

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ
ВОЛГОГРАДСКАЯ АКАДЕМИЯ

О. А. Решняк, А. А. Лихолетов, Д. Н. Евлушина

**ОСОБЕННОСТИ КВАЛИФИКАЦИИ
И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ,
ПРЕДУСМОТРЕННЫХ СТАТЬЕЙ 187
УГОЛОВНОГО КОДЕКСА
РОССИЙСКОЙ ФЕДЕРАЦИИ**

Учебное пособие

Волгоград
ВА МВД России
2024

УДК 345.985.7:343.7(075.8)
ББК 67.523.12я73
Р 47

Одобрено
редакционно-издательским советом
Волгоградской академии МВД России

Решняк, О. А.

Р 47 Особенности квалификации и расследования преступлений, предусмотренных статьями 187 Уголовного кодекса Российской Федерации : учебное пособие / О. А. Решняк, А. А. Лихолетов, Д. Н. Евлушина. – Волгоград : ВА МВД России, 2024. – 60 с.

ISBN 978-5-7899-1514-1

Пособие посвящено особенностям квалификации преступлений, связанных с неправомерным оборотом средств платежей, а также совершенствованию методики расследования указанных преступлений. В работе проанализированы нормы уголовного законодательства и смежных отраслей права, следственно-судебная практика Российской Федерации, необходимые для квалификации преступлений, связанных с незаконным оборотом средств платежей. Раскрыты особенности возбуждения уголовных дел по фактам преступлений, предусмотренных статьями 187 УК РФ, а также способы совершения указанных преступлений и тактика производства отдельных следственных действий.

Издание ориентировано на курсантов и слушателей образовательных организаций системы МВД России, сотрудников органов внутренних дел Российской Федерации.

УДК 345.985.7:343.7(075.8)
ББК 67.523.12я73

Авторы: О. А. Решняк – § 3–5, введение, заключение; А. А. Лихолетов – § 1, 2; Д. Н. Евлушина – § 6.

Рецензенты: доцент кафедры криминологии Московского университета МВД России им. В. Я. Кикотя кандидат юридических наук, доцент *Е. Е. Колбасина*; начальник ОЗО ГСУ ГУ МВД России по Волгоградской области *Р. В. Феофанов*.

ISBN 978-5-7899-1514-1

© Решняк О. А., § 3–5,
введение, заключение, 2024
© Лихолетов А. А., § 1, 2, 2024
© Евлушина Д. Н., § 6, 2024
© Волгоградская академия МВД России, 2024

ОГЛАВЛЕНИЕ

Введение.....	4
§ 1. Уголовно-правовая характеристика преступлений, связанных с неправомерным оборотом средств платежей.....	6
§ 2. Особенности квалификации преступлений, связанных с неправомерным оборотом средств платежей.....	10
§ 3. Особенности возбуждения уголовных дел по фактам совершения преступлений, связанных с неправомерным оборотом средств платежей.....	16
§ 4. Способы совершения преступлений, связанных с неправомерным оборотом средств платежей.....	25
§ 5. Тактика производства отдельных следственных действий при расследовании преступлений, связанных с неправомерным оборотом средств платежей.....	37
§ 6. Особенности использования специальных знаний при расследовании преступлений, связанных с неправомерным оборотом средств платежей.....	48
Заключение.....	56
Список рекомендуемой литературы	58

ВВЕДЕНИЕ

Переход на безналичный оборот денежных средств и новые формы расчетов, представленные в цифровом формате, освобождает граждан от ношения при себе больших сумм денег, что удобно при необходимости совершения любых финансовых операций и сокращает их время. Тем не менее такие формы расчетов не обеспечивают безопасность от преступных посягательств, так как злоумышленники подстраиваются под современные технологии и адаптируются к их изменениям. Одним из видов современных преступлений, адаптированных под развивающиеся технологии, является неправомерный оборот средств платежей, к которым относятся кредитные либо расчетные карты, распоряжения о переводе денежных средств, электронные носители информации. В уголовном законодательстве данные преступления отнесены к ст. 187 Уголовного кодекса Российской Федерации.

Негативную динамику по указанным преступлениям можно проследить, анализируя официальные статистические данные МВД России, представленные за пять лет. Так, в 2018 г. по ст. 187 УК РФ привлечены к уголовной ответственности 56 человек (49 получили условное осуждение), в 2019 г. наказано 66 человек (условное осуждение в отношении 48), в 2020 г. – 129 (в отношении 108 условное осуждение), в 2021 г. – 366 (в отношении 301 условное осуждение)¹. За первое полугодие 2022 г. по данной категории преступлений было осуждено 320 человек. Указанные сведения свидетельствуют об экстремально низком уровне раскрываемости².

Следственные органы сталкиваются с проблемами расследования данных преступлений, так как добыть прямые доказательства причастности конкретного лица к преступной деятельности, осуществляемой с использованием информационно-телекоммуникационных технологий, очень сложно, в основном все доказательства будут нести косвенный характер. Кроме этого, специфика механизма совершения преступления накладывает определенные сложности на получение

¹ См.: Судебная статистика РФ. Уголовное судопроизводство: данные о назначенном наказании по статьям УК РФ. URL: <https://stat.xn> (дата обращения: 05.05.2023).

² Последняя статистика по данным преступлениям зарегистрирована за первое полугодие 2022 г.

следов, так как они будут отображаться в основном в цифровой форме. В связи с чем следователи должны четко понимать алгоритм действий по проведению следственных и иных мероприятий, направленных на установление и фиксацию доказательств преступной деятельности конкретного лица и его причастности к совершенному преступлению.

Вышеизложенное позволяет говорить об актуальности рекомендаций по квалификации и расследованию преступлений, предусмотренных ст. 187 УК РФ.

§ 1. Уголовно-правовая характеристика преступлений, связанных с неправомерным оборотом средств платежей

Объектом преступления следует признать общественные отношения, обеспечивающие установленный законом порядок оборота средств платежей.

В отличие от охраняемых ст. 187 УК РФ общественных отношений, не имеющих материализованного воплощения, у предмета уголовно наказуемого деяния всегда есть определенные физические параметры, т. е. предметом преступления следует считать «ту часть объекта посягательства, которая имеет материальное выражение, или информацию, воздействуя на которую, субъект причиняет вред общественным отношениям, составляющим данный объект»¹.

Предмет преступления – поддельные платежные карты, распоряжения о переводе денежных средств, документы или средства оплаты, а также электронные средства, электронные носители информации, технические устройства, компьютерные программы.

Платежная (пластиковая, банковская) карта – средство для составления расчетных и иных документов, подлежащих оплате за счет его собственника. В России предусмотрен оборот расчетных (дебетовых)², кредитных³ и предоплаченных⁴ платежных карт¹.

¹ Уголовное право. Общая часть: учебник / под ред. В. В. Намнясовой. Волгоград: ВА МВД России, 2021. С. 83.

² Электронное средство платежа, используемое для совершения операций ее держателем в пределах расходного лимита – суммы денежных средств клиента, находящихся на его банковском счете, и (или) кредита, предоставляемого кредитной организацией – эмитентом клиенту при недостаточности или отсутствии на банковском счете денежных средств (овердрафт).

³ Электронное средство платежа, используемое для совершения ее держателем операций за счет денежных средств, предоставленных кредитной организацией – эмитентом клиенту в пределах расходного лимита в соответствии с условиями кредитного договора (см.: Положение об эмиссии платежных карт и об операциях, совершаемых с их использованием, утв. Банком России 24.12.2004 № 266-П. URL: <https://www.consultant.ru> (дата обращения: 12.10.2023)).

⁴ Электронное средство платежа, используемое для осуществления перевода электронных денежных средств, возврата остатка электронных денежных средств в пределах суммы предварительно предоставленных держателем денежных средств кредитной организации – эмитенту в соответствии с требованиями Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе».

В качестве *распоряжений о переводе денежных средств* могут выступать различного рода документы, в том числе платежные или инкассовые поручения, платежные требования, банковские ордера и т. д.²

К *документам оплаты* относятся, например, инкассовые чеки. В регулятивном законодательстве³ платежные поручения, инкассовые поручения, платежные требования, платежные ордера, банковские ордера определены единой дефиницией – расчетные (платежные) документы, что приводит к ряду проблем, связанных с разграничением предмета преступления: распоряжения и платежного документа⁴.

К *средствам оплаты* относятся аккредитивы и электронные средства платежа⁵.

Перечисленные выше предметы преступления должны быть поддельными. Применительно к поддельным официальным документам высшая судебная инстанция дала разъяснения, что таковыми следует считать в том числе подлинные документы, в которых произведено незаконное изменение отдельных их частей путем подчистки, дописки, замены элементов и др., искажающее их действительное содержание, а также вновь изготовленные, в том числе с использованием подлинных бланка, печати, штампа, официальные документы,

¹ См.: Об эмиссии платежных карт и об операциях, совершаемых с их использованием: положение Банка России от 24.12.2004 № 266-П. URL: <https://www.consultant.ru> (дата обращения: 12.10.2023).

² См.: Комментарий к Уголовному кодексу Российской Федерации / Университет прокуратуры Российской Федерации; под общ. ред. О. С. Капинус; науч. ред. В. В. Меркурьев. М.: Проспект, 2018. С. 704.

³ См.: Об эмиссии платежных карт и об операциях, совершаемых с их использованием: положение Банка России от 24.12.2004 № 266-П. URL: <https://www.consultant.ru> (дата обращения: 12.10.2023).

⁴ См.: Уголовное право. Особенная часть: учебник / под общ. ред. д-ра юрид. наук, проф. С. А. Денисова, д-ра юрид. наук, проф. Л. В. Готчиной, д-ра юрид. наук, доц. А. Г. Хлебушкина. СПб.: Санкт-Петербургский университет МВД России, 2021. С. 399.

⁵ Электронные средства платежа – средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств (Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платежной системе»).

но содержащие заведомо ложные сведения¹. Таким образом, Пленум Верховного Суда России указывает на два вида подлога – материальный и интеллектуальный.

Представляется, что подобный подход вполне возможно экстраполировать и на платежные карты, которые могут быть изготовлены в установленном порядке, но с одновременным внесением заведомо ложных сведений, имеющих юридическое значение (например, относительно данных держателя карты), либо путем создания полностью подложного средства платежа неуполномоченными на то лицами (например, создание карт-клонов). При этом предмет подделки должен иметь существенное сходство с подлинными средствами платежей по форме и физическим характеристикам, поскольку явное несоответствие делает невозможным его участие в обороте и исключает основания для квалификации содеянного по ст. 187 УК РФ².

Дефиниции «*электронное средство*», равно как и «электронное средство... предназначенное для осуществления приема, выдачи, перевода денежных средств» на нормативном уровне не выработано. В данном случае комплексный анализ положений позитивного законодательства³ и формулировки диспозиции ст. 159³ УК РФ позволяет сделать вывод, что в качестве «электронного средства» как предмета преступления, предусмотренного ст. 187 УК РФ, следует рассматривать именно *электронное средство платежа*, под которым понимается средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств⁴.

¹ См.: О некоторых вопросах судебной практики по делам о преступлениях, предусмотренных статьями 324–327.1 Уголовного кодекса Российской Федерации: постановление Пленума Верховного Суда РФ от 17.12.2020 № 43. URL: <https://www.consultant.ru> (дата обращения: 12.10.2023).

² См.: Нудель С. Л., Печегин Д. А. Вопросы квалификации неправомерного оборота средств платежей (по признаку предмета) // Уголовное право. 2020. № 3. С. 35.

³ См.: О национальной платежной системе: федер. закон от 27.06.2011 № 161-ФЗ. URL: <https://www.consultant.ru> (дата обращения: 12.10.2023).

⁴ Там же.

Электронный носитель информации – материальные носители, используемые для оборота информации с помощью ЭВМ¹. К таковым относятся USB-накопители², часто используемые для аутентификации пользователя или подтверждения проведенных транзакций в системе онлайн-платежей³, а также различные внешние жесткие диски, карты памяти и др.

К *техническим устройствам* следует относить приспособления, предназначенные для осуществления незаконных операций с денежными средствами. Таковыми являются, например, скимминговое оборудование, поддельные POS-терминалы или банкоматы и др.

Программа для ЭВМ – описанная на языке программирования совокупность данных и команд, которые должна выполнить ЭВМ с целью решения конкретной задачи⁴. К таковым относятся «мобильный банкинг», «интернет-банкинг»⁵.

Необходимо отметить, что последние три из перечисленных предметов должны быть предназначены для неправомерного приема, выдачи, перевода денежных средств.

Объективная сторона представлена рядом альтернативных действий.

Под *изготовлением* необходимо понимать полное создание какого-либо предмета преступления, либо частичную подделку средств платежей, находящихся в легальном обороте.

Приобретение – получение предмета деяния любым способом (покупка, получение в дар, обмен и т. д.).

¹ См.: О введении в действие межгосударственных стандартов: приказ Росстандарта от 22.11.2013 № 1628-ст. URL: <https://www.consultant.ru> (дата обращения: 12.10.2023).

