Научная статья
УДК 343.985.7:343.7:[336.747.5:004.6]

Ольга Александровна Решняк
Волгоградская академия МВД России, Волгоград, Россия, volakdm@va-mvd.ru

МЕХАНИЗМ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЯ, СВЯЗАННОГО С НЕПРАВОМЕРНЫМ ОБОРОТОМ СРЕДСТВ ПЛАТЕЖЕЙ, В СТРУКТУРЕ ЧАСТНОЙ МЕТОДИКИ РАССЛЕДОВАНИЯ

Аннотация. Одним из основополагающих и значимых элементов в методике расследования преступлений является механизм его совершения, подробное и качественное изучение которого дает возможность следователю установить истину по делу. При расследовании преступлений, предусмотренных ст. 187 Уголовного кодекса Российской Федерации, у следователей возникают трудности, связанные с установлением всех обстоятельств совершенного преступления, а соответственно, и правильной квалификации содеянного, так как они не в полной мере обладают пониманием состава и содержания его механизма. Процесс познания механизма преступления в науке невозможен без практического подкрепления, в связи с чем автором в статье изучены позиции ученых в области криминалистики, а также проанализирована судебно-следственная практика по преступлениям, связанным с неправомерным оборотом средств платежей, на основе чего структурированы элементы механизма совершения преступления по указанному составу и раскрыто их содержание.

Ключевые слова: механизм преступления, электронные средства платежа, неправомерный оборот, методика расследования, криминалистическая характеристика, статья 187 УК РФ

Для цитирования: Решняк О. А. Механизм совершения преступления, связанного с неправомерным оборотом средств платежей, в структуре частной методики расследования // Общество, право, государственность: ретроспектива и перспектива. 2024. № 3 (19). С. 67–76.

Original article

Olga A. Reshnyak
Volgograd Academy of the Ministry of Internal Affairs of Russia, Volgograd, Russia, volakdm@va-mvd.ru

THE MECHANISM OF COMMITTING A CRIME, RELATED TO THE ILLEGAL TURNOVER OF PAYMENT FUNDS IN THE STRUCTURE OF A PRIVATE INVESTIGATION METHODOLOGY

Abstract. One of the fundamental and significant elements in the methodology of investigating crimes is the mechanism of its commission, a detailed and qualitative study of which allows the investigator to establish the truth in the case. When investigating crimes under Article 187 of the Criminal Code of the Russian Federation, investigators have difficulties in establishing all the circumstances of the crime committed, and, accordingly, the correct qualification of the deed, since they do not fully understand the composition and content of its mechanism. The process of cognition of the mechanism of crime in science is not possible without practical support, in connection with which, the author in the article studies the ideas of scientists in the field of criminology, as well as analyzes the judicial and investigative practice on crimes related to the illegal circulation of means of payments, on the basis of which the elements of the mechanism of committing a crime according to the specified composition are structured and their content is disclosed.

Keywords: crime mechanism, electronic means of payment, illegal turnover of means of payment, investigation methodology, forensic characteristics, Article 187 of the Criminal Code of the Russian Federation

For citation: Reshnyak O. A. The mechanism of committing a crime, related to the illegal turnover of payment fuds in the structure of a private investigation methodology // Society, law, statehood: retrospective and perspective. 2024. No. 3 (19). P. 67–76. (In Russ.)

Введение

Статья 187 Уголовного кодекса Российской Федерации (далее – УК РФ) подверглась значительной модернизации в связи с изданием Федерального закона от 8 июня 2015 г. № 153-ФЗ «О внесении изменений в статью 187 Уголовного кодекса Российской Федерации»[1], в соответствии с которым ее название «Изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов» изложено в новой редакции – «Неправомерный оборот средств платежей». У некоторых следователей возникло затруднение с определением предмета преступного посягательства и средств совершения преступления. Кроме того, возникли сложности с доказыванием действий виновного, так как не совсем понятен способ совершения преступления, а именно, что подразумевается под неправомерным оборотом и какие действия в него входят. В связи с чем возникла необходимость в изучении судебно-следственной практики и мнений исследователей в указанной области с целью структурирования элементов механизма совершения преступления, предусмотренного статьей 187 УК РФ, а также уточнения их содержания.

