Министерство внутренних дел Российской Федерации
Нижегородская академия

ОСОБЕННОСТИ КВАЛИФИКАЦИИ И РАССЛЕДОВАНИЯ ХИЩЕНИЙ ЭЛЕКТРОННЫХ ДЕНЕЖНЫХ СРЕДСТВ, В ТОМ ЧИСЛЕ СОВЕРШЕННЫХ ПОСРЕДСТВОМ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Учебное пособие

Допущено Министерством внутренних дел Российской Федерации в качестве учебного пособия для курсантов и слушателей образовательных организаций системы МВД России, сотрудников органов внутренних дел Российской Федерации

Нижний Новгород
НА МВД России
2022

УДК 373
ББК 67.408.1
О76

Рецензенты:
Ю. Ю. Савельев (Следственный департамент МВД России);
кандидат юридических наук *С. В. Мурадян,*
кандидат юридических наук, доцент *В. В. Пушкарев*
(Московский университет МВД России имени В.Я. Кикотя);
кандидат юридических наук, доцент *Т. В. Валькова*
(Санкт-Петербургский университет МВД России);
кандидат юридических наук, доцент *В. В. Намнясева,*
кандидат юридических наук, доцент *А. А. Лихолетов,*
кандидат юридических наук *Д. Г. Скориков*,
кандидат юридических наук *К. А. Трифонова*
(Волгоградская академия МВД России);
кандидат юридических наук *Н. М. Журавлева, Н. С. Расулова*
(Уральский юридический институт МВД России);
кандидат юридических наук *Р. В. Колесников*,
кандидат юридических наук, доцент *А. И. Гайдин*
(Воронежский институт МВД России)

О76 **Особенности** квалификации и расследования хищений электронных денежных средств, в том числе совершенных посредством использования информационно-телекоммуникационных сетей : учебное пособие / А. Ю. Ушаков, А. Г. Саакян, Р. С. Поздышев, М. А. Степанова. – Нижний Новгород : Нижегородская академия МВД России, 2022. – 61 с.

Основное внимание в учебном пособии уделено вопросам квалификации преступлений о хищениях электронных денежных средств, в том числе совершаемых посредством использования информационно-телекоммуникационных сетей; выработаны меры по совершенствованию правоприменительной практики в области производства предварительного следствия по рассматриваемому виду преступлений.

Пособие дополняет учебный материал дисциплин «Расследование преступлений в сфере компьютерной информации», «Расследование преступлений в сфере экономической деятельности», «Уголовное право», а также «Криминалистика» по темам, связанным с особенностями квалификации и расследования хищений электронных денежных средств, в том числе совершенных посредством информационно-телекоммуникационных сетей.

Издание предназначено для курсантов и слушателей образовательных организаций Министерства внутренних дел Российской Федерации, обучающихся по специальности 40.05.01 «Правовое обеспечение национальной безопасности (специализация – уголовно-правовая)». Оно может быть использовано и в практической деятельности сотрудниками органов предварительного следствия, а также в рамках их служебной подготовки.

ISBN 978-5-88840-189-7

Печатается по решению редакционно-издательского совета
Нижегородской академии МВД России

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Информационно-телекоммуникационные сети стали неотъемлемой частью современной жизни. С их помощью изменились формы безналичных расчетов. Доступность и простота электронных платежей сделала их для большинства граждан повседневным атрибутом.

Безналичный оборот в финансовом секторе вызвал повышенный интерес у нарушителей закона, стремящихся совершать хищения электронных денежных средств. Российское законодательство предусматривает ответственность за хищения подобного рода в п. «г» ч. 3 ст. 158 Уголовного кодекса Российской Федерации (далее – УК РФ), однако проблемные аспекты в разграничении квалификации от иных хищений существенно осложняют возможность применения данной нормы. Кроме того, в действующем уголовном праве установлена ответственность за мошенничество в сфере компьютерной информации (ст. 159^6 УК РФ), но при этом необходимо отметить отсутствие единообразной практики применения данной нормы, сложности в разграничении ее со смежными составами преступлений, предусмотренными ст. 159, 272 и 273 УК РФ.

Подготовка учебного пособия, направленного на решение актуальных вопросов, возникающих в ходе расследования хищений электронных денежных средств, в том числе совершаемых посредством использования информационно-телекоммуникационных сетей, в определенной мере позволит использовать превентивный потенциал уголовного и уголовно-процессуального законов и как результат – более эффективно производить предварительное следствие по уголовным делам о преступлениях рассматриваемого вида.

Настоящее пособие нацелено на решение следующих задач:

1) анализ имеющегося опыта расследования уголовных дел о хищениях электронных денежных средств, в том числе совершаемых посредством использования информационно-телекоммуникационных сетей;

2) выявление проблемных аспектов квалификации и выработка мер по совершенствованию правоприменительной практики в области производства предварительного следствия по рассматриваемому виду преступлений.

В работе применяются системный подход; структурно-функциональный, документальный анализ; статистический метод, метод экспертных оценок, анкетирование, интервьюирование.

Настоящее учебное пособие разработано в соответствии с рабочей программой учебной дисциплины «Расследование преступлений в сфере компьютерной информации».

РАЗДЕЛ 1. ВОПРОСЫ КВАЛИФИКАЦИИ ХИЩЕНИЙ ЭЛЕКТРОННЫХ ДЕНЕЖНЫХ СРЕДСТВ, В ТОМ ЧИСЛЕ СОВЕРШЕННЫХ ПОСРЕДСТВОМ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Федеральным законом от 23 апреля 2018 г. № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» ч. 3 ст. 158 УК РФ дополнена п. «г»: «с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного ст. 159^3 настоящего Кодекса)». В пояснительной записке указано, что данное изменение внесено с целью более эффективного противодействия противоправным посягательствам на электронные денежные средства и средства граждан, находящиеся на банковских счетах.

Положения п. «г» ч. 3 ст. 158 УК РФ в действующей редакции позволяют говорить о том, что законодатель выделяет разновидности денежных средств. В этой связи необходимо уточнить предмет рассмотрения и сделать, на наш взгляд, существенную оговорку. Несмотря на конкретную формулировку темы учебного пособия, мы также будем затрагивать вопросы о хищениях денежных средств с банковского счета, поскольку они являются альтернативными признаками объективной стороны одного квалифицированного состава преступлений, характеризуются общими правовыми и криминалистическими особенностями и вызывают схожие проблемы в юридической практике.

Проведенный анализ информационно-аналитических справок о правоприменительной практике, складывающейся при квалификации хищений денежных средств с банковского счета путем обналичивания в банкоматах платежных карт потерпевших, представленных территориальными подразделениями во исполнение распоряжения заместителя Министра внутренних дел Российской Федерации – начальника Следственного департамента МВД России от 30 января 2019 г. № 1/807, показал, что ряд регионов, как правило, сталкивается с вопросами о правильной квалификации рассматриваемой категории хищений. С целью создания единой на территории России правоприменительной практики по делам о хищениях электронных денежных средств, в том числе с использованием информационно-телекоммуникационных сетей, нами изучены информационно-аналитические справки и выявлены основные особенности квалификации.

Предлагаем прежде всего рассмотреть квалифицирующие признаки, указанные в п. «г» ч. 3 ст. 158 УК РФ: «с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного ст. 159^3 настоящего Кодекса)».

Электронные денежные средства – это особый предмет преступления. В соответствии с п. 18 ст. 3 Федерального закона от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе» (далее – Закон о национальной платежной системе) 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. При этом не являются электронными денежными средствами денежные средства, полученные организациями, осуществляющими профессиональную деятельность на рынке ценных бумаг, клиринговую деятельность, деятельность по организации привлечения инвестиций и/или деятельность по управлению инвестиционными фондами, паевыми инвестиционными фондами и негосударственными пенсионными фондами и осуществляющими учет информации о размере предоставленных денежных средств без открытия банковского счета в соответствии с законодательством, регулирующим деятельность указанных организаций[1].

Кража с банковского счета предусматривает тайное хищение денежных средств. Конкретное определение понятия банковского счета в нормативных правовых актах отсутствует. Исходя из анализа главы 45 Гражданского кодекса Российской Федерации (далее – ГК РФ), данную категорию представим как счет, открываемый банком по договору банковского счета, в соответствии с которым банк обязуется принимать и зачислять поступающие на счет, открытый клиенту (владельцу счета), денежные средства, выполнять распоряжения клиента о перечислении и выдаче соответствующих сумм со счета и проведении других операций по нему. Банковский счет может быть открыт на условиях использования электронного средства платежа.

Электронное средство платежа – это 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-

[1] Следует отметить, что ни бонусные баллы, ни «игровые» деньги, ни криптовалюта не могут быть предметом преступлений, предусмотренных п. «г» ч. 3 ст. 158 и 159^3 УК РФ. Хищение указанного имущества квалифицируется в зависимости от его способа по ст. 158, 159, 159^6, 160, 161, 162 УК РФ.

коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств.

Согласно позиции судов отдельных регионов Российской Федерации квалифицирующий признак кражи, совершенной с банковского счета, имеет место только при хищении безналичных и электронных денежных средств путем их перевода в рамках применяемых форм безналичных расчетов в порядке, установленном ст. 5 Закона о национальной платежной системе[1]. При этом из объема данных хищений необоснованно, по нашему мнению, исключаются случаи обналичивания денежных средств.

Так, президиумом Мурманского областного суда в нескольких решениях резюмировано, что по буквальному толкованию положений п. 12 ст. 3 Закона о национальной платежной системе операция снятия наличных денежных средств, совершаемая по картам, эмитированным банком, в устройствах банка (банкоматах и терминалах) рассматриваться как перевод денежных средств в рамках этого Федерального закона не может.

Между тем не учитывается тот факт, что выдача денежных средств в наличной форме через устройство самообслуживания клиентов (банкомат) посредством использования поддельной или принадлежащей другому лицу платежной карты сопровождается одновременным списанием соответствующей суммы с банковского счета потерпевшего.

Данная позиция нашла отражение в постановлении президиума Московского областного суда от 30 октября 2019 г. № 468 по делу № 44у-241/2019. Действия лица, завладевшего платежной картой потерпевшего и тайно осуществившего изъятие денежных средств, находящихся на банковском счете, в наличной форме через устройство самообслуживания клиентов (банкомат), квалифицированы по п. «г» ч. 3 ст. 158 УК РФ.

Аналогичная квалификация хищений имущества, находящегося на счете потерпевшего, подтверждена определением Судебной коллегии по уголовным делам Верховного Суда Российской Федерации (далее – Верховный Суд РФ) от 11 марта 2020 г. № 10-УДп20-1.

Так, по смыслу уголовного закона для квалификации действий виновного по п. «г» ч. 3 ст. 158 УК РФ юридически значимым является то обстоятельство, что предметом преступления выступают денежные средства, находящиеся на банковском счете, а равно электронные денежные средства. Банковская карта лишь инструмент управления денежными средствами, находящимися на банковском счете. При снятии наличных денежных средств через банкомат они списываются непосредственно с банковского счета потерпевшего.

---

[1] См., напр.: постановления президиума Мурманского областного суда от 3 июня 2019 г. № 44у-15/2019, от 7 октября 2019 г. № 44у-31/2019, от 11 ноября 2019 г. № 44у-36/2019; постановление Хабаровского краевого суда от 21 октября 2019 г. № 44у-139/2019. Доступ из СПС «КонсультантПлюс» (дата обращения: 28.12.2021).

В настоящее время аналогичным правовым подходом в отдельных субъектах Российской Федерации руководствуются органы предварительного следствия, прокуратура и суд при принятии решения о квалификации действий лиц, совершивших хищение денежных средств с банковского счета путем обналичивания денежных средств, находящихся на счете платежных карт потерпевших.

В некоторых территориальных органах МВД России, например в Красноярском крае, сложилась практика квалификации действий лица, совершившего кражу денежных средств с причинением значительного ущерба гражданину с банковского счета путем обналичивания в терминале самообслуживания без применения методов социальной инженерии, по п «в» ч. 2 ст. 158 УК РФ. Аргументация данной, по нашему мнению, юридически необоснованной позиции следующая: в случае когда потерпевший самостоятельно передает банковскую карту и пин-код к ней виновному лицу или снятие денежных средств через банкомат осуществляется с найденной банковской карты без использования специальных знаний либо технических средств, квалификация деяния по п. «г» ч. 3 ст. 158 УК РФ (тяжкое преступление) с точки зрения общественной опасности не в полной мере отвечает смыслу уголовного закона.

Приведенные правовые позиции не могут быть поддержаны, поскольку не соответствуют принципу законности.

С целью устранения проблемных аспектов, связанных с квалификацией, а также выработки мер по совершенствованию правоприменительной практики в области противодействия данному виду преступлений рассмотрим ряд вопросов.

Как определить, что совершена кража с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного ст. 159^3 УК РФ)?

Для выявления способа совершения хищения электронных денежных средств необходимо руководствоваться положениями постановлений Пленума Верховного Суда РФ от 27 декабря 2002 г. № 29 «О судебной практике по делам о краже, грабеже и разбое» (далее – постановление ПВС № 29) и от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» (далее – постановление ПВС № 48).

В соответствии с положениями п. 25.1 и 25.2 постановления ПВС № 29:

1. Надлежит квалифицировать как кражу по признаку «с банковского счета, а равно в отношении электронных денежных средств» тайное изъятие денежных средств с банковского счета или электронных денежных средств, например, если безналичные расчеты или снятие наличных денежных средств через банкомат были осуществлены с использованием

чужой или поддельной платежной карты. Подпунктом «г» ч. 3 ст. 158 УК РФ квалифицируются действия лица и в том случае, когда оно тайно похитило денежные средства с банковского счета или электронные денежные средства, использовав необходимую для получения доступа к ним конфиденциальную информацию владельца денежных средств (например, персональные данные владельца, данные платежной карты, контрольную информацию, пароли).

2. Кражу следует считать оконченной с момента изъятия денежных средств с банковского счета их владельца или электронных денежных средств, в результате которой владельцу этих денежных средств причинен ущерб. Местом окончания такой кражи является местонахождение подразделения банка или иной организации, в котором владельцем денежных средств был открыт банковский счет или велся учет электронных денежных средств без открытия счета.

Важно помнить, что кража – это тайное хищение чужого имущества. Способ совершения указанного преступления – тайный. Иными словами, изъятие и/или обращение денежных средств, а равно электронных денежных средств осуществляются в отсутствии потерпевшего или посторонних лиц. Действия обманного характера направлены только на живого человека и при краже могут выступать способом получения конфиденциальной информации от потерпевшего или других лиц для упрощения совершения тайного хищения денежных средств.

Также в соответствии с положениями п. 17 и 21 постановления ПВС № 48:

1. Действия лица будут квалифицироваться как кража и в случаях, когда оно похитило безналичные денежные средства, воспользовавшись необходимой для получения доступа к ним конфиденциальной информацией держателя платежной карты (например, персональными данными владельца, данными платежной карты, контрольной информацией, паролями), переданной злоумышленнику самим держателем карты под воздействием обмана или злоупотребления доверием.

В этих случаях обман или злоупотребление доверием являются лишь способом упрощения доступа к предмету преступления, а непосредственно хищение совершается тайно.

