Министерство внутренних дел Российской Федерации
Барнаульский юридический институт МВД России

А.А. Лукьянова

ДОКАЗЫВАНИЕ И ЮРИДИЧЕСКАЯ ОЦЕНКА ДЕЙСТВИЙ ЛИЦА, СОВЕРШИВШЕГО ХИЩЕНИЕ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА

Учебное пособие

Барнаул
2023

УДК 343.985.7:343.7
ББК 67.410.104я73+67.52я73
Л 844

Рецензенты:

заместитель начальника отдела следственной части Главного следственного управления ГУ МВД России по Алтайскому краю *И.М. Шаталин*;
заместитель начальника кафедры уголовного процесса Восточно-Сибирского института МВД России канд. юрид наук, доцент *В.Н. Гапонова*.

Лукьянова, Алина Александровна.

Л 844 Доказывание и юридическая оценка действий лица, совершившего хищение с использованием электронных средств платежа : учебное пособие / А.А. Лукьянова. – Барнаул : Барнаульский юридический институт МВД России, 2023. – 48 с.

ISBN 978-5-94552-545-0

Учебное пособие посвящено уголовно-процессуальным особенностям доказывания по уголовным делам о хищениях с использованием электронных средств платежа, специфике квалификации преступления и юридической оценки действий лица, совершившего такое хищение.

Пособие предназначено для обучающихся образовательных организаций МВД России, сотрудников органов предварительного расследования.

УДК 343.985.7:343.7
ББК 67.410.104я73+67.52я73

ISBN 978-5-94552-545-0

Введение

Глобальные научно-технические достижения последних десятилетий, развитие новейших отраслей человеческого знания, цифровизация многих социальных сфер уже не воспринимаются как нечто неординарное. Современные технологии прочно вошли в повседневную жизнь человека и закономерно оказывают на нее влияние. Сложно представить себе среднестатистического россиянина, у которого не было бы собственного банковского счета, пластиковой карты, личного кабинета на портале государственных услуг РФ, мобильного банка, аккаунта в социальных сетях и других интернет-площадках.

Реализация мер, направленных на снижение уровня преступности в экономической сфере, предупреждение и пресечение правонарушений и преступлений, совершаемых с использованием информационно-коммуникационных технологий, является одним из стратегических национальных приоритетов Российского государства[1].

В этом контексте все более актуальными становятся вопросы защиты граждан, общества и государства от угроз криминального характера, которые сообразно техническому прогрессу активно видоизменяются. Усложняется механизм совершения преступления, появляются малоизученные в юридическом аспекте способы и средства, используемые злоумышленниками для сокрытия своих преступных намерений и обеспечивающие достижение преступного результата. Существенно возрастает вред, причиняемый преступлениями, в механизме совершения которых присутствуют цифровые элементы.

Не является исключением и такая категория преступлений против собственности, как хищения чужого имущества. Карманные кражи стали заменять хищения с банковского счета в отношении электронных денежных средств. Мошенничества «переквалифицировались» в сферу компьютерной информации, на использование методов социальной инженерии. Изъятие чужого имущества из владения все чаще происходит посредством электронных

[1] О Стратегии национальной безопасности Российской Федерации [Электронный ресурс]: Указ Президента РФ от 02.07.2021 № 400. Доступ из справ.-правовой системы «КонсультантПлюс».

средств платежа с использованием информационно-коммуникационных технологий и электронных носителей информации.

Ожидаемой реакцией законодателя на вызовы преступности, приспособившейся к образу жизни человека в режиме онлайн, стало создание новых мер государственного воздействия. Постепенное реформирование законодательства по пути усиления мер уголовно-правовой охраны, в частности, выразилось в расширении уголовной ответственности, дифференциации новых составов преступлений и квалифицирующих признаков в отношении деяний, совершенных с использованием электронных средств платежа.

Вместе с тем статистические данные о состоянии преступности в России[1] свидетельствуют о следующем. Каждое четвертое преступление из числа зарегистрированных в РФ – преступление, совершенное с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации[2]. При этом почти три четверти из этих преступлений совершаются с использованием сети Интернет – 381,1 тыс.; более трети – средств мобильной связи (213,0 тыс.). Три четверти данных преступлений совершаются путем кражи или мошенничества (371,2 тыс.). Стабильно высоким остается количество таких квалифицированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, как совершенные с использованием или применением расчетных (пластиковых) карт – 127 149, мошенничества с использованием электронных средств платежа (ст. 159.3 УК РФ) – 7288.

Считаем необходимым отметить, что названные преступные деяния обладают высокой степенью латентности. Практика не успевает за развитием современных технологий, которые лица используют при совершении неправомерных действий. Поэтому в процессе расследования уголовных дел всегда возникают трудности, в частности связанные с доказыванием, квалификацией

[1] Отчет ГИАЦ МВД России о состоянии преступности за январь – декабрь 2022 г. URL: https://мвд.рф/ (дата обращения: 10.03.2023).

[2] Всего в 2022 г. в РФ зарегистрировано 1966,8 тыс. преступлений, из них 522,1 тыс. – преступления, совершенные с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 0,8% больше, чем в 2021 г.

преступления и юридической оценкой действий лиц, его совершивших.

В связи с чем учебное пособие закономерно носит прикладной характер, но вместе с тем может использоваться в образовательной деятельности как дополнение к учебному материалу по дисциплинам «Уголовно-процессуальное право (Уголовный процесс)», «Предварительное следствие в органах внутренних дел», «Дознание в органах внутренних дел».

1. Особенности предмета и пределов доказывания хищений, совершенных с использованием электронных средств платежа

Процесс доказывания в уголовном судопроизводстве обретает особенности через предмет доказывания. Являясь фактологической основой для разрешения уголовно-правового спора, принятия процессуального решения, завершающего производство по уголовному делу, предмет доказывания транслитерируется в квалификацию деяния.

О значении предмета доказывания образно писал М.С. Строгович: «Если предмет доказывания отчетливо определен по данному уголовному делу, следователь, прокурор и суд сосредотачивают свое внимание на фактах, действительно имеющих значение для правильного разрешения дела, и не отвлекаются на выяснение фактов, для дела значения не имеющих»[1].

Наличие особенностей предмета доказывания по уголовным делам о хищениях, совершенных с использованием электронных средств платежа, предопределено в первую очередь нестандартной для гуманитарного профиля категорией – «электронное средство платежа».

Так, использование электронных средств платежа как самостоятельный квалифицирующий признак хищения в УК РФ иллюстрирует повышенное внимание законодателя к названной общественно опасной деятельности. Необходимо отметить, что данная правовая категория проникала в российское уголовное право постепенно.

Прошедшая в 2012 г. реформа уголовного законодательства была обусловлена необходимостью создания со стороны государства адекватных уголовно-правовых мер воздействия. Существовавший на тот момент в УК РФ состав мошенничества не в полной мере учитывал особенности тех или иных экономических отношений, а также не позволял обеспечить на должном уровне защиту

[1] Строгович М.С. Курс советского уголовного процесса: в 2 т. Т. 1: Основные положения науки советского уголовного процесса. М.: Наука, 1968. С. 361.

интересов граждан, пострадавших от мошеннических действий[1]. Вследствие чего с принятием федерального закона от 29.11.2012 № 207-ФЗ появились новые составы преступлений, совершенных в форме мошенничеств: с использованием платежных карт (ст. 159.3 УК РФ) и в сфере компьютерной информации (ст. 159.6 УК РФ)[2].

Дальнейшее реформирование уголовного законодательства пошло по пути усиления охраны отношений в платежных системах: расширение уголовной ответственности за неправомерный оборот средств платежей[3] (см. табл. 1), введение нового состава ст. 274.1 УК РФ (неправомерное воздействие на критическую информационную инфраструктуру РФ[4]).

Таблица 1

Изменения, внесенные в диспозицию ч. 1 ст. 187 УК РФ с принятием федерального закона от 08.06.2015 № 153-ФЗ

Редакция диспозиции **ч. 1 ст. 187 УК РФ**, действовавшая до принятия федерального закона от 08.06.2015 № 153-ФЗ	Актуальная редакция диспозиции **ч. 1 ст. 187 УК РФ**
Статья 187. Изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов	**Статья 187. Неправомерный оборот средств платежей** 1. Изготовление, приобретение, хранение, транспортировка в целях

[1] Пояснительная записка к законопроекту № 53700-6 «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации». URL: https://sozd.duma.gov.ru/bill/53700-6 (дата обращения: 10.03.2023).

[2] О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации [Электронный ресурс]: федеральный закон от 29.11.2012 № 207-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

[3] О внесении изменений в статью 187 Уголовного кодекса Российской Федерации [Электронный ресурс]: федеральный закон от 08.06.2015 № 153-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

[4] О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]: федеральный закон от 26.07.2017 № 194-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

1. Изготовление в целях сбыта или сбыт поддельных кредитных либо расчетных карт, а также иных платежных документов, не являющихся ценными бумагами…	использования или сбыта, а равно сбыт поддельных платежных карт, распоряжений о переводе денежных средств, документов или средств оплаты (за исключением случаев, предусмотренных ст. 186 УК РФ), а также электронных средств, электронных носителей информации, технических устройств, компьютерных программ, предназначенных для неправомерного осуществления приема, выдачи, перевода денежных средств…

В 2014-2015 гг. Банком России отмечены значительный рост хищений со счетов клиентов банков, увеличение числа несанкционированных операций, совершенных с использованием систем дистанционного банковского обслуживания, а также тенденция к перемещению интересов «карточных» мошенников из контактной инфраструктуры (банкоматы, материальные носители платежных карт) в более технологичную инфраструктуру дистанционного доступа (системы дистанционного банковского обслуживания, электронные кошельки, интернет- и мобильные транзакции)[1].

