

Сухарев Михаил Сергеевич

заместитель прокурора Юго-Восточного административного округа Москвы; аспирант, Российский новый университет, Москва.

Электронный адрес: mssuharev@yandex.ru

Sukharev Mikhail Sergeevich

Deputy Prosecutor, Prosecutor's Office of the South-Eastern Administrative District of Moscow; postgraduate, Russian New University, Moscow.

E-mail address: mssuharev@yandex.ru

ДИСТАНЦИОННЫЕ ХИЩЕНИЯ КАК ПОСТОЯННО МЕНЯЮЩИЙСЯ ВИД ПРЕСТУПНОСТИ

Аннотация. Прогресс цифровых технологий, обеспечивая скорость транзакций, облегчает также и противоправный доступ к денежным средствам граждан и организаций. Дистанционные хищения с использованием электронных средств платежа, цифровых данных и устройств имеют тенденцию к расширению, усложнению и диверсификации. Для противодействия этой тенденции только уголовно-правовых средств недостаточно, необходима активная и непримиримая к дроппингу и иным аналогичным действиям политика банков и Центрального банка России. Латентность рассматриваемых «неявных» преступлений может быть существенно сокращена за счёт изучения цифровых следов средствами искусственного интеллекта по уже имеющемуся зарубежному опыту. Исходя из анализа быстрого развития сегмента дистанционных хищений, совершаемых с применением цифровых данных и средств, необходимо превентивное прогнозирование рисков внедрения каждого нового цифрового сервиса.

Ключевые слова: дистанционные хищения, электронные средства платежа, мошенничество, дроппинг, банки.

Для цитирования: Сухарев М.С. Дистанционные хищения как постоянно меняющийся вид преступности // Вестник Российского нового университета. Серия: Человек и общество. 2025. № 1. С. 117–125. DOI: 10.18137/RNUV9276.25.01.P.117.

REMOTE THEFT AS A CONSTANTLY CHANGING TYPE OF CRIME

Abstract. The progress of digital technologies, ensuring the speed of transactions, also facilitates illegal access to monetary resources of individuals and organizations. Remote theft with the use of electronic means of payment, digital data and devices tends to expand, become more complex and diversify. To counter this trend, criminal law alone is not enough; an active and uncompromising policy towards dropping and other similar actions by banks and the Central Bank of Russia is needed. The latency of the considered “hidden” crimes can be significantly reduced by analyzing digital traces using artificial intelligence based on the existing foreign experience. An analysis of the the rapid development of the segment of remote thefts committed with the use of digital data and means shows the necessity for preventive forecasting of the risks of introducing each new digital service.

Keywords: remote theft, electronic means of payment, fraud, dropping, banks.

For citation: Sukharev M.S. (2025) Remote theft as a constantly changing type of crime. *Vestnik of Russian New University. Series: Man and Society.* No. 1. Pp. 117–125. DOI: 10.18137/RNUV9276.25.01.P.117 (In Russian).

Несмотря на принимаемые правоохранительными органами меры в сфере криминального использования информационно-телекоммуникационных технологий, уровень дистанционных хищений и мошеннических действий с использованием ИТ-средств на протяжении нескольких лет остается стабильно высоким.

В 2023 году, по статистике ЦБ РФ, у граждан было похищено 15,8 млрд руб. (в 2022 году – 14,1 млрд руб.¹, в 2020 году – 9 млрд руб.). Пострадавших обманом заставили набрать кредитов более чем на 200 млрд руб.², что является историческим максимумом. В 2023 году было проведено свыше 1,17 млн операций по незаконному выводу средств (+33% к 2022 году). В результате потери клиентов банков выросли на 11,5 %³. При этом чаще всего граждане под воздействием обмана добровольно переводили средства или сообщали реквизиты электронных средств платежа.

Хищения, совершенные дистанционным способом, – один из самых распространенных видов преступной деятельности. Так, в 2022 году в Москве зарегистрировано 50,5 тыс. таких преступлений, в 2023 году – 60,9 тыс.⁴

Среди наиболее распространенных способов совершения преступлений в сфере

информационно-телекоммуникационных технологий в литературе выделяются следующие виды мошенничества: звонок от имени сотрудника банка или правоохранительных органов, объявление в сети Интернет (покупка-продажа товаров), предложение об освобождении родственника (близкого лица) от ответственности за совершенное преступление, оформление микрозайма в сети Интернет, сообщения о взломе социальной сети (мессенджера) с последующим займом средств у коллег (друзей) [1–10].