2. В случаях когда хищение совершается путем использования учетных данных собственника или иного владельца имущества, независимо от способа получения доступа к таким данным (лицо тайно либо путем обмана воспользовалось телефоном потерпевшего, подключенным к услуге «мобильный банк»; авторизовалось в системе интернет-платежей под известными ему данными другого лица и т. п.), такие действия подлежат квалификации как кража. При этом изменение данных о состоянии банковского счета и/или о движении денежных средств, происшедшее в результате использования виновным учетных

данных потерпевшего, не может признаваться незаконным воздействием на программное обеспечение серверов, компьютеров или на сами информационно-телекоммуникационные сети.

Если изготовление, приобретение, хранение, транспортировку 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, лицо совершило в целях противоправного деяния, предусмотренного ч. 3 или 4 ст. 158, ч. 3 или 4 ст. 159, ч. 3 или 4 ст. 159^3 либо ч. 3 или 4 ст. 159^6 УК РФ, однако по независящим от него обстоятельствам не смогло довести до конца, то содеянное следует квалифицировать как совокупность приготовления к преступлению и оконченного преступления, предусмотренного ст. 187 УК РФ.

Как определить, что совершено мошенничество с использованием электронных средств платежа?

На сегодняшний день остается нерешенной ситуация привлечения лица к уголовной ответственности за совершение мошенничества с использованием электронных средств платежа. В связи с этим на основании проведенного анализа судебной практики и положений постановлений ПВС № 29 и 48 предлагаем следующий вариант пояснений.

Так, в соответствии со ст. 159 УК РФ мошенничество – это хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.

Следовательно, криминообразующим признаком мошенничества является обман или злоупотребление доверием. Обман представляет собой сообщение заведомо ложных сведений или умолчание о информации, имеющей юридическое значение. Действия обманного характера могут быть направлены только на живого человека (обмануть банкомат, терминал или любой другой механизм невозможно).

Таким образом, мошенничество с использованием электронных средств платежа характеризуется обманом или злоупотреблением доверия в отношении человека (кассира, операциониста банка, работника торговой или иной организации, иного лица), которому предоставляется поддельная или не принадлежащая виновному лицу платежная карта или иное техническое устройство, позволяющее осуществлять перевод денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий (телефона, часов, браслета, пластиковой карты и др.), и последний принимает участие в осуществлении операций по списанию денежных средств с банковского счета.

Преступления, совершенные до начала действия новой редакции ст. 159[3] УК РФ, в соответствии с положениями п. 17 постановления ПВС № 48 (действующее до внесения изменений в июне 2021 г.) следует квалифицировать по указанной норме в случаях, когда хищение имущества осуществлялось с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты путем сообщения уполномоченному работнику кредитной, торговой или иной организации заведомо ложных сведений о принадлежности указанному лицу такой карты на законных основаниях.

Например, *приговором Миасского городского суда Челябинской области К. признан виновным в совершении преступления, предусмотренного ч. 2 ст. 159[3] УК РФ, то есть мошенничества с использованием электронных средств платежа с причинением значительного ущерба гражданину при следующих обстоятельствах: К. в ходе распития спиртных напитков в гостях у своего знакомого, воспользовавшись тем, что последний оставил в комнате на шкафу оформленную на свое имя дебетовую карту ПАО «Почта Банк» с лимитом денежных средств на сумму 9 217 рублей 82 копейки, тайно завладел картой. С целью личного обогащения (хищения денежных средств с банковского счета, открытого в ПАО «Почта Банк») путем обмана работников торговых организаций и умолчания о незаконном владении платежной картой в магазинах, расположенных на территории г. Миасса, К. произвел безналичные расчеты с карты.*

Таким образом, К. незаконными действиями причинил значительный ущерб потерпевшему на общую сумму 8 811 рублей 80 копеек[1].

В случаях если обман не направлен непосредственно на завладение чужим имуществом, а используется только для упрощения доступа к нему, действия виновного, в зависимости от способа совершения хищения, образуют состав кражи или грабежа (п. 2 постановления ПВС № 48).

Анализ правоприменительной практики показал, что в отдельных случаях обман, используемый преступником с целью оплаты похищенной банковской картой приобретаемого в магазине товара, расценивается как средство более простого доступа к имуществу[2].

Если присутствующее при незаконном изъятии чужого имущества лицо не осознает противоправность действий, содеянное квалифицируется как кража чужого имущества (п. 4 постановления ПВС № 29).

Из приведенного выше примера мы можем заключить, что работник торговой организации не осознает незаконность изъятия денежных средств

---

[1] Приговор Миасского городского суда Челябинской области. URL: https://sudact.ru/regular/doc/vG70dKMsd6Yj/ (дата обращения: 27.12.2021).

[2] О подпункте 14.3 решения коллегии: информационное письмо Договорно-правового департамента МВД России от 15 мая 2020 г. № 25/16368. Документ опубликован не был.

и, следовательно, не раскрывает обмана, не зная реального владельца банковской карты. При проведении безналичных расчетов предъявлять документ, удостоверяющий личность, не является обязанностью, а также отметим, что действующими нормативными актами на уполномоченных работников торговых организаций, осуществляющих платежные операции с банковскими картами, обязанность идентификации держателя карты по документам, удостоверяющим его личность, не возлагается[1].

Таким образом, лицо, осуществляющее расчет чужой банковской картой, не обманывает и не вводит в заблуждение работника, хотя совершает действия по умолчанию о незаконном владении им платежной картой.

Неверная на сегодняшний день позиция отражена в апелляционном постановлении Свердловского областного суда от 2 апреля 2018 г. по делу № 22-2232/2018.

Судебная коллегия Восьмого кассационного суда общей юрисдикции приняла решение об изменении приговора и переквалификации действий осужденного Ф., связанных с хищением имущества ФИО, с п. «г» ч. 3 ст. 158 УК РФ на ч. 2 ст. 159[3] УК РФ. Ф., взяв банковскую карту ФИО, желая похитить денежные средства с банковского счета, несколько раз в кафе и магазинах осуществил расчет за товар, произведя операции по списанию принадлежащих ФИО денежных средств. Было похищено 9 310 рублей 90 копеек.

В качестве аргумента судебная коллегия указала, что осужденный совершил преступление, расплатившись за покупки в торговых организациях банковской картой, принадлежащей потерпевшей, умолчав о том, что использует ее незаконно. Выдача Ф. наличных денежных средств посредством банкомата не производилась[2].

Верховный Суд РФ в своем определении однозначно указал, что в данной ситуации имеет место кража с банковского счета, а равно в отношении электронных денежных средств.

С учетом того, что определение способа совершения преступлений, предусмотренных п. «г» ч. 3 ст. 158 и ст. 159[3] УК РФ, влияет на правильную уголовно-правовую оценку деяния, а также ввиду смежности указанных составов преступлений приходим к следующим заключениям.

Отметим, что проблема разграничения квалификации одного и того же деяния по п. «г» ч. 3 ст. 158 и ст. 159[3] УК РФ существует и среди правоприменителей. Принятые в постановлении ПВС № 48 изменения

---

[1] Определение Верховного Суда Российской Федерации от 29 сентября 2020 г. № 12-УДП20-5-К6 (в порядке главы 47.1 УПК РФ). URL: www.consultant.ru/cons/cgi/online.cgi?req=doc&base=ARB&n=640673#0399853207625604 9 (дата обращения: 27.12.2021).

[2] Определение Восьмого кассационного суда общей юрисдикции от 5 марта 2020 г. по делу № 77-38/2020. Доступ из СПС «КонсультантПлюс».

устранили существующую неопределенность в разграничении составов кражи в полном объеме, что, несомненно, будет являться ориентиром для правоприменителя, но вместе с тем необходимо обратить внимание, что вопрос привлечения к уголовной ответственности за мошенничество с использованием электронных средств платежа остался нерешенным, поэтому считаем, что в этой части требуется изменение уголовного закона.

В случаях, когда виновное лицо использует электронные средства платежа одновременно с обманом или злоупотреблением доверием человека для списания денежных средств со счета потерпевшего, его действия будут квалифицированы по ст. 159^3 УК РФ, то есть как мошенничество с использованием электронных средств платежа. Если же происходит оплата бесконтактным способом путем умолчания о незаконном владении им платежной картой или иным средством платежа или без участия иных лиц, то содеянное будет квалифицировано по п. «г» ч. 3 ст. 158 УК РФ как кража с банковского счета, а равно в отношении электронных денежных средств.

Как определить, что совершено мошенничество в сфере компьютерной информации (ст. 159^6 УК РФ)?

В теории уголовного права высказана позиция о том, что мошенничество в сфере компьютерной информации представляет собой самостоятельную форму хищения и не относится к его специальным видам.

Так, Н. А. Лопашенко применительно к ст. 159^6 УК РФ считает более правильным говорить о тайном хищении, поскольку в этой норме «речь идет фактически о фальсификации компьютерной информации <…>, не предполагающей участие в этой схеме конкретного собственника имущества»[1]. Косвенно эту позицию разделяет Верховный Суд РФ. Так, при определении способов совершения мошенничества в п. 1 постановления ПВС № 48 о ст. 159^6 УК РФ даже не упоминается.

Таким образом, обман и/или злоупотребление доверием как способы совершения преступления не характерны для мошенничества в сфере компьютерной информации.

В соответствии с диспозицией ч. 1 ст. 159^6 УК РФ способами совершения мошенничества в сфере компьютерной информации являются ввод, удаление, блокирование, модификация компьютерной информации либо иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, следовательно, способ совершения преступления, предусмотренного ст. 159^6 УК РФ, можно определить как вмешательство в функционирование средств хранения, обработки или

[1] *Лопашенко Н. А.* Законодательная реформа мошенничества: вынужденные вопросы и вынужденные ответы // Криминологический журнал Байкальского государственного университета экономики и права. 2015. Т. 9. № 3. С. 507.

передачи компьютерной информации или информационно-телекоммуникационных сетей.

В соответствии с п. 20 постановления ПВС № 48 под вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей понимается целенаправленное воздействие программных и/или программно-аппаратных средств на серверы, средства вычислительной техники (далее – СВТ) (компьютеры), в том числе переносные (портативные): ноутбуки, планшетные компьютеры, смартфоны, снабженные соответствующим программным обеспечением, или на информационно-телекоммуникационные сети, которое нарушает установленный процесс обработки, хранения, передачи компьютерной информации, что позволяет виновному или иному лицу незаконно завладеть чужим имуществом или приобрести право на него.

Мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа к ней или создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по ст. 272, 273 или 274[1] УК РФ.

Например, *приговором Кировского районного суда г. Екатеринбурга М. признан виновным по ч. 2 ст. 273, ч. 3 ст. 272 и ч. 4 ст. 159[6] УК РФ.*

М., используя свои познания в области компьютерной техники, совместно с другими лицами создал вредоносную компьютерную программу, предназначенную для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации. Программа была распространена на компьютерах ключевых пользователей и других элементах инфраструктуры Сибирского филиала Банка «Т» и использована для совершения хищения денежных средств с его счета. Кроме того, указанными преступными действиями М. осуществил доступ к охраняемой законом компьютерной информации, повлекший ее уничтожение, блокирование, модификацию и копирование.

В результате указанных преступных действий произошло несанкционированное списание денежных средств в размере 997 050 00 рублей. Деньги были перечислены в различных суммах на подконтрольные участникам организованной группы банковские счета неосведомленных о преступном умысле соучастников физических лиц в кредитных организациях, которые были переданы ими в распоряжение участников преступной группы. Последние обналичивали похищенные денежные средства в различных банкоматах и в соответствии с установленной схемой распределяли преступную прибыль[1].

---

[1] Приговор Кировского районного суда г. Екатеринбурга в отношении М. по ч. 2 ст. 273, ч. 3 ст. 272 и ч. 4 ст. 159[6] УК РФ. URL: https://sudact.ru/regular/doc/YwQr7ZHgaQgR/ (дата обращения: 23.12.2021).

Квалификация по совокупности ст. 159^6 и 272 УК РФ вызывает сомнения как среди теоретиков, так и на практике[1]. На наш взгляд, такое положение является необоснованным. Деяние, запрещенное ст. 272 УК РФ, заключается в неправомерном доступе к охраняемой законом компьютерной информации. В диспозиции ст. 159^6 УК РФ неправомерный доступ к компьютерной информации не указан, а следовательно не является способом совершения рассматриваемого преступления. В случае таких противоправных действий, как правильно указал Верховный Суд РФ в своем постановлении, требуется дополнительная квалификация по ст. 272 УК РФ.

В судебной практике встречаются случаи вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей без неправомерного доступа к охраняемой законом компьютерной информации. Тогда дополнительная квалификация по ст. 272 УК РФ не требуется.

Например, *приговором Фрунзенского районного суда г. Саратова гражданка М. признана виновной в совершении преступления, предусмотренного п. «а» ч. 3 ст. 159^6 УК РФ.*

3 января 2017 г. М., занимая должность специалиста по сопровождению корпоративных клиентов Поволжского филиала – Саратовского регионального отделения ПАО «МегаФон» (далее – ПАО), из корыстных побуждений, умышленно, используя свое служебное положение, путем модификации компьютерной информации в информационно-биллинговой системе ПАО незаконно осуществила перевод денежных средств в сумме 7 269 рублей 84 копейки, принадлежащих ПАО, со счета МУ МВД России «Энгельсское» по Саратовской области на свой лицевой счет, зарегистрированный на вымышленное имя «Зотова Н. Н.» и находящийся в пользовании М. В результате гражданка похитила денежные средства, получив реальную возможность ими распоряжаться[2].

Как уже упоминалось ранее, в случаях когда хищение совершается путем использования учетных данных собственника или иного владельца имущества, независимо от способа получения доступа к таким данным (тайно либо путем обмана лицо воспользовалось телефоном потерпевшего, подключенным к услуге «мобильный банк»; авторизовалось в системе интернет-платежей под известными ему данными другого лица и т. п.),

---

[1] См.: *Кибальник А. Г.* Квалификация мошенничества в новом постановлении Пленума Верховного Суда Российской Федерации // Уголовное право. 2018. № 1. С. 61–67.

[2] Приговор Фрунзенского районного суда г. Саратова в отношении М. по п. «а» ч. 3 ст. 159^6 УК РФ. URL: https://sudact.ru/regular/doc/qtCZQWKOpk5x/t (дата обращения: 23.12.2021).

такие действия подлежат квалификации как кража, если виновным не было оказано незаконного воздействия на программное обеспечение серверов, компьютеров или на сами информационно-телекоммуникационные сети. При этом изменение данных о состоянии банковского счета и/или движении денежных средств, произошедшее в результате использования виновным учетных данных потерпевшего, не может признаваться таким воздействием.

Резюмируя изложенное, можно утверждать, что ст. 159^6 УК РФ применяется в том случае, если преступник использует специальную вредоносную компьютерную программу для совершения хищения либо, получив доступ к программному обеспечению серверов, компьютеров или к информационно-телекоммуникационным сетям, незаконно осуществляет ввод, удаление, блокирование или модификацию компьютерной информации в программах, обеспечивающих их работу и/или учет материальных ценностей, и таким образом совершает хищение.

В случае кражи с банковского счета или в отношении электронных денежных средств, а также мошенничества с их использованием воздействие оказывается на электронные средства платежа, а при совершении преступления, предусмотренного ст. 159^6 УК РФ, – на программное обеспечение серверов, компьютеров или информационно-телекоммуникационные сети, обеспечивающие учет денежных средств и иных материальных ценностей.

