Министерство внутренних дел Российской Федерации

Федеральное государственное казенное образовательное учреждение
высшего образования «Казанский юридический институт
Министерства внутренних дел Российской Федерации»

Кафедра криминалистики

ДИПЛОМНАЯ РАБОТА

на тему: «Проблемы расследования мошенничества в сфере компьютерной информации»

Выполнил: Кузнецов Адель Ленарович

40.05.01 – Правовое обеспечение национальной безопасности, год набора – 2018, 181 учебная группа

Руководитель
доцент, доцент кафедры криминалистики
кандидат юридических наук, доцент
полковник полиции
Миролюбов Сергей Леонидович

Рецензент:
Заместитель начальника ГСУ МВД по Республике Татарстан – начальник СЧ ГСУ МВД по Республике Татарстан
полковник юстиции,
Хайруллин Тимур Ильгизарович

Оценка _____

Дата защиты:"____"_____20___г.

Казань 2023

СОДЕРЖАНИЕ

ВВЕДЕНИЕ 3
ГЛАВА 1. УГОЛОВНО-ПРАВОВАЯ И КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ 8
§1. Уголовно-правовая характеристика 8
§2. Криминалистическая характеристика 16

ГЛАВА 2. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЕ ПОЛОЖЕНИЯ РАССЛЕДОВАНИЕ МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ 29
§1. Программа действий на этапе проверки сообщения о преступлении и возбуждения уголовного дела 29
§2. Особенности производства следственных действий и оперативно-розыскных мероприятий на первоначальном этапе 35
§3. Последующий этап расследования 42

ГЛАВА 3. ТАКТИЧЕСКИЕ ОСОБЕННОСТИ ПРОВЕДЕНИЯ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ 46
§1. Тактические особенности проведения допроса 46
§2. Тактические особенности назначения и производства судебных экспертиз 54

ЗАКЛЮЧЕНИЕ 60
СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ 66
ПРИЛОЖЕНИЯ 74

ВВЕДЕНИЕ

Актуальность темы исследования. Компьютеризация ознаменовала новую эпоху научно – технического прогресса. Все новейшие изобретения создавались с целью упростить жизнь человека в современном обществе, сделать его наиболее мобильным и оперативным. Но, как известно, у каждого прогресса есть как положительные стороны, так и отрицательные. В данном случае, это появление нового вида противоправных деяний, преступлений в сфере компьютерной информации. Данный вид противоправного деяния имеет свою специфику, как по механизму его совершения, так и по его способам. Однако, преступления в сфере компьютерной информации характеризуются большой латентностью и низкой раскрываемостью, что способствует увеличению количества деяний и совершенствование навыков лиц их совершающих.

Все больше и больше данных содержится и обрабатывается в компьютерных информационных системах. Применение компьютерных технологий в целях обработки и обмена данными между различными пользователями информационного пространства практически во всех сферах жизни общества является положительным моментом, соответствующим требованиям времени. В данном контексте возникает две точки зрения: первая – информационное пространство и компьютерные технологии дают возможность совершенствовать социально-экономические процессы на современном этапе развития общества в процессе цифровизации; вторая – появилась киберпреступность.

В настоящее время разнообразные государственные и негосударственные организации содержат большое количество разнообразных сведений на электронных носителях, в том числе о конкретных физических лицах, деятельности и иных данных, а также перемещениях в пространстве, проводимых операциях, банковских и иных финансовых операциях, наличии движимого имущества и недвижимость и многое другое. На первый взгляд,

популяризация электронных (информационных) баз данных и компьютеризация жизнедеятельности общества и населения должны только позитивно сказаться на развитии общества в целом. Для преступников незаконное приобретение сведений любого характера «развязывает им руки» для совершения преступлений из корыстных целей, мотивов и (или) побуждений.

Следует отметить, что борьба с преступлениями, предусмотренными ст. 159.6 Уголовного-кодекса Российской Федерации (далее – УК РФ)«Мошенничество в сфере компьютерной информации» будет эффективной только в том случае, если правоохранительные органы будут вооружены научными регламентами и разработанными на их основе практическими рекомендациями по расследованию исследуемого вида преступления. Сегодня следователи, дознаватели и сотрудники оперативных подразделений в своей профессиональной деятельности руководствуются методическими рекомендациями по расследованию компьютерных преступлений. Уровень эффективности данных методических рекомендаций остается под вопросом, поскольку на сегодняшний день сотрудники органов внутренних дел испытывают весьма серьезные трудности в процессе расследования преступлений, предусмотренных ст. 159.6 УК РФ. Частично это связано с отсутствием профессиональной подготовки следователей, дознавателей, оперативников в процессе раскрытия и расследования данного вида преступления.

Согласно статистическим данным за 2019-2022 гг. в России было зарегистрировано: 687, 761, 431, и 334 преступлений соответственно по ст. 159.6 УК РФ (приложение 1)[1].

Итак, актуальность настоящей дипломной работы обусловлена тем, что в настоящее время возникают некоторые трудности в процессе расследования преступлений, предусмотренных ст. 159.6 УК РФ, которые предстоит рассмотреть в процессе исследования выбранной темы дипломной работы.

---

[1] Состояние преступности в Российской Федерации. URL: https://xn--b1aew.xn--p1ai/dejatelnost/statistics (дата обращения: 17.09.2022).

Целью настоящей дипломной работы является комплексное исследование проблем, возникающие в процессе расследования мошенничеств в сфере компьютерной информации.

