УДК 343.14
DOI 10.36511/2078-5356-2021-1-143-148

Поздышев Роман Сергеевич
Roman S. Pozdyshev

кандидат юридических наук, старший преподаватель кафедры предварительного расследования Нижегородская академия МВД России (603950, Нижний Новгород, Анкудиновское шоссе, 3)

candidate of science (law), senior teacher of the chair of preliminary investigation
Nizhny Novgorod academy of the Ministry of internal affairs of Russia (3 Ankudinovskoe shosse, Nizhny Novgorod, Russian Federation, 603950)

E-mail: rmanpzdyshev@rambler.ru

Проблемные вопросы практики расследования хищений безналичных и электронных денежных средств

Problematic issues in the practice of investigating the theft of non-cash and electronic funds

В статье анализируются проблемные вопросы, возникающие в ходе расследования хищений безналичных и электронных денежных средств. Рассматриваются материалы судебно-следственной практики по указанной категории уголовных дел, а также трудности, с которыми сталкиваются следователи при их расследовании. В ходе исследования выявлен положительный опыт противодействия рассматриваемым хищениям и предложены пути совершенствования следственной практики.

Ключевые слова: хищение, кража, мошенничество, безналичные деньги, электронные деньги, расследование.

The article analyzes the problematic issues that arise during the investigation of theft of non-cash and electronic funds. The materials of judicial and investigative practice on this category of criminal cases are considered, as well as the difficulties faced by investigators in their investigation. During the research, the positive experience of countering the considered embezzlement was revealed and ways to improve investigative practice were proposed.

Keywords: theft, fraud, non-cash money, electronic money, investigation.

С развитием информационных технологий и их полномасштабным и глубоким внедрением в обыденную жизнь использование денежных средств и финансовых инструментов в нематериальном виде становится распространенным и обычным явлением для всех слоев населения. Трансформирование значительного количества ценностей в цифровую форму провоцирует смещение зоны интереса криминальных элементов, связанных с преступлениями против собственности, с реальных вещей на имущество, не имеющее вещественной природы. Такое умозаключение подтверждает статистика, содержащаяся в обзоре Центрального Банка России, согласно которому в 2019 году объем всех операций, совершенных без согласия клиентов (физических и юридических лиц) с использованием электронных средств платежа, составил 6426,5 млн рублей. Количество таких операций — 576 566 единиц [1]. Данные обстоятельства обусловливают необходимость усиления внимания правоохранительных органов к указанной растущей проблеме и подтверждают актуальность настоящего исследования.

Эмпирической базой исследования явились материалы судебной и следственной практики, в частности, материалы уголовных дел о преступлениях, связанных с хищениями безналичных и электронных денег, находящихся в производстве органов предварительного следствия МВД России за период с 2017 по 2020 годы. Кроме того, в рамках данной работы было проведено интервьюирование и анкетирование 84 представителей следственных подразделе-

ний МВД России, представляющих различные территориальные органы нескольких регионов. Результатом применение указанных методов явилось выявление наиболее распространенных проблем процессуального и организационного характера, возникающих при расследовании преступлений указанной категории. Данные проблемы для наглядности целесообразно объединить в условные агрегированные группы.

Проблемы, связанные с получением информации от кредитных организаций, операторов по переводу денежных средств, интернет-провайдеров, операторов сотовой связи.

Данная группа проблем является наиболее распространенной. Следственные органы почти всех субъектов Российской Федерации указывают ее в качестве основного препятствия расследованию преступлений указанной категории. При этом одним из ключевых факторов, влияющих на успех расследования хищений электронных денежных средств, является надлежащее взаимодействие с различными структурами и организациями, предоставляющими услуги по переводу денежных средств, а также услуги телекоммуникационной, мобильной и интернет-связи.