Также следует отметить, что на основании проведенного анализа, поступивших обзоров судебной практики и опубликованных приговоров по исследуемой категории дел потерпевшим от мошенничества в сфере компьютерной информации, как правило, является организация, обеспечивающая учет, хранение, обработку денежных средств или материальных ценностей, а в других рассматриваемых нами составах – гражданин, имеющий учетную запись в вышеназванных организациях.

Как определить, что совершено простое мошенничество?

Если хищение или приобретение права на чужое имущество осуществляются путем распространения заведомо ложных сведений в информационно-телекоммуникационных сетях, включая сеть «Интернет» (например, создание поддельных сайтов благотворительных организаций, интернет-магазинов, использование электронной почты), то такое мошенничество следует квалифицировать по ст. 159 УК РФ.

Например, Л. в ноябре 2014 года, используя свои знания компьютерной техники, а также имея доступ в сеть «Интернет» с целью получения материальной выгоды, из корыстных побуждений решил совершать хищения денежных средств путем обмана граждан, проживающих на территории разных регионов Российской Федерации, под видом продажи наборов для сбора ручек «ballpoint» следующим образом: для привлечения клиентов разместил в сети «Интернет» на

электронной базе «www.Farpost.ru» сайт «penpoint.ru» о предложении работы на дому по сбору ручек. Если клиент соглашался на приобретение набора для сбора ручек, Л. указывал клиенту реквизиты (номер мобильного телефона, номер QIWI Wallet (киви-кошелек). Не осведомленный о преступных намерениях клиент оплачивал требуемую сумму, переводил денежные средства, а Л., получив от клиента информацию о денежном переводе на свой счет, снимал высланные ему денежные средства и впоследствии тратил их на собственные нужды. Получив денежные средства, Л. прекращал переписку с клиентом.

Кроме того, для конспирации своих преступных намерений Л. пользовался QIWI Wallet, принадлежащим неустановленному в ходе предварительного следствия лицу, а также номерами лицевых счетов абонентских номеров компании «МТС», принадлежащих неустановленным в ходе предварительного следствия лицам. Л. совершил уголовно наказуемые деяния, предусмотренные ч. 2 ст. 159 УК РФ в отношении граждан, проживающих в разных городах Российской Федерации[1].

Необходимо отметить, что в подобных случаях перечисление денег потерпевшими осуществляется с использованием электронных средств платежа, но сам преступник не использует их для совершения противоправных действий. Он может воспользоваться поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной картой, но она выступает не средством совершения преступления (непосредственно участвует при обмане и списании денежных средств со счета лица), а способом сокрытия следов совершения преступления и недопущения его изобличения.

Отметим, что 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, носителей информации, технических устройств, компьютерных программ, предназначенных для неправомерного осуществления приема, выдачи, перевода денежных средств, заведомо непригодных к использованию, образует состав мошенничества и подлежит квалификации по ст. 158[1] или соответствующей части ст. 159 УК РФ.

В случае когда лицо изготовило, приобрело, хранило, транспортировало с целью сбыта указанные средства платежа, заведомо непригодные к использованию, однако по независящим от него обстоятельствам не смогло их сбыть, содеянное должно быть квалифицировано в соответствии с ч. 1 ст. 30 УК РФ как приготовление к мошенничеству, если обстоятельства дела свидетельствуют о том, что эти

[1] Приговор Первомайского районного суда г. Владивостока в отношении Л. по ч. 2 ст. 159 УК РФ. URL: https://sudact.ru/regular/doc/ (дата обращения: 14.04.2022).

действия были направлены на совершение преступлений, предусмотренных ч. 3 или 4 ст. 159 УК РФ.

Как квалифицировать хищения денежных средств, если сумма ущерба не более 2 500 рублей?

В случае если сумма хищения не превышает 2 500 рублей и действия виновного лица формально подпадают под ч. 1 ст. 158, ч. 1 ст. 159, ч. 1 ст. 159^1, ч. 1 ст. 159^2, ч. 1 ст. 159^3, ч. 1 ст. 159^5, ч. 1 ст. 159^6, ч. 1 ст. 160 УК РФ, то имеет место мелкое хищение, предусмотренное ст. 7.27 Кодекса об административных правонарушениях Российской Федерации (далее – КоАП РФ).

В случае если виновное лицо совершило хищение на сумму, не превышающую 2 500 рублей, и при этом в его действиях усматриваются квалифицирующие признаки, предусмотренные п. «г» ч. 3 ст. 158 УК РФ, то содеянное должно квалифицироваться по этой норме уголовного закона.

Например, преступники, похищая (находя) карты, расчет по которым на сумму до 1 000 рублей возможен без введения пин-кода, снимают денежные средства через банкомат, терминал, мобильный банк, кассу самообслуживания, а с учетом определения Верховного Суда РФ от 29 сентября 2020 г. № 12-УДП20-5-К6[1] и в случаях оплаты бесконтактным способом, самое главное без участия уполномоченного работника банка или иной организации, обязанных идентифицировать держателя карты, и причиняют ущерб потерпевшему на сумму, не превышающую 2 500 рублей, то содеянное квалифицируется по п. «г» ч. 3 ст. 158 УК РФ.

Вопрос конкуренции ст. 7.27 КоАП РФ и ст. 158–160 УК РФ нельзя путать с положениями о возможности применения к уголовно наказуемому хищению ч. 2 ст. 14 УК РФ, согласно которой не является преступлением действие (бездействие), хотя формально и содержащее признаки противоправного деяния, предусмотренного УК РФ, но в силу малозначительности не представляющее общественной опасности. В мелком хищении состав уголовно наказуемого деяния отсутствует и формально[2].

Малозначительность деяния является оценочным понятием и определяется крайне небольшой степенью вреда, причиненного преступлением, и направленностью умысла лица на нанесение именно незначительно вреда. В силу этого обстоятельства деяние, формально подпадающее под признаки преступления, не представляет общественной опасности.

---

[1] Определение Верховного Суда Российской Федерации от 29 сентября 2020 г. № 12-УДП20-5-К6 (в порядке главы 47^1 УПК РФ). URL: www.consultant.ru/cons/cgi/online.cgi?req=doc&base=ARB&n=640673#03998532076256049 (дата обращения: 23.12.2021).

[2] См.: *Яни П. С.* Квалификация хищений: момент окончания, безвозмездность, ущерб // Законность. 2015. № 12. С. 43–47.

Также необходимо помнить, что общественная опасность преступления характеризуется не только размером причиненного имущественного ущерба, но и способом его совершения, формой вины и другими обстоятельствами. Необходимо отметить, что вопрос о малозначительности хищения решается в каждом конкретном случае в зависимости от материального положения потерпевшего и с учетом всех обстоятельств произошедшего[1].

Также в соответствии с положением п. 25.4 постановления ПВС № 29 при решении вопроса, является ли малозначительным деяние, например кража, формально содержащая квалифицирующие признаки состава данного преступления, судам необходимо учитывать совокупность таких обстоятельств, как степень реализации преступных намерений, размер похищенного, роль подсудимого в преступлении, совершенном в соучастии, характер обстоятельств, способствовавших совершению деяния, и др.

Необходимо отметить, что в исследованной нами судебной практике прекращение уголовного дела в связи с малозначительностью всегда сопровождалось переквалификацией на ч. 1 ст. 158 УК РФ или ч. 1 ст. 159^3 УК РФ, примеров применения ч. 2 ст. 14 УК РФ нами не было обнаружено.

В качестве примера вышеизложенного приведем постановление о прекращении уголовного дела в связи с отказом государственного обвинителя от обвинения Киржачского районного суда Владимирской области в отношении И. Гражданину было предъявлено обвинение в совершении кражи, то есть тайном хищении чужого имущества с банковского счета (п. «г» ч. 3 ст. 158 УК РФ).

15 октября 2019 г. И., находясь на автомобильной стоянке у магазина «Пятерочка», нашел пластиковую банковскую карту. У него возник преступный умысел, направленный на тайное хищение чужих денежных средств, то есть на совершение с корыстной целью противоправного безвозмездного изъятия и обращения в свою пользу чужого имущества (денежных средств).

Реализуя преступный умысел, действуя из корыстных побуждений, И. в магазине «Чайка» совершил банковскую операцию, расплатившись способом бесконтактной оплаты, то есть путем приложения найденной банковской карты к считывающему устройству для списания денежных средств за покупки (две пачки сигарет марок «Winston» и «Parlament Aqua») общей стоимостью 332 рубля 00 копеек. Тем самым И. совершил тайное хищение с банковской карты средств, принадлежащих

[1] О направлении информации по хищениям денежных средств с банковских счетов граждан в адрес Следственного департамента МВД России: информационное письмо Главного управления МВД России по Красноярскому краю от 30 апреля 2020 г. № 4/5832. Документ опубликован не был.

потерпевшему, и причинил своими преступными действиями материальный ущерб в указанном размере.

В ходе судебного разбирательства государственный обвинитель О. заявил, что в соответствии с п. 17 постановления Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» действия лица следует квалифицировать по ст. 159³ УК РФ: хищение имущества осуществлялось с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты путем сообщения уполномоченному работнику кредитной, торговой или иной организации заведомо ложных сведений о ее принадлежности на законных основаниях либо путем умолчания о незаконном владении картой.

Следовательно, в действиях И. не содержится признаков кражи, и они были переквалифицированы с п. «г» ч. 3 ст. 158 УК РФ на ч. 1 ст. 159³ УК РФ.

Учитывая положения ч. 1 ст. 7.27 КоАП РФ, определяющие размер хищения чужого имущества, представитель государственного обвинения О., руководствуясь ч. 7 ст. 246 УПК РФ, придя к убеждению о том, что имеющиеся в уголовном деле доказательства не подтверждают предъявленное И. обвинение, отказался от поддержания обвинения в отношении подсудимого И. по ч. 1 ст. 159³ УК РФ.

Уголовное дело было прекращено по п. 2 ч. 1 ст. 24 Уголовно-процессуального кодекса Российской Федерации (далее – УПК РФ) за отсутствием в деянии состава преступления[1].

Например, апелляционным определением Судебной коллегии по уголовным делам Самарского областного суда от 16 октября 2019 г. № 22-6241 приговор по обвинению К. по ч. 3 ст. 30, п. «г» ч. 3 ст. 158 УК РФ отменен, уголовное дело прекращено на основании п. 2 ч. 1 ст. 24 УПК РФ за отсутствием в его действиях состава преступления.

Судебная коллегия в определении указала, что из предъявленного К. обвинения следует, что он лишь прикладывал карту к платежному терминалу, не вводя при этом специальный код и не используя никакой контрольной и/или конфиденциальной информации. Незаконное и несанкционированное воздействие на информационно-коммуникационные сети, компьютеры, серверы или их программное обеспечение осужденным не осуществлялось. При таких обстоятельствах действия К. надлежит квалифицировать по ч. 1 ст. 158 УК РФ, однако, исходя из размера

[1] Постановление о прекращении уголовного дела в связи с отказом государственного обвинителя от обвинения по делу № 1-139/2019 Киржачского районного суда Владимирской области от 30 декабря 2019 г. № 1-139/2019. URL: https://sudact.ru/regular/doc/MLSBvwPvs0HS/ (дата обращения: 23.12.2021).

похищенного (2 163 рубля 02 копейки), его действия не образуют состава преступления[1].

Также считаем важным обратить внимание на вопрос о том, ***что является моментом окончания совершения и местом преступления при хищении денежных средств с банковского счета, а равно в отношении электронных денежных средств потерпевшего?***

Хищения чужого имущества по законодательной конструкции объективной стороны относятся к материальным составам преступления: момент его окончания связан с наступлением общественно опасных последствий, в частности, когда виновное лицо причинило ущерб собственнику имущества. Ущерб считается причиненным, если лицо получило реальную возможность этим имуществом пользоваться или распоряжаться по своему усмотрению.

Отметим, что практика высшего судебного органа исходит из того, что моментом окончания хищения является время, когда имущество изъято и виновный имеет реальную возможность им пользоваться или распоряжаться по своему усмотрению (например, обратить похищенное имущество в свою пользу или в пользу других лиц, распорядиться им с корыстной целью иным образом)[2], когда указанное имущество поступило в незаконное владение виновного или других лиц и они получили реальную возможность (в зависимости от потребительских свойств этого имущества) пользоваться или распоряжаться им по своему усмотрению.

Учитывая тот факт, что безналичные денежные средства, в том числе электронные, по смыслу положений примеч. 1 к ст. 158 УК РФ и ст. 128 ГК РФ в полной мере отвечают всем критериям предмета преступления, хищение средств следует считать оконченным с момента их изъятия у владельца и фактического причинения ему ущерба[3]. В остальных случаях, пока не появилось реальной возможности распоряжения похищенными средствами, преступление будет считаться неоконченным.

Традиционно под местом совершения преступления понимаются определенная территория, часть пространства, где оно совершено[4]. Так как преступление – это общественно опасное деяние, следовательно, и место совершения преступления – это место совершения такого деяния.

---

[1] Апелляционное определение Судебной коллегии по уголовным делам Самарского областного суда от 16 октября 2019 г. № 22-6241. URL: https://bsr.sudrf.ru (дата обращения: 23.12.2021).

[2] О судебной практике по делам о краже, грабеже и разбое: постановление Пленума Верховного Суда Российской Федерации от 27 декабря 2002 г. № 29 // Бюллетень Верховного Суда Российской Федерации. 2003. № 2.

[3] О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 // Бюллетень Верховного Суда Российской Федерации. 2018. № 2.

[4] См.: Уголовное право России. Общая часть: курс лекций / под ред. А. П. Кузнецова, Е. Е. Черных. Нижний Новгород, 2019.

Местом совершения преступления является определенная территория, часть пространства, где совершено общественно опасное деяние.

Общественно опасное деяние можно рассматривать как обязательный признак объективной стороны состава преступления. Деяние может выражаться как в форме действия, так и в форме бездействия виновного в совершении преступления. В зависимости от описания признаков конкретного состава преступления в УК РФ может по-разному определяться и место его совершения. Так, например, при хищении общественно опасное деяние заключается в противоправном безвозмездном изъятии и/или обращении чужого имущества в пользу виновного или других лиц. Место совершения хищения – это территория, часть пространства, где преступник осуществляет изъятие или обращение чужого имущества.

При простой краже, грабеже, разбое или мошенничестве место совершения преступления – это место изъятия чужого имущества; те места, где преступник непосредственно находился с потерпевшим либо иным лицом, используемым для совершения преступления (кассир в магазине, операционист в банке, регистратор и др.) путем его обмана или злоупотребления доверием.

С развитием науки и техники все больше появляется возможностей совершения преступлений удаленно – без непосредственного контакта с потерпевшим или иными лицами. Такая форма на первоначальном этапе расследования каждый раз вызывает сложности в определении именно места совершения общественно опасного деяния.

Учитывая классические изыскания, под местом совершения хищения денежных средств с банковского счета, а равно в отношении электронных денежных средств, следует понимать то место, где осуществлялись преступные действия.

Например, если изъятие денежных средств осуществляется с использованием компьютера, то место его расположения с привязанным IP-адресом и является местом совершения преступления[1]; если применяется мобильное устройство, то местом преступления является место выхода в сеть телефона (абонентского устройства), с которого в банк поступило смс-сообщение с кодом подтверждения перевода электронных денежных средств; если банковской карты – место, где осуществляется снятие денежных средств с этой карты (банкомат, отделение банка, магазин и прочее), однако с учетом существующих технологий место выхода

[1] В рамках учебного пособия не будут рассматриваться особенности отображения и фиксации следов преступной деятельности в информационной и компьютерной среде, в том числе способы идентификации лица при использовании IP-адресации. См.: Основы раскрытия и расследования мошеннических действий, совершенных с использованием средств сотовой связи и сети «Интернет»: методические рекомендации УУР УМВД России по Тамбовской области. Тамбов, 2018.