² Смарт-карты eToken, носители, содержащие ключ электронной подписи или ключ проверки электронной подписи, и т. п.

³ См.: Уголовно-правовая охрана финансово-бюджетной сферы: науч.-практ. пособие / В. Ю. Артемов, Н. А. Голованова, Е. В. Горенская [и др.]; отв. ред. И. И. Кучеров, О. А. Зайцев, С. Л. Нудель. М.: ИЗиСП: КОНТРАКТ, 2021. URL: <https://www.consultant.ru> (дата обращения: 12.10.2023).

⁴ См.: Воройский Ф. С. Информатика. Энциклопедический систематизированный словарь-справочник: введение в современные информационные и телекоммуникационные технологии в терминах и фактах. М.: Физматлит, 2006. С. 327.

⁵ См.: О рекомендациях по организации управления рисками, возникающими при осуществлении кредитными организациями операций с применением систем интернет-банкинга: письмо Банка России от 31.03.2008 № 36-Т. URL: <https://www.consultant.ru> (дата обращения: 12.10.2023).

Хранением следует признавать нахождение предмета преступления в каком-либо месте либо при лице, в том числе в условиях, обеспечивающих сохранность таковых.

Транспортировка – перемещение предмета деяния из одного места в другое с использованием транспорта.

Сбытом необходимо считать любые действия по безвозвратному отчуждению и передаче предмета преступления (продажа, дарение, обмен и т. д.) другому лицу.

Субъект преступления – физическое вменяемое лицо, достигшее возраста 16 лет.

Субъективная сторона характеризуется прямым умыслом, а также целью – использование или сбыт.

Виновное лицо осознает общественную опасность своих действий и желает их совершить. При этом Конституционный Суд России обратил внимание на то, что ответственность по ст. 187 УК РФ наступает «лишь при условии доказанности умысла лица на совершение этих действий, в том числе включающего осознание им предназначения изготавливаемых или сбываемых документов как платежных, а также возможности их использования именно в таком качестве»¹.

Таким образом, если лицо изготовило предмет деяния, например с целью демонстрации своих умений без намерения введения средств платежей в оборот, то рассматриваемый состав преступления в его действиях отсутствует.

§ 2. Особенности квалификации преступлений, связанных с неправомерным оборотом средств платежей

Отсутствие разъяснений высшей судебной инстанции России относительно отдельных вопросов квалификации деяний, предусмотренных ст. 187 УК РФ, приводит к возникновению ряда проблем в правоприменительной практике, которые необходимо решать с учетом сложившихся в теории правил.

¹ См.: Об отказе в принятии к рассмотрению жалобы гражданина Тырлышкина Вячеслава Геннадьевича на нарушение его конституционных прав частью первой статьи 187 Уголовного кодекса Российской Федерации: определение Конституционного Суда РФ от 31.03.2022 № 761-О. URL: <https://www.consultant.ru> (дата обращения: 12.10.2023).

Преступления, предусмотренные ст. 159³, п. «г» ч. 3 ст. 158, ст. 159⁶ и ст. 187 УК РФ, являются смежными. Отличие названных деяний, наряду с объектом, заключается в их предмете, который прямо указан в диспозициях перечисленных норм.

Согласно позиции Верховного Суда России если лицо изготавливает (приобретает, хранит, транспортирует) поддельные предметы, перечисленные в ст. 187 УК РФ, в целях¹ их использования им же для совершения хищения, которое по объективным обстоятельствам не было доведено до конца, то содеянное, согласно положениям ч. 2 ст. 30 УК РФ, необходимо квалифицировать как совокупность приготовления к хищению (с учетом способа) и оконченного неправомерного оборота средств платежей².

Изложенное позволяет резюмировать, что использование виновным поддельного средства платежа (например, распоряжения о переводе денежных средств) при совершении корыстного противоправного безвозмездного изъятия и (или) обращения чужого имущества в пользу виновного или других лиц является основанием для квалификации содеянного по совокупности как оконченного хищения (в зависимости от способа) по ст. 187 УК РФ.

Л., занимая должность главного бухгалтера у индивидуального предпринимателя П., с помощью программы «1С: Бухгалтерия» изготовила платежные поручения, загрузила их в программу «Банк-Клиент», подписала вверенной ей электронной подписью ИП и направила на расчетно-кассовое обслуживание. В результате чего денежные средства в сумме 50 000 рублей с расчетного счета, принадлежащего П., были похищены и зачислены на банковский счет, принадлежащий виновной. Л. осуждена по ч. 3 ст. 159 и ч. 1 ст. 187 УК РФ³.

Следует согласиться с мнением Л. В. Боровых, Е. А. Соловьевой указывающих, что в рассматриваемой ситуации ст. 187 УК РФ

¹ См.: Хисамова З. И. Уголовно-правовые меры противодействия преступлениям, совершаемым в финансовой сфере с использованием информационно-телекоммуникационных технологий: дис. ... канд. юрид. наук. Краснодар, 2016. С. 45.

² См.: О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного Суда РФ от 30.11.2017 № 48. URL: <https://www.consultant.ru> (дата обращения: 12.10.2023).

³ См.: Приговор Брянского районного суда Брянской области от 23.07.2020 по делу № 1-96/2020. URL: <https://sudact.ru> (дата обращения: 11.03.2023).

предусматривает ответственность за приготовление к будущему хищению и, следовательно, совершение этих действий не совпадает с объективной стороной совершаемого хищения¹.

Вместе с тем в некоторых решениях суды исключают из объема обвинения преступление, предусмотренное ст. 187 УК РФ, в подобных случаях. Так, в обоснование такого решения Кимрский городской суд Тверской области указал, что изготовление осужденной Х. «поддельных распоряжений о переводе денежных средств являлось способом совершения мошенничества»².

С представленной позицией судебной инстанции согласиться сложно, поскольку действия виновной содержат признаки двух самостоятельных составов преступлений. Кроме этого, рассматривая схожие ситуации применительно к мошенничеству, совершаемому с использованием предметов, указанных в диспозиции ст. 327 УК РФ, Верховный Суд России обратил внимание на то, что использование поддельных документов при хищении путем обмана или злоупотребления доверием охватывается составом ст. 159 УК РФ, без дополнительной квалификации только в случаях, если поддельный документ был изготовлен другим лицом, т. е. тем, кто не выполняет действий, образующих объективную сторону мошенничества³.

Если осуществляется сбыт предметов, перечисленных в ст. 187 УК РФ, заведомо непригодных к использованию, деяние подлежит правовой оценке как мошенничество⁴.

На практике могут возникнуть ситуации, связанные с разграничением неправомерного оборота средств платежей и подделки, изготовления или оборота поддельных документов, государственных наград, штампов, печатей или бланков, поскольку платежные документы признаются правоприменителем официальными документами,

¹ См.: Боровых Л. В., Соловьева Е. А. К вопросу о разграничении неправомерного оборота средств платежей и иных преступлений против интересов предпринимательской деятельности // Пермский юридический альманах. 2020. № 3. С. 590–598.

² Приговор Кимрского городского суда Тверской области от 16.05.2019 по делу № 1-161/2018. URL: <https://sudact.ru> (дата обращения: 11.03.2023).

³ См.: О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного Суда РФ от 30.11.2017 № 48. URL: <https://www.consultant.ru> (дата обращения: 12.10.2023).

⁴ Там же.

т. е. использование заведомо подложных предметов преступления образует объективную сторону и в ст. 187 УК РФ, и в ст. 327 УК РФ¹.

В данном случае усматривается соотношение общей (ст. 327 УК РФ) и специальной (ст. 187 УК РФ) норм, что является основанием для правовой оценки именно по специальной норме.

В настоящее время распространение получили преступления, совершаемые с использованием реквизитов так называемых «фирм-однодневок» (обналичивание денежных средств, уклонение от уплаты налогов, мошенничество в сфере кредитования и т. д.).

Одним из подобных деяний является использование незаконно созданной организации, в том числе через подставных лиц, для осуществления неправомерного оборота средств платежей.

Сочетание самостоятельных групп признаков объективных сторон и различие непосредственных объектов в ст. 173¹ и ст. 187 УК РФ служит основанием для квалификации по совокупности в случаях использования виновным «фирмы-однодневки» для осуществления неправомерного оборота средств платежей.

Е. предложил Н. за вознаграждение выступить в качестве подставного лица при регистрации организации. Убедив Н., что созданное юридическое лицо будет осуществлять легальную финансово-хозяйственную деятельность, Е. получил от последнего паспорт и ИНН. После этого осужденный представил документы в налоговый орган, на основании чего была внесена запись в ЕГРЮЛ о регистрации ООО «Спектр» с указанием Н. в качестве директора данной организации.

После регистрации ООО «Спектр» Е. вновь обратился к Н. и предложил за вознаграждение открыть в банке расчетный счет указанной организации. Согласившись, Н. получил в банке ключевой носитель клиента Рутокен, содержащий файлы ключей электронной подписи Н. и файл сертификата ключа банка, предназначенные для доступа к системе дистанционного банковского обслуживания, которые передал Е. согласно ранее достигнутой договоренности. В последствии Е. за денежное вознаграждение сбыл указанные средства платежей неустановленному лицу с целью неправомерного осуществления

¹ См.: Хисамова З. И. Уголовно-правовые меры противодействия преступлениям, совершаемым в финансовой сфере с использованием информационно-телекоммуникационных технологий: дис. ... канд. юрид. наук. Краснодар, 2016. С. 45.

приема, выдачи, перевода денежных средств третьим лицам. Е. осужден по ст. 173¹ и 187 УК РФ¹.

Квалификация по совокупности преступлений, предусмотренных ст. 173² и ст. 187 УК РФ, производится и в ситуациях, когда неправомерному обороту средств платежей предшествовало представление документа, удостоверяющего личность, для внесения в ЕГРЮЛ сведений о подставном лице.

Б., не намереваясь осуществлять финансово-хозяйственную деятельность, предоставила паспорт гражданина Российской Федерации и другие документы в ИФНС России г. Кемерово, где была внесена запись в ЕГРЮЛ о создании ООО «XXX» и возложении полномочий директора указанной организации на Б. После государственной регистрации ООО «XXX» Б. обратилась в отделение ПАО «Сбербанк», где открыла расчетные счета для организации и получила электронный носитель информации для осуществления приема, выдачи и перевода денежных средств, платежные средства (USB-token с данными для осуществления платежей), которые за вознаграждение передала не установленному следствием лицу. Б. осуждена по ст. 173² и ст. 187 УК РФ².

Таким образом, случаи создания фирм-однодневок для последующего осуществления неправомерного оборота средств платежей судебная практика, в зависимости от обстоятельств, оценивает по совокупности ст. 187 и 173¹ или 173² УК РФ.

Нередко неправомерный оборот средств платежей сопутствует осуществлению незаконной банковской деятельности в том числе и легально функционирующими организациями, т. е. имеющими государственную регистрацию, но при этом не получившими лицензию на проведение банковских операций. Подобные ситуации характерны для нелегального снятия наличности с расчетных счетов юридических лиц (обналичивание).

В случае извлечения дохода (причинения ущерба) от подобных операций на сумму, превышающую 2 250 000 рублей, возникают основания для квалификации по ст. 172 УК РФ.

В частности, такие действия представляют собой следующие банковские операции: переводы денежных средств по поручению

¹ См.: Приговор Волжского городского суда Республики Марий Эл от 20.11.2019 по делу № 1-221/2019. URL: <https://sudact.ru> (дата обращения: 11.03.2023).

² См.: Приговор Заводского районного суда г. Кемерово от 15.07.2020 по делу № 1-567/2020. URL: <https://sudact.ru> (дата обращения: 11.03.2023).

физических лиц без открытия банковских счетов; инкассация денежных средств и кассовое обслуживание физических и юридических лиц; привлечение денежных средств физических и юридических лиц и др.¹

Так, главный бухгалтер ООО «Уютный дом» Ш. по предварительному сговору с генеральным директором Ф. без лицензии осуществляли банковскую деятельность, связанную с проведением операций по обналичиванию денежных средств. За период преступной деятельности по инициативе лиц ООО «1», ООО «2» и ООО «3», заинтересованных в получении наличности, на расчетные счета ООО «Уютный дом» в безналичной форме перечислены денежные средства на сумму, превышающую 58 000 000 рублей, в результате чего Ш. был извлечен доход 5 292 420 рублей, составлявший 9 % от зачисленных на расчетный счет денежных средств. При совершении перечислений в назначениях платежей Ш. указывала не соответствующие действительности основания.

Для осуществления указанных незаконных банковских операций Ш. при помощи программного обеспечения «1С: Бухгалтерия» и сети Интернет изготовила для управления расчетными счетами ООО «Уютный дом» распоряжения о переводе денежных средств, документы и иные средства оплаты. Ш. осуждена по ч. 1 ст. 172, ч. 1 ст. 187 УК РФ².

Е. А. Соловьева указывает, что если при изготовлении электронных средств платежей происходит противоправный доступ к базам данных оператора платежной системы или создается и используется вредоносная компьютерная программа, предназначенная для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, содеянное подлежит дополнительной квалификации по ст. 272, 273, 274¹ УК РФ³.

