

Дата поступления рукописи в редакцию: 22.11.2025 г.
Дата принятия рукописи в печать: 14.12.2025 г.

DOI: 10.24412/2076-1503-2025-11-649-655

АЛЕШКО Борислав Евгеньевич,
студент 4 курса юридического факультета
Финансового университета при Правительстве РФ,
e-mail: bakin-yes@yandex.ru

Научный руководитель:
БЕЛОУСОВ Андрей Леонидович,
доцент кафедры правового регулирования
экономической деятельности
Финансового университета
при Правительстве РФ,
e-mail: ALBelousov@fa.ru

ОТВЕТСТВЕННОСТЬ БАНКОВ ЗА ДЕЙСТВИЯ ТЕЛЕФОННЫХ МОШЕННИКОВ (СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ): ПРОБЛЕМЫ ПРАВОПРИМЕНЕНИЯ

Аннотация. Статья посвящена комплексному анализу проблем привлечения коммерческих банков к гражданско-правовой ответственности за финансовые потери клиентов, вызванные применением методов социальной инженерии. Актуальность темы обусловлена ростом киберпреступности и недостаточной эффективностью существующих механизмов правовой защиты. В работе исследуются действующие нормы гражданского и банковского законодательства, регулирующие обязанности банков по защите средств на счетах. В результате исследования формулируются конкретные предложения по совершенствованию законодательства и правоприменительной практики. Предложенные меры направлены на усиление защиты прав потребителей банковских услуг, установление справедливого баланса интересов сторон и укрепление безопасности национальной платежной системы.

Ключевые слова: банковское право, ответственность банков, социальная инженерия, телефонное мошенничество, защита прав потребителей, договор банковского счета, необоснованное списание, судебная практика, возмещение ущерба.

ALESHKO Borislav Evgenievich,
A fourth-year law student
at the Financial University under the Government
of the Russian Federation

Scientific supervisor:
BELOUSOV Andrey Leonidovich,
Associate Professor,
Department of Legal Regulation of Economic Activity
Financial University under the Government
of the Russian Federation

BANKS' LIABILITY FOR TELEPHONE FRAUD (SOCIAL ENGINEERING): ENFORCEMENT PROBLEMS

Annotation. This article provides a comprehensive analysis of the challenges of holding commercial banks civilly liable for customer financial losses caused by the use of social engineering techniques. The topic is relevant given the rise of cybercrime and the ineffectiveness of existing legal protection mechanisms. The paper examines current civil and banking legislation governing banks' obligations to protect account funds. The study formulates specific proposals for improving legisla-

tion and law enforcement practices. The proposed measures are aimed at strengthening consumer protection for banking services, establishing a fair balance between the interests of the parties, and strengthening the security of the national payment system.

Key words: *banking law, bank liability, social engineering, telephone fraud, consumer protection, bank account agreement, unjustified write-off, judicial practice, compensation for damages.*

Введение

Актуальность темы исследования обусловлена беспрецедентным ростом киберпреступности в банковской сфере, представляющей прямую угрозу финансовой безопасности граждан и стабильности национальной платежной системы. Ключевым инструментом злоумышленников сегодня выступают методы социальной инженерии — психологические манипуляции, направленные на то, чтобы жертва добровольно раскрыла конфиденциальную информацию или совершила перевод денежных средств. Масштаб проблемы наглядно демонстрирует официальная статистика

Банка России: в 2024 году объем операций, совершенных без согласия клиентов, увеличился по сравнению с 2023 годом на 74,36%, достигнув почти 27,5 млрд рублей [11]. При этом, как отмечается в криминологических исследованиях, подавляющее большинство таких хищений совершается именно с применением социальной инженерии [10]. Особую тревогу вызывает тот факт, что доля возвращенных клиентам похищенных средств в 2024 году составила всего 9,9% [11], что свидетельствует о системных пробелах в механизмах правовой защиты потребителей банковских услуг.