Возникшие угрозы криминального характера требовали усиления уголовной ответственности за противоправные действия, которые могли совершать лишь лица, обладающие специальными знаниями и использующие технические средства, что приводило к нарушению не только права собственности, но и банковской тайны. Общественную опасность указанных деяний усиливала специфика способа совершения преступления – использование удаленного доступа к банковскому счету при помощи технических средств, позволяющего лицу оставаться анонимным и совершать преступление из любой точки мира, имея лишь доступ к сети Интернет[2].

[1] URL: https://cbr.ru/press/event/?id=242 (дата обращения: 10.03.2023).

[2] Пояснительная записка к законопроекту № 186266-7 «О внесении изменений в Уголовный кодекс Российской Федерации (в части усиления уголовной ответственности за хищение денежных средств с банковского счета или электронных денежных средств)». URL: https://sozd.duma.gov.ru/bill/53700-6 (дата обращения: 10.03.2023).

Федеральным законом от 23.04.2018 № 111-ФЗ изменена диспозиция ст. 159.3 УК РФ, ее действие распространено на использование не только платежных карт, но и электронных средств платежа (см. табл. 2). Кроме того, кража денежных средств со счетов банка и электронных денежных средств была выделена в квалифицированный состав ст. 158 УК РФ[1].

Таблица 2

Изменения, внесенные в диспозицию ч. 1 ст. 159.3 УК РФ с принятием федерального закона от 23.04.2018 № 111-ФЗ

Редакция диспозиции **ч. 1 ст. 159.3 УК РФ**, действовавшая до принятия федерального закона от 23.04.2018 № 111-ФЗ	Актуальная редакция диспозиции **ч. 1 ст. 159.3 УК РФ**
Статья 159.3. Мошенничество с использованием платежных карт 1. Мошенничество с использованием платежных карт, то есть хищение чужого имущества, совершенное с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты путем обмана уполномоченного работника кредитной, торговой или иной организации…	**Статья 159.3. Мошенничество с использованием электронных средств платежа** 1. Мошенничество с использованием электронных средств платежа…

В настоящее время уголовная ответственность за хищения с использованием электронных средств платежа регулируется статьями УК РФ следующей конструкции:

п. «г» ч. 3 ст. 158 УК РФ – кража, совершенная с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного ст. 159.3 УК РФ);

ст. 159.3 УК РФ – мошенничество с использованием электронных средств платежа;

[1] О внесении изменений в Уголовный кодекс Российской Федерации [Электронный ресурс]: федеральный закон от 23.04.2018 № 111-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

п. «в» ч. 3 ст. 159.6 УК РФ – мошенничество в сфере компьютерной информации, т.е. хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, совершенное с банковского счета, а равно в отношении электронных денежных средств.

Нельзя исключать и другие классические формы хищений (грабеж, разбой, присвоение и растрата), при совершении которых деньги, находящиеся на банковском счете, электронные денежные средства выступают в качестве предмета преступного посягательства. Однако в следственно-судебной практике такого рода деяния встречаются значительно реже.

Бесспорно, для хищений, совершенных с использованием электронных средств платежа, уголовно-процессуальным законом не установлено специального предмета доказывания. Вместе с тем посредством детализации обстоятельств, регламентированных ст. 73 УПК РФ, в процессе расследования уголовного дела общий предмет доказывания наполняется неповторимым содержанием. Стоит отметить, что наряду с обстоятельствами, подлежащими доказыванию при производстве по уголовному делу, устанавливаются и иные обстоятельства, имеющие значение для уголовного дела (ч. 1 ст. 74 УПК РФ).

Основываясь на концептуальных взглядах профессора С.А. Шейфера на уголовно-процессуальное доказывание, правомерно говорить о трех различных уровнях предмета доказывания.

Первый выступает как его обобщенная нормативная модель, структура и содержание которой обрисованы в ст. 73 УПК РФ и в нормах Общей части УК РФ (круг обстоятельств более свободен от признаков конкретного преступления). Второй уровень определяется на уровне норм Особенной части УК РФ, в которых сформулированы юридические признаки конкретного уголовно наказуемого деяния. Третий уровень же определяется путем конкретизации его с учетом обстоятельств совершения отдельного преступления[1].

[1] Шейфер С.А. Доказательства и доказывание по уголовным делам: проблемы теории и правового регулирования. М.: Норма, 2009 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

Сопоставляя с предметом доказывания обстоятельства, подлежащие доказыванию по уголовному делу, последние условно можно разделить на следующие группы:

- обстоятельства, которые являются основанием для уголовного преследования и привлечения к уголовной ответственности, применения меры уголовно-правового характера в виде конфискации имущества (событие преступления, виновность, характер и размер причинённого преступлением вреда, преступность происхождения имущества – п. 1, 2, 4, 8 ч. 1 ст. 73 УПК РФ);

- обстоятельства, необходимые для индивидуализации уголовной ответственности и назначения наказания (характеристика личности, смягчающие и отягчающие наказание обстоятельства – п. 3, 6 ч. 1 ст. 73 УПК РФ);

- обстоятельства, которые могут исключить преступность и наказуемость деяния, повлечь за собой освобождение от уголовной ответственности и наказания (п. 5, 7 ч. 1 ст. 73 УПК РФ).

Указанный перечень, являясь типовым по своей сути, непременно должен дополняться сообразно уголовно-правовой квалификации преступления. Поэтому применительно к хищениям, совершенным с использованием электронных средств платежа, специфика предмета доказывания строится, прежде всего, на таких дефинициях, как «электронное средство платежа», «электронные денежные средства», «платежная система».

Необходимо отметить, что механизм совершения хищения с использованием электронных средств платежа предполагает, что указанные платежные средства, как правило, используются в качестве средства совершения преступления. Характерным предметом преступного посягательства в таком случае выступают денежные средства, безналичные, в электронной форме, которые могут находиться на банковском счете (в т.ч. на привязанной к нему банковской карте), храниться при помощи иного платежного инструмента – аналога банковского счета (например, на электронном кошельке).

Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платежной системе» содержит следующие значимые в настоящем контексте определения:

электронное средство платежа – средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения в целях осу-

ществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в т.ч. платежных карт, а также иных технических устройств;

электронные денежные средства – денежные средства, которые предварительно предоставлены одним лицом (лицом, предоставившим денежные средства) другому лицу, учитывающему информацию о размере предоставленных денежных средств без открытия банковского счета (обязанному лицу), для исполнения денежных обязательств лица, предоставившего денежные средства, перед третьими лицами и в отношении которых лицо, предоставившее денежные средства, имеет право передавать распоряжения исключительно с использованием электронных средств платежа;

платежная система – совокупность организаций, взаимодействующих по правилам платежной системы в целях осуществления перевода денежных средств, включающая оператора платежной системы, операторов услуг платежной инфраструктуры и участников платежной системы, из которых как минимум три организации являются операторами по переводу денежных средств.

Раскрыть особенности предмета доказывания по уголовным делам о хищениях, совершенных с использованием электронных средств платежа, также представляется рациональным через отдельные объективные признаки преступления.

Напомним, что под *хищением* понимаются совершенные с корыстной целью противоправные безвозмездное изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, причинившие ущерб собственнику или иному владельцу этого имущества.

Согласно примечанию к ст. 158 УК РФ предметом хищения является чужое имущество, которое обладает тремя признаками.

Вещный признак имущества как предмета хищения предполагает, что имущество как предмет хищения должно иметь определенную физическую форму. Вместе с тем невещные предметы (к ним, прежде всего, относятся безналичные (электронные) денежные средства, а также криптовалюта) также могут являться предметом хищения.

Экономический признак имущества как предмета хищения предполагает обладание объективной экономической стоимостью.

Юридический признак имущества как предмета хищения предполагает, во-первых, что оно не является изъятым из свободного гражданского оборота и ограниченно оборотоспособным (ст. 129 ГК РФ), и, во-вторых, что оно является для виновного в правовом смысле чужим[1].

В этом контексте особый интерес представляет криптовалюта, а также иные виды цифровой валюты и цифровых финансовых активов[2]. В соответствии со ст. 128 ГК РФ к числу объектов гражданских прав относятся не только вещи, но и имущественные права (включая безналичные денежные средства, бездокументарные ценные бумаги, цифровые права).

Однако не все электронные валюты могут считаться полноценным платежным средством. Это обусловлено их высокой волатильностью, а также отсутствием официальных эмитентов, на которых бы возлагались обязательства по выпущенной валюте. Кроме того, денежной единицей в РФ является рубль, денежная эмиссия которого осуществляется исключительно Центральным банком РФ[3]. Эта валюта обеспечена золотовалютными резервами и прочими активами государства. Именно рубль – единственное законное средство наличного платежа на территории РФ, введение же других денежных единиц и выпуск денежных суррогатов запрещены[4].

Здесь следует отметить, что в настоящее время в Государственной Думе РФ находится законопроект № 270838-8 «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с внедрением цифрового рубля», содержащий

---

[1] Комментарий к Уголовному кодексу Российской Федерации. 9-е изд., перераб. и доп. / под ред. Г.А. Есакова. Проспект, 2021 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации [Электронный ресурс]: федеральный закон от 31.07.2020 № 259-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

[3] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

[4] О Центральном банке Российской Федерации (Банке России) [Электронный ресурс]: федеральный закон от 10.07.2002 № 86-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

концепцию цифрового рубля. Согласно указанной законотворческой инициативе и предложенным основам правового регулирования цифровой рубль может стать валютой[1] Российской Федерации и самостоятельным электронным денежным средством[2]. То есть рубль будет существовать в наличной форме, безналичной (на счетах в банках) и цифровой (электронной).