устройства в сеть может быть подменено либо скрыто. В таком случае определить место совершения хищения денежных средств с банковского счета, а равно в отношении электронных денежных средств невозможно либо требует достаточно длительного времени.

Если преступление совершается с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет», то местом следует считать фактическое местонахождение лица, откуда оно осуществляло общественно опасные деяния, непосредственно направленные на изъятие денежных средств. К таким действиям можно отнести следующие: незаконное воздействие на программное обеспечение серверов, компьютеров или на сами информационно-телекоммуникационные сети; изменение данных о состоянии банковского счета и/или о движении денежных средств, происшедшее в результате использования виновным учетных данных потерпевшего.

Место производства предварительного расследования регламентировано ст. 152 УПК РФ. По общему правилу оно должно производиться там, где было совершено деяние, содержащее признаки преступления.

В соответствии с положением п. 25.3 постановления ПВС № 29 территориальную подсудность уголовного дела о краже денежных средств с банковского счета или электронных денежных средств судам следует определять с учетом места совершения преступления, а также других указанных в законе обстоятельств (ч. 1–3 и 5^1 ст. 32 УПК РФ). В случае если не все участники производства по такому делу проживают на территории, на которую распространяется юрисдикция суда, и все обвиняемые согласны на изменение территориальной подсудности данного уголовного дела, а также в иных случаях, указанных в ч. 4 ст. 32 и в ст. 35 УПК РФ, территориальная подсудность уголовного дела может быть изменена.

Таким образом, учитывая судебную практику, а также положение постановления ПВС № 29, целесообразно полагать, что местом окончания преступления, предусмотренного п. «г» ч. 3 ст. 158 УК РФ, является местонахождение подразделения банка или иной организации, в котором владельцем денежных средств был открыт банковский счет или велся учет электронных денежных средств без открытия счета.

Проанализировав правоприменительную практику, авторы учебного пособия пришли к следующим выводам.

1. Ряд регионов имеют проблемы, связанные с вопросами правильной квалификации хищений денежных средств с банковского счета, а равно в отношении электронных денежных средств.

2. При решении вопроса квалификации необходимо руководствоваться положениями уголовного закона Российской Федерации, постановлений Пленума Верховного Суда РФ от 27 декабря 2002 г. № 29 «О судебной

практике по делам о краже, грабеже и разбое» и от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», а также определения Верховного Суда РФ от 29 сентября 2020 г. № 12-УДП20-5-К6 (в порядке главы 47^1 УПК РФ).

3. При решении вопроса, связанного с разграничением кражи с банковского счета, а равно в отношении электронных денежных средств от смежных составов, необходимо определить способ совершения хищения денежных средств и руководствоваться основными положениями постановлений Пленума Верховного Суда РФ от 27 декабря 2002 г. № 29 и от 30 ноября 2017 г. № 48.

4. Вопрос о малозначительности хищения решается в каждом конкретном случае в зависимости от материального положения потерпевшего и с учетом всех обстоятельств произошедшего.

5. При определении момента окончания и установлении места совершения хищения с банковского счета, а равно в отношении электронных денежных средств (п. «г» ч. 3 ст. 158 УК РФ) необходимо руководствоваться положением п. 25.2 постановления Пленума Верховного Суда РФ от 27 декабря 2002 г. № 29 «О судебной практике по делам о краже, грабеже и разбое».

Вопросы для самоконтроля

1. Что понимается под электронными денежными средствами в соответствии с Федеральным законом от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе»?
2. Что является предметом кражи с банковского счета, а равно в отношении электронных денежных средств?
3. Чем необходимо руководствоваться при решении вопроса, связанного с разграничением кражи с банковского счета, а равно в отношении электронных денежных средств от смежных составов?
4. Как необходимо квалифицировать действия лица, совершившего преступление, предусмотренное ч. 1 ст. 159^3 УК РФ, если сумма ущерба составила 2 500 рублей или менее?
5. Что является моментом окончания совершения преступления при хищении денежных средств с банковского счета, а равно в отношении электронных денежных средств потерпевшего?
6. Что является местом преступления при хищении денежных средств с банковского счета, а равно в отношении электронных денежных средств потерпевшего?

Практическое задание

Ситуация: в 2021 году четверо несовершеннолетних детей остались сиротами. Над ними оформила опеку двоюродная бабушка, которая создавала им комфортные условия жизни. Государство в свою очередь перечисляло на ее личный счет денежные средства, полагающиеся несовершеннолетним по случаю потери кормильца.

Родной сын женщины-опекуна знал об этом и перевел себе на счет 300 тысяч рублей, принадлежавших двум детям. О пропавших деньгах женщина узнала случайно, после чего она обратилась в правоохранительные органы.

Квалифицируйте деяние и обоснуйте свой ответ.

РАЗДЕЛ 2. ОСОБЕННОСТИ ПРОИЗВОДСТВА ОТДЕЛЬНЫХ СЛЕДСТВЕННЫХ И ИНЫХ ПРОЦЕССУАЛЬНЫХ ДЕЙСТВИЙ В КОНКРЕТНЫХ СЛЕДСТВЕННЫХ СИТУАЦИЯХ ПО УГОЛОВНЫМ ДЕЛАМ О ХИЩЕНИЯХ ЭЛЕКТРОННЫХ ДЕНЕЖНЫХ СРЕДСТВ, В ТОМ ЧИСЛЕ СОВЕРШЕННЫХ ПОСРЕДСТВОМ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Производство следственных действий при расследовании уголовных дел о хищениях электронных денежных средств, в том числе совершенных посредством использования информационно-телекоммуникационных сетей, требует от следователя знаний в области юриспруденции, экономики и финансов.

Подавляющее большинство преступлений рассматриваемой категории совершается с использованием сети «Интернет», выход в которую не может быть осуществлен без применения компьютерной техники. Таким образом, следователь должен обладать еще и специальными знаниями в сфере высоких технологий и компьютерной информации. В настоящее время с сожалением можно констатировать тот факт, что такими навыками владеет минимальная часть сотрудников. Данное обстоятельство с учетом роста количества уголовных дел рассматриваемой категории является весьма неутешительным и выступает одной из главных проблем, обсуждаемых территориальными следственными органами.

Кроме того, способы совершения хищений электронных денежных средств, в том числе посредством использования информационно-телекоммуникационных сетей, постоянно видоизменяются и имеют все более изощренные приемы маскировки.

Учитывая данную ситуацию, следователям необходимо применять передовые методики расследования и тактики производства следственных действий, а также рекомендуется консультироваться с профильными специалистами, а в случае необходимости привлекать их в качестве участвующих лиц.

В зависимости от квалификации конкретного преступления и следственной ситуации обстоятельства, подлежащие установлению, могут варьироваться, однако, учитывая специфику рассматриваемой категории уголовных дел, алгоритм их расследования во многом совпадает.

В настоящем разделе представлены основные понятия и термины, используемые при расследовании уголовных дел рассматриваемой категории; особенности наиболее значимых, обладающих спецификой следственных и процессуальных действий, а также решений, производимых при расследовании уголовных дел о хищениях электронных денежных средств, в том числе совершенных посредством использования информационно-телекоммуникационных сетей: допрос, производство

обыска, назначение и производство судебной экспертизы, направление запросов.

Как было отмечено ранее, практически все преступления рассматриваемой категории не могут быть совершены без выхода в интернет и соответственно без использования технических устройств – компьютеров, сотовых телефонов, планшетов и т. п. Именно эта техника является одним из главных источников доказательственной информации, так как посредством нее лица, совершающие противоправные деяния, дистанционно контактируют с потерпевшим в различных социальных сетях и на сайтах, осуществляют онлайн-транзакции, администрирование виртуальными счетами различных систем электронных платежей. Данные сведения, как правило, хранятся с помощью накопителей на жестких магнитных дисках, ssd-накопителях и в оперативной памяти этих устройств.

Таким образом, для успешного расследования уголовного дела и установления по нему истины одними из первостепенных задач следователя являются установление местонахождения СВТ, которые выступают в качестве средства совершения преступления, и последующее их изъятие в установленном законом порядке с целью дальнейшего осмотра и назначения компьютерной экспертизы.

Для осуществления целей, обозначенных выше, следователю необходимо обладать знаниями в области компьютерной информации, непосредственно связанными с процедурой выхода в интернет, и, в частности, владеть основными терминами и понятиями, применяемыми в ходе расследования всех уголовных дел о преступлениях, совершенных с использованием данной информационно-телекоммуникационной сети.

Рассмотрим некоторые из них:

1. Интернет-сайт (*web-site*: *web* – «паутина, сеть», *site* – «место») – это интернет-ресурс, который включает в себя объединенные ссылками и общей структурой документы (веб-страницы). Также применимы названия «веб-сайт», «сайт».

Интернет-сайты располагаются на специальных серверах, предоставляемых хостинговыми компаниями (также хостинг-провайдеры) как на платной, так и бесплатной основах. Услуга по предоставлению ресурса для размещения информации на сервере называется хостингом. В свою очередь наименование сайта (его символьное имя, которое следует за обозначением всемирной сети *«www.»*) называется доменным адресом (также доменом, доменным именем); например, *instagram.com, facebook.com, rt.ru* и т. д.

2. Интернет-браузер (*web-browser*) – это прикладная программа, предназначенная для загрузки и просмотра страниц, скачивания файлов, управления приложениями и решения других задач в сети «Интернет»; например, *Yandex.browser, Firefox, Internet Explorer* и др.

Интернет-браузер при определенных настройках сохраняет историю посещений сайтов, а также cookie-файлы и cache-файлы; запоминает пароли и логины к определенным сайтам; предоставляет широкий спектр иных возможностей, например, создание личного кабинета, который открывает доступ к пользованию всеми ресурсами и службами (ЮМани; Яндекс.Музыка; Яндекс.Почта и т. д.).

3. IP-адрес (*Internet Protocol Address*) – это уникальный сетевой адрес узла в компьютерной сети. Для выхода в интернет устройство (компьютер, планшет, мобильный телефон и др.) использует IP-адрес, предоставленный интернет-провайдером. Существует несколько версий IP-адресов, в частности «IPv4» и «IPv6». В настоящее время наиболее распространенной является версия «IPv4», которая представляет собой 32-битное число, записанное в виде четырех десятичных чисел со значением от 0 до 255, разделенных между собой точками, например, 172.13.235.2.

IP-адреса условно делятся на:

– внешние (публичные, глобальные) – для выхода в интернет;

– внутренние (локальные, частные) – для работы в локальной сети;

– динамические – выдаются из свободного в конкретный момент диапазона адресов; меняются при каждом новом выходе в сеть;

– статические – неизменны; привязываются к каждому устройству автоматически либо вручную и сохраняются в дальнейшем за ним.

Органы предварительного следствия, располагая данными об IP-адресе и сделав соответствующий запрос интернет-провайдеру, имеют возможность установления сведений о лице, которому был предоставлен конкретный IP-адрес в соответствии с заключенным договором об оказании услуг связи (ФИО, место проживания, номер телефона, тарифный план и т. д.), что соответственно повышает вероятность установления местонахождения вычислительной техники, с помощью которой осуществлялся выход в сеть «Интернет», которая, в свою очередь, считается весьма ценным доказательством, так как является средством совершения преступления. При этом отметим, что точное установление местонахождения СВТ более вероятно в том случае, если соединение происходит посредством проводного соединения, то есть подключения напрямую к СВТ либо через маршрутизатор (например, Wi-Fi-роутер). В случае если выход в сеть «Интернет» происходит посредством мобильного телефона либо планшета и т. д., например с помощью LTE- либо 3G-соединения, то установление точного местоположения СВТ становится более затруднительным ввиду мобильности устройства. Иными словами, установление точного местонахождения СВТ в момент подключения к сети «Интернет» возможно, однако вероятность его нахождения в том же месте по прибытии сотрудников правоохранительных органов значительно ниже, нежели чем при

указанном выше стационарном (проводном) соединении, так как подключение к сети «Интернет» через LTE- и 3G-сети может происходить абсолютно в любом месте, не привязанном к месту проживания, либо работы, либо иному помещению, оснащенному стационарным узлом для выхода в сеть «Интернет».

Однако при запросе необходимой информации об IP-адресах у администрации интернет-сайта либо интернет-провайдера стоит учитывать некоторые нюансы адресации в сети «Интернет»: NAT и VPN (краткий принцип действия рассмотрим ниже).

4. NAT (*Network Address Translation* – «преобразование сетевых адресов») – это специальный механизм, реализованный в сетях «TCP», «IP», который позволяет изменять IP-адреса пересылаемых пакетов (внутренних или частных IP, которые присылаются на сетевой шлюз) во внешние (глобальные) с последующей отправкой в сеть «Интернет». Такие пакеты нередко называют транзитными.

Данная технология возникла в связи с критической нехваткой IP-адресов версии «IPv4», в которой максимальное количество адресов может достигать до 4,3 млрд. В целях устранения проблемы еще до создания адресов версии «IPv6» была разработана технология «NAT».

С технической точки зрения данная технология довольно тяжела для полного понимания, особенно без имеющихся минимальных знаний об устройстве адресации в сети «Интернет», однако если говорить максимально просто, то одним из достоинств NAT является расширение диапазона IP-адресов, в том числе вплоть до предоставления одного IP-адреса нескольким пользователям одновременно. Логично предположить, что применение данной технологии может создать существенные препятствия в расследовании уголовных дел.

Следователь истребует сведения об абоненте у интернет-провайдера, которому были предоставлены в пользование конкретные IP-адреса; он должен указывать точное время обращения и конкретное наименование ресурса. В противном случае интернет-провайдер может дать ответ о том, что интересующий IP-адрес в определенный момент времени был предоставлен сразу нескольким десяткам, а может быть и сотням лиц.

Таким образом, конкретизация запрашиваемых сведений существенно сужает круг лиц, которым предоставлялся интересующий следствие IP-адрес, что позволит в короткие сроки провести анализ полученного ответа и скоординировать дальнейшие действия.

К сожалению, проблема, возникающая в результате использования технологии «NAT», не единственная. Преступники, совершая хищения, зачастую используют способы анонимизации. Самыми популярными из них являются технологии «VPN».

5. VPN (*Virtual Private Network* – «виртуальная частная сеть») – общее наименование технологий, которые позволяют обеспечить одно или

несколько сетевых соединений (логическую сеть) поверх другой сети. Упрощенный принцип действия VPN выглядит следующим образом.

В сети каждому пользователю интернет-провайдером дается IP-адрес, а в свою очередь VPN-сервис предоставляет подменный IP-адрес, принадлежащий в подавляющем большинстве случаев иностранному интернет-провайдеру, который физически может находиться в любой части города, страны, а как правило, на территории иностранных государств. Очевидно, что данный факт значительно осложняет расследование уголовного дела как с процессуальной, так и технической точек зрения и в итоге заводит следствие в тупик.

На сегодняшний день гарантированных способов деанонимизации VPN не существует, однако некоторые из них могут быть эффективны в определенной степени, например, используемые многими сайтами cookie-файлы.

