Анна Павловна АЛЕКСЕЕВА,
доктор юридических наук, профессор, ORCID 0000-0002-4569-7564
Санкт-Петербургский университет МВД России (г. Калининград)
профессор кафедры уголовного права, криминологии и уголовно-исполнительного права Калининградского филиала
Заслуженный юрист Российской Федерации
alexeeva.klg-mvd@yandex.ru

Андрей Николаевич БЕРЕСТОВОЙ,
кандидат юридических наук, доцент, ORCID 0000-0003-0805-900X
Российский государственный университет правосудия (г. Санкт-Петербург)
доцент кафедры уголовного права Северо-Западного филиала
andreyberestovoy@gmail.com

Научная статья
УДК 343.85

ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ И СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ В МЕХАНИЗМАХ ДИСТАНЦИОННЫХ ХИЩЕНИЙ

КЛЮЧЕВЫЕ СЛОВА. Дистанционное хищение, социальная инженерия, методы мошенничества, киберпреступность, информационно-телекоммуникационные технологии, эмоциональное воздействие, психологические приемы.

АННОТАЦИЯ. ***Введение.*** *В статье рассматривается феномен дистанционных хищений, совершаемых посредством информационно-телекоммуникационных технологий и методов социальной инженерии. Подчеркивается рост числа таких преступлений, их массовый характер и значительный материальный ущерб. В частности, отмечается, что более 60% преступлений реализуются через психологическое воздействие на жертву с целью получения доступа к средствам или конфиденциальной информации. Особое внимание уделяется недостаточной цифровой и финансовой грамотности жертв, а также особенностям манипуляций, основанных на эксплуатации эмоций (страха, жадности, альтруизма и др.).* ***Методы.*** *Исследование, результаты которого представлены в статье, выполнено на основе анализа статистических данных МВД России и Банка России за 2020-2024 гг., изучения материалов судебной и следственной практики, отечественных и зарубежных научных публикаций. В ходе работы был применен междисциплинарный подход: использован формально-юридический анализ нормативных актов и практики, изучены кейсы типичных преступлений, выполнена криминологическая систематизация методов социальной инженерии. Проведено сопоставление психологических приемов с их цифровыми и речевыми проявлениями, а также усредненных портретов преступников и жертв.* ***Результаты.*** *Выделены и описаны десять базовых методов социальной инженерии, включая фишинг, вишинг, претекстинг, подмену интерфейсов и манипуляцию эмоциональными состояниями жертв. Представлен криминологический и психологический портрет преступников, использующих такие методы: это мужчины 22-36 лет, обладающие коммуникативными и актерскими навыками, со сниженным уровнем эмпатии. Подтверждено, что в рассматриваемых случаях основным фактором виктимности является сочетание низкой цифровой грамотности и высокой степени подверженности эмоциональному воздействию жертвы преступления. Сформулированы рекомендации по профилактике дистанционных хищений, предусматривающие, в частности, технические меры фильтрации подозрительных коммуникаций и использование законодательных отсрочек на спорные переводы, а также обучение граждан критическому восприятию информационных угроз.*

ВВЕДЕНИЕ

Дистанционные хищения, совершаемые с применением информационно-телекоммуникационных технологий, на протяжении последних пяти лет устойчиво входят в число наиболее массовых и динамичных видов преступлений[1]. В 2024 г. на их долю пришлось около 40% всех зарегистрированных преступлений, а совокупный ущерб, нанесенный ими гражданам, превысил 168 млрд рублей. Более 60% таких деяний реализуются посредством техник социальной инженерии, когда злоумышленник убеждает жертву добровольно перевести деньги либо раскрыть конфиденциальные данные, необходимые для их хищения [1, с. 115].

Несмотря на обилие публикаций о киберпреступности, криминологическое описание используемых ею методов социальной инженерии и характеристик личности киберпреступника до сих пор представлено в научной литературе фрагментарно. Целью исследования, результаты которого представлены в настоящей статье, было обобщение открытых статистических сведений, материалов следственной и судебной практики, а также новейших достижений науки для определения типовых методов социальной инженерии и соотнесения их с личностными, мотивационными и поведенческими особенностями преступников, совершающих дистанционные хищения с применением информационно-телекоммуникационных технологий.