Методы

В исследовании использованы диалектический метод познания проблемных вопросов, обозначенных в начале работы; общенаучные методы дедукции, индукции и интерпретации, анализа и синтеза, аналогии и сравнения; частно-научные методы познания: системно-структурный, социологический, формально-логический, сравнительно-правовой, юридико-технический и другие. Данные методы позволят детально рассмотреть предмет настоящего исследования, входящий в сферу изучения криминалистики.

Результаты

Проанализировав научный мир в области криминалистики, обозначим выводы ученых о структуре механизма совершения преступления. И. А. Возгрин считает, что содержание механизма преступления включает в себя такие элементы, как личность преступника и потерпевшего [1, с. 43], В. Я. Колдин, Д. П. Поташник и др. предлагают: субъект, предмет, орудия (средства) и место (обстановка) [2, с. 333–334], В. В. Клочков и В. А. Образцов выделяют: лицо, совершившее преступление, поведение преступника, элементы окружающей среды [3, с. 47–48].

По преступлениям, предусмотренным статьей 187 УК РФ, на наш взгляд, механизм его совершения наиболее полно будет отражать следующая структура: предмет преступного посягательства, обстановка совершения преступления, способ совершения, личность преступника.

Предметом преступного посягательства, как правило, является то, на что направлен умысел преступника. Это может быть жизнь и здоровье гражданина, денежные средства, имущество, оружие, наркотические средства, авторские права и иные предметы и ценности, представляющие для него интерес.

На основе анализа мнений различных авторов по поводу предмета преступной деятельности, относящегося к составу преступления, квалифицированного по статье 187 УК РФ, можно увидеть неоднозначный подход к его пониманию, но большинство ученых к предмету данного преступления относят средства платежей. Например, Ю. С. Белик в качестве предмета преступного посягательства при совершении неправомерного оборота средств платежей указывает поддельные банковские карты, распоряжения о переводе денежных средств, поддельный

[1] О внесении изменений в статью 187 Уголовного кодекса Российской Федерации : федеральный закон Российской Федерации от 8 июня 2015 г. № 153-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

платежный ордер, электронные средства платежа и др. [4, с. 176]. Н. О. Карпов соглашается с мнением Ю. С. Белик, поясняя это тем, что указанные предметы относятся именно к диспозиции неправомерного оборота средств платежа, а сами денежные средства – к предмету другого состава преступления, то есть хищению [5, с. 21].

Согласно разъяснениям Верховного суда Российской Федерации, если человек изготовил, приобрел, хранил, перевозил поддельные средства платежа, предназначенные для приема, перевода, выдачи денежных средств, с целью их использования, то состав преступления считается оконченным по статье 187 УК РФ, а в случае использования данных средств для хищения денег деяния будут квалифицированы по смежным составам со статьей 158 УК РФ[1].

Таким образом, платежное средство является инструментом для доступа к денежным средствам, в том числе как для снятия наличных, так и осуществления безналичных операций, но только в том случае, если осуществляется их хищение.

Соответственно, под предметом преступления, связанного с неправомерным оборотом средства платежа, будут пониматься объекты материального мира, предназначенные для незаконных действий с денежными средствами.

К средствам платежей, используемых в неправомерном обороте, относят:

– поддельные платежные карты;

– распоряжения о переводе денежных средств, документов или средств оплаты;

– электронные средства и электронные носители информации, а также технические устройства, компьютерные программы, предназначенные для неправомерного осуществления приема, выдачи, перевода денежных средств.

Рассмотрим каждое средство более подробно в соответствии с его целевым назначением.

