Научная статья
УДК 343.98
DOI: 10.37973/VESTNIKKUI-2024-58-10

КРАЖИ С БАНКОВСКОГО СЧЕТА, А РАВНО В ОТНОШЕНИИ ЭЛЕКТРОННЫХ ДЕНЕЖНЫХ СРЕДСТВ: ПРОБЛЕМЫ РАСКРЫТИЯ

Ильнур Асгатович Гумаров,
Казанский юридическийо институт МВД России, Казань, Россия,
ilnur_gumar@mail.ru
Тырышкин Виктор Владимирович,
Барнаульский юридический институт МВД России, Барнаул, Россия,
witsan333@yandex.ru

Аннотация

Введение: в статье рассматриваются особенности совершения краж денежных средств с банковского счета, а равно в отношении электронных денежных средств; принимаемые сотрудниками органов внутренних дел меры по раскрытию таких преступлений; даются рекомендации по совершенствованию работы полиции в данной сфере.

Материалы и методы: использованы социологический метод и интервьюирование сотрудников оперативных подразделений, а также проведено изучение уголовных дел и нормативных правовых актов, регламентирующих деятельность оперативных подразделений органов внутренних дел. Применялся контент-анализ научных статей.

Результаты исследования: авторами выработаны предложения по совершенствованию деятельности правоохранительных органов в сфере противодействия кражам с банковского счета, а равно в отношении электронных денежных средств.

Обсуждение и заключение: авторы предлагают наделить оперативные подразделения территориальных органов внутренних дел на районном уровне (именно они сталкиваются с проблемой раскрытия преступлений на первоначальном этапе) полномочиями по прямому обращению к кредитно-финансовым организациям и операторам связи в рамках проведения оперативно-розыскных мероприятий и возможностью получения в режиме реального времени сведений о пользователях соответствующих услуг.

В настоящее время необходимо создать единую межведомственную платформу взаимодействия для получения сведений о всех транзакциях денежных средств в «одном окне». Такую платформу можно реализовать в ФинЦЕРТ Банка России.

Ключевые слова: кража денежных средств с банковского счета; документирование краж с банковского счета; раскрытие кражи с банковского счета; кражи в отношении электронных денежных средств; п. «г» ч. 3 ст. 158 УК РФ; с использованием электронных средств платежа

Для цитирования: 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). С. 78 – 85. DOI: 10.37973/VESTNIKKUI-2024-58-10

Scientific article
UDC 343.98
DOI: 10.37973/VESTNIKKUI-2024-58-10

BANK ACCOUNTS FRAUD AND ONLINE BANKING FRAUD: DISCLOSURE ISSUES

Ilnur Asgatovich Gumarov,
the Kazan Law Institute of the Ministry of Internal Affairs of the Russian Federation, Kazan, Russia,
ilnur_gumar@mail.ru
Victor Vladimirovich Tyryshkin,
Barnaul Law Institute of the Ministry of Internal Affairs of the Russian Federation,
Barnaul, Russia,
witsan333@yandex.ru

Abstract

Introduction: the authors consider features of bank accounts fraud, as well as online banking fraud; crime detection methods taken by internal affairs bodies; recommendations to improve police action in this field.

Materials and Methods: sociological method and interviewing law enforcement officers, as well as criminal cases study and regulatory acts regulating law enforcement activity of the Russian Federation were used when investigating bank accounts fraud, as well as online banking fraud. The authors used content-analysis of scientific articles and

Results: the authors suggest proposals to improve the work of law enforcement in the area of combating bank accounts fraud and online banking fraud.

Discussion and Conclusions: the authors suggest authorize the local internal affairs bodies at district level (they are the ones who face the challenge of solving of crime at the initial stage) to direct appeal to financial institutions and network operators in investigations and obtain information about the users in real-time.

Nowadays it is important to create a single interdepartmental platform to obtain information about all transactions in “a single chart”. Such a platform can be implemented in the Financial Sector Computer Emergency Response Team of the Bank of Russia.