В настоящее время для целей уголовно-правовой квалификации безналичные денежные средства отождествляются с электронными денежными средствами. На это указывает Пленум Верховного Суда РФ, обеспечивая формирование единообразного применения судами норм уголовного закона на примере мошенничества. Согласно названной правовой позиции, «если предметом преступления при мошенничестве являются безналичные денежные средства, в том числе электронные денежные средства, то по смыслу положений п. 1 примечания к ст. 158 УК РФ и ст. 128 ГК РФ содеянное должно рассматриваться как хищение чужого имущества. Такое преступление следует считать оконченным с момента изъятия денежных средств с банковского счета их владельца или электронных денежных средств, в результате которого владельцу этих денежных средств причинен ущерб»[3].

Таким образом, наряду с общими признаками, характеризующими хищение, по уголовным делам о хищениях с использованием электронных средств платежа должно быть доказано наличие особого предмета преступного посягательства, являющегося чужим имуществом, – *денежных средств*, находившихся на банковском счете, *электронных денежных средств*, хранившихся при помощи иного платежного инструмента.

В связи с чем значимым элементом предмета доказывания по уголовном делам о хищениях, совершенных с использованием

---

[1] О валютном регулировании и валютном контроле [Электронный ресурс]: федеральный закон от 10.12.2003 № 173-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Информация с сайта Системы обеспечения законодательной деятельности Государственной Думы РФ. URL: https://sozd.duma.gov.ru/bill/270838-8 (дата обращения: 10.03.2023).

[3] О судебной практике по делам о мошенничестве, присвоении и растрате [Электронный ресурс]: постановление Пленума Верховного Суда РФ от 30.11.2017 № 48. Доступ из справ.-правовой системы «КонсультантПлюс».

электронных средств платежа, являются обстоятельства, которые устанавливают место нахождения подразделения банка или иной организации, в котором владельцем денежных средств был *открыт банковский счет* или *велся учет электронных денежных средств без открытия счета*.

До недавнего времени именно этот адрес территориально считался и местом окончания преступления, и местом совершения преступления, учитывался при определении места производства предварительного расследования (ч. 1 ст. 152 УПК РФ).

Данное правило определения места кражи безналичных (электронных) денежных средств содержится в п. 25.2 постановления Пленума Верховного Суда РФ от 27.12.2002 № 29[1]. В декабре 2022 г. в этот пункт внесены изменения (см. табл. 3), исходя из которых местом совершения кражи данного вида следует считать *место совершения лицом действий, направленных на незаконное изъятие денежных средств.*

Таблица 3

Изменения, внесенные в п. 25.2 постановления Пленума Верховного Суда РФ от 27.12.2002 № 29 с принятием постановления от 15.12.2022 № 38

Редакция **п. 25.2** до принятия постановления Пленума Верховного Суда РФ от 15.12.2022 № 38	Актуальная редакция **п. 25.2** постановления Пленума Верховного Суда РФ от 27.12.2002 № 29
25.2. Кражу, ответственность за которую предусмотрена пунктом «г» части 3 статьи 158 УК РФ, следует считать оконченной с момента изъятия денежных средств с банковского счета их владельца или электронных денежных средств, в результате которого владельцу этих денежных средств причинен ущерб. Местом окончания такой кражи является место нахождения подразделения банка или иной организации, в котором владельцем	25.2. Кражу, ответственность за которую предусмотрена пунктом «г» части 3 статьи 158 УК РФ, следует считать оконченной с момента изъятия денежных средств с банковского счета их владельца или электронных денежных средств, в результате которого владельцу этих денежных средств причинен ущерб. Исходя из особенностей предмета и способа данного преступления местом его совершения является, как правило, место со-

[1] О судебной практике по делам о краже, грабеже и разбое [Электронный ресурс]: постановление Пленума Верховного Суда РФ от 27.12.2002 № 29. Доступ из справ.-правовой системы «КонсультантПлюс».

денежных средств был открыт банковский счет или велся учет электронных денежных средств без открытия счета.	вершения лицом действий, направленных на незаконное изъятие денежных средств (например, место, в котором лицо с использованием чужой или поддельной платежной карты снимает наличные денежные средства через банкомат либо осуществляет путем безналичных расчетов оплату товаров или перевод денежных средств на другой счет).

Изменения коснулись и п. 5 постановления Пленума Верховного Суда РФ от 30.11.2017 № 48 (см. табл. 4). Теперь местом совершения мошенничества, если оно состоит в хищении безналичных денежных средств, следует считать *место совершения лицом действий, связанных с обманом или злоупотреблением доверием и направленных на незаконное изъятие денежных средств*.

Таблица 4

Изменения, внесенные в абз. 3 п. 5 постановления Пленума Верховного Суда РФ от 30.11.2017 № 48 с принятием постановления от 15.12.2022 № 38

Редакция **абз. 3 п. 5** до принятия постановления Пленума Верховного Суда РФ от 15.12.2022 № 38 (абзац введен постановлением Пленума Верховного Суда РФ от 29.06.2021 № 22)	Актуальная редакция **абз. 3 п. 5** постановления Пленума Верховного Суда РФ от 30.11.2017 № 48
Местом окончания мошенничества, состоящего в хищении безналичных денежных средств, является место нахождения подразделения банка или иной организации, в котором владельцем денежных средств был открыт банковский счет или велся учет электронных денежных средств без открытия счета.	Местом совершения мошенничества, состоящего в хищении безналичных денежных средств, исходя из особенностей предмета и способа данного преступления, является, как правило, место совершения лицом действий, связанных с обманом или злоупотреблением доверием и направленных на незаконное изъятие денежных средств.

Любопытно, что организация расследования и доказывания обстоятельств, предусмотренных ст. 73 УПК РФ, по уголовным делам о хищениях с использованием электронных средств платежа не всегда будет связана с местом совершения преступления. В настоящее время МВД России предприняты меры по совершенствованию организации раскрытия и расследования отдельных видов хищений, а именно предусмотренных ст. 158, 159-159.3, 159.5, 159.6 УК РФ, совершенных с использованием платежных карт, средств мобильной связи и информационно-телекоммуникационной сети Интернет. В соответствии с приказом МВД России от 03.04.2018 № 196 принятие решения о возбуждении уголовного дела по указанным преступлениям должно осуществляться в органе, в который первоначально поступило сообщение о преступлении. Только после получения достаточных доказательств о совершении преступления на территории обслуживания другого территориального органа МВД России и выполнения всех возможных процессуальных действий по месту возбуждения уголовного дела возможно направление уголовного дела в порядке, предусмотренном ст. 152 УПК РФ[1].

Далее, рассматриваемую группу хищений объединяет схожий механизм совершения преступления, в доказывании которого в т.ч. необходимо учитывать следующие его особенности:

- противоправное изъятие чужого имущества чаще всего происходит с банковского счета или иного инструмента электронного финансового оборота (доказательственным значением в этом контексте будут обладать сведения о владельце платежного инструмента; дате его активации (открытия); периоде использования; устройствах, с которых осуществлялся доступ к платежному инструменту; лицах, имевших доступ к нему);

- при совершении преступления, как правило, используются технические средства – информационные технологии, компьютерное оборудование, например, для облегчения доступа к предмету преступного посягательства, получения данных о его владельце (поэтому важные для доказывания информационные следы можно

[1] О некоторых мерах по совершенствованию организации раскрытия и расследования отдельных видов хищений [Электронный ресурс]: приказ МВД России от 03.04.2018 № 196. Доступ из справ.-правовой системы «КонсультантПлюс».

обнаружить, установив местонахождение соответствующего программного обеспечения, мобильного приложения, аппаратно-программных средств и компьютерных устройств, которые использовались при подготовке, совершении преступления, а также после его окончания);

- электронные платежные системы и электронные средства платежа, их использование, в т.ч. в процессе вывода похищенных денежных средств (обналичивания), демонстрируют дистанционный режим распоряжения финансовыми активами (в связи с чем пользование платежными платформами, программами дистанционного банкового обслуживания, клиент-банком, электронными кошельками, виртуальной картой может оставлять значимые информационные следы в виде персонифицированных сведений, данных процедуры идентификации клиента).

Пределы доказывания характеризуют состояние доказанности сведений об исследуемых обстоятельствах уголовного дела в сочетании с достаточностью доказательств. Они находятся в прямой корреляционной зависимости от предмета доказывания. В отечественной теории доказательств это соотношение определяется следующим образом: «Пределы доказывания предполагают определение по конкретному делу его границ таким образом, чтобы собранная совокупность доказательств с качественной стороны обеспечивала установление каждого элемента предмета доказывания»[1]. То есть пределы доказывания характеризуют степень доказанности обстоятельств, которые входят в предмет доказывания.

Поэтому очевидно, что особенности материально-правовой конструкции состава преступления, совершенного с использованием электронных средств платежа, могут влиять и на определение пределов доказывания. Правильное определение пределов доказывания по уголовным делам о преступлениях названной категории препятствует загромождению их материалов излишними доказательствами.

Таким образом, предмет и пределы доказывания хищений, совершенных с использованием электронных средств платежа, в

[1] Теория доказательств в советском уголовном процессе / Р.С. Белкин, А.И. Винберг, В.Я. Дорохов, Л.М. Карнеева и др.; редкол.: Н.В. Жогин (отв. ред.), Г.М. Миньковский, А.Р. Ратинов, В.Г. Танасевич и др. 2-е изд., испр. и доп. М.: Юрид. лит-ра, 1973. С. 186-197.

значительной мере обладают особенностями, которые детерминированы уникальными обстоятельствами отдельного события преступления, но ориентиром для процессуальной конструкции предмета доказывания является конструкция соответствующего состава преступления. Вместе с тем обстоятельства, входящие в предмет доказывания, устанавливаются совокупностью доказательств, система которых специфична для хищений, совершенных с использованием электронных средств платежа.