1. Поддельные платежные карты. Одно из самых распространенных по применению в обществе средств, с помощью которых производится безналичный расчет в различных сферах деятельности, например, при получении заработной платы, оплате жилищно-коммунальных и других услуг, оплате товаров в онлайн и оффлайн магазинах, межличностных переводах и т. д. Банком России от 24 декабря 2004 г. № 266-П утверждено Положение об эмиссии платежных карт и об операциях, совершаемых с их использованием[1], согласно п. 1.6 которого платежные карты подразделяют на три вида: расчетные (дебетовые), кредитные и предоплаченные карты [6]. Данные карты выпускаются банком-эмитентом, осуществляющим обслуживание расчетных счетов клиентов, и являются собственностью банка.

Расчетные карты – это дебетовая банковская карта, платежи по которой проводятся за счет собственных средств ее владельца, но дает возможность уходить в кредит (овердрафт) в пределах оговоренной суммы в случае нехватки денег на расчетном счету. От кредитной карты она отличается тем, что овердрафт составляет, как правило, небольшой лимит и погашается в течение месяца.

Кредитная карта – это инструмент проведения транзакций за счет средств, принадлежащих банку, в размере оговоренного в договоре лимита. Лимит может быть разным – в зависимости от финансовой состоятельности клиента. Потраченные денежные средства возвращаются держателем карты на счет в течение срока, указанного в договоре; на потраченную сумму могут назначаться проценты.

Предоплаченная карта является виртуальной картой или материальным пластиком, который не привязан к счету клиента и не содержит его персональных данных. На ней имеются денежные средства, заранее внесенные банком в определенном лимите. На данную карту можно вносить собствен-

[1] См.: Об эмиссии платежных карт и об операциях, совершаемых с их использованием : положение Банка России от 24 декабря 2004 г. № 266-П (в ред. от 28.09.2020) (зарегистрировано в Минюсте России 25.03.2005 № 431). Доступ из справ.-правовой системы «КонсультантПлюс».

ные средства, а также пользоваться средствами банка, которые в дальнейшем должны быть возвращены. Предназначена она для оплаты покупок в магазинах.

Указанные карты становятся предметом преступной направленности в том случае, если их изготовили, приобрели, хранили, перевозили с целью их использования.

2. Распоряжения о переводе денежных средств, документов и средств оплаты [7].

Согласно Положению Банка России от 29 июня 2021 г. № 762-П «О правилах осуществления перевода денежных средств»[1] банки России, кредитные организации осуществляют безналичные переводы денежных средств по счетам клиентов на основании распоряжений о переводе денежных средств, составляемых плательщиками, получателями средств, а также лицами, органами, имеющими право на основании федеральных законов предъявлять распоряжения к банковским счетам плательщиков, банками. К указанным распоряжениям относятся платежные поручения, аккредитив, инкассовые поручения, расчетные чеки по требованию получателя средств.

3. Электронные средства и электронные носители информации, предназначенные для неправомерного осуществления приема, выдачи, перевода денежных средств.

Понятия «электронное средство» и «электронный носитель информации» законодательно нигде не закреплены, в связи с чем у правоприменителей возникают значительные затруднения с их определением, а в научной среде зарождаются дискуссионные вопросы. Понятие «электронные средства» как отдельное определение не существует и в научном мире не обсуждается. В нашем понимании «электронное средство» и «электронный носитель информации» [8] идентичны по своему значению, и будем их рассматривать как одно целое. Электронные носители информации изучались В. Н. Григорьевым и О. А. Максимовым, которые выделяли определенные его особенности: материальность, предоставление информации в зашифрованном виде, отсутствие материальных следов при внесении изменений [6, с. 40].

А. Ю. Федюкина относит к электронным носителям информации сим-карты, флеш-карты, оптические диски, жесткие диски, магнитные ленты. Также в данной категории она указывает мобильные устройства, компьютеры, ноутбуки, планшеты, банковские платежные карты [7, с. 45]. С указанным мнением невозможно не согласиться, так как перечисленные предметы действительно могут содержать в себе электронную информацию различного рода, соответственно, будут являться электронными носителями информации. С помощью данных устройств могут осуществляться операции по приему, выдаче или переводу денежных средств.

