Научная статья
УДК 343

# КРИМИНАЛИСТИЧЕСКИЙ ПОДХОД К ДИСТАНЦИОННЫМ ХИЩЕНИЯМ

Аслям Наилевич Халиков,
Московская академия Следственного комитета РФ имени А.Я. Сухарева, Москва, Россия,
Уфимский университет науки и технологий, Уфа, Россия,
han010@yandex.ru

***Аннотация***

**Введение:** в статье рассматриваются проблемы хищений, совершаемых дистанционно: путем тайного списания денежных средств с банковских счетов граждан либо путем обмана граждан, в результате чего последние переводят свои деньги на банковские счета преступников. Раскрываемость данных преступлений минимальна.

**Материалы и методы:** методологическую основу статьи составил всеобщий метод материально-диалектического познания при исследовании вопросов виртуальных способов дистанционных хищений денежных средств граждан с помощью цифровых и психолого-лингвистических методов. В статье использовались общенаучные исследовательские методы, в частности, сравнительно-правовой, системно-структурный, а также применялся анализ как частно-научный метод познания.

**Обсуждение и заключение:** способов дистанционных хищений множество, и все они зависят от способов проникновения преступников в банковские системы либо от степени психического воздействия на человека. Раскрываемость таких деяний очень низкая. К уголовной ответственности в основном привлекаются пособники, не играющие активную роль в совершении преступлений. Эти проблемы решаются в зависимости от установления конкретных обстоятельств деяния и их доказанности по результатам расследования.

**Результаты исследования:** криминалистическая деятельность, включающая в себя общие положения правоохранительной деятельности, оперативно-розыскной и следственной работы, требует радикальной перестройки способов выявления, раскрытия и расследования дистанционных хищений. Необходимы новые подходы к взаимодействию с операторами связи, банками, трансформация получения судебных разрешений на производство следственных действий и оперативно-розыскных мероприятий. В связи с этим в определенной степени могут быть ограничены интересы банков и операторов сотовой связи

*Ключевые слова: банковские операции; дистанционные хищения; киберпреступления; кража; мошенничество; обман; способы преступления*



**Для цитирования:** Халиков А.Н. Криминалистический подход к дистанционным хищениям // Вестник Казанского юридического института МВД России // Вестник Казанского юридического института МВД России. 2025. Т. 16. № 4 (62). С. 185 – 192.

Scientific article
UDC 343

# FORENSIC APPROACH TO REMOTE THEFT

Aslyam Nailevich Khalikov,
Moscow Academy of the Investigative Committee of
Russian Federation named after A.Ya. Sukharev, Moscow, Russia,
Ufa University of Science and Technology, Ufa, Russia,
han010@yandex.ru

***Abstract***

**Introduction:** the article examines the problems of multi-billion dollar thefts committed remotely: by secretly writing off funds from citizens' bank accounts or by deceiving citizens, as a result of which the latter transfer their money to the bank accounts of criminals. The detection rate of these crimes is minimal.

**Materials and Methods:** the methodological basis of the article was the general method of material-dialectical cognition in the study of issues of virtual methods of remote thefts using digital and psychological-linguistic methods of stealing citizens' money. The article uses general scientific research methods, in particular, comparative legal, systemic and structural, and also applies analysis as a specific scientific method of cognition.

**Discussion and Conclusions:** there are many ways of remote theft, and they all depend on the methods of penetration of criminals into banking systems or on the degree of psychological influence on a person. The detection rate of such acts is very low. Criminal liability is mainly brought to accomplices who do not play an active role in committing crimes. These problems are solved depending on the establishment of specific circumstances of the act and their proof based on the results of the investigation.

**Results:** forensic activity, including general provisions of law enforcement, operational-search and investigative work requires a radical restructuring of the methods of detection, detection and investigation of remote theft. New approaches to interaction with telecom operators, banks, transformation of obtaining court permissions for investigative actions and operational-search activities are needed. In this regard, the interests of banks and mobile operators will be limited to a certain extent

*Keywords: banking operations; remote theft; cybercrime; theft; fraud; deception; methods of crime*



**For citation:** Khalikov A.N. Forensic Approach to Remote Theft. Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia Bulletin of the Kazan Law Institute of MIA of Russia. 2025;16(4):185-192. (In Russ.).