За 2023 год в Юго-Восточном административном округе Москвы количество зарегистрированных преступлений против собственности увеличилось на 2,2 % и составило 11 629, из них 5408, или 46,5 %, составили дистанционные хищения⁵.

Рассмотрим типичное многоэпизодное дело. В июне 2023 года в суд для рассмотрения по существу направлено уголовное дело в отношении Алексева М.Э. по обвинению в совершении 33 преступлений, предусмотренных ч. 4 ст. 159 УК РФ, и 18 преступлений, предусмотренных ч. 3 ст. 30, ч. 4 ст. 159 УК РФ, которые совершались в составе организованной группы посредством подмены купюр в банкоматах банковских учреждений и использования

¹ Объем похищенных мошенниками средств в 2023 году вырос до 15,8 млрд рублей // Интерфакс. 2024. 13 февраля. URL: <https://www.interfax.ru/russia/945907> (дата обращения 01.10.2024).

² Кинякина К., Тюняева М. Мошенники в 2023 году похитят у граждан 19 млрд рублей // Ведомости. 2023. 15 ноября. URL: <https://www.vedomosti.ru/finance/articles/2023/11/15/1005850-moshenniki-v-2023-godu-pohityat-u-grazhdan-19-mlrd?ysclid=lto0mh44zx290731820> (дата обращения - 01.10.2024).

³ В 2023 году банки предотвратили мошеннические хищения на 5,8 трлн рублей // Банк России. Новости. 2024. 13 февраля. URL: <https://www.cbr.ru/press/event/?id=18419> (дата обращения - 01.10.2024).

⁴ Информационно-аналитическая записка о результатах оперативно-служебной деятельности подразделений системы ГУ МВД России по г. Москве за 2023 год // ГУ МВД России по г. Москве. URL: <https://77.мвд.рф/Dejatelnost/rezultati/rezultaty-deyatelnosti/2023-rod?ysclid=m2ufugi4uj581863750> (дата обращения 01.10.2024).

⁵ Там же.

Дистанционные хищения как постоянно
меняющийся вид преступности

телефонной связи в отношении банковских учреждений в Московском регионе.

Из материалов дела следует, что неустановленное лицо № 1 создало организованную группу для систематического совершения хищений денежных средств путем обмана, посредством подмены купюр в банкоматах банковских учреждений и использования телефонной связи в отношении банковских учреждений, расположенных на территории Московского региона, для чего привлекло в состав организованной группы А. и неустановленных лиц.

Согласно разработанному неустановленным лицом № 1 преступному плану, используя заранее приисканные А. мобильные телефоны и сим-карты различных операторов связи с неустановленными абонентскими номерами, зарегистрированные на номинальных лиц, а также банковские карты ПАО ВТБ, АО «Альфа-Банк» и АО «Райффайзенбанк», оформленные на лиц, не осведомленных о преступной деятельности, участники организованной группы должны были осуществлять зачисления денежных средств на банковские счета, прикрепленные к указанному банковским картам номинальных лиц, находящихся в распоряжении членов организованной группы. После этого под видом снятия указанных денежных средств с банковского счета с помощью банковской карты в банкоматах банков в момент выдачи банкоматом денежных купюр должны были осуществлять подмену денежных купюр в модуле приема/выдачи денежных средств банкомата путем изъятия денежных купюр номиналом по 5000 руб. каждая и одновременно помещать в модуль приема/выдачи денежных средств банкомата денежные купюры номиналом по 100 руб. каждая, тем самым завуалировав свои преступные действия. Далее они звонили в службу поддержки

банков с абонентских номеров, сим-карты которых оформлены на номинальных лиц, и сообщали заведомо ложную информацию о том, что банкоматом не выдана запрошенная сумма денежных средств по банковской карте, оформленной на номинальное лицо. Так мошенники пытались ввести в заблуждение операторов клиентского обслуживания банков.

В ходе телефонного разговора с операторами клиентского обслуживания банков А. представлялся клиентом банка, на чье имя оформлена банковская карта, и сообщал операторам клиентского обслуживания банков заведомо не соответствующую действительности информацию о том, что банкомат по заявке клиента предоставил к выдаче денежные купюры непотребного вида, либо клиент не успел за предоставленные программой банкомата 45 секунд получить денежные средства, в связи с чем указанные денежные средства клиентом не получены и обратно на банковский счет клиента не зачислены. На основе этой информации сотрудники банков составляли претензии, по рассмотрении которых банки перечисляли денежные средства с внутреннего счета банка на банковский счет клиента, которому средства якобы не были выданы. В последующем А. производил снятие этих денежных средств, осуществляя хищение денежных средств, принадлежащих банкам, путем обмана.

