Министерство внутренних дел Российской Федерации
Казанский юридический институт

Т.И. Гарипов

Доказывание по уголовным делам о преступлениях, совершенных с использованием современных информационно-телекоммуникационных технологий

Казань
КЮИ МВД России
2022

ББК 67.410.204.1
Г20

Одобрено редакционно-издательским советом КЮИ МВД России

Рецензенты:
кандидат юридических наук, доцент **Д.Н. Рудов**
(Белгородский юридический институт МВД России
им. И.Д. Путилина);
М.В. Барышева
(Управление организации дознания
МВД по Республике Татарстан)

Г20 **Гарипов Т.И.**

Доказывание по уголовным делам о преступлениях, совершенных с использованием современных информационно-телекоммуникационных технологий: учебное пособие / Т.И. Гарипов. – Казань: Казанский юридический институт МВД России, 2022. – 89 с.

В пособии раскрываются актуальные вопросы доказывания по уголовным делам о преступлениях, совершенных с применением современных информационно-телекоммуникационных технологий.

Предназначено для преподавателей, курсантов, слушателей образовательных организаций системы МВД России, сотрудников органов внутренних дел Российской Федерации.

ББК 67.410.204.1

ОГЛАВЛЕНИЕИЕ

ВВЕДЕНИЕ

Актуальность темы исследования обусловлена интенсивным развитием современных цифровых технологий и активным внедрением их в повседневную жизнь общества. На сегодняшний день в информационных системах как частных, так и государственных организаций содержится достаточно большое количество обрабатываемых данных. Любые операции с этими данными осуществляются с использованием информационных технологий, которые, с одной стороны, повышают эффективность деятельности организаций и учреждений, облегчают повседневную жизнь граждан, снижая издержки и экономя время, но с другой стороны – создают угрозы уязвимости таких информационных систем. В связи с этим в последнее десятилетие все большую актуальность приобретает проблема киберпреступности – преступлений, совершаемых с использование информационно-телекоммуникационных технологий. В частности, данная проблема касается преступлений корыстной направленности, связанных с хищением денежных средств, как правило, в безналичной форме или с использованием электронных средств платежа. Среди преступлений, совершаемых с применением высоких технологий, подавляющее большинство (более 80%) составляют различные формы хищения (см. приложение № 4). Наибольшую актуальность приобрели различные виды мошенничества, основным орудием совершения которых выступают цифровые технологии, и совершаются они, как правило, в дистанционной форме без фактического взаимодействия с потерпевшим. Так, за 12 месяцев 2021 года количество зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий, выросло на 1,4% по сравнению с аналогичным периодом прошлого года. При этом примерно три четверти таких преступлений (75%) совершается путем кражи или мошенничества. Всего в период с января по декабрь 2021 года за-

регистрировано 249 249 мошенничеств, совершенных с использованием информационно-телекоммуникационных технологий (см. приложение № 1). Прирост таких мошенничеств составляет 13,3%[1]. В связи с этим нагрузка на правоохранительные органы по выявлению, раскрытию и расследованию данных преступлений все более возрастает, что обусловливает необходимость в выработке рациональных подходов в криминалистическом обеспечении деятельности следователя или дознавателя. Сложность расследования подобных преступлений заключается не только в особом алгоритме и тактике производства следственных и процессуальных действий, но и в недостатке специальных познаний следователя в сфере современных цифровых технологий ввиду их интенсивного развития. Правоохранительные органы просто «не успевают» реагировать на новые технологические способы совершения мошенничества, а когда методика расследования подобных преступлений уже разработана, то появляются новые виды мошенничеств, требующие разработки новой методики. Поэтому актуализация и разработка современных методик расследования мошенничества с использованием цифровых технологий представляется нам архиважной.

Степень разработанности темы исследования. Методика расследования мошенничеств различных видов достаточно широко освещена в современной криминалистической науке. Особенно актуальными стали исследования последних лет, посвященные вопросам расследования киберпреступлений. Так, различные аспекты расследования корыстных преступлений с использованием современных информационных технологий рассматривали в своих работах Р.С. Атаманов, А.С. Вражнов, В.В. Крылов, В.А. Мещеряков, Ю.В. Гаврилин, Н.Г. Шурухнов, В.Б. Вехов, Р.А. Белевский, Е.С. Шевченко и другие.

Объектом исследования выступают общественные отношения, которые складываются в сфере преступной деятельности лиц, совершающих мошеннические действия с использованием цифровых технологий, и проявляющиеся в закономерностях механизма совершения преступления, следообразо-

[1] Состояние преступности в Российской Федерации за январь-декабрь 2021. URL: https://мвд.рф/reports/item/28021552/ (дата обращения 12.10.2022).

вания и возникновения информации о преступлении, о его участниках и поисково-познавательной деятельности должностных лиц, производящих предварительное расследование данной категории преступлений.

Предметом исследования выступают положения действующего уголовного и уголовно-процессуального законодательства в части, касающейся расследования преступлений с использованием цифровых технологий, материалы следственно-судебной практики, диссертации, монографии и иные научные публикации по исследуемой теме.

Целью настоящего исследования является комплексное рассмотрение вопросов методики расследования мошенничества с использованием цифровых технологий, а также разработка и формулирование на основе проведенного анализа научно обоснованных криминалистических рекомендаций по расследованию вышеуказанной категории преступлений.

На основании поставленной цели, следует сформулировать следующие основные **задачи исследования:**

- раскрыть уголовно-правовую характеристику мошенничеств, совершаемых с использованием цифровых технологий;
- проанализировать криминалистическую характеристику цифровых мошенничеств, определив основные обстоятельства, подлежащие установлению при расследовании данных преступлений;
- дать характеристику организационно-тактическим особенностям возбуждения уголовного дела и планированию первоначального этапа расследования мошенничеств с использованием цифровых технологий;
- рассмотреть тактические особенности первоначальных следственных действий при расследовании мошенничеств, совершенных с использованием цифровых технологий;
- сформулировать научно-обоснованные криминалистические рекомендации, определяющие рациональные подходы при планировании и организации производства предварительного расследования по уголовным делам о мошенничествах, совершенных с использованием цифровых технологий.

Методику проведения настоящего исследования составляют общенаучные и частнонаучные методы познания объективной действительности: формально-логический, системно-структурный анализ, методы обобщения и описания, моделирования, статистический и сравнительно-правовой методы.

Структурно настоящая работа состоит из введения, двух глав, разделенных на четыре параграфа, заключения, списка использованной литературы и приложений.

ГЛАВА 1. УГОЛОВНО-ПРАВОВАЯ И КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ ЦИФРОВЫХ ТЕХНОЛОГИЙ

§ 1. Понятие и содержание уголовно-правовой характеристики мошенничества с использованием цифровых технологий

В связи со стремительным развитием цифровых технологий в последнее десятилетие методы и области их использования становятся все разнообразнее и зачастую преступают рамки законов. Вместе с процессом развития технологий сети Интернет, кибернетического пространства появляются новые виды обмана и злоупотребления доверием как физических, так и юридических лиц. Именно обман и злоупотребление доверием являются условиями квалификации такого преступного деяния, как мошенничество.

Так как преступления в сфере мошенничества с использованием цифровых технологий имеют тенденцию роста, в связи с этим актуальность данной темы не вызывает сомнений.

Понятие цифровых технологий в контексте юридического толкования не имеет четкого определения. В широком смысле слова, технология – это примененные научные знания, необходимые для решения практических задач. На сегодняшний день электронными или цифровыми технологиями принято называть те средства и электронные приборы, с помощью которых человек выполняет поставленные практические задачи на основании определенного алгоритма, заранее созданного для дальнейшего его внедрения и применения[1].

[1] Зварыгин В.Е., Машинникова Н.О. Некоторые вопросы, связанные с

В рамках данной работы под цифровыми технологиями понимается совокупность электронных устройств и соответствующего программного обеспечения, выполняющих определенные задачи. Применительно к преступлениям, связанным с мошенничеством, могут использоваться такие виды цифровых технологий, как компьютерная техника, сеть Интернет, электронная почта, электронные средства платежа, банковские системы, базы данных, информационно-телекоммуникационные сети, сотовая связь, а также остальное огромное множество информационных технологий, существующих на сегодняшний день.

Само по себе мошенничество с использованием цифровых технологий в большинстве случаев является дистанционным способом мошенничества и может применяться в таких сферах экономики, как производственные отношения, производство, финансы, услуги; в сфере политики, в деятельности органов власти, общественных организаций, а также в таких сферах жизнедеятельности общества, как культура, образование, спорт, искусство. Законодатель определяет содержание мошенничества в ч. 1 ст. 159 Уголовного кодекса Российской Федерации (далее – УК РФ) «как хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием»[1].

Преступления в сфере мошенничества с использованием электронных технологий нашли своё место в следующих статьях уголовного кодекса: ст. 159 «Мошенничество», 159.1 «Мошенничество в сфере кредитования», 159.2 Мошенничество при получении выплат», 159.3 «Мошенничество с использованием электронных средств платежа», 159.5 «Мошенничество в сфере страхования» и 159.6 «Мошенничество в сфере компьютерной информации». Во всех вышеуказанных составах преступления использование электронных технологий конкретно не предусмотрено диспозицией статьи, поэтому следует понимать, что любое преступление, предусмотренное пунктами статьи 159 УК РФ, воз-

---

определением предмета мошенничества по статье 159 УК РФ // Вестник Удмуртского университета. Серия «Экономика и право». 2016. С. 96.

[1] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 28.01.2022) // Собрание законодательства Российской Федерации. 17.06.1996. № 25. Ст. 2954.

можно совершить и зачастую совершается путем фальсификации официальных документов, средств обработки фотографий, текста, наложения поддельной печати, иных видов фальсификации через компьютерные программы, электронные устройства и иные программные продукты. При этом сам факт использования того или иного электронного устройства на квалификацию преступного деяния влиять не будет[1].

Мошенничество достаточно часто совершается с использованием сотовых телефонов, электронной почты и социальных сетей, поддельных интернет сайтов, на которых размещена заведомо ложная информация, способная привести к имущественному ущербу. Мошенники используют различные программные продукты, например, для смены голосовой речи при аналоговой или цифровой связи и многое другое, что дает возможность обманывать и вводить в заблуждение не только физических лиц, но и юридические структуры[2].

Непосредственным объектом мошенничества с использованием цифровых технологий является собственность конкретных физических и юридических лиц как та цель, на которую нацелены деяние злоумышленников.

Предметом мошенничества с использованием цифровых технологий является как собственность, имущество физического или юридического лица, так и право на это имущество. Это могут быть денежные средства – как наличные, так и безналичные, а также имущество – как движимое, так и недвижимое. Говоря о предмете мошенничества в виде безналичных денежных средств, прежде всего следует упомянуть такие платежные системы, как банковская кредитная карта, электронные кошельки, которые способны поддерживать максимальную анонимность преступника, адреса, приуроченные к криптовалютным биржам.

При квалификации мошенничества обман и злоупотребление доверием служат способом завладения имуществом, между ними

---

[1] О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 // Бюллетень Верховного Суда Российской Федерации. 2018. № 2. .

[2] Машинникова Н.О. Мошенничество. Сущность. Способы совершения // European journal of law and political sciences. 2016. С. 46.

и переходом имущества во владение виновного должна быть установлена причинная связь[1].

Субъект мошенничества общий – вменяемое лицо, достигшее шестнадцатилетнего возраста, за исключением ч. 3 ст. ст. 159 – 159.6, где указано о служебном положении субъекта преступления, в случае чего он будет уже именоваться специальным субъектом преступления. Кроме того, субъект мошенничества с использованием цифровых технологий должен обладать хотя бы одним из видов этих цифровых технологий. Тенденция данного вида мошенничества сегодня направлена на контакт с жертвой преступления через мобильную или интернет связь, распространяется также и подделка банковских карт через сконструированные электронные приборы[2].

Субъективная сторона, помимо формы вины, характеризуется мотивом и целью преступления. Говоря о совершении мошенничества с использованием цифровых технологий, в большинстве случаев мотив схож с его целью – корысть.

Процесс создания и распространения методов борьбы с мошенничеством с использованием цифровых технологий в настоящее время активно ведется как правоохранительными органами, так и учеными – юристами и криминологами. Вместе с тем для эффективного противодействия данному виду преступлений необходимо соответствующее техническое оснащение правоохранительных органов, а также привлечение к данной деятельности специалистов, прежде всего в сфере информационных технологий.

В связи с увеличением количества преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, актуализируются вопросы разграничения смежных составов преступлений, предусмотренных п. «г» ч. 3 ст. 158, ст. 159, 159.3 УК РФ.

Введение специальных составов мошенничества преследовало цель дифференцировать различные виды мошенничеств, по-

---

[1] Веремеенко М.В. Объект мошенничества в сфере предпринимательской деятельности // Уголовная юстиция. 2014. С. 6.

[2] Кошаева Т.О. Совершенствование уголовного законодательства об ответственности за мошенничество // Журнал российского права. 2018.

скольку существовавшая конструкция ст. 159 УК РФ, по мнению авторов проекта Федерального закона от 29.11.2012 № 207-ФЗ, не в полной мере учитывала особенности современных экономических отношений, связанных с модернизацией банковского сектора, страховых отношений и т.д.[1] Среди одной из основных задач законопроекта обосновывалось способствование «правильной квалификации содеянного органами предварительного расследования и судом»[2]. Вместе с тем, как отмечается в научной литературе, вопросы относительно правильной квалификации и отграничений смежных составов преступлений такого рода хищений возникают до сих пор[3]. Весьма сложной является проблема разграничения преступлений, предусмотренных п. «г» ч. 3 ст. 158 и ст. 159.3 УК РФ. Интересен тот факт, что смежность данных составов преступлений подчеркнута законодателем при конструировании п. «г» ч. 3 ст. 158 УК РФ: «Кража, то есть тайное хищение чужого имущества с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного статьей 159.3 настоящего Кодекса)».

Представляется, что разграничение данных составов будет происходить исходя из общих оснований разграничения краж и мошенничеств, дополненных особенностями, связанными с юридически значимыми признаками данных составов.

Одним из таких оснований является признак наличия (отсутствия) тайности деяния. Кража совершается тайно, т.е. потерпевший не осведомлен об изъятии принадлежащего ему имущества. При совершении мошенничества потерпевший или иное лицо передает имущество или право на него виновному, но не осознает

---

[1] Пояснительная записка «К проекту Федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации и иные законодательные акты Российской Федерации» (в части дифференциации мошенничества на отдельные составы). С. 1.

[2] Там же. С. 3.

[3] Например, см.: Рогозина И.Г. Уголовно-правовая политика противодействия преступлениям против собственности // Вестник Омской юридической академии. 2016. № 2; Смолин С.В. Мошенничество в сфере компьютерной информации: проблемы толкования и применения ст. 159 УК РФ // Информационное право. 2015. № 4.

неправомерность такой передачи, поскольку находится под воздействием обмана или злоупотребления доверием[1].

Например, если лицо, представляясь сотрудником службы безопасности банка, в ходе телефонного разговора просит потерпевшего сообщить персональные данные (пин-код, данные банковской карты и код CW2/CVC2 на её обороте) якобы для предотвращения списания денежных средств или под другим предлогом, а затем, используя полученные данные, самостоятельно похищает денежные средства потерпевшего путем их перевода на другой банковский счет, то данные действия квалифицируются как кража (п. «г» ч. 3 ст. 158 УК РФ). Так, Архипова осуществила телефонный звонок на мобильный номер, зарегистрированный на Б., и, представившись сотрудником банка, сообщила последней заведомо ложную информацию о том, что с ее банковской карты осуществляется несанкционированное списание денежных средств и для блокировки транзакций необходимо сообщить номер карты и пароли, которые поступят в СМС. Получив от потерпевшей Б. необходимую информацию, Архипова посредством мобильной связи перевела и, таким образом, тайно похитила со счета банковской карты, принадлежащие последней денежные средства[2].

Однако если лицо не самостоятельно переводит денежные средства, а, например, склоняет потерпевшего к их переводу на «защитный счет» под предлогом необходимости предотвращения попытки неправомерного списания, то его действия должны быть квалифицированы как мошенничество (ст. 159 УК РФ).

Другим основанием для разграничения рассматриваемых составов преступлений выступает способ совершения преступления. При совершении кражи обман и злоупотребление доверием могут использоваться лишь для облегчения доступа к имуществу, в то время как непосредственно изъятие имущества осуществляется

[1] Безбородов Д.А., Зарубин А.В., Краев Д.Ю., Попов А.Н. Специальные вопросы квалификации преступлений против собственности: учебное пособие / под общ. ред. А.Н. Попова. Санкт-Петербург: Санкт-Петербургский юридический институт (филиал) Университета прокуратуры Российской Федерации, 2019. С. 96.

[2] Приговор Домодедовского городского суда Московской области от 6.05.2019 по уголовному делу № 1-82/2019 // СПС «КонсультантПлюс».

самим субъектом преступления (путем перевода их с одного счета на другой, снятия их посредством использования банкомата). При совершении мошенничества обман и злоупотребление доверием служат непосредственным способом завладения имуществом, т.е. потерпевший или иное лицо, находясь под их воздействием, самостоятельно передает или не препятствует изъятию имущества или права на него субъектом преступления.

Вместе с тем, совершая преступление, предусмотренное ст. 159.3 УК РФ, субъект преступления осуществляет хищение путем обмана или злоупотребления доверием уполномоченного работника кредитной, торговой или иной организации, например, при совершении удостоверяющей подписи в чеке о покупке банковской картой, не принадлежащей виновному. Причем согласно разъяснениям, данным в постановлении Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», такой обман или злоупотребление доверием могут выражаться как в сообщении ложных сведений о принадлежности банковской карты лицу, так и в пассивном обмане – несообщении сведений о незаконном владении платежной картой.

Так, по уголовному делу № 1-270/2020 Воскресенским городским судом Московской области установлено, что лицо, обнаружив на земле банковскую карту ПАО «ВТБ», оборудованную чипом системы бесконтактной оплаты «PayPass», последовательно совершило 14 покупок сначала в нескольких кафе, затем в аптеке и других торговых организациях, причинив значительный ущерб владельцу карты, в связи с чем действия виновного были квалифицированы по ч. 2 ст. 159.3 УК РФ[1].

