УГОЛОВНО-ПРАВОВЫЕ НАУКИ/CRIMINAL LAW SCIENCES

DOI: https://doi.org/10.60797/IRJ.2025.162.69

РЕТРОСПЕКТИВНЫЙ АНАЛИЗ СПОСОБОВ МОШЕННИЧЕСТВА, СОВЕРШЕННОГО С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ, КАК ЭЛЕМЕНТА КРИМИНАЛИСТИЧЕСКОЙ ХАРАКТЕРИСТИКИ ПРЕСТУПЛЕНИЯ

Научная статья

Богацкая У.И.[1, *]

[1] ORCID : 0009-0009-4698-6403;

[1] СУ УМВД России по Красносельскому району г. Санкт-Петербурга, Санкт-Петербург, Российская Федерация

* Корреспондирующий автор (mitrofanova.ulyana2016[at]yandex.ru)

Аннотация

Криминалистическая характеристика способов мошенничества, совершенного с использованием информационных и телекоммуникационных технологий, играет ключевую роль в обеспечении системного подхода к раскрытию и предупреждению преступлений. Проведенный анализ ранних классических способов совершения мошенничества выявил, какие изменения с ними произошли в сравнении с новыми способами адаптированными к современным методам борьбы с мошенничеством, осуществлённым с использованием информационных и телекоммуникационных технологий. Теоретические и практические аспекты рассмотрены с учетом трансформации и эволюции способов совершения мошенничества.

Методологическую основу исследования составил диалектический метод познания, позволяющий всесторонне и объективно рассмотреть проблематику способов совершения мошенничества. Системно-структурный метод при анализе разрозненного нормативного материала позволил обобщить полученные сведения. Метод контент-анализа публикаций СМИ применялся при исследовании новейших и современных способов совершения мошенничества. Научная новизна исследования заключается в формулировании на основе комплексного анализа уголовного законодательства и правоприменительной практики взглядов на способы мошенничества, совершенного с использованием информационных и телекоммуникационных технологий.

Автором сделан вывод о том, злоупотребление доверием не является самостоятельным способом совершения мошенничества с использованием ИТТ, поскольку вышеуказанные преступления совершаются лицом, которое никогда не было знакомо с потерпевшим. Мошенничество совершается при личном контакте (контактное мошенничество), в случае участия курьеров и без личного контакта с потерпевшим (дистанционное мошенничество). Говорить в таком случае о злоупотреблении доверием не приходится, поскольку отсутствует длительное знакомство виновного с потерпевшим. Проведенный анализ ранних классических способов совершения мошенничества выявил, какие изменения с ними произошли в сравнении с новыми способами, адаптированными к современным методам борьбы с мошенничеством.

Ключевые слова: криминалистическая характеристика, мошенничество, способ преступления, информационные телекоммуникационные технологии, обман, злоупотребление доверием, хищение, фишшинг, сим-своппинг, дроппер.

RETROSPECTIVE ANALYSIS OF METHODS OF FRAUD COMMITTED USING INFORMATION AND TELECOMMUNICATIONS TECHNOLOGIES AS AN ELEMENT OF THE CRIMINALISTIC PROFILE OF A CRIME

Research article

Bogackaya U.I.[1, *]

[1] ORCID : 0009-0009-4698-6403;

[1] Investigative Department of the Ministry of Internal Affairs of Russia for the Krasnoselsky district of St. Petersburg, Saint-Petersburg, Russian Federation

* Corresponding author (mitrofanova.ulyana2016[at]yandex.ru)

Abstract

The criminalistic profile of methods of fraud committed using information and telecommunications technologies plays a key role in ensuring a systematic approach to the detection and prevention of crimes. An analysis of early classic methods of fraud has identified the changes that have occurred in comparison with new methods adapted to modern methods of combating fraud committed using information and telecommunications technologies. Theoretical and practical aspects are reviewed, taking into account the transformation and evolution of fraud methods.

The methodological basis of the study was the dialectical method of cognition, which allows for a comprehensive and objective examination of the issues surrounding methods of fraud. The systemic-structural method used in the analysis of fragmented normative material made it possible to generalise the information obtained. The content analysis method of media publications was used to study the latest and most modern methods of committing fraud. The scientific novelty of the research lies in the formulation, based on a comprehensive analysis of criminal legislation and law enforcement practice, of views on methods of fraud committed using information and telecommunications technologies.