Вместе с тем в полной мере согласиться с подобной точкой зрения сложно.

Действия по созданию или распространению вредоносных компьютерных программ, предназначенных для нейтрализации средств

¹ См.: Коренная А. А. Проблемы квалификации действий по незаконному обналичиванию денежных средств // Адвокат. 2017. № 3. С. 75.

² См.: Приговор Ленинского районного суда г. Ульяновска от 20.07.2020 по делу № 1-211/2020. URL: <https://sudact.ru> (дата обращения: 15.03.2023).

³ См.: Соловьева Е. А. Преступления, совершаемые в платежных системах: дис. ... канд. юрид. наук. Саратов, 2019. С. 145.

защиты банковской компьютерной информации, содержащие признаки ст. 273 УК РФ, идентичны по своему составу запрещенным ст. 187 УК РФ изготовлению или сбыту компьютерных программ, предназначенных для неправомерного осуществления приема, выдачи, перевода денежных средств.

В такой ситуации возникает конкуренция уголовно-правовых норм, которая с учетом объектов уголовно-правовой охраны, особенностей предмета и объективной стороны преступлений должна решаться в пользу специальной нормы, т. е. неправомерного оборота средств платежа.

§ 3. Особенности возбуждения уголовных дел по фактам совершения преступлений, связанных с неправомерным оборотом средств платежей

Возбуждение уголовного дела является одной из основополагающих стадий предварительного расследования. Именно здесь решается вопрос о наличии состава преступления по сообщению или обнаруженной информации. На данной стадии сотрудниками правоохранительных органов проводится первоначальная проверка, по результатам которой следователь принимает законное и обоснованное процессуальное решение в соответствии со ст. 145 УПК РФ.

Изначально при поступлении сообщения о преступлении или получении информации о совершенном деянии, связанном с неправомерным оборотом средств платежей, анализируется место и время произошедшего деяния для возможности решения вопроса о территориальности дальнейшего проведения проверки и расследования преступления. После решения данного вопроса проводится комплекс мероприятий, позволяющих принять правильное процессуальное решение. Данная стадия еще обозначается как доследственная проверка и ограничивается определенными процессуальными сроками в соответствии с уголовно-процессуальным законодательством Российской Федерации. В определенные УПК РФ сроки необходимо установить достаточность обстоятельств, указывающих на наличие либо отсутствие в деянии состава преступления, по результатам которых будет решаться вопрос о возбуждении уголовного дела либо отказе в его возбуждении.

Возможные мероприятия, проводимые на стадии доследственной проверки, направленные на достижение ее целей и задач:

- анализ источников информации, из которых поступило сообщение о преступлении (устанавливается личность лица, подавшего заявление, его характеризующие данные, достоверность сообщенной информации, может ли данное сообщение использоваться в качестве повода для возбуждения уголовного дела.);

- определение территориальности и подведомственности преступления, о котором идет речь в сообщении, органам предварительного следствия и дознания;

- установление наличия предмета преступного деяния, его стоимости, общей суммы ущерба;

- определение лица или круга лиц, которым в результате совершенного деяния причинен вред;

- установление способа совершения преступления, технических средств, используемых при его совершении как преступником, так и потерпевшим;

- установление круга лиц, кому могло быть выгодно совершение преступления, кто мог обладать информацией о жертве и ее финансовых данных (счетах, номерах карт и т. д.);

- сопоставление связей жертвы с кругом ее общения, анализ взаимоотношений;

- формирование доследственных версий; и т. п.

Из анализа рассмотренных уголовных дел по преступлениям, предусмотренным ст. 187 УК РФ, были выявлены общие источники, из которых можно получить информацию о совершенном преступлении:

- банки-эмитенты, выпускающие платежно-расчетные документы, процессинговые компании, являющиеся провайдерами процесса приема платежей на сайте, которые могут обладать информацией о фактах использования или попытках использования поддельных платежных средств;

- организации, оказывающие финансовые услуги и являющиеся в этой связи участниками оборота электронных средств платежа (банки, кредитные организации)¹;

¹ См.: Плотникова А. Г. Методика расследования изготовления или сбыта поддельных кредитных либо расчетных карт и иных платежных документов. Волгоград, 2023. С. 48.

– из заявлений законного держателя (владельца) электронного средства платежа, чьи платежные средства были подделаны злоумышленником и использованы в преступных целях;

– при расследовании другого уголовного дела, не связанного с незаконным оборотом средств платежа (например, из допросов, обысков и т. д.);

– иные источники, например из информационных ресурсов сети Интернет, онлайн-трансляций, социальных сетей, а также в ходе проведения оперативно-разыскных мероприятий, в том числе мониторинга виртуального пространства и др.

В настоящее время технологии на основе искусственного интеллекта позволяют кредитным финансовым организациям проводить мониторинг транзакций, в ходе которого выявлять наличие подозрительных признаков, указывающих на незаконные действия с платежными средствами, брать их на контроль, собирать и анализировать первоначальную информацию, которую передают в правоохранительные органы, что влечет поводы для дальнейшей проверки и принятия решения о возбуждении уголовного дела.

Алгоритмы нейросети устроены таким образом, что на основе заложенного интеллекта происходит постоянный мониторинг транзакций платежных систем, где отслеживается периодичность переводов, обналичивания, остатков на счетах, суммы операций, между какими счетами осуществлялись переводы. В случае если за долгий период держатель осуществлял переводы мелкими суммами и вдруг заявлена операция на перевод крупной суммы, система запрашивает дополнительную информацию на выполнение транзакции. Если пользователь пытается осуществить перевод на счет, на который ранее средства не переводились, искусственный интеллект также предупреждает об обнаружении подозрительной операции и направляет запрос на ее подтверждение.

Таких признаков много, и алгоритмы работы нейросетей постоянно совершенствуются, развиваются, что позволяет обеспечить комплексный подход к аналитике пользования электронными средствами платежа и выявить в них определенные закономерности, могущие говорить о наличии потенциального риска преступного посягательства¹.

¹ См.: Плотникова А. Г. Методика расследования изготовления или сбыта поддельных кредитных либо расчетных карт и иных платежных документов. Волгоград, 2023. С. 50.

В качестве обстоятельств, влияющих на принятие решения о возбуждении уголовного дела по признакам состава преступления, предусмотренного ст. 187 УК РФ, необходимо рассматривать:

- задержание лица с поличным в момент попытки использования поддельного платежного средства;
- факты несанкционированного списания торгово-сервисной организацией денежных средств с банковского счета потерпевшего по поддельному слипу;
- факты причастности торгово-сервисной организации (в лице конкретных сотрудников или управляющего персонала) к обороту поддельных электронных средств платежа и иных предметов преступления, предусмотренного ст. 187 УК РФ;
- факт получения субъектом prepaid карты по поддельным документам, превышения им открытого счета и невозвращения банку-эмитенту потраченных денежных средств¹;
- наличие подтвержденной информации о том, что платежные средства ранее уже терялись их законным держателем.

В ходе доследственной проверки рекомендуется проводить комплекс мероприятий, направленных на установление обстоятельств произошедшего, дающих возможность принятия законного и обоснованного итогового решения по наличию признаков преступления, предусмотренного ст. 187 УК РФ:

- отбор объяснения у заявителя об обстоятельствах произошедшего события, с указанием обстановки, места, времени, используемых технических средств осуществления незаконных расчетов с применением пластиковой карты;
- обследование с участием специалиста места происшествия (торгово-сервисной организации либо места нахождения банкомата);
- беседа со специалистами в области изготовления и оборота пластиковых карт по поводу способов изготовления, использования, отличительных признаков;
- получение объяснений от задержанного лица, держателя карты, сотрудников банка или торгово-сервисной организации, осуществлявшей обслуживание карты, свидетелей (очевидцев);

¹ См.: Плутникова А. Г. Методика расследования изготовления или сбыта поддельных кредитных либо расчетных карт и иных платежных документов. Волгоград, 2023. С. 50.

- получение образцов почерка и подписи у задержанного лица и держателя карты для сравнительного исследования;

- сбор фото- и видеоматериалов, имеющих непосредственное отношение к операции с использованием поддельной, утерянной либо украденной платежной карты (возможно получение записи с камеры видеонаблюдения, расположенной на банкомате, в банке, где происходило обналичивание денежных средств);

- сбор слипов по проведенным операциям платежной карты жертвы, содержащих подпись лица, осуществившего платеж, и иных образцов почерка и подписи держателя карты для сравнительного исследования;

- получение от службы безопасности банка, обслуживающего клиента, материалов расследования осуществления незаконных транзакций;

- составление фоторобота подозреваемого и организация его розыска;

- проведение оперативно-разыскных мероприятий с целью выявления лиц, имеющих отношение к использованию поддельной, утерянной либо украденной платежной карты, организация наблюдения за ними, их связями, прослушивание телефонных переговоров, контроль почтовой и телеграфной корреспонденции, снятие информации с технических каналов связи;

- наведение справок путем направления запросов в банки, торгово-сервисные организации, орган государственной регистрации;

- получение заключений специалистов о предварительном исследовании изъятых документов и других доказательств;

- исследование документов, регламентирующих порядок проведения операций с использованием платежных карт (нормативных актов Банка России, договоров, заключенных между участниками расчетов, правил и инструкций, нормативно-справочных, технических и технологических документов, устанавливающих порядок совершения операций с использованием платежных карт).

По окончании доследственной проверки по имеющейся информации о совершенном преступлении, связанном с незаконным оборотом средств платежей, следователь на основании собранных материалов принимает процессуальное решение о возбуждении или отказе в возбуждении уголовного дела.

В случае подтверждения наличия состава преступления и принятия решения о возбуждении уголовного дела по квалифицирующим признакам, предусмотренным ст. 187 УК РФ, на момент вынесения постановления у следователя на основе собранной информации формируются следственные ситуации.

В следственной практике известны несколько типичных следственных ситуаций, свойственных рассматриваемому составу преступления, которые складываются к моменту возбуждения уголовного дела, их можно классифицировать в зависимости от оснований.

Первая классификация зависит от наличия поддельного платежного средства и предполагает следующие ситуации.

Ситуация 1. Обнаружены в ходе неправомерного оборота поддельные платежные карты или иные средства оплаты (при этом обнаружить их могут как торговая или финансовая организации, так и обычные граждане). Данная ситуация считается одной из самых сложных, так как какая-либо информация о лице, совершившем преступление, отсутствует. Дефицит первоначальной информации должен быть восполнен проведением достаточно большого количества мероприятий, направленных на установление всех лиц, причастных к совершению преступления, и обстоятельств произошедшего.

Первичным мероприятием должен стать осмотр места происшествия, где было обнаружено поддельное средство платежа. В ходе осмотра места происшествия устанавливаются лица, которые обнаружили данное средство, свидетели и очевидцы, присутствующие на месте обнаружения поддельного средства платежа в момент его использования, обращается внимание на наличие камер видеонаблюдения. Производится опрос вышеуказанных лиц с выяснением информации о лице, использовавшем поддельное средство платежа, признаках его внешности, об одежде, поведении, действиях на месте до обнаружения поддельного средства платежа. Основной задачей в данной следственной ситуации является установление личности всех участников, причастных к совершенному преступлению (изготовителя, пособников, исполнителя)¹.

¹ См.: Расследование преступлений в сфере экономики: учеб. пособие / под ред. В. Ю. Алферова, Е. Т. Барбакадзе, К. И. Богомолова [и др.]. Саратов: Саратовский социально-экономический институт федерального государственного бюджетного образовательного учреждения высшего образования «Российский экономический университет им. Г. В. Плеханова», 2018. С. 202.

Ситуация 2. Поддельные платежные карты или иные средства оплаты обнаружены в момент их сбыта, сбытчик с места преступления скрылся, данные о его личности не установлены, имеется средство платежа. Эта ситуация также является достаточно сложной, так как информации о личности сбытчика и лицах, причастных к совершению преступления, практически нет, имеется информация о внешности сбытчика и осталась в наличии поддельная платежная карта или иное средство оплаты. В данной ситуации необходимо также произвести осмотр места происшествия, которым будет являться место сбыта, обращается внимание на наличие камер видеонаблюдения на месте осмотра и прилегающей территории, рядом расположенных объектах; производится опрос лица, которому преступник пытался сбыть поддельное средства платежа, выясняется информация о признаках внешности преступника; составляется его фоторобот; рассылаются ориентировки по всем постам и нарядам для осуществления розыска преступника по горячим следам; средство платежа подвергается дактилоскопическому исследованию с целью обнаружения на нем отпечатков пальцев рук преступника, при их наличии проводится проверка по базам дактилоскопического учета на совпадение.