В то же время дискуссионным остается вопрос о том, может ли преступление по ст. 159.3 УК РФ быть совершено путем пассивного обмана в виде несообщения работнику кредитной, торговой или иной организации сведений о неправомерном владении платежной картой, например, когда совершается бесконтактная

[1] Приговор Воскресенского городского суда Московской области от 30.07.2020 № 1-270/2020 по делу № 1-270/2020: судебные и нормативные акты Российской Федерации. URL: https://sudact.ru/regular/doc/SRBxx56elLr9/ (дата обращения: 12.10.2022).

оплата на кассе самообслуживания и работник организации фактически не задействован при её проведении. Некоторую определенность в отношении поставленной проблемы вносят материалы судебной практики Верховного Суда Российской Федерации.

В определении суда кассационной инстанции Судебной коллегии по уголовным делам Верховного Суда Российской Федерации[1] (далее – Определение) по уголовному делу в отношении Кактана Ю.Ю. ставится под сомнение переквалификация судом кассационной инстанции действий Кактана Ю.Ю. с ч. 3 ст. 30, п. «г» ч. 3 ст. 158 УК РФ на ч. 3 ст. 30, ч. 1 ст. 159.3 УК РФ. Из материалов уголовного дела следует, что Кактан Ю.Ю., найдя во дворе банковскую карту с функцией бесконтактной оплаты, произвел оплату товаров в различных магазинах и кафе с использованием банковской карты потерпевшего аналогично обстоятельствам дела, описанным в приведенном ранее приговоре.

В Определении указывается, что ссылка судов на п. 17 ППВС РФ № 48 о возможности осуществления мошенничества путем пассивного обмана является необоснованной, поскольку данные разъяснения были даны применительно к прежней редакции ст. 159.3 УК РФ, а ввиду принятия Федерального закона от 23.04.2018 № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» в диспозицию ст. 159.3 УК РФ были внесены изменения, и этим же законом введена уголовная ответственность за кражу с банковского счета (п. «г» ч. 3 ст. 158 УК РФ).

Согласно правовой позиции, представленной в Определении, действующим законодательством не предусмотрена обязанность по идентификации держателя платежной карты по удостоверяющим личность документам уполномоченными работниками торговых организаций, осуществляющих платежные операции.

Исходя из этого, при совершении операций по списанию денежных средств с банковского счета без непосредственного участия работников торговых организаций (например, при проведе-

[1] Определение суда кассационной инстанции Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 29.09.2020 по делу № 12-УДП2О-5-К6: сайт Верховного Суда Российской Федерации. URL: https://www.vsrf.ru/stor_pdf.php?id=1954970.

нии бесконтактной оплаты на кассе самообслуживания), ложные сведения о принадлежности карты субъектом преступления не сообщаются, и работники в заблуждение не вводятся. Следовательно, совершение подобного деяния должно быть квалифицировано не по ст. 159.3 УК РФ, а по п. «г» ч. 3 ст. 158 УК РФ.

Поэтому главным при квалификации деяния по ст. 159.3 УК РФ является то обстоятельство, что при использовании виновным не принадлежащей ему карты и расходовании средств вопреки воле её держателя, совершается обман уполномоченного работника кредитной, торговой или иной организации. Особенность данного состава будет заключаться также в том, что, хотя обманом или злоупотреблением доверием в заблуждение вводится уполномоченный работник кредитной, торговой или иной организации, потерпевшим по такому уголовному делу признается владелец карты, средства которой использовались при осуществлении соответствующей операции.

Особого внимания заслуживает сравнение санкций рассматриваемых составов преступлений. Преступление по п. «г» ч. 3 ст. 158 УК РФ является тяжким преступлением и предусматривает наказание в виде лишения свободы на срок до шести лет, в то время как состав преступления, предусмотренный ч. 1 ст. 159.3 УК РФ при отсутствии квалифицирующих признаков, является преступлением небольшой тяжести и его совершение влечет наказание в виде лишения свободы на срок до трех лет, а приготовление к такому преступлению уголовно ненаказуемо.

Именно поэтому в судебной практике возникают ситуации, когда адвокаты в целях осуществления защиты по уголовному делу стараются добиться переквалификации инкриминируемого преступления с п. «г» ч. 3 ст. 158 УК РФ на ст. 159.3 УК РФ. Так, в кассационной жалобе на приговор Истринского городского суда Московской области от 21.02.2020 защитник, выражая несогласие с приговором, полагает, что действия С. следует квалифицировать не по п. «г» ч. 3 ст. 158 УК РФ, а по ст. 159.3 УК РФ. При этом в судебном заседании установлено, что С., воспользовавшись банковской картой потерпевшего, произвела дважды операции по снятию денежных средств в банкомате. Вместе с тем судом ука-

зывается, что С. действовала тайно для потерпевшего, в связи с чем деяние было правильно квалифицировано судом первой инстанции по п. «г» ч. 3 ст. 158 УК РФ[1].

Таким образом, в данном параграфе были проанализированы уголовно-правовая характеристика мошенничества с использованием цифровых технологий и основания для разграничения преступления, предусмотренного ст. 159.3 УК РФ, от смежных составов с учетом действующего законодательства и правоприменительной практики. В заключение ещё раз отметим необходимость уточнения юридически значимых критериев отграничения мошенничеств с использованием электронных средств платежа не только от краж, но и от прочих специальных составов мошенничества с использованием цифровых технологий.

[1] Определение Судебной коллегии по уголовным делам Первого кассационного суда общей юрисдикции от 23.09.2020 по уголовному делу № 77-1775/2020 // СПС «КонсультантПлюс».

§ 2. Криминалистическая характеристика, обстоятельства, подлежащие установлению при расследовании мошенничества с использованием цифровых технологий

В век информационных технологий «информация», в том числе и цифровая компьютерная, имеет особое значение для человека, в связи с чем нередко становится объектом, предметом, а также средством совершения преступления. Ее «виктимность» определяется низким уровнем либо полным отсутствием системы защиты. Повышенный интерес к конкретным информационным ресурсам и особая ценность компьютерной информации определяет наличие попыток противоправного воздействия даже при очень надежной защите. В связи с этим нам представляется необходимым начать рассмотрение криминалистической характеристики мошенничества, совершаемого с использованием цифровых технологий, с понятия компьютерной информации, чаще всего выступающей в качестве дополнительного предмета преступного посягательства.

Уголовное законодательство содержит ряд норм, предусматривающих ответственность за совершение преступлений в сфере цифровых технологий. Мошенничество с использованием цифровых технологий, в ходе которого основным непосредственным объектом преступления выступают имущественные отношения (собственность), все же следует считать частью компьютерных преступлений, поскольку компьютерная информация и цифровые технологии являются предметом (орудием) совершения преступления. Ввод, удаление, блокирование и модификация цифровой информации позволяют совершить хищение чужого имущества.

Компьютерная информация представляет собой сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Компьютерная информация неразрывно связана с ее носителем – электронно-вычислительной машиной. Посредством электрических сигналов возможна передача информации, не предназначен-

ной для обработки средствами вычислительной техники, т. е. не являющейся компьютерной (например, радиосвязь)[1].

Потерпевшим признается физическое лицо, которому преступлением причинен физический, имущественный, моральный вред, а также юридическое лицо в случае причинения преступлением вреда его имуществу и деловой репутации (ч. 1 ст. 42 Уголовно-процессуального кодекса Российской Федерации (далее – УПК РФ))[2]. Процессуальное признание потерпевшим осуществляется путем вынесения соответствующего постановления. При этом в некоторых случаях личность потерпевшего характеризуется виктимным поведением.

С учетом специфики рассматриваемого вида мошенничества для решения задач расследования очень важно иметь представление о «портрете» преступника, именно он представляет наибольший интерес. Личность преступника – собирательное понятие, включающее весь комплекс характеризующих его признаков и связей: сведения о поле, возрасте, гражданстве, образовании, социальном и должностном положении и др.[3]

Говоря о личности преступника, совершающего хищение с использованием интернет-технологий, важно для начала определить, что же понимается под «личностью преступника» в криминалистике.

История развития и становления личности преступника в отечественной криминалистике началась в XVIII веке. Базисом рассмотрения личности обвиняемого как самостоятельного направления является активное исследование данного понятия в 60-70 гг. XX века.

Ведя речь о личности преступника, совершающего хищения с использованием интернет-технологий, необходимо отметить на-

---

[1] Старичков М.В. Понятие «компьютерная информация» в российском уголовном праве // Вестник Восточно-Сибирского института Министерства внутренних дел России. 2014. № 1 (68). С. 16-20.

[2] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 30.12.2021, с изм. от 23.09.2021) // Собрание законодательства Российской Федерации, 24.12.2001, № 52 (ч. I), ст. 4921.

[3] Сударев Л.А. Личность преступника, совершающего компьютерные преступления // Вестник Московского университета МВД России. Москва: Московский университет МВД РФ им. В.Я. Кикотя, 2007. № 1. С. 98-103.

личие профессиональной подготовки, оперативность выполнения задач, умение систематизировать материал; также в большинстве случаев преступники имеют неоконченное техническое образование.

При характеристике пола личности, совершившего преступление с помощью интернет-технологий, значительное число ученых считают, что преступления с использованием интернет-технологий совершаются в основном мужчинами. Женщины чаще всего в таких преступлениях выступают в роли соучастников. При этом представляет интерес, что наблюдается тенденция к увеличению числа преступлений с использованием интернет-технологий, совершаемых женщинами.

Что касается образования, уровня подготовки и навыков личности преступника, совершающего хищения с использованием интернет-технологий, то их знания в данной области во многом предопределяют тактику действий и степень сложности преступления.

Принято считать, что общественно опасные деяния в сфере информационных технологий совершают «компьютерные гении», «хакеры», что они обладают высшим техническим образованием. На самом деле это далеко не так. Большинство преступников имеют среднее техническое или неоконченное высшее образование, а уровень профессиональной подготовки и знаний не является качественным. Отсюда следует, что преступником в рассматриваемой сфере может быть как профессионал, высококвалифицированный специалист, так и любитель, «квазихакер». Это дает основание сделать вывод о разном интеллектуальном уровне лиц, совершающих преступления с использованием интернет-технологий.

В век информационных технологий почти каждый обладает элементарными навыками работы с компьютерной техникой, поэтому представляется, что круг лиц, которые совершают преступления в сфере компьютерной информации, довольно широк.

Для совершения рассматриваемого преступления недостаточно наличия поверхностных знаний о работе компьютерного оборудования, поэтому преступники, совершающие мошенни-

чество в сфере компьютерной информации, характеризуются, прежде всего, наличием профессиональных навыков в области работы компьютерной техники и программирования. Таким образом, классификация компьютерных мошенников осуществляется в зависимости от уровня знания, владения и умения пользоваться программным обеспечением и технически сложными устройствами, в частности компьютерно-техническими средствами:

- профессиональные субъекты преступной деятельности, имеющие специализированное образование («хакеры»);
- непрофессиональные субъекты преступной деятельности («самоучки») или лица, имеющие доступ к компьютерным системам в силу профессиональной деятельности (секретарь, бухгалтер и др.)

Кроме того, образовательный уровень преступников всецело влияет на выбор способа совершения мошенничества в сфере компьютерной информации.

Гендерная принадлежность преступника и его возраст зависят от вида совершаемого преступления. Так, рассматриваемое преступное деяние – мошенничество с применением информационных технологий – можно охарактеризовать как «мужское» преступление. Доля преступников мужского пола достигает 90%. Оставшиеся 10% преступников рассматриваемой категории – женщины. Возраст же преступников определяется категорией «молодой» – от 16 до 30 лет (60-70%). Что касается жертвы мошенничества, то данному виду преступления более подвержены лица женского пола в силу своей эмоциональности и активности. Здесь преобладают потерпевшие в возрасте от 45 до 58 лет (28%) (см. приложение № 2).

Кроме того, следует отметить и психологические аспекты личности компьютерного мошенника. Для него даже при наличии аналитического склада ума характерны замкнутость и скрытность, элементы фанатизма и изобретательности, нередко – болезненной компьютерной зависимости.

Таким образом, обобщенная характеристика такого преступника может быть представлена следующим образом – это молодой

человек, имеющий специальное образование или высокий уровень технических знаний, ранее не судимый, совершающий преступление в одиночку.

Одним из основных элементов криминалистической характеристики является способ совершения мошенничества в сфере компьютерной информации. Рассматривая данную преступную деятельность, можно отметить, что способ реализации преступного умысла имеет полноструктурное строение, то есть он состоит из подготовки к совершению мошенничества, реализации самого способа совершения, а также деятельности, которая направлена на сокрытие следов преступления.

Как правило, подготовка к совершению рассматриваемого преступления носит сложный характер, поскольку хищение имущества или приобретения права на имущество должно быть осуществлено специальным предусмотренным УК РФ способом: вводом, удалением, блокированием, модификацией компьютерной информации либо иным вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, то есть с использованием цифровых технологий, а это требует от преступника определенной подготовки.

Подготовительным этапом мошенничества в сфере компьютерной информации могут выступать методы аудиовизуального и электронного перехвата информации. Полученная таким образом информация позволит получить, например, пароли, коды доступа, номера счетов, механизм проведения банковских операций. Кроме сложных подготовительных информационных действий, подготовка может заключаться в подборе необходимого оборудования, орудий и средств совершения преступления, выборе доступного способа посягательства, объекта посягательства и др.

Необходимо отметить, что уже на первоначальном этапе, а именно при непосредственной подготовке к совершению преступления, продумывается и стадия сокрытия следов преступления. Так, например, хищение имущества может быть осуществлено путем создания вредоносных программ, которые позволяют проникать в компьютер жертвы без информирования её об этом либо

после хищения происходит автоматическое удаление используемой программы.

Стадия выполнения действий, направленных на достижение преступной цели, отличается большим разнообразием применяемых способов. Однако привести их исчерпывающий перечень не представляется возможным. На сегодняшний день наиболее распространенными из них признаются:

- незаконное получение регистрационных данных, позволяющих получить доступ к имуществу;
- создание сайтов с размещением на них ложной информации с целью ввести в заблуждение потенциальную жертву о возможности получения сверхкрупных прибылей;
- хищение денежных средств путем взлома электронных кошельков;
- рассылка писем-оферт об инвестировании бизнеса посредством пополнения счетов денежными средствами;
- рассылка спам-писем на электронную почту, в которых содержатся вредоносные программы;
- получение денег через виртуальные интернет-магазины;
- организация благотворительных акций через сеть Интернет;
- хищение посредством вредоносного программного обеспечения либо сайтов-двойников номеров пластиковых карт жертв[1].

В качестве примера приведем способ, связанный с хищениями денежных средств со счетов компаний. Гр. К. вступил в преступный сговор с гр. Л., который работал менеджером по работе с корпоративными клиентами ЗАО «РТК», предоставляющей услуги мобильной связи. К. предоставлял Л. сведения на предполагаемых абонентов для заключения с ними абонентских договоров. В свою очередь Л. заключал с клиентами абонентские договоры, осуществлял регистрацию и активацию сим-карт с тарифным планом, предусматривающим кредитный лимит 3000 рублей, и передавал активированные сим-карты К. После этого К. при помощи сотового телефона путем отправки СМС осуществлял перевод денежных средств с активированных сим-карт на платные

[1] Коломинов В.В. О способе совершения мошенничества в сфере компьютерной информации // Человек: преступление и наказание. 2015. № 3 (90). С. 145-149.

короткие номера, указанные на сайте «VK.com» в сети Интернет, которыми в дальнейшем распоряжался по своему усмотрению[1]. Очевидно, что с развитием информационно-телекоммуникационных технологий будут появляться новые способы мошенничества, а существующие – совершенствоваться, поэтому целесообразно вести речь только об их типологии.

Обстановка совершения преступления способствует уяснению механизма совершения преступления. На обстоятельства подготовки, совершения и сокрытия мошенничества с использованием цифровых технологий огромное влияние оказывает деятельность потерпевшей стороны. Так, нарушение правил работы с компьютерной информацией, пренебрежение правилами ее защиты, слабый контроль над использованием компьютерной информации или полное его отсутствие могут способствовать совершению мошенничества в рассматриваемой сфере.

Мотивом совершения мошенничества с использованием цифровых технологий, как и в любом преступлении против собственности, являются корыстные побуждения, цель – противоправное обогащение.

Следует помнить, что в соответствии с ч. 2 ст. 9 УК РФ временем совершения преступления признается время совершения общественно опасного деяния (т. е. его окончания) независимо от времени наступления последствий.

Как правило, мошенничество в сфере компьютерной информации относится к длящимся видам преступлений, поэтому время определяется различными по продолжительности периодами, связанными с противоправной деятельностью. Время совершения мошенничества в сфере компьютерной информации не всегда устанавливается с точностью до дня и тем более – до часов и минут. Обычно это удается, когда момент подключения / отключения фиксируется в системных журналах, в протоколах соединений, на сервере тарификации и т. п.

Значительное место в криминалистической характеристике рассматриваемого преступления занимает механизм следообразования.

---

[1] Архив Озерского городского суда Московской области, уголовное дело № 1-523/2013. URL // https://rospravosudie.com.

В современном информационном обществе все чаще для совершения преступлений используются информационно-телекоммуникационные технологии. В 2020 году число так называемых киберпреступлений выросло на 94,6%, в том числе тяжких и особо тяжких – на 129,7%[1]. Эта тенденция в совокупности с ежегодным увеличением количества электронных носителей, ростом их доступности для населения, появлением новых изобретений в данной сфере требует разработки эффективных методов исследования цифровых следов и их носителей в криминалистике.

Некоторые авторы, в частности В.Б. Вехов[2] и А.Н. Яковлев[3], предлагают для криминалистического обеспечения расследования преступлений, совершаемых с использованием компьютерных средств и систем, создать новую науку – «цифровую криминалистику». Е.Р. Россинская, в свою очередь, считает, что криминалистика едина, имеет свой предмет, систему, задачи, объекты и изучаемые закономерности. Развитие криминалистики происходит за счет изучения новых закономерностей, новых механизмов следообразования, новых технологий собирания (выявления, фиксации, изъятия), исследования, оценки и использования криминалистически значимой информации. Следовательно, нет оснований и необходимости создавать новую науку[4]. Мы поддерживаем данную точку зрения.

Думается, что «цифровую криминалистику» следует определять как отрасль криминалистики, которая направлена на изуче-

---

[1] В 2020 году число киберпреступлений в России выросло на 94,6%. URL: https://rg.ru/2020/08/19/mvd-v-2020-godu-chislo-kiberprestuplenij-v-rossii-vyroslo-na-946.html (дата обращения: 08.01.2022).