2. Система доказательств, используемых в доказывании по уголовным делам о хищениях, совершенных с использованием электронных средств платежа

Содержанием доказательств по уголовному делу являются сведения, с помощью которых могут быть установлены обстоятельства, подлежащие доказыванию при производстве по уголовному делу. Нормативная классификация доказательств представлена в ч. 2 ст. 74 УПК РФ. К числу доказательств относятся:

1) показания подозреваемого, обвиняемого;
2) показания потерпевшего, свидетеля;
3) заключение и показания эксперта;
4) заключение и показания специалиста;
5) вещественные доказательства;
6) протоколы следственных и судебных действий;
7) иные документы.

В доказывании по уголовным делам о хищениях, совершенных с использованием электронных средств платежа, в системе доказательств условно можно выделить следующие ключевые группы:

- доказательства «типового» хищения (по нормам Общей части УК РФ и п. 1 примечания к ст. 158 УК РФ);

- доказательства специфичного механизма совершения преступления, способа хищения сообразно конкретной уголовно-правовой конструкции;

- доказательства действий по «использованию» электронных средств платежа при совершении преступления, а также особого предмета преступного посягательства.

Анализ правоприменительной практики борьбы с цифровой преступностью[1], ее специфики позволяет охарактеризовать содержание отдельных доказательств следующим образом.

Показания подозреваемого (обвиняемого)

Показания подозреваемого и показания обвиняемого во многом схожи содержательно, т.к. они излагаются одним и тем же лицом, обладающим равным объёмом доказательственной информации о событии преступления. Отличается процессуальный статус лица, порядок допроса. Предмет допроса обвиняемого ограничен объёмом предъявленного обвинения.

Наряду с общими аспектами, входящими в предмет допроса подозреваемого (обвиняемого) и раскрывающими отношение к подозрению (обвинению), степень знакомства с потерпевшим, мотивы совершения преступления, характеризующими соучастие в преступлении при наличии, показания подозреваемого (обвиняемого) в совершении хищения с использованием электронных средств платежа могут содержать сведения, детально характеризующие механизм совершения преступления, использованные средства.

Показания потерпевшего

Являясь средством установления истины по уголовному делу, показания потерпевшего содержательно могут включать в себя следующие сведения, представляющие доказательственный интерес в расследовании хищения с использованием электронных средств платежа:

- сведения о банковском счете или ином инструменте электронного финансового оборота, с которого было похищено имущество (дата, время, место открытия или оформления платежного инструмента; реквизиты платежного инструмента, имеются ли привязанные к нему пластиковые карты, вещные атрибуты; привязан ли к платежному инструменту абонентский номер оператора сотовой связи; пользуется ли платежным инструментом через ин-

[1] Были изучены материалы уголовных дел, находившиеся в производстве следователей СЧ ГСУ ГУ МВД России по Алтайскому краю в 2020-2022 гг.

тернет-банкинг и какое программное обеспечение для совершения финансовых операций использует; подключены ли Google Pay, Apple Pay);

- сведения о непосредственном хищении имущества с платежного инструмента (если списание денежных средств произошло без участия потерпевшего: как давно стало известно о списании денежных средств; совершал ли накануне нестандартные, подозрительные для него действия, например, открывал отправленные в электронной почте или мессенджере письма, скачивал файлы, посещал интернет-сайты, проходил по ссылкам на интернет-страницы; если хищение сопровождалось вербальным контактом, использованием методов социальной инженерии злоумышленником при звонке или переписке: был ли ранее знаком со злоумышленником, с какого номера был осуществлен звонок, кем представился звонивший, с какой целью звонил, какие сведения испрашивал звонивший, какие действия выполнял по просьбе звонившего, каким мобильным устройством пользовался в момент звонка, каким компьютерным устройством пользовался, посещая интернет-площадку, откуда и когда узнал про интернет-площадку, содержание переписки);

- сведения о владении навыками информационной безопасности (сколько в течение дня пользуется сетью Интернет; пользуется ли социальными сетями; размещает ли персональные данные в свободном доступе; пользуется ли услугами интернет-магазинов; совершал ли оплату товаров в системе безналичных платежей; использует ли функцию автосохранения аутентификационных данных аккаунта в платежных системах);

- сведения о вреде, причиненном преступлением.

Показания свидетеля – сведения, сообщенные им на допросе, проведенном в ходе досудебного производства по уголовному делу или в суде. Свидетель может быть допрошен о любых относящихся к уголовному делу обстоятельствах (ст. 79 УПК РФ). Предмет показаний свидетеля по уголовным делам о хищениях, совершенных с использованием электронных средств платежа, зависит от личности самого свидетеля, способа восприятия сведений, имеющих значение для уголовного дела, и характера указанной доказательственной информации. Условно свидетелей названного рода преступлений можно разделить на следующие категории:

- лица – сотрудники правоохранительных органов, осуществлявшие документирование преступной деятельности, раскрытие преступления, производившие задержание лиц, совершивших преступление.

К данной категории относятся, прежде всего, сотрудники оперативных подразделений, которые в силу исполнения обязанностей по выявлению и раскрытию преступлений в ходе оперативно-розыскных мероприятий устанавливали механизм совершения преступления. Как следствие, указанным лицам известны синтезированные данные об используемых сим-картах, IMEI-номерах, банковских картах, профилях в социальных сетях, IP-адресах, используемых для выхода в сеть Интернет.

Если преступление или отдельные действия, составляющие его объективную сторону, совершены на улице, в общественном месте, то доказательственной информацией могут обладать сотрудники, которые анализировали записи камер видеонаблюдения. Например, когда имело место снятие наличных в банкомате, расчет в кассовой зоне магазина.

Кроме того, юридически значимые сведения также можно получить от сотрудников патрульно-постовой службы полиции, которые задерживали преступника по ориентировке, производили изъятие похищенных денежных средств, орудий и средств совершения преступления, иных значимых предметов и документов;

- лица, которым известны обстоятельства получения противоправного доступа к электронному средству платежа и его использования.

К данной категории относятся граждане, которые видели, к примеру, как злоумышленник нашел банковскую карту и оставил ее себе (в контексте п. «г» ч. 3 ст. 158 УК РФ).

Свидетель мог непосредственно воспринимать преступные действия, составляющие объективную сторону, например, если речь идет о мошенничестве через объявления о продаже на сайте «Авито», то действия по размещению фиктивных объявлений о продаже, переписку и телефонные беседы с гражданами с уговорами о переводах денежных средств якобы для оплаты товара.

Учитывая распространенность организованной преступности, прежде всего в сфере телефонных мошенничеств, следует уделить внимание свидетелю, в чьих показаниях устанавливается не только

механизм преступления, но и организация, особенности такой преступной деятельности.

Например, как следует из показаний свидетеля В., в марте текущего года он искал работу. Его пригласили на собеседование в офис, где ранее незнакомый ему Г. рассказал, в чем заключается «работа». Со слов Г., необходимо осуществлять звонки согласно «базе», читать текст на листке («скрипт») и от имени банка сообщать людям, что тем одобрен кредит, необходимо склонять людей к дистанционной форме получения кредита. При согласии гражданина необходимо тому разъяснить, что за перевод кредита будет взыматься «комиссия», которую гражданин должен оплатить. Он понял, что на самом деле никаких кредитов людям не выдавали, а просто происходил обман. Поэтому от предложения Г. отказался, а в дальнейшем от сотрудников полиции ему стало известно.

Другой пример.

Как следует из показаний свидетеля Ф., в начале прошлого года он находился в трудном финансовом положении, нуждался в заработке. С А. он знаком с детства, поэтому, когда А. предложил «работу», он заинтересовался. Со слов А., он занимается выдачей кредитов, а «работа» связана с осуществлением «холодных звонков» гражданам, в ходе которых необходимо предлагать получить кредит. О том, что деятельность незаконная, А. не пояснял. Он объяснил А., что не сможет так работать, не умеет общаться с людьми. Тогда А. сказал, что есть другая подработка, необходимо снимать с банковских карт денежные средства, которые будут поступать от граждан, погашающих кредитную задолженность в их организации. Он думал, что деятельность по снятию денежных средств с карт законная, просто А. таким образом обходит уплату налогов;

- лица, которым известны обстоятельства использования сети Интернет в механизме совершения преступления.

Например, как следует из показаний свидетеля И., с гр. А. он не знаком. Около месяца назад он, находясь у себя дома по месту жительства, с компьютера выходил в сеть Интернет через установленный у него Wi-Fi-роутер, заходил в свой аккаунт, зарегистрированный в Google. В тот момент система безопасности затребовала у него подтверждение пароля, т.к. было подключено

новое устройство для входа в его аккаунт. Вследствие чего он изменил пароль. В результате осмотра своей страницы он обнаружил, что в его аккаунт производились выходы с мобильного устройства под маркой Samsung. Марки такого телефона ни у него, ни у его жены никогда не было. Кроме того, пароль от его аккаунта знает только он, номер IP-адреса своего роутера он не знает, возможно, этот номер указан в договоре, который заключен с провайдером.

Другие примеры.

Из показаний свидетеля Б. следует, что с А. она находится в дружеских отношениях. У нее в квартире установлен Wi-Fi-роутер с беспроводной сетью Интернет. На ее имя оформлен договор с провайдером «Ростелеком», подключение к Wi-Fi осуществляется только при вводе пароля. А. часто бывал у нее в гостях, осведомлен о логине и пароле для подключения к Wi-Fi, пользовался им без ограничений.

Как следует из показаний свидетеля В., с А. она находится в дружеских отношениях. А. часто, находясь у нее в гостях, с ее ноутбука выходил в социальную сеть «ВКонтакте», используя профиль под именем «Миша Григорьев».

В аналогичном ключе могут быть допрошены подлинные владельцы профилей в социальных сетях, от имени которых размещались фиктивные объявления. На подставных лиц оформляются электронные кошельки, сим-карты, осуществляется регистрация на интернет-площадках, подмена профиля.