## Введение

Сегодня количество хищений, совершаемых дистанционно, вышло на уровень значительного преступного вала, увеличивающегося и ускоряющегося, темпами, перед которым государство и правоохранительные органы пока не в силах устоять. По последним данным, объем хищений денежных средств, совершенных с применением средств мобильной связи, составляет от 150 до 250 млрд рублей в год, посягательству подвергается 83% населения России, то есть практически все, кто пользуется средствами сотовой связи [1]. Из этого объем хищений у граждан только по банковским вкладам составил в 2024 году 27 миллиардов рублей [2, с. 1, 5]. В то же время раскрываемость преступлений, совершенных с использованием мобильных средств связи, в 2024 г. составила лишь 12,8%, а раскрываемость преступлений, совершенных в сети Интернет, – 21,6%. При этом уголовная статистика показывает, что доля дистанционных преступлений в общем массиве всех преступлений приближается к 40%, когда почти соответственно росту дистанционных хищений более чем наполовину снижается количество краж, грабежей, разбоев [3, с. 35 – 39].

Особенностью дистанционных хищений денежных средств является особое – виртуальное – пространство, где нет государственных границ, поскольку цифровая среда объединяет мир в особое поле человеческой деятельности, в том числе криминальное. Данный эволюционный фактор развития цифрового компонента в мире неизменим, как и неустранимы сами явления сохранения и совершенствования киберпреступности и создаваемые ею новые способы дистанционных хищений. Как пишет О.В. Дамаскин, складывается ситуация, когда не внедрять новые технологии

невозможно, потому что это объективный процесс, но как и кем это будет реально использовано, ясности нет, что образует опасную ситуацию неопределенности [4, с. 75].

Соответственно, криминалистическая характеристика дистанционных хищений, совершаемых с использованием средств связи, показывает тесную связь с цифровым пространством, с киберпреступлениями, являясь их частью, когда активно используются компьютерные и иные цифровые устройства или новые телекоммуникационные технологии. Как определяет Верховный Суд РФ, к числу подобных компьютерных устройств могут быть отнесены любые электронные устройства, способные принимать, обрабатывать, хранить и передавать информацию, закодированную в форме электрических сигналов: мобильные телефоны, смартфоны, иные электронные устройства, способные взаимодействовать друг с другом или с внешней средой без участия человека. Для совершения рассматриваемых хищений применяется совокупность способов, типичных для киберпреступлений: заражение компьютерными вирусами-шпионами и кибератаки, создание ложных объектов в виде поддельных документов, включая паспорта, дипфейки и др. [5, с. 61 – 64]. В различных вариациях перечисленные и другие современные технологии могут быть использованы для совершения сложных дистанционных хищений, которые трудно поддаются своевременному выявлению, раскрытию и пресечению. На этом фоне современные реалии международных отношений, недостаточный уровень взаимодействия правоохранительных органов России с зарубежными правоохранительными организациями, слабость оперативно-технического оснащения показывают, что своевременное и эффективное раскрытие и расследование транснациональных преступлений, включая дистанционные хищения, требуют существенного совершенствования.

Одним из серьезных недостатков криминалистического подхода в борьбе с дистанционными хищениями является законодательный и практический разрыв между оперативно-розыскной и следственной деятельностью. В свое время А.Ф. Волынский писал, что что ни в одной из западно-европейских стран нет столь категоричного и искусственного разграничения оперативно-розыскной и процессуальной деятельности, а в некоторых из них исторически сложилось и нашло законодательное закрепление так называемое «полицейское расследование», в котором органически сочетаются гласные и негласные методы и средства получения доказательств, но под действенным контролем судебных органов [6, с. 5].

Также к основным причинам роста числа дистанционных хищений и их низкой раскрываемости относятся факторы, требующие тесного взаимодействия с соответствующими организациями:

– невозможность тесного сотрудничества правоохранительных органов с операторами сотовой связи, посредством которой совершаются мошенничества. Любое установление информации о телефонных соединениях требует судебных санкций, на что необходимо определенное время и процедуры;

– невозможность тесного сотрудничества правоохранительных органов с банками, которые слабо контролируют систему безопасности при движении денежных средств в дистанционном режиме. Любое установление информации о банковских операциях также требует судебных санкций, а значит времени;

– слабый уровень либо полное отсутствие международного сотрудничества правоохранительных органов России с зарубежными правоохранительными органами.