6. Cookie-файлы – это небольшие фрагменты текстовых файлов, отправляемые веб-сервером браузеру и хранящиеся в памяти компьютера либо иного технического устройства.

Интернет-браузер при открытии страницы сайта пересылает фрагменты текстовых файлов веб-серверу в составе HTTP-запроса. В дальнейшем при повторном обращении к данному сайту он уже будет узнавать пользователя и располагать о нем определенной информацией. Другими словами, сервер обменивается с браузером различного рода данными о веб-сайтах, посещаемых пользователем. Например, данные файлы могут содержать сведения о статистике посещений сайтов, логинах и паролях от личных кабинетов пользователей сайтов или сервисов, сведения о регионе, а также о запросах, сделанных пользователем в поисковой строке браузера. Данная информация анализируется сервером и в последующем пользователю не приходится каждый раз вводить логин и пароль при обращении к конкретному ресурсу.

Также при работе в сети периодически могут появляться всплывающие рекламные окна с предложениями о покупке того или иного товара, составленными на основе запросов пользователя, а также часто посещаемых интернет-страниц. Например, при выборе онлайн-кинотеатров пользователю предлагаются к просмотру фильмы, сделанные на основе его личных предпочтений. Такое положение основано на анализе cookie-файлов, получаемых сервером.

Необходимо отметить, что cookie-файлы не подвержены изменениям, в том числе в случаях, когда соединение происходит с использованием VPN. Из этого замечания следует, что при истребовании информации у администрации сайтов о предоставлении IP-адресов необходимо также запросить сведения о cookie-файлах и произвести их анализ. Эти меры помогут идентифицировать устройство, с которого осуществлялся выход в сеть, а в некоторых случаях – его местонахождение. Кроме того,

результаты анализа полученных cookie-файлов могут быть эффективно применены при проверке лица на причастность к совершению иных аналогичных преступлений, совершенных именно с данного интернет-браузера и технического устройства.

Рассматриваемый вид преступлений отличается вариативностью и неординарностью, в связи с чем их расследование нельзя описать единым алгоритмом. Эффективность предварительного следствия зависит во многом от инициативности следователя, творческого подхода и отсутствия «шаблонного» мышления. Ниже нами будут приведены рекомендации по производству отдельных следственных и иных процессуальных действий, однако следует учитывать, что в большей степени они являются ориентирующими и в зависимости от следственной ситуации должны модифицироваться.

Говоря о специфике производства следственных и иных процессуальных действий по уголовным делам о хищениях электронных денежных средств, совершенных в том числе с использованием информационно-телекоммуникационных сетей, следует заметить, что указанная категория преступлений является неоднородной по своему составу, соответственно и специфика их расследования имеет некоторые отличия.

В связи с изложенными обстоятельствами целесообразно объединить данные хищения в четыре агрегированные группы, которые также имеют свои подгруппы.

1. Преступник завладел банковской картой потерпевшего и при ее использовании совершил хищение денежных средств.

Данная группа преступлений представляется наименее сложной в доказывании, но при этом занимает немалую долю среди общего количества рассматриваемой категории хищений. Зачастую действия преступника в этих случаях сводятся либо к обналичиванию денежных средств через банкомат, либо к оплате картой товаров или услуг на кассе.

Ключевая информация при складывающейся ситуации появляется в первую очередь в рамках осуществления процессуальных действий с потерпевшим лицом.

1.1. При допросе потерпевшего выясняются следующие обстоятельства:

– сведения в отношении банковской карты и счета, с которого были похищены денежные средства (наименование банка, дата открытия счета по банковской карте, реквизиты данного счета, тип карты, ее номер, срок действия, остаток денежных средств на момент хищения, сведения об использовании услуг «Мобильный банк» и «Онлайн-банк»; если потерпевший – пользователь системы электронных платежей (например, QIWI, ЮМани и др.), необходимо указать реквизиты виртуальных электронных кошельков и карт, сведения о привязке их к банковским

картам систем «Visa», «MasterCard» и др., электронным почтовым ресурсам, телефонным номерам);

– сведения о местонахождении и владении банковской картой (место хранения, когда, кому и по каким причинам карта передавалась и др.);

– обстоятельства хищения (когда и каким образом стало известно о хищении, способ хищения, личность лица, похитившего денежные средства и др.);

– иные сведения (исходя из обстоятельств, сообщенных заявителем).

1.2. Сведения, сообщенные потерпевшим, являются идеальными следами преступления, ввиду чего целесообразно их закрепление соответствующими процессуальными действиями: в первую очередь получить их в распоряжение следствия, изучить и приобщить к материалам уголовного дела. Например, выписку по счету можно получить непосредственно от потерпевшего после того, как он ее запросит в банке, либо получить от сотрудников оперативного аппарата. Также справки по банковским счетам предоставляются по запросу следователя с согласия руководителя следственного органа в соответствии со ст. 26 Федерального закона от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности» (далее – Закон о банках и банковской деятельности).

Изучая справку по счету, необходимо обратить внимание на способ списания денежных средств: оплата товара на кассе; оплата товара в интернет-магазине; снятие наличных в банкомате и др. Это обстоятельство будет влиять на квалификацию преступления (см. раздел 1 о квалификации по ст. 158 и 159^3 УК РФ; особое внимание обратить на сумму ущерба).

Кроме того, необходимо предпринимать безотлагательные меры, направленные на изъятие видеозаписи с камер наблюдения, установленных в местах списания денежных средств со счета потерпевшего (банкомат, магазин и др.).

1.3. К специфике данной группы преступлений следует также отнести необходимость установления обстоятельств распоряжения похищенным имуществом. Для этого целесообразно:

– изымать приобретенные на похищенные денежные средства предметы, а также документы, подтверждающие их приобретение;

– запрашивать сведения о наличии похищенных денежных средств на банковских счетах, абонентских счетах иных лиц, в случае их наличия предпринимать меры к наложению ареста на имущество.

2. Преступник завладел сведениями о банковской карте (номер, ФИО владельца, срок действия, CVV/CVN-код) и при их использовании совершил хищение денежных средств потерпевшего.

Примерами преступлений данной группы могут быть следующие: мошенник обращается по объявлению, размещенному, например на платформе «Авито», и под предлогом внесения предоплаты за товар выясняет указанные реквизиты карты, после чего похищает денежные

средства путем их перевода на иные счета или оплаты товаров в интернет-магазинах; мошенник под предлогом разблокировки банковского счета узнает информацию о банковской карте потерпевшего.

В большинстве случаев при списании денежных средств при указанных обстоятельствах проходит двойная верификация платежа: реквизиты карты и код из смс-сообщения, который также сообщается преступнику потерпевшим, однако функционируют интернет-магазины, осуществляющие платежи только при предоставлении реквизитов банковской карты.

Ключевая информация при складывающейся ситуации также появляется в рамках осуществления процессуальных действий с потерпевшим лицом.

2.1. Сведения, которые необходимо выяснить у потерпевшего, а также способы документального подтверждения события преступления отражены в п. 1.1 и 1.2 настоящего раздела. Указанные преступления квалифицируются по п. «г» ч. 3 ст. 158 УК РФ, независимо от суммы ущерба (подробнее см. раздел 1).

2.2. Ход расследования осуществляется по трем следовым направлениям:

2.2.1. Абонентский номер лица, при использовании которого связывались с потерпевшим.

Необходимо провести следственное действие, направленное на получение информации о соединениях между абонентами и/или абонентскими устройствами с целью выяснения следующей информации:

– о персональных данных лица, на которое зарегистрирован абонентский номер, и сведений об IMEI-номерах абонентских устройств, в которых была установлена сим-карта с указанным абонентским номером, за интересующий следствие период;

– соединениях между абонентскими устройствами с указанным абонентским номером и иными абонентами за интересующий следствие период с указанием установочных данных абонентов оператора сотовой связи и адресов базовых станций, к которым происходило подключение указанных абонентских номеров, секторов их действия, азимута направленности использованных антенных блоков и угла охватываемой ими территории;

– входящих и исходящих платежах по лицевому счету абонентского номера;

– IP-адресах, предоставленных провайдером абоненту для выхода в интернет;

– копиях регистрационной формы при продаже и регистрации сим-карты.

В случае если абонентский номер относится к SIP-телефонии, необходимо также устанавливать следующие сведения:

– каким образом была произведена регистрация номера, регистрационные данные абонента (иные абонентские номера, адреса электронной почты и др.);

– об IP-адресах, использованных для регистрации абонентского номера;

– IP-адресах, использованных для входа в личный кабинет, панель управления по администрированию данным абонентским номером для осуществления звонков;

– абонентских номерах, на которые осуществлялась переадресация звонков;

– статистику звонков за интересующий период;

– информацию об оплате услуг связи с указанием полных реквизитов плательщика.

Исходя из полученной в результате данного следственного действия информации, необходимо производство следующих следственных и иных процессуальных действий:

а) ориентирование оперативного аппарата на установление лица, на которое зарегистрирован конкретный абонентский номер, или лиц по новым абонентским номерам, фигурируемым в исходной информации;

б) при установлении таких лиц осуществление их допроса по обстоятельствам уголовного дела;

в) по адресам электронной почты необходимо:

– производство выемки у провайдеров входящих и исходящих сообщений и их последующего анализа с целью дальнейшего установления обстоятельств, имеющих значение для уголовного дела;

– установление IP-адресов, с которых осуществлялось подключение к электронной почте;

г) установление по IMEI-номерам марок и моделей используемых телефонов и в дальнейшем ориентированность на их изъятие в ходе дальнейшего расследования;

д) осуществление анализа по детализации соединений места нахождения по базовым станциям и круга абонентов, с которыми устанавливалось соединение. При наличии звонков на горячие линии различных компаний организация изъятия аудиозаписи разговоров с целью получения образцов голоса подозреваемого;

е) производство анализа по лицевым счетам о движении денежных средств и направление дополнительных запросов в случае установления сомнительных переводов;

ж) по IP-адресам необходимо:

– установление провайдера услуг и направление в его адрес запроса на установление лица или лиц, которым они предоставлялись;

– проведение обыска по месту предоставления IP-адресов;

– осуществление допроса лиц, которым предоставлялись IP-адреса.

2.2.2. Счет, на который были переведены денежные средства потерпевшего.

В соответствии со ст. 26 Закона о банках и банковской деятельности с согласия руководителя следственного органа необходимо направить запрос о предоставлении следующей информации:

– о персональных данных владельца счета (ФИО, привязанные абонентские номера и адреса электронной почты);

– движении денежных средств по счету за период с момента открытия по настоящее время с расшифровкой получателя и назначением платежа;

– IP-адресах, при использовании которых осуществлялось подключение интернет-платформы по управлению счетом;

– IP-адресах и иных счетах, подключение к которым происходило при использовании одного интернет-браузера и которые получены посредством анализа cookie-файлов.

По выявленным данным владельца счета необходимо дальнейшее производство следственных действий в отношении этого лица, в зависимости от следственной ситуации (допрос, обыск в жилище, обыск по месту работы и др.).

По сведениям о движении денежных средств необходимо проведение анализа, при их дальнейшем переводе – направление соответствующих аналогичных запросов, а в случае фактов обналичивания – установление банкоматов и принятие мер к изъятию видеозаписей с камер наблюдения (не только банкоматов, но и помещений, где они расположены, а также прилегающей территории).

С помощью IP-адресов также важно определить провайдера и направить запрос на установление лица, которому предоставлялся данный IP-адрес; провести обыск по месту предоставления IP-адресов и последующий допрос лиц.

2.2.3. Третьим направлением расследования в случае звонка потерпевшему по объявлению на интернет-сервисе по размещению рекламной информации является данная организация.

Необходимо направление запроса в организацию, владеющую указанным интернет-сайтом, о предоставлении сведений в отношении пользователей, просматривающих объявление потерпевшего за интересующий следствие период:

– об IP-адресах, с которых осуществлялся просмотр указанной страницы;

– в случае если обращение к объявлению осуществлялось авторизованным пользователем – сведения о его аккаунте: дата регистрации, регистрационные данные (ФИО, абонентский номер, адрес электронной почты и др.);

– об иных IP-адресах и аккаунтах пользователя, подключение к которым происходило при использовании одного интернет-браузера и которые получены посредством анализа cookie-файлов.

По найденным IP-адресам необходимо определить провайдера и направить запрос на установление лица, которому предоставлялся данный IP-адрес, произвести следственные действия в зависимости от следственной ситуации (допрос, обыск в жилище, обыск по месту работы и др.).

3. Преступник под различными предлогами путем введения потерпевшего в заблуждение уговорил его перевести со своего счета денежные средства.

Примеры преступлений данной группы: перевод денежных средств в качестве предоплаты за товар по объявлению на интернет-сервисе по размещению объявлений; перевод денежных средств в качестве оплаты товара при покупке через интернет-магазин; перевод денежных средств под предлогом передачи их в долг знакомому, аккаунт в социальной сети которого взломали, и др.

3.1. Сведения, которые необходимо выяснить у потерпевшего, а также способы документального подтверждения события преступления отражены в п. 1.1 и 1.2 настоящего раздела. Указанные преступления квалифицируются по соответствующей части ст. 159 УК РФ (подробнее см. раздел 1).

3.2. Далее ход расследования осуществляется по трем следовым направлениям:

3.2.1. Абонентский номер, при использовании которого связывались с потерпевшим (см. п. 2.2.1).

3.2.2. Счет, на который были переведены денежные средства потерпевшего (см. п. 2.2.2).

3.2.3. Интернет-страница, с которой осуществлялось введение в заблуждение потерпевшего. В данном случае распространенными являются три варианта: сайт интернет-магазина; страница пользователя или группы в социальной сети; страница на интернет-сервисе по размещению объявлений.

3.2.3.1. Сайт интернет-магазина. Посредством интернет-сервисов необходимо установить регистратора доменного имени сайта и организацию, предоставляющую услуги хостинга. В данные организации направляются запросы о предоставлении следующих сведений:

– данные лица, на которое зарегистрировано доменное имя и которому предоставляются услуги хостинга (ФИО, наименование организации, абонентские номера, адреса электронной почты и др.);

– об оплате услуг регистратора/хостинга (даты и способ оплаты с указанием реквизитов);

– IP-адресах пользователя при регистрации доменного имени/при получении услуг хостинга.

По полученным персональным данным, в зависимости от следственной ситуации, необходимо производство следственных действий в отношении лица (допрос, обыск в жилище, обыск по месту работы и др.).

По сведениям об оплате услуг необходимо направление запроса в отношении счета, с которого были переведены деньги (см. п. 2.2.2).

По полученным IP-адресам необходимо установление провайдера и направление запроса на установление лица, которому предоставлялся данный IP-адрес; производство последующих действий, в зависимости от следственной ситуации (допрос, обыск в жилище, обыск по месту работы и др.).

3.2.3.2. Страница пользователя или группы в социальной сети/страница на интернет-сервисе по размещению объявлений.

Необходимо направление запроса в соответствующую организацию о предоставлении следующих сведений:

– даты регистрации аккаунта; регистрационных данных (ФИО, абонентские номера, адреса электронной почты и др.);

– об IP-адресах, с которых осуществлялось подключение к аккаунту с момента регистрации по настоящее время;

– об иных IP-адресах и аккаунтах пользователя, подключение к которым происходило при использовании одного интернет-браузера и которые получены посредством анализа cookie-файлов.

По выясненным персональным данным, в зависимости от следственной ситуации, необходимо производство следственных действий в отношении лица (допрос, обыск в жилище, обыск по месту работы и др.).