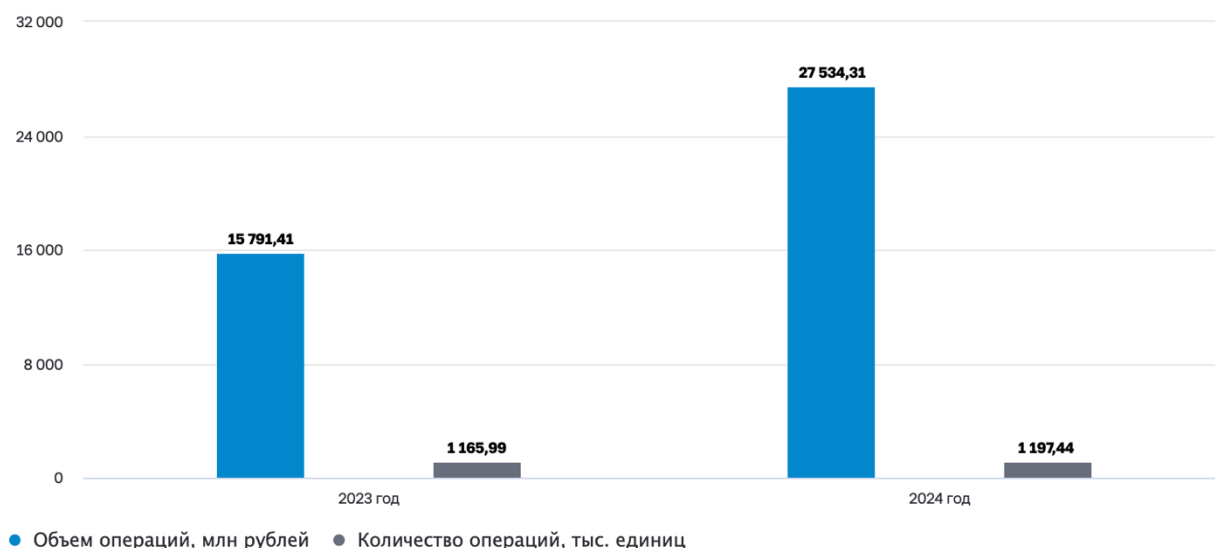


Рисунок 1. Динамика общего объема и количества операций без добровольного согласия клиентов за период 2023 – 2024 гг.

Научная проблема исследования заключается в глубоком противоречии между формальным соблюдением банком законодательства и наличием порока воли у клиента, действующего под влиянием обмана. С одной стороны, кредитная организация исполняет надлежащим образом оформленное распоряжение клиента, действуя в соответствии со статьями 847 и 854 Гражданского кодекса РФ (далее ГК РФ). С другой стороны, такое волеизъявление клиента не является свободным, а на банке, как на профессиональном участнике, лежит обязанность по обеспечению безопасности операций и противодействию мошенничеству, закрепленная в статье 9 Феде-

рального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе» (далее – ФЗ «О НПС») [2]. Существующая правовая неопределенность в разграничении «грубой неосторожности» клиента и недостаточной эффективности банковских антифрод-систем порождает неоднородную судебную практику и ставит под вопрос справедливое распределение рисков.

Целью настоящей статьи является комплексный анализ проблем правоприменения в сфере ответственности банков за финансовые потери клиентов от действий телефонных мошенников и разработка предложений по совершенствованию действующего законодательства.

Для достижения поставленной цели необходимо решить следующие задачи:

- исследовать правовую природу социальной инженерии как способа совершения противоправных действий в банковской сфере;
- проанализировать действующие нормы гражданского и банковского законодательства, регулирующие обязанности банков по обеспечению безопасности операций по счетам клиентов;
- систематизировать и проанализировать актуальную судебную практику по спорам о возмещении ущерба, причиненного в результате мошеннических списаний;
- выявить ключевые проблемы правового регулирования и предложить пути их решения для установления справедливого баланса интересов сторон.

Правовая квалификация ответственности коммерческих банков за списание денежных средств со счетов клиентов в результате мошеннических действий основывается на совокупности норм гражданского, банковского и специального законодательства, регулирующего национальную платежную систему. Фундаментальной основой правоотношений между банком и клиентом выступает договор банковского счета, в соответствии с которым банк обязуется принимать и зачислять поступающие на счет клиента денежные средства, выполнять распоряжения клиента о перечислении и выдаче соответствующих сумм со счета и проведении других операций по счету (ст. 845 ГК РФ) [1]. Ключевым принципом, закрепленным в статье 854 ГК РФ, является недопустимость списания денежных средств со счета без распоряжения клиента. Ответственность банка за ненадлежащее совершение операций по счету предусмотрена статьей 856 ГК РФ, а общие принципы ответственности за нарушение обязательств, основанные на начале вины, установлены статьей 401 ГК РФ [1].