МЕТОДЫ

Методологическую основу исследования составил диалектический метод познания, позволяющий рассматривать изучаемые явления в динамике их развития и во взаимосвязи с другими явлениями и различными правовыми институтами.

Формально-юридический метод применялся для анализа нормативно-правовых актов при разработке авторской типологии приемов социальной инженерии. Были изучены определения, имеющиеся в Федеральном законе «О персональных данных» и Методических рекомендациях Банка России, что исключило противоречия с действующим законодательством.

Системно-структурный анализ позволил прийти к выводу о том, что изменение любого элемента (например появления deepfake-технологий) ведет к трансформации всей системы и порождает новые варианты преступных действий.

Метод классификации применялся для систематизации видов дистанционных хищений, совершаемых с применением информационно-телекоммуникационных технологий, определения их характерных признаков и особенностей воздействия на противоправное поведение мошенников.

Статистический метод был востребован для анализа выборки официальных данных МВД России и Банка России за 2020-2024 гг., с помощью чего производилась оценка масштабов рассматриваемой проблемы.

Эмпирическую базу исследования сформировали материалы научных публикаций, диссертационных исследований, монографий и статей ведущих специалистов в области криминологии, а также данные правоприменительной практики.

РЕЗУЛЬТАТЫ

Криминологические исследования преступности, связанной с применением методов социальной инженерии, показывают, что злоумышленниками обычно применяются десять базовых приемов для обмана потенциальных жертв (см. таблицу 1).

1. Предварительный сбор данных о потенциальной жертве. Злоумышленник анализирует открытые источники (социальные сети, справочные базы), получает сведения о личных особенностях, привычках, финансовом положении и контактах жертвы [2, с. 15].

2. Исполнение заранее отработанной роли. При обращении к жертве преступник выдает себя, как правило, за сотрудника банка, правоохранительных органов, пенсионного фонда или иной официальной структуры, что повышает уровень доверия и снижает критичность восприятия [3, с. 152].

3. Использование заготовленного сценария разговора. Все этапы диалога, от обращения до ответов на возможные вопросы, строятся по заранее разработанному алгоритму, который позволяет вывести жертву из психологического равновесия и подтолкнуть ее к действиям, в совершении которых заинтересован преступник [4, с. 535].

4. Специальная «подача» информации. Текст и тон сообщений рассчитаны на создание ощущения срочной необходимости тех или иных действий, формирование чувства страха или, наоборот, предположения о возможности получения выгоды. Жертва испытывает эмоциональный дискомфорт или преждевременную радость, что блокирует логику и побуждает к необдуманным поступкам [5, с. 61].

5. Создание фишинговых ресурсов и подмена интерфейса. Для сбора персональных данных используются клоны банковских сайтов и мобильных приложений, с которых жертва вводит логины, пароли и реквизиты платежных карт [6, с. 107].

6. Подмена телефонного номера и голоса. С помощью программ «Call Voice Changer», SIP-мостов, VPN и других программных инструментов злоумышленник скрывает свой номер телефона и меняет голос так, чтобы абонент воспринимал его как сотрудника надежной организации [7, с. 216].

7. Удаленный доступ к телекоммуникационному устройству жертвы. Программы «AnyDesk», «TeamViewer» и аналогичные им устанавливаются на оборудование под предлогом выполнения действий по технической поддержке, после чего преступник получает полный контроль над смартфоном или компьютером жертвы [8, с. 125].

8. Получение конфиденциальной информации. Жертве предлагают пройти «процедуру проверки безопасности» или «заблокировать попытку мошенничества» путем передачи кода из SMS, CVV-кода, одноразовых паролей и т.п. [9, с. 102].

9. Создание искусственного дефицита времени. Преступник настаивает на немедленных дейст-

[1] Статистика и аналитика // МВД России: сайт // URL: https://мвд.рф/dejatelnost/statistics (дата обращения: 23.02.2025).