Ситуация 3. В момент сбыта или использования поддельного средства платежа был задержан преступник, поддельное средство платежа изъято и имеется в наличии у сотрудников правоохранительных органов. Указанная ситуация является самой благоприятной, так как имеется достаточно информации и о личности преступника, и о предмете преступления. В данной ситуации первоначальные мероприятия необходимо начинать с личного досмотра задержанного с целью обнаружения при нем иных поддельных средств платежа или документов, указывающих на признаки преступной деятельности или причастность к ней иных лиц, также изымается сотовый телефон, который в дальнейшем осматривается на предмет обнаружения поддельников данного преступления. Следующее мероприятие – осмотр места задержания на предмет обнаружения выброшенных предметов преступной деятельности и иных доказательств, указывающих на причастность к совершенному преступлению, предусмотренному ст. 187 УК РФ, задержанного лица. По изъятому поддельному платежному средству (средствам) необходимо установить

их настоящего владельца, для этого направляется запрос в банк-эмитент с указанием реквизитов. Производится допрос задержанного лица с целью установления иных подельников преступления, иных эпизодов преступной деятельности. Последующий этап расследования предполагает допросы законных владельцев средств платежей, проведение обысков по месту жительства задержанного лица и его подельников, установление информации о финансовом состоянии всех лиц, причастных к совершенному преступлению, о их личных банковских счетах и счетах их родственников, совершенных транзакциях, анализ этих транзакций. Проведение опознания законным владельцем средства платежа задержанного лица с целью установления уровня их знакомства. Проверка по учетам задержанного лица на причастность к совершению иных нераскрытых преступлений.

Вторым основанием для классификации следственных ситуаций по преступлениям, связанным с неправомерным оборотом средств платежей, является место совершения преступления. По данному основанию возможно выделить следующие типичные следственные ситуации.

Ситуация 1. Имеется информация о совершении преступления или покушении на совершение преступления, предусмотренного ст. 187 УК РФ, с использованием конкретного банкомата. В данной ситуации следователю необходимо произвести осмотр банкомата, в ходе которого предпринять меры к обнаружению и изъятию в нем поддельного средства платежа и (или) белого пластика. Средства платежа или белый пластик направляются на исследование с целью установления информации, записанной на магнитную полосу. В случае уже проведенной инкассации банкомата необходимо произвести выемку у представителей банка поддельного средства платежа или белого пластика, а также документов о проведенной инкассации. Опрашиваются все лица, участвовавшие в проведении инкассации банкомата, осуществляется их дактилоскопирование, чтобы в последующем при дактилоскопическом исследовании пластика исключить совпадение папиллярных узоров, обнаруженных на пластике, с узорами инкассаторов. Необходимо также предпринять меры для изъятия записи с камеры видеонаблюдения, расположенной на банкомате, для этого в обслуживающем банкомат банке производится выемка данной записи за конкретный период, который представляет

интерес для следствия. Изъятая запись подлежит осмотру и предъявляется потерпевшему для опознания лица, осуществившего транзакцию по поддельной карте¹.

Ситуация 2. Имеется информация о совершении преступления или покушении на совершение преступления, предусмотренного ст. 187 УК РФ, с использованием технологии эквайринга, то есть терминала, принимающего безналичные платежи посредством использования банковских карт с системой бесконтактной оплаты. В сложившейся ситуации рекомендуется изначально провести опрос кассира торговой организации, который принимал оплату с использованием системы эквайринга, с целью выяснения данных о признаках внешности лица, использовавшего поддельный пластик. С этой целью целесообразно также опросить охранника и другой вспомогательный персонал, работающий в этот день. Произвести осмотр места происшествия в торговой организации с изъятием записей с камер видеонаблюдения, на которых зафиксировано подозреваемое лицо. Допросить законного держателя платежного средства, которое было подделано и использовано, и в случае наличия на видео записи, изъятый с торговой организации подозреваемого, предъявить ее потерпевшему для опознания преступника. Кроме этого, обязательно следует произвести выемку в банке-эмитенте, через который была осуществлена незаконная транзакция по поддельному средству платежа, документов, подтверждающих платеж. Документы о платеже также необходимо изъять в торговой организации (как правило, это кассовая лента с копией чека об оплате), возможно, на чеке имеется подпись лица, осуществившего платеж, по которой можно назначить почерковедческую экспертизу.

Ситуация 3. Имеется информация о совершении преступления или покушении на совершение преступления, предусмотренного ст. 187 УК РФ, с использованием сети Интернет, какие-либо следы отсутствуют, информации о лице, совершившем преступление, не имеется. Расследование по данной ситуации начинается с отработки источника информации, из которого получены данные о покушении на преступление или его совершении. Необходимо осуществить запрос в банк-эмитент, проводивший подозрительную транзакцию, с целью

¹ См.: Бураева Л. А. К вопросу о классификации типичных следственных ситуаций по преступлениям, совершаемым с использованием банковских платежных карт // Бизнес в законе: эконом.-юр. журн. 2015. С. 108–110.

установления номера счета, на который был осуществлен перевод, его владельца. Устанавливается информационно-телекоммуникационный ресурс, используемый при совершении преступления, это могут быть сайты интернет-магазинов, социальные сети, онлайн-банки и т. д. После установления интернет-ресурса необходимо установить время совершения транзакции и IP-адрес устройства, с которого был осуществлен выход в сеть. По IP-адресу устанавливаем провайдера, которому он принадлежит, и запрашиваем регистрационные данные пользователя выделенной линией. С целью обнаружения цифровых следов рекомендуется осуществить осмотр технических устройств, с которых потерпевшим осуществлялся выход в интернет-пространство, возможно, в рамках данного следственного действия будут установлены сайты или иные интернет-площадки, которые посещал потерпевший, где предположительно мог незаметно поймать «вирус». Кроме этого, подробно допрашивается потерпевший обо всех обстоятельствах, способствующих предоставлению помощи в установлении значимой информации по делу.

Таким образом, наличие первоначальной информации, имеющейся в распоряжении следователя, дает возможность определить типичную следственную ситуацию на первоначальном этапе расследования и использовать типовой алгоритм мероприятий, способствующих установлению обстоятельств события, связанного с неправомерным оборотом средств платежей.

§ 4. Способы совершения преступлений, связанных с неправомерным оборотом средств платежей

Механизм преступления включает в себя такие элементы, как подготовка к совершению преступления, сам процесс совершения преступления и сокрытие следов преступной деятельности. Любой процесс совершения преступления немыслим без средств, с помощью которых оно совершается. Для того чтобы понять сущность механизма преступления, следует детально разобрать его средства. Средствами платежей, используемыми в неправомерном обороте, могут являться:

- 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 из указанных средств по целевому назначению при совершении преступления, предусмотренного ст. 187 УК РФ.

Первым и самым широко используемым средством при совершении указанных преступлений является *платежная карта*. Согласно п. 1.6 Положения об эмиссии платежных карт и об операциях, совершаемых с их использованием, утвержденного Банком России 24.12.2004 № 266-П¹, платежные карты подразделяют на три вида: расчетные (дебетовые), кредитные и предоплаченные карты.

Данные карты являются банковским продуктом, выпускаемым банком-эмитентом, осуществляющим обслуживание расчетных счетов граждан, представляют собой пластик стандартных (общепринятых) размеров, на котором размещены реквизиты банка и пользователя, и являются способом управления банковским счетом физического или юридического лица.

Пластиковая карта, в соответствии с вышеуказанным положением, является собственностью банка, на основании заключенного договора выдается физическому или юридическому лицу на определенный срок для управления банковским счетом, зарегистрированным в банке-эмитенте. По истечении срока использования пластик должен сдаваться в банк, его выдавший.

Все виды карт (расчетная, предоплаченная и кредитная) схожи по своему назначению и являются электронным инструментом осуществления транзакций безналичным способом, однако между ними есть некие различия, заключающиеся в принадлежности используемых денежных средств, содержащихся на расчетном счете.

Расчетная карта – это дебетовая банковская карта, платежи по которой осуществляются 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

¹ См.: Об эмиссии платежных карт и об операциях, совершаемых с их использованием: положение Банка России от 24.12.2004 № 266-П (в ред. от 28.09.2020). URL: <https://www.consultant.ru> (дата обращения: 12.10.2023).

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 используется для осуществления перевода электронных денежных средств, возврата остатка электронных денежных средств в пределах суммы предварительно предоставленных держателем денежных средств кредитной организации-эмитенту в соответствии с Федеральным законом от 27.06.2011 № 161-ФЗ «О национальной платежной системе».

В пункте 19 ст. 3 вышеуказанного закона электронное средство платежа определяется как средство и (или) способ, позволяющие клиенту составлять, удостоверять и передавать распоряжения оператору электронных денежных средств (далее – ЭДС) в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств. Исходя из указанной дефиниции, следует вопрос: что именно относится к электронным средствам платежа? Согласно п. 1.5 положения Центрального банка РФ от 24.12.2004 № 266-П «Об эмиссии платежных карт и об операциях, совершаемых с их использованием», к электронным средствам платежа отнесены расчетные (дебетовые), кредитные и предоплаченные карты, держателями которых являются физические лица, в том числе уполномоченные юридические лица и индивидуальные предприниматели¹. Понятие, назначение, способ использования расчетных и кредитных карт уже были рассмотрены выше. Охарактеризуем предоплаченные карты.

Так, в соответствии со ст. 26 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе» предоплаченной

¹ См.: Об эмиссии платежных карт и об операциях, совершаемых с их использованием: положение Центрального банка РФ от 24.12.2004 № 266-П (в ред. от 28.09.2020). URL: <https://www.consultant.ru> (дата обращения: 12.10.2023).

является платежная карта, предоставляемая клиенту оператором электронных денежных средств и используемая для перевода электронных денежных средств. При этом все предоплаченные карты подразделяются на персонифицированные и неперсонифицированные в зависимости от того, осуществляется ли идентификация клиента при переводе электронных¹ денежных средств или не осуществляется в соответствии с требованиями Федерального закона от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»².

В то же время согласно положению Банка России от 28.02.2013 «О применении отдельных положений Федерального закона „О национальной платежной системе“» к электронным средствам платежа, кроме того, относятся бонусные, подарочные, дисконтные, накопительные карты, которые могут использоваться гражданами для расчетов в магазинах-партнерах, но отличаются от платежных карт банков-эмитентов³. В. Б. Гольцов и Н. М. Голованов, рассматривая вопрос использования электронного средства платежа, обозначают особенности, по которым их возможно разграничить: «В связи с употреблением законодателем весьма широкой дефиниции электронного средства платежа как формы безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, а также иных технических устройств и возникающей в связи с этим неопределенностью в отнесении тех или иных технических устройств к электронным средствам платежа необходимо руководствоваться двумя критериями, первый из которых состоит в возможности составлять, удостоверять и передавать распо-

¹ См.: Плотникова А. Г. Методика расследования изготовления или сбыта поддельных кредитных либо расчетных карт и иных платежных документов. Волгоград, 2023. С. 25.

² См.: О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма: федер. закон от 07.08.2001 № 115-ФЗ (в ред. от 29.12.2022) // Собрание законодательства РФ. 2001. № 33. Ст. 3418 (ч. I); 2023. № 1. Ст. 54 (ч. I).

³ См.: О применении отдельных положений Федерального закона «О национальной платежной системе»: информация Банка России от 28.02.2013. URL: <https://www.consultant.ru> (дата обращения: 12.10.2023).

ряжения оператору ЭДС в целях осуществления перевода денежных средств, а второй – в оформлении указанной возможности договором, заключаемым с оператором ЭДС, являющимся кредитной организацией»¹.

Следующим, также достаточно распространенным средством совершения преступлений, предусмотренных ст. 187 УК РФ, является *распоряжение о переводе денежных средств, документов и средств оплаты*.

Опираясь на положение Банка России от 29.06.2021 № 762-П «О правилах осуществления перевода денежных средств»², банки России, кредитные организации осуществляют перевод денежных средств по банковским счетам и без открытия банковских счетов в рамках применяемых форм безналичных расчетов 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. Банки используют следующие виды безналичных переводов: платежные поручения, аккредитив, инкассовые поручения, расчетные чеки, по требованию получателя средств. Использовать данные виды переводов имеют право юридические, физические лица, индивидуальные предприниматели. Перевод денежных средств банками осуществляется в электронном виде, в том числе с использованием электронных средств платежа, или на бумажных носителях.

Электронные средства и электронные носители информации, а также технические устройства, предназначенные для неправомерного осуществления приема, выдачи, перевода денежных средств. Разберем по отдельности каждый из элементов, перечисленных в данном пункте.

Электронные средства и электронные носители информации, предназначенные для неправомерного осуществления приема, выдачи, перевода денежных средств. Законодателем не дано четкое опре-

¹ Правовое регулирование перевода электронных денежных средств: монография / под ред. В. Б. Гольцова, Н. М. Голованова. СПб., 2019. С. 51–52.

² См.: О правилах осуществления перевода денежных средств: положение Центрального банка РФ от 29.06.2021 № 762-П (ред. от 03.08.2023). URL: <https://www.consultant.ru> (дата обращения: 12.10.2023).

