Дата поступления рукописи в редакцию: 02.04.2026 г.
Дата принятия рукописи в печать: 25.04.2026 г.
DOI: 10.24412/2782-3849-2026-4-149-153

БОДЯКОВ Владимир Николаевич,

кандидат юридических наук, доцент, доцент кафедры уголовно-процессуального права и криминалистики юридического факультета, ВЮИ ФСИН России,

e-mail: krim33@mail.ru

МОРОЗОВ Роман Михайлович,

кандидат юридических наук, доцент, доцент кафедры уголовно-правовых наук, Северо-Западный институт (филиал) Университета имени О.Е. Кутафина (МГЮА),

e-mail: morozur@mail.ru

ТАКТИКО-КРИМИНАЛИСТИЧЕСКИЕ АСПЕКТЫ ВЗАИМОДЕЙСТВИЯ СЛЕДОВАТЕЛЯ И СПЕЦИАЛИСТА ПРИ ПРОИЗВОДСТВЕ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ В ХОДЕ РАССЛЕДОВАНИЯ ДИСТАНЦИОННОГО МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ МАРКЕТПЛЕЙСОВ

Аннотация. *Рассматриваются вопросы, касающиеся современных видов мошенничества, совершаемого с использованием дистанционных технологий. Определен механизм совершения дистанционного мошенничества, а также признаки и обстоятельства, обуславливающих проблемные вопросы, возникающие в процессе работы органов дознания и предварительного следствия на стадии возбуждения уголовного дела и предварительного расследования. Также сформулированы отдельные рекомендации по производству отдельных следственных действий с привлечением к участию в них третьих лиц.*

Ключевые слова: *мошенничество, следственный осмотр, допрос, взаимодействие, дистанционное мошенничество, маркетплейс, расследование преступлений, хищение.*

BODYAKOV Vladimir Nikolaevich,

candidate of legal sciences, associate professor Docent at the Department of department of criminal justice and forensic science of the Faculty of Law, Faculty of Law of the Higher Educational Institution of the Federal Penitentiary Service of Russia

MOROZOV Roman Mikhailovich

candidate of legal sciences, associate professor Associate Professor of the Department of Criminal Law Sciences at the North-Western Institute (Branch) of the Kutafin University (MSAL)

TACTICAL AND FORENSIC ASPECTS OF THE INTERACTION BETWEEN AN INVESTIGATOR AND A SPECIALIST DURING THE PRODUCTION OF INVESTIGATIVE ACTIONS IN THE COURSE OF INVESTIGATING REMOTE FRAUDS USING MARKETPLACES

Annotation. *The article discusses modern types of fraud committed using remote technologies. It defines the mechanism of committing remote fraud, as well as the signs and circumstances that cause problems during the work of the investigative and pre-investigative bodies at the stage of initiating a criminal case and conducting preliminary investigations. The article also provides specific recommendations for conducting certain investigative actions involving third parties.*

Key words: *fraud, investigative examination, interrogation, interaction, remote fraud, marketplace, crime investigation, theft.*

Хищение чужого имущества путем обмана или злоупотребления доверием составили около четверти преступлений (23,2%), выявленных правоохранительными структурами в 2025 году. Из более чем 411,7 тыс. фактов совершения мошеннических действий 84,5% были совершены с использованием информационных технологий и компьютерной информации [7]. При общей позитивной тенденции сокращения преступлений рассматриваемой категории по сравнению с предыдущим 2024 годом (– 7,6%), количество раскрытых преступлений, связанных

с совершением мошенничества составляет менее шестой доли (16,1%) от их общего числа. В этой связи согласимся с мнением профессоров Давыдова В.О. и Тишутиной И.В., которые в своем исследовании отметают, что не смотря на фактически новые возможности получения доказательственной и ориентирующей информации правоохранительными структурами за счет цифровизации расследования, то есть использования цифровых методов и средств, «действовать приходится по принципу догоняющих» [Давыдов, Тишутина, с. 20]. Связано это, по нашему мнению, прежде всего с высоким уровнем дистанционного мошенничества, сложностью выявления фактического местонахождения лица, виновного в совершении преступления, а также недостаточным уголовно-процессуальным закреплением порядка и алгоритмизации работы со следами в цифровой среде (телекоммуникационном пространстве).