Anna P. ALEKSEEVA,
Doctor of Law, Professor, ORCID 0000-0002-4569-7564
Saint Petersburg University of the Ministry
of the Interior of Russia (Kaliningrad, Russia)
Professor of the Department of Criminal Law, Criminology
and Criminal Executive Law of the Kaliningrad Branch
Honored Lawyer of the Russian Federation
alexeeva.klg-mvd@yandex.ru

Andrey N. BERESTOVOY,
Cand. Sci. (Jurisprudence), Associate Professor, ORCID 0000-0003-0805-900X
Russian State University of Justice (Saint Petersburg, Russia)
Associate Professor of the Criminal Law Department of the North-West Branch
andreyberestovoy@gmail.com

INFORMATION AND TELECOMMUNICATION TECHNOLOGIES AND SOCIAL ENGINEERING IN THE MECHANISMS OF REMOTE THEFT

KEYWORDS. Remote theft, social engineering, fraud methods, cybercrime, information and telecommunication technologies, emotional impact, psychological techniques.

ANNOTATION. *I**ntroduction.** The article examines the phenomenon of remote thefts committed through information and telecommunication technologies and social engineering methods. The article emphasizes the growing number of such crimes, their mass nature and significant material damage. In particular, it is noted that more than 60% of crimes are committed through psychological impact on the victim in order to gain access to funds or confidential information. Particular attention is paid to the insufficient digital and financial literacy of victims, as well as the peculiarities of manipulations based on the exploitation of emotions (fear, greed, altruism, etc.). **Methods.** The study, the results of which are presented in the article, is based on the analysis of statistical data of the Ministry of Internal Affairs of Russia and the Bank of Russia for 2020-2024, the study of materials of judicial and investigative practice, domestic and foreign scientific publications. In the course of the work, an interdisciplinary approach was used: a formal-legal analysis of regulatory acts and practice was used, cases of typical crimes were studied, and a criminological systematization of social engineering methods was performed. A comparison of psychological techniques with their digital and speech manifestations, as well as average portraits of criminals and victims was carried out. **Results.** Ten basic methods of social engineering are identified and described, including phishing, vishing, pretexting, interface substitution and manipulation of emotional states of victims. A criminological and psychological portrait of criminals using such methods is presented: these are men aged 22-36 years old, with communication and acting skills, with a reduced level of empathy. It has been confirmed that in the cases under consideration the main factor of victimization is a combination of low digital literacy and a high degree of susceptibility to the emotional impact of the victim of the crime. Recommendations for the prevention of remote thefts have been formulated, which include, in particular, technical measures for filtering suspicious communications and the use of legislative deferrals for disputed transfers, as well as training citizens in critical perception of information threats.*

виях («заявка действует десять минут», «карта заморозится»), чтобы не дать жертве возможности проверить достоверность сообщения [10, с. 31].

10. Многоступенчатое обналичивание похищенных средств. После перевода денег на «безопасный счет» злоумышленники делят поступившую сумму на мелкие части, используют посредников и программные схемы для быстрого вывода наличности и затруднения отслеживания денежных потоков правоохранительными органами [11, с. 134].

Сочетание нескольких из перечисленных методов образует цельный механизм психологического и технического воздействия, позволяющий дистанционно похищать чужие деньги, сохранять анонимность преступника и минимизировать сопутствующие его действиям риски.

Что касается личности дистанционного мошенника, то речь идет о развитом интеллекте, обладании широким спектром коммуникативных навыков, умении вводить жертв в состояние когнитивного диссонанса. Эмпатия при этом носит утилитарный характер и используется как инструмент манипуляции. В криминологическом аспекте эмоциональное состояние жертвы выступает причиной необдуманности ее действий. Анализ 74 приговоров, вынесенных судами по результатам рассмотрения уголовных дел о дистанционном мошенничестве[1], показал, что 68% исполнителей – это мужчины 22-36 лет, 31% – женщины (расширение их участия в преступной деятельности рассматриваемого вида объясняется наймом операторов колл-центров); 54% имеют среднее профессиональное образование, 11% – незаконченное высшее, 7% – IT-специальности; 38% были ранее судимы за имущественные преступления. К числу ключевых личностных особенностей таких лиц можно отнести высокоразвитый вербальный интеллект, умение быстро устанавливать психологи-

[1] В 2025 году изучались приговоры, имеющиеся в открытом доступе на портале «СудАкт» (Судебные и нормативные акты РФ // URL: https://sudact.ru/).