[2] Вехов В.Б. «Электронная криминалистика»: понятие и система // Криминалистика: актуальные вопросы теории и практики: сб. тр. участников Междунар. науч.-практ. конф. (Ростов на-Дону, 25.05.2017). Ростов на-Дону: Ростов. юрид. ин-т МВД России, 2017. С. 40-46.

[3] Яковлев А.Н. Цифровая криминалистика и ее значение для расследования преступлений в современном информационном обществе // Совершенствование следственной деятельности в условиях информатизации: сб. материалов Междунар. науч.- практ. конф. (Минск, 12-13 апр. 2018 г.). Минск, 2018. С. 357-362.

[4] Россинская Е.Р. К вопросу об инновационном развитии криминалистической науки в эпоху цифровизации // Юридический вестник Самарского университета. 2019. № 4. С. 144-151.

ние, обнаружение, фиксацию, а также дальнейшее использование в раскрытии и расследовании преступлений цифровых следов, которые образуются в ходе совершения преступлений в «виртуальном мире»[1]. Под цифровым следом понимается след, оставляемый в различных информационных базах данных средствами мобильной связи, кредитными, дисконтными картами, проездными документами, снабженными магнитным кодом, персональными компьютерами, подключенными к сети Интернет, электронными товарными бирками, специальными чипами и другими подобными устройствами[2]. Цифровые (виртуальные[3]) следы необходимо отграничивать от иных следов в криминалистике. Так, виртуальный след не имеет цвета, запаха, определенной геометрической формы – всего того, что позволяло традиционно выявить некоторые черты преступника, включающие в себя ДНК, особый запах или папиллярный узор[4].

Устройствами, которые могут использоваться для установления обстоятельств преступления, поиска преступника, содержащими цифровые следы преступления, могут быть: мобильные телефоны и смартфоны; стационарные компьютеры, ноутбуки, планшеты, смарт-часы, иные электронные гаджеты; элементы коммуникационных систем и операторов, оказывающих услуги связи. Как показывает следственная практика, наибольшее количество криминалистически значимой информации можно получить из мобильных телефонов и смартфонов преступника или потерпевшего. В первую очередь это СМС, мессенджеры (WhatsApp, Viber, Telegram), социальные сети (ВКонтакте, Instagram, Facebook, TikTok), а также история звонков. В совокупности с изучением

[1] Русанова Д.Ю. Цифровая криминалистика: возможности и перспективы развития // Международный журнал гуманитарных и естественных наук. 2019. № 12-4 (39). С. 142-145.

[2] Ищенко Е.П. Криминалистика: главные направления развития // Уголовно-процессуальные и криминалистические чтения: материалы междунар. науч.-практ. интернет-конф. (Иркутск, 16-30 апр. 2012 г.). Иркутск: Изд-во БГУЭП, 2012. С. 201-209.

[3] По своему сущностному содержанию цифровые и виртуальные следы в литературе рассматриваются как синонимы.

[4] Поляков В.В. Средства совершения компьютерных преступлений // Доклады Томского государственного университета систем управления и радиоэлектроники. 2014. № 2. С. 162-166.

дополнительной информации от операторов сотовой связи о зарегистрированных телефонных номерах и детализации телефонных звонков это позволит выявить лиц, связанных с преступлением, а также хронологию событий в целом.

К сожалению, в настоящее время криминалистическое обеспечение расследования преступлений не успевает за развитием цифровых технологий. В первую очередь это влияет на эффективность проводимых следственных действий в тех случаях, когда сотрудники правоохранительных органов сталкиваются с цифровыми следами. Задачу их фиксации осложняет нематериальная природа таких следов. Во избежание их уничтожения, повреждения и изменения следует прибегать к помощи специалиста, имеющего необходимые знания и материально-техническое оснащение.

Для корректной фиксации цифровых следов, получения и исследования содержащейся в них информации и упрощения поиска лиц, совершивших преступления, в том числе и на месте происшествия, разработаны специализированные программы. На данный момент для этих целей часто используют UFED[1]. Функции программы включают извлечение, восстановление и декодирование информации с различных устройств: мобильных телефонов и смартфонов, GPS-навигаторов, карт памяти и некоторых других. С помощью UFED могут быть обнаружены и зафиксированы такие цифровые следы, как сообщения голосовой почты, фотографии и их геолокация, тексты СМС и т. д. Однако наиболее важные возможности – дешифровка информации из мессенджеров (WhatsApp, Viber, Telegram) и извлечение данных из облачных хранилищ.

Еще одна не так давно появившаяся программа с большим спектром функций – «Мобильный криминалист». Разработчики заявляют, что с ее помощью можно анализировать полученную информацию. Информационно-аналитический комплекс позволяет определить часто посещаемые места конкретного лица или места пересечения группы лиц, верный хронологический порядок

[1] Рогова И.А., Бурцева Е.В. Практика применения UFED – универсального устройства для криминалистического исследования мобильных устройств // Евразийский союз ученых. 2015. № 7 (16). С. 97-100.

событий, а также связь между владельцами устройств и их контактами, частыми звонками и т. д. Считается, что этот программный продукт позволит экспертам-криминалистам еще более эффективно работать с данными.

Несмотря на наличие программ, позволяющих обнаружить цифровые следы, практика их использования при расследовании преступлений оставляет желать лучшего. Это связано, во-первых, с неосведомленностью большинства сотрудников правоохранительных органов о данных продуктах и их функционале, во-вторых, с нехваткой специалистов, имеющих необходимые знания для работы с указанными программами.

В связи с этим необходимо повышение квалификации экспертов-криминалистов, совершенствование их профессиональных навыков при работе с программным обеспечением, компьютерной техникой, устройствами связи, информационным пространством и со следами, возникающими в связи с этим, а также осведомленности у сотрудников правоохранительных органов о программных продуктах цифровой криминалистики. Кроме этого, следует разработать методические рекомендации по обнаружению, изъятию и фиксации цифровых следов. Это будет способствовать получению необходимых для расследования преступлений данных, которые могут иметь решающее значение в доказывании виновности лица либо, наоборот, явно показывать непричастность подозреваемого к совершению преступления.

Таким образом, проблемы, связанные с обнаружением, изъятием и фиксацией цифровых следов, в целях повышения эффективности процесса раскрытия и расследования преступлений требуют особого внимания и своевременного решения. Только в этом случае борьба с преступлениями, связанными с информационно-телекоммуникационными технологиями, может быть максимально эффективной.

Типичными следами по делам о мошенничестве в сфере компьютерной информации будут являться:

- традиционные следы: следы человека в местах нахождения конкретного лица в момент совершения преступления (следы пальцев рук на клавиатуре и других компьютерно-технических

устройствах и т. д.), различные документы, в том числе изготовленные с помощью средств компьютерной техники, предметы и пр.;

- «компьютерные» следы, которые при любых действиях с компьютером или иными программируемыми устройствами получают свое отображение в электронной памяти;

- идеальные следы, т. е. данные, сохранившиеся в памяти участников и очевидцев события.

К «компьютерным» следам относятся:

- следы, характеризующие результаты воздействий на компьютерную систему путем уничтожения, блокирования, модификации, копирования компьютерной информации, нейтрализации средств защиты компьютерной информации. Их местонахождение сходно со следами в компьютерной системе нарушителя (следами на орудии преступления);

- следы на иных компьютерных средствах, характеризующие подготовку к совершению преступления, т.е. содержащие криминалистически значимую информацию в компьютерах, мобильных телефонах, цифровых фотоаппаратах, видеокамерах и диктофонах, смарт-картах и пр.

Можно отметить, что специфика образования цифровых следов тесно взаимосвязана с другими элементами криминалистической характеристики, а именно с таким элементом, как место совершения мошенничества с использованием цифровых технологий.

Отличительным свойством места совершения мошенничества в сфере компьютерной информации выступает удаленность нередко на значительные расстояния места совершения общественно опасных деяний от места возникновения последствий. В связи с этим местом совершения мошенничества в сфере компьютерной информации считается как сама информационно-телекоммуникационная сеть, в которой происходит удаление, блокирование, модификация компьютерной информации, так и место нахождения конкретного компьютера, с помощью которого выполняется объективная сторона преступления. Данным принципом руководствуются при определении территориальной подследственности в соответствии со ст. 152 УПК РФ.

В отличие от места совершения преступления место происшествия характеризуется наличием следовой картины, оставленной в результате преступления. Местом происшествия при расследовании мошенничества в сфере компьютерной информации могут быть признаны:

- место реализации преступного умысла (т. е. где осуществлялся доступ в компьютерную сеть, вводились команды и информация, создавались вредоносные компьютерные программы и т. п.);
- место нахождения средств хранения, обработки или передачи компьютерной информации, вмешательство в функционирование которых повлекло причинение вреда;
- место, где наступили вредные последствия;
- иные места (место расположения транзитных носителей и др.).

Перечисленные места могут совпадать в любой комбинации, но могут и различаться. Следовательно, мест происшествия для мошенничества в сфере компьютерной информации может быть несколько, в том числе значительно удаленных друг от друга и расположенных не только в разных помещениях, но и в разных населенных пунктах и даже за рубежом. Последнее возможно в связи с широким использованием информационно-телекоммуникационных сетей и в первую очередь сети Интернет.

Интернет-технологии в современном мире безудержно развиваются, заполняя жизнь людей, тем самым создавая специфику к совершению преступлений с их использованием. Трудность состоит в том, что все это происходит виртуально, отсутствует тактильная связь, то есть человек не может потрогать, пощупать какую-либо вещь. Даже осознавая, что преступления совершаются с помощью интернет-технологий, с применением различных устройств, разобраться, как все устроено и работает, зачастую бывает сложно.

В Российской Федерации такая ситуация связана с информатизацией общества, возможностью доступа граждан к информации, связанной с работой тех или иных органов государственной власти, а также подачей электронных документов дистанционно, особенно это стало актуально в связи с распространением коронавирусной инфекции.

Безусловно, использование интернет-технологий во многом упрощает жизнь, но, к сожалению, создается «пространство» для совершения преступлений.

Существующая государственная программа «Информационное общество», которая действует до 2024 года, направлена на обеспечение высокой степени интеграции Российской Федерации в мировое информационное общество; предупреждение информационной изолированности отдельных граждан и социальных групп; достижение такого уровня развития технологий защиты информации, который обеспечивает неприкосновенность частной жизни, личной и семейной тайны, безопасность информации ограниченного доступа.

Интересны статистические данные по преступлениям с использованием интернет-технологий за 2020 год в России. Так, наблюдается, что их число по сравнению с 2019 годом выросло на 94,6%, многие из них относятся к категории особо тяжких (см. приложение № 1).

Сложившаяся на сегодняшний день ситуация, а в особенности методика расследования хищений с использованием интернет-технологий вызывает интерес.

Таким образом, криминалистическая характеристика мошенничества с использованием цифровых технологий, являющаяся подсистемой частной криминалистической методики расследования преступлений, представляет собой систему криминалистически значимой информации о типичных его признаках, в структуру которой включены данные о способе совершения преступления, предмете преступного посягательства, личности преступника, механизме следообразования и обстановке совершения преступления. Знание содержания указанных элементов имеет большое значение для правильной организации расследования мошенничества с использованием цифровых технологий, а также формирования обоснованных следственных версий о расследуемом событии в целом и отдельных его обстоятельствах.

Такое преступление, как вымогательство, как и любое криминальное деяние, обладает определенными признаками и качествами, которое позволяет отграничить его от иных противо-

правных явлений. В предыдущем параграфе мы уже установили, что рассматриваемое деяние имеет давнюю историю. Подобное деяние в своей первоначальной итерации рассматривалось как вид должностного преступления, а не посягательство на чью-то собственность. В рамках данного толкования под вымогательством понимались действия чиновника, направленные на получение взятки путем шантажа или иных угроз. На сегодняшний день толкование вымогательства достаточно объемно, что подтверждается диспозицией действующей нормы, предусмотренной ст. 163 УК РФ. Ранее мы уже приводили содержание данной нормы. Особый интерес для нас, однако, представляет вопрос о способах совершения вымогательства, поскольку современный научно-технический прогресс обуславливает появление новых приемов и методов криминальной деятельности. При этом перечень подобных способов вымогательства год от года становится все шире. Поэтому именно способ совершения вымогательства мы выделим в дальнейшем в качестве основного признака для раскрытия характеристики его как преступления, на котором оставило свой отпечаток интенсивное развитие информационно-телекоммуникационных технологий.

Изучение способов совершения вымогательства необходимо не только для теоретической разработки положений криминалистической науки, но и имеет практическое значение для организации раскрытия и предварительного расследования таких преступлений, заставляет правоприменителя идти в ногу со временем и не отставать от технически оснащенных и квалифицированных преступников-вымогателей.

Нами ранее было отмечено, что вымогательства – достаточно сложно раскрываемые и высоколатентные преступления. Это можно объяснить появившимися в последние годы новыми способами совершения указанных преступлений, в том числе с использованием сети Интернет.

К классическим способам совершения вымогательств следует отнести требование об оплате услуг, стоимость которых несоразмерна их содержанию. Например, оказание консультаций за реализацию товара или оказания охранных услуг. Нередко вымо-

гательства такого рода совершаются с помощью посредников – представителей организованных преступных групп. В последнее десятилетие подобные способы мошенничества все менее актуальны и встречаются только в криминальной деятельности этнических преступных группировок в отношении выходцев из тех же стран ближнего зарубежья. Ранее вымогательство также вуалировалось под видом сделки о купле-продаже товара по нерыночной завышенной цене. Директора коммерческих предприятий были вынуждены соглашаться, выплачивая вымогателям на постоянной основе денежные средства и закладывая данные «издержки» в стоимость своих товаров и услуг. С позиций предпринимателя риск от реализации угрозы вымогателей в результате обращения в правоохранительные органы достаточно высок, и в связи с этим постоянные выплаты становятся предпочтительнее. Поэтому вымогательство относится к высоколатентным преступлениям.

К распространенным способам вымогательства также следует относить психологическое насилие путем непосредственной открытой угрозы жизни и здоровью потерпевшего, в том числе через демонстрацию оружия и иных орудий пыток, в том числе осуществляя соответствующие высказывания в адрес жертвы. При этом в случае неисполнения требований вымогателей угрозы претворяются в жизнь как в отношении потерпевшего, так и в отношении его близких родственников.

К более современным способам совершения вымогательства относится угроза разглашения коммерческой тайны или данных о доходе, полученных противоправным путем, об уклонении от уплаты налогов и т. д. При этом потерпевшие зачастую бывают действительно причастны к совершению аморальных или противоправных деяний.

Возвращаясь к основной теме нашего исследования, отметим необходимость подробного рассмотрения вымогательства с использованием сети Интернет. На сегодняшний день данный способ совершения вымогательства наиболее распространен.

Так, например, И.В. Третьяк полагает, что современная преступность все чаще использует новые способы осуществления своей деятельности с целью уйти от уголовной ответственности.

Поэтому в последнее десятилетие так остро встает вопрос киберпреступности[1]. При этом законодателем подобный способ в описании соответствующего состава преступления никак не учитывается.

Отдельные авторы также отмечают, что общественная опасность вымогательства с использованием сети Интернет представляет собой гораздо большую общественную опасность по сравнению с традиционными способами совершения преступления. Это обусловлено тем, что коммуникационный уровень технологий позволяет в короткие сроки создавать сплоченные преступные группы и согласовывать действия, не прибегая к серьезным усилиям. Кроме этого, отмечается, что правоохранительные органы с отставанием реагируют на появление современных цифровых способов вымогательства, что также влияет и на раскрываемость данных преступлений[2].

Отметим, что на современном этапе использование сети Интернет для вымогательства становится более предпочтительным в связи с отсутствием визуального контакта с вымогателем, что усложняет его дальнейшее установление личности. К преимуществам данного способа также относится его дистанционный характер, который позволяет совершать преступление, находясь в тысячах километрах от потерпевшего, что в целом, естественно, препятствует объективному и всестороннему расследованию данных преступлений.

Достаточно часто для реализации своего преступного замысла, направленного на вымогательство в сети Интернет, злоумышленники предварительно создают вредоносное программное обеспечение (компьютерные вирусы), которые приводят к блокированию информации, находящейся на устройстве потерпевшего, требуя в дальнейшем за разблокировку денежные средства. Подобное вредоносное программное обеспечение может быть распространено через специальные интернет-браузеры при просмотре определенных сайтов или же может быть случайно скачано

[1] Третьяк И.В. Новые виды вымогательства в сети Интернет // Вестник наук. 2018. № 7 (7). С. 95-100.

[2] Сафронов А.Ю. Об особенностях способов совершения и тактики раскрытия вымогательства // E-SCIO. 2020. № 3 (42). С. 348-354.

вместе с нелицензионным программным обеспечением, предназначенным для личного использования потерпевшим.

Так, наиболее популярной у вымогателей вирусной программой является Trojan Archiveus, основной функционал которой заключается в блокировании отдельных файловых папок пользователя, с последующем истребованием пароля доступа и предоставлением его за отдельную плату на реквизиты счета злоумышленника.

Следующей не менее популярной программой выступает Ransom A, которая автоматически в определенный период времени может удалять отдельные файлы пользователя в случае невнесения денежных средств на счет вымогателя.

В качестве более изощренных способов интернет-вымогательства также следует выделить способ путем распространения программы Trojan-Ransom.Win32, которая якобы предоставляет пользователю бесплатный полный доступ к учетным записям пользователей социальных сетей. В этих целях, запуская скачанный файл программы «взломщика аккаунтов», на компьютер пользователя устанавливается вредоносное ПО, которое запускает экран с просьбой отправить платное СМС для получения доступа к учетной записи любого пользователя соцсети. После этого скачивается дополнительная программа в архиве VK-Hack.zip, которая при запуске также требует внесение дополнительных денежных средств. В результате неоднократно повторенных таким образом манипуляций потерпевший может передать злоумышленнику значительную итоговую сумму[1].

К не менее популярным способам интернет-вымогательства также можно отнести неправомерный доступ к личной учетной записи пользователя соцсети с последующим получением полной информации о пользователе, включая имеющиеся фото- и видеоизображения, содержание личных электронных сообщений, данные других пользователей и т. д. Получив доступ к аккаунту потерпевшего, вымогатель, используя одноразовую учетную запись, вступает с жертвой в переписку, сообщая ей, что учетная запись взломана и в случае неисполнения требований все данные будут

[1] Столбова Н.А. Криминалистическая характеристика основных способов вымогательства на современном этапе // Научный дайджест Восточно-Сибирского института МВД России. 2020. № 4 (7). С. 110-114.