Так, из показаний свидетеля Г. следует, что у него есть профиль в социальной сети «ВКонтакте» под именем «Миша Григорьев». С А. он находится в дружеских отношениях. Поэтому А. имел доступ к профилю «Миша Григорьев», мог заходить в указанный профиль со своего компьютера. Он долгое время не пользовался социальной сетью «ВКонтакте». От сотрудников полиции ему стало известно, что его профиль «Миша Григорьев» был переименован в «Константин Смирнов» и использовался А. в мошеннических схемах.

- лица, которым известны обстоятельства распоряжения похищенным имуществом.

Так, например, из показаний свидетеля А. следует, что он работает водителем такси. При оказании услуг по перевозке гр. А.

оплата за поездку происходила путем перевода денежных средств на его банковскую карту ПАО «Сбербанк». Перевод осуществлялся по номеру телефона, который он продиктовал гр. А. Принадлежащую ему банковскую карту он в пользование гр. А. не передавал. От сотрудников полиции ему стало известно, что указанные денежные средства были похищены гр. А. в результате совершения мошеннических действий на сайте meshok.net.

Другой пример.

Из показаний свидетеля К. следует, что постоянного источника дохода он не имеет, гр. П. является его знакомым, с которым он поддерживает дружеские отношения. Около полугода назад П. предложил ему «пассивный» заработок, с доходом 5000 рублей в месяц. Со слов П. необходимо было открыть виртуальную банковскую карту, реквизиты которой, а также логин и пароль аккаунта в программе дистанционного банкового обслуживания предоставить П. На предложение П. он согласился, выполнив необходимые действия, и передал реквизиты П. После чего в течение 5 месяцев П. переводил на его электронный кошелек 5000 рублей ежемесячно. О намерениях П. он не был осведомлен, как использовалась открытая на его имя виртуальная карта, ему не было известно, как и о производимых по ней финансовых операциях. От сотрудников полиции ему стало известно, что указанная карта использовалась как «дроп-карта» при совершении мошенничества.

Подобные дроп-схемы получили широкое распространение в механизме совершения хищений с использованием электронных средств платежа. «Дроппер» может не только вслепую предоставлять свои банковские реквизиты, но и недвусмысленно находиться в преступном сговоре с мошенником.

Например, как следует из показаний свидетеля Б., ему известно о мошеннических действиях Х., который размещает объявления о продаже различных товаров в различных группах в социальных сетях. Для этого Х. приобрел себе через разные сайты профили, зарегистрированные на других лиц. С Х. он состоит в дружеских отношениях. Неоднократно Х. предупреждал его о том, что на его банковскую карту должны поступить денежные средства, из которых 500 рублей он должен оставить себе, а остальные снять наличкой и при встрече передать Х.

Обладать значимой информацией в этом юридическом контексте также могут сотрудники торговых организаций, которые могли непосредственно воспринимать действия по распоряжению чужим имуществом, например, если лицо рассчитывалось не принадлежащей ему картой за совершенную покупку в магазине.

Например, из показаний В. следует, что она работает в должности продавца-кассира в магазине «Мария-Ра». В магазине имеются две кассовые зоны, оборудованные терминалами для безналичного расчета, в т.ч. бесконтактным способом без ввода пин-кода при совершении покупок до 1000 рублей. 4 апреля текущего года в вечернее время в магазин зашел ранее незнакомый ей мужчина, который рассчитываться за товары подошел к ней на кассу № 2. Общая сумма покупки составила свыше 1000 рублей. Мужчина достал из кармана банковскую карту «Тинькофф Банк», которой попытался рассчитаться, но при оплате терминал запросил ввести пин-код для подтверждения операции. Тогда мужчина попросил разделить покупку на два чека. Рассчитавшись картой, мужчина покинул магазин.

К данной категории свидетелей относятся родственники, знакомые самого преступника, которые присутствовали в момент использования чужой банковской карты (снятии наличных в банкомате, расчете в торговых организациях);

- близкие и родственники потерпевшего.

Виртуальный платежный инструмент, пластиковая карта могут находиться в фактическом пользовании указанных лиц. Родственники жертвы могут быть осведомлены об отдельных обстоятельствах совершенного преступления, происхождении похищенных денежных средств.

Например, из показаний свидетеля Р. следует, что потерпевший М. является ее отцом. В декабре прошлого года отец неоднократно просил ее занять различные суммы денег, всего около 200 000 рублей. Занять указанную сумму отцу она не смогла. В дальнейшем от М. ей стало известно, что его обманули телефонные мошенники, он перевел им более 150 000 рублей.

Другой пример.

*Из показаний свидетеля М. следует, что когда она пришла в гости к родителям, ее мать разговаривала по телефону с аб. № 960-***-**-**. Со слов отца, звонят сотрудники банка, т.к. с кредитной карты матери пытаются незаконно снять денеж-*

*ные средства. Она взяла телефон матери, с ней стала разговаривать женщина, которая представилась сотрудницей ПАО «Сбербанк», поясняла, что банковскую карту ее матери необходимо заблокировать, чтобы пресечь незаконное снятие денежных средств. Затем на мобильный телефон матери с аб. № 960-***-**-**, к которому была подключена услуга «Мобильный банк», с номера 900 от ПАО «Сбербанк» стали поступать смс-сообщения с кодами.*

Не исключено, что вместо потерпевшего его родственники и сами могут совершать действия, в результате которых происходит хищение денежных средств.

*Как следует из показаний М., ей позвонил муж, сказал, что необходимо взять карту Сбербанк № 42**********, проследовать к банкомату, чтобы получить перевод на карту денежных средств в качестве задатка за автомобиль, который муж продавал на сайте «Авито».*

В случае если по уголовному делу проводились очные ставки для устранения существенных противоречий в показаниях допрошенных лиц, в доказывании могут быть использованы и результаты очной ставки, отраженные в протоколе указанного следственного действия.

Заключение эксперта и показания эксперта, заключение специалиста и показания специалиста

Заключение эксперта – представленные в письменном виде содержание исследования и выводы по вопросам, поставленным перед экспертом лицом, ведущим производство по уголовному делу, или сторонами.

Показания эксперта – сведения, сообщенные им на допросе, проведенном после получения его заключения, в целях разъяснения или уточнения данного заключения (ст. 80 УПК РФ).

Заключение специалиста – представленное в письменном виде суждение по вопросам, поставленным перед специалистом сторонами.

Показания специалиста – сведения, сообщенные им на допросе об обстоятельствах, требующих специальных познаний, а также разъяснения своего мнения (ст. 80 УПК РФ).

Специальные знания в науке, технике, искусстве или ремесле используются в процессе доказывания по уголовному делу для всестороннего и объективного исследования обстоятельств, со-

ставляющих предмет доказывания[1]. Характер следовой картины хищения, совершенного с использованием электронных средств платежа, отличается насыщенностью не только специфичными вещными объектами (банковскими инструментами, средствами сотовой связи, всевозможной компьютерной техникой), но и цифровыми следами. Сказанное предопределяет значимость участия лиц, обладающих специальными знаниями, в расследовании, в рамках самостоятельного исследования, разъяснения и уточнения выводов по его результатам, в обнаружении, закреплении и изъятии предметов и документов, имеющих значение для уголовного дела.

Достаточно распространенной судебной экспертизой, назначаемой в ходе расследования уголовных дел о хищениях с использованием электронных средств платежа, является компьютерная экспертиза (исследование компьютерной информации)[2]. Российский федеральный центр судебной экспертизы при Министерстве юстиции Российской Федерации называет данную экспертизу судебной компьютерно-технической экспертизой, а согласно видовой классификации выделяет: аппаратно-компьютерную экспертизу; программно-компьютерную экспертизу; информационно-компьютерную экспертизу (данных); компьютерно-сетевую экспертизу[3].

Указанные экспертизы могут проводиться по электронным носителям информации, компьютерным и мобильным устройствам, находящимся на них цифровым данным, программному обеспечению. По результатам экспертизы могут быть обнаружены имеющие значение в доказывании объекты, например, файлы, переписка и информация о соединениях абонентских номеров, иден-

---

[1] О судебной экспертизе по уголовным делам [Электронный ресурс]: постановление Пленума Верховного Суда РФ от 21.12.2010 № 28. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации [Электронный ресурс]: приказ МВД России от 29.06.2005 № 511. Доступ из справ.-правовой системы «КонсультантПлюс».

[3] Возможности Российского федерального центра судебной экспертизы при Министерстве юстиции Российской Федерации. URL: http://www.sudexpert.ru/possib/comp.php (дата обращения: 10.03.2023).

тификационные данные (абонентские номера, номера сим-карт, IMEI-номера), лог-файлы, вредоносные программы.

Кроме того, для установления последовательности движения денежных средств, способа распоряжения похищенным имуществом целесообразно производство бухгалтерской судебной экспертизы, например, когда имеется возможность проанализировать финансово-хозяйственные операции, отраженные в бухгалтерском учете отдельной организации.

Фоноскопическая судебная экспертиза (для идентификации лиц по фонограммам речи, технического исследования фонограмм) может быть проведена, например, когда имеется аудиозапись телефонных переговоров (фонограмма, в т.ч. спорная) между преступником и жертвой, между членами организованной преступной группы.

Портретная судебная экспертиза (для идентификации (отождествления) личности по признакам внешности) целесообразна, когда в материалах уголовного дела имеются фото- и видеоизображения. Например, потерпевший, разговаривая с мошенником по видеосвязи (схема продажи на «Авито»), имел возможность сделать скриншот лица звонившего и в дальнейшем выдал этот скриншот следователю. Цифровые фото- и видеоматериалы в следовой картине обусловлены и использованием социальных сетей в механизме совершения преступления.

Лингвистическая судебная экспертиза может быть назначена и проведена по тексту переписки из мессенджеров в целях решения вопросов смыслового понимания отдельных высказываний.