Таблица 1

КЛАССИФИКАЦИЯ МЕТОДОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

№	Метод	Краткое содержание	Доля эпизодов	Примечание
1	Фишинг/ смэшинг	Массовая рассылка e-mail/SMS-ссылок на фальш-сайты	27%	Часто комбинируется с поддельными платежными формами
2	Вишинг	Телефонные звонки от «службы безопасности банка»	23%	Зачастую используется подмена CLI-номера
3	Претекстинг	Создание легенды (сотрудник МВД, ЦБ, соцслужбы и т.д.)	14%	Требуются знания в сфере деятельности оргструктур и терминологии
4	QR-инжиниринг	Подмена платежных QR-кодов, перевод «на безопасный счет»	8%	Рост показателей произошел после внедрения СБП в 2022 г.
5	Deepfake-аудио	Искажение голоса, звонки от «родственников»	5%	Используются нейросети-клонировщики
6	Remote-Access Scam	Установка AnyDesk/TeamViewer под видом «помощи»	7%	Позволяет управлять приложением
7	Байтинг	«Вознаграждение за опрос», «выигрыш»	4%	Акцент на жадность
8	Quid pro quo	Бесплатная «техподдержка» или «повышение лимита»	4%	Метод активно применялся во время пандемии
9	Курьерская схема	Вывоз наличных «курьером из ЦБ/МВД»	6%	Задействуются дропперы
10	Tailgating digital	Захват сессии «Госуслуг» через код СМС	2%	Чаще используется в отношении несовершеннолетних

ческий контакт; демонстративные и истероидные черты, склонность к артистизму; низкую эмпатию, рациональность («банк всё равно застрахует убытки»); выраженную мотивацию «эго-челленджа» – удовольствие от управления жертвой. Роли в организованных группах распределялись следующим образом: рекрутеры (10%), скрипт-райтеры (5%), операторы-вишеры (45%), техподдержка (15%), обналичники/дропперы (25%).

Типичная жертва хищения, совершенного с использованием приемов социальной инженерии, в последнее время представляет собой не просто случайного пользователя банковских или интернет-сервисов: она – носитель ряда характерных личностных и ситуационно проявляющихся черт. Чаще всего это люди в возрасте 25-40 лет, находящиеся на пике экономической и социальной активности; имеющие стабильное материальное положение, которого оказывается не всегда достаточно для удовлетворения внезапно возникающих потребностей; не склонные к глубокому анализу юридических и финансовых рисков. Для них характерен низкий или средний уровень правовой и финансовой грамотности: они плохо знакомы с механизмами дистанционного банковского обслуживания и защиты персональных данных; не разбираются в тонкостях условий кредитных договоров, не способны отличить официальные сервисы от фальшивых сайтов-двойников. Как правило, жертвы дистанционных хищений имеют уверенные, но поверхностные навыки работы с онлайн-банкингом и мобильными приложениями; это преимущественно пользователи мобильных устройств, редко проверяющие URL и сертификаты сайтов; они не используют VPN-клиенты и не меняют стандартных настроек конфиденциальности. Такие люди склонны самостоятельно вводить пароли и коды из SMS и мессенджеров по первому требованию «службы безопасности»; дают согласие на дистанционное «блокирование» карт или перевод средств с «восстановительными» целями; быстро реагируют на инструкции без паузы на обдумывание или консультацию с родственниками и банком.

Их эмоционально-волевая сфера отличается повышенной степенью доверчивости и эмпатии:

Таблица 2

ЭМОЦИОНАЛЬНЫЕ ПРИЧИНЫ ВИКТИМНОГО ПОВЕДЕНИЯ ЖЕРТВЫ В МЕХАНИЗМЕ ДИСТАНЦИОННОГО МОШЕННИЧЕСТВА

Эмоциональные причины	Содержание криминального приема	Типичные формулы-приманки	Возможные последствия
Страх	Индукция угрозы утраты денег, свободы, здоровья	«Переведите средства на резервный счет»; «Ваш кабинет будет заблокирован»	Срочные переводы, разглашение ОТР-кодов
Раздражение	Создание информационной перегрузки; предложение «отписаться»	Массовый спам с кнопкой «Отказаться»	Переход на фишинговый сайт, загрузка malware-apk
Любопытство	Апелляция к желанию знать скрытую информацию	«Смотри видео, как ты веселишься»; «Секретная карта заражения»	Установка вредоносного ПО, перехват данных
Жадность	Обещание выгоды без усилий	«Вы выиграли автомобиль»; «Билеты со скидкой 90%»	Передача платежных реквизитов, предоплаты
Желание помочь	Манипуляция альтруистическими установками	«Сбор средств на лечение ребенка»	Перевод средств на счета злоумышленников
Невнимательность	Эксплуатация опечаток и автоматических исправлений	Домен-двойник sberbamk.ru, gismete0.ru и т.д.	Авторизация на фишинговых ресурсах

предрасположены воспринимать сообщение «сотрудника банка» как безусловную истину; поддаются давлению дефицита времени («срочно», «моментально»), эмоциональному нажиму («опасность потери средств», «официальное предупреждение»); имеют низкий уровень стрессоустойчивости в ситуациях финансовой неопределенности. Среди коммуникативных особенностей у них наиболее выражены: готовность вступать в доверительный контакт в случае уверенной, профессионально поставленной речи собеседника; склонность отвечать на телефонные и SMS-провокации без дополнительной проверки источника; отсутствие привычки проверять полученную информацию на официальных сайтах и по альтернативным каналам связи (см. таблицу 2).

Отмечается корреляция между количеством размещенных в сети персональных данных и вероятностью успешного осуществления атаки преступников, совершающих дистанционные хищения с применением информационно-телекоммуникационных технологий, на владельца этих данных, что актуализирует проведение профилактической работы, направленной на обеспечение информационной гигиены [12, с. 117].

Таким образом, жертва мошенничества, осуществляемого в киберпространстве при помощи приемов социальной инженерии, характеризуется сочетанием технической неграмотности, доверчивости и эмоциональной уязвимости, что позволяет злоумышленникам создавать благоприятные условия для манипуляции ее поведением, минимизируя возможность критической оценки происходящего и побуждая к совершению тех или иных (нередко противоправных) операций.

Преступники используют эмоции жертвы (представлены в таблице 2), комбинируя такое воздействие с возможностями современных технологий: подмена номера и голоса создает иллюзию авторитета («сотрудник банка» или «ФСБ»), усиливая страх жертвы [13, с. 681]; рассылка вредоносных apk-файлов через мессенджеры под названием, например, «видео о смерти знакомого» и т.д. играет на любопытстве и дает возможность установить шпионское программное обеспечение [14, с. 214]; использование инсайдерской информации (ФИО, платежная история) повышает уровень доверия и снижает критичность жертвы [15, с. 24]; внедрение RAT и VPN позволяет злоумышленникам удаленно управлять устройством после эмоционального воздействия на жертву.

ЗАКЛЮЧЕНИЕ

Социальная инженерия исполняет ключевую роль в совершении дистанционных хищений, обеспечивая переход от технических методов взлома к манипуляциям с сознанием жертвы. Проведенное нами исследование позволило систематизировать наиболее распространенные в России методы социальной инженерии и определить частоту их использования; выявить типичные черты современного дистанционного мошенника (высокий уровень речевой компетентности, актерские навыки и пониженная эмпатия); подтвердить, что главными факторами риска остаются низкий уровень финансовой грамотности и эмоциональная нестабильность потенциальных жертв хищений, совершаемых с использованием информационно-телекоммуникационных технологий.

Эмоциональная неустойчивость жертвы является неотъемлемой частью механизма дистанционного мошенничества. Его научное описание способствует совершенствованию методов противодействия преступлениям данного вида, разработке мер профилактики, формированию у населения критического отношения к информационным угрозам. Благоприятное воздействие на ситуацию может оказать и введение 48-часового периода ожидания при выполнении денежных переводов, вызывающих подозрение: такая пауза снижает давление срочности и помогает избежать поспешных решений[1]. Более широкое использование мобильными операторами автоматических систем, распознающих ключевые фразы («переведите на безопасный счет», «код подтверждения»), позволяют блокировать нежелательные сообщения на ранних этапах. Перспективы дальнейших разработок в области противодействия дистанционным хищениям включают в себя расширение использования автоматизированных систем, связывающих акустические характеристики телефонных звонков с вероятностными признаками преступника, что позволит оперативно выявлять подозрительную активность и снижать результативность мошеннических схем. ■

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Бадиков Д.А., Елисеева К.А. Мошенничество с использованием электронных средств платежа: к вопросу об уголовно-правовой характеристике // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2024. № 2 (99). С. 115-123.