The author concludes that abuse of trust is not an independent method of committing fraud using ITT, since the above crimes are committed by a person who has never been acquainted with the victim. Fraud is committed through personal contact (contact fraud), with the involvement of couriers and without personal contact with the victim (remote fraud). In such cases,

there is no question of abuse of trust, since the perpetrator has no long-standing acquaintance with the victim. An analysis of early classic methods of fraud has highlighted the changes that have taken place in comparison with new methods adapted to modern anti-fraud techniques.

Keywords: criminal profile, fraud, method of crime, information and telecommunications technologies, deception, breach of trust, theft, phishing, SIM swapping, dropper.

Введение

Развитие инновационных технологий и их активное внедрение в повседневную деятельность организаций и граждан стали неотъемлемой их частью, изменяя привычные сферы и создавая новые возможности. Однако доступность, комфорт и скорость получения различного рода услуг влияют на скорость темпа внедрения информационных технологий. Нельзя забывать, что новые технологии несут и новые угрозы — киберриски. С развитием технологий риски становятся сложнее и масштабнее, в последующем приводят к потере данных и нарушению их конфиденциальности, причинению имущественного и репутационного ущерба. Признание киберрисков неотъемлемой частью прогресса позволит их минимизировать путем регулярного обучения, обновления систем, установлением многоуровневой защиты. Выявление и анализ угроз онлайн, принятие комплексных решений помогут снизить уровень и количество потенциальных угроз.

Ключевую роль в обеспечении системного подхода к раскрытию и предупреждению преступлений занимает криминалистическая характеристика. Криминалистическая характеристика позволяет выявлять закономерности и систематизировать данные о преступлении, определять тактику расследования и прогнозировать действия преступника.

О.В. Волхова в своем труде писала, что «проблема борьбы с мошенничеством стала в последнее десятилетие одной из весьма актуальных проблем» [1]. По прошествии двадцати лет феномен мошенничества продолжает выступать предметом дискуссий и непрекращающегося научного интереса как среди ученых-теоретиков, так и правоприменителей.

Анализ актуальных данных о состоянии преступности в России за 2024 год показал, что, как и прежде, значимое положение (это больше половины всех зарегистрированных преступлений 50,5%) продолжают составлять хищения чужого имущества. При этом, проводя анализ структуры хищений, ее основу составляют хищения, совершенные путем кражи — 499,6 тыс., и мошенничества — 445,7 тыс., на второй план уходят хищения, совершенные путем грабежа — 17,6 тыс., и разбоя – 2,8 тыс [2]. При этом сумма ущерба по оконченным и приостановленным уголовным делам о «дистанционных хищениях» (из числа находившихся в производстве) за 2024 год составила более 197,5 млрд. рублей (в 2023 году — 133 млрд. рублей). В 2024 году объем операций без добровольного согласия клиентов увеличился по сравнению с 2023 годом на 74,4 % и составил 119 млн. на общую сумму 27,5 млрд. рублей [3].

Основные результаты и обсуждение

В рамках исследования внимание уделяется одному из признаков объективной стороны — способу совершения преступления. В криминалисте способ понимается как средство установления механизма преступления, а в уголовном процессе — как предмет доказывания. Способом совершения мошенничества является обман и злоупотребление доверием. В научной литературе уже много лет ведется дискуссия по поводу разграничения данных понятий. Важный момент заключается в том, что и обман, и злоупотребление доверием представляют собой акт человеческого поведения. Оба понятия раскрыты законодателем в разъяснении Пленума Верховного Суда РФ [4]. При этом, условно существующие в науке определения обмана и злоупотребления доверием, можно разделить на два наиболее популярных направления. Первое направление — это мнение о том, что злоупотребление доверием является самостоятельным способом совершения мошенничества. Второе определение заключатся в том, что злоупотребление доверием рассматривают как одну из разновидностей обмана.