4. Технические устройства, предназначенные для неправомерного осуществления приема, выдачи, перевода денежных средств. К указанным устройствам относятся: банкоматы и эквайринговые терминалы (POS-терминалы). Банкоматы – это устройства, предназначенные для внесения или получения наличных денежных средств по счету клиента, осуществления переводов между счетами и осуществления платежей. Данные устройства изготавливаются гражданскими организациями и сдаются в аренду банкам-эмитентам. Эквайринговые терминалы – это устройства, предназначенные для безналичной оплаты товаров и услуг в организациях, их предоставляющих.

5. Компьютерные программы, предназначенные для неправомерного осуществления приема, выдачи, перевода денежных средств. В отношении компьютерных программ стоит учитывать то обстоятельство, что их работа должна осуществляться исключительно на программном обеспечении, то есть в контексте преступления, предусмотренного ст. 187 УК РФ. Под предметом преступления в виде компьютерной программы

[1] О правилах осуществления перевода денежных средств : положение Банка России от 29 июня 2021 г. № 762-П (ред. от 03.08.2023). Доступ из справ.-правовой системы «КонсультантПлюс».

[11] подразумевается программное обеспечение, позволяющее совершать операции с денежными средствами в обход законных требований. Примером таких манипуляций можно назвать разработку вирусной программы для внедрения в платежную систему «Банк-клиент», позволяющую без ведома законного владельца счета списывать денежные средства гражданина или организации в пользу преступника. Такими программами могут быть, например, Trojan.PWS. SpySweep (SpyEye), Trojan.PWS. OSMP, Android.SpyEye, при этом и достоверность назначения данных программ должна быть установлена [12, с. 197].

На основе изученной судебно-следственной практики можно сделать вывод, что из всех перечисленных предметов преступного посягательства при совершении преступления, предусмотренного статьей 187 УК РФ, чаще всего преступниками используются распоряжения о переводе денежных средств, документы или средства оплаты. Такого же мнения придерживается В. Ф. Васюков [13], полагая, что иные средства преступниками не используются ввиду сложности их изготовления и высоких материальных затрат. С указанным мнением следует согласиться, так как, действительно, для изготовления белого пластика требуется дорогостоящее оборудование, которое необходимо сначала установить на банкоматы для получения и сбора информации о реквизитах карты его законного держателя, затем переписать на белый пластик декодированные данные. Для разработки вирусных программ также требуются специальное программное обеспечение, дорогостоящее оборудование и наличие специальных знаний в указанной области, которые имеют особую специфику и требуют определенных навыков.

К способам совершения указанных преступлений мы будем относить: изготовление, приобретение, хранение, перевозку поддельного средства платежа, предназначенного для приема, перевода, выдачи денежных средств с целью их использования или сбыта, а равно сбыт.

Изготовление поддельной платежной карты. Для изготовления поддельной платежной карты преступнику необходимо подготовиться: получить информацию о держателе карты и все ее данные. Для этого преступник приобретает считывающие устройства, накладки на клавиатуру, накладные камеры видеонаблюдения, RFID-считыватель (устройство, позволяющее улавливать радиосигналы, сохранять их и передавать), которые в дальнейшем устанавливает на банкоматы, и при помещении пластиковой банковской карты в карт-ридер считывает информацию о номере счета, номере карты, CVV-код, ФИО держателя карты, дату действия и др. Также приобретается оборудование для изготовления карт: эмбоссеры (устройства, предназначенные для выдавливания идентификационной информации на пластиковой карте клиента: номера карты и срока действия, имени и фамилии держателя), энкодеры (кодирующее устройство, предназначенное для преобразования информации на магнитную полосу карты или RFID-метку), токен-генераторы (программы для создания одноразовых паролей для пластиковых карт). RFID-считыватель по своим функциям похож на бесконтактный POS-терминал, способный считывать данные без непосредственного взаимодействия с картой. В своих работах К. В. Гурьянов описывает принципы работы данного устройства: «RFID-метка – это микрочип, активирующийся при поступлении радиосигнала извне. При контакте RFID-метки со считывателем она получает необходимое для работы питание: запускаются операционная система и установленное приложение, которое передает информацию обратно в зашифрованном виде на считыватель. Эта технология беспроводной высокочастотной связи малого радиуса действия является расширением стандарта бесконтактных карт ISO 14443 и объединяет в одно устройство смарт-карту и считыватель» [14]. Чтобы получить зашифрованную информацию на RFID-метке пластиковой карты ее законного держателя, злоумышленнику достаточно приблизить-