деление, что относится к предмету преступления, понимаемому под электронным средством или электронным носителем информации в контексте диспозиции ст. 187 УК РФ. По нашему мнению, назначение электронных средств и электронных носителей информации разное. Предназначение данных инструментов заключается в получении, сборе, переработке, использовании информации в цифровой форме. В соответствии с Законом о национальной платежной системе «электронное средство платежа – средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств»¹. Самыми известными и распространенными электронными средствами приема, перевода денежных средств являются онлайн-банки (Сбербанк, ВТБ, Альфабанк, Ренесанс банк, Тинькофф и др.), электронные кошельки (Яндекс Деньги, Qiwi, WebMoney, Payeer, PayPal, Perfect Money и др.).

Электронные носители информации представляют собой устройства, предназначенные для приема, хранения и передачи информации в цифровом формате. Основными видами электронных носителей информации являются: жесткие диски, флеш-накопители, CD-ROM, DVD-ROM, Blu-ray диски, карты памяти. Кроме этого, они могут использоваться с целью обработки различной информации как содержащейся на нем, так и извне. В целях совершения неправомерного приема, выдачи, перевода денежных средств электронные носители информации подсоединяют к техническим устройствам, с помощью которых происходит прием, выдача либо перевод денежных средств, и используют записанную на нем информацию или программу как инструмент доступа.

Что касается технических устройств, применяемых для неправомерного осуществления приема, выдачи, перевода денежных средств, к ним относятся: банкоматы и POS-терминалы. Банкоматы – это устройства, изготавливаемые специальными компаниями и сдаваемые

¹ О национальной платежной системе: федер. закон от 27.06.2011 № 161-ФЗ (посл. ред.). URL: <https://www.consultant.ru> (дата обращения: 23.10.2023).

в аренду банкам-эмитентам для использования гражданами в целях осуществления электронных переводов, платежей, получения и внесения денежных средств. Эквайринговые терминалы (POS-терминалы) – это технические устройства, предназначенные для получения и осуществления оплаты за товар в различных торговых, финансовых организациях. Как правило, данные технические устройства являются подлинными, но с целью совершения преступлений, связанных с неправомерным оборотом средств платежей, преступники используют современное оборудование (скиммеры, шиммеры), которое устанавливается на банкоматы для дешифрации цифровой информации с магнитной полосы электронных средств платежей (пластиковых банковских карт) при их использовании. Данное оборудование устанавливается незаметно в карт-ридер и при вставлении пластиковой банковской карты считывает информацию о номере счета, номере карты, CVV-код, ФИО держателя карты, дату действия и др. При использовании POS-терминала для проведения оплаты товара преступники могут вводить неверные суммы, превышающие реальные, либо проводить оплату несколько раз за один и тот же товар. Кроме непосредственных технических устройств, применяемых с целью неправомерного оборота денежных средств, используются также и опосредованные. К ним относятся: эмбоссеры (устройства, предназначенные для выдавливания идентификационной информации на пластиковой карте клиента: номера карты, срока ее 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), наклейки на клавиатуру, накладные камеры видеонаблюдения, RFID-считыватель (устройство, позволяющее улавливать радиосигналы, сохранять их и передавать). RFID-считыватель по своим функциям похож на бесконтактный POS-терминал, способный считывать данные без непосредственного взаимодействия с картой. В своих трудах 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: запускается операционная система и установленное приложение, которое передает информа-

цию 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»¹. Чтобы получить зашифрованную информацию на RFID-метке пластиковой карты ее законного держателя, злоумышленнику достаточно приблизиться считывающим устройством к карте на расстояние NFC (взаимодействие ближнего 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.

Компьютерные программы, предназначенные для неправомерного осуществления приема, выдачи, перевода денежных средств. Говоря о компьютерных программах, 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 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.

На основе изученной судебно-следственной практики можно сделать вывод, что из всех перечисленных предметов преступного посяательства при совершении преступления, предусмотренного ст. 187 УК РФ, чаще всего преступниками используются распоряжения о переводе денежных средств, документы или средства оплаты. Такого же мнения придерживается В. Ф. Васюков², полагая, что иные

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

² См.: 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: сб. матер. Орел: Орловский юридический институт Министерства внутренних дел Российской Федерации имени В. В. Лукьянова, 2018. С. 20–26.

средства преступники не используют 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 требуется специальное программное обеспечение, дорогостоящее оборудование и наличие специальных знаний в указанной области, которые имеют особую специфику и требуют определенных навыков.

Как указано ранее, вышеперечисленные средства совершения преступления входят в состав механизма совершения преступления и являются его неотъемлемой частью. Механизм совершения преступления, предусмотренного ст. 187 УК РФ, также включает в себя способы совершения. Первый из способов совершения неправомерного оборота средств платежей – подделка платежной карты. Например, Г. Р. Гаджиев и В. И. Тюнин в своих исследованиях говорят, что «в мировой практике, которая имеет более давнюю историю оборота платежных карт, выделяют несколько способов подделки карт: частичная и полная»¹. При этом частичная подделка предполагает внесение лишь некоторых изменений в существующий настоящий пластик, тогда как полная подделка подразумевает полностью изготовление точной копии пластиковой банковской карты, под залив данных, которую не сможет отличить ни один работник кредитной или торговой организации. Изготовление точной копии пластиковой банковской карты требует особых навыков и наличия специального оборудования, о котором мы уже упоминали выше.

Следующий способ совершения преступлений, предусмотренных ст. 187 УК РФ, – *подделка распоряжений о переводе денежных средств* – является одним из самых распространенных в связи с простотой его подготовки и использования. Т. И. Розовская в своей работе анализирует данный способ: «По банковским правилам судьи относят к поддельным платежным документам документы, включаю-

¹ Гаджиев Г. Р., Тюнин В. И. Вопросы противодействия преступлениям, совершаемым с использованием электронных средств платежа // StudNet. 2021. № 7. С. 21–30.

шие любую информацию, которая не соответствует установленным реквизитам платежного документа: сумма, назначение платежа, наименование товара или работ, за которые производится оплата. В качестве подтверждения факта отсутствия взаимоотношений между участниками сделки правоприменитель может сослаться на поддельный счет на оплату, акты выполненных работ / оказанных услуг, которые на самом деле не исполнялись или исполнялись организациями или индивидуальными предпринимателями, отличными от указанных в документе, контракты без намерения их исполнения в действительности или на тот факт, что подписант по контракту не подписывал его»¹.

Кроме этого, Л. П. Ломовцева и А. В. Сачихин, рассматривая в данном способе уголовно-правовую характеристику, утверждают: «...в качестве объективной стороны криминального деяния в настоящее время выступает лишь сам факт составления подобного платежного поручения, который абсолютно вне зависимости от его реального использования для перевода денежных средств сам по себе уже квалифицируется как не только незаконная операция с „иными платежными документами, не являющимися ценными бумагами“, но и как их оборот»². Указанный состав преступления по своим квалифицирующим признакам носит формальный характер, в связи с чем при установлении обстоятельств, подлежащих доказыванию, следует обращать внимание не только на факт совершения неправомерной транзакции по переводу денежных средств, но и на способ изготовления распоряжения о переводе денежных средств, в обязательном порядке проверяется подлинность документа, на основании которого совершена финансовая операция. В процессе расследования указанной категории преступлений правоохранительными органами допускаются серьезные ошибки при квалификации содеянного преступниками. Так,

¹ Розовская Т. И., Куликов Р. С., Грезин А. С. Неправомерный оборот средств платежей (ст. 187 УК РФ) как инструмент легализации преступных доходов: особенности уголовно-правового противодействия // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2021. № 4 (56). С. 99–104.

² Ломовцева Л. П., Сачихин А. В. Негативные тенденции применения ст. 187 УК РФ в уголовных делах экономической направленности // Вестник науки и образования. 2020. № 25–1 (103). С. 46–54.

следователи неправильно трактуют незаконные изготовление платежного средства и подделку платежного средства. Под незаконным изготовлением в рамках квалификации по ст. 187 УК РФ следует понимать, например, производство пластиковых банковских карт или платежного поручения в нарушение правил эмиссии таких документов, установленных государством. Примером таких нарушений могут являться действия сотрудника банка по изготовлению платежной пластиковой карты на имя гр-на К. без его ведома. То есть сама карта будет подлинной, но выпущена незаконно, так как гр-н К. своего согласия на ее выпуск не давал. Другая ситуация будет говорить о том, что карта или платежный документ является поддельным, когда с подлинной карты была считана информация о ее действительном держателе и нанесена путем эмбосирования на белый пластик.

Е. Н. Балябин и В. В. Кулешов в своей статье приводят попытку отграничения составов преступлений, связанных с мошенничеством и неправомерным оборотом средств платежей на основе определения подлинности и поддельности карт: «...с учетом существования ст. 159.3 УК РФ представляется, что как сбыт поддельных расчетных и кредитных банковских карт по ст. 187 УК РФ можно квалифицировать, во-первых, выпуск их в обращение при отсутствии обмана относительно их сути, например, изготовление партии подделок и ее продажа заинтересованным лицам, которые планируют так или иначе их использовать, и, во-вторых, ситуации, в которых с помощью обмана и поддельных (либо чужих) платежных карт виновный незаконно получает не вещи, а услуги, которые по сути своей не подпадают под признаки предмета мошенничества»¹.

Изучив и проанализировав судебную практику, мнения различных ученых в области уголовно-правовых наук, подведем итоги, касающиеся способов совершения преступлений, связанных с неправомерным оборотом средств платежей, используемых преступниками в своих корыстных целях:

– неправомерное изготовление средств платежей, распорядительных документов без ведома на то действительного владельца финансового счета в нарушение правил эмиссии таких документов,

¹ Балябин В. Н., Кулешов В. В. О разграничении сбыта поддельных платежных карт и мошенничества с их использованием // Банковское право. 2015. № 1. С. 12–14.

установленных государством с целью проведения дальнейших денежных операций по расчетным счетам жертвы¹;

- создание поддельной пластиковой банковской карты (белый пластик) с заливом на ее магнитную полосу или RFID-метку конфиденциальной информации, заранее похищенной путем скиминга или шиминга с подлинной карты ее реального владельца, с целью дальнейшего обналичивания или перевода денежных средств, размещенных на расчетном счету жертвы²;

- создание специальных вирусных программ для внедрения в платежные системы «Банк-клиент» с целью дальнейшего управления финансовыми операциями по счетам организации или клиентов;

- сбыт 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 платежей³;

- создание фейковых электронных кошельков (Яндекс Деньги, Qiwi, WebMoney, Payeer, PayPal, Perfect Money и др.) для осуществления неправомерного оборота с денежными средствами граждан;

- использование специальных технических устройств, предназначенных для хищения конфиденциальных данных держателей пластиковых банковских карт в момент их использования в POS-терминалах, банкоматах;

- применение ключей доступа в рамках использования служебного положения сотрудниками банка с целью незаконного распоряжения

¹ См., напр.: Приговор Первомайского районного суда г. Ижевска Удмуртской Республики по делу № 1428/19 от 16.11.2019; Приговор Индустриального районного суда г. Ижевска Удмуртской Республики по делу № 1375/2020 от 11.10.2020; Приговор Первомайского районного суда г. Краснодара по делу № 1-70/2019 (1-532/2018) от 22.02.2019; Приговор Индустриального районного суда г. Перми по делу № 1-97/2019 от 20.05.2019. URL: <https://www.consultant.ru> (дата обращения: 12.10.2023).

² См., напр.: Приговор Тушинского районного суда г. Москвы от 20.11.2017 по уголовному делу № 1-701/17. URL: <https://www.consultant.ru> (дата обращения: 12.10.2023).

³ См., напр.: Приговор Ленинского районного суда г. Воронежа от 03.11.2021 по уголовному делу № 1-206/21. URL: <https://www.consultant.ru> (дата обращения: 12.10.2023).

счетами организаций или физических лиц и неправомерного оборота средств платежей¹.

Таким образом, при подготовке к совершению преступления, предусмотренного ст. 187 УК РФ, преступники приискивают средства, с помощью которых возможно добыть конфиденциальную информацию о банковских счетах юридических, физических лиц и индивидуальных предпринимателей, а также изготавливают инструменты для осуществления неправомерного оборота средств платежей².

§ 5. Тактика производства отдельных следственных действий при расследовании преступлений, связанных с неправомерным оборотом средств платежей

Расследование любого преступления предполагает проведение комплекса отдельных следственных действий, направленных на получение доказательств совершенного события и причастности к нему конкретного лица или круга лиц. Любое расследование, в том числе и по преступлениям, квалифицированным по ст. 187 УК РФ, планируется в зависимости от сложившейся первоначальной следственной ситуации, которая в дальнейшем может меняться с учетом установленных обстоятельств и полученной информации.

Какие следственные действия необходимо провести в той или иной сложившейся ситуации, следователь определяет самостоятельно. По преступлениям, связанным с незаконным оборотом средств платежей, в предыдущих параграфах уже приведен перечень следственных действий и мероприятий, рекомендуемых для производства в рамках расследования. Некоторые из следственных действий, проводимых

¹ См., напр.: Приговор Советского районного суда г. Ростова-на-Дону от 25.05.2019 по уголовному делу № 1-206/19. URL: <https://www.consultant.ru> (дата обращения: 12.10.2023).

² См.: 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: сб. матер. Орел: Орловский юридический институт Министерства внутренних дел Российской Федерации имени В. В. Лукьянова, 2018. С. 20–26.