Так, А.А. Красикова считает, что мошенничество может совершаться только одним способом — это обман [5]. По этому поводу дискуссии в научных кругах ведутся по настоящее время. С одной стороны, злоупотребление доверием не рассматривают как самостоятельный способ мошенничества, с другой стороны, обман и злоупотребление доверием рассматривают как существенно отличающиеся друг от друга самостоятельные способы совершения хищения. В.К. Барчук в работе отмечает, что нередко при совершении мошенничества вышеуказанные способы реализуются одновременно, в связи с чем у многих авторов может сложиться мнение, что данные понятия тождественные, и обман также включает в себя злоупотребление доверием. При этом с практической точки зрения такой способ, как обман, является наиболее распространённым. В качестве аргумента В.К. Барчук приводит факт возможности совершения мошенничества только путем злоупотребления доверием [6]. Н.А. Лопашенко рассматривает злоупотребление доверием как самостоятельный способ совершения мошенничества, при этом проводя отдельную классификацию преступного поведения при совершении преступлений указанным способом [7]. Б.В. Волженкин полагает, что злоупотребление доверием в цифровой среде требует отдельной уголовно-правовой оценки, что находит отклик в научной среде.

Несмотря на то, что законодатель проводит разграничение данных понятий, аргументы, поддерживающие такую позицию, не представляются весьма убедительными. Б.В. Волженкин полагает, что доверие может существовать впоследствии родственных или дружеских отношений, длительного знакомства и сотрудничества, либо при наличии положительных рекомендаций и характеристик, гарантийных обязательств, служебного положения [8]. Если первая часть утверждения понятна и не требует разъяснений, то вторая часть высказывания вызывает ряд вопросов. Так, наличие положительной рекомендации само по себе не может служить началом доверительных отношений. На наш взгляд, положительная рекомендация может послужить началом доверительных отношений между людьми в процессе их взаимодействия только в случае, если она была дана лицом, с которым у потерпевшего были доверительные отношения или он является для него авторитетом. Положительная рекомендация или характеристика может быть

подложным документом, в таком случае действия лица по отношению к потерпевшему стоит расценивать как обман, поскольку сведения, указанные в таком документе, будут ложными. Отдельно стоит обратить внимание на служебное положение как к составляющей злоупотребления доверием. При совершении мошенничества виновный зачастую осуществляет звонок и представляется сотрудником государственных органов, государственных и коммерческих организаций, при этом таковым не является. Это позволяет мошеннику привлечь и удерживать внимание жертвы, доверять и ответственно относиться к информации, которую он сообщит, тем самым формируя у потерпевшего ошибочное восприятие и осмысления ситуации в целом. Поэтому обман может выступать не только способом изъятия или обращения чужого имущества в пользу виновного, но и способом завладения конфиденциальной информацией, которая в последующем используется в преступных целях.

Рассматривая способ совершения мошенничества, совершенного с использованием информационных и телекоммуникационных технологий, стоит отметить, что такой способ как злоупотребление доверием уходит на второй план. Мошенничества с использованием ИТТ, как правило, совершаются лицом, которое никогда не было знакомо с потерпевшим. Мошенничество совершается при личном контакте (контактное мошенничество), в случае участия курьеров и без личного контакта с потерпевшим (дистанционное мошенничество). Говорить в таком случае о злоупотреблении доверием не приходится, поскольку отсутствует длительное знакомство виновного с потерпевшим.

Бадзарадзе Г.Д., рассматривая дискуссионные вопросы установления места совершения мошенничества, осуществленного с использованием информационных технологий, указывает на взаимосвязь способа совершения преступления и его предмета, характера оставляемых при этом следов, проводя анализ системы мест, которые можно считать местом совершения подобных мошенничеств, в криминалистическом смысле [9].

Анализ обмана как способа совершения мошенничества показал, что с учетом исторического развития рыночных отношений, внедрения ИТТ во все сферы жизни, произошла трансформация самых ранних способов мошенничества, послуживших основой для многих мошеннических схем, которые смогли адаптироваться к современным реалиям с учетом противодействия со стороны государства и правоохранительных органов.

Так, с появлением сети «Интернет» и распространением использования массовых рассылок по электронной почте одной из ранних мошеннических схем являлись «нигерийские письма» с просьбой оказать помощь в переводе наследства за вознаграждение. Современными распространенными формами мошенничества выступают фишшинг (создание поддельных веб-сайтов, отправление писем с фишинговыми ссылками) [10]. С 2023 года мошенники активно используют ChatGPT, передовые технологии искусственного интеллекта позволяют генерировать убедительные тексты писем, реклам с использованием реквизитов, печатей и штампов государственных организаций, что повышает доверие со стороны потерпевшего.