ся считывающим устройством к карте на расстояние NFC (взаимодействие близкого поля) – это не более 8,5 см, тогда активируется RFID-метка. После получения сигнала считыватель записывает все данные карты держателя, которые в дальнейшем передает на энкодер для создания белого пластика. Установка считывающего оборудования на банкоматы и его последующее снятие осуществляется, как правило, в ночное время, когда на улицах малолюдно. Считывание информации RFID-считывателем осуществляются в местах массового скопления: на рынках, в общественном транспорте, на вокзалах в очередях и др. Время также может быть утреннее или вечернее, час пик, выходные дни.

Место и время изготовления белого пластика преступник выбирает наиболее удобное для себя, как правило, это арендованное помещение. Время может быть любое, но так как данные преступления, как правило, обычно становятся основным источником дохода преступника, то процесс изготовления поддельных платежных карт может происходить в дневное время.

Изготовление распоряжений о переводе денежных средств также может происходить в дневное, рабочее время; как правило, в этом процессе участвуют работники банковской сферы; местом изготовления являются банки.

Изготовление специальных вирусных программ для внедрения в платежные системы «Банк-клиент» с целью дальнейшего управления финансовыми операциями по счетам организации или клиентов осуществляется в местах работы или дома у лиц, обладающих специальными знаниями в области компьютерных программ. Время как дневное, так и ночное.

Сбыт и приобретение изготовленных платежных банковских карт или электронных носителей информации с вирусными программами или похищенной конфиденциальной информацией о клиентах или организациях за определенную денежную сумму с целью дальнейшего использования в рамках неправомерного оборота средств платежей осуществляются в вечернее или ночное время, в малолюдных местах. Могут происходить путем оставления «закладок» в тайниках, местоположение которых в дальнейшем сообщается покупателю посредством месенджеров, а денежные средства за изготовленные поддельные платежные средства перечисляются на электронные кошельки по номерам телефонов, оформленным на подставных лиц. В таком случае личного контакта сбытчика и приобретателя не происходит, и информации о преступниках не имеется. Как правило, переписка происходит в мессенджере «Телеграм» без идентификационных данных о номерах телефонов покупателя и продавца.

Хранение изготовленных или приобретенных поддельных платежных банковских карт или электронных носителей информации с вирусными программами или похищенной конфиденциальной информацией о клиентах или организациях осуществляется по месту жительства преступника.

Ярким примером преступлений, связанных с неправомерным оборотом средств платежа стал случай, произошедший в г. Тольятти, где к гр. А. обратилось неустановленное лицо, которое предложило ему за денежное вознаграждение лично обратиться в отделение ПАО «Сбербанк» для открытия расчетного счета ООО «ТЕХНОРОС», где гр. А. будет являться подставным лицом и иметь возможность дистанционного банковского обслуживания для осуществления в дальнейшем неправомерного оборота, то есть приема, выдачи и перевода денежных средств, на что гр. А. согласился. Таким образом, у гр. А. возник преступный умысел, направленный на приобретение, хранение в целях сбыта электронных средств, предназначенных для неправомерного осуществления приема, выдачи и перевода денежных средств. В Единый государственный реестр юридических лиц неустановленным лицом внесены недостоверные сведения о государственной регистрации ООО «ТЕХНОРОС» о том, что гр. А. является единственным учредителем