Заметим, что традиционные виды мошенничества таких как покупка безвыигрышных лотерейных билетов или проверка оборудования подставной газовой службой, трансформировались в поле неправомерного завладения чужим имуществом (правом на чужое имущество) путем кражи пользовательских (учетных) идентификационных данных, использования дистанционных электронных платежных систем, интернет-площадок, маркетплейсов, сервисов по предоставлению государственных и муниципальных услуг («Госуслуги»), а также уникальных форм безналичной оплаты (QR-кода), фейковой рекламы, чат-ботов. Так, в феврале 2026 года на Интернет-портале официального издания «Российской газеты» была размещена информация об участившихся случаях совершения мошеннических действий в отношении пенсионеров и иных получателей социальных мер поддержки путем направления в их адрес сообщений о необходимости проверки размера средств (выплат) после индексации пенсий и пособий в январе, феврале 2026 года [8]. Это говорит о непрерывной адаптивности способов совершения дистанционного мошенничества к современным изменениям в области социальной государственной политики и, очевидно, требует анализа и разработки новых путей и инструментов противодействия указанной группе противоправных действий. Также, среди негативных факторов, влияющих на процесс расследования мошенничества, М.М. Коблева, на примере раскрытия кибермошенничества, выделяет не только несовершенство норм материального права, недостаточную координацию взаимодействия правоохранительных органов с иными государственными структурами и частными организациями, специализирующимися на обеспечении компьютерной безопасности, но и отсутствие криминалистического обеспечения процедуры расследования мошенничества [Коблева, с. 190-191].

Отметим, что в содержании формулировки «дистанционное мошенничество», исследователи также не пришли к единому мнению. Так, большинство ученых связывают признак «дистанционности»:

- с отсутствием контакта потерпевшего с мошенником [Богданов, с. 16];
- с использованием средств мобильной связи, при котором лицо, совершившее мошенничество выступает в качестве «криминального оператора» [Литвинов, с. 76];
- с онлайн-мошенничеством, т.е. использованием современных компьютерных средств и технологий сотовой связи, в которых они выступают средством информационного обеспечения противоправной деятельности, промежуточным или автоматизированным средством совершения преступления [Яковлева, с. 78-79];
- с активным использованием информационного пространства, а также использованием психологических манипуляций и современных программных продуктов [Старостенко, с. 153].

Механизм совершения дистанционного мошенничества, а также вышеперечисленные признаки и обстоятельства, характеризующие, по мнению ученых, противоправное деяние, по большей части обуславливают количество проблемных вопросов, возникающих в процессе установления виновного лица, сбора доказательственной базы, а также в целом работы органов дознания и предварительного следствия на стадии возбуждения уголовного дела и предварительного расследования. При этом анализ отдельных аспектов криминалистического обеспечения своевременного выявления и расследования дистанционного мошенничества может позволить алгоритмизировать и оптимизировать действия субъектов раскрытия преступлений на каждом из этапов движения информации на пути от первично полученной к криминалистически значимой.

Криминалистическое обеспечение раскрытия мошенничества включает следующие основные элементы:

- информационное обеспечение, включающее порядок получения информации правоохранительными

структурами об обстоятельствах произошедшего события;

- технико-криминалистическое обеспечение расследования преступного события, представленного использованием компьютерной техники, позволяющей собрать и исследовать компьютерную информацию, т.е. сведения, находящиеся в телекоммуникационном пространстве (IP-адреса, истории браузеров, личных кабинетов, переписки и иные коммуникации в мессенджерах, специализированное программное обеспечение - VPN, технологии SIP-телефонии и т.д.);
- тактико-криминалистическое обеспечение, подразумевающее не только совокупность тактических приемов и рекомендаций производства отдельных следственных действий в рамках проведения предварительной проверки сообщения о преступлении (предварительного расследования), но и тактические особенности внутреннего и межведомственного взаимодействия правоохранительных структур, а также взаимодействие субъекта раскрытия преступления с иными учреждениями (операторы связи, компании, интернет-платформы, банки и иные кредитно-финансовые организации).

Раскроем взаимодействие следователя как аспект криминалистического обеспечения на примере расследования мошеннических действий с использованием маркетплейсов.