По полученным абонентским номерам и адресам электронной почты необходимо установить лиц, которые их использовали (см. п. 2.2.1).

По IP-адресам необходимо определение провайдера и направление запроса на установление лица, которому предоставлялся данный IP-адрес; производство последующих действий – в зависимости от следственной ситуации (допрос, обыск в жилище, обыск по месту работы и др.).

4. Хищение совершается при использовании вредоносных компьютерных программ или неправомерного доступа к компьютерной информации.

4.1. При допросе потерпевшего выясняются обстоятельства, отраженные в п. 1.1, а также следующие сведения:

– адреса банкоматов, которые использовались для снятия наличных средств и осуществления транзакций (с целью выявления возможного скиммингового устройства);

– технические устройства, с помощью которых осуществлялся доступ в личный кабинет при пользовании услугой «интернет-банкинг», например, ВТБ-онлайн, Сбербанк-онлайн и др. (указать тип, марку, IMEI-номер, mac-адрес);

– сохранена ли информация о реквизитах банковских карт и кошельков (номер карты, пароль, CVV2/CVC2, сведения о держателе карты, срок ее действия) в интернет-браузере технического устройства;

– сохранены ли данные о логинах и паролях для доступа в личный кабинет сервиса «интернет-банкинг» в интернет-браузере технического устройства;

– с какой организацией-интернет-провайдером заключен договор об оказании услуги доступа в сеть «Интернет» (договор об оказании услуг связи);

– периодичность выхода потерпевшего в интернет; какие ресурсы при этом наиболее часто посещает, в том числе подозрительные;

– каким интернет-браузером пользуется потерпевший во время выхода в интернет; его настройки (сохраняется ли история посещений, cache-память, cookie-файлы и т. п.);

– кто имеет беспрепятственный доступ к работе с компьютером;

– имели ли место некорректная работа, сбои, неполадки в процессе работы компьютера, его программном обеспечении, электронных сетей; если такие факты выявлены, то выяснить, когда именно они случались и в чем это выражалось;

– установлено ли на компьютере (смартфоне) антивирусное программное обеспечение; если да, то важно выяснить, является ли оно лицензионным; с какой периодичностью проводятся мониторинг на наличие либо отсутствие вредоносных файлов, программ, каковы результаты мониторинга за последнее время;

– как часто производится обновление операционной системы и каким именно образом;

– каким образом производятся обслуживание и ремонт компьютерной техники (кем, где, как часто);

– каким образом устроено сетевое подключение компьютеров в организации; кто отвечает за работу сервера;

– переходил ли заявитель по подозрительным ссылкам в сети «Интернет». Например, «Я по объявлению на Авито. Не интересует обмен с моей доплатой? Ссылка: www.avit0.ru/VnshTTYkm»; «Смотри, нашел тебя на этой фотке. Ссылка: www.bit.ly/ZreizE1eaAa».

Данная группа преступлений, как правило, квалифицируется по соответствующей части ст. 159^6 УК РФ (подробнее см. раздел 1).

4.2. К специфике расследования уголовных дел данной категории следует отнести необходимость назначения судебных компьютерных экспертиз.

В рамках судебной компьютерной экспертизы решаются следующие задачи:

– поиск информации на машинных носителях, установленных в СВТ, созданной с помощью прикладных программ;

– поиск информации на машинных носителях, установленных в СВТ, о действиях пользователя (процессах обработки файлов, ведении баз данных, работе в сетях передачи данных и т. п.);

– определение свойств программ и программных продуктов;

– выявление возможностей совершения каких-либо действий с помощью СВТ;

– определение принадлежности программ и данных к конкретным классам;

– установление материальных объектов по компьютерной информации (проводится в комплексе с другими видами экспертиз);

– установление фактических обстоятельств совершения преступления (проводится при наличии информации, полученной из различных источников).

Объектами судебной компьютерной экспертизы могут выступать: информация, содержащаяся на электронных носителях, имеющихся в составе персональных компьютеров (настольные, портативные); периферийные устройства; сетевые аппаратные средства (серверы, рабочие станции, активное оборудование и т. д.); интегрированные системы (органайзеры, мобильные телефоны и т. п.); микросхемы памяти, сим-карты, магнитные и оптические диски, магнитные ленты, платежные карты, карты памяти и т. д. и/или средства, обладающие возможностью хранения электронной информации, представленной в виде файловых структур.

Примерные вопросы, задаваемые при назначении судебной компьютерной экспертизы в ходе расследования хищений электронных денежных средств, в том числе совершенных посредством информационно-телекоммуникационных сетей:

1. Имеются ли на предоставленном для исследования носителе информации сведения о посещении ресурса (указывается конкретный адрес)?

2. Хранятся ли на предоставленном на исследование носителе информации файлы, содержащие историю посещения интернет-ресурсов?

3. Содержатся ли на предоставленном на исследование носителе информации сведения о логинах и паролях доступа к интернет-ресурсам?

4. Имеются ли на предоставленном на исследование носителе информации сведения о логинах и паролях доступа к установленной программе (указывается конкретная программа)?

5. Какие сетевые настройки и параметры, в том числе MAC-адрес, имеет представленное оборудование?

6. Имеются ли на предоставленном на исследование носителе информации файлы, содержащие «____», «____», «____» (указываются ключевые слова)? Если да, то каковы временные атрибуты обнаруженных файлов?

7. Содержатся ли на предоставленном на исследование носителе информации файлы, детектируемые антивирусным программным обеспечением? Если да, то какими функциональными возможностями обладают?

8. Установлены ли на предоставленном на исследование носителе информации компьютерные программы или другая компьютерная информация, которые обладают функциональными возможностями скрытно от пользователя копировать сведения, необходимые для аутентификации в операционной системе, но при этом не являются компонентом этой системы?

9. Имеются ли на предоставленном на исследование носителе информации средства удаленного администрирования и управления компьютером?

10. Хранятся ли на предоставленном на исследование носителе информации файлы, содержащие электронные почтовые сообщения? О каких электронных почтовых ящиках имеются сведения на предоставленном на исследование носителе информации?

11. Имеются ли на предоставленном на исследование носителе информации файлы, содержащие историю сообщений, обмена сообщениями в сети «Интернет»?

Кроме того, независимо от выделенных групп рассматриваемой категории преступлений особой спецификой характеризуется производство обыска. При обыске одними из основных искомых объектов являются компьютерная техника, всевозможные носители электронной информации, денежные средства, финансовые документы, средства защиты информации, образцы почерка и подписи, различного рода литература, с помощью которой была осуществлена подготовка к преступлению, и другие предметы и документы, которые могут иметь значение для уголовного дела.

При подготовке к производству обыска следователю необходимо:

1. Направить органу дознания поручение с целью установления:

– количества компьютерной техники, которая находится в помещении, где предполагается производство обыска;

– специфики пропускного режима в организации (при его наличии);

– особенностей коммуникации для обмена информацией между компьютерами (наличие Wi-Fi-сети, локальной сети между компьютерами, местонахождение сервера);

– особенностей электропитания компьютерной техники и расположения мест обесточивания помещения;

– сведений о лицах, которые могут находиться в помещении, где предполагается производство обыска (правовой статус, образование, возраст, наличие профессиональных навыков).

2. Уточнить конкретные места и помещения, в которых будет производиться обыск, время его проведения; принять меры, связанные с безопасностью и конфиденциальностью, при производстве данного следственного действия, чтобы исключить возможность утечки информации.

3. В случае производства обыска в жилом помещении либо в местах, где могут находиться лица с особым правовым статусом, принять меры к получению судебного решения для его производства.

4. В случаях проведения обысков в нескольких помещениях одновременно провести инструктаж участников следственной группы о порядке его производства и перечне объектов, подлежащих поиску и изъятию. Кроме того, важно организовать связь между следственными группами, находящимися на разных адресах.

5. Привлечь специалистов для производства данного следственного действия, так как значительная часть объектов, подлежащих поиску, – это носители компьютерной информации. Чаще всего таковыми выступают эксперты экспертно-криминалистических подразделений МВД России, которые специализируются на производстве компьютерных судебных экспертиз, и сотрудники подразделений информационных технологий, связи и защиты информации.

Непосредственно при проведении обыска, помимо общих требований, предъявляемых законом к его производству, следователю необходимо обратить внимание на следующие особенности:

1. Запретить лицам, находящимся в помещении, осуществлять какие-либо манипуляции с компьютерной техникой и источниками ее питания, даже под предлогом их добровольной выдачи.

2. Установить наличие сети между компьютерами, выяснить принцип ее функционирования, местонахождение серверного оборудования.

3. Изъять любые электронные носители, в первую очередь системные блоки, ноутбуки, моноблоки, видеокарты, накопители на жестких магнитных дисках, карты памяти различных форматов, твердотелые накопители и др.

4. Изъятые технические устройства целесообразно упаковывать для недопущения дальнейшей работы с ними.

Напомним, что в соответствии с требованиями ст. 164^1 УПК РФ электронные носители информации подлежат изъятию с участием специалиста.

Специалистом по ходатайству лица, которому принадлежат электронные носители, может быть произведено копирование информации с изъятых носителей. Если, по его мнению, такое копирование может повлечь повреждение или уничтожение информации, то его можно не производить. В протоколе следственного действия делается отметка о копировании информации и передаче электронных носителей, на которых она содержится, законному владельцу изымаемых электронных носителей информации или обладателю содержащейся на них информации.

На заключительном этапе рассмотрения особенностей проведения обыска при расследовании уголовных дел данной категории необходимо определить понятие электронного носителя информации.

Согласно ГОСТ 2.051-2013 «Единая система конструкторской документации. Электронные документы. Общие положения» электронным носителем информации является материальный носитель, используемый для записи, хранения и воспроизведения информации, обрабатываемой с помощью средств вычислительной техники. К нему следует относить:

– оптические компакт-диски различных видов и форматов (CD-R, CD-RW, DVD-R, DVD-RW, BLU-RAY и т. д.);

– накопители на жестких магнитных дисках;

– карты памяти различных форматов (Compact Flash, Secure Digital, Multimedia Card, Memory Stick и др.);

– USB-флэш-накопители и др.

Таким образом, исходя из действующего уголовно-процессуального законодательства, можно сделать вывод о том, что к электронным носителям информации относится весь спектр технических устройств, указанных выше. На основании изложенного факта их изъятие в любой форме необходимо производить с участием специалиста.

В связи с данным обстоятельством возникает вопрос о том, как следует производить изъятие таких технических устройств, которые находятся в каждодневном обиходе, но по сути своей тоже являются электронными носителями информации. Например, MP3-плееры в первую очередь служат для чтения аудиофайлов; сотовые телефоны – для звонков и передачи сообщений; цифровые фотоаппараты – для производства фотографий и видеозаписи; видеорегистраторы – для фиксации в видеоформате обстановки на дороге. Тем не менее в каждом из перечисленных устройств присутствует один из видов памяти для сохранения той или иной информации.

Уголовно-процессуальный закон не регламентирует конкретного перечня электронных носителей информации, подлежащих изъятию с участием специалиста, поэтому оно также должно проводиться с участием последнего.

Определенной спецификой при расследовании уголовных дел о преступлениях рассматриваемого вида обладает осмотр компьютерной техники. Указанное следственное действие также требует от следователя специальных знаний в области компьютерной информации.

Так, например, довольно часто возникают случаи, когда изъятая в ходе следствия компьютерная техника для включения требует введения пароля. Данное обстоятельство существенно затрудняет производство указанного следственного действия. Самым быстрым и эффективным решением данной проблемы может являться привлечение к осмотру владельца этой техники для добровольной передачи сведений о пароле или

же самостоятельного его введения участвующим лицом на условиях, исключающих ознакомление с ним следователя. В дальнейшем участие владельца компьютерной техники в осмотре также целесообразно, поскольку он может указать на точное наименование, а также место хранения интересующих следствие файлов и дать по каждому из них пояснения, тем самым существенно сэкономить временные затраты следователя.

Довольно часто возникают случаи, когда владелец компьютерной техники отказывается предоставлять сведения о пароле следователю. В этом случае следователь назначает компьютерную судебную экспертизу, ставя на разрешение перед экспертом интересующие его вопросы. Стоит отметить, что, как показывает практика, экспертиза компьютерной техники, для включения которой необходимо введение пароля или предоставления иных способов идентификации личности (наличие сканера отпечатка пальца, датчика разблокировки по лицу и др.), не всегда приносит желаемый результат. Это обусловлено несколькими факторами, в частности, сложностью пароля, современностью технического устройства и установленных на нем средств идентификации личности и видами защиты от несанкционированного доступа к устройству (например, полная блокировка устройства после нескольких неудачных попыток введения пароля или автоматическое полное удаление всей информации после активации устройства), а также типа операционной системы и ее версии (Windows, Linux, Android, MacOs, iOS и др.). Особую сложность для производства экспертизы в описанных случаях представляют устройства компании «Apple» с установленными на них операционными системами «закрытого типа», таких как «iOS», «MacOS» и др.

В качестве основных рекомендаций при осмотре компьютерной техники следует выделить следующие:

1. Вне зависимости от уровня знаний в области компьютерной информации, а также участия владельца осматриваемого технического устройства в следственном действии всегда привлекать к участию в осмотре специалиста, желательно, из числа имеющих опыт в проведении компьютерных судебных экспертиз.

2. Во взаимодействии со специалистом тщательно подготовиться к осмотру, в частности, выяснить информацию о типе осматриваемого устройства, его функциональных особенностях, об установленной на нем операционной системе и специфике ее работы, особенно в тех случаях, если до момента осмотра с ней не приходилось сталкиваться.

3. Выяснить информацию об установленных на конкретном устройстве типах защиты от несанкционированного доступа и о возможных способах их деактивации.

4. В ходе осмотра не производить действий, о которых имеется слабое представление (например, не запускать программное обеспечение,

назначение которого не известно, или не допускать соединений с сетью «Интернет» без удостоверения в безопасности данной манипуляции), в противном случае, такие действия могут привести к полному удалению информации, а в итоге и к потере значимого доказательства в виде протокола осмотра предметов.

5. Непосредственно при осмотре интересующих файлов указывать путь к месту их хранения, даты создания, изменения, а также указывать сведения о лице, их создавшем и сохранившем.

6. Производить пошаговое фотографирование осматриваемого объекта и (или) производить скриншоты (снимки экрана) файлов, представляющих интерес, которые впоследствии необходимо копировать и вставлять в текст протокола осмотра с соответствующими пояснениями.

7. При копировании информации с осматриваемого устройства подключать только проверенные на безопасность физические носители (магнитные диски на жестких носителя, USB-флэш-накопители и др.), иначе в файловой системе осматриваемого объекта окажется вредоносное программное обеспечение, что может повлечь искажение либо удаление информации.

8. Рекомендуется отработка запланированных в осмотре действий на аналогичном устройстве. Это позволит следователю и специалисту лучше ознакомиться с предназначенным к осмотру устройством, а также снизит риски от непредвиденных ситуаций различного рода.

Необходимо также обратить внимание на то, что при осмотре компьютерной техники и, в частности содержащихся в ней файлах, нередко можно столкнуться с необходимостью осмотра содержимого переписки, сообщений в социальных сетях, электронных почтовых ресурсах и т. д.