В связи с этим на сегодня УПК РФ и ФЗ «Об оперативно-розыскной деятельности» с криминалистических позиций недостаточно обеспечивают оперативный и доказательственный сектор борьбы с дистанционными хищениями.

**Материалы и методы**

Как известно, криминалистика изучает закономерности совершения, выявления, раскрытия, пресечения, расследования и предупреждения преступлений [7, с. 116 – 117]. С позиций методики расследования отдельных видов преступлений, чтобы познать и раскрыть преступление, необходимо смоделировать его криминалистическую характеристику, установить механизмы совершения преступных действий, психологическую линию криминального события, познав в системном единстве особенности способов совершения рассматриваемых преступлений, в том числе дистанционных [8, с. 102 – 106]. Затем на основе полученных данных разработать организационные положения расследования преступлений, которые влияют на формирование различных следственных ситуаций, планирование процесса расследования и в целом на установление всех обстоятельств, подлежащих доказыванию (ст. 73 УПК РФ).

Конструктивные способы дистанционных хищений постоянно изменяются в зависимости от конкретной криминальной ситуации. В этом отношении способы совершения дистанционных хищений можно классифицировать на контакт-

ные и бесконтактные. Первыми, как правило, совершаются мошенничества, поскольку хищения денег осуществляются в результате речевого или виртуального контакта мошенника с жертвой. Бесконтактный способ исключает непосредственное общение, когда совершаются кражи, то есть тайные хищения денежных средств дистанционным путем.

Несмотря на то что речь идет о составе мошенничества или кражи, в данном случае мы говорим о деяниях совершенно нового свойства, связанных с виртуальными отношениями материи и человека. Потерпевшее лицо часто не может увидеть или оценить криминальную обстановку, не способно противостоять психическому воздействию, когда доминирующим направлением отношений между людьми является процесс доверия к друг другу. Это позволяет получить доступ к денежным средствам, находящимся в банке, или открыть счет на имя потерпевшего с оформлением кредита без его согласия с целью последующего хищения кредитных средств.

С позиций следовой картины криминалистики, идеальные, или вербальные, отношения переходят в виртуальные, а затем в материальные. То есть изначально происходит некая игра с психикой человека, когда субъект не в состоянии контролировать свои действия и становится ведомым при совершении хищений. В этом отношении отличают дистанционные хищения от других преступлений следующие факторы или отличительные элементы их криминалистической характеристики:

- использование чувства доверия психологически неподготовленных лиц по отношению к посторонним лицам из числа преступников;

- использование средств сотовой связи для контакта с потерпевшим;

- использование банковских технологий дистанционного обслуживания граждан, работающих в автономном режиме;

- скорость и скрытость проведения речевых приемов и дистанционных денежных акций в цифровом пространстве;

- разнообразие и «художественность» способов дистанционных хищений со стороны преступников.

Основным действующим элементом при совершении дистанционных мошенничеств является психология контакта между преступником и потерпевшим [9, с. 16]. Специалисты по анализу речевого общения называют несколько апробированных подходов и приемов, применяемых к жертве мошенничества с целью выполнить необходимые действия для хищения денег, к числу которых относятся речевые приманки, когда положительные ориентированы на человеческую жадность, а отрицательные – на страх. В таком ключе психологической основой речевых афер является дестабилизация жертвы, когда сообщаемая информация нарушает мировосприятие человека, а также интимность и, учитывая особенности телефонной связи, невозможность вмешательства других лиц.

Сегодня специалисты, благодаря компьютерному моделированию, могут распознавать речь мошенников [10, с. 83 – 89; 9, с. 93 – 99] и даже вести их учет, создавая «голосовые портреты» [11, с. 89 – 96]. Более того, существуют специальные телефонные программы отвлечения телефонных мошенников ничего не значащими разговорами [12, с. 8].

Далее, с учетом состояния жертвы, совершаются различные манипуляции, результатом которых являются действия потерпевшего по перечислению денег преступнику [13, с. 65 – 72]. При манипуляциях с применением методов социальной инженерии расчет делается на такие качества, как любопытство, невнимательность, доверчивость [14, с. 110 – 113;].