Сначала функционирования единого портала государственных и муниципальных услуг Российской Федерации, предоставляющего гражданам доступ к широкому сектру услуг в цифровом формате, мошенники стали активно использовать данную платформу в своих преступных схемах. Установление личности и местонахождения лиц, совершивших преступление вышеуказанным способом, представляет особую сложность. Так, Канавинским районным судом г. Н.Новгорода 06.12.2024 вынесен приговор в отношении группы лиц, действующей по предварительному сговору за совершение преступлений, предусмотренных ч. 2 ст. 159 УК РФ (5 эпизодов преступной деятельности), ч.3 ст.30 ч.2 ст. 159 УК РФ (11 эпизодов преступной деятельности), при этом лица, которым отводилась роль в приискании личных данных граждан, имеющих положительную и перспективную кредитную историю, хищении указанных личных данных путем осуществления взлома личных кабинетов физических лиц на Едином портале государственных и муниципальных услуг Российской Федерации, подделке при помощи графических редакторов документов — фотографий паспортов с внесением в них изменений о личности гражданина, предоставления логинов и паролей в личные кабинеты физических лиц Единого портала государственных и муниципальных услуг Российской Федерации, не были установлены в ходе предварительного расследования [11].

Классическим способом совершения мошенничества, который сохранился и в настоящее время является «фальшивая лотерея». Потерпевшим рассылают смс-сообщения с требованием оплатить налог для получения выигрыша. В настоящее время мошенниками в целях конспирации используются поддельные сайты с лотереями и розыгрышами. После ухода из России мировых брендов распространенным способом мошенничества стали «фейковые магазины» с поддельными сайтами, на которых потерпевшему к покупке предлагается товар по цене ниже рынка по предоплате.

Нельзя не отметить эволюцию социальной инженерии. Классический способ мошенничества — «телефонные аферы», заключающиеся в осуществлении телефонных звонков лицами, которые представляются сотрудниками государственных организаций, родственниками потерпевшего [12]. В настоящее время чат-боты в мессенджере «Телеграмм» подменяют номера, автоматизированные системы имитируют голос близких, звонки от банков, государственных органов, в связи с чем потерпевшие видят официальные номера государственных организаций, слышат голоса близких людей, что приводит к ошибочному восприятию ситуации. Для создания реалистичного фото/видеоизображения человека и аудиозаписей мошенники стали использовать новый инструмент обмана — дипфейк-технологии.

В настоящее время понятие дипфейк не имеет законодательного закрепления, впрочем, как и отсутствуют специальные нормы, которые регулировали создание, использование и распространение технологий подмены личности. Вместе с тем остро ощущается необходимость правового регулирования данных вопросов, создания необходимой правовой базы, отвечающей на современные вызовы и угрозы. В Государственную Думу РФ на рассмотрение внесены два законопроекта, которые предусматривают законодательные изменения по вопросам регулирования биометрических данных граждан. Первый законопроект о внесении изменений в УК РФ в части установления уголовной ответственности за совершение преступлений с использованием технологий подмены личности, в котором предложено введение дополнительных квалифицирующих составов преступлений,

предусматривающих повышенные меры ответственности за совершение деяний с использованием изображения или голоса (в том числе фальсифицированных или искусственно созданных) потерпевшего или иного лица, а равно с использованием их биометрических персональных данных [13]. Второй законопроект предполагает внесение изменений в часть первую Гражданского кодекса Российской Федерации (об охране голоса), регулирующую вопросы охраны голоса гражданина и предусматривает, что обнародование и дальнейшее использование голоса (в том числе записи, в которой он содержится, или записи, в которой содержится воссозданный с помощью специальных технологий голос гражданина) допускаются только с согласия этого гражданина [14].

