

Научная статья

УДК: 343.98

DOI: 10.55001/2587-9820.2024.76.66.020

**КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА КРАЖИ,
СОВЕРШЕННОЙ С БАНКОВСКОГО СЧЕТА,
А РАВНО В ОТНОШЕНИИ ЭЛЕКТРОННЫХ ДЕНЕЖНЫХ СРЕДСТВ**

Максим Владимирович Старичков¹, Игорь Петрович Парфиненко²

¹Восточно-Сибирский институт МВД России, г. Иркутск, Российская Федерация, maximstar@narod.ru

²Байкальский государственный университет, г. Иркутск, Российская Федерация

Аннотация. В последние годы в России отмечается резкий рост преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, в частности краж, совершенных с банковских счетов, а равно в отношении электронных денежных средств. На основе анализа имеющихся научных публикаций и обобщения следственно-судебной практики в статье приводятся обобщенные сведения об элементах криминалистической характеристики данного вида преступлений. Особое внимание уделяется способу совершения преступления, выделяется три группы в зависимости от способа доступа к банковскому счету.

Ключевые слова: криминалистическая характеристика, способ совершения преступления, механизм слеодообразования, кража, банковский счет, электронные денежные средства, платежная карта, информационно-телекоммуникационные преступления, компьютерные преступления

Для цитирования: Старичков, М. В., Парфиненко, И. П. Криминалистическая характеристика кражи, совершенной с банковского счета, а равно в отношении электронных денежных средств // Криминалистика: вчера, сегодня, завтра : сб. науч. тр. Иркутск : Восточно-Сибирский институт МВД России. 2024. Т. 32. № 4. С. 194–204. DOI: 10.55001/2587-9820.2024.76.66.020

**CRIMINALISTIC CHARACTERISTICS OF THEFT COMMITTED FROM A BANK
ACCOUNT, AS WELL AS IN RELATION TO ELECTRONIC MONEY**

Maxim V. Starichkov¹, Igor P. Parfinenko²

¹East Siberian Institute of the MIA of Russia, Irkutsk, Russian Federation, maximstar@narod.ru

²Baikal State University, Irkutsk, Russian Federation

Abstract. In recent years, Russia has seen a sharp increase in crimes committed using information and telecommunication technologies, in particular, thefts committed from bank accounts, as well as in relation to electronic money. Based on the analysis of available scientific publications and generalization of investigative and judicial practice, the article provides generalized information about the elements of the criminalistic characteristics of this type of crime. Special attention is paid to the method of committing a crime, three groups are distinguished depending on the method of access to a bank account.

Keywords: criminalistic characteristics, method of committing a crime, mechanism of trace formation, theft, bank account, electronic money, payment card, information and telecommunication crimes, computer crimes

For citation: Starichkov, M. V., Parfinenko, I. P. Kriminalisticheskaya harakteristika krazhi, sovershennoj s bankovskogo scheta, a ravno v otnoshenii elektronnyh denezhnyh sredstv [Criminalistic characteristics of theft committed from a bank account, as well as in relation to electronic money]. *Kriminalistika: vchera, segodnya, zavtra* = Forensics: yesterday, today, tomorrow. 2024, vol. 32 no. 4, pp. 194–204. (in Russ.). DOI: 10.55001/2587-9820.2024.76.66.020

Введение

Современная цивилизация характеризуется стремительным развитием информационных технологий, которые прочно вошли в повседневную жизнь. Широкий спектр использования, практически неограниченные возможности и доступность цифровых технологий и цифровых инструментов значительно расширяют возможности человека, приводя к повышению эффективности взаимодействия субъектов в различных видах деятельности. Повсеместная цифровизация общества способствует революционным изменениям в технологической и экономической отраслях, формируя новый социум – информационный.