размещены в открытом доступе. Как правило, информация, содержащаяся в учетной записи потерпевшего, носит компрометирующий характер. В случае если вымогатель будет заблокирован пользователем или будет сообщено администрации соцсети о факте вымогательства, то данные учетной записи автоматически размещаются в общем доступе и таким образом распространяются. Чаще всего к подобному способу вымогательства прибегают лица, ранее состоявшие в романтических отношениях с потерпевшим и достоверно осведомленные о наличии в файлах жертвы материалов личного характера, способных опозорить потерпевшего.

К смежным способам подобного интернет-вымогательства следует отнести использование злоумышленниками сайтов знакомств. Так, злоумышленник вступает с потерпевшим с заочную переписку, в ходе которой возможен обмен интимными фото- и видеоизображениями. В результате полученные изображения становятся предметом шантажа, а в случае невыполнения требований могут быть публично обнародованы в любых ресурсах сети Интернет с последующим распространением таких изображений среди друзей и родственников жертвы.

Оба рассмотренных вышеуказанных случая относятся к относительно новому виду интернет-вымогательства, которое в последнее время набирает активные обороты. Далее поговорим о нем подробнее.

Так называемое «порно-вымогательство» посредством электронных отправлений известно с 2018 года, однако в 2021 году действия злоумышленников стали изощрённее.

Рассматриваемый вид общественно опасного деяния получил распространение в зарубежных государствах и охватывается англоязычным термином – «sextortion», который в буквальном смысле интерпретируется как шантаж, связанный с разоблачениями из чьей-то личной половой жизни[1].

«Sextortion» – представляет собой алгоритм преступных действий по рассылке на электронную почту жертвы информационных писем с целью принудительного изъятия имущества последней под предлогом распространения позорящих сведений.

[1] Cambridge English Pronouncing Dictionary, Cambridge University Press, 2011. 580 page.

Чтобы обезопасить себя, преступники предлагают жертве суммы так называемого «выкупа» перечислить на криптокошелек, ранее преобразовав в финансовые цифровые активы.

В соответствии с национальным уголовным законодательством «Sextortion» квалифицируется в соответствии с нормами ст. 163 УК РФ, 272 УК РФ, 138 УК РФ.

С учетом диспозиций статей 146 и 151 УПК РФ, положений Федерального закона «О порядке рассмотрения обращений граждан Российской Федерации» № 59-ФЗ решение о возбуждении уголовного дела по соответствующим заявлениям правомочен принимать следователь СК России.

Верховный Суд Российской Федерации разъясняет, что угроза, которой сопровождается требование при вымогательстве, должна восприниматься потерпевшим как реальная, однако не приводит примеров, когда угроза может восприниматься таковой, и не указывает критерии реальности[1]. В связи с этим возможен отказ в возбуждении уголовного дела и непризнание судами «порно-вымогательств» преступлениями. Потерпевшие воспринимают «порно-вымогательство» в качестве реальной угрозы, тогда как сотрудники правоохранительных органов на практике соглашаются с этим только тогда, когда угроза подкрепляется фактическим компроматом, т.е. порнографическими фото/видео.

Способ совершения: полноструктурный, т. е. подразумевает действия по приготовлению, реализации преступного умысла, сокрытию преступления.

Подготовка к совершению рассматриваемого вида преступления предполагает наличие специальных компьютерных навыков, необходимых для получения *несанкционированного доступа* к почтовым аккаунтам предполагаемых потерпевших путем незаконного приобретения, получения охраняемых законом персональных данных пользователей, в том числе паролей, логинов, почтовых серверов.

Так, согласно приказу Минтруда России № 348н «Об обработке персональных данных в Министерстве труда и социальной защи-

[1] О судебной практике по делам о вымогательстве (статья 163 Уголовного кодекса Российской Федерации): постановление Пленума Верховного Суда Российской Федерации от 17.12.2015 № 56 // Российская газета. 2015. 28 декабря.

ты Российской Федерации»[1], адрес электронной почты отнесен к персональным данным.

А суды отказывают в удовлетворении ходатайств об истребовании логина и пароля электронного почтового ящика, обосновывая выводы наличием в переписке персональных данных как владельца почты, так и третьих лиц[2].

Если злоумышленник не знаком с потенциальной жертвой «порно-вымогательства», а умысел направлен на случайных пользователей почтовых сервисов, выбранных случайно, то используются базы данных держателей почтовых ящиков, украденные и незаконным образом размещенные на информационных ресурсах в том числе и в «теневом» сегменте сети Интернет.

Так, одна из массовых «утечек» паролей почтовых серверов «Yandex» (к аккаунту на Яндексе могут быть привязаны электронные кошельки) и «Mail.ru» произошла в сентябре 2014 года, а в июле 2018 года поисковые системы предоставляли данные и пароли пользователей, хранящиеся в «Google Cloud».

Так, «О» в феврале 2015 года, имея умысел, направленный на неправомерный доступ к охраняемой законом компьютерной информации, используя находящуюся по адресу: <адрес> компьютерную технику – ПК с установленным жестким диском «Western Digital», серийный номер №..., в ходе электронной переписки с помощью электронной компьютерной программы QIP, используя учетную запись в данной программе №..., вступил в предварительный преступный сговор с неустановленным следствием лицом, находящимся в неустановленном следствием месте, осуществляющим электронную переписку с помощью электронной компьютерной программы QIP с учетной записью №..., на совер-

---

[1] Об обработке персональных данных в Министерстве труда и социальной защиты Российской Федерации (вместе с «Правилами обработки персональных данных в Министерстве труда и социальной защиты Российской Федерации»): приказ Минтруда России от 29.05.2014 № 348н (Зарегистрировано в Минюсте России 01.09.2014 № 33914) // Российская газета. 2014. 26 декабря.

[2] Постановления арбитражного суда Северо-Кавказского округа по делам об обжаловании определений об отказе в истребовании доказательств в виде данных логина и пароля почтовых ящиков должника по делу о банкротстве (от 16.08.2019 по делу № А53-23516/2017, от 15.07.2019 по делу № А53-23514/2017.

шение неправомерного доступа к охраняемой законом компьютерной информации – а именно, информации о пароле <данные изъяты>, соответствующему электронному почтовому ящику <данные изъяты>, принадлежащему законному владельцу, хранящейся на компьютерах пользователей <данные изъяты>, преследуя цель дальнейшего использования логинов и паролей к электронным почтовым ящикам <данные изъяты>, <данные изъяты>[1].

Реализация преступного умысла. Направление непосредственно электронного сообщения, в тексте которого содержатся сведения об осведомленности злоумышленника о «позорящих» потенциального потерпевшего действиях, событиях, а также форме и размере имущества, способе его передаче, для целей непридания гласности компрометирующей информации.

В соответствии с постановлением Пленума Верховного Суда РФ от 17.12.2015 № 56, касающемся судебной практики по делам о вымогательстве, под позорящими данными следует понимать сведения, порочащие честь, достоинство или подрывающие репутацию лица или его близких (фото/видео изображения аморального поступка, в том числе информации о приватном посещении «порно-контента»). При этом значения не имеет, соответствуют ли действительности сведения, под угрозой распространения которых совершается вымогательство.

Для придания реальности содержавшейся в электронном сообщении информации с целью формирования у жертвы «порно-вымогательства» подлинного представления о возможности распространения компрометирующей ее информации о пользовании «порно-контентом», злоумышленник детально расписывает где, как и каким образом получил так называемый «компромат», путь его возможного распространения, а также способ передачи имущества жертвы в обмен на «сохранение личной тайны».

Так, злоумышленник, вводя в заблуждение, сообщает, что незаконным образом получил доступ и удаленным способом активировал Web-камеру персонального компьютера, создал видеофайл, содержащий смонтированные кадры порнографического видео, а

[1] Приговор Центрального районного суда г. Челябинска по делу № 1141/2017 (ч. 3 ст. 272 УК РФ).

также видео действий самого скомпрометированного лица в момент пребывания на порно-ресурсе.

В ряде случаях вымогатели предлагают жертвам самостоятельно убедиться в реальности угрозы распространения порочащих фото/видеофайлов, указывая электронный адрес ссылки на архив ZIP, в котором якобы содержатся компрометирующие пользователя видеоматериалы.

Однако в международной судебной практике имеются случаи привлечения к уголовной ответственности и за реальную «слежку с помощью Web-камеры ПК» и последующее «порно-вымогательство» посредством электронной почты.

Так, гражданин Кипра осужден на 4 года лишения свободы за незаконный доступ к Web-камере с целью скрытого наблюдения за жизнью несовершеннолетней девушки.

47-летний компьютерщик незаконно создал и применил вредоносную компьютерную программу для получения удаленного контроля над Web-камерой жертвы. Персональный компьютер потерпевшей был «инфицирован» после того, как девушка открыла вложение из незнакомого письма, пришедшего на ее электронную почту.

Преступник, угрожая отправить незаконным образом тайно сделанные приватные снимки друзьям жертвы, принуждал последнюю позировать обнаженной перед веб-камерой[1].

Однако в большинстве случаев у «порно-вымогателя» нет доступа к Web-камере персонального компьютера адресата.

Для введения в заблуждение, создания ложного представления о реальности угроз злоумышленник использует адрес электронной почты жертвы в качестве адреса отправителя письма. Т. е. фактически жертва направила письмо с угрозами «сама себе».

С целью придания угрозе огласки большей убедительности злоумышленники в ряде случаев приводят в тексте сообщений пароли почтовых ящиков жертв, полученные посредством различных утечек данных.

Следует отметить, что электронное письмо по протоколу SMTP (Simple Mail Transfer Protocol – простой протокол пере-

[1] Хакер получил 4 года тюрьмы за взлом веб-камеры. URL: https://www.securitylab.ru/news/356788.php (дата обращения: 02.10.2022)

дачи почты) – общедоступный сетевой протокол, предназначенный для отправления электронной почты в сетях TCP/IP.) состоит из так называемого «конверта», «заголовков» и «содержания» письма. Информация о получателе (MAIL FROM) и отправителе (RCPT TO) размещена в «конверте», а также показывается в заголовках.

При помощи ввода стандартных команд протокола вымогатель имеет возможность внести изменения в адрес отправителя письма (RCPT TO) в заголовке и даже поменять обратный адрес. В этом случае в качестве обратного адреса письма будет транслироваться почта получателя, у которого, в свою очередь, формируется ложное понимание реальности угрозы злоумышленника о возможности распространения компрометирующих его информации и медиафайлов.

Сокрытие. Чтобы обезопасить себя, преступники предлагают жертве суммы так называемого «выкупа» перечислить на криптокошелек, ранее преобразовав в финансовые цифровые активы.

Ранее, до 2017 года, вымогательство в криптовалюте по национальному законодательству не квалифицировалось в соответствии с нормами уголовного закона.

Однако судебная практика пошла по пути так называемой «легализации» цифровых финансовых активов, приравнивая их к категории иного имущества, ссылаясь на нормы Гражданского кодекса РФ.

Так, в определении Верховного суда Республики Башкортостан от 20.02.2017 № 33-3487/2017 суд указал, что «виртуальная валюта», ... является не средством платежа за товар, а непосредственно товаром»[1].

В Постановлении 9 Арбитражного Апелляционного суда от 15.05.2018 № 09АП-16416/2018 по делу № А40-124668/2017, по мнению суда, криптовалюта не может быть расценена применительно к ст. 128 ГК РФ иначе как иное имущество[2].

---

[1] Определение Верховного суда Республики Башкортостан от 20.02.2017 № 33-3487/2017. Режим доступа: http://vs.bkr.sudrf.ru/ (дата обращения 16.10.22).

[2] Постановление 9 Арбитражного Апеляционного суда от 15.05.2018 № 09АП-16416/2018. Режим доступа: https://9aas.arbitr.ru/ (дата обращения: 16.10.22).

По мнению Председателя Следственного комитета Российской Федерации – «... признание финансовых цифровых активов (криптовалюты) в качестве имущества для целей уголовного и уголовно-процессуального законодательства является необходимым условием расследования уголовных дел, по которым цифровая валюта выступает, например, предметом взятки или хищения»[1].

Таким образом, в исследовании нашло отражение способа совершения «порно-вымогательства» («sextortion») – базового элемента криминалистической характеристики, детальный анализ которого необходим для практики расследования рассматриваемой категории преступления.

Подводя итог проведенному в данном параграфе исследованию общей характеристики вымогательства с использованием сети Интернет, следует отметить о все большем его распространении. Такое положение обусловлено отсутствием действенной методики раскрытия и расследования подобных преступлений, что влечет за собой безнаказанность вымогателей.

Однако, несмотря на небольшой объем вымогательства в общей структуре преступлений против собственности, данный вид преступности имеет потенциальную способность причинить существенный вред охраняемым интересам государства. Это обусловлено как латентным характером данного вида преступности, так и совершенствующимися способами совершения вымогательств. Для эффективного противодействия вымогательствам, совершаемым в интернет-пространстве, правоприменителю необходимо обладать специальными познаниями в сфере современных информационных технологий и умело применять их на практике. В частности, любому следователю и дознавателю необходимо четко знать механизм совершения подобных преступлений, понимать те способы, которые используются преступниками. В свою очередь наука также должна идти в ногу со временем и разрабатывать современные эффективные методики раскрытия и расследования подобных преступлений для их непосредственого применения правоохранительными органами.

---

[1] Интервью А.И. Бастрыкина от 08.12.20. Режим доступа: https://ria.ru/20201208/kriptovalyuta-1588242025.html (дата обращения: 16.10.2022).

ГЛАВА 2. ОРГАНИЗАЦИОННО-ТАКТИЧЕСКИЕ ОСОБЕННОСТИ РАССЛЕДОВАНИЯ МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ ЦИФРОВЫХ ТЕХНОЛОГИЙ

§ 1. Особенности возбуждения уголовного дела и обстоятельства, подлежащие установлению по делам о мошенничествах, совершенных с использованием цифровых технологий

Стадия возбуждения уголовного дела по признакам состава преступления, предусмотренного ст. 159.6 УК РФ и иным уголовно-правовым нормам, предусматривающим мошенничество с использованием цифровых технологий, обладает определенной спецификой, связанной, прежде всего, с проведением предварительной проверки заявления или сообщения о преступлении.

В соответствии с ч. 3 ст. 20 УПК РФ в основном уголовные дела о мошенничестве, совершенном с использованием цифровых технологий, относятся к делам частно-публичного обвинения в случаях:

- если такое преступление совершено индивидуальным предпринимателем или членом органа управления коммерческой организации;

- если оно не совершено с причинением вреда интересам государственного и (или) муниципального унитарного предприятия, государственной корпорации, государственной компании, коммерческой организации с прямым участием в уставном (складочном) капитале (паевом фонде) государства и (или) муниципального образования, если к тому же предметом преступления не явилось государственное и (или) муниципальное имущество.

Для принятия решения о возбуждении такого уголовного дела требуется наличие заявления потерпевшего или его законного представителя. Если же мошенничества в сфере компьютерной информации совершены без наличия вышеперечисленных условий, то они являются делами публичного обвинения, и уголовное преследование осуществляется независимо от волеизъявления потерпевшего.

Таким образом, поводом к возбуждению уголовных дел о мошенничестве с использованием цифровых технологий могут выступать как заявление о преступлении, так и явка с повинной, сообщение о совершённом или готовящемся преступлении, полученное из иных источников, и постановление прокурора о направлении соответствующих материалов в орган предварительного расследования для решения вопроса об уголовном преследовании.

Поскольку мошенничество в сфере компьютерной информации в большинстве своем характеризуется неочевидностью, для решения вопроса о возбуждении уголовного дела необходимо проведение проверки. Для наиболее эффективной и результативной проверки заявлений и сообщений законодатель определил перечень действий, которые могут осуществляться в ходе ее проведения[1] (ст. 144 УПК РФ). Целью данной проверки является установление фактического основания для возбуждения уголовного дела, т. е. наличия признаков преступления. В этот перечень кроме процессуальных действий включен ряд следственных: осмотр места происшествия, документов, предметов, освидетельствование, изъятие образцов для сравнительного исследования, судебная экспертиза.

Выбор и объем проверочных действий зависит от ситуации, складывающейся на момент получения информации о преступлении, а также от источника поступления и ее характера. Заявить о преступлении может как физическое лицо, так и юридическое, представляющее публично-правовую организацию.

Немаловажным фактором, влияющим на порядок проверки сообщения о преступлении, выступает сложившаяся на момент по-

[1] Методика расследования отдельных видов мошенничества: учеб. пособие. Москва: МосУ МВД России, 2014. С. 41.

лучения сообщения о преступлении следственная ситуация. К основными следственным ситуациям можно отнести следующие:

- преступление не окончено, имеется взаимосвязь преступника с потерпевшим;

- преступление окончено, взаимосвязь между потерпевшим и преступником отсутствует.

Вторая ситуация наиболее сложная и в то же время наиболее распространенная.

Совершенно очевидно, что какая бы ситуация ни сложилась, определяющим и необходимым средством проверки сообщения о преступлении является получение объяснений.

Получение объяснений возможно от потерпевшего или иных лиц, являющихся очевидцами преступления. Несмотря на отсутствие доказательного значения объяснений, их получение сразу или в течение непродолжительного времени после совершения преступления благодаря свежести в памяти деталей преступного события позволят в более полном объеме собрать информацию об обстоятельствах преступления. В конечном итоге в объяснении потерпевшего должны быть отражены признаки преступления.

В целях сбора объектов, которые являются следами или их носителями, в ходе предварительной проверки по делам о мошенничестве в сфере компьютерной информации должны быть изъяты и истребованы различные документы. К ним могут относиться: документы, свидетельствующие о наличии у потерпевшего похищенного имущества, документы, свидетельствующие об оказании провайдером услуг подключения к информационно-телекоммуникационной сети, а также иные документы, которые могут содержать следы преступления.

Они могут быть изъяты как в ходе производства осмотра места происшествия, так и истребованы должностным лицом, проводящим проверку. Для возможной квалификации преступления по признакам ст. 159.6 УК РФ следует установить не только наличие факта хищения чужого имущества, но и то, что оно было похищено путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функциониро-

вание средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Для этого следует осмотреть источники хранения этой информации или же назначить компьютерную экспертизу.