и директором, то есть подставным лицом. После чего гр. А. получил от неустановленного лица правоустанавливающие документы ООО «ТЕХНОРОС», печать ООО «ТЕХНОРОС», а также мобильный телефон с сим-картой, абонентский номер которой используется неустановленным лицом, и кодовое слово для получения в дальнейшем с его помощью одноразовых SMS-паролей, предназначенных для дистанционного банковского обслуживания открытого расчетного счета юридического лица. Далее гр. А. лично обратился в отделение ПАО «Сбербанк России» для открытия расчетного счета ООО «ТЕХНОРОС», где лично передал сотруднику банка копии документов, в присутствии сотрудника банка заполнил и подписал заявление о присоединении клиента ООО «ТЕХНОРОС», скрепив его оттиском печати организации. Между ООО «ТЕХНОРОС» в лице директора гр. А. и ПАО «Сбербанк России» заключен договор о предоставлении услуг с использованием системы дистанционного банковского обслуживания и открыт расчетный счет. В соответствии с данным договором клиент от имени компании посредством использования информационно-телекоммуникационной сети Интернет может подавать платежные документы в банк на проведение финансово-хозяйственных операций в электронном виде, а банк обязуется их принимать и проводить по ним транзакции. Для указанных целей банком гр. А. была выдана банковская карта с логином и паролем, которые с целью сбыта он стал хранить при себе. Позже банковскую карту с пин-кодом, с логином и паролем от личного кабинета «Сбербанк-онлайн», мобильный телефон с сим-картой, предназначенные для неправомерного осуществления приема, выдачи и перевода денежных средств по расчетному счету, открытому в ПАО «Сбербанк России», гр. А. передал неустановленному лицу, т. е. осуществил сбыт электронных средств, предназначенных для неправомерного осуществления приема, выдачи и перевода денежных средств по данному расчетному счету.

Перевозка изготовленных поддельных платежных банковских карт или электронных носителей информации с вирусными программами или похищенной конфиденциальной информацией о клиентах осуществляется любым видом транспорта, как правило, в замаскированном виде. Так как данные объекты имеют малый размер, то их очень легко спрятать и при себе, и в транспортном средстве.

Важным аспектом является личность преступника. В зависимости от способа совершения рассматриваемого преступления преступников можно подразделить на несколько групп [15, с. 65–66]:

1. Разработчики компьютерных программ, предназначенных для неправомерного осуществления приема, выдачи, перевода денежных средств. Как правило, к данным лицам относятся молодые люди в возрасте 16–35 лет, обладающие знаниями в области компьютерных технологий, имеющие специальное образование в данной сфере, ведущие замкнутый образ жизни.

2. Заказчик – лицо, осуществляющее заказ на изготовление поддельной платежной карты, распоряжения, компьютерной программы или электронного носителя информации для неправомерного осуществления приема, выдачи, перевода денежных средств. Данные лица более зрелого возраста – 30–55 лет, не имеющие специальных знаний в области компьютерных технологий, но имеющие высшее образование, пренебрегающие нормами закона и не желающие зарабатывать честным путем.

3. Исполнители – лица, обладающие знаниями в области компьютерных технологий, имеющие техническое образование. По возрасту – 25–35 лет. Активные, хитрые, официально не имеющие постоянного источника дохода, желающие заработать легких денег, ведущие антиобщественный образ жизни, возможно, ранее судимые.

Заключение

На основании изученной судебно-следственной практики и мнений ученых-криминалистов нами выявлен ряд проблем, возникающих у следователей при расследовании

преступлений, связанных с неправомерным оборотом средств платежей, в частности, с установлением элементов механизма совершения неправомерного оборота средств платежей и дальнейшей квалификацией содеянного. С целью решения указанных проблем мы структурировали указанные элементы, которые определены как предмет преступного посягательства, способ совершения преступления, личность преступника. Далее уточнено содержание каждого элемента.

К предмету преступной деятельности неправомерного оборота средств платежей относятся:

1. Поддельные платежные карты, подразделяющиеся на расчетные, кредитные, предоплаченные.