Keywords: theft of funds from a bank account; documentation of thefts from a bank account; disclosure of theft from a bank account; theft in relation to electronic funds; paragraph "d" of Part 3 of Article 158 of the Criminal Code of the Russian Federation; using electronic means of payment

For citation: Gumarov I.A., Tyryshkin V.V. Bank Accounts Fraud and Online Banking Fraud: Disclosure Issues. Bulletin of the Kazan Law Institute of MIA of Russia. 2024;15(4):78-85. (In Russ.). DOI: 10.37973/VESTNIKKUI-2024-58-10

Введение

В последнее десятилетие компьютерные технологии стали применять практически во всех сферах жизнедеятельности человека, активно развиваются интернет-торговля, криптовалютные биржи, цифровые продукты кредитно-финансовых организаций.

Цифровые ресурсы используются и при предоставлении государственных услуг, кредитов для населения. Граждане все чаще совершают покупки дистанционно, приобретая товары или услуги через Интернет и дистанционное банковское обслуживание. Электронные торговые платформы значительно помогают сэкономить время потребителей.

Цифровые ресурсы обмена денежными средствами все чаще становятся предметом преступных посягательств. Наиболее распространенными стали хищения денежных средств, находящихся на счетах граждан. Противодействие данной категории преступлений является одним из приоритетных направлений деятельности органов внутренних дел. Стало распространенным неправомерное завладение данными банковских карт для дальнейшей кражи денег со счетов граждан. Часто такие действия связаны с созданием интернет-площадок, в том числе с использованием «зеркальных» сайтов (схожих с официальными, которые принадлежат известным организациям), взломом страниц в социальной сети и др.

Обман для получения доступа к банковским картам и последующей краже денег на интернет-площадках бесплатных объявлений имеет схожий сценарий, когда преступники звонят инициатору объявления о продаже и представляются заинтересованной стороной, продавец сообщает номер банковской карты для перевода средств, «фиктивный покупатель» под различным предлогом выманивает SMS-пароль подтверждения перевода средств. Заключительный этап имеет разные варианты реализации преступного умысла, например, преступник просит через банкомат подключить к своей карте посторонний номер (якобы для подтверждения достоверности номера телефона перед банком), получает доступ к мобильному банку и списывает все денежные средства со счета граждан.

Кроме этого, завладение логинами и паролями к цифровым банковским продуктам потерпевших происходит путем проведения массовых рассылок электронных писем от имени популярных брендов, личных сообщений внутри различных сервисов, например, от имени банка или внутри социальных сетей.

Способы совершения данных деяний постоянно совершенствуются, становятся все более изощренными и латентными. Следует отметить, что денежные средства, находящиеся на виртуальных банковских картах, а также электронных счетах, утрачивают свойства материальных объектов. Этот факт усложняет уголовно-процессуальные возможности проведения в отношении них таких следственных и процессуальных действий, как выемка, осмотр, приобщение к материалам уголовного дела в качестве вещественных доказательств и т.д.

Обзор литературы

В последние несколько лет в связи с актуальностью рассматриваемых преступлений появилось много литературы и методических рекомендаций, посвященных борьбе с хищениями денежных средств с банковского счета, а равно в отношении электронных денежных средств. Об этом писали Е.А. Адмиралова [1], Л.Н. Бочарникова [2], А.С. Пудовиков [3], Е.А. Русскевич [5], А.Г. Саакян [4], С.В. Скляров [6], Б.Э. Шавалеев [8], К.Б. Чернова [5] и др.

Нормативная правовая основа отражена в Уголовном и Уголовно-процессуальном кодексах Российской Федерации, федеральных законах «О полиции»[1], «Об оперативно-розыскной деятельности»[2], «О связи»[3], «О национальной платежной системе»[4], «О банках и банковской деятельности»[5], приказе МВД России от 31.03.2023 № 199 «Об утверждении Перечня оперативных подразделений органов внутренних дел Российской Федерации, правомочных осуществлять оперативно-розыскную деятельность».

Материалы и методы

В процессе исследования применялись социологические методы опроса и интервьюирования сотрудников оперативных подразделений, а также изучение уголовных дел в МВД по Республике Татарстан, нормативных правовых актов, регламентирующих деятельность оперативных подразделений органов внутренних дел. Также проведен контент-анализ научных статей.