Особенно это заметно в банковской сфере, где наряду с положительными изменениями отмечаются и негативные тенденции, выражающиеся в криминальных проявлениях. Кражи, совершенные с банковских счетов, а равно в отношении электронных денежных средств (п. «г» ч. 3 ст. 158 УК РФ¹), стали одним из самых распространенных способов хищения: в 2022 году было зарегистриро-

вано 113 565, в 2023 году – 119 212 таких преступлений².

Частная криминалистическая методика расследования данного вида преступлений в настоящее время только формируется, при этом она постоянно нуждается в совершенствовании с учетом существующей криминальной обстановки и имеющегося опыта правоохранительных органов.

Целью настоящей статьи является рассмотрение элементов криминалистической характеристики кражи, совершенной с банковского счета, а равно в отношении электронных денежных средств, как одного из источников разработки частной криминалистической методики расследования.

Основная часть

Частная криминалистическая методика расследования преступлений обычно начинается с криминалистической характеристики. По нашему мнению, такой подход вполне оправдан, поскольку криминалистическая характеристика направлена на выявление криминалистически значимых свойств данного вида (группы) преступлений, их обобщении, и тем самым выступает в качестве источника формирования самой методики расследования. Хотя криминалистическая характеристика носит вероятностный характер, она имеет

¹ Уголовный кодекс Российской Федерации : УК : принят Гос. Думой 24 мая 1996 года : одобрен Советом Федерации 5 июня 1996 года : послед. ред. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 10.10.2024).

² Статистика и аналитика // Министерство внутренних дел Российской Федерации : офиц. сайт. URL: <https://мвд.рф/dejatelnost/statistics> (дата обращения: 10.10.2024).

не только научное, но и практическое значение, позволяя создавать модели преступления, приближенные к реальной, и на их основании выдвигать наиболее вероятные следственные версии.

Существует множество подходов к структуре криминалистической характеристики, названию и количеству ее элементов. Различаясь по форме, они в основном совпадают по содержанию, определяя криминалистическую характеристику как комплекс криминалистически значимых сведений о преступлении, являющийся результатом обобщения следственно-судебной практики и научных исследований.

В качестве основных структурных элементов кражи, совершенной с банковского счета, а равно в отношении электронных денежных средств, можно выделить следующие криминалистически значимые сведения [1, с. 22]:

- о предмете преступного посягательства и личности потерпевшего;
- о личности преступника, мотивах и целях его преступного поведения;
- об обстановке преступных посягательств, включающей время, место и иные обстоятельства;
- о способе преступления, включая его подготовку, непосредственное совершение и посткриминальное поведение, а также действия, направленные на сокрытие преступления и его следов;
- о механизме следообразования;
- об обстоятельствах, способствовавших совершению преступления.

Предметом рассматриваемого вида кражи выступают денежные средства в российских рублях и иностранной валюте, хранящиеся на банковском счете и (или) представ-

ленные в виде электронных денежных средств. Характерной особенностью является то, что воздействие осуществляется не непосредственно на предмет (как в ходе «обычной» кражи), а на его «информационную составляющую» – сведения о самом предмете (права на денежные средства). Таким образом, фактически осуществляется воздействие на информационные ресурсы кредитно-финансовой организации, где открыт соответствующий электронный денежный счет.

Поскольку у собственности (в данном случае денежных средств, хранящихся на банковских счетах) всегда существует собственник, он и будет являться потерпевшим. В силу более строгого контроля доступа к банковским счетам юридических лиц потерпевшими значительно чаще оказываются физические лица – владельцы таких счетов. Таким образом, социально-демографическая структура потерпевших примерно соответствует социально-демографической структуре клиентов кредитно-финансовых организаций. Здесь можно отметить, что вероятность стать жертвой подобной кражи существенно повышается у лиц, не принимающих необходимых мер по ограничению возможности доступа посторонних к своим банковским счетам и информации о них (банковским картам и паролям доступа к ним, устройствам мобильной связи с установленным приложением «мобильный банк» и т. п.).