Право тайны переписки гарантировано в ст. 23 Конституции Российской Федерации. Уголовно-процессуальный принцип тайны переписки, телефонных и иных переговоров, почтовых, телеграфных и иных сообщений закреплен в ст. 13 УПК РФ, а ч. 1 указанной статьи говорит о том, что ограничение права гражданина на тайну переписки, телефонных и иных переговоров, почтовых, телеграфных и иных сообщений допускается только на основании судебного решения. Таким образом, можно предположить, что в случаях необходимости осмотра содержимого переписки, содержащейся в памяти технических устройств (персональных компьютеров, мобильных телефонов, ноутбуков и т. д.), следователь должен обратиться с ходатайством в суд о разрешении осмотра корреспонденции, однако заметим, что ст. 29 УПК РФ не содержит соответствующего правомочия суда на принятие решения о разрешении осмотра корреспонденции.

Интервьюирование следователей органов внутренних дел с опытом работы от 2 до 12 лет за период с 21 по 29 марта 2022 года показало, что

большая часть, а именно 18 из 21 респондентов из территориальных подразделений органов предварительного следствия (СУ УМВД России по Кировской и Ульяновской областям, ГСУ ГУ МВД России по Нижегородской и Самарской областям) осматривают содержимое переписки без получения разрешения суда, ссылаясь на отсутствие соответствующего правомочия у последнего. Лишь несколько следователей сообщили о том, что имели опыт ходатайства перед судом о разрешении осмотра корреспонденции, однако получали отказ по описанным выше основаниям. Ярким примером такой позиции суда является апелляционное постановление Московского городского суда от 2 февраля 2015 г. № 22-455/15 22К-455/2015 по делу № 22К-455/2015.

Таким образом, исходя из сложившейся ситуации на практике, при возникновении необходимости осмотра содержимого переписки в ходе осмотра технических устройств следователь с целью обеспечения конституционных прав гражданина и соблюдения уголовно-процессуальных принципов может выйти с ходатайством перед судом о разрешении осмотра корреспонденции, однако он должен иметь в виду, что вероятность его удовлетворения не велика.

В приложениях 1, 2, 3 приведены образцы процессуальных документов, позволяющих инициировать получение наиболее важных сведений при расследовании указанной категории преступлений.

Вопросы для самоконтроля

1. Дайте определение понятиям: web-site, web-browser, NAT, IP-адрес, cookie-файлы, VPN.
2. Дайте характеристику четырем условным группам хищений электронных денежных средств, в том числе совершенных посредством использования информационно-телекоммуникационных сетей.
3. В чем состоят особенности производства допроса при расследовании хищений электронных денежных средств, в том числе совершенных посредством использования информационно-телекоммуникационных сетей?
4. В чем состоят особенности производства обыска при расследовании хищений электронных денежных средств, в том числе совершенных посредством использования информационно-телекоммуникационных сетей?
5. Назовите вопросы, задаваемые при назначении судебной компьютерной экспертизы, при расследовании хищений электронных денежных средств, в том числе совершенных посредством использования информационно-телекоммуникационных сетей.

Практическое задание

Ситуация: 22 сентября 2021 года Михайлов С. В., проживающий в г. Москве, с целью приобретения мобильного телефона, бывшего в употреблении, зарегистрировался на интернет-сервисе объявлений Авито. В этот же день он, выбрав по привлекательной цене мобильный телефон Samsung Galaxy S20 стоимостью 30 000 рублей, связался посредством сервиса сообщений внутри ресурса Avito.ru с продавцом телефона под ником «DanilaD». Михайлов С. В. попросил продавца «DanilaD» встретиться для осмотра товара перед покупкой, на что последний ответил отказом, сославшись на тяжелую семейную ситуацию, при этом уточнив, что может прислать фотографии телефона с различных ракурсов. Михайлов С. В. согласился. Изучив фотографии, Михайлов принял решение о покупке, о чем сообщил продавцу. В свою очередь, «DanilaD» попросил у Михайлова С. В. совершить сделку дистанционно, при этом произвести предоплату на карту ПАО «Сбербанк» 1111 2222 3333 4444, после чего он гарантировал отправку телефона в тот же день. Михайлов С. В. согласился и в 15:00 того же дня перевел денежные средства в размере 15 000 рублей на указанный номер карты. После этого «DanilaD» перестал отвечать на сайте Авито и около 18:00 того же дня его аккаунт был удален. Подождав 2 дня, Михайлов С. В., осознав, что был обманут, написал заявление в полицию.

По данному факту 26 сентября 2021 года возбуждено уголовное дело № 123456789001112 по признакам преступления, предусмотренного ч. 2 ст. 159 УК РФ.

1. Составить план допроса Михайлова С. В., отразив наиболее значимые вопросы, подлежащие выяснению.
2. Определить перечень наиболее значимой информации, подлежащей истребованию, и составить проект запроса в Авито.
3. Определить перечень наиболее значимой информации, подлежащей истребованию, и составить проект запроса в ПАО «Сбербанк».
4. Получив сведения об IP-адресах в результате ответа на запросы из Авито и ПАО «Сбербанк», составить проект запроса интернет-провайдеру, предоставлявшему IP-адреса при подключении к сети «Интернет» для работы с указанными ресурсами (наименование IP-адреса и интернет-провайдера обучающиеся определяют самостоятельно).

ЗАКЛЮЧЕНИЕ

Результаты рассмотрения данной темы позволяют сделать вывод о том, что в настоящее время действительно отсутствует единообразная практика применения положений, закрепленных в п. «г» ч. 3 ст. 158 УК РФ, а также имеются сложности в разграничении этой нормы от смежных составов преступлений, предусмотренных ст. 159, 272 и 273 УК РФ.

В представленном учебном пособии авторский коллектив провел подробный анализ имеющегося опыта расследования уголовных дел о хищениях электронных денежных средств, а также совершаемых посредством использования информационно-телекоммуникационных сетей. Были выявлены проблемные вопросы квалификации и приведены отдельные меры по совершенствованию правоприменительной практики в области производства предварительного следствия по рассматриваемому виду преступлений.

Подготовленные материалы могут быть использованы следователями и руководителями следственных подразделений территориальных органов внутренних дел Российской Федерации, а также обучающимися образовательных организаций системы МВД России.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

Нормативные правовые акты

1. Конституция Российской Федерации : принята всенародным голосованием 12 декабря 1993 года (с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 года) // Официальный интернет-портал правовой информации. – 2020. – URL: http://publication.pravo.gov.ru/Document/View/0001202007040001?index=0&rangeSize=1 (дата обращения: 28.12.2021). – Текст : электронный.

2. О банках и банковской деятельности : Федеральный закон Российской Федерации от 2 декабря 1990 года № 395-1 (с изменениями и дополнениями) // СПС «КонсультантПлюс» : [сайт]. – URL: http://www.consultant.ru/document/cons_doc_LAW_5842/ (дата обращения: 28.12.2021). – Текст : электронный.

3. О связи : Федеральный закон Российской Федерации [от 7 июля 2003 года № 126-ФЗ] : принят Государственной Думой Федерального Собрания Российской Федерации 18 июня 2003 года : одобрен Советом Федерации Федерального Собрания Российской Федерации 25 июня 2003 года (с изменениями и дополнениями) // Собрание законодательства Российской Федерации. – 2003. – № 28. – Ст. 2895. – Текст : непосредственный.

4. О национальной платежной системе : Федеральный закон Российской Федерации от 27 июня 2011 года № 161-ФЗ : принят Государственной Думой Федерального Собрания Российской Федерации 14 июня 2011 года : одобрен Советом Федерации Федерального Собрания Российской Федерации 22 июня 2011 года (с изменениями и дополнениями) // СПС «КонсультантПлюс» : [сайт]. – URL: http://www.consultant.ru/document/cons_doc_LAW_115625/ (дата обращения: 23.12.2021). – Текст : электронный.

5. Гражданский кодекс Российской Федерации. Часть первая : Федеральный закон Российской Федерации от 30 ноября 1994 года № 51-ФЗ : принят Государственной Думой Федерального Собрания Российской Федерации 21 октября 1994 года (с изменениями и дополнениями) // СПС «КонсультантПлюс» : [сайт]. – URL: http://www.consultant.ru/document/cons_doc_LAW_5142/ (дата обращения: 28.12.2021). – Текст : электронный.

6. Уголовно-процессуальный кодекс Российской Федерации : Федеральный закон Российской Федерации [от 18 декабря 2001 года] № 174-ФЗ : принят Государственной Думой Федерального Собрания Российской Федерации 22 ноября 2001 года : одобрен Советом Федерации Федерального Собрания Российской Федерации 5 декабря 2001 года (с изменениями и дополнениями) // Российская газета. – 2001. – 22 декабря. – Текст : непосредственный.

7. Уголовный кодекс Российской Федерации : Федеральный закон Российской Федерации [от 13 июня 1996 года] № 63-ФЗ : принят Государственной Думой Федерального Собрания Российской Федерации 24 мая 1996 года : одобрен Советом Федерации Федерального Собрания Российской Федерации 5 июня 1996 года (с изменениями и дополнениями) // Собрание законодательства Российской Федерации. – 1996. – № 25. – Ст. 2954. – Текст : непосредственный.

8. О Стратегии экономической безопасности Российской Федерации на период до 2030 года : Указ Президента Российской Федерации от 13 мая 2017 года № 208 // СПС «Гарант» : [сайт]. – URL: http://www.garant.ru/products/ipo/prime/doc/71572608/ (дата обращения: 21.12.2021). – Текст : электронный.

Основная литература

9. Глоссарий по информационному обществу / под общ. ред. Ю. Е. Хохлова. – Москва : Институт развития информационного общества, 2009. – 162 с. – ISBN 978-5-901907-20-7. – Текст : непосредственный.

10. **Кузьмин, И. А.** Раскрытие мошенничеств, совершенных с использованием информационно-коммуникационных технологий : учебное пособие / И. А. Кузьмин ; Восточно-Сибирский институт МВД России. – Иркутск : ВСИ МВД России, 2021. – 80 с. – Текст : непосредственный.

11. Особенности расследования преступлений, связанных с хищением денежных средств в сфере компьютерной информации (ст. 159.6 Уголовного кодекса Российской Федерации) : учебное пособие / Т. Ф. Скогорева [и др.] ; Волгоградская академия МВД России. – Волгоград : ВА МВД России, 2019. – 52 с. – Текст : непосредственный.

12. Расследование мошенничества в сфере компьютерной информации : учебное пособие / Восточно-Сибирский институт МВД России; авт.-сост.: П. А. Капустюк [и др.]. – Иркутск : ВСИ МВД России, 2018. – 48 с. – Текст : непосредственный.

13. Расследование хищений денежных средств с банковских счетов граждан, совершенных с использованием систем дистанционного банковского обслуживания : учебно-практическое пособие / В. Н. Чаплыгина [и др.] ; Орловский юридический институт МВД России имени В. В. Лукьянова. – Орел : ОрЮИ МВД России им. В. В. Лукьянова, 2019. – 36 с. – Текст : непосредственный.

14. **Решняк, О. А.** Расследование хищений чужого имущества, совершенных с использованием информационно-телекоммуникационных технологий : учебное пособие / О. А. Решняк, С. А. Ковалев ; Волгоградская академия. – Волгоград : ВА МВД России, 2021. – 58 с. – Текст : непосредственный.

15. **Русскевич, Е. А.** Мошенничество в сфере компьютерной информации : монография / Е. А. Русскевич, М. Д. Фролов. – Москва : ИНФРА-М, 2020. – ISBN 978-5-16-016464-9. – 148 с. – Текст : непосредственный.

16. Уголовное право России. Общая часть: курс лекций / под ред. А. П. Кузнецова, Е. Е. Черных. – Нижний Новгород, 2019. – 714 с. – ISBN 978-5-88840-168-2. – Текст : непосредственный.

17. **Ушаков, А. Ю.** Расследование преступлений, совершенных с использованием информационно-коммуникационных технологий : учебно-практическое пособие / А. Ю. Ушаков, А. М. Столповский. – Нижний Новгород : Нижегородская академия МВД России, 2019. – 59 с. – Текст : непосредственный.

Дополнительная литература

18. **Аксенов, В. С.** К вопросу об интерпретации электронных денег / В. С. Аксенов. – Текст : непосредственный // Вестник РГГУ. – 2011. – № 10. – С. 14–22.

19. **Багмет, А. М.** Цифровые следы преступлений : монография / А. М. Багмет, В. В. Бычков, С. Ю. Скобелин, Н. Н. Ильин. – Москва : Проспект, 2021. – 168 с. – ISBN 978-5-392-32868-0. – Текст : непосредственный.

20. **Баяхчев, В. Г.** Расследование хищений, совершаемых в кредитно-финансовой сфере с использованием электронных средств / В. Г. Баяхчев, В. В. Улейчик. – Текст : непосредственный // Законодательство. – 2000. – № 6. – С. 53–59.

21. **Боровых, Л. В.** Проблема квалификации хищения с использованием банковских карт / Л. В. Боровых, Е. А. Корепанова. – Текст : непосредственный // Российский юридический журнал. – 2014. – № 2. – С. 82–87.

22. **Воронцова, С. В.** Защита прав потерпевших по уголовным делам, возбужденным по фактам мошенничества с банковскими картами / С. В. Воронцова. – Текст : непосредственный // Российский судья. – 2010. – № 11. – С. 22–24.

23. **Гарбатович, Д. А.** Проблемные аспекты эффективности норм, предусматривающих уголовную ответственность за совершение преступлений в сфере компьютерной информации / Д. А. Гарбатович. – Текст : непосредственный // Библиотека криминалиста. – 2013. – № 5. – С. 6–14.

24. **Грачев, С. А.** Расследование преступлений в сфере экономической деятельности : учебное пособие / С. А. Грачев, М. В. Лелетова, А. Ю. Ушаков. – Москва : ДГСК МВД России, 2020. – 176 с. – Текст : непосредственный.

25. **Кибальник, А. Г.** Квалификация мошенничества в новом постановлении Пленума Верховного Суда Российской Федерации / А. Г. Кибальник. – Текст : непосредственный // Уголовное право. – 2018. – № 1. – С. 61–67.

26. Криминалистика : учебник / Т. В. Аверьянова, Р. С. Белкин, Ю. Г. Корухов, Е. Р. Россинская. – Москва : Норма ; ИНФРА-М, 2017. – 928 с. – ISBN 978-5-91768-334-8. – Текст : непосредственный.

27. Криминалистика : учебник для вузов / И. В. Александров [и др.]. – Москва : Издательство «Юрайт», 2020. – 376 с. – ISBN 978-5-534-06661-6. – Текст : непосредственный.

28. **Лопашенко, Н. А.** Законодательная реформа мошенничества: вынужденные вопросы и вынужденные ответы / Н. А. Лопашенко. – Текст : непосредственный // Криминологический журнал Байкальского государственного университета экономики и права. – 2015. – Т. 9. – № 3. – С. 507.

29. **Мещеряков, В. А.** Следы преступлений в сфере высоких технологий / В. А. Мещеряков. – Текст : непосредственный // Библиотека криминалиста. – 2013. – № 5. – С. 265–270.

30. **Минин, А. Я.** О специфике противодействия киберпреступности / А. Я. Минин. – Текст : непосредственный // Российский следователь. – 2013. – № 8. – С. 37–39.

31. **Петраков, С. В.** Раскрытие и расследование преступлений, совершаемых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации : учебное пособие / С. В. Петраков, А. Ю. Ушаков, А. А. Попов, К. Н. Дудаль. – Санкт-Петербург : Санкт-Петербургская академия Следственного комитета, 2021. – 84 с. – Текст : непосредственный.

