two days, even despite the client's consent? [Electronic resource]/Bank of Russia. - URL: https://www.cbr.ru/Reception/TopicalMessage/Page/9627 (access date: 13.02.2026).

[7] Lopashenko N. A. Crimes against property: author's course: monograph: in 4 books. Kn. 1: General theoretical study of property infringements. - M.: Yurlitinform, 2019. - 294 p.

[8] Overview of information security incident reporting for funds transfers. Q3 2025 [Electronic Resource]/Bank of Russia. - 13.11.2025. - URL: https://www.cbr.ru/statistics/ib/review_3q_2025/ (access date: 13.02.2026).

[9] Review of judicial practice of the Supreme Court of the Russian Federation No. 3 (2021) (clause 49): approved by Presidium of the Supreme Court of the Russian Federation 10.11.2021 [Electronic resource]//ConsultantPlus: legal system. - URL: https://www.consultant.ru/document/cons_doc_LAW_400312/ (access date: 13.02.2026).

[10] Ovsyukov D.A. Mercenary crimes against property using information and telecommunication networks: qualification issues: monograph/scientific. ed. S. M. Kochoi. - M.: Prospect, 2023.

[11] Transactions without voluntary consent of clients: results of the first quarter [Electronic resource]/Bank of Russia. - 16.05.2025. - URL: https://cbr.ru/press/event/?id=24608 (access date: 13.02.2026).

[12] Statistical information on the state of crime in 2025 [Electronic resource]/Press center of the Ministry of Internal Affairs of Russia//Ministry of Internal Affairs MEDIA. — 29.01.2026. — URL: https://mvdmedia.ru/news/official/statisticheskie-svedeniya-o-sostoyanii-prestupnosti-v-2025-godu/ (дата обращения: 13.02.2026).

[13] Russian criminal law. The parts are general and special: a textbook for bachelors/ed. A.I. Raroga. - M.: Prospect, 2022. - 1345 s.