В соответствии с ч. 1 ст. 42 УПК РФ³, потерпевшим является физическое лицо, которому преступлением причинен физический, имущественный, моральный вред, а также юридическое лицо – в случае причинения преступлением вреда его имуществу и (или) деловой репутации. Потерпевший – это процессуальный статус, который возникает у лица после возбуждения уголовного дела и принятия решения о признании его таковым. Однако вред преступлением может быть причинен другим лицам, и не только прямой, но и косвенный. Поэтому в данном случае наряду с «потерпевшим» целесообразно использовать понятие «пострадавшая сторона», объединяющее как участников уголовного процесса (потерпевшего, гражданского истца, их представителей), так и иных лиц, чьи права и законные интересы были нарушены. В некоторых случаях такой «пострадавшей стороной» будет выступать кредитно-финансовая организация, поскольку любое хищение с банковского счета, даже при наличии неосторожности со стороны его владельца, косвенно наносит ущерб деловой репутации банка.

Важным компонентом, характеризующим преступление, являются сведения об особенностях личности преступника. Характеристики личности преступника, совершающего кражу с банковского счета, а равно в отношении электронных денежных средств, очень сильно варьируются в зависимости от способа совершаемого преступления [2, с. 93]. В то время как одни способы требуют достаточ-

но хороших знаний в области информационно-телекоммуникационных технологий, другие не предполагают каких-либо специальных навыков.

Как и у любого хищения, мотив кражи, совершенной с банковского счета, а равно в отношении электронных денежных средств, – корыстный, цель – получение чужого имущества (денежных средств) и обращение его в свою пользу или в пользу третьих лиц, т. е. обогащение за чужой счет.

Совершаемые с использованием информационно-телекоммуникационных сетей кражи и мошенничества могут поощряться со стороны враждебных Российской Федерации государств, и в этом случае к корыстному добавляется политический мотив. Фактически проводится диверсионная деятельность, направленная на подрыв экономической безопасности и политической стабильности России.

Обстановка совершения преступления включает взаимодействующие между собой до и в момент преступления материальные и социально-психологические факторы среды, в которой происходит преступное деяние. Она во многом определяет особенности поведения преступника и пострадавшей стороны, оказывает влияние на формирование остальных характеристик преступления рассматриваемого вида.

Время и место кражи, совершенной с банковского счета, а равно в отношении электронных денежных средств, также определяется способом совершения преступления. Важно отметить, что сама кража (перевод денежных средств со счета потерпевшего) производится мгновенно, и момент транзакции фиксируется на сервере кредитно-финансовой организации. Также существенным выступает то обстоятельство, что

³ Уголовно-процессуальный кодекс Российской Федерации: УПК: принят Гос. Думой 22 ноября 2001 года : одобрен Советом Федерации 5 декабря 2001 года : послед. ред. // КонсультантПлюс : сайт. URL: http://www.consultant.ru/document/cons_doc_LAW_34481/ (дата обращения: 10.10.2024).

в случае завладения преступником банковской картой либо устройством сотовой связи с установленным приложением «мобильный банк» у него имеется относительно немного времени для совершения кражи, пока владелец не заблокировал свой счет.

Отличительным свойством кражи, совершенной с банковского счета, а равно в отношении электронных денежных средств, является то, что общественно опасные действия могут совершаться в одном месте, а вредоносные последствия наступать в другом, часто находящемся на значительном расстоянии. В связи с этим, в соответствии с п. 19 Постановления Пленума Верховного Суда Российской Федерации от 15.12.2022 г. № 37⁴, под местом совершения такого преступления следует понимать место, где было совершено общественно опасное деяние – дана команда на производство перечисления денежных средств со счета потерпевшего, т. е. где преступник воспользовался информационно-телекоммуникационным оборудованием с установленным приложением «мобильный банк» или расплатился чужой банковской картой (где находился банковский терминал) и т. п.

Применительно к данному виду преступлений можно также говорить о месте получения преступником возможности доступа к счету потерпевшего (завладение банковской

картой, получение информации о паролях и т. д.), которое можно рассматривать как место приготовления к преступлению.