Хищение электронных денежных средств, в том числе с использованием информационно-телекоммуникационных технологий, в большинстве случаев совершается путем осуществления различными способами безналичных переводов на банковские счета, электронные счета (например «Киви-кошелек») и на счета абонентских номеров операторов сотовой связи, которые зарегистрированы на несуществующих либо на подставных лиц. При этом данные последних используются без их ведома (например, с использованием утерянных паспортов, либо персональные данные могут быть получены из различных незаконных источников). Вторым распространенным способом совершения преступлений рассматриваемой категории является создание интернет-сайтов, электронных страниц (вложений), с целью их использования для хищения наличных и безналичных денежных средств, в том числе путем обмана (например, под предлогом предоплаты за покупку товаров, сведения о продаже которых размещаются на сайтах объявлений и интернет-магазинов, либо под предлогом разблокировки якобы заблокированной банковской карты, в результате чего потерпевшие сами сообщают необходимые коды для осуществления операций по переводу денежных средств, либо оплате товаров через Интернет), а также для неправомерного доступа к компьютерной информации. При этом для создания интернет-сайтов, размещения объявлений и создания электронной страницы в социальных сетях («Одноклассники», «Вконтакте» и др.) достаточно введения любых недостоверных личных данных, которые в дальнейшем не позволяют идентифицировать лицо, осуществившее указанные действия. Кроме того, создание и использование интернет-ресурсов осуществляется дистанционно и в большинстве случаев доступ к сети «Интернет» осуществляется через мобильные телефоны с использованием сим-карт операторов сотовой связи, установить пользователей которых в большинстве случаев практически невозможно по вышеуказанным причинам, тем более если мобильный телефон и сим-карта использовались только в целях совершения конкретных однократных преступных действий.

Кроме того, преступники с целью избежания их идентификации в сети могут использовать различные средства анонимизации: VPN, прокси-серверы, TOR браузер и др.

Все вышеуказанное является объективными причинами, обусловливающими рассматриваемые проблемы получения нужной информации. При этом существуют и субъективные детерминанты.

К таким относится длительность исполнения запросов. Согласно информации, представленной органами предварительного следствия субъектов Российской Федерации, ответы на запросы из указанных организаций зачастую поступают в сроки свыше месяца, а в некоторых случаях и свыше шести месяцев. При этом получение необходимой информации характеризуется последовательностью, то есть для направления запроса, например, операторам сотовой связи, необходимо сначала получить ответ на запрос от интернет-провайдера, содержащий необходимую информацию. Кроме того, дополнительным осложняющим фактором является возможность представления некоторыми операторами связи информации в отношении абонентов, зарегистрированных исключительно на территории их регионального обслуживания.

Также к субъективным причинам проблем получения информации следует отнести малую информативность ответов на запросы. В ответах на запросы не всегда содержится значимая для органов следствия информация, не указываются номера счетов (банковских карт), на которые были переведены денежные средства потерпевших, и другая важная информация.

Названные факторы являются серьезным препятствием своевременному производству следственных действий, так как к моменту получения информации о преступной деятельности следы преступления могут быть безвозвратно утрачены. Например, при несвоевременном получении сведений в отношении обналичивания денежных средств видеозапись камер наблюдения в подразделении банка и банкомата может быть удалена. Наложение ареста на денежные средства, хранящиеся на банковских счетах, также является крайне затруднительным с учетом быстроты их перевода и длительности получения информации об этом.

Решением данных проблем представляется организация электронного документооборота между органами внутренних дел и иными организациями. Положительные примеры таких решений есть в ряде регионов Российской Федерации. Так, некоторыми территориальными подразделениями МВД России заключены соответствующие соглашения об организации документооборота с региональными отделениями ПАО «Сбербанк России», ПАО «Почта Банк», КИВИ Банк (АО), ПАО «Мегафон», ООО «Т2 Мобайл» и др. Данные соглашения позволяют снизить срок предоставления информации с месяца и более до нескольких суток, а также согласовать содержание запроса для получения необходимых сведений в полном объеме. Для повышения оперативности получения имеющей значение для расследования информации необходимо продолжение работы по заключению подобных соглашений, в том числе на федеральном уровне.

В качестве несистемного решения проблем длительности и малой информативности ответов следует указать на необходимость осуществления контроля исполнения запроса на всех его стадиях и установления личного контакта с исполнителем. Кроме того, необходимо обеспечение своевременного реагирования во всех случаях неисполнения запросов путем внесения представления в порядке части 2 статьи 158 Уголовно-процессуального кодекса Российской Федерации [2] (далее — УПК РФ) и решения вопроса о привлечении к административной ответственности по статье 17.7 Кодекса об административных правонарушениях Российской Федерации [3] (далее — КоАП РФ).

Проблемы, связанные с производством следственных и иных процессуальных действий, а также оперативно-разыскных мероприятий за пределами места производства предварительного расследования.