32. **Ушаков, А. Ю.** Особенности квалификации и расследования преступлений, связанных с хищениями имущества кредитных организаций : учебное пособие / А. Ю. Ушаков, О. И. Долгачева, А. Г. Саакян. – Казань : «Бук», 2019. – 62 с. – ISBN 978-5-00118-446-1. – Текст : непосредственный.

33. **Яни, П. С.** Квалификация хищений: момент окончания, безвозмездность, ущерб. – Текст : непосредственный / П. С. Яни. – Текст : непосредственный // Законность. – 2015. – № 12. – С. 43–47.

Эмпирические материалы

34. Апелляционное определение Судебной коллегии по уголовным делам Самарского областного суда от 16 октября 2019 года № 22-6241 // ГАС «Правосудие» : [сайт]. – URL: https://bsr.sudrf.ru (дата обращения: 21.12.2021). – Текст : электронный.

35. О направлении информации по хищениям денежных средств с банковских счетов граждан в адрес Следственного департамента МВД России : Информационное письмо Главного управления МВД России по Красноярскому краю № 4/5832 от 30 апреля 2020 года. Документ опубликован не был.

36. О направлении информации по хищениям денежных средств с банковских счетов граждан в адрес Следственного департамента МВД России : Информационное письмо УМВД России по Приморскому краю № 27/24 от 10 января 2020 года. Документ опубликован не был.

37. О судебной практике по делам о краже, грабеже и разбое : Постановление Пленума Верховного Суда Российской Федерации от 27 декабря 2002 года № 29 // Бюллетень Верховного Суда Российской Федерации. – 2003. – № 2. – Текст : непосредственный.

38. О судебной практике по делам о мошенничестве, присвоении и растрате : Постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 года № 48 // Бюллетень Верховного Суда Российской Федерации. – 2018. – № 2. – Текст : непосредственный.

39. О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем : Постановление Пленума Верховного Суда Российской Федерации от 7 июля 2015 года № 32 (в ред. от 26.02.2019) // Бюллетень Верховного Суда Российской Федерации. – 2015. – № 9. – Текст : непосредственный.

40. Определение Верховного Суда Российской Федерации от 29 сентября 2020 года № 12-УДП20-5-К6 (в порядке главы 47^1 УПК РФ) // СПС «КонсультантПлюс» : [сайт]. – URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=ARB&n=640673#03998532076256049 (дата обращения: 28.12.2021). – Текст : электронный.

41. Определение Восьмого кассационного суда общей юрисдикции от 5 марта 2020 года по делу № 77-38/2020 // СПС «КонсультантПлюс» : [сайт]. – URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&ts=tfaFOuSwL1yxZFN9&cacheid=7B65ED93EF31D4E1A9EE4327A1E694A4&mode=splus&base=KSOJ008&n=3993&rnd=FD602990ED6958E4546AC60FE895F7DB#4LcFOuSmWwN5I3d71 (дата обращения: 28.12.2021). – Текст : электронный.

42. Постановления президиума Мурманского областного суда от 3 июня 2019 года № 44у-15/2019; от 7 октября 2019 года № 44у-31/2019; от 11 ноября 2019 года № 44у-36/2019 // СПС «КонсультантПлюс» (дата обращения: 28.12.2021). – Текст : электронный.

43. Постановление Хабаровского краевого суда от 21 октября 2019 года № 44у-139/2019 // СПС «КонсультантПлюс» : [сайт]. – URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&ts=tfaFOuSwL1yxZFN9

&cacheid=72CA19C4126CA5C628E8FB8F5C442179&mode=splus&base=SODV&n=131559&rnd=FD602990ED6958E4546AC60FE895F7DB#ngzGOuS8cbJjEtf6 (дата обращения: 28.12.2021). – Текст : электронный.

44. Постановление о прекращении уголовного дела в связи с отказом государственного обвинителя от обвинения по делу № 1-139/2019 Киржачского районного суда Владимирской области // Интернет-ресурс «Судебные и нормативные акты Российской Федерации» (СудАкт.Ру) : [сайт]. – 2021. – URL: https://sudact.ru/regular/doc/MLSBvwPvs0HS/ (дата обращения: 27.12.2021). – Текст : электронный.

45. Приговор Кировского районного суда г. Екатеринбурга в отношении М. по ч. 2 ст. 273, ч. 3 ст. 272 и ч. 4 ст. 159^6 УК РФ // Интернет-ресурс «Судебные и нормативные акты Российской Федерации» (СудАкт.Ру) : [сайт]. – 2021. – URL: https://sudact.ru/regular/doc/YwQr7ZHgaQgR/ (дата обращения: 24.12.2021). – Текст : электронный.

46. Приговор Фрунзенского районного суда г. Саратова в отношении М. по п. «а» ч. 3 ст. 159^6 УК РФ // Интернет-ресурс «Судебные и нормативные акты Российской Федерации» (СудАкт.Ру) : [сайт]. – 2021. – URL: https://sudact.ru/regular/doc/qtCZQWKOpk5x/t (дата обращения: 23.12.2021). – Текст : электронный.

Приложение 1

ОБРАЗЦЫ ЗАПРОСОВ

Угловой штамп следственного органа

Управляющему _____
ФИО _____
603006, г. Н. Новгород,____
_____

Уважаемая(-ый), *Имя Отчество*!

В связи с расследованием уголовного дела № ____, возбужденного *дата* по признакам состава преступления, предусмотренного ____ УК РФ, на основании ч. 4 ст. 21 УПК РФ и ст. 26 Федерального закона от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности» прошу Вас предоставить справку по операциям по счету № _____, содержащую следующие сведения:

– персональные данные владельца счета (ФИО, привязанные абонентские номера и адреса электронной почты);

– движение денежных средств по счету за период с момента открытия по настоящее время с расшифровкой получателя и назначения платежа;

– сведения об IP-адресах, при использовании которых осуществлялось подключение к интернет-платформе по управлению счетом;

– сведения об IP-адресах и иных счетах, подключение к которым происходило при использовании одного интернет-браузера, полученные посредством анализа cookie-файлов.

В связи с ограниченными сроками расследования ответ прошу направить на e-mail: _____ с последующим отправлением почтой по адресу: _____.

Следователь

СОГЛАСЕН:

Руководитель следственного органа

Угловой штамп следственного органа

Генеральному директору
ООО «ВебМани.Ру»
ФИО _____

119049, г. Москва,
ул. Коровий вал, д. 7

Уважаемая(-ый), *Имя Отчество*!

В связи с расследованием уголовного дела № _____, возбужденного *дата* по признакам состава преступления, предусмотренного ____ УК РФ, на основании ч. 4 ст. 21 УПК РФ и ст. 26 Федерального закона от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе» прошу Вас предоставить информацию об электронных кошельках Z 1444*****088, Z 3193*****794, а именно:

1. Когда и с какого IP-адреса были созданы указанные кошельки.
2. Какие регистрационные данные указали о себе владельцы данных электронных кошельков.
3. С каких IP-адресов осуществлялись авторизации на указанные электронные кошельки с момента регистрации по настоящее время.
4. Проведенные транзакции с использованием вышеуказанных электронных кошельков за период с момента регистрации по настоящее время.

В связи с ограниченными сроками расследования ответ прошу направить на e-mail: _____ с последующим отправлением почтой по адресу: _____.

Следователь

СОГЛАСЕН:

Руководитель следственного органа

Угловой штамп следственного органа

Руководителю
Нижегородского филиала
ПАО «ВымпелКом»
ФИО _____

г. Нижний Новгород,
ул. Кулибина, д. 3

ЗАПРОС

В связи с расследованием уголовного дела № _____, возбужденного *дата* по признакам состава преступления, предусмотренного ____ УК РФ, на основании ч. 4 ст. 21 УПК РФ прошу Вас предоставить сведения об абоненте, которому был предоставлен IP-адрес 92.***.201.31 26 декабря 2016 г. в 14 часов 17 минут 45 секунд. Предположительно с указанного IP-адреса доступ был осуществлен к www._____.ru[1] (IP-адрес 92*****22).

В связи с ограниченными сроками расследования ответ прошу направить на e-mail: _____ с последующим отправлением почтой по адресу: _____.

Следователь

[1] Указание сведений о ресурсе, к которому был осуществлен доступ с интересующего IP-адреса, обязательно при использовании провайдером системы преобразования сетевых адресов «NAT» (см. раздел 2). Ресурс, к которому был осуществлен доступ, – тот же ресурс, предоставивший сведения об IP-адресах.

Угловой штамп следственного органа

Генеральному директору
по безопасности
ООО «ВКонтакте»

Черненко Н.В.

г. Санкт-Петербург,
пр. Лиговский,
д. 61, стр. 3

ЗАПРОС

В связи с расследованием уголовного дела № _____, возбужденного *дата* по признакам состава преступления, предусмотренного ____ УК РФ, на основании ч. 4 ст. 21 УПК РФ прошу Вас предоставить следующую информацию в отношении пользователя «Иван Петров» (id275949102):

– дата регистрации аккаунта, регистрационные данные (ФИО, абонентские номера, адреса электронной почты и др.);

– сведения об IP-адресах, с которых осуществлялось подключение к аккаунту с момента регистрации по настоящее время;

– сведения об иных IP-адресах и иных аккаунтах пользователя, подключение к которым происходило при использовании одного интернет-браузера, полученные посредством анализа cookie-файлов.

В связи с ограниченными сроками расследования ответ прошу направить на e-mail: _____ с последующим отправлением почтой по адресу:_____.

Следователь

Угловой штамп следственного органа

Председателю правления
АО «КИВИ Банк»

117648, г. Москва,
мкр. Чертаново Северное,
д. 1А, корп. 1

Уважаемая(-ый), *Имя Отчество*!

В связи с расследованием уголовного дела № _____, возбужденного *дата* по признакам преступления, предусмотренного ____ УК РФ, в соответствии с требованиями ст. 26 Федерального закона «О банках и банковской деятельности» прошу Вас предоставить сведения о дате, времени создания электронных кошельков QIWI № 7909***4728, 7909***4736, 7964***7604, 7964***7640, 7909***7332, 79091***341, 7905***2320, 79091***469, об IP-адресах (с указанием точной даты и времени), с которых осуществлялись регистрация, доступ и администрирование кошелька с момента регистрации по настоящее время.

Кроме того, прошу предоставить сведения о движении денежных средств по электронным кошелькам QIWI № 7909***4728, 7909***4736, 7964***7604, 7964***7640, 7909***7332, 79091***341, 7905***2320, 79091***469 с момента регистрации по настоящее время, а также сведения о перечислениях с кошельков на банковские карты с указанием их номеров и наименования банка-эмитента.

В связи с ограниченными сроками расследования ответ прошу направить на e-mail: _____ с последующим отправлением почтой по адресу: _____.

Следователь

СОГЛАСЕН:

Руководитель следственного органа

Приложение 2

ВЫДЕРЖКА ИЗ РЕЗОЛЮТИВНОЙ ЧАСТИ ПОСТАНОВЛЕНИЯ О ВОЗБУЖДЕНИИ ПЕРЕД СУДОМ ХОДАТАЙСТВА О РАЗРЕШЕНИИ ПОЛУЧЕНИЯ ИНФОРМАЦИИ О СОЕДИНЕНИЯХ МЕЖДУ АБОНЕНТАМИ

СОГЛАСЕН

Руководитель
следственного органа
_____ ФИО
(подпись)
«___» _____ 20__ г.

ПОСТАНОВЛЕНИЕ
о возбуждении перед судом ходатайства о разрешении получения информации о соединениях между абонентами

На основании изложенного и руководствуясь ст. 13, п. 7 ч. 2 ст. 29, ч. 1 ст. 165, ст. 186[1] УПК РФ,

ПОСТАНОВИЛ:

1. Ходатайствовать перед _____ судом о разрешении получения информации о соединениях между абонентами в учреждении связи – Северо-Западном филиале ПАО «Мегафон», расположенном по адресу: г. Санкт-Петербург, ул. Караванная, д. 10, а именно:

– о лицах, на которых зарегистрирован абонентский номер «921****555»;

– о соединениях между абонентами по абонентскому номеру «921****555» в виде распечаток за период с 01.01.2017 по настоящее время;

– об IMEI-номерах мобильных телефонов, в которых использовался абонентский номер: «921****555»;

– об используемых базовых станциях (с указанием их адреса и места расположения) во время соединений абонентского номера «921****555» за период с 01.01.2017 по настоящее время;

– о движении денежных средств по счету абонентского номера «921****555» за период с 01.01.2017 по настоящее время.

2. Копию настоящего постановления направить прокурору _____.

Следователь

Приложение 3

ВЫДЕРЖКА ИЗ РЕЗОЛЮТИВНОЙ ЧАСТИ ПОСТАНОВЛЕНИЯ О ВОЗБУЖДЕНИИ ПЕРЕД СУДОМ ХОДАТАЙСТВА О ПРОИЗВОДСТВЕ ВЫЕМКИ В УЧРЕЖДЕНИИ СВЯЗИ

СОГЛАСЕН

Руководитель
следственного органа
_____ ФИО
(подпись)
«___» _____ 20__ г.

ПОСТАНОВЛЕНИЕ
о возбуждении перед судом ходатайства о производстве выемки в учреждении связи

На основании изложенного и руководствуясь ст. 13, п. 7 ч. 2 ст. 29, ч. 1 ст. 165, ч. 3 ст. 183 УПК РФ, ст. 53 Федерального закона от 7 июля 2003 г. «О связи»,

ПОСТАНОВИЛ:

1. Ходатайствовать перед _____ судом о разрешении производства выемки в учреждении связи – Нижегородском филиале ПАО «Ростелеком», расположенном по адресу: г. Нижний Новгород, ул. Б. Покровская, д. 56, данных об абоненте, которому 12 июня 2017 г. в 00 часов 20 минут 34 секунды выдавался IP-адрес 79.***.11.88, и данные об абоненте, которому 11 июня 2017 г. в 12 часов 39 минут выдавался IP-адрес 93.***.189.8.
2. Копию настоящего постановления направить прокурору _____.

Следователь

Учебное издание

кандидат юридических наук, доцент
Ушаков Андрей Юрьевич
(Нижегородский филиал Санкт-Петербургской академии
Следственного комитета России);
кандидат юридических наук, доцент
Саакян Артём Григорьевич,
кандидат юридических наук
Поздышев Роман Сергеевич,
кандидат юридических наук, доцент
Степанова Марина Анатольевна
(Нижегородская академия МВД России)

ОСОБЕННОСТИ КВАЛИФИКАЦИИ И РАССЛЕДОВАНИЯ ХИЩЕНИЙ ЭЛЕКТРОННЫХ ДЕНЕЖНЫХ СРЕДСТВ, В ТОМ ЧИСЛЕ СОВЕРШЕННЫХ ПОСРЕДСТВОМ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Учебное пособие

Редактор *Т. Ю. Булганина*
Компьютерная верстка *Т. Ю. Булганиной*
Дизайн обложки *К. А. Быкова*

Подписано в печать 31.08.2022. Формат 60x84/16. Усл. печ. л. 3,53
Тираж 100 экз. Заказ № 168

Редакционно-издательский отдел
Нижегородской академии МВД России

Отпечатано в отделении полиграфической и оперативной печати
Нижегородской академии МВД России

603144, Н. Новгород, Анкудиновское шоссе, 3