по рассматриваемому составу преступления, обладают определенной спецификой и тактическими особенностями, в связи с чем требуют дополнительного рассмотрения.

Допрос подозреваемого. Допрос, как и любое следственное действие, предполагает три этапа его проведения. Первый этап подготовительный, второй рабочий и третий заключительный.

На подготовительном этапе следователь должен учитывать два исхода событий, в которых может пройти допрос подозреваемого, это бесконфликтная обстановка, когда подозреваемый дает правдивые показания, готов изобличить всех соучастников преступления и идет на сотрудничество со следствием, и конфликтная, когда подозреваемый, как правило, отказывается от дачи показаний либо дает ложные показания, специально вводит следствие в заблуждение с целью избежания или смягчения уголовного наказания. Бесконфликтная обстановка является достаточно благоприятным обстоятельством, которое требует менее трудозатрат и действий, чем конфликтная. Кроме этого, в процессе допроса обстановка может измениться, то есть из конфликтной перейти в процесс бесконфликтной, в большинстве случаев это напрямую зависит от следователя, от его информированности по обстоятельствам преступления, умения нивелировать доказательствами, поэтому, чтобы направить ход допроса в ту сторону, которая будет более благоприятной, следователь должен хорошо к нему подготовиться. Необходимо досконально изучить все материалы уголовного дела, проанализировать имеющиеся доказательства с целью дальнейшего представления подозреваемому для опровержения его ложных показаний, составить список вопросов, которые подлежат выяснению в ходе допроса. При допросе подозреваемого по рассматриваемым видам преступлений выяснению подлежат, как правило, следующие обстоятельства:

- анкетные данные, характеризующие личность подозреваемого (где живет, с кем живет, род деятельности, вид и источники дохода, совершал ли ранее преступления, имеет ли заболевания, их степень и т. д.);

- имеются ли у него какие-либо специальные навыки в области компьютерных технологий, изготовления платежных средств, документов, если да, то когда и как он их приобрел;

– имеются ли знакомые в банках, кредитных, торговых организациях, уровень знакомства, вид отношений, когда и при каких обстоятельствах познакомились;

– имеются ли у подозреваемого личные банковские расчетные счета, открытые на его имя, если да, то в каких банках, сколько счетов, их вид, суммы денежных средств по остаткам, для каких целей они были открыты, кто ими пользуется, кто имеет к ним доступ;

– имеет ли доступ подозреваемый к счетам, открытым не на его имя, если да, то кому принадлежат эти счета, каким образом он получил к ним доступ и с какой целью;

– с каких технических устройств подозреваемый осуществляет доступ к расчетным счетам;

– анкетные и контактные данные лиц, являющихся соучастниками совершенного преступления, роль каждого в их совершении;

– каким способом ими совершено преступление, используемые технические средства, где, когда и каким образом их приобретали;

– где именно происходила подготовка к совершению преступления, где изготавливали поддельные платежные средства, где хранится оборудование для их изготовления;

– источники получения конфиденциальной информации об организациях, физических лицах и их расчетных счетах, финансовых оборотах, которые явились объектами преступной деятельности;

– временной промежуток, потребовавшийся для совершения преступления, от самого начала до обналичивания денежных средств;

– в какой момент возник корыстный умысел, что явилось основанием для совершения преступления, как выбиралась жертва, по каким критериям;

– сколько всего аналогичных преступлений им лично или в соучастии было совершено, какая сумма хищений по каждому эпизоду, каким образом распорядился похищенными денежными средствами.

Кроме этого, в ходе подготовки к допросу подозреваемого следователь выбирает наиболее удобное для него место и время, как правило, это кабинет следователя, так как на своем рабочем месте он будет чувствовать себя в большей безопасности, чем в каком-либо другом месте. Заранее нужно изучить личность подозреваемого, его судимости, круг общения, род занятий, спортивные навыки, привычки, физическое, интеллектуальное развитие, получить характеристику с места жительства от соседей для понимания, с кем придется

работать, чтобы выбрать соответствующую тактику поведения и в определенных случаях принять меры безопасности.

Следующий этап допроса – рабочий, характеризуется непосредственно уже самим процессом общения следователя с подозреваемым, целью которого является установление истины по делу и максимально исчерпывающей информации о механизме совершения преступления и лицах, к нему причастных. Результат данного этапа будет зависеть от линии и позиции, занятой подозреваемым, а также тактических приемов, которые использует следователь для установления истины и разоблачения лжи. Допрос подозреваемого в основном всегда проходит в присутствии его защитника, поэтому все действия и тактические приемы, которые может использовать следователь в процессе допроса, должны соответствовать уголовно-процессуальному законодательству Российской Федерации и не нарушать прав его участников. Тактические приемы следователь использует, как правило, в конфликтной ситуации, поэтому в зависимости от занятой подозреваемым позиции следователь смотрит на поведение допрашиваемого и предпринимает меры к его изменению. При отказе подозреваемого давать показания, в зависимости от настроения допрашиваемого, рекомендуется прием – налаживание психологического контакта, то есть простая беседа без протокола о жизни, семье, следователь может рассказать о себе, своем жизненном пути, ненавязчиво поинтересоваться образом жизни подозреваемого, объяснить свою позицию по поводу преступления, тем самым расположив подозреваемого к себе. Ни в коем случае нельзя переходить на личности, унижать достоинство допрашиваемого, показывать свой приоритет, высказывать угрозы, это может, наоборот, усугубить ситуацию, подозреваемый может отказаться от общения. В ситуации, когда подозреваемый дает показания, не соответствующие действительности, следователь с целью выявления лжи может задать провокационные или неожиданные вопросы, которые введут допрашиваемого в заблуждение, поэтому очень важно, чтобы следователь хорошо владел уже имеющейся информацией в деле. Стоит также обратить внимание на невербальные признаки, выдающие допрашиваемого, которые он не может контролировать (жесты, мимика, потоотделение, заикание, долгое раздумье, волнение, покраснение и т. д.). Еще одним тактическим приемом является предъявление доказательств, имеющихся в деле, прямо или косвенно указывающих

на причастность допрашиваемого к преступлению (видеозаписи, заключения экспертиз, допросы иных лиц и др.), и попросить пояснений подозреваемого по этим доказательствам.

Обязательным условием при проведении допроса подозреваемого является разъяснение ему окончательного исхода по делу при вынесении приговора судом в случае, если он даст правдивые показания, пойдет на сотрудничество со следствием и окажет помощь в выявлении всех участников совершенного преступления, что будет являться обстоятельством, смягчающим наказание, и будет учитываться судом при вынесении приговора; в противоположной ситуации он может получить максимальное наказание.

Еще один тактический прием – фиксация хода проведения допроса с применением видео- или аудиозаписи. Данное мероприятие помогает следователю избежать в дальнейшем отказа подозреваемого от дачи своих показаний либо изменения показаний, ссылок на давление со стороны сотрудников правоохранительных органов. Кроме этого, использование записывающих устройств дисциплинирует участников уголовного судопроизводства как со стороны обвинения, так и со стороны защиты, поскольку пресекает соблазн нарушения хода следственного действия и прав его участников¹.

Третий этап проведения данного следственного действия – фиксация результата допроса. На данном этапе следователь составляет протокол, предъявляет его для ознакомления подозреваемому и его защитнику, если использовалась видеозапись, то она обязательно просматривается всеми участниками, в протоколе об этом делается отметка и даются пояснения подозреваемого и защитника о наличии или отсутствии дополнений, нарушений, все участники следственного действия подписывают протокол, а диск с видео- или аудиозаписью следователь упаковывает и приобщает к протоколу.

Следственный осмотр. В классической криминалистике следственные осмотры принято подразделять на несколько видов в зависимости от объекта осмотра:

- осмотр места происшествия;
- осмотр участков местности и помещений, не являющихся местом происшествия;

¹ См.: Родивилина В. А., Машков С. А., Зубенко Е. В. Изобличение лжи при производстве следственных действий // Криминалистика: вчера, сегодня, завтра: науч. журн. 2019. № 2 (10). С. 39–45.

- осмотр жилища;
- осмотр предметов;
- осмотр документов;
- осмотр трупа;
- освидетельствование.

По преступлениям, предусмотренным ст. 187 УК РФ, важны только осмотр места происшествия и осмотр предметов и документов.

Местами происшествия по рассматриваемым составам преступлений будут являться¹:

- место изготовления поддельных средств платежа или иных распорядительных документов на проведение неправомерной финансовой операции;
- место выпуска неправомерно изготовленных средств платежей или иных документов (банки, кредитные организации);
- место, где осуществлялось неправомерное декодирование конфиденциальной информации реального держателя платежного средства;
- место перевода, обналичивания денежных средств, полученных путем неправомерного оборота средств платежей.

В своих высказываниях П. В. Малышкин² обращает внимание на то, что «если задержание подозреваемого в совершении преступления происходило в момент изготовления, приобретения, хранения, транспортировки с целью использования или сбыта, а также сбыта поддельных платежных (кредитных либо расчетных) пластиковых карт, то осматривается с соблюдением всех криминалистических правил и рекомендаций производственное (жилое или подсобное) помещение; а также имеющееся оборудование, инструменты, материалы и заготовки поддельных платежных (кредитных либо расчетных) пластиковых карт»³.

¹ См.: Шигуров А. В. Проблемы регулирования порядка проведения следственных действий, сопровождающихся изъятием электронных носителей информации // Библиотека криминалиста: науч. журн. 2013. № 5 (10). С. 135–140.

² См.: Малышкин П. В. Особенности тактики производства следственных действий на первоначальном этапе расследования, изготовления, хранения, транспортировки и сбыта поддельных платежных пластиковых карт // Мир науки и образования. 2017. № 1 (9). С. 4.

³ Малышкин П. В. Особенности тактики производства следственных действий на первоначальном этапе расследования, изготовления, хранения, транспортировки и сбыта поддельных платежных пластиковых карт // Мир науки и образования. 2017. № 1 (9). С. 7.

В ходе осмотра места происшествия необходимо использовать специальные тактические приемы, дающие возможность наиболее полно обнаружить, зафиксировать и изъять все возможные следы преступления. Как и в предыдущем рассмотренном следственном действии, осмотр делится на три этапа: подготовительный, рабочий и заключительный.

На подготовительном этапе следователь выясняет особенности места, куда предстоит выезд, собирает необходимые средства для осмотра и упаковки следов преступной деятельности, инструктирует участников осмотра об их действиях на месте происшествия.

В процессе рабочего этапа основная задача следователя – обнаружить, зафиксировать, изучить и изъять в максимальном количестве все следы преступления, которые могут быть оставлены преступником. Конечно, в этом следователю должен помогать специалист, так как данные преступления обладают особой спецификой и требуют определенных специальных знаний, которых у следователя, возможно, не имеется.

Для получения наиболее высокого результата осмотра рекомендуется использовать такие тактические приемы, как эксцентрический, концентрический или линейный. Эксцентрический прием – это осмотр от центра к периферии. Концентрический – это осмотр от периферии к центру. Как правило, они используются в помещении. Если в помещении несколько комнат, то необходимо определить последовательность осмотра комнат и использовать один из наиболее подходящих приемов. Они помогают соблюдать последовательность изучения обстановки в помещении и не пропустить мелкие следы. Линейный прием чаще всего используется на открытой местности, где сначала следователю необходимо определить границы осмотра и затем двигаться параллельно линиям от одного края к другому.

В ходе осмотра следует обращать внимание на наличие: оборудования, которое, возможно, могло использоваться при изготовлении пластиковых карт (энкодеры, токены, эмбоссеры и др.); слипов, носителей электронной информации (CD, DVD, Blu-ray – диски, жесткие диски, флеш-карты и др.); остатков от средств ламинирования, белого пластика; бумажных носителей информации с данными предполагаемых жертв, планируемыми финансовыми операциями, их контактами; устройств для незаконного считывания и декодирования конфиденциальной информации с платежных средств пользователей.

Третий этап заключается в фиксации результатов осмотра, которая осуществляется путем занесения обстановки, обнаруженной на месте происшествия, и следов преступной деятельности в протокол, составлении схем, фототаблиц. В протоколе указываются вид осматриваемого объекта или участка, его особенности, месторасположение, а также все предметы, находящиеся на нем, предположительно применяемые при совершении преступления. Указываются их вид, цвет, размеры, модель, марка, наличие серийных номеров, состояние, количество и другие индивидуализирующие признаки. Данные предметы обязательно изымаются с места происшествия и подлежат более детальному осмотру в кабинете у следователя.

Осмотр предметов и документов – это следственное действие, которое проводится следователем в служебном кабинете и какой-то специально подготовки не требует. С учетом соблюдения всех процессуальных требований следователь производит осмотр предметов и документов, изъятых с места происшествия, результаты которого фиксирует в протоколе.