С учетом зачастую межрегионального характера рассматриваемой категории преступлений у органов предварительного расследования возникает необходимость производства следственных и иных процессуальных действий, а также оперативно-разыскных мероприятий за пределами места производства предварительного расследования. В большинстве таких случаев должностные лица направляют соответствующие поручения в порядке статьи 152 УПК РФ. Однако результаты поручений далеко не всегда содержат необходимые сведения. Эта группа проблем является второй по распространенности исходя из сведений, предоставленных территориальными органами внутренних дел, что не может не вызывать серьезных опасений.

Так, согласно указанным сведениям, зачастую направленные поручения исполняются не в установленный срок и формально, допросы носят неинформативный характер, а иногда сотрудники при исполнении поручения ограничиваются лишь предоставлением формальных справок и рапортов о невозможности установить местонахождение лица, что приводит к необходимости направления повторных поручений. Это неизбежно ведет к необоснованному затягиванию сроков расследования, потере наступательности следственных действий, безвозвратной утрате следов преступной деятельности и приостановлению предварительного следствия в связи с неустановлением лица, подлежащего привлечению в качестве обвиняемого.

Примером является уголовное дело № 11901870007050747, возбужденное СО ОМВД России по г. Ухте 13 июня 2019 года по признакам преступления, предусмотренного частью 2 статьи 159 Уголовного кодекса Российской Федерации [4] (далее — УК РФ), по факту хищения денежных средств у П., который через сайт «Авито» пытался приобрести надувную лодку. По месту производства предварительного расследования полностью установлены данные продавца — С., который проживает в Забайкальском крае. Незамедлительно после возбуждения уголовного дела направлено поручение в указанный регион о производстве следственных действий и оперативно-разыскных мероприятий в отношении С., далее направлялось напоминание. Однако ответ в установленные законом сроки получен не был.

Решением данной проблемы представляется усиление контроля за исполнительской дисциплиной со стороны руководителей, в частности за исполнением поручений, поступивших в

порядке статьи 152 УПК РФ. Кроме того, инициаторам поручений необходимо лично осуществлять контроль за их исполнением на всем протяжении путем установления личного контакта с исполнителем. А в тех случаях, когда необходимо производство следственных и иных процессуальных действий с потенциальным подозреваемым или ключевыми свидетелями, целесообразна организация командировки и личного производства этих мероприятий.

Проблемы, связанные с кадровой обеспеченностью подразделений органов внутренних дел.

Расследование уголовных дел о хищениях электронных денежных средств, в том числе совершенных с использованием информационно-телекоммуникационных сетей, в ряде случаев связано с использованием специальных знаний. В частности, возникает необходимость в производстве таких следственных действий, как осмотр компьютерной техники с участием специалиста, производство компьютерных, фоноскопических и иных узкоспециализированных экспертиз.

От ряда территориальных подразделений МВД России поступили сведения об отсутствии необходимого количества специалистов в области проведения технико-компьютерных и программно-технических судебных экспертиз. Также существует проблема по срокам исполнения фоноскопических экспертиз в связи с нехваткой экспертов в некоторых регионах и значительным объемом представляемых на экспертизу объектов. На исследование экспертам предоставляется большое количество аудиофайлов, в связи с чем длительное время занимает их обработка. Сократить количество файлов, где происходит общение и обман потерпевшего, невозможно, поскольку необходимо установить одним или несколькими лицами совершено преступление. Указанные обстоятельства существенно затягивают сроки предварительного следствия на несколько месяцев.

Кроме того, в результате интервьюирования сотрудников органов предварительного следствия и органов дознания выявлено, что не все сотрудники указанных подразделений по своим профессиональным качествам способны успешно противодействовать рассматриваемой категории преступлений. Для расследования данных преступлений сотрудник должен обладать определенными знаниями в сфере информационно-телекоммуникационных технологий: владеть соответствующим понятийным аппаратом, иметь базовые представления об архитектуре сетей связи, работе интернет-сайтов, современных средств анонимизации пользователя в сети и др. Все это необходимо для грамотного составления запросов, назначения экспертиз, производства допросов и др. В качестве положительного примера решения этой проблемы можно привести создание во многих территориальных органах подразделений и следственно-оперативных групп, специализирующихся на раскрытии и расследования хищений электронных денежных средств, в том числе совершенных с использованием информационно-телекоммуникационных сетей.