На основе криминалистических закономерностей дистанционных хищений возможно прогнозировать дальнейшее развитие их криминальных тенденций, которые необходимо использовать при осуществлении оперативно-розыскных мероприятий и следственных действий. В то же время такое прогнозирование включает в содержание действий преступников и реагирование на эти действия правоохранительных органов, банков, операторов сотовой связи, иных организаций, обеспечивающих работу в цифровом пространстве (например, организации по переводу денег за рубеж). Соответственно, содержание тактики деятельности оперативных работников по активной борьбе с дистанционными хищениями должно содержать не просто взаимодействие с банковскими структурами или операторами сотовой связи, а практически внедрение в деятельность данных организаций при сотрудничестве с соответствующими службами безопасности. Невозможно вести активную борьбу с дистанционными хищениями, находясь вне механизмов банковской деятельности и сотовых операторов. Но для подобной деятельности требуется правовое обеспечение, что возможно выполнить на основе криминалистических исследований.

Как условно положительный пример можно привести ст. 115-2 УПК РФ о полномочиях следователя или дознавателя по приостановлению операций с денежными средствами, введенную

Федеральным законом от 31 июля 2025 г. (№ 278-ФЗ). Названная норма дает следователю (дознавателю) право приостановить банковские операции с любыми денежными средствами путем вынесения постановления с согласия руководителя следственного органа. Однако до применения предоставленных следователю или дознавателю полномочий он должен возбудить уголовное дело, выполнить ряд процессуальных и следственных действий и только затем вынести решение о приостановке денежных операций. Вряд ли это будет эффективно, если дистанционные хищения будут совершены в течение минимального времени с обналичиванием похищенных денег. Соответственно, подобные полномочия о приостановлении денежных операций должны быть и у органов, осуществляющих оперативно-розыскную деятельность, тогда быстрое и эффективное взаимодействие оперативных и следственных мер будет вести к успеху по пресечению и раскрытию рассматриваемых преступлений.

В то же время банк сам может немедленно приостановить платежную операцию на двое суток на основании ст. 8 ФЗ «О национальной платежной системе» при наличии соответствующих сведений о подозрениях криминального характера. И именно в этом случае будет эффективным тесное взаимодействие банков, оперативно-розыскных и следственных органов.

**Результаты исследования**

Изучение уголовных дел в следственных подразделениях МВД России и результаты мониторинга сообщений из средств массовой информации показывают, что *дистанционные мошенничества* совершаются в основном в зависимости от интеллекта и возможностей преступных элементов, которые в виртуальном пространстве постоянно множатся и совершенствуются. Звонки от преступников идут якобы от службы госуслуг, налоговой службы, пенсионного фонда, медицинских учреждений, вневедомственной охраны или службы установки дверей и т.д. В результате перечисленных действий у потерпевших лиц похищаются деньги на банковских вкладах, на них может быть оформлен кредит, а денежные средства переводятся на счета преступников.

Возможно ли с помощью оперативных и следственных действий, а в целом криминалистического обеспечения борьбы с дистанционными хищениями эффективно противостоять действиям преступников? Как мы указали, для этого необходимо право оперативных органов быть вводимыми в работу банковских структур и в систему деятельности операторов связи. Так, пока происходит разговор преступника с будущей жертвой по телефонной связи, оперативные работники могут об этом не знать, да и самого хищения в данном случае не существует, а лишь происходит подготовка к совершению мошенничества или кражи. Однако когда начинается движение денежных средств с необычными, а значит, большими суммами, с переводом на неизвестные счета, не использовавшиеся до этого клиентом банка, иные операции, не характерные для наблюдаемого (проверяемого) лица, то это должно быть основанием для начала оперативной проверки денежной операции и лица ее осуществляющего, началом проведения системы оперативно-розыскных мероприятий. Причем банковская практика определила подозрительные банковские операции, как в отдельном нормативном акте – Приложении к Положению Банка России от 2 марта 2012 г. № 375-П «О требованиях к правилам внутреннего контроля кредитной организации в целях противодействия легализации (отмыванию) доходов, полученных преступным путем и финансированию терроризма», так и в других нормативных актах Банка России. Однако, несмотря на достаточную разработанность названных нормативных актов, демонстрирующих множество алгоритмов преступных действий в банковской и финансовой сфере, они, к сожалению, мало истребованы в оперативно-розыскных и следственных целях по пресечению и раскрытию преступлений.