Использование специальных знаний в структуре доказывания хищений, совершенных с помощью электронных средств платежа, не ограничено только возможностями перечисленных судебных экспертиз. Обстоятельства, устанавливаемые в ходе «выводного» исследования и являющиеся предметом судебной экспертизы, могут охватывать сферу судебного почерковедения, криминалистического исследования документов, судебной психиатрии.

Кроме того, нельзя недооценивать роль специалиста в обнаружении, закреплении и изъятии предметов и документов, имеющих значение для уголовного дела. Поэтому к участию в процессуальных действиях, прежде всего связанных с изъятием электронных носителей информации и копированием с них информации, обязательно привлекается специалист (ст. 164.1 УПК РФ).

Вещественные доказательства и иные документы

Вещественными доказательствами признаются любые предметы: которые служили орудиями, оборудованием или иными средствами совершения преступления или сохранили на себе следы преступления; на которые были направлены преступные действия; деньги, ценности и иное имущество, полученные в результате совершения преступления; иные предметы и документы, которые могут служить средствами для обнаружения преступления и установления обстоятельств уголовного дела (ст. 81 УПК РФ).

Иные документы не обладают признаками, указанными в ч. 1 ст. 81 УПК РФ, но могут допускаться в качестве доказательств по уголовному делу, если имеют значение для установления обстоятельств, указанных в ст. 73 УПК РФ (ст. 84 УПК РФ).

Служить средством к установлению искомых обстоятельств по уголовному делу о хищении, совершенному с использованием электронных средств платежа, как вещественное доказательство или иной документ могут следующие объекты:

- *объекты, в которых отражены следы совершения финансовых операций* (пластиковые карты, банковские ключи; чеки по операциям по карте; информация, выписки и банковские справки по операциям; детализации расходов абонентских номеров абонентов сотовой связи; скриншоты, фотографии приложений системы дистанционного банковского обслуживания (СДБО); скриншоты, фотографии экрана мобильного телефона с смс-сообщениями от номера 900; сами похищенные денежные средства, если имело место хищение денежных средств с банковской карты путем снятия в банкомате);

- *объекты, в которых отражены следы принадлежности лицам определенных платежных инструментов, личных кабинетов в СДБО, аккаунтов, профилей, учетных записей в социальных сетях, интернет-сервисах для размещения объявлений, мессенджерах IP, сотовой связи, связи в сети передачи данных Интернет* (информация и банковские справки о владельце банковской карты, дате открытия счета, месте открытия счета, подключении услуги «Мобильный банк»; сведения о регистрационных данных электронного кошелька; сим-карты, сведения о регистрационных данных владельцев абонентского номера; сведения о регистрационных данных почтового ящика Mail.ru, пользователя на сайте «Авито»; сведения о регистрационных данных профиля в социальных

сетях, мессенджерах IP; сведения интернет-провайдера о регистрационных данных клиента, которому предоставлялся IP-адрес, и адресе предоставления; сведения о регистрации доменного имени);

- *объекты, в которых отражены следы совершения действий в сети Интернет, сотовой связи* (компьютерные устройства; сведения интернет-провайдера о предоставлении абоненту услуги доступа к сети Интернет с указанием IP-адреса, времени и места; информация об IP-адресах обращения к аккаунтам, профилям, учетным записям в социальных сетях, в интернет-сервисах для размещения объявлений, на других интернет-порталах, в мессенджерах IP; лог-файлы на компьютерных и мобильных устройствах; мобильные устройства; детализация абонентского номера, сведения о соединениях между абонентскими номерами с указанием даты и времени соединений, местах расположения базовых станций, IMEI-номерах);

- *объекты, в которых отражены следы совершения действий по использованию социальных сетей, интернет-сервисов для размещения объявлений, мессенджеров IP* (скриншоты, фотографии переписки во «ВКонтакте», WhatsApp, на «Авито»; информация ООО «ВКонтакте», «Авито» со сведениями об IP-адресах профиля конкретного пользователя);

- *объекты, в которых отражены идентификационные следы лица* (видеозаписи из магазинов, устройств самообслуживания, банкоматов; записи и скриншоты видеозвонков; скриншоты с камер видеонаблюдения «Безопасный город»; аудиозаписи телефонных переговоров (фонограммы), голосовые сообщения; фото- и видеоматериалы аккаунтов, профилей, учетных записей в социальных сетях, интернет-сервисах для размещения объявлений, пользователей мессенджеров IP).

Протоколы следственных действий

Доказательствами по уголовному делу являются протоколы процессуальных (следственных) действий, которые направлены на собирание и проверку доказательственных фактов. Как источник доказательств по уголовному делу о хищении, совершенном с использованием электронных средств платежа, могут использоваться протоколы следующих следственных действий:

- *следственных осмотров*.

Характерной особенностью хищений, совершенных с использованием электронных средств платежа, следует считать следовую картину преступления. Наряду с привычными материальными следами в расследовании указанной категории преступлений необходимо учитывать специфичные информационные следы. Поэтому в числе следственных осмотров по названной категории уголовных дел, безусловно, будут превалировать осмотры, фиксирующие описание виртуальных цифровых объектов.

Необходимо учитывать, что цифровые следы обладают высокой скоростью трансформации, их можно легко уничтожить, видоизменить, например, если электронный носитель информации, на котором сохранены указанные следы, имеет доступ к сети Интернет. Поэтому в ходе осмотра сначала выявляются материальные следы преступления, а затем обнаруживаются, закрепляются и изымаются следы, находящиеся в цифровой среде.

Закономерно, что юридическое оформление результатов таких осмотров чаще всего будет осуществляться в процессуальной *форме осмотра места происшествия, осмотра предметов и документов.* Вместе с тем в зависимости от объекта, представляющего доказательственный интерес, искомые следственные осмотры можно разделить:

1) на осмотр компьютерных устройств, мобильных устройств, т.е. техники, при помощи которой доступ в виртуальную среду имело не только лицо, совершившее преступления, но и сам потерпевший;

2) предметов и документов, в которых содержатся сведения о соединениях между абонентами IP-телефонии, пользователями сети передачи данных Интернет, содержании разговоров и переписки, местонахождении лиц в этот момент, используемых данных в процедуре идентификации личности;

3) осмотр предметов и документов, в которых содержатся сведения о совершенных электронных платежах, снятии наличных, используемых при этом платежных инструментах и сервисах, принадлежности указанных инструментов определенным лицам и используемых.

Необходимо отметить, что осмотр места происшествия необходим, прежде всего, для изучения механизма совершения преступления. Например, если имело место распоряжение похищен-

ными денежными средствами путем расчета за товары в торговой точке, то в протоколе осмотра места происшествия будут зафиксированы обстановка и наличие терминала с функцией бесконтактной оплаты (без ввода пин-кода). Аналогичным образом доказывать факт незаконного использования электронного средства платежа будут и результаты осмотра места происшествия, объектом которого может выступить банкомат, в котором происходило снятие денежных средств;

- *обысков и выемок.*

Данные следственные действия предполагают обеспеченное государственным принуждением процессуальное изъятие имеющих значение для уголовного дела предметов и документов, когда само местонахождение объекта имеет доказательственное значение (например, изъятие предмета преступного посягательства, средств совершения преступления в жилище подозреваемого). К числу предметов и документов, на которых могли остаться следы хищения, совершенного с использованием электронных средств платежа, подлежащих изъятию в ходе обыска (выемки), относятся уже перечисленные ранее специфичные объекты осмотра, в частности, компьютерные и мобильные устройства, сим-карты, электронные носители информации, пластиковые карты, банковские ключи и пр.;

- *проверок показаний на месте и следственных экспериментов.*

Проверка показаний на месте предполагает дачу лицом показаний и воспроизведение им своих действий в месте, о котором он ранее уже давал показания. Соответственно, проверка показаний на месте подозреваемого может быть связана с местом возникновения преступного умысла, приготовления к преступлению или сокрытия следов совершенного преступления, хищения или находки электронного средства платежа (например, пластиковой карты в банкомате), с местом, где производились действия по незаконному изъятию или происходило распоряжение уже похищенными денежными средствами. Показания потерпевшего, свидетеля могут быть уточнены или подвергнуты проверке, например, когда указанные лица наблюдали за действиями, составляющими объективную сторону преступления.

Следственный эксперимент, являясь специальным проверочным следственным действием, может быть использован в доказывании, к примеру, для уточнения времени, необходимого для совершения определенных действий с платежным инструментом или сервисом, компьютерным или мобильным устройством, возможности совершения определенных действий, в т.ч. требующих специальных навыков в сфере IT-технологий;

- *предъявления для опознания.*

Содержательно указанное следственное действие состоит в мысленном сопоставлении живым лицом предъявленного для обозрения лица или объекта с образом, ранее воспринятым в связи с расследуемым событием. Поэтому результаты указанного следственного действия могут быть использованы в доказывании в ситуации, когда жертва разговаривала с преступником по видеосвязи, телефону и в ее сознании сохранился мысленный образ, необходимый для установления тождества.

Необходимо отметить, что приведенный перечень примеров доказательств отнюдь не является исчерпывающим и зависит от конкретной следственной ситуации. При этом установление всех обстоятельств, входящих в предмет доказывания, их легитимное закрепление способами, регламентированными уголовно-процессуальным законодательством, является основой правильной квалификации преступления и юридической оценки действий лица, его совершившего. С учетом существующего разнообразия предусмотренных уголовным законом составов противоправных посягательств, совершенных с использованием электронных средств платежа и по видовым признакам характеризующихся как хищение, первостепенное значение обретает использование в доказывании всего арсенала доказательств.

3. Специфика квалификации преступления и юридической оценки действий лица, совершившего хищение с использованием электронных средств платежа

Квалификацию преступления следует определять как процесс отождествления общественно опасного деяния, событие которого установлено посредством уголовно-процессуального доказывания, с признаками конкретного состава преступления, предусмотренного статьями Особенной части УК РФ.