Кроме вышеназванных проблем и предлагаемых путей их решения, следует упомянуть о положительной практике территориальных подразделений МВД России, позволяющих системно изменить сложившуюся в целом негативную ситуацию, связанную с расследованием рассматриваемого вида преступлений.

В некоторых территориальных подразделениях созданы базы данных, аккумулирующие криминалистически значимую информацию о хищениях электронных денежных средств, в том числе совершенных с использованием информационно-телекоммуникационных технологий. Так, например, на базе ИЦ УМВД России по Мурманской области создана информационно-поисковая система «Дистанционное мошенничество», группирующая уголовные дела по заданным реквизитам (номера телефонов, на которые перечислялись денежные средства; IMEI телефонных аппаратов; адреса базовых станций; номера счетов и банковских карт; Ф. И. О. физических лиц; адреса снятия денежных средств). Благодаря данной базе автоматизирован и значительно упрощен процесс выявления преступлений, имеющих признаки серийности, что положительно влияет на полноту расследования уголовных дел и установление виновных лиц. За 12 месяцев 2019 года информационно-поисковой базой «Дистанционное мошенничество» по уголовным делам о преступлениях в сфере современных информационно-коммуникационных технологий выявлено 605 совпадений по телефонным номерам, номерам банковских карт и номерам банковских счетов. Соединено 457 уголовных дел, снято с учета 330 преступлений.

Вместе с тем, представляется необходимым создание аналогичной базы на федеральном уровне. Такое решение позволит своевременно и более эффективно раскрывать преступления и значительно снизит сроки расследования уголовных дел.

Среди положительных сторон во взаимодействии с кредитными учреждениями стоит отметить практику ГУ МВД России по Ставропольскому краю, где заключено соглашение с ПАО «Сбербанк России», согласно которому сотрудники банка обязаны информировать орган внутренних дел о совершении подозрительной операции с признаками мошенничества. В соответствии с указанным соглашением от сотрудников ПАО «Сбербанк» при обнаружении подозрительной операции по снятию или переводу денежных средств незамедлительно поступает информация в территориальные органы внутренних дел.

В ряде территориальных подразделений ведется централизованный список операторов сотовой связи и платежных систем, компаний, представляющих услуги ip-телефонии, банков и иных кредитных организаций, а также организаций, обслуживающих информационные ресурсы сети «Интернет», с указанием их почтовых и электронных адресов, телефонов сотрудников, осуществляющих исполнение запросов. Данный список постоянно поддерживается в актуальном состоянии, дополняется и рассылается в подчиненные подразделения.

В некоторых региональных управлениях МВД России успешно организовано взаимодействие с подразделениями ФСИН России. Так, в УФСИН России по Мурманской области на постоянной основе проводятся мероприятия по установлению используемых на территории исправительных учреждений абонентских номеров. На основании получаемой информации и в соответствии со статьей 64 Федерального закона от 7 июля 2009 года № 126-ФЗ «О связи» [5], пунктом 8 статьи 13 Федерального закона от 12 августа 1995 года № 144-ФЗ «Об оперативно-розыскной деятельности» [6], частью 8 статьи 82 Уголовно-исполнительного кодекса Российской Федерации [7], Правил внутреннего распорядка исправительных учреждений, утвержденных приказом Минюста России от 16 декабря 2016 года № 295 [8] в адрес компаний, предоставляющих услуги мобильной связи на территории Мурманской области, направляются соответствующие решения с целью приостановления использования активных абонентских номеров в местах дислокации исправительных учреждений. В случае обнаружения и изъятия средств мобильной связи у осужденных сотрудниками оперативных подразделений исправительных учреждений в адрес территориальных подразделений уголовного розыска УМВД России по Мурманской области направляется информация с целью ее использования для раскрытия преступлений, совершенных с привлечением средств мобильной связи.

В завершение перечисления положительных примеров противодействия хищениям электронных денежных средств, в том числе совершаемых с использованием информационно-телекоммуникационных технологий, следует упомянуть о превентивных мерах.