Результаты исследования

Исследуемое преступление предусмотрено п. «г» ч. 3 ст. 158 УК РФ и очень похоже на деяние, охватываемое диспозицией ст. 159^3 УК РФ. Эти составы предусматривают применение преступником в качестве средства совершения противоправного деяния электронных средств платежа (ЭСП). В то же время в рамках статьи не преследуется цель исследования уголовно-правовых особенностей указанных хищений, они затрагиваются лишь в связи с особенностями применения сотрудниками правоохранительных органов мер по раскрытию краж с банковского счета, а равно в отношении электронных денежных средств.

Рассматриваемые деяния суды чаще всего квалифицируют по п. «г» ч. 3 ст. 158 УК РФ как тайное хищение чужого имущества, совершённое с банковского счёта, как правило, при отсутствии признаков преступления, предусмотренного ст. 159^3 УК РФ, и с учетом смягчающих обстоятельств назначают небольшие сроки, обычно до

[1] О полиции: Федеральный закон от 07.02.2011 № 3-ФЗ // Собрание законодательства Российской Федерации. 2011. 14 февраля. № 7. Ст. 900.

[2] Об оперативно-розыскной деятельности: Федеральный закон от 12.08.1995 № 144-ФЗ // Собрание законодательства Российской Федерации. 1995. 14 августа. № 33. Ст. 3349.

[3] О связи: Федеральный закон от 07.07.2003 № 126-ФЗ (ред. от 04.08.2023) (с изм. и доп., вступ. в силу с 01.12.2023). СПС «КонсультантПлюс» (дата обращения: 10.07.2024).

[4] О национальной платежной системе: Федеральный закон от 27.06.2011 № 161-ФЗ (ред. от 19.12.2023) (с изм. и доп., вступ. в силу с 25.07.2024). СПС «КонсультантПлюс» (дата обращения: 18.08.2024).

[5] О банках и банковской деятельности: Федеральный закон от 02.12.1990 № 395-1 (ред. от 22.07.2024). СПС «КонсультантПлюс» (дата обращения: 18.08.2024).

двух лет лишения свободы условно (без изоляции от общества)[1].

Соглашаясь с Е.А. Адмираловой [1], отметим, что если у лица отсутствует право на распоряжение чужим имуществом, хищение совершено против воли потерпевшего в условиях неочевидности для последнего и других лиц, то деяние следует квалифицировать по п. «г» ч. 3 ст. 158 УК РФ.

Изучение судебной практики за последние два года в различных регионах России позволяет сделать вывод, что после изменения уголовного законодательства и разъяснений Верховного Суда Российской Федерации суды чаще всего стали вменять именно кражу. Так, например, несмотря на то, что обвиняемый обманным путем получал доступ к банковским приложениям под предлогом оплаты услуг на интернет-площадке «Авито» или под предлогом необходимости совершения денежного перевода за услуги репетиторства (многоэпизодное уголовное дело), суд квалифицировал такие действия как тайное хищение чужого имущества, совершенное с банковского счета[2].

Следует отметить, что, несмотря на «тонкую грань» между этими составами преступлений, значительно отличаются санкции за их совершение. Максимальное наказание за совершение преступления, предусмотренного ч. 1 ст. 159[3] УК РФ, – лишение свободы на срок до трех лет, тогда как максимальное наказание за совершение кражи с банковского счета, а равно в отношении электронных денежных средств (п. «г» ч. 3 ст. 158 УК РФ) – лишение свободы на срок до шести лет. То есть рассматриваемый состав преступления уже подпадает по категорию тяжкого преступления.

Указанное, в свою очередь, влияет на выбор оперативно-розыскных мер сотрудниками оперативных подразделений. Так, в соответствии со ст. 8 Федерального закона «Об оперативно-розыскной деятельности»[3], проведение таких оперативно-розыскных мероприятий, как прослушивание телефонных и иных переговоров, оперативный эксперимент, допускается только по преступлениям средней тяжести, тяжким или особо тяжким преступлениям, а также в отношении лиц, которые могут располагать сведениями об указанных противоправных деяниях. Таким образом, в рамках получения информации о совершении хищения с банковского счета возможности проведения оперативно-розыскных мероприятий ограничены при квалификации такого деяния по ч. 1 ст. 159[3] УК РФ, так как такое правонарушение не подпадает даже под преступление средней тяжести.