Таким образом, в рамках рассмотрения сообщения о мошенничестве в сфере компьютерной информации в порядке ст. 144 УПК РФ следователю или лицу, производящему дознание, целесообразно:

получить объяснение от заявителя;

провести осмотр компьютерно-технических средств;

назначить компьютерную экспертизу;

изъять, осмотреть необходимые документы;

назначить ревизию хозяйственной деятельности юридического лица для выявления факта хищения материальных ценностей, совершенного путем исследуемого вида мошенничества;

дать поручение оперативным работникам о производстве оперативно-розыскных мероприятий, направленных на установление свидетелей, а также лиц, причастных к совершению преступления.

Необходимо отметить, что по данному виду преступления основным оперативно-розыскным мероприятием, обеспечивающим получение криминалистически значимой информации в компьютерных сетях оперативным путём, является снятие информации с технических каналов связи (СИТКС)[1].

Подводя итог вышесказанному, отметим, что полученные в ходе проверки сообщения о преступлении сведения должны отражать наличие признаков состава преступления – мошенничества с использованием цифровых технологий, предусмотренного УК РФ и в полном объеме использоваться в ходе дальнейшего расследования. Результат проведенной проверки должен найти отражение в принятом законном решении о возбуждении уголовного дела, отказе в возбуждении или передаче сообщения по подследственности.

---

[1] Осипенко А.Л., Сералинов Ж.Т. Проблемы соблюдения прав граждан при снятии информации с технических каналов связи в глобальных компьютерных сетях // Актуальные проблемы борьбы с преступностью на современном этапе: тезисы докл. и сообщ. всерос. науч.-практ. конф. Омск, 2010. С. 154-157.

В ходе расследования мошенничества в сфере компьютерной информации необходимо установить и доказать обстоятельства, определенные ст. 73 УПК РФ. К ним относятся:

- факт хищения чужого имущества или приобретения права на чужое имущество, в какой форме хищение было совершено, каким способом: путем ввода, удалениям, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей;

- место совершения преступления: место нахождения предмета преступления (компьютерной информации, на которую оказывалось воздействие); место, откуда осуществлялись ввод, удаление, блокирование, модификация компьютерной информации или иное вмешательство;

- время совершения мошеннических действий, время наступления вредных последствий, время обнаружения факта совершения преступления;

орудия преступления, то есть компьютерные и телекоммуникационные средства, системы, а также программное обеспечение, использованные для совершения мошенничества;

- субъект компьютерного мошенничества, его служебное положение, наличие судимости (если это преступная группа, то распределение ролей между ее участниками, наличие предварительного сговора организованной преступной группы); виновность и форма вины;

- характер и размер причиненного преступлением материального ущерба.

Часть перечисленных обстоятельств устанавливается на этапе проверки сообщения о преступлении, однако в рамках расследования эти обстоятельства необходимо доказать.

Формирование следственных ситуаций первоначального этапа расследования мошенничества в сфере компьютерной информации зависит от уже сформированной ситуации на момент поступления сообщения о преступлении. Таким образом, для первоначального этапа расследования компьютерного мошен-

ничества можно выделить следующие исходные следственные ситуации.

Имеется только информация о событии преступления, о способе совершения преступления и личности преступника.

Имеются сведения о событии преступления, способе его совершения, но личность преступника не установлена.

Известен факт преступления, способы его совершения и сокрытия, личность преступника и другие обстоятельства.

С учетом сложившейся следственной ситуации определяется алгоритм деятельности следователя, который должен найти свое отражение в плане проведения следственных действий и оперативно-розыскных мероприятий по уголовному делу. Ключевым звеном в организации работы следователя является программно-целевой процесс планирования расследования, который в первую очередь дисциплинирует всю работу следователя, способствует наиболее рациональному использованию времени и обязывает следователя в предусмотренные планом сроки выполнить намеченные им следственные действия и иные мероприятия.

В рамках планирования расследования определяются способы и средства решения следственных задач по уголовному делу в целом. При планировании производства следственного действия следует определить способ эффективного решения задачи при его проведении.

Процесс планирования включает в себя соблюдение принципов реальности, динамичности, индивидуальности и конкретности.

Реальность составленного плана, прежде всего, предполагает наличие баланса между запланированными мероприятиями и сроками их исполнения, т. е. нагрузка на следователя не должна превышать его реальных возможностей выполнить намеченное. В процессе расследования мошенничества в сфере компьютерной информации непрерывно поступают новые сведения, обнаруживаются ранее неизвестные обстоятельства, что предполагает необходимость изменения плана действий с учетом новых реалий и задач. Это говорит о процессе расследования как о развивающемся явлении, о его динамичности. Составление плана расследования уголовного дела требует от следователя творческого подхода

с учетом общих закономерностей и индивидуальных специфических особенностей мошенничества в сфере компьютерной информации. План должен содержать конкретные задачи, мероприятия, срок их исполнения и исполнителя.

Ввиду того, что большинство случаев мошенничества в сфере компьютерной информации обладают особой сложностью совершения, их расследование характеризуется большим объемом и трудоемкостью следственных действий. С учетом изложенного следователь должен тщательно планировать производство расследования по уголовному делу. Развернутый план расследования составляется после производства первоначальных следственных действий. К этому времени определяется круг общих следственных версий, которые требуют дальнейшей проверки.

При реализации плана расследования по уголовному делу нельзя обойтись без планирования отдельных следственных действий. К рекомендациям планирования проведения следственных действий следует отнести:

- изучение исходной информации о преступлении;
- определение задач, которые следует решить в рамках следственного действия;
- определение места и времени проведения следственного действия;
- определение круга необходимых участников, изучение их личности и обеспечение явки;
- определение тактических приемов, обеспечивающих решение поставленных задач, с учетом возможного поведения лиц, участвующих в следственном действии;
- определение и подготовка необходимых технических средств.

Сам план следственного действия зачастую составляется схематично и содержит только последовательность выполняемых следователем действий.

Приведем пример из следственной практики, наглядно демонстрирующий эффективность грамотно спланированного расследования.

Уголовное дело № 678578, в ходе расследования которого установлено, что Гасанов Р.Р. и Колонщаков А.В. совместно с неуста-

новленным пользователем сети Интернет под псевдонимом «Den Adel» («Robusto») путем подбора электронно-цифровой подписи и неправомерного доступа к аутентификационным данным агента похитили денежные средства с расчетного счета ООО «СимМетрия» в платежной системе «КиберПлат» банка «Платина» на общую сумму более 3 млн рублей. Похищенные денежные средства перечислялись соучастниками на лицевые счета абонентских номеров оператора сотовой связи ОАО «ВымпелКом» и использовались ими по своему усмотрению. Уголовно дело направлено в суд Следственным департаментом МВД России. Действия Гасанова Р.Р. и Колонщакова А.В. квалифицированы по ч. 3 ст. 159.6 УК РФ. В суде состоялся обвинительный приговор, виновные получили наказание в виде лишения свободы сроком на 2 года условно.

В ходе ежегодной коллегии МВД России в марте 2021 года Президентом Российской Федерации В.В. Путиным отмечен рост числа преступлений, совершенных в сфере информационных технологий. Обращено внимание на тот факт, что в сложившейся эпидемиологической ситуации передовые технологии играют ключевую роль в развитии государства, т.к. затрагивают все сферы жизни общества. Киберпреступления, приняв массовый характер, дестабилизируют равновесие социальных и экономических процессов.

Проведенный анализ динамики совершения преступлений в сфере телекоммуникаций и компьютерной информации на основе ведомственной отчётности (см. приложение 3) позволяет отметить наличие неблагоприятных тенденций, складывающихся в области криминализации информационного пространства сети Интернет, а также недостаточный уровень реагирования органов внутренних дел на эти тенденции.

После выявления преступления мероприятия по установлению лица являются основной задачей ОВД. Установление личности преступника даёт возможность проведения комплекса оперативно-розыскных мероприятий и следственных действий, способствующих всестороннему изучению событий произошедшего, сбора необходимой доказательной базы. Количество выявленных

преступлений с установленными лицами, несомненно, повышает вероятность направления уголовных дел в суд для рассмотрения по существу.

Так, достаточно давно в деятельности органов предварительного следствия наблюдается тенденция к возбуждению уголовных дел с установленными лицами, где не только очевиден состав преступления, но и достаточно узок круг подозреваемых лиц.

Наряду с этим имеется большая доля приостановленных дел по причине отсутствия лиц, привлекаемых в качестве обвиняемых. Такими примерами могут служить факты отсутствия достаточной доказательной базы либо розыск подозреваемого или обвиняемого в том случае, когда лицо установлено, но его местонахождение неизвестно. В практической деятельности возникают ситуации, когда установить полные сведения о подозреваемом лице не представляется возможным. Обычно имеются обрывки информации, такие как пол, рост, национальность, элементы даты рождения, некоторые цифры из номера телефона, возможный круг друзей и др. Такие данные могут добываться частями и на протяжении длительного времени. Важным источником получения дополнительной информации могут служить ресурсы сети Интернет. Практический опыт показывает эффективность использования такой информации при расследовании уголовных дел и раскрытии преступлений. Информационно-телекоммуникационные технологии позволяют установить дополнительные сведения о личности фигуранта и выявить ряд идентификационных признаков, например адрес электронной почты, реквизиты учетных записей, окружение в социальных сетях, сетевой адрес пользователя и иное.

В том случае, когда целенаправленный поиск на основе имеющихся данных не позволяет идентифицировать пользователя, применение отдельных методов обработки информации в виртуальной среде может помочь предоставить достаточный объем сведений для установления личности преступника. Появление новой информации возможно при сопоставлении имеющихся сведений с ранее накопленным хранилищем таких данных. В процессе сравнения возможны совпадения по одному или нескольким параметрам. Конечным результатом такой обработки может служить

сформированный профиль пользователя сети. Достаточный объем поисковых признаков позволит выдать результат в виде одного или нескольких таких профилей. Процент совпадений признаков в каждом из них позволит выбрать максимально удовлетворяющий запросу.

Внедрение и применение методов идентификации пользователей на системной, организованной и постоянной основе позволит формировать и накапливать идентификационную признаковую базу лиц, потенциально представляющих интерес в связи с совершенными преступлениями. Использование накопленных ресурсов позволит создать условия для совершенствования деятельности ОВД в рамках мероприятий по установлению лиц, совершивших преступления, и привлечения их к уголовной ответственности.

Подводя итог, можно отметить, что фундаментальным показателем деятельности полиции является поддержание социально-экономического климата государства. Соблюдение норм и правил гражданами государства является залогом его стабильного развития и функционирования. Положительным результатом деятельности по раскрытию и расследованию преступлений служит привлечение к ответственности лиц, их совершивших. Каждое неустановленное лицо – это приостановленное производством уголовное дело. Внедрение и использование в деятельности ОВД методов идентификации пользователей сети Интернет позволит увеличить число установленных лиц по совершенным преступлениям и, как результат, сократит количество фактов ухода от заслуженного наказания.

Таким образом, достижение поставленных в рамках планирования следственных целей является основным компонентом достижения успеха в раскрытии и расследовании мошенничества в сфере компьютерной информации.

§ 2. Тактика первоначальных следственных действий по делам о мошенничестве с использованием цифровых технологий

К одним из самых распространенных в следственно-судебной практике следственных действий следует отнести следственный осмотр. Не являются исключением и уголовные дела о преступлениях, совершенных с использованием современных цифровых технологий. Так, среди наиболее типичных видов следственного осмотра по названной категории уголовных дел отдельно следует выделить осмотр места происшествия, осмотр электронных устройств, в том числе компьютерной техники, осмотр электронных носителей информации и осмотр документов.

Основной целью производства осмотра места происшествия по делам о мошенничестве с использованием цифровых технологий является обнаружение и установление конкретного электронного устройства или оборудования, которое может иметь значение для обстоятельств по уголовному делу и содержать на себе следы преступления, представленные в электронном виде. Так, при производстве данного вида следственного действия наиболее целесообразным является использование эксцентрического тактического приема, который заключается в постепенном осмотре от центра к периферии помещения, в котором располагается интересующее следствие оборудование.

После осмотра места происшествия следует приступить к непосредственному осмотру компьютерного устройства. Подобный осмотр производится в целях обнаружения на данном устройстве следов и иных вещественных доказательств, которые позволят установить лиц, причастных к совершению мошенничества, установления общей обстановки совершения преступления, а также установления технических характеристик и состояния обнаруженного электронного компьютерного устройства.

Еще одним дополнительным видом осмотра по уголовным делам о мошенничествах с использованием цифровых технологий выступает осмотр электронного носителя информации, производство которого допускается как в рамках общего осмотра места происшествия, так и в ходе отдельного следственного действия.

Отметим, что к электронным носителям информации следует относить не только маломобильные электронно-вычислительные устройства, такие как персональные компьютеры и др., но и современные электронные мобильные гаджеты – смартфоны, планшеты, умные колонки и пр. На данных устройствах также в составе имеется постоянное запоминающее устройство, которое может содержать в себе имеющую значение для уголовного дела электронную информацию. Не стоит забывать и о классических электронных носителях информации без функции вычисления – жесткие диски, флеш-накопители, твердотельные накопители и т. д.

Осмотр электронного носителя информации целесообразнее осуществлять с фактическим участием специалиста в сфере высоких технологий. Как правило, такой осмотр может быть начат с описания вида и предназначения устройства, его основных технических характеристик, после чего при помощи программного обеспечения следует приступать к исследованию содержания электронных носителей информации.

В рамках осмотра электронных носителей информации также возможен осмотр электронных документов, выполненных при помощи какого-либо специального программного обеспечения (текстовых редакторов, электронных таблиц и пр.). Такой осмотр рекомендуется производить при участии специалиста соответствующего направления специальных познаний в зависимости от содержания осматриваемых документов (в области финансово-хозяйственной деятельности, инженерно-технической сфере и т.д.).

Основной целью осмотра электронного документа выступает выявление и получение информации о его реквизитах, внешних атрибутах, а также анализ его содержания. Также одной из задач в ходе осмотра является установление фиктивности, подложности электронного документа.

При осмотре электронного документа, выполненного на соответствующем электронном устройстве, также следует учитывать требования локальных нормативных актов конкретного предприятия и учреждения, которые регулируют порядок создания, выполнения и удостоверения подлинности названного вида документов.

Отдельного внимания заслуживает осмотр документов, которые располагаются в информационно-телекоммуникационной сети Интернет и хранятся удаленно на серверах. Сложность осмотра подобных документов заключается в особенностях их удаленного хранения на серверах, которые порою расположены на территории иностранных государств, что затрудняет доступ к ним отечественных правоохранительных органов. В таком случае, лицам производящим расследование, ничего не остается, как производить осмотр документа удаленно, используя сеть Интернет.

Осмотр электронного документа, хранящегося на электронном носителе информации, имеет существенное значение для выдвижения новых следственных версий и дальнейшего направления хода расследования мошенничества.

Тактические особенности производства таких следственных действий, как обыск и выемка по уголовным делам о преступлениях в сфере компьютерной информации неоднократно становились предметом исследования некоторых ученых[1].

Как правило, такое следственное действие, как обыск, выступает в качестве типичного первоначального следственного действия по уголовным делам о мошенничестве с использованием цифровых технологий и нуждается в тщательной подготовке перед началом его производства.

Предлагаем следующий алгоритм производства данного следственного действия по прибытии к месту его проведения:

1) оперативно обеспечить проникновение в помещение, где проходит обыск (или сразу в несколько помещений, при необходимости);

---

[1] Вехов В.Б. Особенности расследования преступлений, совершаемых с использованием средств электронно-вычислительной техники: учеб.-метод. пособие / 2-е изд., доп. и испр. Москва: ЦИиНМОКП МВД России, 2000. С. 33 – 42.

2) в случае столкновения с сопротивлением лиц, находящихся в обыскиваемом помещении (например, лиц, проживающих совместно с подозреваемым, представителей частных охранных организаций), следует незамедлительно нейтрализовать его, если необходимо, то с применением специальных средств и физической силы в составе следственной группы или при оказании содействия силовыми подразделениями ОВД или Росгвардии;

3) следует как можно скорее обеспечить охрану обыскиваемого помещения и прилагаемой к ней территории. Так, особое внимание необходимо уделить охране границ обыскиваемого помещения, технических электронных устройств (персональных компьютеров, серверов), электронных носителей информации, узлов электропитания и охранной сигнализации и иных технических помещений.

Следующим этапом производства обыска выступает обзорная стадия, в ходе реализации которой необходимо обратить внимание на следующие моменты.

Следует установить расположение и отключить от питания, выключить средства защиты информации, хранящейся на любых электронных устройствах и компьютерной техники. При наличии возможности, в случае блокирования доступа к содержанию и функционалу электронных устройств необходимо получить пароли и ключи доступа к указанным электронным устройствам. Они могут быть записаны на бумажном носителе по месту производства обыска или о них могут быть осведомлены присутствующие при обыске лица.

Далее следует обнаружить и установить доступные для подключения устройств сети как между собой по схеме локальной сети, так и с подключением к серверу, располагающиеся вне помещения обыска, а также с подключением к сети Интернет. При этом особое внимание следует уделить подключению компьютеров к периферийным устройствам по месту производства обыска.

После обзорного этапа обыска следует перейти к его детальной стадии. Данный этап занимает большую часть времени при его производстве и является достаточно трудоемким. В ходе данного

этапа целесообразно привлечь специалиста, который обладает познаниями в сфере информационных технологий.

Все поисковые мероприятия должны быть точно спланированы с учетом возможного обнаружения каких-либо тайников, скрытых полостей, в которых могут находиться предметы, интересующие следствие, – электронные носители информации, вычислительные устройства, периферийное оборудование и т. д.

В целях обнаружения вероятных мест сокрытия цифровых устройств, которые выступали в качестве орудия совершения мошенничества, следует ориентироваться на условия их хранения и эксплуатации. Как и любое технически сложное устройство электронные носители информации либо иные электронные устройства не выдерживают слишком высоких температур – 65°С и выше. Также весьма пагубное влияние оказывает на такие устройства высокая влажность. Электронные носители, имеющие в составе ферромагнитные элементы, также могут быть повреждены и при отрицательной температуре (в особенности жесткие магнитные диски). Помимо этого достаточно агрессивная внешняя среда – прямые солнечные лучи, сильные вибрации, удары, пыль – может оказать существенное воздействие на дееспособность устройств.