2. Ганиева И.А. Личность преступника, совершающего дистанционное мошенничество // Актуальные вопросы борьбы с преступлениями. 2023. № 5. С. 15-18.

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

4. Назмеева Л.Р., Богомолов С.Ю. Личность преступника, совершающего мошеннические действия с использованием электронных средств платежа: криминологическая оценка // Вестник Казанского юридического института МВД России. 2021. Т. 12. № 4 (46). С. 535-541.

5. Дерюгин Р.А. Криминалистическая характеристика хищений денежных средств, совершаемых с использованием персональных данных пользователей сети Интернет // Вестник Уральского юридического института МВД России. 2024. № 2 (42). С. 61-66.

6. Горбова В.В., Самороковский С.А. Оперативно-разыскное противодействие мошенничествам, совершаемым с использованием средств мобильной связи // Вестник Воронежского института ФСИН России. 2020. № 4. С. 107-112.

7. Сычева А.В. Криминалистическая характеристика мошенничества в сфере компьютерной информации // Юристъ-Правоведъ. 2025. № 1 (112). С. 216-222.

8. Ковалик Б.В. О механизме совершения мошеннических действий дистанционным способом // Вестник Академии МВД Республики Беларусь. 2023. № 2 (46). С. 125-133.

9. Макашева М.Н. Сеть Интернет и общая оценка ее влияния на личность несовершеннолетнего // Вестник Санкт-Петербургского университета МВД России. 2021. № 3 (91). С. 102-109.

10. Зотина Е.В. Криминологические детерминанты телефонного мошенничества, совершаемого с использованием приемов социальной инженерии // Ученые записки Казанского юридического института МВД России. 2023. Т. 8. № 1 (15). С. 31-35.

11. Савицкая А.В., Фролов В.В. Использование элементов криминалистической характеристики мошенничества: сведения о личности преступника и способе его совершения при построении версий о лице, его совершившем // Эпомен. 2022. № 70. С. 134-146.

12. Ивасюк О.Н. Современные проблемы противодействия киберпреступности // Вестник экономической безопасности. 2022. № 6. С. 117-120.

13. Осипенко А.Л., Соловьев В.С. Основные направления развития криминологической науки и практики предупреждения преступлений в условиях цифровизации общества // Всероссийский криминологический журнал. 2021. Т.15. № 6. С. 681-691.

14. Щербаченко А.К. Криминалистическое обеспечение борьбы с мошенничеством как потребность правоприменения // Юристъ-Правоведъ. 2024. № 1 (108). С. 214-220.

[1] Указание Банка России от 18.02.2022 № 6071-У «О внесении изменений в Положение Банка России от 17 апреля 2019 г. № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента»».

15. Алексеева А.П. Перспективы развития уголовного законодательства в киберсфере // Подготовка сотрудников полиции к использованию информационных технологий в борьбе с преступностью. Сборник научных трудов по материалам Всероссийской межвузовской научно-практической конференции. Вып. 2. Волгоград: ВА МВД России, 2017. С. 24-31.

REFERENCES

1. Badikov D.A., Yeliseyeva K.A. Moshennichestvo s ispol'zovaniyem elektronnykh sredstv platezha: k voprosu ob ugolovno-pravovoy kharakteristike // Nauchnyy vestnik Orlovskogo yuridicheskogo instituta MVD Rossii imeni V.V. Luk'yanova. 2024. № 2 (99). S. 115-123.

2. Ganiyeva I.A. Lichnost' prestupnika, sovershayushchego distantsionnoye moshennichestvo // Aktual'nyye voprosy bor'by s prestupleniyami. 2023. № 5. S. 15-18.

3. Starostenko N.I. Ponyatiye i vidy metodov sotsial'noy inzhenerii, primenyayemykh pri sovershenii prestupleniy v sfere informatsionno-telekommunikatsionnykh tekhnologiy // Yuridicheskaya nauka i praktika: Vestnik Nizhegorodskoy akademii MVD Rossii. 2023. № 1 (61). S. 152-159.