Кроме того, из смысла ст. 25 УПК РФ прекратить уголовное дело о рассматриваемой краже денег примирением сторон не представляется возможным. При этом за кражу денег с банковской карты на сумму в 1 тыс. рублей (что ранее являлось административным правонарушением) суд имеет право предъявить обвинение по п. «г» ч. 3 ст. 158 УК РФ (то есть в совершении тяжкого преступления).

Исследователями в рассматриваемой сфере высказываются мнения, что ст. 159[3] УК РФ пополнит список «мертвых» норм, исключенных из области фактического правоприменения, в связи с тем что Верховный Суд Российской Федерации акцентирует внимание на наличии тайности при хищениях с использованием ЭСП [5]. Аналогичного мнения придерживается профессор С.В. Скляров [6, с. 107]. В связи с этим, учитывая судебную практику и мнения различных ученых, законодателю следует пересмотреть целесообразность ст. 159[3] УК РФ в действующей формулировке.

Мы исходим из того, что любые манипуляции на техническом устройстве фиксируются в его памяти (от информации о включении до его выключения, в том числе действия в мессенжерах, изменение или создание файлов). При этом есть возможность проанализировать время таких манипуляций [7]. Выявленные манипуляции дают возможность определить алгоритм действий правонарушителя.

Информация о возможном правонарушителе, совершившем кражу с банковского счета, а равно

[1] Приговор Псковского городского суда Псковской области от 22.12.2023 по уголовному делу № 1-661/2023; приговор Псковского городского суда Псковской области от 21.09.2023 по уголовному делу № 1-270/2023; приговор Руднянского районного суда Смоленской области от 27.07.2023 по уголовному делу № 1-76/2023; приговор Дзержинского районного суда г. Ярославля от 10.07.2023 по уголовному делу № 1-316/2023; приговор Яровского районного суда Алтайского края от 22.02.2024 по уголовному делу № 1-13/2024 (1-82/2023); приговор Тихорецкого районного суда Краснодарского края от 22.02.2024 по уголовному делу №1-13/2024; приговор Малодербетовского районного суда Республики Калмыкия от 20.02.2024 №1-11/2024; приговор Йошкар-Олинского городского суда Республики Марий Эл от 26.01.2024 № 1-103/2024 (серия преступлений); приговор Полярного районного суда Мурманской области от 25.01.2024 по уголовному делу № 1-14/2024 (№ 1-111/2023); приговор Невского районного суда города Санкт-Петербурга от 22.01.2024 по уголовному делу № 1-200/2024 (78RS0015-01-2023-008256-52). URL: https://sudact.ru/ (дата обращения: 18.08.2024).

[2] Приговор Набережночелнинского городского суда Республики Татарстан от 30.01.2024 по уголовному делу № 1-2216/2023. URL: https://sudact.ru/ (дата обращения: 18.08.2024).

[3] Об оперативно-розыскной деятельности: Федеральный закон от 12.08.1995 № 144-ФЗ (ред. от 29.12.2022). СПС «КонсультантПлюс» (дата обращения 27.06.2024 г.).

в отношении электронных денежных средств, может быть получена:

- из технического устройства («гаджета») заявителя о преступлении;

- от операторов IP-телефонии (сведения об IP-адресе, MAC-адресе, времени и продолжительности связи, точке доступа к сети Интернет);

- от операторов сотовой связи;

- от операторов платежных систем, банков и иных кредитных учреждений;

- от организаций, представляющих услуги по обмену криптовалютой (различные биржи по выводу «фиатных» денег);

- из технического средства подозреваемого лица;

- из информационных ресурсов сети Интернет.