При работе в ходе обыска с изъятыми электронными устройствами и средствами компьютерной техники лицу, производящему расследование, следует ориентироваться на следующие криминалистические рекомендации.

В случае если на месте производства обыска вскрытие корпуса обнаруженного устройства не представляется возможным в силу угрозы повреждения и утраты хранящейся на нем информации, такое устройство следует изъять целиком в целях последующего экспертного исследования.

Если в ходе обыска обнаружены любые электронные носители информации, то они, безусловно, подлежат изъятию, даже при наличии возможности ознакомиться с их содержимым по месту производства обыска. Такое требование выполняется в целях детального экспертного исследования носителя информации с применением специализированного лабораторного оборудования.

В ходе обыска категорически не рекомендуется использовать специальные технические средства, содержащие в качестве элементов источник электро-магнитных излучений, например, рентгеноаппараты, металлодетекторы и пр. При этом могут быть использованы образцы современных поисковых устройств (нелинейные локаторы), которые не наносят существенного вреда содержанию электронных носителей информации.

В случае необходимости изъятия жесткого диска компьютера или твердотельного накопителя наиболее целесообразным будет изъятие всего системного блока целиком, чтобы исключить опасность повреждения отдельных элементов и составных частей компьютера.

Если изъятию подлежит периферийное оборудование, например, принтер, то следует иметь ввиду, что вопрос о криминалистической идентификации указанного оборудования может быть разрешен только в отношении так называемого матричного (струйного) печатающего устройства. В отношении лазерного принтера исследование идентифицирующих признаков возможно только в исключительно редких случаях, например, при производстве трасологической экспертизы в отношении прижимных валиков устройства подачи бумаги принтера.

Завершающим этапом производства обыска выступает подведение его итогов и фиксация результатов. Так, в соответствии с требованиями уголовно-процессуального закона должен быть составлен протокол обыска, в качестве приложений к которому могут выступать план-схема помещений, на которой указано место обнаруженных и изъятых электронных устройств. Помимо этого, в данной схеме может быть указана схема соединения компьютеров по локальной сети, расположения помещений с сервером и т. д. Также в качестве дополнительного способа фиксации результатов обыска может выступать фотосъемка или видеозапись производимого обыска.

По уголовным делам о мошенничестве с использованием цифровых технологий в качестве предмета выемки выступает электронно-вычислительная техника, иные электронные носители информации, а также документы, в том числе в электронном виде.

Подлежат также изъятию устройства защиты информации или получения доступа к информации и пр.

Кроме указанных выше объектов фактическому изъятию также подлежат любые предметы, которые могли быть использованы в качестве средств изготовления орудия преступления, например, подложные документы, электронные носители информации, использовавшиеся для несанкционированного доступа к информации в целях мошенничества и пр. Могут быть полезными в доказывании также черновики с образцами поддельной подписи, бланки учетно-регистрационной работы предприятия, документы о движении денежно-материальных ценностей, а также специальная техническая литература, посвященная вопросам использования электронного документооборота в работе предприятия или учреждения.

Согласно требованиям уголовно-процессуального законодательства, предусматривающим особый порядок обращения с электронными носителями информации при их изъятии, выемку таких носителей следует осуществлять с участием соответствующего специалиста. Кроме этого, обязательными участниками данного следственного действия выступают понятые. Их основная задача – зафиксировать ход и результаты произведенного следственного действия. В случае необходимости законный владелец носителя информации вправе потребовать копирования информации с изымаемых носителей, которое осуществляется специалистом в присутствии понятых. В таком случае копирование производится на иной резервный носитель информации, который предоставляется законным владельцем, о чем в протоколе делается соответствующая запись.

Особого внимания заслуживает порядок изъятия мобильных электронных устройств. При изъятии указанных устройств действуют те же правила, что и при изъятии электронных носителей информации. При изъятии мобильных телефонов, планшетов и иных мобильных устройств следует использовать специальное сканирующее оборудование, которое направлено на установление наиболее значимых следов, в том числе и в электронном виде. Рекомендуется по возможности принять меры к обнаружению и изъятию зарядного устройства и иной документации, прилага-

емой к мобильному устройству (например, договор об оказании услуг связи). В случае если лицо, у которого изымается мобильное устройство, отказывается сообщить пароль для доступа к его содержимому, то данный факт должен быть отражен в соответствующем протоколе следственного действия. При описании изъятого мобильного устройства в протоколе обязательно должны быть отражены вид и модель устройства, отличительные признаки внешнего вида (сколы, царапины, потертости), а также текущий функциональный статус устройства – выключено/включено; заблокировано/доступно. После завершения изъятия, если доступ к устройству является свободным (без пароля и пин-кода), мобильное устройство следует выключить, чтобы избежать израсходования заряда аккумуляторной батареи, и осуществить его упаковку по правилам криминалистической техники. В противном случае выключение устройства не рекомендуется, так как повторный доступ к нему после включения может вызвать затруднения.

В случае необходимости на месте производства обыска изъятые предметы могут быть подвергнуты дополнительному осмотру. Однако ввиду слишком большого объема информации такой осмотр на месте затруднителен, поэтому осмотру подлежит лишь информация о входящих и исходящих соединениях абонента. В протоколе об этом делается отметка с указанием, что оставшаяся информация, хранящаяся на устройстве, осмотру не подвергалась. Подробную электронную информацию, в том числе и ту, которая скрыта от пользователя, целесообразно получить в ходе экспертного исследования в рамках производства компьютерно-технической экспертизы.

При описании в протоколе следственного действия вида и типа электронного устройства большое внимание следует уделять терминологии, используемой следователем. Так, небольшие по размеру устройства, обладающие разъемом типа USB, могут быть названы как флеш-накопители, однако точно такой же внешностью может обладать адаптер беспроводной связи (Bluetooth), который не является носителем информации, а выступает лишь телекоммуникационным устройством. Положение усугубляется, когда описание типа устройства в виде надписи на нем стирается

в силу эксплуатации. Аналогичная ситуация характерна для так называемых устройств считывания карт памяти (картридеров), которые сами по себе электронными носителями информации не являются, однако отдельные виды таких считывателей обладают встроенным объемом памяти, что также позволяет отнести их к носителям информации. В связи с этим рекомендуется при описании подобных устройств в протоколе использовать нейтральный термин «USB устройство», не указывая конкретный его тип и групповую принадлежность.

Подобные рекомендации в первую очередь необходимы для обеспечения исполнения требований уголовно-процессуального законодательства при изъятии электронных носителей информации. В противном случае при нарушении указанных норм, изъятые предметы могут быть признаны недопустимыми доказательствами и потерять свое юридическое значение для установления обстоятельств уголовного дела и расследования преступления.

Тактические особенности производства допроса в ходе расследования преступления с использованием цифровых технологий рассматриваются исследователями уже на протяжении долгого времени[1].

В ходе расследования мошенничества с использованием цифровых технологий такое следственное действие, как допрос, осуществляется по тем же правилам, разработанным криминалистической наукой для данного вида следственного действия. Особое внимание следователю следует уделять подготовительной части допроса при изучении личности допрашиваемого лица. Как правило, при допросе подозреваемого (обвиняемого) по названной категории уголовных дел следует учитывать, что зачастую подобные лица обладают высшим образованием в специфической сфере деятельности, связанной с высокими технологиями. По понятным причинам их лексикон может быть непонятен следователю. В связи с этим следователь должен быть готов к производству допроса с точки зрения материальной базы, а если все же какие-то формулировки ему непонятны, то целесообразно задавать уточня-

[1] Расследование неправомерного доступа к компьютерной информации: учеб. пособие / под ред. Н.Г. Шурухнова; 2-е изд., доп. и перераб. Москва: Московский университет МВД России, 2004. С. 217 – 226.

ющие вопросы, которые детально отражают содержание показаний допрашиваемого.

Если сравнивать рассматриваемый вид мошенничества с мошенничеством общеуголовным, то очевидна будет особенность, которая заключается в более простом уяснении смысла механизма совершения преступления, его способов и средств. Для того чтобы понять способ совершения мошенничества с использованием цифровых технологий, следователю также необходимо обладать специальными познаниями в данной сфере. Однако далеко не все следственные работники в этом разбираются. В связи с этим даже при производстве такого следственного действия, как допрос, иногда целесообразно привлекать специалиста. Также в ходе допроса помощь может оказать оперуполноченный специализированного подразделения – отдел «К», – который осуществляет оперативное сопровождение уголовного дела. Тем более что УПК РФ такую возможность допускает. Консультация со специалистом также необходима до начала допроса для приготовления списка вопросов, которые надлежит поставить перед допрашиваемым.

Представляет особый интерес ситуация, получившая в настоящее время типичный характер, когда следователем предлагается потерпевшему в рамках проведения допроса либо осмотра документа получить доступ к его личному абонентскому кабинету в целях получения детализации соединений за интересующий следствие период. Техническая особенность получения детализации счета из личного кабинета предполагает необходимость использования SIM-карты потерпевшим, которая была помещена в мобильное устройство в период, интересующий следствие. Только в этом случае имеется возможность получения доступа к личному кабинету. В связи с этим также возникает вопрос – возможно ли следователю получить информацию из личного кабинета абонента без его согласия? Представляется, что нет, так как технически автоматическая выборка соединений, производимая абонентом в сети Интернет, является разновидностью детализации входящих и исходящих соединений, которая в соответствии с позицией Конституционного Суда Российской Федерации, отраженной в опре-

делении от 02.10.2003 № 345-О1, охраняется тайной телефонных переговоров.

При подготовке к допросу следователю необходимо уделить внимание следующим вопросам, подлежащим установлению по рассматриваемой категории преступлений.

Каков принцип воздействия на компьютерную информацию (неправомерный доступ, использование вредоносного программного обеспечения, манипулирование данными и т. п.)?

Каков характер воздействия на операционную систему электронного устройства? Связано ли это с уничтожением, модификацией или копированием данных, хранящихся на конкретном устройстве?

Каковы были последствия от несанкционированного доступа к цифровой информации, содержащейся в устройстве?

Каким минимальным уровнем образования должно обладать лицо для совершения мошенничества в сфере цифровых технологий? Могло ли такое лицо использовать свое служебное положение для облегчения совершения преступления? Возможно ли совершение подобного преступления группой лиц или исполнитель мог совершить его единолично?

Наиболее точный ответ на вышеуказанные вопросы зависит в первую очередь от более подробных экспертных исследований непосредственно самих носителей информации. Однако специалист в сфере высоких технологий способен самостоятельно проанализировать собранные материалы дела и высказать общие предположения о механизме совершения преступления. На основании предположений специалиста следователь может выдвигать следственные версии и планировать дальнейшее расследование преступления, в том числе подготовиться к допросу участников производства по делу. В том случае, если следователь обладает достаточной квалификацией, чтобы ответить на указанные вопросы, привлечение специалиста в данном случае необязательно. Однако это не означает, что следователь должен игнорировать помощь специалистов из других областей специальных познаний, например, в налоговой, финансово-кредитной сферах, в области инженерии, строительства и т. п. Такая помощь следователю мо-

жет быть оказана в целях установления мотивов и целей преступного посягательства в сфере цифровых технологий.

При подготовке допроса подозреваемого следователь должен определиться с уровнем его квалификации в сфере высоких технологий. От определения данного критерия зависит выбор конкретных тактических приемов допроса и принятия решения о приглашении специалиста для участия в допросе.

Одним из способов защиты подозреваемого в ходе первого допроса могут быть показания о том, что несанкционированный доступ к электронному устройству или компьютерной информации был осуществлен случайно, по незнанию, либо в силу действий третьих лиц. Подозреваемый может утверждать об отсутствии у него умысла на неправомерный доступ к информации.

В ходе допроса подозреваемого в мошенничестве с использованием цифровых технологий также следует задавать стандартные для любого допроса вопросы, касающиеся обстоятельств, характеризующих его личность, и других обстоятельств совершенного преступления. Отбывал ли он ранее уголовное наказание? За какие преступления? Каким образом стало известно о конкретной схеме мошенничества? Что выступило основным мотивом совершения мошеннических действий? Если преступление совершенно с использованием мобильных устройств, то какие абонентские номера были использованы подозреваемым в ходе совершения преступления? На кого зарегистрированы данные номера, каким образом были получены SIM карты с абонентскими номерами. Если механизм мошеннических действий предполагал массовую рассылку СМС (например, о блокировке банковской карты, о списании со счета денежных средств), то следует выяснить, на какие номера такая рассылка осуществлялась, а также дословное ее содержание. Если у подозреваемого с потерпевшим был непосредственный контакт в виде телефонного разговора, то следует выяснить – откуда осуществлялись телефонные соединения, каким образом от потерпевшего были получены денежные средства (путем перечисления безналичных средств через онлайн-банк или путем передачи наличных курьеру)? В последнем случае следует выяснить – кто именно

получал денежные средства от потерпевшего, был ли он в сговоре с подозреваемым или добросовестно заблуждался о характере своих действий. Необходимо выяснить у подозреваемого – как он распорядился полученными денежными суммами. Потрачено ли все похищенное у потерпевшего или что-то осталось.

В целях изобличения подозреваемого эффективной может быть грамотная реализация оперативной информации, полученной в результате проведения комплекса оперативно-розыскных мероприятий. Кроме того, в ходе допроса допускается предъявление подозреваемому предметов, выступавших в качестве орудия совершения преступления (например, технических устройств, при помощи которых им был получен несанкционированный доступ к цифровой информации). Тактически грамотное применение вышеуказанных приемов и оперативной информации позволит изобличить подозреваемого в совершении мошенничества, если допрос производится в условиях конфликтной ситуации, в особенности при производстве первого допроса сразу после задержания.

Если подозреваемый использует специальные термины, целесообразно в конце допроса (а иногда и по ходу) предложить ему пояснить их. Дело в том, что специалисты в различных отраслях компьютерных технологий одни и те же слова могут использовать в разных значениях, иногда отличных от общеупотребительных. Даже в словарях определения терминов могут существенно отличаться. Кроме того, некоторые начинающие «хакеры», желая показать свои «знания» в сфере информационных технологий, используют термины неправильно, не понимая их смысл. Поэтому допрашиваемому можно предложить существующие легальные и словарные определения, с которыми он либо согласится, либо предложит свою формулировку.

Иногда подозреваемые (это свойственно несовершеннолетним), желая показать свое превосходство над следователем в области знания компьютерных технологий, описывают события, невозможные с технической точки зрения. Специалист способен сразу распознать ложь и тем самым нейтрализовать попытку противо-

действия расследованию, понудить подозреваемого к даче правдивых показаний.

Специалист может помочь и в использовании такого тактического приема, как «проговорка» допрашиваемого. С подозреваемым, отрицающим свою вину, но не отказывающимся отвечать на общие вопросы, беседуют на различные темы, связанные с компьютерами. Постепенно ему предлагают охарактеризовать, например, используемую потерпевшим (не акцентируя на этом внимание) систему защиты информации или программное обеспечение, которое, предположительно, использовалось для несанкционированного доступа. Не исключено, что допрашиваемый назовет уязвимые места системы, расскажет, как ее можно «взломать», что, по крайней мере, в оперативном плане (а возможно, и процессуально) позволит установить причастность лица к совершению преступления. Только специалист способен построить систему таких вопросов-ловушек и определить, какие из ответов имеют отношение к делу. В данном случае это, вероятно, будет оперативный сотрудник отдела «К».

Для успешного проведения допроса обвиняемого необходимо тщательно изучить все материалы дела, особенности личности обвиняемого, способы совершения преступления, доказательства, указывающие на виновность конкретного лица, и т. п. Ко времени привлечения лица в качестве обвиняемого, следствие должно располагать двумя категориями доказательств. В первой из них предусматривается доказывание обстоятельств, свидетельствующих о том, что расследуемое событие (деяние) имело место, во второй – что это деяние совершено привлекаемым к уголовной ответственности лицом, и оно соответствует составу преступления, предусмотренного соответствующей статьей УК РФ.

Допрос обвиняемого является одним из важнейших, наиболее сложных и зачастую конфликтных следственных действий. Не преследуя цели рассмотрения тактики допроса обвиняемого в целом, отметим, что обвиняемые дают правдивые показания в тех случаях, когда убедятся, что расследованием установлен круг фактических данных. Поэтому обычно наиболее результативны приемы представления допрашиваемым собранных по делу до-

казательств и подробного изложения обстоятельств преступления без ссылки на источники.

Круг вопросов, подлежащих выяснению у обвиняемого, определяется конкретной следственной ситуацией, сложившейся по уголовному делу.

Основными тактическими задачами допроса потерпевших и свидетелей при расследовании дел рассматриваемой категории являются: выявление элементов состава преступления в наблюдавшихся ими действиях, установление обстоятельств, места и времени совершения значимых для расследования действий, способа и мотивов его совершения и сопутствующих обстоятельств, признаков внешности лиц, участвовавших в нем, определение предмета преступного посягательства, размера причиненного ущерба, детальные признаки похищенного, установление иных свидетелей и лиц, причастных к совершению преступления.

Для решения указанных задач в процессе допроса свидетелей необходимо выяснить:

- не проявлял ли кто-либо интереса к компьютерной информации, программному обеспечению, компьютерной технике данного предприятия, организации, учреждения, фирмы или компании;
- не появлялись ли в помещении, где расположена компьютерная техника, посторонние лица, не зафиксированы ли случаи работы сотрудников с информацией, не относящейся к их компетенции;
- не было ли сбоев в работе программ, хищений носителей информации и отдельных компьютерных устройств;
- зафиксированы ли сбои в работе компьютерного оборудования, электронных сетей, средств защиты компьютерной информации;
- как часто проверяются программы на наличие вирусов, каковы результаты последних проверок;
- как часто обновляется программное обеспечение, каким путем, где и кем оно приобретается;
- каким путем, где и кем приобретается компьютерная техника, как осуществляется ее ремонт и модернизация;

- каков на данном объекте порядок работы с информацией, как она поступает, обрабатывается и передается по каналам связи;

- кто еще является абонентом компьютерной сети, к которой подключены компьютеры данного предприятия, организации, учреждения или фирмы, каким образом осуществляется доступ в сеть, кто из пользователей имеет право на работу в сети, каковы их полномочия;

- как осуществляется защита компьютерной информации, применяемые средства и методы защиты и др.;

- имели ли место случаи неправомерного доступа к компьютерной информации ранее, если да, то как часто;

- могли ли возникшие последствия стать результатом неосторожного действия лица или неисправности работы компьютерной системы, сбоев программного обеспечения и т. п.;

- каков характер изменений информации;

- кто является собственником (владельцем или законным пользователем) скопированной (уничтоженной, модифицированной, блокированной) информации и др.