2. Распоряжения о переводе денежных средств, документов и средств оплаты, к которым относятся платежные поручения, аккредитив, инкассовые поручения, расчетные чеки по требованию получателя средств.

3. Электронные средства и электронные носители информации, предназначенные для неправомерного осуществления приема, выдачи, перевода денежных средств: сим-карты, флеш-карты, оптические диски, жесткие диски, магнитные ленты, мобильные устройства, компьютеры, ноутбуки, планшеты, банковские платежные карты.

4. Технические устройства, предназначенные для неправомерного осуществления приема, выдачи, перевода денежных средств: банкоматы и эквайринговые терминалы (POS-терминалы).

5. Компьютерные программы, предназначенные для неправомерного осуществления приема, выдачи, перевода денежных средств: Trojan.PWS.SpySweep (SpyEye), Trojan.PWS. OSMP, Android.SpyEye.

К способам совершения указанных преступлений относятся изготовление, приобретение, хранение, перевозка поддельных средств платежа, предназначенного для приема, перевода, выдачи денежных средств, с целью их использования или сбыта, а равно сбыт.

Личность преступника можно разделить на три группы в зависимости от способа совершения преступления: разработчики, заказчики и исполнители.

Благодаря четкому пониманию структурных элементов механизма совершения преступления, связанного с неправомерным оборотом средств платежей, следователи смогут быстро и правильно устанавливать обстоятельства, влияющие на принятие решения по квалификации содеянного, и планировать дальнейшее расследование.

СПИСОК ИСТОЧНИКОВ

1. Возгрин И. А. Принципы методики расследования отдельных видов преступлений. Ленинград : ВПУ МВД СССР, 1977. 80 с.

2. Криминалистика социалистических стран / В. Я. Колдин, Д. П. Поташник, Э. Штельцер и др. ; под ред. В. Я. Колдина. М. : Юридическая литература, 1986. 509 с.

3. Клочков В. В., Образцов В. А. Преступление как объект криминалистического познания // Вопросы борьбы с преступностью. 1985. № 42. С. 44–54.

4. Белик Ю. С. К вопросу о предмете неправомерного оборота средств платежей (ст. 187 УК РФ) // Вестник Московского университета МВД России. 2016. № 4. С. 174–179.

5. Карпов Н. О. Предмет неправомерного оборота средств платежей (правовой и криминалистический аспекты) // Вестник Санкт-Петербургского университета МВД России. 2017. № 3 (75). С. 119–122.

6. Мошенничество в платежной сфере / Л. Лямин и др. ; Центр исслед. платежных систем и расчетов. М. : Интеллектуальная лит., 2016. 343 с.

7. Нудель С. Л., Печегин Д. А. Вопросы квалификации неправомерного оборота средств платежей (по признаку предмета) // Уголовное право. 2020. № 3. С. 27–38.

8. Хакимова З. И. Уголовно-правовые меры противодействия преступлениям, совершаемым в финансовой сфере с использованием информационно-телекоммуникационных технологий : дис. … канд. юрид. наук. Краснодар, 2016. 222 с.

9. Григорьев В. Н., Максимов О. А. Понятие электронных носителей информации в уголовном судопроизводстве // Вестник Уфимского юридического института МВД России. 2019. № 2. С. 33–44.

10. Федюкина А. Ю. Электронный носитель информации как доказательство по уголовным делам // Отечественная юриспруденция. 2016. № 12. С. 44–46.

11. Соловьева Е. А. Преступления, совершаемые в платежных системах : дис. … канд. юрид. наук. Саратов, 2019. 254 с.

12. Аксенова Л. Ю. Установление данных о предмете и способе преступления по делам о неправомерном обороте средств платежей // Вестник Омской юридической академии. 2018. Том 15. № 2. С. 192–199.

13. Васюков В. Ф., Шалыгина А. В. Некоторые элементы криминалистической характеристики преступлений, связанных с неправомерным оборотом средств платежа // Уголовно-процессуальные и криминалистические проблемы борьбы с преступностью : сборник материалов. Орловский юридический институт МВД России имени В. В. Лукьянова. 2018. С. 20–26.