В настоящее время традиционные методы идентификации не обеспечивают в полной мере достаточный уровень безопасности, позволяя мошенникам получить доступ к персональным данным, учетным записям и аккаунтам граждан. В этой связи, представляется весьма своевременным и необходимым использование современных технологий, таких как биометрическое распознавание лиц и отпечатков пальцев, асимметричное шифрование и технология блокчейн, в целях противодействия мошенничеству. Так, Утеев Г. предложил разработать децентрализованную систему идентификации личности на основе блокчейна и биометрических данных, что позволит повысить защищенность персональных данных граждан и обеспечить их конфиденциальность [15].

С появлением сим-карт, которые изначально предназначались для идентификации абонента в сотовой сети, у мошенников появились новые возможности для совершения преступлений. Такая мошенническая схема получила название сим-своппинг. Подмена сим-карты заключается в захвате мошенником мобильного номера телефона потерпевшего, с целью получения доступа к смс-сообщениям. В настоящее время сим-карта может быть использована как один из способов подтверждения личности в различных системах и приложениях. На абонентский номер поступает смс-сообщение с код подтверждением, позволяющим осуществить интерактивный вход в приложение Банка онлайн, Госуслуги. Справедливо отметим, что процедура удаленного запроса и смены пароля от учетной записи на «Госуслугах» (по коду из смс-сообщений) не отвечает текущим вызовам. Также в настоящее время за передачу сим-карты третьим лицам уголовная ответственность не предусмотрена, что дает возможность широко использовать сим-карты в преступных целях. Кроме того, уголовно-правовые нормы, предусматривающие привлечение к уголовной ответственности за совершение преступления вышеуказанным способом, отсутствуют не только в законодательстве РФ, но и в законодательстве зарубежных стран. Технологические изменения внедряются во все сферы жизнедеятельности стремительно, в то время как разработка законодательства в ответ на новые угрозы — это сложный и динамичный процесс, который требует гибкости, международной координации и учета быстро меняющихся технологий. Поспешные разработка и принятие законов могут иметь негативные последствия, в том числе привести к неоднозначному толкованию проектируемых положений. Вопросы подмен сим-карт широко обсуждаются в научных кругах. Так, М.Р. Нугра Морочо, С.А. Мальдонадо Арчила, Дж.А. Пачеко Солано в исследовании указывают, что фишинг занимает одно из первых мест по количеству сообщений о преступлениях такого рода, за ним следует подмена SIM-карт и другие виды компьютерных преступлений. В этой связи полагают необходимым криминализировать данный способ на законодательном уровне [16]. Поэтому исследования теоретических и практических вопросов, связанных с сим-своппингом положат основу для реформирования существующих и создания новых нормативно-правовых актов.

Зотина Е.В. выделяет два основных приема социальной инженерии – алгоритм (претекст) и фишинг [17]. Претекстинг — относительно новое понятие, характеризующее технику социальной инженерии, в основу которой положено доверие потерпевшего для получения конфиденциальной информации или выполнения последним действий, которые он обычно не совершает.

Заключение

Проведенный анализ ранних классических способов совершения мошенничества выявил, какие изменения с ними произошли в сравнении с новыми способами, адаптированными к современным методам борьбы с мошенничеством. Изучение способов мошенничества с использованием ИТТ имеет критически важное значение для государства, общества и каждого гражданина и обуславливает необходимость продолжить в дальнейшем исследование, с целью разработки перспективных законодательных инициатив, направленных на борьбу с преступлениями указанной категории и осуществлением эффективного предварительного расследования. Представляется целесообразным с учетом трансформации и эволюции способов совершения мошенничества пересмотреть законодательные акты, устанавливающие правовые основы деятельности в области связи, национальной платежной системы, банках и банковской деятельности.

Конфликт интересов

Не указан.

Рецензия

Маршалова И.Н., Основная общеобразовательная школа №17 имени Героя Советского Союза Н.А. Катина, Зеленодольск Российская Федерация

DOI: https://doi.org/10.60797/IRJ.2025.162.69.1

Все статьи проходят рецензирование. Но рецензент или автор статьи предпочли не публиковать рецензию к этой статье в открытом доступе. Рецензия может быть предоставлена компетентным органам по запросу.

Conflict of Interest

None declared.