Местом наступления общественно опасных последствий будет выступать физическое местонахождение сервера кредитно-финансовой организации, на котором хранится информация о счетах клиентов.

К иным факторам, определяющим обстановку преступления, можно отнести наличие средств видеофиксации лица, производящего банковские операции, его аутентификацию и др.

Важнейшим и определяющим элементом, характеризующим любое преступление, в том числе и кражу с банковского счета (в отношении электронных денежных средств), является совокупность данных о способе его совершения. Способы совершения рассматриваемого вида краж, как и прочих преступлений с использованием информационно-телекоммуникационных технологий, отличаются большим разнообразием. Например, А. Т. Анешева называет следующие типичные способы совершения таких краж [3, с. 10–11]:

- получение доступа к мобильному телефону потерпевшего с подключенной услугой «мобильный банк», перечисление денежных средств на свой счет и последующее их обналичивание;
- хищение платежной карты, пароль доступа к которой заранее известен преступнику, и дальнейшее обналичивание денежных средств через банкомат;
- доступ к платежной карте, подключение ее к своему мобильному приложению и перевод денежных средств на свой банковский счет;
- оплата товаров в магазинах с помощью найденной платежной карты.

⁴ О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»: Постановление Пленума Верховного Суда Российской Федерации от 15.12.2022 г. № 37 // КонсультантПлюс: сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_434573/ (дата обращения: 10.10.2024).

Отмечая, что все перечисленные способы достаточно активно используются преступниками, считаем необходимым сделать уточнение. Анализ следственно-судебной практики и научной литературы по теме исследования позволяет выделить три основные группы способов совершения краж с банковского счета, а равно в отношении электронных денежных средств:

1) кражи, совершенные с использованием платежных карт;

2) кражи, совершенные с использованием информационно-телекоммуникационных сетей для доступа к банковским счетам через «личный кабинет» (приложение «мобильный банк»);

3) несанкционированный доступ к банковскому счету в обход штатных средств с последующим перечислением денежных средств.

Кражи первой и второй группы могут совершаться «случайными» («ситуативными») преступниками. Так, например, происходит, когда лицо находит потерянную платежную карту (первая группа способов). Вместо того, чтобы предпринять действия по возврату находки законному владельцу (сдать платежную карту в отделение банка), с банковской карты производится безналичная оплата приобретенных товаров и оказанных услуг. При этом само лицо не всегда осознает, что совершает кражу, поскольку на бытовом уровне такая находка воспринимается аналогично находке «обезличенных» денег, которые безнаказанно можно потратить на личные нужды. Такие действия нередко совершают несовершеннолетние, еще не достигшие возраста уголовной ответственности (по ст. 158 УК РФ – 14 лет). Однако такая «находка» действует, пока законный владелец счета не заблокировал карту. Кроме того, на оплату без ввода

пароля (пин-кода) обычно устанавливается лимит до 1000 руб., реже – несколько больше. Поэтому действия нашедшего по скорейшему использованию содержащихся на счете денежных средств свидетельствуют о наличии противоправного умысла.

Аналогичная ситуация имеет место, когда лицо находит незаблокированный сотовый телефон с подключенной услугой «мобильный банк» либо приобретает сим-карту с ранее уже использовавшимся абонентским номером, прежний владелец которого не аннулировал привязку к банковскому счету (вторая группа способов). Однако преступник уже целенаправленно входит в «личный кабинет» потерпевшего и производит перевод денежных средств на свой счет. Очевидно, что подобные способы не требуют от лица каких-либо специальных знаний и навыков (в т. ч. «криминальных»).

Схожие способы совершения кражи с банковского счета связаны с предшествующим хищением имущества. Например, преступник похищает сумочку, в которой обнаруживает банковскую карту или устройство мобильной связи с абонентским номером, привязанным к банковскому счету. Дальнейшее поведение преступника будет аналогично рассмотренным выше способам, но он уже изначально преступным способом завладел указанными предметами.