Одной из указанных форм мошенничества выступает совершение хищения собственности (товаров), принадлежащих маркетплейсу, путем обмана, сопряженного с использованием специализированного программного обеспечения работы ПВЗ (ПВЗ – пункт выдачи заказа маркетплейса) (приложения по выдаче заказа, оформлению отказа от заказа и возврату товара на сортировочный центр, склад). Так, в соответствии с содержанием Приговора Ступинского городского суда Московской области № 1/248-2023 от 14.09.2023 Бурдина П.С., осуществляя трудовую деятельность в ПВЗ ООО «Вайлдберриз» и имея доступ к программе «WB Point», производила оформление заказов товаров на себя и иных лиц, но при их доставке в ПВЗ, помещала в программном обеспечении в «виртуальную коробку отказов», присваивала товары себе и тем самым, не возвращала их на склад, не вносила стоимость товаров в кассу ПВЗ. Предмет преступного посягательства был представлен более чем 400 наименованиями товаров, среди которых корм для собак, картина по номерам, нижнее белье, одежда, бытовая химия, косметические принадлежности, предметы интерьера, мелкая бытовая техника, секс-игрушки, аксессуары для компьютера и мобильных устройств, спортивное питание, украшения [9]. Сумма товаров, похищенных путем обмана, составила 576 413, 27 руб.

Как правило, поводом к возбуждению уголовного дела при дистанционных хищениях с использованием маркетплейсов является заявление лица, проводившего инвентаризацию. Заявление, в соответствии с содержанием ст. 141 УПК РФ, составляется в письменной форме. При этом, особенностью указанного заявления служит его составление и направление для последующей регистрации в отдел полиции, по месту нахождения ПВЗ маркетплейса, а не расположения склада, в который товар должен быть возвращен, а был похищен путем обмана мошенником. Также лицо, проводившее инвентаризацию и выявившее хищение товаров и материальных ценностей, составляет заявление в отношении не установленного лица, даже при наличии явных признаков фактического доступа к заказам только одного сотрудника (менеджера), что в свою очередь говорит о характере частно-публичной формы уголовного преследования.

Главным обстоятельством, подлежащим установлению на первоначальном этапе расследования совершения дистанционного мошенничества товаров с маркетплейсов является установление личности подозреваемого, а также размера причиненного ущерба.

Анализ материалов правоприменительной практики установления обстоятельств преступлений, предусмотренных ст. 159 УК РФ и связанных с хищением товарно-материальных ценностей с использованием маркетплейса, позволяет нам вычленить две основные тактико-криминалистические рекомендации при производстве отдельных следственных действий:

1. Производство осмотра предметов (документов) должно сопровождаться привлечением специалиста.

С учетом специфики способа совершения рассматриваемой группы преступлений, проводятся следующие виды осмотра:

- осмотр места происшествия (помещения, строения, используемого в качестве ПВЗ маркетплейса);
- осмотр документов, связанных с движением товара (договора оферты о реализации товара на маркетплейсе и об оказании услуг по доставке товаров физическим лицам, полученный из открытых источников сети «Интернет»; актов инвентаризаций, выборочных проверок наличия товарно-материальных

ценностей на складах, сортировочных пунктах, местах хранения; отчетов об утрате товаров; справок о причиненном маркетплейсу ущербе, в том числе в форме ответа на запрос следователя, направленного в адрес руководителя (регионального представителя) маркетплейса);

- осмотр предметов (оптических дисков с видеозаписями действий лица, осуществлявшего мошенничество, при обработке товаров; предметов, изъятых в ходе производства обыска, выемки);
- осмотр документов, связанных с движением денежных средств (выписок со счета маркетплейса о выплате и зачислении агентских вознаграждений по договору оферты).

В данном случае, в качестве специалиста целесообразно привлекать менеджера по работе с клиентами маркетплейса либо заместителя регионального руководителя - лиц, на регулярной основе задействованных в операционной работе по контролю и анализу логистики, оформлению сопровождающих документов, мониторингу остатков товаров на складах, инвентаризации, т.е. напрямую связанных с работой ПВЗ маркетплейса.

2. Производство допроса свидетелей предполагает допрос сотрудника (специалиста) службы безопасности маркетплейса.

Тактические особенности производства вопросно-ответного этапа рабочей стадии допроса специалиста службы безопасности следователем сводятся к выяснению следующих обстоятельств:

- основных видов электронной торговли маркетплейса;
- порядка, требований к заключению договора оферты с представителем маркетплейса;
- функциональных возможностей маркетплейса;
- порядка видеонаблюдения за клиентской зоной ПВЗ, а также операциями менеджера при приемке, выдаче, раскладке, возврату товаров (заказов);
- алгоритму (маршрутной карте) движения товаров (заказов);
- сведений о направлении заявки на открытие ПВЗ (дата, анкетные данные заявителя, реквизиты организации);
- сведений о мониторинге товаров, которые не были обнаружены на складах, а также о проверке данных личного кабинета покупателей маркетплейса.