Review

Marshalova I.N., Basic Secondary School No. 17 named after Hero of the Soviet Union N.A. Katin, Zelenodolsk Russian Federation

DOI: https://doi.org/10.60797/IRJ.2025.162.69.1

All articles are peer-reviewed. But the reviewer or the author of the article chose not to publish a review of this article in the public domain. The review can be provided to the competent authorities upon request.

Список литературы / References

1. Волхова О.В. Современные способы совершения мошенничества: особенности выявления и расследования / О.В. Волхова, под ред. проф. Е.П. Ищенко. — Москва: Юрлитинформ, 2005. — С. 3.

2. МВД РФ ФКУ «ГИАЦ». Состояние преступности в России за январь – декабрь 2024 года. — URL: https://xn--b1aew.xn--p1ai/reports/item/60248328 (дата обращения: 05.06.2025).

3. Обзор операций, совершенных без добровольного согласия клиентов финансовых организаций // Банк России. — URL: https://www.cbr.ru/analytics/ib/operations_survey/2024/ (дата обращения: 05.06.2025).

4. Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 (ред. от 15.12.2022) «О судебной практике по делам о мошенничестве, присвоении и растрате» // Российская газета. — 2017. — № 280, 11.12.2017.

5. Красикова А.А. Приобретение права на чужое имущество и хищение чужого имущества путем обмана или злоупотребления доверием: автореф. дис. … канд. юрид. наук / А.А. Красикова. — Екатеринбург, 2013. — С. 3.

6. Барчуков В.К. К вопросу о способах совершения мошенничества / В.К. Барчуков // Проблемы экономики и юридической практики. — 2017. — № 2. — URL: https://cyberleninka.ru/article/n/k-voprosu-o-sposobah-soversheniya-moshennichestva (дата обращения: 05.06.2025).

7. Лопашенко Н.А. Посягательства на собственность: монография / Н.А. Лопашенко. — Москва: Норма, Инфра-М, 2012. — С. 230.

8. Волженкин Б.В. Мошенничество: Серия «Современные стандарты в уголовном праве и уголовном процессе» / Б.В. Волженкин. — Санкт-Петербург, 1998. — С. 31.

9. Бадзарадзе Г.Д. Вопросы установления места совершения мошенничества, осуществленного с использованием информационных технологий: криминалистический и уголовно-процессуальный аспекты / Г.Д. Бадзарадзе // Сибирское юридическое обозрение. — 2022. — Т. 19, № 2. — С. 156–164. — DOI: 10.19073/2658-7602-2022-19-2-156-164.

10. Лещенко В.П. Мошенничество с использованием электронных средств платежа: уголовно-правовая характеристика и особенности квалификации: учеб. пособие / В.П. Лещенко. — Ставрополь: АГРУС Ставропольского гос. аграрного ун-та, 2024. — С. 36.

11. Приговор № 1-247/2024 от 5 декабря 2024 г. по делу № 1-247/2024 Канавинского районного суда г. Нижнего Новгорода. — URL: https://sudact.ru/regular/doc/tzrH2i4Bs1WK/ (дата обращения: 05.06.2025).

12. Белоусов А.Д. Телефонное мошенничество: психологический анализ и технологии развития устойчивости: научно-практическое пособие / А.Д. Белоусов. — Москва: Проспект, 2024. — С. 22.

13. О внесении изменений в Уголовный кодекс Российской Федерации (в части установления уголовной ответственности за совершение преступлений с использованием технологий подмены личности): проект федерального закона № 718538-8 // Система обеспечения законодательной деятельности ГАС «Законотворчество». — URL: https://sozd.duma.gov.ru/bill/718538-8 (дата обращения: 05.06.2025).

14. О внесении изменений в часть первую Гражданского кодекса Российской Федерации (об охране голоса): проект федерального закона № 718834-8 // Система обеспечения законодательной деятельности ГАС «Законотворчество». — URL: https://sozd.duma.gov.ru/bill/718834-8 (дата обращения: 05.06.2025).

15. Утеев Г. Разработка децентрализованной системы идентификации личности по биометрическим данным с помощью технологии блокчейн и компьютерного зрения / Г. Утеев, Р.Ф. Гибадуллин // Международный научно-исследовательский журнал. — 2024. — № 4 (142). — DOI: 10.23670/IRJ.2024.142.6.