Весь период функционирования организованной группы ее члены придерживались высокой степени маскировки, использовали систему мгновенного обмена сообщениями через мессенджер «Телеграм» (Telegram) с автоматически исчезающими сообщениями через определенное время, используемыми для связи между собой, и киви-кошелек, номер счета которого следствием установлен не был, зарегистрированный на номинальное лицо,

используемый и контролируемый неустановленным лицом № 1 для осуществления зачисления денежных переводов похищенных денежных средств и последующего их распределения между участниками организованной группы.

Деятельность организованной группы не требовала локального местонахождения и проживания постоянных ее членов ввиду того, что главным и обязательным условием, способствующим и обеспечивающим возможность совершения преступлений, являлась необходимость нахождения ее членов в зоне покрытия сотовой связи и мобильного интернета в момент совершения преступлений, а в целях конспирации исполнители преступлений, не зная друг друга, узнавали о времени, месте и способе совершения преступлений через мессенджер «Телеграм» от организатора – неустановленного лица № 1.

Преступная деятельность неустановленного лица № 1, А. и неустановленных лиц № 2, №3, № 4, действовавших в составе вышеуказанной организованной группы, выразилась в совершении 51 преступления в период времени с 15 августа 2022 года по 14 ноября 2022 года в отношении АО «Альфа-Банк» на сумму 75 000 руб., в отношении АО «Райффайзенбанк» на сумму 2 980 000 руб. и в отношении ПАО ВТБ на сумму 2 619 000 руб.

Мошенники относительно легко выводили крупные суммы, в том числе пользуясь несовершенной системой внутреннего контроля банков.

Другое направление дистанционного тайного хищения денежных средств рассмотрим на примере уголовного дела в отношении О. по обвинению в совершении 34 преступлений, предусмотренных п. «а» ч. 4 ст. 158 УК РФ, и одного преступления, предусмотренного ч. 3 ст. 30 п. «а» ч. 4 ст. 158 УК РФ. В данном случае неустанов-

ленное лицо № 1 создало этническую организованную группу для систематического совершения хищений денежных средств посредством списания денежных средств с банковского счета ООО «Вайлдберриз», привлекло в состав организованной группы О. и Б.

Согласно разработанному неустановленным лицом № 1 преступному плану, объектами преступлений должен был стать маркетплейс товаров – ООО «Вайлдберриз». Используя заранее приисканные Б. сим-карты различных операторов связи, зарегистрированные на номинальных лиц, а также заранее приисканные Б. и О. банковские карты, зарегистрированные на лиц, не осведомленных об их преступной деятельности, соучастники должны были регистрироваться на сайте маркетплейса товаров – ООО «Вайлдберриз», заказывать и получать различные товары по своему усмотрению, в том числе посредством неосведомленных лиц, использующих сим-карты операторов связи и банковские карты, зарегистрированные на себя. Затем О., используя предоставленные неустановленным лицом № 1 коды доступа (пароли), позволяющие списывать денежные средства с банковского счета ООО «Вайлдберриз» на банковские счета заказчиков товара, в размере стоимости оплаченного товара, используя услугу по возврату товара, который в действительности не возвращен, тем самым завуалировав свои преступные действия, распоряжались похищенными денежными средствами путем обналичивания, списания на подконтрольные неустановленному лицу № 1 банковские счета или использования для оплаты следующих заказов на маркетплейсе товаров – ООО «Вайлдберриз», то есть осуществляли хищение денежных средств, принадлежащих маркетплейсу товаров – ООО «Вайлдберриз».

Дистанционные хищения как постоянно
меняющийся вид преступности

Весь период функционирования организованной группы ее члены придерживались высокой степени маскировки, использовали системы мгновенного обмена сообщениями «Телеграм» (Telegram) для связи между собой, а также использовали неустановленные банковские карты, зарегистрированные на номинальных лиц и контролируемые участниками данной организованной группы для осуществления зачисления похищенных денежных средств и последующего их распределения между собой.

Конкретная преступная деятельность неустановленного лица № 1, Б. и О., действовавших в составе организованной группы, выразилась в совершении в 2022–2023 годах 35 преступлений. В целом преступники причинили ООО «Вайлдберриз» ущерб более чем на 2 млн руб.