Для достижения поставленной цели, необходимо решить следующие **задачи**:

– рассмотреть уголовно-правовую характеристику;

– проанализировать криминалистическую характеристику;

– исследовать программу действия на этапе проверки сообщения о преступлении и возбуждения уголовного дела;

– проанализировать особенности производства следственных действий и оперативно-розыскных мероприятий на первоначальном этапе;

– рассмотреть последующий этап расследования;

– проанализировать тактические особенности проведения допроса;

– изучить тактические особенности назначения и производства судебных экспертиз.

Объектом настоящей дипломной работы выступают общественные отношения, возникающие при расследовании преступлений, предусмотренных ст. 159.6 УК РФ.

Предметом настоящей дипломной работы выступают закономерности осуществления преступной деятельности путем мошенничества в сфере компьютерной информации, закономерности возникновения информации о ней и ее участниках, закономерности собирания, исследования и использования этой криминалистически значимой информации в процессе расследования уголовных дел по фактам совершения преступлений, предусмотренных ст. 159.6 УК РФ.

Методологическая основа исследования включает в себя систему идей научного познания, а именно: универсально-методологический диалектический метод и структурно-системный подход; общенаучные методы познания: анализ, синтез, индукция, дедукция, сравнение, общение, и частнонаучные методы познания: уголовно-статистический, изучение нормативно-правовых актов,

результаты авторского социологического исследования.

Нормативная база исследования включает в себя: Конституцию Российской Федерации; нормы международно-правовых актов; Уголовный кодекс Российской Федерации; Уголовно-процессуальный кодекс Российской Федерации и иные нормативно-правовые акты России, регулирующие вопросы раскрытия и расследования мошенничества в сфере компьютерной информации.

Эмпирическая основа включает в себя: материалы правоприменительной практики, статистические данные Министерства внутренних дел Российской Федерации, Генеральной прокуратуры Российской Федерации, Судебного департамента при Верховном суде Российской Федерации и иных правоохранительных органов.

Степень научной разработанности проблемы. Различными аспектами исследования проблем, возникающих в процессе расследования мошенничества в сфере компьютерной информации занимались такие авторы, как: Н.А. Аменицкая, Д.А. Влезько, И.А. Возгрин, Н.Н. Егоров, В.М. Журавлев, Н.Д. Иващенко, Е.П. Ищенко, Казанцев С.Я., В.В. Коломинов, Е.Р. Россинская, А.А. Топорков, А.Г. Филиппов и др.

Апробация и внедрение в практику результатов исследования. Основные положения исследования отражены в исследованиях и выступлениях на международных и всероссийских научно-практических мероприятиях:

1. Всероссийский круглый стол «Цифровые активы: правовое регулирование и перспективы развития в условиях цифровизации гражданского оборота» (КЮИ МВД России, 2023) – Электронные средства платежа: возможности и риски их использования в противоправных целях;

2. Всероссийский научно-практический семинар «Основы кибербезопасности» (КЮИ МВД России, 2023) – Проблемы расследования мошенничества в сфере компьютерной информации.

Структура настоящей дипломной работы. Работа состоит из введения, трех глав, включающих в себя семь параграфов, заключения, списка использованной литературы.

ГЛАВА 1. УГОЛОВНО-ПРАВОВАЯ И КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

§1. Уголовно-правовая характеристика

Современный этап общественного развития связан с повсеместным проникновением и использованием сети Интернет. Однако вместе с явными преимуществами, такими, как мгновенный доступ к информации, возможность онлайн оплаты товаров и практически любых видов услуг, условия для мгновенной и беспрепятственной коммуникации с любой точкой мира, развитие сети Интернет несет и глобальные угрозы, снижающие экономическую безопасность государства. Одной из таких угроз, является Интернет-мошенничество, которое развивается вместе с глобальной сетью[1].

Исследование проблем противодействия экономической преступности показывает, что соответствующие правовые институты функционируют неэффективно, создают серьезные препятствия на пути дальнейшего улучшения благополучия общества. Наблюдается системное запаздывание со стороны законодателя с адекватной правовой оценкой динамики имущественных отношений. В отдельных случаях законодательные новеллы принимаются без социально-экономической обоснованности и достаточной научной проработанности, законодатель не учитывает реальную обстановку, руководствуется интересами отдельных групп лиц. Повышение эффективности правового регулирования института имущественных отношений, таким образом, является серьезной проблемой для законодателя.

Криминализация имущественных отношений, оказывая негативное влияние на экономику, принуждает законодателя расширить сферу уголовно-правового воздействия. В этих условиях и с учетом массового характера проявления злоупотреблений в сфере имущественных отношений возникла

[1] Иващенко Н.Д. Мошенничество в сфере компьютерной информации: проблемные вопросы // Столица науки. 2020. № 6 (23). С. 269-276.

острая необходимость обобщения национального, зарубежного опыта законодательной регламентации ответственности за преступления против собственности. Экономическая безопасность как сложная категория может быть обеспечена различными формами практической деятельности человека. В частности, к ним можно отнести законотворческую и правоприменительную форму[1].

Мошенничество – одно из самых распространенных способов преступной деятельности. Как правило, мошенничеством признается хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.

На наш взгляд, следует рассмотреть уголовно-правовую характеристику мошенничества в сфере компьютерной информации. В настоящем исследовании большой интерес представляет мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ), под которым следует понимать хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей[2].

Традиционно, обязательными признаками состава любого преступления являются объективная сторона, субъективная сторона, объект и субъект. Рассмотрим данные признаки поподробнее.