14. Гурьянов К. В. Современные риски бесконтактных платежей с использованием RFID-технологий // Базис. 2019. № 1 (5). С. 50–63.

15. Олиндер Н. В. Преступления, совершенные с использованием электронных платежных средств и систем: криминалистический аспект : монография. М. : Юстиция, 2016. 120 с.

REFERENCES

1. Vozgrin I. A. Principles of the methodology of investigation of certain types of crimes. Leningrad : Higher political school of the Ministry of Internal Affairs of the USSR, 1977. 80 p. (In Russ.)

2. Criminalistics of socialist countries / V. Ya. Koldin, D. P. Potashnik, E. Stelzer, et al. edited by V. Ya. Koldin. M. : Legal literature, 1986. 509 p. (In Russ.)

3. Klochkov V. V., Obraztsov V. A. Crime as an object of forensic knowledge // Issues of combating crime. 1985. No. 42. P. 44–54. (In Russ.)

4. Belik Yu. S. On the issue of the subject of illegal turnover of means of payment (Article 187 of the Criminal Code of the Russian Federation) // Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia. 2016. No. 4. P. 174–179. (In Russ.)

5. Karpov N. O. The subject of illegal turnover of means of payment (legal and criminalistic aspects) // Bulletin of the St. Petersburg University of the Ministry of Internal Affairs of Russia. 2017. No. 3 (75). P. 119–122. (In Russ.)

6. Fraud in the payment sphere / L. Lyamin et al. ; Center for Research. payment systems and settlements. M. : Intellectual lit., 2016. 343 p. (In Russ.)

7. Nudel S. L., Pechegin D. A. Issues of qualification of illegal turnover of means of payment (based on the subject) // Criminal law. 2020. No. 3. P. 27–38. (In Russ.)

8. Khakimova Z. I. Criminal law measures to counteract crimes committed in the financial sphere using information and telecommunication technologies : dis. ... Cand. of Law. Krasnodar, 2016. 222 p. (In Russ.)

9. Grigoriev V. N., Maksimov O. A. The concept of electronic media in criminal proceedings // Bulletin of the Ufa Law Institute of the Ministry of Internal Affairs of Russia. 2019. No. 2. P. 33–44. (In Russ.)

10. Fedyukina A. Yu. Electronic media as evidence in criminal cases // Domestic jurisprudence. 2016. No. 12. P. 44–46. (In Russ.)

11. Solovyova E. A. Crimes committed in payment systems : dis. ... Cand. of Law. Saratov, 2019. 254 p. (In Russ.)

12. Aksenova L. Yu. Establishing data on the subject and method of the crime in cases of illegal turnover of payment funds // Bulletin of the Omsk Law Academy. 2018. Volume 15. No. 2. P. 192–199. (In Russ.)

13. Vasyukov V. F., Shalygina A.V. Some elements of the criminalistic characteristics of crimes related to the illegal circulation of means of payment // Criminal procedural and criminalistic problems of combating crime : collection of materials. Oryol Law Institute of the Ministry of Internal Affairs of the Russian Federation named after V. V. Lukyanov. 2018. P. 20–26. (In Russ.)

14. Guryanov K. V. Modern risks of contactless payments using RFID technologies // Basis. 2019. No. 1 (5). P. 50–63. (In Russ.)

15. Olinder N. V. Crimes committed using electronic means of payment and systems: criminalistic aspect : monograph. M. : Justice, 2016. 120 p. (In Russ.)

Информация об авторе:
О. А. Решняк – кандидат юридических наук, доцент.

Information about the author:
O. A. Reshnyak – Candidate of Law, Associate Professor.

Статья поступила в редакцию 04.04.2024; одобрена после рецензирования 02.08.2024; принята к публикации 27.09.2024.

The article was submitted 04.04.2024; approved after reviewing 02.08.2024; accepted for publication 27.09.2024.