4. Nazmeyeva L.R., Bogomolov S.Yu. Lichnost' prestupnika, sovershayushchego moshennicheskiye deystviya s ispol'zovaniyem elektronnykh sredstv platezha: kriminologicheskaya otsenka // Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii. 2021. T. 12. № 4 (46). S. 535-541.

5. Deryugin R.A. Kriminalisticheskaya kharakteristika khishcheniy denezhnykh sredstv, sovershayemykh s ispol'zovaniyem personal'nykh dannykh pol'zovateley seti Internet // Vestnik Ural'skogo yuridicheskogo instituta MVD Rossii. 2024. № 2 (42). S. 61-66.

6. Gorbova V.V., Samorokovskiy S.A. Operativno-razysknoye protivodeystviye moshennichestvam, sovershayemym s ispol'zovaniyem sredstv mobil'noy svyazi // Vestnik Voronezhskogo instituta FSIN Rossii. 2020. № 4. S. 107-112.

7. Sycheva A.V. Kriminalisticheskaya kharakteristika moshennichestva v sfere komp'yuternoy informatsii // Yurist"-Pravoved". 2025. № 1 (112). S. 216-222.

8. Kovalik B.V. O mekhanizme sovershenіya moshennicheskikh deystviy distantsionnym sposobom // Vestnik Akademii MVD Respubliki Belarus'. 2023. № 2 (46). S. 125-133.

9. Makasheva M.N. Set' Internet i obshchaya otsenka yeye vliyaniya na lichnost' nesovershennoletnego // Vestnik Sankt-Peterburgskogo universiteta MVD Rossii. 2021. № 3 (91). S. 102-109.

10. Zotina Ye.V. Kriminologicheskiye determinanty telefonnogo moshennichestva, sovershayemogo s ispol'zovaniyem priyemov sotsial'noy inzhenerii // Uchenyye zapiski Kazanskogo yuridicheskogo instituta MVD Rossii. 2023. T. 8. № 1 (15). S. 31-35.

11. Savitskaya A.V., Frolov V.V. Ispol'zovaniye elementov kriminalisticheskoy kharakteristiki moshennichestva: svedeniya o lichnosti prestupnika i sposobe yego sovershenіya pri postroyenii versiy o litse, yego sovershivshem // Epomen. 2022. № 70. S. 134-146.

12. Ivasyuk O.N. Sovremennyye problemy protivodeystviya kiberprestupnosti // Vestnik ekonomicheskoy bezopasnosti. 2022. № 6. S. 117-120.

13. Osipenko A.L., Solov'yev V.S. Osnovnyye napravleniya razvitiya kriminologicheskoy nauki i praktiki preduprezhdeniya prestupleniy v usloviyakh tsifrovizatsii obshchestva // Vserossiyskiy kriminologicheskiy zhurnal. 2021. T.15. № 6. S. 681-691.

14. Shcherbachenko A.K. Kriminalisticheskoye obespecheniye bor'by s moshennichestvom kak potrebnost' pravoprimeneniya // Yurist"-Pravoved". 2024. № 1 (108). S. 214-220.

15. Alekseyeva A.P. Perspektivy razvitiya ugolovnogo zakonodatel'stva v kibersfere // Podgotovka sotrudnikov politsii k ispol'zovaniyu informatsionnykh tekhnologiy v bor'be s prestupnost'yu. Sbornik nauchnykh trudov po materialam Vserossiyskoy mezhvuzovskoy nauchno-prakticheskoy konferentsii. Vyp. 2. Volgograd: VA MVD Rossii, 2017. S. 24-31.

Авторы заявляют об отсутствии конфликта интересов.
Авторами внесён равный вклад в написание статьи.
The authors declare no conflicts of interests.
The authors have made an equal contribution to the writing of the article.

ССЫЛКА ДЛЯ ЦИТИРОВАНИЯ

Алексеева А.П., Берестовой А.Н. Информационно-телекоммуникационные технологии и социальная инженерия в механизмах дистанционных хищений // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2025. № 3 (81). С. 18-24.