Пределы действия статьи 159.6 УК РФ устанавливаются, в том числе, посредством толкования специальных терминов, с помощью которых описана объективная сторона деяния.Общественная опасность противоправных действий в области электронной техники и информационных технологий

[1]Абдульмянова Т.В., Фролкина И.А. Предупреждение мошенничества в сфере материнского капитала // Вопросы российского и международного права. 2018. № 10. С. 139-144.

[2] Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 № 63-ФЗ (ред. от 01.07.2021) (с изм. и доп., вступ. в силу с 01.12.2021) // Российская газета. 1996. № 113-115.

выражается в том, что они могут повлечь за собой нарушение деятельности автоматизированных систем управления и контроля различных объектов, серьезное нарушение работы ЭВМ и их систем, несанкционированные действия по уничтожению, модификации, искажению, копированию информации и информационных ресурсов, иные формы незаконного вмешательства в информационные системы, которые способны вызвать тяжкие и необратимые последствия, связанные с имущественным ущербом.

Объективная сторона преступления, предусмотренного ст. 159.6 УК РФ характеризуется действием в целях хищение чужого имущества; приобретение права на чужое имущество. Способ совершения: обман посредством ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

По смыслу статьи 159.6 УК РФ вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей признается целенаправленное воздействие программных и (или) программно-аппаратных средств на серверы, средства вычислительной техники (компьютеры), в том числе переносные (портативные) – ноутбуки, планшетные компьютеры, смартфоны, снабженные соответствующим программным обеспечением, или на информационно-телекоммуникационные сети, которое нарушает установленный процесс обработки, хранения, передачи компьютерной информации, что позволяет виновному или иному лицу незаконно завладеть чужим имуществом или приобрести право на него.

Мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных

компьютерных программ, требует дополнительной квалификации по статье 272, 273 или 274.1 УК РФ[1].

Диспозиция комментируемой нормы имеет бланкетный характер, следовательно, ее применению должен предшествовать факт установления конкретной нормативной базы, регламентирующей отношения виновного и потерпевшего в области компьютерных технологий. Поскольку таковые образуют область специальных познаний, то предъявлению обвинения по комментируемой статье должно предшествовать проведение соответствующих технических экспертиз.

Обязательным признаком исследуемого вида преступления является способ совершения преступления[2].Согласно материаламправоприменительной практики по уголовным делам, предусмотренных ст. 159.6 УК РФ, выделяются несколько способов преступных действий:

1) взлом с последующим хищением данных;

2) оформлениебанковских карт с применениемкраденныхданныхжертвы;

3) кремминг;

4) «инвестиционные копилки»;

5) покупка акций по минимальной цене и распространение заведомо ложные сведения о юридическом лице через информационное пространстводлясозданиябольшого спроса на них, ссылаясь на обладание секретной информацией о важном корпоративном событии;

6) использование электронных платежных средств (*WebMoney*, Яндекс.Деньги, *Assist*, *Robox*, *Qiwi*и др.);

7) спуффинг-атаки[3];

8) псевдоблаготворительность.

---

[1] О судебной практике по делам о мошенничестве, присвоении и растрате: Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 // Российская газета. 2017. № 280.

[2] Кулешова Н.Н., Христофорова Е.И. Особенности квалификации мошенничества в сфере компьютерной информации // Вопросы науки и образования. 2014. № 18. С. 43.

[3]Коломинов В.В. Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа: дис. … канд. юрид. наук. Иркутск, 2017. С. 12.

Преступление признается оконченным с момента получения виновным суммы денег (чужого имущества), а равно приобретения им юридического права на распоряжение такими деньгами (имуществом).

Общим объектом исследуемого вида преступления выступает вся совокупность общественных отношений, охраняемая уголовным законодательством.

Родовой объект исследуемого вида преступления – общественные отношения в сфере экономики.

Видовой объект исследуемого вида преступления – общественные отношения в области собственности.

Объект анализируемого преступления полностью совпадает с родовым объектом хищения – это общественные отношения, сложившиеся в сфере электронного документооборота. Как и мошенничество вообще, квалифицированное мошенничество в сфере компьютерных технологий – всегда хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.

Предметом преступления становится чужое имущество, хищение или приобретение права, на которое осуществляется путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

К предмету данного преступления законодатель отнес чужое имущество и право на чужое имущество. В этом случае повторяется диспозиция общей статьи об ответственности за мошенничество, хотя такой подход неоднократно подвергался критике. Право на имущество в полном смысле слова не является предметом преступления, а лишь предполагает возникновение субъективного права владеть, пользоваться и распоряжаться имуществом. Тем более что момент окончания преступления в этом случае связан лишь с государственной регистрацией, что не соответствует общепринятому моменту окончания

хищения. Было бы лучше предусмотреть специальную норму с приобретением права на имущество путем обмана или злоупотребления доверием. Дополнительным предметом преступления является компьютерная информация, с помощью которой виновный осуществляет обманные действия и завладевает имуществом или приобретает право на имущество. Поэтому незаконный доступ к охраняемой компьютерной информации и иные незаконные действия в данной сфере требуют квалификации по совокупности со ст. ст. 272 или 273 УК.

Субъективная сторона мошенничества в сфере компьютерной информации «выражается форме прямого умысла. Виновное лицо осознает, что завладение чужим имуществом или правами на него производится путем ввода, удаления, блокирования, модификации компьютерной информации либо иным вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей». Тем не менее, указанные выше обстоятельства не обязательно могут означать наличие признаков состава мошенничества в сфере компьютерной информации. Каждый конкретный случай должен быть объективно устанавливать, что лицо, совершившее определенные в диспозиции статьи 159.6 УК РФ действия, заведомо намеревалось использовать полученную информацию в корыстных целях.