Третье направление дистанционного хищения денежных средств представим на примере пресечения в 2023 году правоохранительными органами Юго-Восточного административного округа Москвы деятельности организованной преступной группы, члены которой представлялись сотрудниками правоохранительных органов.

В данном случае неустановленное лицо создало организованную группу для систематического совершения хищений денежных средств путем обмана посредством телефонной связи в отношении граждан, проживающих на территории г. Москвы, в состав которой неустановленное лицо привлекло Ф., которая привлекла П.

Согласно разработанному преступному плану, объектами преступлений должны были стать пожилые москвичи. Представляясь по телефону сотрудниками полиции и органов предварительного следствия, неустановленное лицо сообщало пожилым абонентам заведомо ложную информацию об их родственниках, якобы попав-

ших в беду, предлагая перевести деньги для их вызволения. Неустановленное лицо, представляясь сотрудником полиции и органов предварительного следствия, предлагало жертве передать денежные средства водителю ООО «Яндекс.Такси», не осведомленному о преступной деятельности. В свою очередь, Ф. согласно отведенной ей неустановленным лицом роли в организованной группе, являясь исполнителем преступлений, должна сообщать П. информацию о дате, времени и адресе прибытия водителя такси, давать указания П. получать от последнего денежные средства, добытые путем обмана лиц пожилого возраста, оплачивать водителю такси выполнение заказа. В свою очередь, П., являясь исполнителем преступлений, должен был получать от водителей ООО «Яндекс.Такси» денежные средства, добытые путем обмана лиц пожилого возраста, и привозить их по адресу совместного проживания с Ф., которая и осуществляла зачисление похищенных денежных средств на неустановленные банковские счета, подконтрольные неустановленному лицу. Весь период функционирования организованной группы ее члены придерживались высокой степени маскировки, использовали систему мгновенного обмена сообщениями «Телеграм» (Telegram) для связи между собой.

При совершении дистанционных хищений распространены случаи использования банковских карт дропперов – лиц, на чьи карты перечисляются похищенные денежные средства.

В настоящее время в производстве специализированного отдела по расследованию преступлений общеуголовной направленности «дистанционные хищения» СУ УВД по ЮВАО ГУ МВД России по г. Москве находится уголовное дело в отношении группы лиц, в числе которых К.,

имея умысел на систематическое совершение тяжких преступлений корыстной направленности, а именно тайное хищение денежных средств с банковских счетов пожилых москвичей, под предлогом выплаты пенсионных начислений и других социальных выплат создал в Ростове-на-Дону преступное сообщество с высокой степенью организованности, сплоченности, взаимозаменяемости и взаимопомощи участников.

Действуя по ранее разработанному плану, К. как руководитель преступного сообщества создал не менее трех внутренне, территориально и функционально обособленных структурных подразделений. Одно из них, действуя в г. Шахты Ростовской области, открывало банковские счета на лиц, не осведомленных о преступной деятельности, для перечисления на них похищенных с банковских счетов денежных средств. Второе территориально и функционально обособленное структурное подразделение преступного сообщества было создано в Ростове-на-Дону для хищения средств с банковских счетов пожилых граждан. Для этого было создано некое подобие колл-центра с использованием средств сотовой связи, зарегистрированных на других лиц. Часть переговоров и переписки велась на цыганском языке. Преступники представлялись сотрудниками Пенсионного фонда, путём обмана получали данные для входа в личные кабинеты потерпевших с целью тайного хищения денежных средств с банковских счетов граждан. Третье территориально и функционально обособленное структурное подразделение преступного сообщества (преступной организации) работало на территории Ростовской области и Краснодарского края и отвечало за материально-техническое обеспечение.

В совокупности перечисленные структурные подразделения действовали на

территории Волгоградской, Ростовской, Саратовской, Липецкой областей, Ставропольского, Краснодарского краев и Московского региона. Организацию отличали следующие черты: сплоченность соучастников на основе единого преступного умысла, стабильность состава (в том числе из числа родственников) и согласованность действий соучастников, ограничение контактов членов преступного сообщества между собой в конспиративных целях, общность материально-финансовой базы, взаимодействие посредством руководителей различных ее подразделений в целях реализации общих преступных намерений, а также длительность периода преступной деятельности с отработанной системой совершения преступлений и масштабностью преступной деятельности.