Для документирования следов преступления с применением информационно-телекоммуникационных технологий наиболее эффективным будет проведение таких оперативно-розыскных мероприятий, как «Исследование предметов и документов», «Наблюдение» и «Сбор образцов для сравнительного исследования». Здесь важно грамотно зафиксировать результаты проведения таких мероприятий. В целях фиксации информации следует использовать фотоаппарат и видеокамеру, такие функции на компьютере, как сочетания клавиш *PrtSc* (позволят зафиксировать снимок экрана и перенести в открытый файл), *Alt PrtSc* (для фиксации отдельного «окна» на экране), *Win Shift S* (для копирования части «окна» на экране). Все эти действия следует проводить в присутствии представителей общественности, которых в дальнейшем можно будет привлечь в качестве свидетелей по уголовному делу.

Для эффективного документирования краж с банковского счета, а равно в отношении электронных денежных средств следует разрабатывать и применять специальные программные средства, которые позволяют деанонимизировать преступников.

Вместе с тем полагаем, необходимо наделить оперативные подразделения территориальных органов внутренних дел на районном уровне полномочиями по прямому обращению к кредитно-финансовым организациям и операторам связи в рамках проведения оперативно-розыскных мероприятий и возможностью получения в режиме реального времени сведений о пользователях соответствующих услуг. Это будет возможно при создании единой межведомственной платформы взаимодействия на основе ФинЦЕРТ Банка России для получения сведений о всех транзакциях денежных средств в «одном окне», с предоставлением возможности оперативного доступа сотрудникам подразделений специальных технических мероприятий.

Также очередной мерой по противодействию указанным правонарушителям может стать ведение на базе подразделений специальных технических мероприятий федерального уровня единой базы подозрительных IP-адресов, номеров телефонов, IMEI, MAC-адресов, веб-сайтов во взаимодействии с операторами сотовой связи и финансово-кредитными организациями. Этими данными смогут пользоваться сотрудники ФинЦЕРТ Банка России при их выгрузке в единую межведомственную платформу взаимодействия.

Кроме того, по нашему мнению, представляется целесообразным внести изменение в ст. 44 Федерального закона «О связи»[1], дополнив ее обязанностями операторов связи по обязательной идентификации абонента с привязкой к конкретному адресу либо гражданину (при пользовании мобильной связью).

Также считаем целесообразным запретить использование СМС-боксов, иных средств для анонимизации абонента частными лицами или организациями без специальной лицензии.

Обсуждение и заключение

Кражи с банковского счета, а равно в отношении электронных денежных средств имеют двойственную природу, которая влияет на причины и условия их совершения: с одной стороны, это преступления против собственности, с другой – они совершаются в сфере информационных технологий.

Необходимо учитывать следующие характеристики рассматриваемых преступлений:

- технические особенности перевода денежных средств;

- общедоступность совершения переводов денег при использовании специальных программных продуктов и инфраструктуры;

- недостаточно своевременный контроль за действиями правонарушителей в информационно-телекоммуникационной среде.

Несмотря на различные манипуляции правонарушителей, следы противоправной деятельности остаются в памяти устройств потерпевших и правонарушителей, серверах операторов связи, в облачных хранилищах, других носителях информации, которые использовались в момент совер-

[1] О связи: Федеральный закон от 07.07.2003 № 126-ФЗ (ред. от 04.08.2023) (с изм. и доп., вступ. в силу с 01.12.2023). СПС «КонсультантПлюс» (дата обращения: 10.07.2024).

шения преступления. Поэтому такие сведения необходимо своевременно документировать и использовать в доказывании по рассмотренным преступлениям.

Интервьюирование сотрудников оперативных подразделений[1], проведение оперативно-розыскных мероприятий с потерпевшими от данных краж дают основание утверждать, что жертвы подобных преступлений не обладают достаточным уровнем знаний в области финансовой и информационной безопасности. Поэтому сотрудникам правоохранительных органов необходимо заранее подготовиться к опросу потерпевших, наметив вопросы для установления оперативно-значимой информации.

Очередной проблемой в работе правоохранительных органов по раскрытии кражи с банковского счета, а равно в отношении электронных денежных средств, являются большие временные рамки при предоставлении технической информации, некоторые платформы (например, Telegram) не позволяют получить полной информации о подключениях правонарушителей. Затягиванию процедуры установления преступника способствуют некорректные ответы на запросы правоохранителей со стороны сотрудников банка (когда не предоставляются полные данные банковского счета или гражданина, который неправомерно получил денежные средства).