Подобная оперативная проверка может допустить оперативный эксперимент путем имитации перечисления денег либо попытки перечисления на требуемый счет с организацией наблюдения за соответствующими лицами, использующими данный счет. В информационном плане со стороны оперативно-розыскных органов следует совмещение необычных перечислений и абонентских контактов между клиентом банка и владельцем счета, на который перечисляются деньги. Затем, в зависимости от развития оперативной ситуации, следуют дальнейшие действия оперативных работников вплоть до задержания соответствующих лиц и начала уголовного преследования после возбуждении уголовного дела.

Мы привели наиболее типичный алгоритм действий, который возможно выполнить активными действиями оперативных работников и следователей. Заметим, что все это производится в течение короткого времени и, разумеется, без судебных санкций, но с последующим информированием прокурора и суда и получением разрешения на арест банковского счета. В то же время на сегодня подобные действия затруднены, поскольку ни банки, ни операторы сотовой связи не допустят оперативных работников к своей де-

ятельности без судебных санкций в системе немедленного реагирования при начале совершения преступлений. Поэтому следует разрабатывать нормативный материал, приемлемый как для целей деятельности правоохранительных органов, так и интересов коммерческих организаций в виде банков и операторов сотовой связи.

Опыт оперативно-розыскной и следственной работы позволяет говорить о необходимости упреждающего направления криминалистической деятельности. Недостаточная раскрываемость показывает отсутствие должной наступательности в сфере дистанционных хищений, совершаемых в условиях крайней неочевидности. В то же время к мерам оперативной работы относятся такие активные оперативно-розыскные мероприятия как проверочная закупка, оперативный эксперимент, контролируемая поставка, которые осуществляются практически совместно со следователями и направлены непосредственно на выявление и раскрытие как преступления, так и преступников. К сожалению, мы не встречали попыток оперативного эксперимента после телефонного звонка мошенников или контролируемой поставки денег через банковские операционные системы. Причем в данном случае исключается провокация преступления, поскольку первый шаг к совершению хищения делает преступник путем телефонного звонка, а далее следуют меры оперативно-розыскного характера при сопровождении их следственными действиями.

**Обсуждение и заключение**

Криминалистическая характеристика дистанционных хищений, но, к сожалению, не опыт их раскрытия и расследования, которого пока очень немного, актуализируют мысль о необходимости оптимального соотношения следственной и оперативно-розыскной деятельности в связи с вызовами преступлений в цифровом пространстве. Криминалистика изучает закономерности совершения преступлений и соответствующие им закономерности раскрытия и расследования этих преступлений (Р.С. Белкин). И вторая часть данного определения – закономерности – требует эффективной взаимодействующей деятельности оперативно-розыскных служб и следственных подразделений.

Как мы указали выше, сегодня возможно принять самые элементарные меры выявления и пресечения названных преступлений – предоставить больше прав оперативным работникам и следователям при получении информации из банков и операторов сотовой связи; разрешить работникам следственно-оперативных органов немедленное блокирование переводов денег с последующим получением судебной санкции (в течение трех суток) без возбуждения уголовного дела; переводы за рубеж больше определенной суммы осуществлять только после их проверки правоохранительными органами и т.д. Такие предложения звучат во множестве исследований по данной теме, однако проблема в сфере правоохранительной деятельности, с позиций криминалистического подхода очень медленно решается [15, с. 78 – 85].

Раскрытие любого дистанционного преступления требует своевременного получения информации, быстрой реакции на действия преступников, а в современных условиях – владения новыми технологиями, такими как нейросети, искусственный интеллект, большие данные [16, с. 364 – 393; 17, с. 37 – 43]. Однако количество и качество совершаемых в цифровой среде преступлений показывает, что пока действующими оперативными, криминалистическими или правовыми механизмами с такими преступлениями бороться затруднительно в силу названных выше причин.

## СПИСОК ИСТОЧНИКОВ

1. Вихарева Е. Мошенники совершенствуют схемы и готовятся разводить даже самых продвинутых пользователей. URL: www.kommersant.ru (дата обращения: 06.02.2025).
2. Маркелов Р. В нажиме реального времени // Российская газета, 20 февраля 2005 г. № 38 (9577).
3. Павлинов А.В., Помыкалова И.В. «Телефонное мошенничество» и провокация дачи взятки как новая угроза безопасности Российского государства // Журнал зарубежного законодательства и сравнительного правоведения. 2023 Т. 19, № 4.
4. Дамаскин О.В. Актуальные криминологические аспекты противодействия преступности в современном цифровом обществе: проблемы и перспективы // Труды Института государства и права РАН. 2021. Т. 16, № 1.
5. Бешукова З.М. Мошенничество с использованием методов социальной инженерии: механизм совершения и основные способы защиты // Цифровые технологии и право: сборник научных трудов II Международной научно-практической конференции: в 6 т. Казань, 2023. Т. 1.