Однако общие положения ГК РФ получают свою конкретизацию в специальном законодательстве. Центральное место в регулировании рассматриваемых отношений занимает ФЗ «О НПС» [2]. Именно статья 9 данного закона устанавливает особый порядок рассмотрения споров о возврате денежных средств, списанных без согласия клиента. Закон возлагает на банк ряд императивных обязанностей: незамедлительно информировать клиента о совершении каждой операции, а также обеспечить возможность направления клиентом уведомления о несанкционированном списании. В случае своевременного уведомления со стороны клиента банк обязан возместить сумму операции, если не докажет, что

клиент нарушил порядок использования электронного средства платежа, что повлекло совершение несанкционированной операции. Таким образом, ФЗ «О НПС» устанавливает опровержимую презумпцию ответственности банка, переноса на него бремя доказывания вины клиента.

Как отмечается в юридической доктрине, целью введения данных норм являлось обеспечение баланса интересов сторон договора об использовании электронного средства платежа и усиление защиты клиента как экономически более слабой стороны [6; 7].

Применение указанных норм сталкивается со значительными сложностями в условиях использования мошенниками методов социальной инженерии. В криминологической и правовой доктрине под социальной инженерией понимается совокупность психологических и манипулятивных приемов, направленных на получение неправомерного доступа к конфиденциальной информации или побуждение человека к совершению определенных действий [11;12]. В отличие от технического взлома, социальная инженерия использует человеческие слабости: доверие, страх, невнимательность, используя заранее подготовленные сценарии (претекстинг) для введения жертвы в заблуждение [7;8;9].

С юридической точки зрения, это порождает ключевую коллизию: разграничение понятий «операция без согласия клиента» и «операция с согласием клиента, данным под влиянием обмана». Формально клиент совершает все необходимые действия для подтверждения транзакции: вводит пароли, сообщает коды из СМС-сообщений, тем самым выражая свое распоряжение банку. Именно на этом основывается основная линия защиты кредитных организаций в судах. Однако такое волеизъявление является дефектным, поскольку оно сформировано не свободно, а в результате целенаправленных противоправных действий третьих лиц. Таким образом, центральной проблемой правоприменения становится определение того, является ли юридически ничтожным согласие, данное под влиянием обмана, и должен ли банк как профессиональный участник оборота, оснащенный современными системами мониторинга (антифрод-системами), распознавать и пресекать такие подозрительные операции. Именно от ответа на этот вопрос зависит распределение финансовой ответственности за причиненный ущерб.

Анализ правоприменительной практики имеет ключевое значение для понимания реального действия правовых норм об ответственности банков, поскольку именно в судебных решениях происходит толкование законодательных положений.

ний и их адаптация к сложным фактическим обстоятельствам, связанным с социальной инженерией. Судебная практика по данной категории дел в последние годы претерпевает существенную трансформацию, смещая фокус с формальной констатации действий клиента на комплексную оценку поведения банка как профессионального участника платежной системы.

Центральным вопросом в спорах данной категории является распределение бремени доказывания. Несмотря на то, что кредитные организации зачастую строят свою защиту на утверждении о нарушении клиентом порядка использования электронного средства платежа, суды все чаще исходят из положений части 15 статьи 9 ФЗ «О НПС» [2].

Согласно данной норме, именно на банк возлагается обязанность доказать, что действия клиента повлекли совершение операции без его согласия. При этом, как показывает практика, суды не ограничиваются формальным установлением факта передачи клиентом кодов или паролей, а требуют от банка доказательств того, что он, в свою очередь, действовал добросовестно и предпринял все необходимые меры для обеспечения безопасности операции.

Ключевые факторы, влияющие на исход дела, наиболее полно раскрываются в недавней практике Верховного Суда Российской Федерации. Суды высшей инстанции последовательно возлагают на банки повышенные стандарты осмотрительности, требуя анализировать не только формальное подтверждение операции, но и ее существенные характеристики. Показательным является Определение ВС РФ от 08.07.2025 N 45-КГ25-7-К7, где была отменена серия судебных актов в пользу банка [4]. Верховный Суд указал, что нижестоящие инстанции не дали оценки тому факту, что за короткий промежуток времени были совершены абсолютно нетипичные для клиента операции: вход в систему с нового устройства, досрочное закрытие вклада, открытие одиннадцати новых цифровых карт и снятие всех денежных средств в банкоматах в другом городе. Особо было отмечено, что антифрод-система банка сработала и заблокировала операции, однако сотрудник банка снял блокировку после звонка мошенников, которые прошли лишь формальную аутентификацию. ВС РФ подчеркнул, что в такой ситуации банк должен был предпринять повышенные меры предосторожности, чтобы убедиться в подлинности волеизъявления клиента.