В настоящее время выработаны механизмы совмещения автоматизированной системы обработки инцидентов ФинЦЕРТ Банка России и подсистемы «Дистанционное мошенничество» программно-технического комплекса интегрированного банка данных коллективного пользования федерального уровня. Во исполнение Федерального закона[2] для укрепления информационного взаимодействия МВД России заключены соответствующие соглашения на федеральном уровне с 33 органами государственной власти Российской Федерации, 7 кредитно-финансовыми организациями и 2 операторами связи[3]. В реальности же сотрудники полиции, которые непосредственно сталкиваются с раскрытием хищений с использованием ЭСП на районном уровне, не могут в должной мере использовать получаемые данные для быстрого раскрытия преступлений.

Мы считаем, что требуются более оперативное реагирование и передача информации о рассматриваемых хищениях. Для совершенствования работы в этом направлении требуется наделить оперативные подразделения территориальных органов внутренних дел на районном уровне (именно они сталкиваются с проблемой раскрытия преступлений на первоначальном этапе) полномочиями по прямому обращению к кредитно-финансовым организациям и операторам связи в рамках проведения оперативно-розыскных мероприятий и возможности получения в режиме реального времени сведений о пользователях соответствующих услуг. Чтобы не перегружать кредитно-финансовые организации, это можно реализовать через подразделения специальных технических мероприятий органов внутренних дел (ПСТМ).

Предлагаем создать единую межведомственную платформу взаимодействия для получения сведений о всех транзакциях денежных средств в «одном окне». Такую платформу можно реализовать в ФинЦЕРТ Банка России, предоставив доступ к ней сотрудникам ПСТМ на региональном уровне. В свою очередь, в ПСТМ следует вести учет подозрительных IP-адресов, номеров телефонов, IMEI, MAC-адресов, веб-сайтов во взаимодействии с операторами сотовой связи и финансово-кредитными организациями для своевременного предупреждения рассматриваемых преступлений.

[1] При подготовке научной статьи проводилось интервьюирование сотрудников уголовного розыска подразделений УУР МВД по Республике Татарстан, специализирующихся на раскрытии рассматриваемых преступлений, в июне 2024 г.

[2] О внесении изменений в ст. 26 Федерального закона «О банках и банковской деятельности» и ст. 27 Федерального закона «О национальной платежной системе»: Федеральный закон от 20.10.2022 № 408-ФЗ. СПС «КонсультантПлюс» (дата обращения: 24.08.2024).

[3] Решение коллегии Министерства внутренних дел Российской Федерации от 24.06.2024 № 2 км: объявлено приказом МВД России от 01.07.2024 № 372.

СПИСОК ИСТОЧНИКОВ

1. Адмиралова Е.А. Проблемы отграничения преступлений, предусмотренных ст. 159.3 УК и п. «г» ч. 3 ст. 158 УК // Электронный журнал E-SCIO. URL https://cyberleninka.ru/article (дата обращения: 07.12.2024).
2. Бочарникова Л.Н. Основные способы совершения бесконтактных мошенничеств и краж: монография. Белгород: Белгородский юридический институт МВД России имени И.Д. Путилина, 2019. 50 с.
3. Пудовиков А.С., Ненашев Е.В. Отдельные особенности предварительной проверки и организация первоначального этапа расследования хищений денежных средств с банковского счета: методические рекомендации. Хабаровск: Дальневосточный юридический институт МВД России, 2022. 45 с.
4. Особенности расследования краж и мошенничеств, совершенных с использованием компьютерных технологий // Саакян А.Г. и др. / Нижний Новгород: Нижегородская академия МВД России, 2019. 66 с.
5. Русскевич Е.А., Чернова К.Б. Актуальные проблемы квалификации хищений, совершаемых с использованием электронных средств платежа // Вестник экономической безопасности. 2021. № 1. С. 128 - 130.
6. Скляров С.В. Обман при хищении // Уголовное право. 2020. № 5. С. 105 - 112.
7. Смушкин А.Б. О структуре электронной цифровой криминалистики // Криминалистика: вчера, сегодня, завтра. 2020. № 3 (15). С. 140-148.
8. Шавалеев Б.Э. Мошенничество с использованием электронных средств платежа: уголовно-правовой и криминологический аспекты. автореф. дис. ... канд. юрид. наук: 5.1.4. Казань, 2024. 26 с.