При расследовании мошенничества в сфере компьютерной информации на первоначальном этапе возникает необходимость допрашивать в качестве свидетелей граждан различных категорий, для каждой из которых существует свой предмет допроса.

При расследовании мошенничества с использование цифровых технологий могут назначаться различные виды экспертиз, характерные для прочих видов мошенничества: трасологические, почерковедческие, технико-криминалистические экспертизы документов, финансово-аналитические, бухгалтерские и др.

Особая форма представления информации – компьютерная – вызывает необходимость применения специальных знаний для проведения экспертных исследований такой информации и ее носителей. Эту функцию выполняет компьютерная экспертиза.

В последнее время мошенничество с использованием цифровых технологий все чаще совершается с использованием устройств мобильной связи, позволяющих не только осуществлять телефонное соединение между абонентами, но и выполняющих функции информационно-телекоммуникационного

оборудования с возможностью подключения к сети Интернет. Исследование таких устройств также входит в задачи компьютерной экспертизы[1].

В связи с разнообразием решаемых компьютерной экспертизой задач и постоянно изменяющимися возможностями информационно-телекоммуникационных систем сформулировать перечень вопросов, которые могут быть поставлены на разрешение компьютерной экспертизы, не представляется возможным. Существующие списки[2] носят ориентирующий характер, а объем и последовательность вопросов в каждом конкретном случае необходимо определять исходя из решаемых задач. Поэтому, прежде чем сформулировать вопросы, следователю необходимо получить консультацию у специалиста – эксперта компьютерной экспертизы.

Рассмотрим один пример из опыта работы ЭКЦ ГУ МВД России по г. Москве.

24.08.2015 в период с 15 часов 00 минут до 15 часов 30 минут неустановленное лицо, находясь в офисе «Агентство авиационных компаний» (г. Москва), через систему «СИРЕНА», с владельцем которой – ЗАО «Транспортная клиринговая палата» – был заключен договор, произвело регистрацию электронного железнодорожного билета № NNNNNNNNNNNNN на имя В. на сумму 35 182,30 рублей, внеся в графы шаблона ООО «УФС» полные анкетные данные указанного лица, тем самым получило 14-значный номер электронного железнодорожного билета. При этом фактический перевод денежных средств за билет на счет ОАО «Приморское агентство авиационных компаний» осуществлен не был, однако 24.08.2015 в билетной кассе железнодорожного вокзала ст. Лена Восточно-Сибирской железной дороги (г. Усть-Кут Иркутской области) был оформлен их возврат.

В ходе производства предварительного расследования с персонального компьютера потерпевшей компании был изъят накопи-

[1] Расследование мошенничеств, совершаемых с использованием мобильной связи: учеб. пособие / авт.-сост. О.П. Грибунов, М.В. Старичков; А.А. Шаевич, О.В. Трубкина, Е.И. Третьякова, В.А. Родивилина. Иркутск: ВСИ МВД России, 2018. С. 27-30.

[2] Расследование преступлений в сфере компьютерной информации и высоких технологий: учеб. пособие / сост. М.В. Старичков; 2-е изд., перераб. и доп. Иркутск: ВСИ МВД России, 2014. С. 110-115.

тель на жестких магнитных дисках (НЖМД) и направлен в ЭКЦ ГУ МВД России по г. Москве для производства компьютерной экспертизы.

Перед экспертом были поставлены следующие вопросы:

1. Имеются ли на жестком диске файлы, содержащие слова «В. [ФИО], паспортные данные XXXX XXXXXX, электронный железнодорожный билет № NNNNNNNNNNNNN на имя В.»?

2. Содержатся ли вирусные программы на предоставленном жестком диске?

3. Имеются ли на представленном жестком диске программы для удаленного доступа?

4. Какие имеются настройки сетевых карт на жестком диске?

Для проведения исследования использовался аппаратно-программный комплекс «Стенд для производства компьютерных экспертиз». Проводилось восстановление ранее удаленной информации, которая сохранялась на НЖМД стендового компьютера с сохранением иерархии каталогов.

В целях обеспечения сохранности информации, располагающейся на исследуемом НЖМД, и гарантии невнесения изменений в его содержимое при помощи специального модуля автономного дублирования жестких дисков «Поиск-Д» производилось полное посекторное копирование исследуемого НЖМД на НЖМД стендового компьютера и в дальнейшем осуществлялось исследование данных диска-клона. С помощью программы «Windows Registry Recovery» были установлены сведения об операционной системе и исследовано содержимое ее реестра.

Для ответа на первый вопрос экспертом осуществлялся поиск интересующей информации, в том числе среди удаленной. В результате поиска на НЖМД было обнаружено 8 файлов. У всех у них дата изменения – 24.08.2015, время изменения – с 14.44 до 16.11.

Для ответа на второй вопрос при помощи антивирусных программ проверялись файлы на исследуемом НЖМД. Было обнаружено 6 файлов трех разновидностей, данные о которых сведены в таблицу.

Для ответа на третий вопрос экспертом просматривались установленные на НЖМД программы для удаленного доступа, а

также содержимое реестра установленной операционной системы. Также была найдена программа для удаленного доступа «TeamViewer».

Для ответа на четвертый вопрос просматривалось содержимое реестра установленной операционной системы. В результате поиска были обнаружены записи о сетевых подключениях.

Дополнительно экспертом было установлено, что при запуске файла «Раздел1\FlashPresentation.scr» (дата создания на диске 20.08.2015, 12.52), который является архивом, на виртуальной машине эксперта в каталог пользователя «Раздел1\Documents and Settings\xxxxxxxx\Local Settings\Temp\» распаковывались файлы: «wget.exe», «xxaupd.cmd». После этого автоматически на исполнение запускался файл «xxaupd.cmd». Запись о файле «FlashPresentation.scr» была найдена в истории загрузки и истории просмотра браузера пользователя. Файлы «RWLN.dll», «vp8decoder.dll», «vp8encoder.dll», «windowsupd.exe», «winmm.dll» были обнаружены на исследуемом НЖМД по адресу: «Раздел1\WINDOWS\» и имели атрибуты файлов «скрытый», «только для чтения» и «системный». Далее в реестре установленной операционной системы на исследуемом НЖМД (файл system, зарегистрированный по адресу Раздел1\Windows\system32\config\) в результате поиска были найдены записи о настройках удаленного сетевого подключения в ветви реестра: «SYSTEM\Remote Utilities\v4\Server\Parameters\».

Таким образом, на НЖМД была установлена программа для удаленного доступа, посредством которой осуществлялся доступ к платежной системе и покупка от лица компании электронного билета с дальнейшим его обналичиванием через третьих лиц. Заметим, что на НЖМД компании антивирусное программное обеспечение не устанавливалось.

Позднее на экспертизу поступали подобные объекты, но хищения по тем эпизодам совершались более двух лет назад, за этот период компьютер активно эксплуатировался, было установлено антивирусное программное обеспечение. В результате практически все следы деятельности злоумышленников, направленные на незаконное приобретение билетов, были уничтожены.

Кроме этого, при назначении компьютерной экспертизы перед экспертом могут быть поставлены следующие дополнительные вопросы:

1. Имеются ли на представленном на экспертизу оптическом компакт-диске … исходные коды компьютерных программ. Если да, то в какой операционной системе данные программы способны выполняться? (частный случай, если известно, что коды представлены в виде готового проекта, иначе их очень сложно представить как программу).

2. Предназначены ли программы, исходные коды которых имеются на представленном на экспертизу оптическом компакт-диске …, для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации?

3. Выводятся ли пользователю операционной системы сообщения при установке программ, исходные коды которых имеются на представленном на экспертизу оптическом компакт-диске …, если да, то какие?

4. Какие действия при установке производят программы, исходные коды которых имеются на представленном на экспертизу оптическом компакт-диске …, если да, то какие?

5. Производят ли программы, исходные коды которых имеются на представленном на экспертизу оптическом компакт-диске …, действия, которые скрыты от пользователя операционной системы, если да, то какие именно?

6. Способны ли программы, исходные коды которых имеются на представленном на экспертизу оптическом компакт-диске …, устанавливать скрытые от пользователя несанкционированные сетевые соединения, если да, то какие именно?

7. Имеют ли программы, исходные коды которых имеются на представленном на экспертизу оптическом компакт-диске …, функции удаленного администрирования (управления), если да, то какие действия происходят при получении команд?

8. Способны ли программы, исходные коды которых имеются на представленном на экспертизу оптическом компакт-диске …, осуществлять скрытую от пользователя операционной системы

отправку коротких текстовых сообщений (СМС), если да, то какие именно?

9. Способны ли программы, исходные коды которых имеются на представленном на экспертизу оптическом компакт-диске …, осуществлять скрытое от пользователя операционной системы чтение входящих коротких текстовых сообщений (СМС), если да, то каких именно?

10. Способны ли программы, исходные коды которых имеются на представленном на экспертизу оптическом компакт-диске …, осуществлять скрытое от пользователя операционной системы блокирование входящих и исходящих коротких текстовых сообщений (СМС), если да, то каких именно?

11. Способны ли программы, исходные коды которых имеются на представленном на экспертизу оптическом компакт-диске …, осуществлять скрытое от пользователя операционной системы удаление входящих и исходящих коротких текстовых сообщений (СМС), если да, то каких именно?

12. Способны ли программы, исходные коды которых имеются на представленном на экспертизу оптическом компакт-диске …, осуществлять сбор какой-либо технической информации об устройстве, на котором они устанавливаются, если да, то какой именно информации, и производится ли скрытое копирование данной информации на иные носители, в том числе посредством информационно-телекомуникационной сети Интернет?

13. Предпринимают ли программы, исходные коды которых имеются на представленном на экспертизу оптическом компакт-диске …, какие-либо действия, направленные на недопущение удаления их из операционной системы стандартными методами, доступными пользователю?

14. Продолжают ли программы, исходные коды которых имеются на представленном на экспертизу оптическом компакт-диске …, функционировать в скрытом режиме после попытки их удаления из операционной системы?

15. Способны ли программы, исходные коды которых имеются на представленном на экспертизу оптическом компакт-диске …,

осуществлять автозапуск при старте операционной системы без инициации данного процесса пользователем?

16. Являются ли представленные на экспертизу на оптическом компакт-диске … файлы «…» (размер … байт), «…» (размер … байт), «…» компьютерными программами. Если да, то в какой операционной системе данные программы способны выполняться?

17. Имеют ли программы, исходные коды которых имеются на представленном на экспертизу оптическом компакт-диске …, и программы, содержащиеся в файлах «…» (размер … байт), «…» (размер … байт), «…», сходные функциональные возможности и алгоритмы исполнения программ?

18. Устанавливались ли программы, исходные коды которых имеются на представленном на экспертизу оптическом компакт-диске …, на мобильный телефон … с серийным номером …, имеющий IMEI …. Если да, то какая программа (файл) и когда именно?

При расследовании преступлений в сфере компьютерной информации принципиальное значение имеет производство судебных экспертиз, поскольку в дальнейшем результаты ее производства будут иметь большое доказательственное значение в суде.

Рассматривая разновидности судебных экспертиз, назначаемых в ходе расследования преступлений указанной категории, отметим, что наряду с традиционными исследованиями, такими как дактилоскопические (по следам пальцев рук), почерковедческие (по рукописям, использованным при подготовке к преступлению), назначаются и специфические судебные экспертизы.

Наиболее простой возможностью получения информации о ПЭВМ, установленных приложениях, запущенных процессах и активности пользователя на первоначальном этапе расследования является изучение системного реестра и файловых каталогов операционной системы. Указанные действия исключают внедрение в текущие процессы на исследуемом объекте и являются основополагающими для установления криминалистически значимой информации.

Одним из подвидов компьютерно-технических экспертиз является информационно-компьютерная экспертиза. Данный вид изучает цифровую информацию, т. е. данные, находящиеся в компьютерной системе. В качестве примера можно привести проектную документацию на разработку и использование компьютерного оборудования и сетей либо конфиденциальную информацию в электронном формате, позволяющую установить тождество при исследовании.

Указанный вид судебной компьютерно-технической экспертизы позволяет завершить расследование, поскольку отвечает на ряд завершающих и ключевых вопросов, связанных с цифровыми документами. Изучение данных, содержащих цифровую информацию, предоставляет возможность получения положительного результата, в частности, выявить механизм следообразования при работе компьютерных программ и приложений, установить движение транзакции, а также отследить пользователя информационных сетей посредством сохраненных (удаленных) им файлов в ЭВМ.

Отметим, что судебная информационно-компьютерная экспертиза решает широкий круг задач, направленных на определение способа форматирования носителя, выявление специфических особенностей физического места нахождения сведений, средств защиты информации, основной атрибутики информации (размеры файлов, их объем, типы, даты создания и др.). Кроме того, посредством указанного вида исследования идентифицируется разновидность обнаруженных файлов, устанавливается способ организации доступа к находящейся на электронном носителе информации и ее особенности.

Следующим подвидом указанных исследований кластера судебных компьютерно-технических экспертиз обозначим судебную компьютерно-сетевую экспертизу. Она получает свое существование на функциональном предназначении компьютерных средств. Все перечисленные выше задачи могут решаться данным видом исследования, поскольку ее объекты дифференцированы из представленных судебных экспертиз.

Для решения задач компьютерно-сетевой экспертизы эксперт, ее осуществляющий, должен обладать специальными знаниями

в сфере сетевых технологий, т. к. имеется необходимость эффективного отслеживания движения информации.

Круг задач, решаемых компьютерно-сетевой экспертизой, заключается в исследовании программных сетевых средств, персональных компьютеров, имеющих выход во всемирную сеть Интернет. В общем случае эксперт по проведению компьютерно-сетевой экспертизы в процессе своей деятельности решает задачи, связанные с установлением связей между использованием определенных сетевых объектов с результатами их деятельности; событием и механизмом действия; отображением сети в информационных пакетах для установления состояния исследуемой сети, где рассматриваются электронные носители информации.

Вместе с тем отметим, что посредством проведения указанного вида исследования устанавливается текущее состояние сетевой системы или сетевого программного или аппаратного средства, наличие физических дефектов аппаратных средств; определяются специфические характеристики сетевой системы, ее конфигурация, тип устройства архитектуры, механизм организации доступа к массивам данных, а также установленных сетевых программно-аппаратных средств.

Компьютерно-сетевая экспертиза является новым видом исследований, однако довольно активно развивающимся. С развитием сетевых технологий и появлением совершенно новых сетевых программ и решений методы их исследования также стремительно обновляются. Практически любые применяемые в сетевых системах технологии на сегодняшний день успешно анализируются и исследуются.

Задачами компьютерно-сетевой экспертизы является определение свойств, причин изменений свойств компьютерной сети; наличие либо отсутствие программных средств для функционирования ЭВМ; наличие либо отсутствие признаков работы ЭВМ в сети Интернет; особенности построения протоколов соединений; наличие сведений, которые подтверждают использование электронных платежей.

Для решения проблем, связанных с назначением судебных компьютерно-технических экспертиз и, соответственно, эффектив-

ным, всесторонним и объективным расследованием уголовных дел указанной категории, имеется необходимость усиления взаимодействия между следственными и экспертными подразделениями как в период назначения, так и во время производства судебной компьютерно-технической экспертизы.

Таким образом, своевременное производство по уголовному делу и назначение компьютерных экспертиз позволяет выявить и зафиксировать следы преступления и в дальнейшем использовать их в качестве доказательств.

ЗАКЛЮЧЕНИЕ

В современном мире высокие технологии занимают ведущее место и являются неотъемлемой частью практически всех сфер жизнедеятельности человека. Стремительно развиваются компьютерные технологии, порождающие ряд негативных последствий, одним из которых является криминализация сферы компьютерной информации и информационно-телекоммуникационных сетей связи. Внедрение все более совершенствованных информационных технологий в различные сферы деятельности человека дает возможность преступникам создавать новые виды преступных посягательств, которые зачастую непосильны в расследовании правоохранительных органов.

На сегодняшний день мошенничество является одним из самых противоречивых и противоправных деяний, так как совершение данного преступления связано с использованием обмана, злоупотреблением доверием. Мошенничество с использованием цифровых технологий реализуется путем процедур ввода, видоизменения, стирания с жестких носителей или прекращения обращения к данным, имеющимся на компьютере и иных электронных устройствах.

Преступления в сфере мошенничества с использованием цифровых технологий отражены в следующих статьях Уголовного кодекса Российской Федерации: ст. 159 «Мошенничество», 159.1 «Мошенничество в сфере кредитования», 159.2 «Мошенничество при получении выплат», 159.3 «Мошенничество с использованием электронных средств платежа», 159.5 «Мошенничество в сфере страхования» и 159.6 «Мошенничество в сфере компьютерной информации». Почти во всех вышеуказанных составах преступления использование цифровых технологий конкретно не предусмотрено диспозицией статьи, поэтому следует понимать, что любое преступление, предусмотренное пунктами статьи 159 УК РФ, возможно совершить и зачастую совершается путем фальсификации

официальных документов, средств обработки фотографий, текста, наложения поддельной печати, иных видов фальсификации через компьютерные программы, электронные устройства и иные программные продукты.

Возбуждению уголовного дела по факту мошенничества с применением цифровых технологий предшествует сбор информации путем оперативно-розыскной, следственной деятельности и иных процессуальных действий при соблюдении правил сохранения первоначальной формы доказательственной информации и без ущерба свойствам изымаемой информации. Достижение данных задач возможно посредством использования технических средств с обязательным привлечением специалиста в данной области и своевременного активного взаимодействия с сотрудниками подразделений, специализирующихся на расследовании и раскрытии данных видов преступлений.

Расследование мошенничества в сфере компьютерной информации предполагает производство достаточно сложных и трудоемких следственных действий. Следователь должен тщательно планировать производство расследования по уголовному делу. Развернутый план расследования составляется после производства первоначальных следственных действий. К этому времени определяется круг общих следственных версий, которые требуют дальнейшей проверки.

Выбор тактики производства следственных и процессуальных действий зависит от самого механизма преступного события, применяемых преступником компьютерно-технических средств, программного обеспечения, установленного на компьютер преступника и потерпевшего, наличия знаний о навыках и умениях лица, совершившего преступление данного вида, а также от предположительных знаний поведения подозреваемых лиц в ходе проведения следственных действий.