Аналогичный подход демонстрируется и в делах, где мошеннические действия совершаются после физической кражи телефона и банковских карт. В апелляционном определении Свердлов-

ского областного суда по делу N 33-5048/2025 суд указал, что сам факт хищения не свидетельствует о нарушении клиентом порядка использования карт [3]. Ключевым фактором для возложения ответственности на банк стало то, что его антифрод-система зафиксировала подозрительные операции и приостановила их, однако в дальнейшем они были возобновлены без надлежащей идентификации клиента (например, без запроса кодового слова). Суд отметил, что банк, предлагая дистанционные услуги, обязан обеспечить их безопасность, чего в данном случае сделано не было.

Особую категорию составляют споры о кредитных договорах, заключенных от имени клиента мошенниками. Здесь судебная практика, вплоть до высшей инстанции, также исходит из необходимости защиты гражданина. В Определении ВС РФ от 09.09.2025 N 5-КГ25-102-К2 был признан недействительным кредитный договор, заключенный через мобильное приложение [5]. Верховный Суд раскритиковал подход нижестоящих судов, которые сочли достаточным формальное подтверждение операции СМС-кодом. Суд указал, что упрощенный порядок предоставления кредита не должен нивелировать гарантии прав потребителя, а банк обязан убедиться, что намерение заключить договор исходит от надлежащего лица. Было отмечено, что в ситуации, когда кредит оформляется и немедленно перечисляется на счета третьих лиц, банк должен проявлять повышенную осмотрительность. Фактически, ВС РФ подтвердил наличие у банка обязанности по анализу нетипичности операций и противодействию мошенническим схемам даже на стадии заключения договора.

Вместе с тем, судебная практика исходит из того, что в случае доказанной грубой неосторожности со стороны самого клиента в удовлетворении иска может быть отказано. К таким случаям, как правило, относится установка клиентом по указанию мошенников программ удаленного доступа (например, AnyDesk), что фактически передает полный контроль над устройством третьим лицам и нивелирует любые меры защиты со стороны банка.

Таким образом, анализ судебной практики свидетельствует о формировании устойчивой тенденции: суды возлагают на банки повышенные требования к обеспечению безопасности операций. Ответственность кредитной организации наступает не только при технических сбоях, но и в случае ее пассивности и неспособности выявить и пресечь операции, обладающие явными признаками мошенничества, даже если формально они были подтверждены аутентификационными данными клиента.

Проведенный анализ законодательства и судебной практики позволяет выявить ряд системных проблем, которые препятствуют эффективной защите прав потребителей банковских услуг и создают правовую неопределенность. Несмотря на усиливающуюся тенденцию судебной практики к защите прав потребителей банковских услуг, существующее правовое регулирование не в полной мере отвечает на вызовы, создаваемые современными методами социальной инженерии.

Во-первых, ключевой проблемой является отсутствие в законодательстве четких критериев «грубой неосторожности» клиента. Данная категория является оценочной, что приводит к формированию неоднородной судебной практики и ставит решение по делу в зависимость от субъективного судейского усмотрения. Действия клиента, такие как передача СМС-кода, в одном случае могут быть расценены как достаточное основание для отказа в иске, в то время как в другом суде аналогичные обстоятельства будут оценены критически с учетом всех факторов, включая поведение банка. Такая неопределенность снижает предсказуемость правосудия и не позволяет выработать единый стандарт поведения как для банков, так и для их клиентов.

Во-вторых, серьезным препятствием для защиты прав потребителя является непрозрачность работы банковских антифрод-систем.

В судебном процессе клиент находится в заведомо более слабом положении, поскольку он не имеет доступа к информации о том, как именно система мониторинга банка отреагировала на оспариваемую операцию. Банк может утверждать, что операция не была расценена как подозрительная, и у клиента практически нет возможности опровергнуть это утверждение. Данное информационное неравенство существенно затрудняет доказывание вины банка в ненадлежащем оказании услуги по обеспечению безопасности счета.