Субъективную сторону мошенничества в сфере компьютерной информации образует прямой умысел на завладение чужим имуществом посредством незаконного вторжения в функционирование средств компьютерной информации[1].

Так, Абдурахманова А.О. 17 июня 2018 г. получила от своего племянника Магомедова А.Р. мобильный телефон, который последний нашел возле скамейки в центральном парке города Кизилюрт Республики Дагестан, после

[1]Абдульмянова Т.В., Асанова И.П., Данилов В.В. Мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ): понятие, уголовно-правовая характеристика и некоторые особенности расследования // Вопросы российского и международного права. 2021. Т. 11. № 1-1. С. 134-145.

чего, обнаружив, что к данному мобильному телефону привязаны банковские карты ПАО «Сбербанк» открытые на имя Гаджиева Р.Э., у себя на работе, 17 июня 2018 года и 13 июля 2018 года путем вмешательства в функционирование средств хранения компьютерной информации, посредством использования возможностей мобильного приложения «Сбербанк-Онлайн», совершила операции по переводу денежных средств в размере 8800 рублей со счета банковской карты «Сбербанк-Маэстро» и денежных средств в размере 8000 рублей со счета банковской карты «Сбербанк-Мир» на счет своей банковской карты, тем самым похитила с расчетного счета Гаджиева Р.Э. денежные средства на общую сумму 16 800 рублей, чем причинила последнему значительный материальный ущерб.

Кизилюртовский городской суд Республики Дагестан 4 июля 2019 года признал Абдурахманову А.О. виновной в совершении преступления, предусмотренного п. «в» ч. 3 ст. 159.6 УК РФ – мошенничество в сфере компьютерной информации, то есть хищение чужого имущества путем вмешательства в функционирование средств хранения по квалифицирующему признаку – с банковского счета[1].

По делу № 1-95/2019 преступник гр. «Л.Р.В.» совершил мошенничество в сфере компьютерной информации. Гр. «Л.Р.В.» преследовал следующую цель: нарушение характеристик защищаемых объектов путем модификации, разрушения или блокирования программных и технических средств, ознакомления с защищаемой информацией, а также навязывания ложной информации или побуждения к принятию неверных решений. Следует отметить, что преступник руководствовался корыстными мотивами[2].

Субъектом преступления признается физическое вменяемое лицо, достигшее 16 лет.

---

[1] Приговор Кизилюртовского городского суда Республики Дагестан от 04.07.2019 г. по делу № 1-67/2019. URL: https://clck.ru/sJy8r (дата обращения: 13.09.2022).

[2] Приговор Октябрьского районного суда г. Владимира № 1-95/2019 от 4 июня 2019 г. по делу № 1-95/2019. URL: https://sudact.ru/regular/doc/v59eyhN7lzJq/ (дата обращения: 13.09.2022).

Субъект преступления, предусмотренный статьей 159.6 УК РФ – общий – дееспособное лицо, достигшее возраста шестнадцати лет. Тем не менее, следует специально отметить, что ч. 3 ст. 159.6 УК РФ, ч. 4 ст. 159.6 УК РФ (деяния, предусмотренные ч. 1, ч.2 или ч. 3 ст. 159.6 УК РФ, совершенные организованной группой либо в особо крупном размере) – для особо квалифицированных составов данного преступления – предусмотрен также и специальный субъект. В качестве специального субъекта выступает лицо, обладающее определенным служебным положением. Так, например, приговором суда Т.В., К. и К. были признаны виновными в совершении мошенничества в сфере компьютерной информации, <…>, организованной группой, в особо крупном размере, а Т.В. также с использованием своего служебного положения. Т.В., ранее не судимый, осужден по ст. 159.6 ч. 4 УК РФ к 6 годам лишения свободы в исправительной колонии общего режима[1].

Следует отметить, что сотрудники правоохранительных органов и суды, в процессе квалификации преступных действий, основываются на положениях Постановления Пленума Верховного Суда РФ от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате». Так, по смыслу статьи 159.6 УК РФ вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей признается целенаправленное воздействие программных и (или) программно-аппаратных средств на серверы, средства вычислительной техники (компьютеры), в том числе переносные (портативные) – ноутбуки, планшетные компьютеры, смартфоны, снабженные соответствующим программным обеспечением, или на информационно-телекоммуникационные сети, которое нарушает установленный процесс обработки, хранения, передачи компьютерной информации, что позволяет

[1] Постановление Апелляционного суда г. Севастополя № 44Г-185/2018 4Г-482/2018 от 30 мая 2018 г. по делу № 2-1155/2017. URL: https://sudact.ru/regular/doc/vSzadn3t6sgj/ (дата обращения: 13.09.2022).

виновному или иному лицу незаконно завладеть чужим имуществом или приобрести право на него.

Мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по статье 272, 273 или 274.1 УК РФ[1].

§2. Криминалистическая характеристика

Криминалистическая характеристика преступлений – важный институт криминалистической методики, в классическом понимании являющийся информационной основой расследования преступлений определенного вида либо группы. Вместе с тем, мнения ученых по поводу места криминалистической характеристики преступлений в структуре частных методик расследования неоднозначны.

И.А. Возгрин под криминалистической характеристикой преступления понимает состояние и меры по предупреждению и борьбы с различными видами преступных посягательств[2].

Криминалистическая характеристика преступлений – актуальный, самостоятельный и востребованный наукой и практикой институт криминалистической методики, представляющий собой систему криминалистически значимой, взаимосвязанной информации о признаках и свойствах преступлений определенного вида либо группы, полученной в результате анализа и обобщения судебно-следственной практики, служащей основанием для выдвижения версий и необходимой для правильной оценки

---

[1] О судебной практике по делам о мошенничестве, присвоении и растрате: Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 // Справ.-правовая система «Гарант» (дата обращения: 12.03.2023).