При осмотре пластиковых банковских карт в протоколе указываются:

- размеры карты;
- ее дизайн (цвет, узор);
- вид карты (Мир, VISA, Mastercard);
- наличие надписей и эмблем, идентифицирующих банк-эмитент;
- наличие реквизитов владельца, каким способом они нанесены, эмбоссированным или простые надписи (имя и фамилия, номер карты, срок действия);
- наличие RFID-метки и магнитной полосы, их размеры (длина, ширина);
- наличие иных надписей и контактных данных банка-эмитента;
- наличие CVV-кода и подписи владельца;
- наличие значка Wi-Fi и место его расположения.

При осмотре слипов, изъятых в торговых организациях, в протоколе указываются: вид слипа, размер, вид надписей, их цвет, наименование торговой организации, адрес, дата и время проведенной операции, количество и вид товара, его стоимость, общая сумма оплаты, наличие скидки, использование бонусов, номер бонусной карты, код товара, сумма НДС, ФИО кассира, наличие QR-кода, наличие подписей и печатей.

Осматривая предметы и документы, не следует забывать об общих криминалистических правилах, которые важно соблюдать, чтобы не уничтожить и не повредить вещественное доказательство или следы, имеющиеся на нем. Осмотр необходимо производить в перчатках, документы не сгибать, поверхность стола, на котором производится осмотр, должна быть чистая, чтобы исключить вероятность загрязнения. Обращаться с вещественным доказательством требуется бережно, аккуратно, а по окончании осмотра упаковать в чистую упаковку, исключающую возможность доступа посторонних лиц¹.

Выемка и обыск. Данное следственное действие по преступлениям, связанным с неправомерным оборотом средств платежей, проводится у потерпевших, подозреваемых, в торговых, кредитных организациях, банках с целью изъятия предметов и документов, имеющих значение для дела. Такими предметами и документами чаще всего выступают: выписки по расчетным счетам клиентов банка, слипы в торговых организациях, платежные документы, пластиковые карты, оборудование для изготовления карт, устройства для несанкционированного считывания конфиденциальной информации с карт, POS-терминалы, банкоматы.

Обыск и выемка, согласно законодательству Российской Федерации, производятся на основании достаточных данных, имеющихся в распоряжении следователя для проведения данного следственного действия, и постановления следователя или суда.

Приведем обобщенный список предметов и документов, подлежащих выемке, в зависимости от организации, в которой она будет производиться:

1. Банки-эмитенты (эквайеры) пластиковых карт. Объектами выемки будут являться:

- а) стоп-листы с перечнем похищенных или утраченных пластиковых карт;
- б) кредитное досье, в котором содержатся данные о подлинном держателе карты;
- в) подлинники слипов или их заверенные копии;

¹ См.: Малышкин П. В. Особенности тактики производства следственных действий на первоначальном этапе расследования изготовления, хранения, транспортировки и сбыта поддельных платежных пластиковых карт // Мир науки и образования. 2017. № 1 (9). С. 5.

г) выписки из журналов учетов запросов на авторизацию, по которым устанавливается дата и время совершения оспариваемой операции.

2. При установлении организации, в которой приобреталось оборудование для считывания конфиденциальной информации с пластиковых карт для изготовления поддельных платежных карт, необходимо изъять: кассовые чеки на приобретение товара, документы на проданное оборудование или их копии.

3. В торговых организациях, в которых происходило неправомерное списание денежных средств при оплате товара:

а) копия чека об оплате товара или кассовая лента с POS-терминала;

б) договор с налоговым органом о постановке POS-терминала на учет или его копия;

в) договор с банком-эмитентом об осуществлении приема платежей безналичным способом;

г) акты о проверке торговой организацией на законность ведения финансовых операций;

Обыск проводится в случае, если следователю достоверно не известно о том, где находятся предметы преступной деятельности, похищенное имущество, но есть предположение об их местонахождении.

О. Г. Сумникова в своих исследованиях по мошенничествам, совершенным с использованием пластиковых карт, высказывает точку зрения о месте проведения обыска: «Обыск по уголовным делам данной категории чаще всего проводится в помещении, где зачастую обнаружению и изъятию подлежат следующие объекты: компьютеры, машинные носители информации, банковские карты, терминальные чеки, квитанции, документы, удостоверяющие личность, сотовые телефоны, почтовые извещения и конверты и т. д.; объектами поиска при обыске должны быть и черновые записи, блокноты, записные книжки, в которых содержится важная информация для дела»¹. Ученый отмечает, что данная информация может быть использована в дальнейшем при доказывании вины подозреваемого (обвиняемого).

¹ Сумникова О. Г. Тактика производства отдельных следственных действий при расследовании мошенничества с использованием платежных карт // Научный вестник Орловского юридического института МВД России имени В. В. Лукьянова. 2015. № 4 (65). С. 101–104.

Специфика обыска по преступлениям рассматриваемой категории выражается в особенностях предмета, подлежащего поиску, так как это будет не только оборудование, которое тяжело спрятать из-за его больших размеров, но и пластиковые карты, бумажные документы, которые, наоборот, очень компактны и легко конспирируются. Поэтому в процессе обыска рекомендуется использовать следующие тактические приемы:

1. Последовательное обследование помещения, то есть здесь не стоит выборочно искать интересующие следствие предметы и документы, так как можно пропустить наличие тайников.

2. Встречное обследование, при котором два сотрудника полиции идут навстречу друг другу, внимательно исследуя все объекты.

3. Сравнение однородных объектов – используется с целью выявления различий в толщине стен, книг, глубине шкафов и т. д.

4. Словесная разведка. Целью данного приема является разговор между двумя обыскивающими лицами, которые обсуждают между собой, где лучше им осуществить поиск, и смотрят на реакцию обыскиваемого, чтобы понять, находится ли в оговоренном месте что-то или нет. То есть подозреваемый может начать нервничать, придумывать уловки для отвлечения внимания от этого места сотрудников правоохранительных органов.

Результаты обыска фиксируются в соответствующем протоколе, где указываются:

- место обнаружения того или иного предмета (документа), представляющего интерес для следствия;
- краткие характеристики этого предмета (документа).

Если обнаружена банковская карта, в протоколе указывается следующее:

- вид карты (Мир, VISA, Mastercard);
- наличие надписей и эмблем, идентифицирующих банк-эмитент;
- наличие реквизитов владельца (имя и фамилия, номер карты, срок действия);
- наличие RFID-метки и магнитной полосы;
- наличие CVV-кода и подписи владельца;
- наличие значка Wi-Fi и место его расположения.

Все предметы и документы изымаются с места обыска, упаковываются соответствующим образом по общепринятым правилам и доставляются на рабочее место следователя.

Следственный эксперимент. При расследовании преступлений, предусмотренных ст. 187 УК РФ, следственный эксперимент целесообразно проводить в случае, если имеются сомнения в показаниях, данных допрошенным лицом. Например, подозреваемый говорит, что он самостоятельно приобрел оборудование для считывания конфиденциальной информации с пластиковых банковских карт их законных держателей, похитил указанную информацию и изготовил поддельные пластиковые карты. Следователь для проверки правдивости данных показаний может провести следственный эксперимент, в ходе которого будет установлено, действительно ли подозреваемый обладает достаточными умениями и навыками и может изготовить пластиковую карту банка самостоятельно на имеющемся оборудовании и в тех условиях, о которых он сообщает. Если результатом следственного эксперимента окажется отсутствие указанных навыков у подозреваемого, это будет говорить о том, что либо он действовал не один, а в составе группы лиц и прикрывает остальных участников преступления, либо по каким-то иным причинам занимается самооговором.

Подводя итог рассмотрению следственных действий, проводимых в рамках предварительного расследования по преступлениям, связанным с неправомерным оборотом средств платежей, хотелось бы акцентировать внимание на том, что приемы, которые выберет следователь в ходе производства следственного действия, напрямую зависят от сложившейся ситуации, а для получения наиболее полного и благоприятного результата для следствия обязательно требуется тщательная подготовка к проведению следственного действия. В ином случае может быть утеряна важная информация и разглашены данные предварительного расследования.

§ 6. Особенности использования специальных знаний при расследовании преступлений, связанных с неправомерным оборотом средств платежей

Следственная практика при расследовании преступлений, предусмотренных ст. 187 УК РФ, испытывает определенные сложности ввиду того, что данные преступления являются относительно новыми, поэтому у следователей еще недостаточно четко сложилось понимание отграничения составов преступных посягательств, не выработаны

алгоритмы действий в сложившихся следственных ситуациях и отсутствуют специальные знания в необходимых случаях.

Проведение следственных действий и процессуальных мероприятий при расследовании преступлений, связанных с неправомерным оборотом средств платежей, требует использования специальных знаний в области компьютерной техники и технологий, финансовых операций, документооборота, технико-криминалистических исследований и др., так как данные преступления совершаются непосредственно с применением специального оборудования и документов. На эти же признаки в своем научном исследовании указывает Ю. Б. Имаева: «Специфика применения специальных знаний по данной категории дел обусловлена следующим обстоятельством: обнаружение многих документов на электронных носителях возможно только с использованием компьютерной техники, а неквалифицированное ее использование может привести к уничтожению информации, имеющей доказательственное значение, если не будет соблюден порядок обращения с носителем информации»¹. Формы специальных знаний, которые необходимы для установления определенных обстоятельств по делу, могут быть различны. В классической криминалистике такие знания подразделяют на процессуальные и непроцессуальные. К процессуальным знаниям относят использование помощи специалиста при проведении следственных действий, например привлечение криминалиста для помощи в изъятии следов преступления, техники в изъятии компьютерных устройств, компьютерщика для получения информации из электронных средств, таких как персональный компьютер, ноутбук, планшет, телефон. В качестве специалиста приглашают видеооператора для проведения видеосъемки хода следственного действия и т. д. Особый вид использования специальных знаний является назначение судебных экспертиз, результатом которых является заключение эксперта в той или иной области, которое может стать основой обвинения по уголовному делу. Непроцессуальная форма использования специальных знаний предполагает помощь, оказываемую специалистом, имеющим знания в той или иной области, следователю. Это могут быть консультации перед

¹ Имаева Ю. Б. Особенности расследования хищений, совершенных с использованием кредитных и расчетных карт: дис. ... канд. юрид. наук. Уфа, 2015. С. 166.

допросом, назначением экспертиз, следственным осмотром и другими мероприятиями. Поэтому вид знаний, которые необходимо использовать следователю в ходе расследования преступлений, связанных с незаконным оборотом средств платежа, будет напрямую зависеть от следственной ситуации и имеющейся в распоряжении следователя информации. Д. Н. Гушин в этом смысле обращает внимание на то, что «в настоящее время стоит отметить случаи появления „суперподделок“, по качеству изготовления которых можно предположить, что они изготовлены каким-либо государством либо при его поддержке, поскольку их изготовление требует использования оборудования металлографической печати, цена которого очень высока. Эксперты выявляют случаи, когда такие „суперподделки“ изготовлены на таком материале и при помощи такой специальной краски, реализация которых происходит исключительно национальным банком»¹.

Как уже было отмечено выше, одним из самых распространенных способов, используемых преступниками при совершении рассматриваемых преступлений, является подделка платежных средств и документов, поэтому для установления их подлинности и поддельности необходимы специальные знания в области технико-криминалистического исследования документов².

Остановимся более подробно на особенностях назначения данных экспертиз. Л. И. Слепнева указывает, что «к объектам экспертизы пластиковых карт относятся непосредственно сами пластиковые карты, слипы, оборудование (полиграфические установки, принтеры, эмбоссеры и прессы для горячего тиснения), а также материалы дела (чаще всего протоколы осмотра места преступления), которые необходимы эксперту для ответа на поставленные перед ним вопросы»³. Как отмечено автором, технико-криминалистическому исследованию подлежат не только пластиковые карты, слипы, платежные

¹ Гушин Д. Н. К вопросу о необходимости развития системы научно-методического обеспечения расследования преступлений в сфере неправомерного оборота средств платежей // Юрист-Правоведь. 2019. № 2 (89). С. 153–157.

² См.: Берова Д. М., Гаужаева В. А. Применение специальных познаний по преступлениям, связанным с использованием пластиковых карт // Пробелы в российском законодательстве. 2015. № 3. С. 136–139.

³ Слепнева Л. И. Некоторые особенности судебно-экспертного исследования пластиковых платежных средств // Вестник Университета имени О. Е. Кутафина. 2019. № 5 (57). С. 121–131.

документы, но и оборудование, которое использовалось для их изготовления, так как вопросы технического характера также могут решаться в рамках данного исследования. Возможности данного экспертного исследования позволяют решить следующие вопросы:

- каким способом изготовлен платежный документ или платежное средство, представленное на исследование, по правилам государственного стандарта или нет;

- какие технические средства использовались при изготовлении платежного документа или платежного средства, представленного на исследование, каковы их характеристики и особенности;

- свойство красящего вещества и давность его нанесения на платежный документ или платежное средство, представленное на исследование;

- каким способом внесены изменения в документ, представленный на исследование, какие технические средства при этом использовались, их особенности;

- на одном и том же оборудовании изготовлены платежные документы или платежные средства, представленные на исследование, какие признаки на это указывают.