Еще один реализуемый способ, относящийся к первой группе, – неправомерное завладение (хищение) банковской карты, пин-код к которой уже известен. Например, злоумышленник может подсмотреть его, когда потерпевший производит операции у банкомата. Знание пароля позволяет похитить все содержащиеся на счете денежные средства. К первой группе способов относятся также все способы, связанные с использованием

поддельных платежных карт. При этом имеет место совокупность преступлений, поскольку само изготовление таких карт уже образует состав преступления, предусмотренного ст. 187 УК РФ.

Способы второй группы не ограничиваются завладением информационно-телекоммуникационным устройством с доступом к банковскому счету. Для кражи с банковского счета достаточно получить информацию, позволяющую произвести его перепривязку к мобильному номеру преступника, и в дальнейшем распоряжаться им как своим. Для этих целей могут использоваться «фишинговые сайты», «тройанские программы» [4] и другое вредоносное программное обеспечение. Особую группу составляет так называемое «телефонное мошенничество» [5]. Если потерпевший не переводит денежные средства, а лишь предоставляет информацию, позволяющую получить доступ к его банковскому счету, то хищение квалифицируется как кража.

Третья группа способов реализуется значительно реже. Она характеризуется явно выраженной направленностью умысла на совершение кражи. В основном такие преступления совершаются «внутренними» нарушителями. Это могут быть работники кредитно-финансовой организации, имеющие доступ к банковским счетам клиентов и производящие несанкционированные транзакции с последующим их сокрытием. Чаще кражи совершаются работниками организаций – клиентов банка, перечисляющими денежные средства вопреки интересам своей организации. Следует отметить, что такие действия следует квалифицировать как кражу только в случае отсутствия материальной ответственности работника за распоряжение денежными средствами на счете. В противном

случае речь идет о присвоении или растрате (ст. 165 УК РФ).

Несанкционированный доступ к банковскому счету в обход штатных средств защиты может осуществляться и «внешними» нарушителями. Поскольку для этого необходимо преодолеть многоконтурную систему защиты информации банка (найти в ней «брешь»), речь идет о высококвалифицированных специалистах, обладающих знаниями как в области технологий банковской информационной безопасности, так и организации самой банковской системы. Очевидно, что такие случаи носят единственный характер. В качестве примера можно привести ставшее уже хрестоматийным дело Владимира Левина [6; 7], действия которого в настоящее время следовало бы квалифицировать именно по п. «г» ч. 3 ст. 158 УК РФ.

Кражи с банковского счета, совершенные «случайными» («ситуативными») преступниками, в большинстве своем не предполагают специальных действий, направленных на сокрытие преступления и его следов. Заранее подготавливаемые кражи, как правило, совершаются благодаря возможности информационно-телекоммуникационных сетей для анонимизации. Так, денежные средства перечисляются на специально открытые на подставных лиц счета с последующим переводом в электронные кошельки и уходом в «теневой сектор» [8].

Важным элементом криминалистической характеристики преступления, без понимания которого невозможно грамотное производство расследования, является механизм следообразования. В настоящее время кражи, совершенные с банковского счета, а равно в отношении электронных денежных средств,

характеризуются следующей следовой картиной [9, с. 36–37; 10, с. 213]:

- следы на средствах ИТ-техники и оборудования, с помощью которых лицо совершало преступление (следы на орудии преступления). Это использовавшееся для неправомерного доступа программное обеспечение, протоколы подключения к информационно-телекоммуникационным сетям, сохраненные коды доступа, тексты программ, скопированная у пострадавшей стороны информация и т. п. Такие следы могут остаться в операционной системе, в аппаратно-программной конфигурации, на электронных носителях;

- следы на «транзитных» (телекоммуникационных) носителях информации, посредством которых лицо осуществляло связь с охраняемыми законом информационными ресурсами: документированная информация о трафике через оператора телематических услуг, размещенная в сети информация, электронная переписка и т. д.;