[2]Возгрин И.А. Общие положения методики расследования отдельных видов преступлений / под ред. И.А. Возгрин. М., 2016. С. 95.

ситуаций, складывающихся в процессе раскрытия и расследования преступлений.

Криминалистическую характеристику преступлений следует рассматривать в качестве первого элемента в структуре частной методики расследования, т. к. вычленение ее из данной структуры ведет к разрыву устоявшихся логических взаимосвязей – рассмотрение каждой криминалистической характеристики преступлений определенного вида либо группы отдельно от методики (комплекса рекомендаций) по их расследованию не только не будет способствовать системности восприятия даже самого ценного научно-практического материала, но и неизбежно повлечет сложности в практическом применении той или иной частной методики[1].

Криминалистическая характеристика преступлений как информационная база частных методов расследования также должна исследоваться как часть системы криминалистической поддержки при раскрытии и расследовании определенных видов преступлений. Под криминалистической характеристикой преступлений мы понимаем информационную модель, которая отражает криминалистическую природу конкретного типа преступления, состоящую из информации об их криминалистически значимых свойств и их естественных отношениях друг с другом, на основе анализа и обобщения практики их раскрытия, расследования и судебного разбирательства важна и для развития частных следственных методов.

В криминалистике среди ученых-криминалистов сложились определенные элементы криминалистической характеристики преступлений, к котором относятся:

– способ совершения преступного посягательства;

– обстановка преступного посягательства;

– сведения о предмете;

---

[1]Шруб М.П. Криминалистическая характеристика преступлений - фантом или информационно-поисковая основа расследования? // Вопросы криминологии, криминалистики и судебной экспертизы. 2020. № 2(48). С. 31-36.

– механизм следообразования;

– сведения о личности преступника и жертвы.

Рассмотрим каждый элемент криминалистической характеристики более подробно.

Способ совершения преступления, предусмотренного ст. 159.6 УК РФ.

Профессор Е. Р. Россинская указывает на то, что «способы компьютерных преступлений являются полноструктурными, причем могут быть выбраны различные технологии подготовки, совершения и сокрытия, слабо коррелирующие с видом преступления»[1]. Под способом совершения преступления понимается взаимосвязанная система действий, которые направленны на подготовку, совершение и сокрытие следов преступного посягательства, связанного с особенностями личности преступника и внешними условиями[2].Л.Н. Симанович в своих трудах говорит, что способ совершения преступления – это конкретный комплекс в субъективных и объективных аспектах, а также содержание действий и методов, которые используют вымогатели, их цели, подготовительные действия и способы сокрытия преступного деяния[3].

Следующим, немаловажным элементом криминалистической характеристики преступления – *обстановка преступного посягательства*.Под обстановкой понимается система объектов, явлений и процессов, которые взаимодействуют между собой до и во время совершения преступления. Обстановка характеризуется временем, местом, климатическим, бытовым, производственным, материальным и другими условиями, спецификой поведения косвенных участников события, спецификой психологического

[1]Россинская Е.Р. Концепция учения об информационно-компьютерных криминалистических моделях как основе методик расследования компьютерных преступлений // Вестник Восточно-Сибирского института МВД России. 2021. № 2 (9). С. 195.

[2]Маазов М.М. Криминалистическая характеристика преступления // Проблемы совершенствования законодательства : сборник научных статей студентов юридического факультета. Махачкала : ООО «АЛЕФ», 2019. – С. 368-370.

[3]Симанович Л.Н. Криминалистическая характеристика вымогательства // Законность. 2016. № 4. С. 17.

взаимодействия между ними, а также другие факторы, влияющие на условия, возможность и другие обстоятельства преступления.

Для подготовки и сокрытия рассматриваемых в данной статье преступлений злоумышленниками используются зачастую те же методы, что и при других видах преступлений (незаконный оборот наркотических средств, организация террористических актов, незаконный оборот огнестрельного оружия, экстремизм и др.) – специальные программно-аппаратные средства для уничтожения значимой для следствия информации при попытке доступа к ней третьих лиц, обеспечения преступником анонимности своих действий в сети Интернет с использованием цепочки прокси-серверов (*VPN*-технологии), подменой номера телефона.

Сходным по способу совершения способ сокрытия следов за счет инсценировки совершения действий самим потерпевшим является и «фарминг». При данном способе используется возможность переадресации с официальных сайтов организации на их мошеннические копии, где преступники и получают необходимые им данные[1]. Внешне это выглядит как действия совершенные потерпевшим, порой совершенные неудачно, например, при попытке заказать товар. Нередко подобные способы используются при создании копий сайтов для заказа билетов, предполагающих введение персональных данных пассажира. Взаимодействие с мошенническим сайтом, который может существовать в сети непродолжительное время либо просто больше не использоваться преступниками, не позволяет достоверно установить, кто именно получил запрошенную информацию, а затем воспользовался ею для своих преступных целей.

Сокрытие следов преступления существенно облегчается в том случае, когда речь идет о групповом совершении преступления, а в особенности при совершении кибермошенничества в составе организованной группы, когда

[1] Новые способы совершения преступлений в сфере информационных технологий на территории государств – участников СНГ: аналитический обзор / под ред. И. Б. Колчевский, В. М. Журавлев, А. Г. Кузнецов и [др.]. М.: ФГКУ «ВНИИМВДРоссии», 2018. С. 34.