В-третьих, механизм возврата похищенных средств остается крайне неэффективным. Как показывают данные Банка России, доля возвращенных средств пострадавшим составляет менее 10% от общего объема хищений [11]. Даже в случае признания судом ответственности банка или установления факта мошенничества, денежные средства, как правило, уже выведены со счетов подставных лиц («дропперов») и обналичены, что делает их фактический возврат практически невозможным.

Для решения обозначенных в исследовании проблем предлагается реализовать следующие меры по совершенствованию законодательства и правоприменительной практики:

1. Усилить ответственность банков за переводы на счета подставных лиц, внося в ФЗ «О национальной платежной системе» норму об опровержимой презумпции вины банка при осуществлении перевода на счет, находящийся в базе данных ЦБ РФ о дропперах.
2. Законодательно закрепить обязанность банков применять усиленные методы аутентификации (видеоидентификация, обязательный подтверждающий звонок) при совершении операций с признаками нетипичности (например, перевод всей суммы сразу после получения кредита), чтобы нивелировать риски, связанные с пороком воли клиента.
3. Инициировать принятие Постановления Пленума Верховного Суда РФ, посвященного спорам о защите прав потребителей финансовых услуг. В нем необходимо разъяснить судам критерии разграничения простой и грубой неосторожности клиента, а также определить стандарты доказывания для банков в части эффективности их систем управления рисками.
4. Сформировать судебную практику, преодолевающую информационное неравенство сторон. Для этого на кредитные организации следует возложить процессуальную обязанность по запросу суда предоставлять детализированные отчеты о работе антифрод-систем по конкретной операции, что позволит объективно оценить действия банка.

Комплексная реализация данных предложений позволит повысить уровень правовой защищенности граждан, установить справедливый баланс ответственности между банками и их клиентами, а также будет способствовать укреплению безопасности национальной платежной системы.

Проведенное исследование проблемы ответственности банков за действия телефонных мошенников позволяет сделать следующие ключевые выводы:

5. Основная правовая коллизия заключается в противоречии между формально законным распоряжением клиента, данным под влиянием обмана, и обязанностью банка как профессионального участника обеспечивать безопасность операций. Это создает правовую неопределенность и приводит к неоднородной судебной практике.
6. Анализ судебной практики показывает формирование устойчивой тенденции по возложению на кредитные организации повышенных стандартов осмотрительности. Суды все чаще признают пассивное исполнение подо-

зрительных операций ненадлежащим оказанием банковской услуги, даже при формальном подтверждении со стороны клиента.

7. Главный вывод исследования — назрела необходимость смещения баланса ответственности в сторону банков как сильной стороны договора, обладающей необходимыми техническими и аналитическими ресурсами для эффективного противодействия мошенничеству.

Таким образом, предложенные в работе меры по совершенствованию законодательства и правоприменительной практики направлены на создание более справедливого механизма распределения рисков. Это не только усилит защиту прав конкретных пострадавших, но и будет способствовать повышению стабильности национальной платежной системы и укреплению доверия граждан к финансовым институтам.

Список литературы:

[1] Гражданский кодекс Российской Федерации (часть вторая): Федер. закон от 26.01.1996 № 14-ФЗ // Собрание законодательства РФ. 1996. № 5. Ст. 410.

[2] Федеральный закон о национальной платежной системе: Федер. закон от 27.06.2011 № 161-ФЗ // Собрание законодательства РФ. 2011. № 27. Ст. 3872.

[3] Апелляционное определение Свердловского областного суда от 25.04.2025 по делу № 33-5048/2025 // СПС «КонсультантПлюс».

[4] Определение Судебной коллегии по гражданским делам Верховного Суда Российской Федерации от 08.07.2025 N 45-КГ25-7-K7 // СПС «КонсультантПлюс».

[5] Определение Судебной коллегии по гражданским делам Верховного Суда Российской Федерации от 09.09.2025 N 5-КГ25-102-K2 // СПС «КонсультантПлюс».

[6] Борисов А. Н. Комментарий к Федеральному закону от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе» (постатейный). 3-е изд., перераб. и доп. М.: Юстицинформ, 2025.