- следы в подвергшейся вредоносному воздействию информационно-телекоммуникационной системе кредитно-финансовой организации, в т. ч. на электронных носителях (следы на предмете преступления): результаты уничтожения, блокирования, модификации, копирования компьютерной информации, нейтрализации средств защиты компьютерной информации; протоколы соединений абонентов и др. Их местонахождение сходно со следами в ИТ-системе нарушителя (следами на орудии преступления);

- следы на ином ИТ-оборудовании, непосредственно не участвовавшем в совершении преступления, но содержащем имеющие значение для уголовного дела сведения, – криминалистически значимая информация в компьютерах,

органайзерах, мобильных телефонах, цифровых фотоаппаратах, видеокамерах и диктофонах, смарт-картах и т. д.;

- документы, изготовленные с использованием средств компьютерной техники;

- документы (в т. ч. поддельные банковские карты), предназначенные для обработки в автоматизированных информационных системах, и иные документы, отражающие преступную деятельность;

- традиционные следы (рук, обуви, орудий, инструментов и т. д.);

- идеальные следы – сведения о преступлении и об относящихся к нему обстоятельствах, сохранившиеся в памяти участников преступления (преступников, потерпевших) и очевидцев (продавцов, кассиров, работников кредитно-финансовых организаций и др.), а также иных лиц.

К обстоятельствам, способствующим совершению кражи с банковского счета (в отношении электронных денежных средств), относятся следующие:

- 1) несовершенство средств защиты информации или полное их отсутствие;

- 2) нарушение правил работы с охраняемой законом информацией, пренебрежение правилами защиты информации, отсутствие контроля над хранением банковских карт и материальных носителей, содержащих информацию о банковских счетах и паролях доступа к ним;

- 3) использование средств компьютерной и информационно-телекоммуникационной техники для обработки посторонней информации, в т. ч. в личных целях;

- 4) неблагоприятный психологический климат в коллективе, конфликты между сотрудниками, неудовлетворенность отдельных

работников своими руководителями или условиями труда.

Нередко данные факторы определяются деятельностью пострадавшей стороны.

Выводы и заключение

Криминалистическая характеристика преступления является важной составляющей криминалистической методики расследования, выступая не только источником сведений о преступлении, но и основой для выдвижения следственных версий, особенно на первоначальном этапе, а также конкретизируя предмет доказывания.

Анализируя элементы криминалистической характеристики кражи, совершенной с банковского счета, а равно в отношении электронных денежных средств, можно сделать вывод о значительном разнообразии

способов ее совершения. Проведенные исследования позволяют объединить их в три группы в зависимости от способа доступа к банковскому счету, с которого совершается кража: с использованием платежной карты, через «личный кабинет» и непосредственно к информации на сервере кредитно-финансовой организации. Способ совершения определяет место и время преступления, детерминирует слеодообразование. В свою очередь, выбор способа определяется преступником исходя из его личностных качеств и с учетом складывающихся обстоятельств, способствующих и препятствующих преступлению, – таким образом проявляется взаимосвязь элементов криминалистической характеристики.

СПИСОК ИСТОЧНИКОВ

1. *Имаева, Ю. Б.* Особенности расследования хищений, совершенных с использованием кредитных и расчетных карт : дис. ...канд. юрид. наук. Уфа, 2015. 233 с.
2. *Ненашев, Е. В.* Особенности личности преступника как важнейший элемент криминалистической характеристики краж, совершенных с банковского счета, а также в отношении электронных денежных средств // Вестник Дальневосточного юридического института МВД России : науч. журн. 2022. № 3 (60). С. 92–97.
3. *Анешева, А. Т.* Способ совершения преступления, как основной элемент криминалистической характеристики краж, совершенных с банковского счета, а равно в отношении электронных денежных средств // Борьба с правонарушениями в сфере экономики: правовые, процессуальные и криминалистические проблемы : сб. мат-лов междунар. науч.-практ. конф., в рамках международного юридического форума «Право и экономика: национальный опыт и стратегии развития», Новосибирск, 27 мая 2021 года. Новосибирск, Новокузнецк : Новосибирский государственный университет экономики и управления; Кузбасский институт ФСИН России. 2021. С. 9–11.
4. *Шевко, Н. Р.* Мошенничество в киберпространстве: реальный ущерб в виртуальном мире // Вестник Восточно-Сибирского института МВД России : науч.-практ. журн. 2023. № 3 (106). С. 276–284.
5. *Бжахов, Г. М.* Об актуальных вопросах, возникающих при раскрытии дистанционных мошенничеств и краж с банковских карт // Пробелы в российском законодательстве : науч. журн. 2022. Т. 15, № 4. С. 39–43.