обеспечивается анонимность руководящих лиц. В результате непосредственные исполнители, которые чаще выявляются правоохранительными органами, ничего не могут сообщить о составе преступной группы, о ее руководстве, масштабах действий и так далее. Причина этого во многом обусловлена спецификой преступлений, а именно, сложностью способов их совершения за счет применения различных приемов сокрытия следов преступлений[1].

Чтобы проиллюстрировать правильность приведенных выше утверждений, необходимо обратиться к анализу судебной правоприменительной практики. По уголовному делу № 1-218/2018, рассмотренному Железногорским городским судом Курской области, преступник, имея правомерный доступ в базам данных сотового оператора в силу того, что являлся его сотрудником, изготавливал поддельные заявления владельцев sim-карт о замене карты[2]. Тем самым он желал создать впечатление, что переводы средств со счетов осуществлялись непосредственно самими правообладателями.

Сходный способ сокрытия следов преступления был применен преступником по делу № 1-345/2019, рассмотренному Кировским районным судом города Ростована-Дону[3]. Однако здесь преступник не только создавал видимость обращения обладателей sim-карт с просьбой о их замене, но и постарался уничтожить информацию непосредственно в системе сотового оператора, чтобы невозможно было установить дату внесения изменений в сведения и даты списания средств со счетов клиентов.

---

[1]Polyakov V. (2019). Criminalistics specifics of methods of committing computer crimes and peculiarities of their prevention. Religacion. Journal of Social Sciences and Humanities. Vol. 4 (21). pp. 90-97.

[2]ПриговорЖелезногорскогогородскогосудаКурскойобластиот 15.10.2018. Уголовноедело № 1-218/2018. URL: https://sudact.ru/regular/doc/BTGs3iNkWxUw/?regular-txt=&regular-case_doc=1-218%2F2018&regularlawchunkinfo=&regular-date_from=&regular-date_to=&regular-workflow_stage=&regular-area=&regularcourt=Железногорский+городской+суд+%28Курская+область%29&regular-judge=&_=1607011682180 - (25.11.2020).

[3] Приговор Кировского районного суда г. Ростова-на-Дону от 13.09.2019. Уголовное дело № 1- 345/2019. URL: https://sudact.ru/regular/doc/LkG0QbZcSoNb/ (30.09.2022).

В число достоверно установленных способов сокрытия следов преступления вошли такие, как:

1) использование устройств, не идентифицированных в ходе следствия;

2) изготовление поддельных заявлений владельцев sim-карт о замене карты с целью придания действиям вида правомерных;

3) использование чужого логина и пароля для доступа к базе данных. Использование вымышленные персональных сведений для регистрации sim-карт, на счета которых переводились денежные средства;

4) создание иных подложных документов с целью придания операциям вида правомерных;

5) использование вредоносного программного обеспечения;

6) перечисление денежных средств на счета третьих лиц, непосредственно не вовлекаемых в совершение преступления и не осведомленных о неправомерном способе получения денежных средств;

7) удаление сведений о сообщениях, связанных с перечислением средств непосредственно из телефона потерпевшего[1].

Особое значение рассматриваемым преступлениям придает тот факт, что они зачастую совершаются группой лиц. Именно данное обстоятельство значительно затрудняет их расследование и определяет его специфику. Как правильно отмечает Н. П. Яблоков, любая преступная группа не является простым механическим сложением некоего числа лиц, совместно совершающих преступление. Каждая преступная группа, с точки зрения психологии и социологической теории «малых групп», объединяя на основе совместного осуществления общественной опасной деятельности нескольких человек, стремящихся к достижению единой преступной цели, с той или иной

[1] Ширяев А.В. Способы сокрытия следов мошенничества в сфере компьютерной информации // Проблемы правовой и технической защиты информации. 2020. Вып. VIII. С. 126-127.

степенью организованности, с устоявшимися межличностными отношениями, фактически превращается в единый субъект криминальной деятельности[1].

Отличительным свойством места совершения мошенничества в сфере компьютерной информации выступает удалённость, нередко на значительные расстояния, места совершения общественно опасных деяний от места возникновения последствий. Вэтой связи 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.

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 ит.п.);

– место, нахождение 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.).

Сведения о предмете преступного посягательства.

Предмет преступления играет немаловажную роль в уголовном праве, процессе и криминалистике. Выяснение характера и размера причиненного преступлением ущерба, отграничение смежных преступных деяний друг от

[1]Родивилин В.А., Коломинов В.В. Криминалистическая характеристика отдельных видов преступлений, совершенных с использованием информационно-телекоммуникационных технологий // Криминалистика: вчера, сегодня, завтра. 2022. № 1(21). С. 117.

друга и даже отграничение преступного деяния от непреступного зависит по большому счету от правильного установления предмета преступления.

По мнению некоторых авторов, под предметом исследуемого вида преступления следует понимать:

1) компьютерная информация (именно на нее сперва посягает преступник, и, изменив, удалив или заблокировав ее, мошенник получает возможность к непосредственному хищению чужого имущества или приобретению права на него).

2) имущество (вещи и иное имущество (имущественные права) (сюда относятся наличные и безналичные денежные средства, ценные бумаги и т.д.)[1].

В последние годы набирает большую популярность новая валюта, именуемая криптовалютой. Криптовалюта от электронных денег отличается, в первую очередь, тем, что у криптовалюты не существует центрального эмитента (то есть организации, которая их выпускает). Следующее немаловажное отличие состоит в различиях в способе их эмиссии и хранения. Хранение и выпуск криптовалюты осуществляется децентрализованно, в то время как информацию об электронных деньгах и операциях с ними возможно централизовать на одном сервере. Существуют и другие отличия, к примеру, обязательное использование асимметричного криптографического шифрования при создании криптовалют и т.д.[2].