Юридическую оценку, в свою очередь, связывают с соотнесением содержания действий конкретного лица, участвовавшего в общественно опасном деянии, с содержанием соответствующей уголовно-правовой нормы. То есть предметом квалификации выступает событие, а уголовно-правовой оценки – действия участника события, его роль в нем. От указанных оценочных процессов зависит наступление правовых последствий, поэтому правильная квалификация и юридическая оценка гарантируют качественную реализацию уголовно-правовых норм.

Анализ практики правоприменительной деятельности демонстрирует, что актуальной проблемой, возникающей при квалификации расследуемого преступления и юридической оценке действий лиц, остается проблема разграничения преступлений. Следует признать, что уголовно-правовые конструкции составов преступлений в действующих нормах, устанавливающих уголовную ответственность за хищения с использованием электронных средств платежа, во многом имеют схожие признаки. Поэтому одинаковые на первый взгляд факты по результатам расследования могут быть квалифицированы по признакам абсолютно разных составов.

Конкуренцию уголовно-правовых норм, которой обусловлены проблемы квалификации и юридической оценки, можно разрешить, детально исследовав механизм совершения преступления. Разберем отдельные примеры.

Хищение путем использования учетных данных собственника электронного средства платежа, полученных путем обмана (конкуренция п. «г» ч. 3 ст. 158, ст. 159 и 159.3 УК РФ)

Пример. *А., руководствуясь корыстными побуждениями, будучи осведомленным о способе и особенностях совершения переводов денежных средств с банковского счета карты, с целью получения систематического незаконного дохода решил совершать в течение продолжительного периода времени тайное хищение денежных средств с банковского счета у неопределенного круга лиц.*

Для осуществления задуманного А. разработал план совершения преступления, согласно которому А., используя имевшиеся в его распоряжении сотовый телефон и сим-карту, должен был случайным набором цифр осуществить звонок на абонентский номер оператора сотовой связи; дозвонившись до абонента, вводя в заблуждение потерпевшего, вести с ним телефонные переговоры, представляясь сотрудником службы безопасности кредитной организации; сообщить потерпевшему заведомо ложные сведения о попытке несанкционированного списания с банковского счета потерпевшего денежных средств и необходимости отмены данной операции, а также дальнейшего обеспечения безопасности имеющихся на банковском счете денежных средств; убедить потерпевшего сообщить реквизиты открытой на его имя банковской карты – сведения о номере, коде банковской карты, сроке ее действия, а также сведения о паролях, необходимых для проведения запрошенных операций, содержащихся в смс-сообщениях, поступающих от банковской системы и операторов сотовой связи на абонентский номер держателя банковской карты; используя технические устройства, оснащенные доступом к сети Интернет, при помощи специальных приложений и сайтов, служащих для осуществления перевода денежных средств с банковского счета карты на банковский счет карты, создав запрос о списании денежных средств с банковского счета карты, принадлежащих потерпевшему, ввести полученные обманным путем от потерпевшего данные в установленную форму запроса системы дистанционного банковского обслуживания клиентов, указав находившиеся в его распоряжении номер счета, номер банковской карты, абонентский номер, номер электронного средства платежа, а также поступившие потерпевшему через услугу «Мобильный банк» с сервисного номера банковской системы пароли,

необходимые для подтверждения запрошенной операции; получив таким образом незаконный доступ к денежным средствам, находящимся на банковском счете карты, принадлежащей потерпевшему, совершить тайное хищение данных денежных средств, произведя их перечисление с банковского счета карты потерпевшего на подконтрольные ему банковские счета электронных средств платежа, тем самым распорядившись ими по своему усмотрению.

В данном случае хищение совершается путем использования учетных данных владельца имущества, электронного средства платежа (реквизитов банковской карты: номера, срока действия, кода безопасности, пароля для подтверждения операции). Способ получения доступа к этим данным не имеет значения[1], поэтому деяние будет квалифицироваться как кража по п. «г» ч. 3 ст. 158 УК РФ.

Другой пример. *У Г., осведомленного о способе и особенностях совершения перечислений денежных средств с банковского счета карты с использованием средств мобильной связи, из корыстных побуждений с целью получения незаконного дохода возник преступный умысел, направленный на тайное хищение чужого имущества, а именно денежных средств, принадлежащих А., с банковского счета последнего.*

Для осуществления задуманного Г. разработал план совершения преступления, согласно которому Г. должен, используя мобильный телефон и сим-карту с абонентским номером оператора связи <…> аб. № <…>, принадлежащие А., с использованием услуги «Мобильный банк», служащей для осуществления перевода денежных средств с банковского счета карты на банковский счет карты, направить смс-сообщения о запросах на списания определенных сумм денежных средств с банковского счета карты А. и зачисления их на указанный им счет; затем направить смс-сообщения с поступившими на используемый им абонентский номер через услугу «Мобильный банк» с сервисного номера паролями, необходимыми для подтверждения запрошенных операций; получив таким образом незаконный доступ к денежным средствам,

[1] О судебной практике по делам о мошенничестве, присвоении и растрате [Электронный ресурс]: постановление Пленума Верховного Суда РФ от 30.11.2017 № 48. Доступ из справ.-правовой системы «КонсультантПлюс».

находящимся на банковском счете карты А., совершить тайное хищение данных денежных средств, произведя их списание с банковского счета карты потерпевшего и зачисление на банковский счет карты, оформленный на его имя, посредством указания находившегося у него в пользовании абонентского номера оператора связи <…> аб. № <…>, тем самым распорядившись ими по своему усмотрению.

Реализуя свой преступный умысел, направленный на тайное хищение чужого имущества с банковского счета, Г., осознавая общественно опасный и противоправный характер своих действий, предвидя неизбежность наступления общественно опасных последствий в виде причинения имущественного ущерба собственнику и желая их наступления, руководствуясь корыстными побуждениями, в период времени с <…> по <…>, более точное время органами предварительного следствия не установлено, находясь по адресу <…>, убедившись, что его действия носят тайный характер и не очевидны для А., используя мобильный телефон и сим-карту с аб. № <…>, принадлежащие последнему, с использованием услуги «Мобильный банк», служащей для осуществления перевода денежных средств с банковского счета карты на банковский счет карты, направил на сервисный номер смс-сообщения с запросами на списания денежных средств с банковского счета карты А., с указанием используемого им аб. № <…>, посредством которых возможно произвести зачисление денежных средств на банковский счет его карты.

Продолжая реализацию своего преступного умысла, Г. получил сведения о паролях, необходимых для подтверждения на проведение запрошенных операций, которые в указанное время поступили в смс-сообщениях от сервисного номера банковской системы на аб. № <…>, получив таким образом незаконный доступ к принадлежащим А. денежным средствам и возможность распоряжаться ими.

После чего Г. направил на сервисный номер смс-сообщения с информацией о паролях, необходимых для подтверждения запрошенных операций, тем самым в период времени с <…> по <…>, более точное время органами предварительного следствия не установлено, произвел перечисления с банковского счета № <…>, открытого в офисе, расположенном по адресу <…>, принадлежащих А. денежных средств на банковский счет № <…> карты,

открытый на имя Г. в офисе, расположенном по адресу <…>, денежные средства в следующих суммах: <…>.

Зачислив на банковский счет карты указанные денежные средства, тем самым в период времени с <…> по <…>, тайно похитив их с банковского счета А., Г. распорядился ими по своему усмотрению, причинив своими умышленными действиями А. материальный ущерб на общую сумму <…> рублей.

В этой ситуации лицо тайно использовало мобильный телефон потерпевшего, таким образом получив доступ к электронному средству платежа, при помощи которого и произошло хищение денежных средств. Деяние будет квалифицироваться как кража по п. «г» ч. 3 ст. 158 УК РФ.

Хищение путем распространения заведомо ложных сведений в информационно-телекоммуникационных сетях (конкуренция ст. 159, 159.3 и 159.6 УК РФ)

Пример. *В., руководствуясь корыстными побуждениями, будучи осведомленным о способе и особенностях совершения мошенничеств в отношении граждан с использованием средств мобильной связи, с целью получения незаконного дохода решил совершить хищение чужого имущества путем обмана.*

Для осуществления задуманного В. разработал план совершения преступления, согласно которому В., используя имевшиеся в его распоряжении технические устройства, оснащенные доступом к сети Интернет, в т.ч. мобильные телефоны и сим-карты, должен был: осуществить доступ на сайт «Авито», где приискать объявление со сведениями о продаже какого-либо имущества; осуществить звонки на указанный в объявлении абонентский номер мобильного телефона гражданина, дозвонившись до абонента либо ответив на поступивший ответный звонок, вводя в заблуждение потерпевшего, вести с ними телефонные переговоры; сообщить ложные сведения о намерении приобрести указанное в объявлении имущество, произведя перечисление задатка безналичным способом – путем перевода денежных средств на банковский счет карты продавца, убедить потерпевшего сообщить номер банковской карты; используя имевшиеся в его распоряжении технические устройства осуществить через приложение «Сбербанк Онлайн» вход в «личный кабинет» владельца банковской карты, убедив потерпевшего сообщить сведения о пароле,

необходимом для подтверждения регистрации банковской карты потерпевшего в приложении «Сбербанк Онлайн», получив, таким образом, доступ к сведениям о состоянии всех банковских счетов и вкладов, открытых на имя потерпевшего, суммах находящихся на них денежных средств; убедить потерпевшего сообщить сведения о пароле, необходимом для подключения услуги «Мобильный банк» по банковской карте потерпевшего, на находившийся в пользовании В. абонентский номер, предоставив, таким образом, В. доступ к сведениям о движении денежных средств; кроме того, убедить потерпевшего проследовать к банкомату или платежному терминалу, где следовать его дальнейшим инструкциям и указаниям по проведению операций с банковскими картами по снятию или переводу денежных средств, а также по переводу наличных денежных средств, имеющихся у потерпевшего, сообщив заведомо ложные сведения о переводе задатка по обеспечению обязательства дальнейшего приобретения имущества, о произошедшем «сбое» в системе обслуживания банка и переводе денежных средств со счетов потерпевшего на его счет, в завуалированной форме продиктовать потерпевшему абонентский номер сим-карты, находившейся в его распоряжении; тем самым обеспечить осуществление перевода денежных средств как с банковского счета карты потерпевшего, так и наличными денежными средствами на счета абонентских номеров, подконтрольные В., таким образом, похитив их; в дальнейшем похищенными денежными средствами, поступившими на подконтрольные В. счета абонентских номеров, распорядиться по своему усмотрению.