Таким образом, взаимодействие следователя со специалистом маркетплейса позволяет установить обстоятельства конкретного факта мошенничества, алгоритмизировать последующий этап расследования преступления, установить возможных соучастников преступного события и минимизировать последствия совершения преступления за счет установления конкретного размера ущерба, подлежащего возмещению в рамках разрешения гражданского иска.

Список литературы:

[1] Богданов А.В., Ильинский И.И., Хазов Е.Н. Киберпреступность и дистанционное мошенничество как одна из угроз современному обществу // Криминологический журнал. 2020. № 1. С.15-20.

[2] Давыдов В.О., Тишутина И.В. Цифровые следы в расследовании дистанционного мошенничества // Известия Тульского государственного университета. Экономические и юридические науки. 2020. № 3. С. 20-27.

[3] Коблева М.М. Тактико-криминалистическое обеспечение расследования мошенничества с использованием компьютерной информации // Пробелы в российском законодательстве. 2019. № 2. С. 190-192.

[4] Литвинов Н.Д., Федоров А.Н. Мошенничество с использованием средств мобильной связи (дистанционное): понятие и особенности совершения // Научно-исследовательские публикации. 2015. № 12. С. 73-80.

[5] Старостенко Н.И. Криминалистические особенности способов совершения хищений с применением методов социальной инженерии и информационно-телекоммуникационных технологий // Вестник Санкт-Петербургского университета. Право 1. 2024. № 1. С. 152-170.

[6] Яковлева Л.В. Современные способы совершения дистанционного мошенничества // Вестник Краснодарского университета МВД России. 2021. №4. С. 77-80.

[7] Краткая характеристика состояния преступности в Российской Федерации за январь - декабрь 2025 года // Официальный сайт Министерства внутренних дел Российской Федерации. URL: https://мвд.рф/reports/item/77848182/.

[8] Соцфонд предупредил о новом виде мошенничества в отношении пенсионеров// Российская газета. URL: https://rg.ru/2026/02/11/socfond-predupredil-o-novom-vide-moshennichestva-v-otnoshenii-pensionerov.html.

[9] Приговор № 1/248-2023 от 14.09.2023. Официальный сайт Ступинского городского суда Московской области. URL: https://stupino--mo.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=647221465&delo_

id=1540006&new=0&text_number=1.

References:

[1] Bogdanov A.V., Ilyinsky I.I., Khazov E.N. Cybercrime and remote fraud as one of the threats to modern society//Criminological Journal. 2020. № 1. S.15-20.
[2] Davydov V.O., Tishutina I.V. Digital traces in the investigation of remote fraud//Izvestia Tula State University. Economic and legal sciences. 2020. № 3. S. 20-27.
[3] Kobleva M.M. Forensic support for the investigation of fraud using computer information// Gaps in Russian legislation. 2019. № 2. S. 190-192.
[4] Litvinov N.D., Fedorov A.N. Fraud using mobile communications (remote): concept and features of the commission//Research publications. 2015. № 12. S. 73-80.
[5] Starostenko N.I. Forensic features of methods of embezzlement using methods of social engineering and information and telecommunication technologies//Bulletin of St. Petersburg University. Right 1. 2024. № 1. S. 152-170.
[6] Yakovleva L.V. Modern methods of committing remote fraud//Bulletin of the Krasnodar University of the Ministry of Internal Affairs of Russia. 2021. №4. S. 77-80.
[7] A brief description of the state of crime in the Russian Federation for January - December 2025// Official website of the Ministry of Internal Affairs of the Russian Federation. URL: https://мвд.рф/reports/item/77848182/.
[8] Sotsfond warned of a new type of fraud against pensioners//Rossiyskaya Gazeta. URL: https://rg.ru/2026/02/11/socfond-predupredil-o-novom-vide-moshennichestva-v-otnoshenii-pensionerov.html.
[9] Sentence No. 1/248-2023 of 14.09.2023. Official website of the Stupinsky City Court of the Moscow Region. URL: https://stupino--mo.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=647221465&delo_id=1540006&new=0&text_number=1.