Своевременное производство по уголовному делу и назначение компьютерных экспертиз позволяет выявить и зафиксировать следы преступления и в дальнейшем использовать их в качестве доказательств.

Таким образом, на основании проведенного исследования пред-

ставлен юридический анализ сущности и понятия мошенничества с использованием цифровых технологий, произведена дифференциация со смежными составами хищений, совершаемых в сфере информационно-коммуникационных технологий; рассмотрены тактические положения организации и проведения отдельных следственных действий при расследовании мошенничества рассматриваемого вида, а также особенности оценки доказательств, полученных в ходе данных следственных действий.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Нормативные правовые акты

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 28.01.2022) // Собрание законодательства Российской Федерации. 17.06.1996. № 25, ст. 2954

2. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 30.12.2021, с изм. от 23.09.2021) // Собрание законодательства Российской Федерации. 24.12.2001. № 52 (ч. I), ст. 4921.

Научная и учебная литература

3. Агибалов В.Ю. Виртуальные следы в криминалистике и уголовном процессе: автореф. дис. … канд. юрид. наук: 12.00.09. / В.Ю. Агибалов. – Воронеж, 2010. – 24 с.

4. Вехов В.Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств её обработки: монография / В.Б. Вехов. – Волгоград: ВА МВД России, 2008. – 314 с.

5. Вехов В.Б. Особенности расследования преступлений, совершаемых с использованием средств электронно-вычислительной техники: учеб.-метод. пособие / В.Б. Вехов; 2-е изд., доп. и испр.– Москва: ЦИиНМОКП МВД России, 2000. – 153 с.

6. Гаврилин Ю.В. Расследование неправомерного доступа к компьютерной информации. / Ю.В. Гаврилин, А.В. Пушкин, Е.А. Соцков, Н.Г. Шурухнов. – Москва, 2004. – 127 с.

7. Методика расследования отдельных видов мошенничества: учеб. пособие. – Москва: МосУ МВД России, 2014. – 163 с.

8. Мещеряков В.А. Основы методики расследования преступлений в сфере компьютерной информации: дис. … д-ра юрид. наук: 12.00.09. / В.А. Мещеряков. – Воронеж, 2001. – 375 с.

9. Расследование мошенничеств, совершаемых с использованием мобильной связи: учеб. пособие / авт.-сост. О.П. Грибунов, М.В. Старичков; А.А. Шаевич, О.В. Трубкина, Е.И. Третьякова, В.А. Родивилина. – Иркутск: ВСИ МВД России, 2018. – 157 с.

10. Расследование неправомерного доступа к компьютерной информации: учеб. пособие / под ред. Н.Г. Шурухнова; 2-е изд., доп. и перераб. – Москва: Московский университет МВД России, 2004. – 185 с.

11. Расследование преступлений в сфере компьютерной информации и высоких технологий: учеб. пособие / сост. М.В. Старичков; 2-е изд., перераб. и доп.– Иркутск: ВСИ МВД России, 2014. – 175 с.

12. Семенов Г.В. Расследование преступлений в сфере мобильных телекоммуникаций: дис. … канд. юрид. наук.: 12.00.09. / Г.В. Семенов. – Воронеж, 2003. – 223 с.

13. Безбородов Д.А. Специальные вопросы квалификации преступлений против собственности: учебное пособие / Д.А. Безбородов, А.В. Зарубин, Д.Ю. Краев, А.Н. Попов; под общ. ред. А.Н. Попова. – Санкт-Петербург: Санкт-Петербургский юридический институт (филиал) Университета прокуратуры Российской Федерации, 2019. –164 с.

Практические материалы

14. Архив Озерского городского суда Московской области, уголовное дело № 1-523/2013. URL: https://sudact.ru.

15. О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 // Бюллетень Верховного Суда Российской Федерации. № 2. 2018

16. Определение суда кассационной инстанции Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 29.09.2020 по делу № 12-УДП2О-5-К6: сайт Верховного Суда Российской Федерации. URL: https://legalacts.ru/sud/opredelenie-

sudebnoi-kollegii-po-ugolovnym-delam-verkhovnogo-suda-rossiiskoi-federatsii-ot-29092020-n-12-udp20-5-k6/

17. Определение Судебной коллегии по уголовным делам Первого кассационного суда общей юрисдикции от 23.09.2020 № 77-1775/2020: судебные и нормативные акты Российской Федерации. URL: https://sudact.ru/regular/doc/SIOtt545672r9/ .

18. Пояснительная записка «К проекту Федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации и иные законодательные акты Российской Федерации» (в части дифференциации мошенничества на отдельные составы).

19. Приговор Воскресенского городского суда Московской области от 30.07.2020 № 1-270/2020 по делу № 1-270/2020: судебные и нормативные акты Российской Федерации. URL: https://sudact.ru/regular/doc/SRBxx56elLr9/ .

20. Приговор Домодедовского городского суда Московской области от 06.05.2019 № 1-82/2019 по делу № 1-82/2019: судебные и нормативные акты Российской Федерации. URL: https://sudact.ru/regular/doc/SDBxx50r9/ .

Научные статьи

21. Веремеенко М.В. Объект мошенничества в сфере интернет предпринимательской деятельности / М.В. Веремеенко // Уголовная юстиция. 2014. – С. 6.

22. Давыдов В.О. Значение виртуальных следов в расследовании преступлений экстремистского характера / В.О. Давыдов, А.Ю. Головин // Известия Тульского государственного университета. Экономические и юридические науки. 2016. – № 3-2. – С. 254-259.

23. Зварыгин В.Е. Некоторые вопросы, связанные с определением предмета мошенничества по статье 159 УК РФ / В.Е. Зварыгин, Н.О. Машинникова // Вестник Удмуртского университета. Серия «Экономика и право». 2016. – С. 96.

24. Коломинов В.В. О способе совершения мошенничества в сфере компьютерной информации / В.В. Коломинов // Человек: преступление и наказание. 2015. – № 3 (90). – С. 145-149.

25. Кошаева Т.О. Совершенствование уголовного законодательства об ответственности за мошенничество / Т.О. Кошаева // Журнал российского права. 2018.

26. Машинникова Н.О. Мошенничество. Сущность. Способы совершения / Н.О. Машинникова // European journal of law and political sciences. 2016. – С. 46.

27. Осипенко А.Л. Проблемы соблюдения прав граждан при снятии информации с технических каналов связи в глобальных компьютерных сетях / А.Л. Осипенко, Ж.Т. Сералинов // Актуальные проблемы борьбы с преступностью на современном этапе: тезисы докл. и сообщ. всерос. науч.-практ. конф. – Омск, 2010. – С. 154-157.

28. Рогозина И.Г. Уголовно-правовая политика противодействия преступлениям против собственности / И.Г. Рогозина // Вестник Омской юридической академии. 2016. – № 2.

29. Смолин С.В. Мошенничество в сфере компьютерной информации: проблемы толкования и применения ст. 159 УК РФ / С.В. Смолин // Информационное право. 2015. – № 4.

30. Старичков М.В. Понятие «компьютерная информация» в российском уголовном праве / М.В. Старичков // Вестник Восточно-Сибирского института Министерства внутренних дел России. 2014. – № 1 (68). – С. 16-20.

31. Сударев Л.А. Личность преступника, совершающего компьютерные преступления / Л.А. Сударев // Вестник Московского университета МВД России. – Москва: Московский университет МВД России им. В.Я. Кикотя, 2007. – № 1. – С. 98-103.

32. Сукманов А.О. Сущность, понятие и виды электронно-цифровых следов, используемых в раскрытии и расследовании преступлений / А.О. Сукманов // Вестник Калининградского юридического института МВД России, 2010. – С. 105.

Электронные ресурсы

33. Состояние преступности в Российской Федерации за январь-декабрь 2021 года. URL: https://мвд.рф/reports/item/26023627/.

ПРИЛОЖЕНИЯ

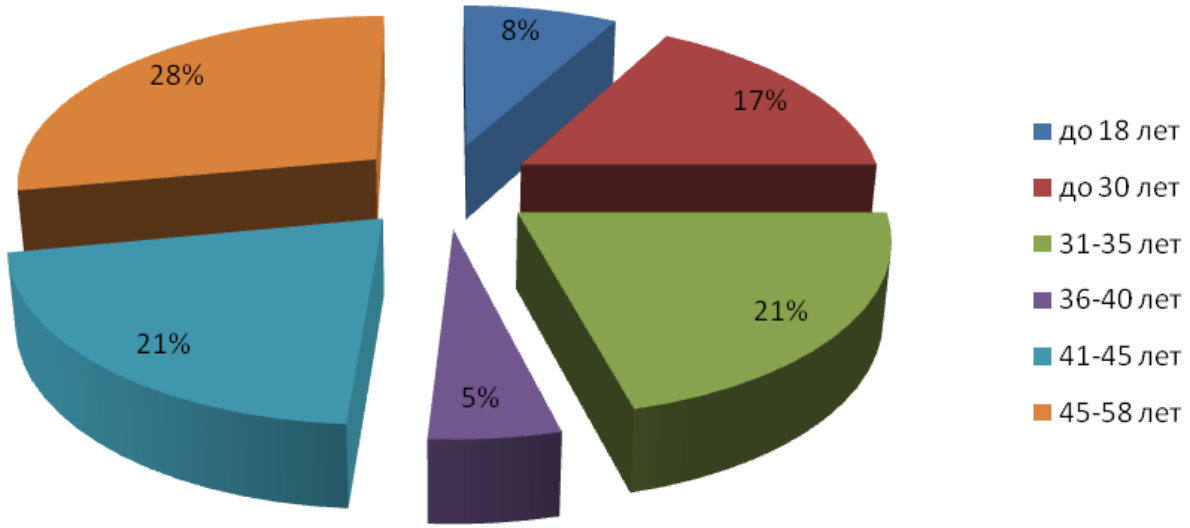
Приложение № 1

Сведения о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, за 2021 год

	ЗАРЕГИСТРИРОВАНО (в отчетном периоде)		в том числе выявленных сотрудниками		
	Всего	+,- в %	следственных органов Следственного комитета Российской Федерации	органов внутренних дел	органов Федеральной службы безопасности
Всего преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации	**517722**	**1,4**	**1492**	**511300**	**2614**
из них					
тяжких и особо тяжких	288312	7,7	1031	284704	1322
в том числе совершенных с использованием или применением:					
расчетных (пластиковых) карт	165658	-12,9	293	164666	96
компьютерной техники	27519	-4,0	161	26160	762
программных средств	7216	-28,2	51	6686	378
фиктивных электронных платежей	954	-30,6	20	905	23
сети "Интернет"	351463	17,0	1031	347189	1811
средств мобильной связи	217552	-0,5	330	216252	450
в том числе					
кража ст. 158 УК РФ	156792	-9,6	381	155760	29
мошенничество ст.ст. 159, 159.3, 159.6 УК РФ	249249	5,1	95	248497	201
из них					
мошенничество ст. 159 УК РФ	238560	13,3	91	237832	195
мошенничество с использованием электронных средств платежа ст. 159.3 УК РФ	10258	-60,3	4	10237	4
мошенничество в сфере компьютерной информации ст. 159.6 УК РФ	431	-43,4	0	428	2
незаконные организация и проведение азартных игр ст. 171.2 УК РФ	614	-17,8	11	557	41
публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма ст. 205.2 УК РФ	315	35,8	1	141	164
незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества ст. 228.1 УК РФ	51444	9,3	333	50296	548
изготовление порнографических материалов ст. 242, 242.1, 242.2 УК РФ	2299	9,5	111	2152	3
публичные призывы к осуществлению экстремистской деятельности ст. 280 УК РФ	455	33,8	0	224	219
преступления в сфере компьютерной информации глава 28 УК РФ	6869	52,7	30	6273	435
в том числе					
неправомерный доступ к компьютерной информации ст. 272 УК РФ	6392	55,7	22	5965	277
создание, использование и распространение вредоносных компьютерных программ ст. 273 УК РФ	317	-14,6	4	229	81

Приложение № 2

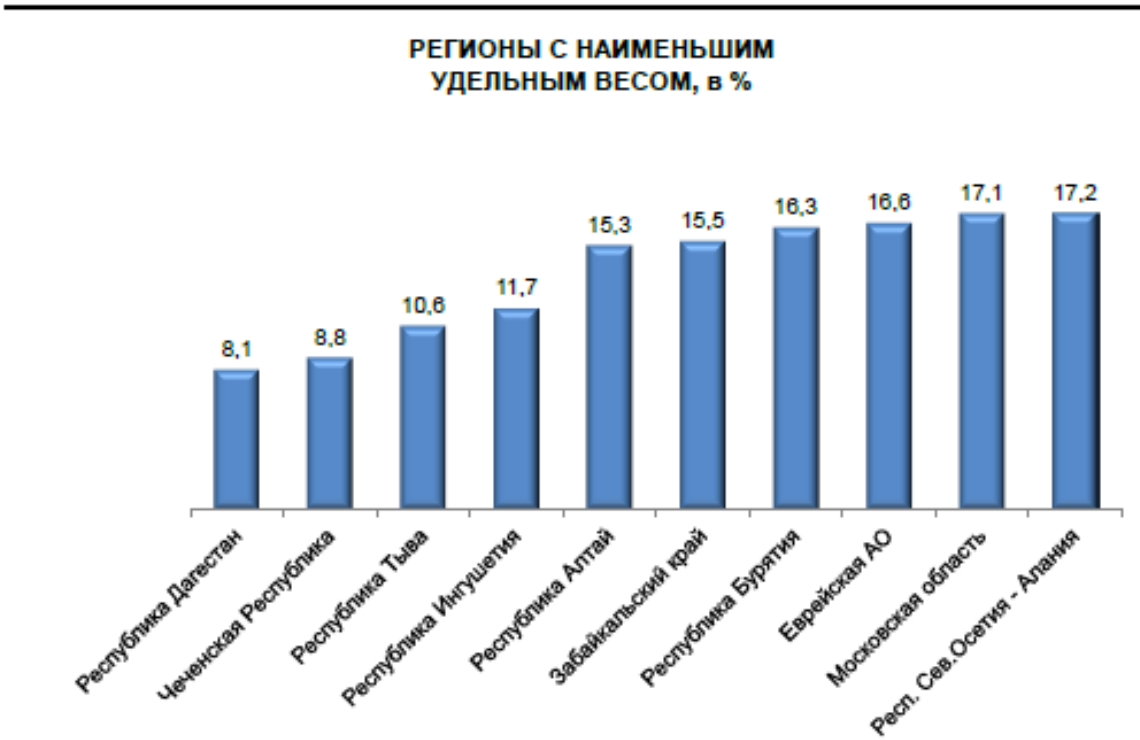
Возрастная градация жертв мошенничества, совершенного с использованием цифровых технологий, в 2019-2020 годах %[1]



[1] Старостенко Олег Александрович. Виктимологическая характеристика мошенничества, совершаемого с использованием информационно-телекоммуникационных технологий// Гуманитарные, социально-экономические и общественные науки. 2020. № 5. URL: https://cyberleninka.ru/article/n/viktimologicheskaya-harakteristika-moshennichestva-sovershaemogo-s-ispolzovaniem-informatsionno-telekommunikatsionnyh-tehnologiy (дата обращения: 03.03.2022).

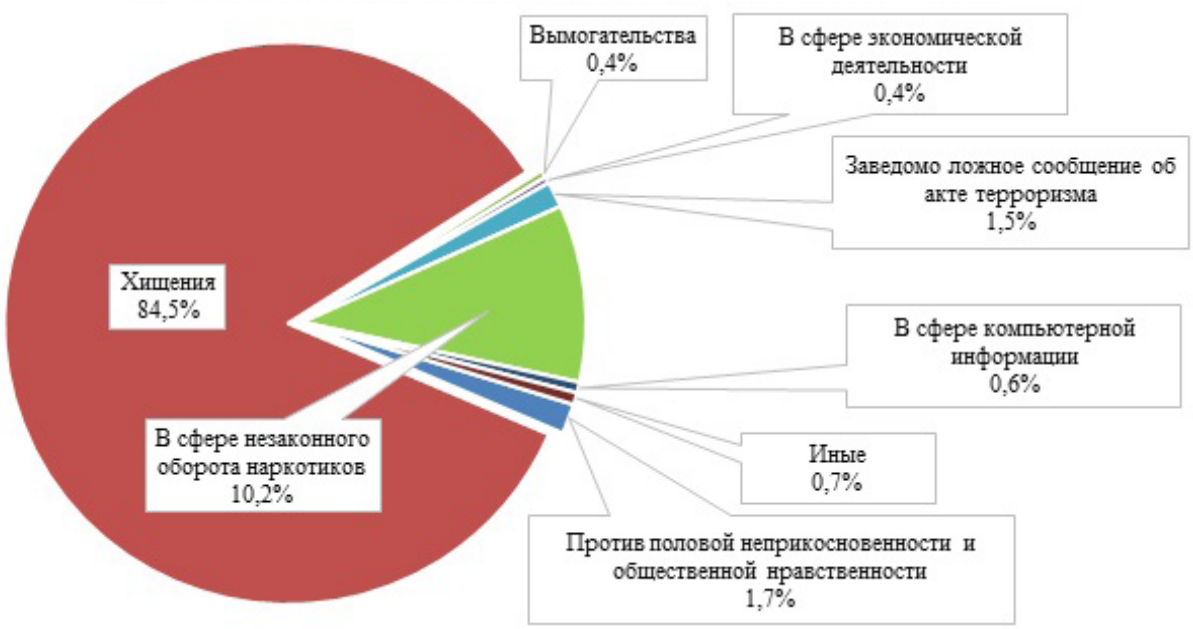
Приложение № 3

Удельный вес преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, (в общей структуре преступности) за 2021 год



Приложение № 4

Структура преступлений, совершаемых с использованием информационно-телекоммуникационных технологий



Учебное издание

Гарипов Тимур Ильгизович

Доказывание по уголовным делам о преступлениях, совершенных с использованием современных информационно-телекоммуникационных технологий

Учебное пособие

Корректура, верстка О.В. Добрыдневой

Формат 60*84 1/16
Усл. печ. л. 6
Дата подписания в печать 28.11.2022
Тираж 50 экз.

Типография КЮИ МВД России
420059, г. Казань, ул. Оренбургский тракт, 130