[7] Белоусов, А. Л. Обращение взыскания на единственное жилье как способ обеспечения исполнения обязательств должником / А. Л. Белоусов // Финансы и кредит. — 2017. — Т. 23, № 20(740). — С. 1173-1183.

[8] Зотина Е. В. Претекстинг как прием социальной инженерии, используемый телефонными мошенниками: криминологический взгляд на проблему // Вестник Казанского юридического института МВД России. 2022. Т. 13, № 4 (50). С. 93–99.

[9] Конорев А. М. Исследование проблемы использования технологии социальной инженерии в банковской сфере // Политика, экономика и инновации. 2022. № 4 (45).

[10] Копылов В. В., Прокофьев О. М., Калюшина Ю. С. Особенности совершения дистанционных хищений денежных средств граждан с использованием метода социальной инженерии // Вестник Московского университета МВД России. 2022. № 3. С. 126–131.

[11] Обзор операций, совершенных без согласия клиентов финансовых организаций в 2024 году [Электронный ресурс]. (дата обращения: 21.10.2025).

[12] Старостенко Н. И. Понятие и виды методов социальной инженерии, применяемых при совершении преступлений в сфере информационно-телекоммуникационных технологий // Вестник Нижегородской академии МВД России. 2023. № 1 (61). С. 152–159.

[13] Шастина А. Р. Социальная инженерия в структуре киберпреступности: к вопросу о противодействии телефонному мошенничеству // Аграрное и земельное право. 2024. № 9(237). С. 300-302.

References:

[1] Civil Code of the Russian Federation (part two): Feder. Law of 26.01.1996 No. 14-FZ//Collection of Legislation of the Russian Federation. 1996. № 5. Art. 410.

[2] Federal Law on the National Payment System: Feder. Law of 27.06.2011 No. 161-FZ//Collection of Legislation of the Russian Federation. 2011. № 27. Art. 3872.

[3] Appeal ruling of the Sverdlovsk Regional Court of 25.04.2025 in case No. 33-5048/2025//SPS "ConsultantPlus."

[4] Determination of the Judicial Collegium for Civil Cases of the Supreme Court of the Russian Federation of 08.07.2025 No. 45-KG25-7-K7//SPS ConsultantPlus.

[5] Determination of the Judicial Collegium for Civil Cases of the Supreme Court of the Russian Federation of 09.09.2025 N 5-KG25-102-K2//SPS ConsultantPlus.

[6] Borisov A. N. Commentary to the Federal Law of June 27, 2011 No. 161-FZ "On the National Payment System" (itemized). 3rd ed., Revised and add. M.: Justicinform, 2025.

[7] Belousov, A. L. Foreclosure on the only housing as a way to ensure the fulfillment of obligations by the debtor/A. L. Belousov//Finance and credit. — 2017. - Т. 23, NO. 20 (740). - S. 1173-1183.

[8] Zotina E.V. Pretexting as a social engineering technique used by telephone scammers: a criminological view of the problem//Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia. 2022. T. 13, NO. 4 (50). S. 93-99.

[9] Konorev A.M. Research on the use of social engineering technology in the banking sector//Politics, economics and innovation. 2022. № 4 (45).

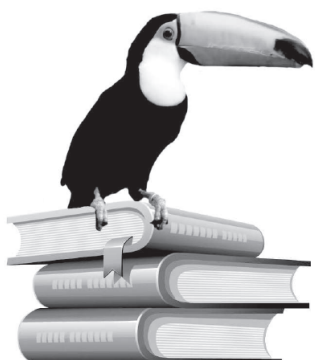
[10] Kopylov V.V., Prokofiev O.M., Kaloshina Yu. S. Features of remote embezzlement of citizens' funds using the method of social engineering//Bulletin of Moscow University of the Ministry of Internal Affairs of Russia. 2022. № 3. S. 126-131.

[11] Overview of transactions performed without the consent of clients of financial institutions in 2024 [Electronic resource]. (accessed on: 21.10.2025).

[12] Starostenko N.I. Concept and types of social engineering methods used in committing crimes in the field of information and telecommunication technologies//Bulletin of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia. 2023. № 1 (61). S. 152-159.

[13] A. Shastina. Social engineering in the structure of cybercrime: on the issue of countering telephone fraud//Agrarian and land law. 2024. № 9(237). S. 300-302.





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