В данном случае хищение осуществляется путем распространения заведомо ложных сведений в информационно-телекоммуникационных сетях, поэтому квалификация деяния по ст. 159.6 УК РФ исключена. Более того, деяние не является кражей, т.к. буквально при совершении противоправного изъятия чужого имущества не используются учетные данные платежного инструмента, потерпевший сам совершает переводы под руководством мошенника[1]. Деяние будет квалифицировано по ст. 159 УК РФ.

[1] О судебной практике по делам о мошенничестве, присвоении и растрате [Электронный ресурс]: постановление Пленума Верховного Суда РФ от 30.11.2017 № 48. Доступ из справ.-правовой системы «КонсультантПлюс».

Хищение, в котором содержание объективной стороны предполагает доступ к электронному средству платежа, но перевод денежных средств осуществляет потерпевший (конкуренция п. «г» ч. 3 ст. 158, ст. 159 и 159.3 УК РФ)

Пример. *Д., руководствуясь корыстными побуждениями, будучи осведомленным о способе и особенностях совершения мошенничеств в отношении граждан с использованием средств мобильной связи, с целью получения незаконного дохода решил совершить хищение чужого имущества путем обмана.*

Для осуществления задуманного Д. разработал план совершения преступления, согласно которому Д., используя мобильный телефон и сим-карту, должен был: осуществить звонок на мобильный телефон гражданина, дозвонившись до абонента либо ответив на поступивший ответный звонок, вводя в заблуждение потерпевшего, вести с ним телефонные переговоры, представляясь сотрудником службы безопасности банка; сообщить заведомо ложные сведения о блокировке банковской карты, подключении к указанной банковской карте услуги «Мобильный банк» абонентского номера, не находящегося в пользовании потерпевшего; убедить потерпевшего сообщить сумму денежных средств, находящихся на банковском счете карты потерпевшего, а также проследовать к банкомату или платежному терминалу, где запросить остаток денежных средств, находящихся на банковском счете карты потерпевшего, сообщить ему данные суммы в целях их хищения, после чего убедить потерпевшего следовать его дальнейшим инструкциям и указаниям по проведению операций с банковскими картами; в завуалированной форме продиктовать потерпевшему абонентский номер сим-карты или номер банковской карты, находившиеся в его распоряжении, в качестве сервисного номера банка для разблокирования банковской карты потерпевшего, а также отключения от указанной банковской карты услуги «Мобильный банк» абонентского номера, не находящегося в пользовании потерпевшего; тем самым обеспечить осуществление перевода денежных средств с банковского счета карты потерпевшего на счета абонентских номеров либо карт, подконтрольных Д., таким образом, похитив их; в дальнейшем похищенными денежными средствами, поступившими на подконтрольные Д. счета абонентских номеров либо карт, распорядиться по своему усмотрению.

В этой ситуации, аналогично предыдущему примеру, деяние не является кражей, т.к. буквально при совершении противоправного изъятия чужого имущества не используются учетные данные платежного инструмента, потерпевший сам совершает переводы под руководством мошенника[1]. Деяние будет квалифицировано по ст. 159 УК РФ.

[1] О судебной практике по делам о мошенничестве, присвоении и растрате [Электронный ресурс]: постановление Пленума Верховного Суда РФ от 30.11.2017 № 48. Доступ из справ.-правовой системы «КонсультантПлюс».

Заключение

Противоправные действия в цифровой среде представляют повышенную общественную опасность. Лица, которые могут совершать их, как правило, обладают специальными знаниями, применяют технические средства. Хищения с использованием электронных средств платежа посягают не только на право собственности, но и на банковскую тайну.

Природа совершения указанных преступлений очень технологична, а само преступление зачастую реализуется через сложный механизм. При этом, как показывает правоприменительная практика, преступные деяния, совершенные с использованием электронных средств платежа, обладают высокой степенью латентности.

Доказывание хищений, совершенных с использованием электронных средств платежа, квалификация и юридическая оценка действий лица, совершившего такое преступление, в значительной мере обладают особенностями, которые детерминированы уникальными обстоятельствами отдельного события преступления, но ориентиром для процессуальной деятельности является конструкция соответствующего состава преступления.

Сложности, с которыми сталкиваются правоприменители, обусловлены не только слабой системностью законодательной регламентации отдельных уголовных и уголовно-процессуальных институтов, спецификой отношений в национальной платежной системе, но и особенностями механизма совершения преступлений, разнообразием способов совершения, форм оказания противодействия правоохранительным органам.

Квалифицированная организация предварительного расследования, правильное определение предмета и пределов доказывания и эффективное использование средств доказывания с учетом особенностей уголовно-правовой конструкции состава преступления значимы для своевременности и правильности принятия итогового процессуального решения по уголовному делу. В этой связи автором и выработаны рекомендации по оптимизации деятельности властных субъектов уголовного процесса, осуществляющих предварительное расследование.

Список литературы

Нормативные правовые акты
и материалы судебной практики

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

2. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

3. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

4. О валютном регулировании и валютном контроле [Электронный ресурс]: федеральный закон от 10.12.2003 № 173-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

5. О национальной платежной системе [Электронный ресурс]: федеральный закон от 27.06.2011 № 161-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

6. О Центральном банке Российской Федерации (Банке России) [Электронный ресурс]: федеральный закон от 10.07.2002 № 86-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

7. О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации [Электронный ресурс]: федеральный закон от 31.07.2020 № 259-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

8. О Стратегии национальной безопасности Российской Федерации [Электронный ресурс]: Указ Президента РФ от 02.07.2021 № 400. Доступ из справ.-правовой системы «КонсультантПлюс».

9. Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации [Электронный ресурс]: приказ МВД России от 29.06.2005 № 511. Доступ из справ.-правовой системы «КонсультантПлюс».

10. О некоторых мерах по совершенствованию организации раскрытия и расследования отдельных видов хищений [Электрон-

ный ресурс]: приказ МВД России от 03.04.2018 № 196. Доступ из справ.-правовой системы «КонсультантПлюс».

11. О судебной практике по делам о краже, грабеже и разбое [Электронный ресурс]: постановление Пленума Верховного Суда РФ от 27.12.2002 № 29. Доступ из справ.-правовой системы «КонсультантПлюс».

12. О судебной практике по делам о мошенничестве, присвоении и растрате [Электронный ресурс]: постановление Пленума Верховного Суда РФ от 30.11.2017 № 48. Доступ из справ.-правовой системы «КонсультантПлюс».

13. О судебной экспертизе по уголовным делам [Электронный ресурс]: постановление Пленума Верховного Суда РФ от 21.12.2010 № 28. Доступ из справ.-правовой системы «КонсультантПлюс».

Научная и учебная литература

14. Гаспарян Г.З. Расследование хищений денежных средств, совершенных с использованием информационных банковских технологий: дис. … канд. юрид. наук. М., 2020. 300 с.

15. Голятина С.М. Методика расследования хищений электронных денежных средств: дис. … канд. юрид. наук. Волгоград, 2022. 196 с.

16. Маилян А.В. Совершенствование методики расследования хищения с использованием электронных средств платежа: дис. … канд. юрид. наук. Ростов н/Д., 2021. 245 с.

17. Маркова Е.А. Уголовно-правовая характеристика хищения, совершаемого с использованием электронных средств платежа: дис. … канд. юрид. наук. СПб., 2021. 251 с.

18. Мира К.А. Установление механизма хищений чужого имущества с использованием информационных технологий: дис. … канд. юрид. наук. М., 2022. 245 с.

19. Перетолчин А.П. Уголовная ответственность за мошенничество с использованием электронных средств платежа: дис. … канд. юрид. наук. Владивосток, 2022. 239 с.

20. Строгович М.С. Курс советского уголовного процесса: в 2 т. Т. 1: Основные положения науки советского уголовного процесса. М.: Наука, 1968. 470 с.

21. Теория доказательств в советском уголовном процессе / Р.С. Белкин, А.И. Винберг, В.Я. Дорохов, Л.М. Карнеева и др.;

редкол.: Н.В. Жогин (отв. ред.), Г.М. Миньковский, А.Р. Ратинов, В.Г. Танасевич и др. 2-е изд., испр. и доп. М.: Юрид. лит-ра, 1973. 736 с.

22. Шейфер С.А. Доказательства и доказывание по уголовным делам: проблемы теории и правового регулирования. М.: Норма, 2009 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

Содержание

Учебное издание

Лукьянова Алина Александровна

Доказывание и юридическая оценка действий лица, совершившего хищение с использованием электронных средств платежа

Учебное пособие

Редактор	Ю.С. Жолобова
Корректура, компьютерная верстка	М.В. Егерь
Дизайн обложки	О.А. Розум

Лицензия ЛР № 0221352 от 14.07.1999 г.
Лицензия Плр № 020109 от 15.07.1999 г.

Подписано в печать 10.07.2023. Формат 60х84/16.
Ризография. Усл. п.л. 3. Тираж 54 экз. Заказ 267.
Барнаульский юридический институт МВД России.
Научно-исследовательский и редакционно-издательский отдел.
656038, Барнаул, ул. Чкалова, 49; бюи.мвд.рф.