6. Гусейнов, Э., Лесков, С. Электронный медвежатник из Петербурга взломал банковские коды самого защищенного банка Америки // Известия. 1995. 18 авг. С. 1–2.
7. Какоткин, А. Компьютерные взломщики // Аргументы и факты. 1997. № 8. С. 9.
8. Макуха, М. Ю. Некоторые вопросы деанонимизации транзакций криптовалют // Охрана, безопасность, связь : науч. журн. 2020. № 5-3. С. 226–230.
9. Виноградова, О. П., Фалькина, Т. Ю. Криминалистические аспекты исследования материальных носителей информации при расследовании преступлений, связанных с нарушением авторских и смежных прав // Вестник Уральского юридического института МВД России : науч. журн. 2014. № 3. С. 34–39.
10. Третьякова, Е. И. Об актуальных элементах криминалистической характеристики мошенничества в сфере компьютерной информации // Научный дайджест Восточно-Сибирского института МВД России : электрон. науч. журн. 2019. № 3 (3). С. 210–215. URL: <https://elibrary.ru/item.asp?id=42365489> (дата обращения: 10.10.2024). Режим доступа: для зарегистрир. пользователей.

REFERENCES

1. *Imaeva, Yu. B.* Osobennosti rassledovaniya khishcheniy, sovershennykh s ispol'zovaniyem kreditnykh i raschetnykh kart [Features of the investigation of thefts committed using credit and settlement cards: dis. ...cand. jurid. sciences' 12.00.12.]. Ufa, 2015. 233 p. (in Russian).
2. *Nenashev, E. V.* Osobennosti lichnosti prestupnika kak vazhnejshij element kriminalisticheskoy harakteristiki krazh, sovershennykh s bankovskogo scheta, a takzhe v otnoshenii elektronnykh denezhnykh sredstv [The identity of the criminal as the most important element of the criminalistic characteristics of thefts committed from a bank account, as well as in relation to electronic money]. Vestnik Dal'nevostochnogo yuridicheskogo instituta MVD Rossii — Bulletin of the Far Eastern Law Institute of the Ministry of Internal Affairs of Russia. 2022. no 3 (60). pp. 92–97. (in Russian).
3. *Anesheva, A. T.* Sposob soversheniya prestupleniya, kak osnovnoj element kriminalisticheskoy harakteristiki krazh, sovershennykh s bankovskogo scheta, a ravno v otnoshenii elektronnykh denezhnykh sredstv [The method of committing a crime, as the main element of the criminalistic characteristics of thefts committed from a bank account, as well as in relation to electronic money]. Bor'ba s pravonarusheniyami v sfere ekonomiki: pravovye, processual'nye i kriminalisticheskie problemy : Sbornik materialov mezhdunarodnoj nauchno-prakticheskoy konferencii, v ramkah mezhdunarodnogo yuridicheskogo foruma «Pravo i ekonomika: nacional'nyj opyt i strategii razvitiya», Novosibirsk, 27 maya 2021 goda. [Combating economic offenses: legal, procedural and criminalistic problems : Proceedings of the international scientific and practical conference within the framework of the international legal forum «Law and Economics: National Experience and Development Strategies», Novosibirsk, May 27, 2021]. Novosibirsk, Novokuzneck: Novosibirskij gosudarstvennyj universitet ekonomiki i upravleniya; Kuzbasskij institut FSIN Rossii. — Novosibirsk, Novokuznetsk: Novosibirsk State University of Economics and Management; Kuzbass Institute of the Federal Penitentiary Service of Russia. 2021. pp. 9-11. (in Russian).
4. *Shevko, N. R.* Moshennichestvo v kiberprostranstve: real'nyj ushcherb v virtual'nom mire [Fraud in Cyberspace: Real damage in the virtual world]. Vestnik Vostochno-Sibirskogo instituta MVD Rossii — Bulletin of the East Siberian Institute of the Ministry of Internal Affairs of Russia. 2023. no 3 (106). pp. 276–284. (in Russian).