6. Волынский А.Ф. Уголовное судопроизводство, задачи и социальные функции криминалистики в его реформировании / Актуальные проблемы теории и практики уголовного судопроизводства и криминалистики: Вопросы современной криминалистики. Сборник статей. Москва, 2004. Часть 2. С. 5.
7. Белкин Р.С. Курс криминалистики в 3 т. Т. 1. Общая теория криминалистики. Москва: Юристъ, 199
8. Машлякевич В.А. К вопросу о структуре и содержании криминалистической характеристики мошенничеств, совершаемых с использованием средств телефонной связи // Алтайский юридический вестник. 2026. № 2.
9. Русскевич Е.А. Актуальные проблемы противодействия хищениям в системе дистанционного банковского обслуживания // Имущественные отношения в Российской Федерации. 2022. № 8 (251).
10. Филимонов А.В., Осипов А.В., Плешакова Е.С., Гатауллин С.Т. Нейросетевые методы распознавания эмоций речи для противодействия мошенничеству в телекоммуникационных системах // Вопросы кибербезопасности. 2022. № 6 (52).
11. Белоусов А.Д. Опросный инструментарий для выявления когнитивно-стилевых предпосылок устойчивости к телефонным мошенникам // Актуальные проблемы психологии правоохранительной деятельности: концепции, подходы, технологии (Васильевские чтения – 2023): материалы международной научно-практической конференции / под ред. Ю.А. Шаранова, В.Л. Ситникова. Санкт-Петербург, 2023.
12. Ярославцева И.В. Критическое мышление пожилых людей – жертв мошеннических действий: теоретический и прикладной аспекты исследования // Известия Иркутского государственного университета. Серия: Психология. 2016. Т. 15.
13. Боровичок А. Десять ударов по мошенникам // Российская газета 26 июня 2025 г. № 138 (9677).
14. Гумаров И.А., Тырышкин В.В. Кражи с банковского счета, а равно в отношении электронных денежных средств: проблемы раскрытия // Вестник Казанского юридического института МВД России. 2024. Т. 15. № 4 (58).
15. Маркелов Р. Вылет без купюр // Российская газета, 21 февраля 2025 г. № 39 (9578).
16. Ткачук Т.А., Михайлов А.Е., Цапанов Р.Е. Социальная инженерия как способ манипуляции людьми с целью получения информации или доступа к ней: обзор проблемы // Вестник Владимирского юридического института. 2021. № 4 (61).
17. Овчинский А.С. Оперативно-розыскная аналитика на пути к искусственному интеллекту // Актуальные проблемы теории оперативно-розыскной деятельности / под общ. ред. К.К. Горяинова, В.С. Овчинского. Москва: "Инфра-М", 2017. С. 364-393.