Созданное К. преступное сообщество также характеризовалось наличием единого руководства, при этом все три его структурных подразделения осуществляли преступную деятельность при четкой координации действий создателем и руководителем преступного сообщества и одновременно руководителем второго и третьего структурных подразделений К. В общей сложности в 2019–2023 годах преступным сообществом было совершено не менее 62 преступлений, потерпевшим причинен ущерб более чем на 43 млн руб.

Анализ упомянутых и аналогичных уголовных дел о преступлениях при участии «дропперов», предоставлявших свои банковские карты, показал сложность их привлечения к ответственности ввиду проблем доказывания умысла на соучастие в хищении. Эти лица передают свои банковские карты неустановленным лицам за денежное вознаграждение, формально не будучи проинформированными об их использовании в целях совершения преступлений. В отсутствие данных, подтверждающих их

Дистанционные хищения как постоянно
меняющийся вид преступности

причастность к мошенничеству, основной для привлечения их к уголовной ответственности не имеется.

В то же время более активную позицию могли бы занять банки. Их правила, как и рекомендации Банка России¹, запрещают любые передачи банковских карт третьим лицам, и если за это была бы предусмотрена санкция, она бы имела действие.

Кроме того, постепенно формируется судебная практика, позволяющая взыскивать с владельцев счетов, на которые перечислялись денежные средства, суммы необоснованного обогащения.

В текущем году прокуратурами Юго-Восточного административного округа г. Москвы в интересах пенсионеров подано пять исковых заявлений о взыскании неосновательного обогащения в порядке ст. 45 ГПК РФ.

Также прокуратурой Юго-Восточного административного округа г. Москвы подготовлен иск в порядке ст. 45 ГПК РФ о признании сделки купли-продажи квартиры недействительной.

В целом с развитием технологий и их доступностью способы хищений, совершаемых дистанционно с использованием электронных средств платежа, цифровых данных, будут расширяться и усложняться-

ся. Следует признать недостаточным применение лишь уголовно-правовых средств противодействия. Более активной и неприемлимой должна быть политика банков и Центрального банка России к дроппингу и иным формам содействия совершению преступлений. Учитывая, с одной стороны, высокую латентность такого рода «невных» преступлений, а с другой – то, что все они оставляют цифровой след, стоит задача более активно использовать искусственный интеллект, как это уже делается в международной практике. Анализ уголовных дел о преступлениях, где потерпевшими были пожилые граждане, показывает недостаточность профилактической работы, что позволяет мошенникам относительно легко добиваться своих целей.

Поскольку дистанционные хищения являются развивающимся и быстро диверсифицирующимся видом преступности, стоит задача прогноза такого развития с учётом как развития технологий, так и уже накопленного опыта противодействия аналогичным преступлениям. Здесь также важна активная позиция банков, которые должны прогнозировать риски при подготовке к внедрению каждой новой платежной технологии.

Литература

1. *Евтушенко И.И., Венедиктов А.А.* Дистанционные хищения: понятие и признаки // Гуманитарные, социально-экономические и общественные науки. 2020. № 12-2. С. 65–67. EDN ZCSTAD. DOI: 10.23672/z6696-2718-7989-m
2. *Иванова Л.В.* Хищение с использованием информационных технологий: проблемы квалификации // Юридическая наука и правоохранительная практика. 2020. № 1 (51). С. 29–36. EDN NMIWMY.
3. *Тюнин В.И., Чабукиани О.А.* Мошенничество с использованием электронных средств платежа (вопросы правоприменения) // КриминалистЪ. 2023. № 4 (45). С. 92–98. EDN OFUYKG.

¹ Методические рекомендации Банка России от 6 сентября 2021 года № 16-МР «О повышении внимания кредитных организаций к отдельным операциям клиентов – физических лиц» // Центральный банк Российской Федерации. URL: https://cbr.ru/StaticHtml/File/117540/20210906_16-mr.pdf (дата обращения 01.10.2024).