На интернет-сайтах многих подразделений МВД России в разделах правового информирования размещаются памятки гражданам о том, как не стать жертвой указанных преступлений. На постоянной основе осуществляется взаимодействие с отделами информации и общественных связей, в ходе которого последними распространяется информация о наиболее значимых находящихся в производстве и оконченных уголовных делах рассматриваемой категории.

Также с целью предупреждения совершения подобного рода преступлений сотрудниками распространяются специальные памятки, ведется разъяснительная работа в ходе осуществления выездов на места происшествий, информация профилактического характера доводится в ходе личных бесед с гражданами. Размещается социальная реклама соответствующего содержания и проводятся выступления сотрудников органов внутренних дел в местных средствах массовой информации, в том числе на телевидении.

В результате реагирования на представления в порядке части 2 статьи 158 УПК РФ в офисах и на интернет-сайтах операторов сотовой связи и кредитных организаций размещается информация, содержащая предупреждение для клиентов об участившихся случаях данного вида преступлений. В случаях выявления несоответствия персональных данных фактического пользователя предоставляемыми услугами связи и заявленных в абонентском договоре операторы сотовой связи прекращают оказание услуг. Кредитные организации рекомендуют установку лицензионного антивирусного программного обеспечения, уведомляют клиентов о последствиях вирусного заражения телефона на этапах оформления и выдачи банковских карт. Например, на официальном сайте ПАО «Сбербанк» размещена бесплатная антивирусная программа, запущена новая версия мобильного приложения со встроенным антивирусом, на все финансовые операции с использованием услуги «мобильный банк» установлены суточные лимиты.

Примечания

1. Обзор операций, совершенных без согласия клиентов финансовых организаций за 2019 год. URL: https://cbr.ru/Content/Document/File/103609/Review_of_transactions_2019 (дата обращения: 24.12.2020).

2. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ // Собрание законодательства РФ. 2001. № 52, ст. 4931.

3. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ // Собрание законодательства РФ. 2002. № 1, ст. 1.

4. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // Собрание законодательства РФ. 1996. № 25, ст. 2954.

5. О связи: федеральный закон от 7 июля 2003 г. № 126-ФЗ // Собрание законодательства РФ. 2003. № 28, ст. 2895.

6. Об оперативно-розыскной деятельности: федеральный закон от 12 августа 1995 г. № 144-ФЗ // Собрание законодательства РФ. 1995. № 33, ст. 3349.

7. Уголовно-исполнительный кодекс Российской Федерации от 8 января 1997 г. № 1-ФЗ // Собрание законодательства РФ. 1997. № 2, ст. 198.

8. Об утверждении Правил внутреннего распорядка исправительных учреждений: приказ Министерства юстиции РФ от 16 декабря 2016 г. № 295 // Официальный интернет-портал правовой информации, 27 декабря 2016 г. URL: www.pravo.gov.ru (дата обращения: 24.12.2020).

References

1. Review of operations performed without the consent of clients of financial organizations for 2019. URL: https://cbr.ru/Content/Document/File/103609/Review_of_transactions_2019 (accessed 24.12.2020). (In Russ.)

2. Criminal procedure code of the Russian Federation no. 174-FZ of December 18, 2001. *Collection of legislative acts of the RF*, 2001, no. 52, art. 4931. (In Russ.)

3. Code of the Russian Federation on administrative offenses of December 30, 2001 no. 195-FZ. *Collection of legislative acts of the RF*, 2002, no. 1, art. 1. (In Russ.)

4. Criminal code of the Russian Federation no. 63-FZ of June 13, 1996. *Collection of legislative acts of the RF*, 1996, no. 25, art. 2954. (In Russ.)

5. About the connection: federal law no. 126-FZ of July 7, 2003. *Collection of legislative acts of the RF*, 2003, no. 28, art. 2895. (In Russ.)

6. On operational search activity: federal law no. 144-FZ of August 12, 1995. *Collection of legislative acts of the RF*, 1995, no. 33, art. 3349. (In Russ.)

7. Criminal Executive code of the Russian Federation no. 1-FZ of January 8, 1997. *Collection of legislative acts of the RF*, 1997. no. 2, art. 198. (In Russ.)

8. On approval of the internal regulations of correctional institutions: order of the Ministry of justice of the Russian Federation no. 295 of December 16, 2016. Official Internet portal of legal information on December 27, 2016. URL: www.pravo.gov.ru (accessed 24.12.2020). (In Russ.)