16. Nugra Morocho M.R. Sim swapping como variante del delito de la violación a la intimidad e integrante de otras infracciones penales [Sim Swapping as a Variant of the Crime of Privacy Violation and a Component of Other Criminal Offenses] / M.R. Nugra Morocho, S.A. Maldonado Archila, J.A. Pacheco Solano [et al.] // Latam. — 2023. — Vol. 4, № 2. — DOI: 10.56712/latam.v4i2.862.

17. Зотина Е.В. Мошенничество с использованием информационно-телекоммуникационных технологий и приемов социальной инженерии: криминологическое исследование: дис. … канд. юрид. наук / Е.В. Зотина. — Казань, 2024. — С. 51. — URL: https://kpfu.ru/dis_card?p_id=3868 (дата обращения: 05.06.2025).

Список литературы на английском языке / References in English

1. Volkhova O.V. Sovremennye sposoby soversheniya moshennichestva: osobennosti vyyavleniya i rassledovaniya [Modern Methods of Committing Fraud: Detection and Investigation Features] / O.V. Volkhova, ed. by Prof. E.P. Ishchenko. — Moscow: Yurlitinform, 2005. — P. 3. [in Russian]

2. Ministry of Internal Affairs of the Russian Federation, State Institution “GIAZ”. Sostoyanie prestupnosti v Rossii za yanvar' – dekabr' 2024 goda [Crime in Russia, January–December 2024]. — URL: https://xn--b1aew.xn--p1ai/reports/item/60248328 (accessed: 06.05.2025). [in Russian]

3. Obzor operatsiy, sovershennykh bez dobrovol'nogo soglasiya klientov finansovykh organizatsiy [Review of Transactions Conducted Without Clients’ Voluntary Consent] // Bank of Russia. — URL: https://www.cbr.ru/analytics/ib/operations_survey/2024/ (accessed: 06.05.2025). [in Russian]

4. Postanovlenie Plenuma Verkhovnogo Suda RF ot 30.11.2017 № 48 (red. ot 15.12.2022) «O sudebnoy praktike po delam o moshennichestve, prisvoenii i rast rate» [Resolution of the Plenum of the Supreme Court of the Russian Federation No. 48 dated November 30, 2017 (rev. December 15, 2022) “On Judicial Practice in Cases of Fraud, Embezzlement and Misappropriation”] // Rossiyskaya gazeta. — 2017. — № 280, December 11, 2017. [in Russian]

5. Krasikova A.A. Priobretenie prava na chuzhoe imushchestvo i khishchenie chuzhego imushchestva putem obmana ili zloupotrebleniya doveriyem [Acquisition of Rights to Another's Property and Theft by Deception or Abuse of Trust]: abst. diss. … PhD in Legal Sciences / A.A. Krasikova. — Yekaterinburg, 2013. — P. 3. [in Russian]

6. Barchukov V.K. K voprosu o sposobakh sovershenіya moshennichestva [On the Methods of Committing Fraud] / V.K. Barchukov // Problemy ekonomiki i yuridicheskoy praktiki [Issues of Economics and Legal Practice]. — 2017. — № 2. — URL: https://cyberleninka.ru/article/n/k-voprosu-o-sposobah-sovershenіya-moshennichestva (accessed: 06.05.2025). [in Russian]

7. Lopashenko N.A. Posyagatel'stva na sobstvennost' [Offenses Against Property]: monograph / N.A. Lopashenko. — Moscow: Norma, Infra-M, 2012. — P. 230. [in Russian]

8. Volzhenkin B.V. Moshennichestvo [Fraud]: Seriya «Sovremennye standarty v ugolovnom prave i ugolovnom protsesse» [Modern Standards in Criminal Law and Criminal Procedure] / B.V. Volzhenkin. — St. Petersburg, 1998. — P. 31. [in Russian]

9. Badzgaradze G.D. Voprosy ustanovleniya mesta sovershenіya moshennichestva, osushchestvlennogo s ispol'zovaniem informatsionnykh tekhnologiy: kriminalisticheskiy i ugolovno-protsessual'nyy aspekty [Issues of Determining the Place of Commission of Fraud Committed Using Information Technologies: Forensic and Criminal-Procedural Aspects] / G.D. Badzgaradze // Sibirskoe yuridicheskoe obozrenie [Siberian Law Review]. — 2022. — Vol. 19, № 2. — P. 156–164. — DOI: 10.19073/2658-7602-2022-19-2-156-164. [in Russian]