4. Степанова М.А., Царёв Е.В. Мошенничество с использованием электронных средств платежа: проблемы квалификации // Вестник Белгородского юридического института МВД России. 2022. № 3. С. 60–63. EDN IJKQFZ.
5. Старостенко Н.И. Понятие и виды методов социальной инженерии, применяемых при совершении преступлений в сфере информационно-телекоммуникационных технологий // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2023. № 1 (61). С. 152–159. EDN IFRAXS. DOI: 10.36511/2078-5356-2023-1-152-159
6. Исанбаев И.С., Якупов Д.Н. Меры по предотвращению преступлений, связанных с хищением денежных средств в сфере информационно-телекоммуникационных технологий с использованием подменного абонентского номера // Аграрное и земельное право. 2024. № 9 (237). С. 303–305. EDN BYPKTZ. DOI: 10.47643/1815-1329_2024_9_303
7. Тарасова М.Ю. О современных способах и видах мошенничества, совершаемого с использованием информационно-телекоммуникационных технологий // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2023. № 3 (73). С. 42–45. EDN IEQWWL.
8. Анненкова Е.А., Волков А.С., Попова Е.А. Преступления в сфере электронных средств платежей как объект криминалистического исследования // Экономическая безопасность и качество. 2020. № 2 (39). С. 43–49. EDN EGZKYU.
9. Москальков А.В. О способах совершения преступлений против собственности в сети Интернет // Известия Юго-Западного государственного университета. Серия: История и право. 2023. Т. 13. № 6. С. 199–208. EDN PATPQU. DOI: 10.21869/2223-1501-2023-13-6-199-208
10. Cherniavskiy S., Babanina V., Vartyletska I., Mykytchuk O. Peculiarities of the Economic Crimes Committed with the Use of Information Technologies // European Journal of Sustainable Development. 2021. Vol. 10. No. 1. Pp. 420. DOI: 10.14207/ejsd.2021.v10n1p420

References

1. Yevtushenko I.I., Venediktov A.A. (2020) Remote theft: Concept and features. *Humanities, socio-economic and social sciences*. No. 12-2. Pp. 65–67. DOI: 10.23672/z6696-2718-7989-m (In Russian).
2. Ivanova L.V. (2020) Theft using information technology: Problems of qualification. *Legal science and law enforcement practice*. No. 1 (51). Pp. 29–36. (In Russian).
3. Tyunin V.I., Chabukiani O.A. (2023) Fraud using electronic means of payment (law enforcement issues). *Kriminalist [Criminalist]*. No. 4 (45). Pp. 92–98. (In Russian).
4. Stepanova M.A., Tsarev E.V. (2022) Fraud using electronic means of payment: problems of qualification. *Vestnik of Putilin Belgorod Law Institute of Ministry of the Interior of Russia*. No. 3. Pp. 60–63. (In Russian).
5. Starostenko N.I. (2023) The concept and types of social engineering methods used in the commission of crimes in the field of information and telecommunication technologies. *Bulletin of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia*. No. 1 (61). Pp. 152–159. DOI: <https://doi.org/10.36511/2078-5356-2023-1-152-159> (In Russian).
6. Isanbayev I.S., Yakupov D.N. (2024) Measures to prevent crimes related to the theft of funds in the field of information and telecommunication technologies using a fake subscriber number. *Agrarian and land law*. No. 9 (237). Pp. 303–305. DOI: http://doi.org/10.47643/1815-1329_2024_9_303 (In Russian).

Дистанционные хищения как постоянно
меняющийся вид преступности

7. Tarasova M.Yu. (2023) On modern methods and types of fraud committed using information and telecommunication technologies. *Bulletin of the Kaliningrad Branch of the Saint-Petersburg University of the Ministry of Internal Affairs of Russia*. No. 3 (73). Pp. 42–45. (In Russian).
8. Annenkova E.A., Volkov A.S., Popova E.A. (2020) Crimes in the sphere of electronic means of payment as an object of criminalistic research. *Ekonomicheskaya bezopasnost' i kachestvo* [Economic security and quality]. No. 2 (39). Pp. 43–49. (In Russian).
9. Moskalkov A.V. (2023) About Ways to Commit Crimes Against Property on the Internet. *Proceedings of the Southwest State University. Series: History and Law*. Vol. 13. No. 6. Pp. 199–208. DOI: <https://doi.org/10.21869/2223-1501-2023-13-6-199-208> (In Russian).
10. Cherniavskiy S., Babanina V., Vartyletska I., Mykytchyk O. (2021) Peculiarities of the Economic Crimes Committed with the Use of Information Technologies. *European Journal of Sustainable Development*. Vol. 10. No. 1. Pp. 420. DOI: 10.14207/ejsd.2021.v10n1p420

Поступила в редакцию: 04.11.2024

Received: 04.11.2024

Поступила после рецензирования: 26.11.2024

Revised: 26.11.2024

Принята к публикации: 10.12.2024

Accepted: 10.12.2024