**REFERENCES**

1. Vihareva E. Moshenniki sovershenstvuyut skhemy i gotovyatsya razvodit' dazhe samyh prodvinutyh pol'zovatelej. URL: www.kommersant.ru (data obrashcheniya: 06.02.2025).
2. Markelov R. V nazhime real'nogo vremeni // Rossijskaya gazeta, 20 fevralya 2005 g. № 38 (9577).
3. Pavlinov A.V., Pomykalova I.V. «Telefonnoe moshennichestvo» i provokaciya dachi vzyatki kak novaya ugroza bezopasnosti Rossijskogo gosudarstva // Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniya. 2023 T. 19, № 4.
4. Damaskin O.V. Aktual'nye kriminologicheskie aspekty protivodejstviya prestupnosti v sovremennom cifrovom obshchestve: problemy i perspektivy // Trudy Instituta gosudarstva i prava RAN. 2021. T. 16, № 1.
5. Beshukova Z.M. Moshennichestvo s ispol'zovaniem metodov social'noj inzhenerii: mekhanizm sovershеniya i osnovnye sposoby zashchity // Cifrovye tekhnologii i pravo: sbornik nauchnyh trudov II Mezhdunarodnoj nauchno-prakticheskoj konferencii: v 6 t. Kazan', 2023. T. 1.
6. Volynskij A.F. Ugolovnoe sudoproizvodstvo, zadachi i social'nye funkcii kriminalistiki v ego reformirovanii / Aktual'nye problemy teorii i praktiki ugolovnogo sudoproizvodstva i kriminalistiki: Voprosy sovremennoj kriminalistiki. Sbornik statej. Moskva, 2004. Chast' 2. S. 5.
7. Belkin R.S. Kurs kriminalistiki v 3 t. T. 1. Obshchaya teoriya kriminalistiki. Moskva: Yurist", 199
8. Mashlyakevich V.A. K voprosu o strukture i soderzhanii kriminalisticheskoj harakteristiki moshennichestv, sovershaemyh s ispol'zovaniem sredstv telefonnoj svyazi // Altajskij yuridicheskij vestnik. 2026. № 2.
9. Russkevich E.A. Aktual'nye problemy protivodejstviya hishcheniyam v sisteme distancionnogo bankovskogo obsluzhivaniya // Imushchestvennye otnosheniya v Rossijskoj Federacii. 2022. № 8 (251).
10. Filimonov A.V., Osipov A.V., Pleshakova E.S., Gataullin S.T. Nejrosetevye metody raspoznavaniya emocij rechi dlya protivodejstviya moshennichestvu v telekommunikacionnyh sistemah // Voprosy kiberbezopasnosti. 2022. № 6 (52).

11. Belousov A.D. Oprosnyj instrumentarij dlya vyyavleniya kognitivno-stilevyh predposylok ustojchivosti k telefonnym moshennikam // Aktual'nye problemy psihologii pravoohranitel'noj deyatel'nosti: koncepcii, podhody, tekhnologii (Vasil'evskie chteniya – 2023): materialy mezhdunarodnoj nauchno-prakticheskoj konferencii / pod red. Yu.A. Sharanova, V.L. Sitnikova. Sankt-Peterburg, 2023.
12. Yaroslavceva I.V. Kriticheskoe myshlenie pozhilyh lyudej – zhertv moshennicheskih dejstvij: teoreticheskij i prikladnoj aspekty issledovaniya // Izvestiya Irkutskogo gosudarstvennogo universiteta. Seriya: Psihologiya. 2016. T. 15.
13. Borovichok A. Desyat' udarov po moshennikam // Rossijskaya gazeta 26 iyunya 2025 g. № 138 (9677).
14. Gumarov I.A., Tyryshkin V.V. Krazhi s bankovskogo scheta, a ravno v otnoshenii elektronnyh denezhnyh sredstv: problemy raskrytiya // Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii. 2024. T. 15. № 4 (58).
15. Markelov R. Vylet bez kupyur // Rossijskaya gazeta, 21 fevralya 2025 g. № 39 (9578).
16. Tkachuk T.A., Mihajlov A.E., Capanov R.E. Social'naya inzheneriya kak sposob manipulyacii lyud'mi s cel'yu polucheniya informacii ili dostupa k nej: obzor problemy // Vestnik Vladimirskogo yuridicheskogo instituta. 2021. № 4 (61).
17. Ovchinskij A.S. Operativno-rozysknaya analitika na puti k iskusstvennomu intellektu // Aktual'nye problemy teorii operativno-rozysknoj deyatel'nosti / pod obshch. red. K.K. Goryainova, V.S. Ovchinskogo. Moskva: \"Infra-M\", 2017. S. 364-393.

**Информация об авторе:**
**Халиков Аслям Наилевич,** доктор юридических наук, профессор, профессор кафедры криминалистики Московской академии Следственного комитета Российской Федерации имени А.Я. Сухарева, Уфимский университет науки и технологий, e-mail: han010@yandex.ru
Автор прочитал и одобрил окончательный вариант рукописи.

**Information about the author:**
**Khalikov Aslyam N.,** Doctor of Law, Professor, Professor of the Department of Criminology at the Moscow Academy of the Investigative Committee of the Russian Federation named after A.Ya. Sukharev, Ufa University of Science and Technology, e-mail: han010@yandex.ru
The author has read and approved the final version of the manuscript.

Статья получена: 20.08.2025.
Статья принята к публикации: 26.12.2025.
Статья опубликована онлайн: 26.12.2025.
Против размещения полнотекстовой версии статьи в открытом доступе в сети Интернет не возражаю.