Таким образом, криптовалюта также не является электронным денежным средством, что усложняет ее отнесение к предмету преступления. Однако в настоящее время в Российской Федерации идет процесс постепенного внедрения такой валюты в правовое поле. В настоящее время согласно ст.128 Гражданского кодекса Российской Федерации (далее – ГК РФ) к имуществу

---

[1]Азмуханов Р.Р. Проблемные аспекты теоретического и практического характера предмета преступления, предусмотренного ст.159.6 УК РФ «мошенничество в сфере компьютерной информации» // Студент года 2020 : сборник статей Международного научно-исследовательского конкурса, Петрозаводск, 11 мая 2020 года. Петрозаводск: Международный центр научного партнерства «Новая Наука», 2020. С. 251.

[2] Цифровое право: учебник / Егорова М.А., Блажеев В.В., Дюфло А., Андреева Л.В. и др.; под общ. ред. В.В. Блажеева, М.А. Егоровой. М.: Проспект, 2020. С. 344.

относятся и цифровые права. Согласно ст.141.1 Федерального закона от 18.03.2019 № 34-ФЗ цифровые права –это:«названные таковыми в законе обязательственные и иные права, содержание и условия осуществления которых устанавливаются в соответствии с правилами информационной системы, отвечающей признакам, установленным законом»[1].

К сожалению, в настоящее время законодатель не рассматривает криптовалюту цифровым правом. Но следует отметить, что до момента включения в состав имущества в цифровые права, суды признают криптовалюту в качестве цифровых прав. В качестве примера, приведем дело № А40-124668/2017, по рассмотрению которого Девятый арбитражный апелляционный суд отнес криптовалюту в качестве имущества. В обоснование суд отметил, что перечень гражданско-правовых интересов в гражданском законодательстве страны является публичным в силу диспозитивности норм.

Во-вторых, суд указывал на то, что действующее гражданское законодательство не содержит определения термина «иное имущество», указанного в ст. 128 ГК РФ, и допускает его предельно расширительное толкование с учетом нынешних экономических реалии и уровень цифровизации. Суд также принял во внимание норму ст.6 ГК РФ, сущность которой заключается в том, что при невозможности использования аналогии закона вступают в силу общие принципы и смысл гражданского права и требования справедливости сила, добросовестность и разумность, в соответствии с которыми определяются права и обязанности сторон[2].

Из вышеприведенного примера можно сделать вывод, что криптовалюту можно считать в качестве собственности (имущества) и может быть предметом криминального вмешательства.

Механизм следообразования.

---

[1] О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации: Федеральный закон от 18.03.2019 № 34-ФЗ // Российская газета. 2019. № 60.

[2] Постановление Девятого арбитражного апелляционного суда от 15 мая 2018 г. № 09АП-16416/2018 по делу № А40-124668/2017. URL: https://www.garant.ru (дата обращения: 20.09.2022).

В своих исследованиях В.А. Гусев под механизмом преступления предлагает понимать сложную динамическую систему обстоятельств, которая обуславливает содержание преступной деятельности. Данная система охватываетобстановку преступного посягательства; совокупность преступных действий и связанных с ним лиц при подготовке, совершении и сокрытии преступления; отношение потерпевшего и преступника, а также поведение потерпевшего и действия лиц, оказавшихся случайными участниками преступления[1].

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

а) 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.);

б) компьютерные следы, которые при любых действиях с компьютером или иными программируемыми устройствами получают своё отображение в электронной памяти. К ним относятся:

–следы, характеризующие результаты воздействий на компьютерную систему путём 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 наиных компьютерных средствах, характеризующие подготовку к совершению преступления, т. е. содержащие криминалистически значимую информацию в компьютерах, органайзерах, мобильных телефонах, цифровых фотоаппаратах, видеокамерах и диктофонах, смарт-картах и пр. Можно отметить, что специфика образования компьютерных следов тесно взаимосвязана с другими элементами криминалистической характеристики и

[1] Дрожжинова А.И. К вопросу о структуре криминалистической характеристики преступлений // Новая наука: От идеи к результату. 2017. Т. 1. № 2. С. 227-230.

имеют характерную взаимосвязь между собой, а именно с таким элементом, как место совершения компьютерного мошенничества[1].

*Сведения о личности преступника и жертвы.*Д.А. Влезько дает следующее определение «криминалистический портрет личности преступника подразумевает применение всех общедоступных данных, необходимых для расследования преступления и выяснения причин его совершения»[2]. Простое применение данной совокупности знаний в правоприменительной практике подразумевает ее важность в литературе. Криминальная психология занимается разработкой типологических портретов и классификаций личности преступника, результаты которых позже применяются в расследовании и раскрытии преступлений.

Исследование личности преступника в криминалистических учениях реализовывается посредством изучения его личностных качеств и черт, которые отражаются в следах преступления. При осуществлении следственных действий данные знания применяются как источник влияния на субъект преступления.

Личность преступника типизируется на основе многих факторов: типа преступной ориентации (эгоистичная, эгоистично-насильственное, насильственное преступление), уровень социальной дезадаптации (совершенное преступление впервые или рецидив), формы вины, поведения после совершения преступления.

На основе изучения материалов правоприменительной практики мы предлагаем следующий портрет лица, совершающего преступления, предусмотренные ст. 159.6 УК РФ.