REFERENCES

1. Admiralova E.A. Problemy otgranicheniya prestuplenij, predusmotrennyh st. 159.3 UK i p. «g» ch. 3 st. 158 UK // Elektronnyj zhurnal E-SCIO. URL https://cyberleninka.ru/article (data obrashcheniya: 07.12.2024).
2. Bocharnikova L.N. Osnovnye sposoby sovershеniya beskontaktnyh moshennichestv i krazh: monografiya. Belgorod: Belgorodskij yuridicheskij institut MVD Rossii imeni I.D. Putilina, 2019. 50 c.
3. Pudovikov A.S., Nenashev E.V. Otdel'nye osobennosti predvaritel'noj proverki i organizaciya pervonachal'nogo etapa rassledovaniya hishchenij denezhnyh sredstv s bankovskogo scheta: metodicheskie rekomendacii. Habarovsk: Dal'nevostochnyj yuridicheskij institut MVD Rossii, 2022. 45 s.
4. Osobennosti rassledovaniya krazh i moshennichestv, sovershennyh s ispol'zovaniem komp'yuternyh tekhnologij // Saakyan A.G. i dr. / Nizhnij Novgorod: Nizhegorodskaya akademiya MVD Rossii, 2019. 66 s.
5. Russkevich E.A., Chernova K.B. Aktual'nye problemy kvalifikacii hishchenij, sovershaemyh s ispol'zovaniem elektronnyh sredstv platezha // Vestnik ekonomicheskoj bezopasnosti. 2021. № 1. S. 128 - 130.
6. Sklyarov S.V. Obman pri hishchenii // Ugolovnoe pravo. 2020. № 5. S. 105 - 112.
7. Smushkin A.B. O strukture elektronnoj cifrovoj kriminalistiki // Kriminalistika: vchera, segodnya, zavtra. 2020. № 3 (15). S. 140-148.
8. Shavaleev B.E. Moshennichestvo s ispol'zovaniem elektronnyh sredstv platezha: ugolovno-pravovoj i kriminologicheskij aspekty. avtoref. dis. ... kand. yurid. nauk: 5.1.4. Kazan', 2024. 26 s.

Информация об авторах:
Гумаров Ильнур Асгатович, кандидат юридических наук, доцент, доцент кафедры оперативно-разыскной деятельности Казанского юридического института МВД России, ilnur_gumar@mail.ru
Тырышкин Виктор Владимирович, кандидат юридических наук, доцент, начальник кафедры конституционного и международного права Барнаульского юридического института МВД России, witsan333@yandex.ru
Авторы прочитали и одобрили окончательный вариант рукописи

Information about the authors:
Gumarov Ilnur A., Candidate in Law (Research doctorate), Associate Professor, Associate Professor of Investigation of the Kazan Law Institute of the Ministry of Internal Affairs of the Russian Federation, ilnur_gumar@mail.ru
Tyryshkin Victor V., Candidate in Law (Research doctorate), Associate Professor, Head of Constitutional and International Law, Barnaul Law Institute of the Ministry of Internal Affairs of the Russian Federation, witsan333@yandex.ru
The authors have read and approved the final version of the manuscript.

Заявленный вклад авторов:
Гумаров Ильнур Асгатович – проведение критического анализа и структурирование собранных материалов, подготовка окончательного варианта текста статьи, формулирование практических рекомендаций.
Тырышкин Виктор Владимирович – подготовка первоначального варианта статьи, структурирование методической части статьи, обобщение научных источников, формулирование первоначального выводов, работа с библиографическим материалом.

Статья получена: 25.08.2024.
Статья принята к публикации: 24.12.2024.
Статья опубликована онлайн: 24.12.2024.
Против размещения полнотекстовой версии статьи в открытом доступе в сети Интернет не возражаем.