Следующая, не менее важная по своему значению и не менее распространенная экспертиза по своей востребованности, назначаемая по рассматриваемым преступлениям, – компьютерная экспертиза. При этом данная экспертиза в разных ведомствах имеет некоторые отличия в своем названии. Так, согласно приказу МВД России от 29.06.2005 № 511¹ данная экспертиза называется «компьютерная». На основании приказа Минюста России от 20.04.2023 № 72²

¹ См.: Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации (вместе с Инструкцией по организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации, Перечнем родов (видов) судебных экспертиз, производимых в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации): приказ МВД России от 29.06.2005 № 511 (ред. от 27.09.2023). URL: <https://www.consultant.ru> (дата обращения: 12.10.2023).

² См.: Об утверждении перечня родов (видов) судебных экспертиз, выполняемых в федеральных бюджетных судебно-экспертных учреждениях Минюста России, и перечня экспертных специальностей, по которым предоставляется право самостоятельного производства судебных экспертиз в федеральных бюджетных судебно-экспертных учреждениях Минюста России: приказ Минюста России от 20.04.2023 № 72. URL: <https://www.consultant.ru> (дата обращения: 12.10.2023).

данная экспертиза называется «компьютерно-техническая». Приказом ФСБ РФ от 23.06.2011 № 277¹ данной экспертизе дано название «компьютерная», а вот Следственный комитет РФ поддерживает позицию Минюста России и называет данную экспертизу «компьютерно-техническая»². Ученые-криминалисты предлагают несколько классификаций данной экспертизы, но самая удачная принадлежит Е. Р. Россинской³, которая привела следующий перечень:

а) судебная аппаратно-компьютерная экспертиза – проводится для исследования самого аппарата, на котором или с помощью которого совершалось преступление, а также его составляющих (принтер, сканер, электронные носители информации);

б) судебная программно-компьютерная экспертиза – подразумевает исследование программного обеспечения, установленного на техническое устройство, его вида, операционной системы, выполняемых функций и т. д.;

в) судебная информационно-компьютерная экспертиза (данных) – исследует содержащуюся на техническом устройстве информацию, созданную пользователем или внесенную посредством использования внешних источников, анализирует ее и дает оценку ее назначению;

г) судебная компьютерно-сетевая экспертиза – целью исследования которой является обнаружение соединений между несколькими техническими устройствами, их функционирование в общей сети.

Для проведения компьютерной экспертизы эксперту на исследование представляется обязательно весь компьютер в сборе (монитор, процессор, клавиатура, мышка), ноутбук, смартфон, планшет.

¹ См.: Об организации производства судебных экспертиз в экспертных подразделениях органов федеральной службы безопасности: приказ ФСБ РФ от 23.06.2011 № 277 (с изм. и доп.). URL: <https://www.consultant.ru> (дата обращения: 12.10.2023).

² См.: Об утверждении Порядка определения, пересмотра уровня квалификации и аттестации экспертов федерального государственного казенного учреждения «Судебно-экспертный центр Следственного комитета Российской Федерации» на право самостоятельного производства судебных экспертиз: приказ Следственного комитета РФ от 24.07.2020 № 77. URL: <https://www.consultant.ru> (дата обращения: 12.10.2023).

³ См.: Россинская Е. Р. Проблемы использования специальных знаний в судебном исследовании компьютерных преступлений в условиях цифровизации // Вестник Университета имени О. Е. Кутафина. 2019. № 5 (57). С. 31–44.

По преступлениям, предусмотренным ст. 187 УК РФ, в рамках проведения компьютерной экспертизы могут решаться следующие вопросы:

- вид, модель технического устройства, представленного на исследование, его технические характеристики;
- в каком состоянии (рабочем или нет) находится техническое устройство, представленное на исследование;
- какое программное обеспечение, с какой операционной системой установлено на техническое устройство, представленное на исследование;
- каков объем жесткого диска технического устройства, представленного на исследование, объем занятого и свободного места;
- какие программы и сервисы установлены на техническом устройстве, представленном на исследование, их назначение;
- имеются ли скрытые программы, установленные на техническом устройстве, представленном на исследование;
- удалялась ли какая-либо информация с технического устройства, представленного на исследование, если да, то какая, когда и возможно ли ее восстановить;
- имеется ли к данному техническому устройству, представленному на исследование, возможность удаленного доступа, если да, то с каких устройств;
- синхронизировано ли техническое устройство, представленное на исследование, с другими устройствами, если да, то с какими и возможно ли получить с них информацию.

Объектами исследования компьютерных экспертиз также являются пластиковые банковские карты, в результате исследования которых возможно установить:

- какая информация содержится в магнитной полосе пластиковой карты и памяти ее микропроцессора;
- каким способом осуществлялась запись информации на магнитную полосу и RFID-метку карты, представленной на исследование;
- подвергалась ли данная информация несанкционированному изменению;
- соответствует ли информация, записанная на магнитной полосе пластиковой карты, представленной на исследование, ее внешним данным, имеющимся на самом пластике;

– является ли пластиковая карта, представленная на исследование, рабочей и может ли быть использована для проведения финансовых транзакций при контакте с терминалами и банкоматами.

При расследовании незаконного оборота средств платежей также назначается судебная трасологическая экспертиза. Объектами данного исследования являются пластиковые банковские карты и оборудование, предназначенное для их изготовления. На разрешение эксперта ставятся следующие вопросы:

– с помощью какого устройства и каким способом была изготовлена банковская пластиковая карта, представленная на исследование;

– использовалось ли оборудование, предоставленное на исследование, для изготовления пластиковой банковской карты, представленной на исследование;

– какова последовательность следов, образованных на банковской пластиковой карте, и оставлены ли они оборудованием, представленным на исследование, или иными устройствами.

Еще одним видом экспертиз, назначаемых достаточно часто при расследовании незаконного оборота средств платежей, является судебная почерковедческая экспертиза.

Данная экспертиза назначается по пластиковой карте или иным платежным документам, распоряжениям, на которых имеется подпись держателя карты или распорядителя. Кроме этого, также на исследование эксперту представляются заявления об открытии расчетного счета, с образцом подписи лица, открывшего счет, а также иные документы, имеющиеся в банке, с подписью проверяемого лица. Поэтому для установления лица, подписавшего платежное средство, необходимы специальные знания в области почерковедения. В рамках данной экспертизы можно установить:

– выполнена ли подпись на платежном средстве, представленном на исследование, его владельцем;

– в каком состоянии находилось лицо в момент выполнения подписи на платежном средстве, представленном на исследование;

– какой рукой, правой или левой, была выполнена подпись на платежном средстве, представленном на исследование;

– какие особенности отразились в подписи, выполненной на платежном средстве, представленном на исследование.

В качестве заключительной экспертизы, проводимой при расследовании незаконного оборота средств платежей, назовем одну из самых распространенных и назначаемых практически по всем уголовным делам, независимо от состава преступления, – это дактилоскопическая экспертиза. Объектами исследования данной экспертизы могут быть абсолютно любые предметы и документы, с которыми мог соприкасаться преступник при подготовке и совершении преступления, содержащие на себе отпечатки пальцев рук. Например, пластиковая платежная карта банка, слипы, оборудование, предназначенное для несанкционированного считывания конфиденциальной информации с банковских карт, устройства, используемые для изготовления поддельных пластиковых карт, платежные POS-терминалы, банкоматы, распорядительные документы на бумажном носителе, компьютерные средства, используемые для осуществления незаконных транзакций, ноутбуки планшеты, смартфоны, жесткие диски, флеш-накопители и многое другое. В рамках производства данной экспертизы можно установить:

- имеются ли на объектах, представленных на исследование, отпечатки пальцев рук, если да, то пригодны ли они для идентификации;
- пальцем какой руки оставлены отпечатки на объектах, представленных на исследование;
- имеются ли индивидуальные признаки на отпечатках пальцев рук, обнаруженных на объекте, представленном на исследование, если да, то каков их характер и особенности;
- принадлежат ли отпечатки пальцев, обнаруженные на объекте, представленном на исследование, гражданину Х., образцы для сравнительного исследования которого представлены.

Предложенный перечень судебных экспертиз, а также вопросов, разрешаемых экспертом, не является исчерпывающим и подлежит корректировке в зависимости от сложившейся следственной ситуации и наличия объектов, подлежащих исследованию. Привлечение лиц, обладающих специальными знаниями в определенных областях, может зависеть от сложности расследуемого преступления и быть индивидуальным для каждого следственного действия.

ЗАКЛЮЧЕНИЕ

Анализ нормативных правовых актов и судебно-следственной практики позволил выявить особенности квалификации преступлений, связанных с незаконным оборотом средств платежей.

Проблемы, возникающие у следователей при расследовании деяний, предусмотренных ст. 187 УК РФ, заключаются в определении предмета преступного посягательства и особенностей его использования в механизме совершения преступлений, так как от этого напрямую зависит правильная квалификация содеянного. В данной работе приведены признаки субъекта, объекта преступной деятельности по указанным преступлениям, рассмотрены субъективная и объективная стороны, разобраны формы вины участников.

В рамках анализа вопросов возбуждения уголовного дела приведены поводы и основания возбуждения уголовного дела, влияющие на принятие законного и обоснованного процессуального решения по совершенному деянию, а также перечислены обстоятельства, подлежащие установлению в рамках проведения доследственной проверки. На основании материалов изученных уголовных дел по рассматриваемым преступлениям сформулированы следственные ситуации, возникающие как на этапе возбуждения уголовного дела, так и на первоначальном этапе расследования. Кроме этого, показан алгоритм расследования по каждой из сложившихся следственных ситуаций.

На первоначальном этапе расследования, при планировании мероприятий и следственных действий, необходимых для установления истины по делу, большую роль играет первоначальная информация, имеющаяся в распоряжении следователя, которая составляет комплекс элементов криминалистической характеристики, включающий в свою структуру: предмет преступления, способ совершения преступления, обстановку, механизм слеодообразования, личность потерпевшего и преступника. В данной работе приведена подробная характеристика наиболее важных элементов для преступлений, связанных с неправомерным оборотом средств платежей: предмет преступления и способ совершения. Выявлены их особенности и даны характеризующие признаки. Уделено внимание тактическим особенностям проведения следственных действий и использованию специальных

знаний при расследовании указанных преступлений. Сведения, содержащиеся в данной работе, могут оказать методическую помощь следователям при возникновении проблемных ситуаций и эффективным образом повлиять на повышение качества расследования.

Список рекомендуемой литературы

1. О деятельности по приему платежей физических лиц, осуществляемой платежными агентами : федер. закон от 3 июня 2009 г. № 103-ФЗ (в посл. ред.) // Справ.-правовая сист. «КонсультантПлюс». – URL : <https://www.consultant.ru> (дата обращения: 12.10.2023).

2. О национальной платежной системе : федер. закон от 27 июля 2011 г. № 161-ФЗ (в посл. ред.) // Справ.-правовая сист. «КонсультантПлюс». – URL : <https://www.consultant.ru> (дата обращения: 12.10.2023).

3. Об эмиссии платежных карт и об операциях, совершаемых с их использованием : положение Банка России от 24 декабря 2004 г. № 266-П (в посл. ред.) // Справ.-правовая сист. «КонсультантПлюс». – URL : <https://www.consultant.ru> (дата обращения: 12.10.2023).

4. Васюков, В. Ф. Некоторые элементы криминалистической характеристики преступлений, связанных с неправомерным оборотом средств платежа / В. Ф. Васюков, А. В. Шалыгина // Уголовно-процессуальные и криминалистические проблемы борьбы с преступностью : сб. матер. – Орел : Орловский юридический институт Министерства внутренних дел Российской Федерации имени В. В. Лукьянова, 2018. – С. 20–26.

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

6. Правовое регулирование перевода электронных денежных средств : монография / под ред. В. Б. Гольцова, Н. М. Голованова ; СПбГАСУ. – Санкт-Петербург, 2019. – 272 с. – ISBN 978-5-9227-0989-7.

7. Фирсов, Е. П. Расследование изготовления или сбыта поддельных денег или ценных бумаг, кредитных либо расчетных карт и иных платежных документов : монография / Е. П. Фирсов. – Москва : Юрлитинформ, 2004. – 160 с. – ISBN: 5-93295-109-5.

Учебное издание

Решняк Ольга Александровна
Лихолетов Александр Александрович
Евлущина Дарья Николаевна

Особенности квалификации
и расследования преступлений,
предусмотренных статьёй 187
Уголовного кодекса
Российской Федерации

Учебное пособие

Редактор *Н. Ф. Руденко*
Компьютерная верстка *Ю. В. Сиволапова*
Дизайн обложки *А. Н. Улизко*

Волгоградская академия МВД России.
400075, Волгоград, ул. Историческая, 130.

Редакционно-издательский отдел.
400005, Волгоград, ул. Коммунистическая, 36.

Подписано в печать 28.02.2024. Формат 60х84/16. Бумага офсетная.
Гарнитура Times New Roman. Физ. печ. л. 3,75. Усл. печ. л. 3,48.
Тираж 100 экз. Заказ № 7.

ОПиОП РИО ВА МВД России. 400005, Волгоград, ул. Коммунистическая, 36.