10. Leschenko V.P. Moshennichestvo s ispol'zovaniem elektronnykh sredstv platezha: ugolovno-pravovaya kharakteristika i osobennosti kvalifikatsii [Fraud Using Electronic Payment Instruments: Criminal-Legal Characteristics and Qualification Features]: study guide / V.P. Leschenko. — Stavropol: AGUS Stavropol State Agrarian University, 2024. — P. 36. [in Russian]

11. Prigovor № 1-247/2024 ot 5 dekabrya 2024 g. po delu № 1-247/2024 Kanavinskogo rayonnogo suda g. Nizhnego Novgoroda [Judgment No. 1-247/2024 of December 5, 2024 in Case No. 1-247/2024 of the Kanavinsky District Court of Nizhny Novgorod]. — URL: https://sudact.ru/regular/doc/tzrH2i4Bs1WK/ (accessed: 06.05.2025). [in Russian]

12. Belousov A.D. Telefonnoe moshennichestvo: psikhologicheskiy analiz i tekhnologii razvitiya ustoychivosti [Telephone Fraud: Psychological Analysis and Resilience-Building Technologies]: manual / A.D. Belousov. — Moscow: Prospekt, 2024. — P. 22. [in Russian]

13. O vnesenii izmeneniy v Ugolovnyy kodeks Rossiyskoy Federatsii (v chasti ustanovleniya ugolovnoy otvetstvennosti za sovershenie prestupleniy s ispol'zovaniem tekhnologiy podmeny lichnosti): proekt federal'nogo zakona № 718538-8 [On Amendments to the Criminal Code of the Russian Federation (Regarding Criminal Liability for Crimes Committed Using Identity Substitution Technologies): Draft Federal Law No. 718538-8] // Sistema obespecheniya zakonodatel'noy deyatel'nosti GAS «Zakonotvorchestvo» [Legislative Process Support System of the State Automated System “Lawmaking”]. — URL: https://sozd.duma.gov.ru/bill/718538-8 (accessed: 06.05.2025). [in Russian]

14. O vnesenii izmeneniy v chast' pervuyu Grazhdanskogo kodeksa Rossiyskoy Federatsii (ob okhrane golosa): proekt federal'nogo zakona № 718834-8 [On Amendments to Part One of the Civil Code of the Russian Federation (on Voice Protection): Draft Federal Law No. 718834-8] // Legislative Activity Support System GAS ‘Lawmaking’. — URL: https://sozd.duma.gov.ru/bill/718834-8 (accessed: 06.05.2025). [in Russian]

15. Uteev G. Razrabotka detsentralizovannoy sistemy identifikatsii lichnosti po biometricheskim dannym s pomoshch'yu tekhnologii blokcheyn i komp'yuternogo zreniya [Development of a Decentralized Biometric Identity System Using Blockchain and Computer Vision] / G. Uteev, R.F. Gibadullin // Mezhdunarodnyy nauchno-issledovatel'skiy zhurnal [International Research Journal]. — 2024. — № 4 (142). — DOI: 10.23670/IRJ.2024.142.6. [in Russian]

16. Nugra Morocho M.R. Sim swapping como variante del delito de la violación a la intimidad e integrante de otras infracciones penales [Sim Swapping as a Variant of the Crime of Privacy Violation and a Component of Other Criminal Offenses] / M.R. Nugra Morocho, S.A. Maldonado Archila, J.A. Pacheco Solano [et al.] // Latam. — 2023. — Vol. 4, № 2. — DOI: 10.56712/latam.v4i2.862.

17. Zotina E.V. Moshennichestvo s ispol'zovaniem informatsionno-telekommunikatsionnykh tekhnologiy i priyomov sotsial'noy inzhenerii: kriminologicheskoe issledovanie [Fraud Using ICT and Social Engineering Techniques: A Criminological Study]: diss. … PhD in Legal Sciences / E.V. Zotina. — Kazan, 2024. — P. 51. — URL: https://kpfu.ru/dis_card?p_id=3868 (accessed: 06.05.2025). [in Russian]