5. *Bzhahov, G. M.* Ob aktual'nyh voprosah, vznikayushchih pri raskrytii distancionnyh moshennichestv i krazh s bankovskih kart [On current issues arising in the disclosure of remote fraud and theft from bank cards]. Probely v rossijskom zakonodatel'stve — Gaps in Russian legislation. 2022. vol. 15 no 4. pp. 39–43. (in Russian).

6. *Gusejnov, E., Leskov, S.* Elektronnyj medvezhatnik iz Peterburga vzlomal bankovskie kody samego zashchishchennogo banka Ameriki [An electronic bear hunter from St. Petersburg hacked the bank codes of America's most secure bank]. Izvestia. 1995. 18 Aug. pp. 1-2. (in Russian).

7. *Kakotkin, A.* Komp'yuternye vzlomshchiki [Computer hackers]. 1997. No. 8. p. 9. Argumenty i fakty. – Arguments and facts. 1997. no. 8. pp. 9. (in Russian).

8. *Makuha, M. Yu.* Nekotorye voprosy deanonimizacii tranzakcij kriptovalyut [Some issues of deanonymization of cryptocurrency transactions]. Ohrana, bezopasnost', svyaz' – Security, security, communication. 2020. no 5-3. pp. 226–230. (in Russian).

9. *Vinogradova, O. P., Fal'kina, T. Yu.* Kriminalisticheskie aspekty issledovaniya material'nyh nositelej informacii pri rassledovanii prestuplenij, svyazannyh s narusheniem avtorskih i smezhnyh prav [Criminalistic aspects of the study of material media in the investigation of crimes related to the violation of copyright and related rights]. Vestnik Ural'skogo yuridicheskogo instituta MVD Rossii — Bulletin of the Ural Law Institute of the Ministry of Internal Affairs of Russia. 2014. no 3. pp. 34–39. (in Russian).

10. *Tret'yakova, E. I.* Ob aktual'nyh elementah kriminalisticheskoy harakteristiki moshennichestva v sfere komp'yuternoj informacii [On the actual elements of the criminalistic characteristics of fraud in the field of computer information] Nauchnyj dajdzhest Vostochno-Sibirskogo instituta MVD Rossii. — Scientific Digest of the East Siberian Institute of the Ministry of Internal Affairs of Russia. 2019. no 3 (3). pp. 210–215. (in Russian).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Старичков Максим Владимирович, кандидат юридических наук, доцент, доцент кафедры криминалистики. Восточно-Сибирский институт МВД России. 664074, Российская Федерация, г. Иркутск, ул. Лермонтова, 110.

Парфиненко Игорь Петрович, кандидат юридических наук, доцент, помощник ректора. Байкальский государственный университет. 664003, Российская Федерация, г. Иркутск, ул. Ленина, 11.

INFORMATION ABOUT THE AUTHORS

Maxim V. Starichkov, Candidate Law, Associate Professor, Associate Professor of the Department of Criminalistics. East-Siberian Institute of the MIA of Russia. 110, st. Lermontov, Irkutsk, Russian Federation, 664074.

Igor P. Parfinenko, Candidate of Law, Associate Professor, Rector's Assistant. Baikal State University. 11, Lenin st., Irkutsk, Russian Federation, 664003.