Результаты статистических исследований 2011 и 2021 годов были практически неизменны (мужчины – 98,2% и 97,2%, женщины – 1,8% и 2,8%

---

[1] Третьякова Е.И. Об актуальных элементах криминалистической характеристики мошенничества в сфере компьютерной информации // Научный дайджест Восточно-Сибирского института МВД России. 2019. № 3(3). С. 213.

[2]Влезько Д.А. Значение личности преступника в криминалистике // Вестник Восточно-Сибирского института МВД России. 2018. №4 (87). С. 187.

соответственно)[1], однако соотношение мужчин и женщин в 2021 году составило 91,1% и 8,9% соответственно. Несмотря на то, что относительная численность женщин выросла втрое, разница на 6,1% (прирост в диапазоне 2011–2021 годов) за 10 лет может считаться незначительной.

По данным исследования, проведенного по 2011 году, распределение преступников по возрасту выглядело следующим образом: до 18 лет – 29,9%; от 18 до 24 лет – 60,4%; старше 24 лет – 9,7%.

По сравнению с исследованиями 2021 года доля преступников группы от 18 до 24 практически не изменилась (65,8%), зато процент преступников, не достигших 18 лет, заметно вырос (12,8% в 2021году)[2].

Совершающий деяние данного вида преступник всегда технически подготовлен и обладает комплексом программно-аппаратных методов и навыков, позволяющих не просто облегчить, но и обеспечить сам факт совершения преступления. Также необходимо отметить, что лица, совершающие преступления, предусмотренные ст. 159.6 УК РФ, обладают более высоким интеллектуальным уровнем, чем преступники в других сферах.В данном случае речь идет не только об образовании в классическом его понимании, но и о стремлении к саморазвитию, которое предопределяет, по сути, процесс выявления в существующих системах (как компьютерных, так и социальных) брешей, позволяющих злоумышленникам улучшить свое материальное положение незаконным путем.

Полученная нами в ходе статистического анализа, проведенного автором за период времени с 2011 по 2021 гг., общая картина распределения преступников по уровню образования имела следующий вид: 34% – среднее образование, 27% – среднее специальное образование (из них 72% – образование в сфере информатики и инфокоммуникаций), 39% – высшее

---

[1] Состояние преступности в Российской Федерации. URL: https://xn--b1aew.xn--p1ai/dejatelnost/statistics (дата обращения: 02.05.2022).

[2]Дремлюга Р.И. Международно–правовое регулирование сотрудничества в сфере борьбы с интернет–преступностью // Библиотека криминалиста. 2018. № 5(10). С. 339–346.

образование (из них высшее техническое образование – 37%, экономические специальности – 52%)[1].

Таким образом, следует отметить, что основная отличительная черта личности преступника, совершающего преступления, предусмотренные ст. 159.6 УК РФ – это тот факт, что преступников может быть любой человек, начиная от несовершеннолетнего, заканчивая лицом в возрасте до 50 лет. Следует принимать во внимание, что сфера компьютерной информации предоставляет гражданам некую конфиденциальность, раскрепощенность и иллюзию безнаказанности. Согласно изученным материалам уголовных дел и судебно-следственной практики, мы пришли к выводу, что в большинстве случаев, преступники, совершающие преступления в информационной сфере обладают высоким уровнем интеллектуальных способностей.

[1] Состояние преступности в России за 2011-2021 гг. URL: https://xn--b1aew.xn--p1ai/dejatelnost/statistics (дата обращения: 24.05.2022).

ГЛАВА 2. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЕ ПОЛОЖЕНИЯ РАССЛЕДОВАНИЕ МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

§1. Программа действий на этапе проверки сообщения о преступлении и возбуждения уголовного дела

В настоящем параграфе рассмотрим действия уполномоченных лиц на этапе доследственной проверке сообщения о преступлении и возбуждения уголовного дела по уголовным делам о преступлении, предусмотренных ст. 159.6 УК РФ. Задачей на стадии возбуждения уголовного дела является выявление поводов и оснований для возбуждения уголовного дела в соответствии с которыми орган дознания, дознаватель, или следователь в пределах компетенции от результатов проверки принимают решение о возбуждении уголовного дела. Возбуждение уголовного дела служит начальным этапом действия уголовно процесса.

На данном этапе:

☐ принимается сообщение о преступлении (заявление о преступлении, явка с повинной, сообщение о преступлении, совершенном или готовящемся, сообщение, полученное из иных источников, постановление прокурора о направлении соответствующих материалов в орган дознания для возбуждения уголовного дела согласно (ст. 140 УПК));

☐ проводится процессуальные действия: получение объяснений, исследование документов и предметов, проведение документальных проверок и ревизий, исследование документов предметов трупов, в случае необходимости привлекаются специалисты, имеющие специальные познания; в порядке исключения проводятся следственные действия: получение образцов для сравнительного исследования, выемка документов предметов, производство судебной экспертизы в разумный срок, осмотр места происшествия, документов предметов трупов, освидетельствование, привлечение специалиста, письменное поручение о производстве оперативно-розыскных мероприятий(ст.

144 УПК РФ); производится анализ результатов (полученной информации) по относимости к признаками конкретного состава преступления содержащегося в УК РФ, по допустимости, достоверности, (ст. 75 УПК РФ недопустимые доказательства, ст. 89 УПК РФ использование в доказывании результатов оперативно-розыскной деятельности);

☐ Принимается решения по сообщению о преступлении: овозбуждение уголовного дела; об отказе в возбуждении(ст.24 основание отказа в возбуждении уголовного дела или прекращения уголовного дела, ст. 25 прекращение уголовного дела в связи с примирением сторон, ст.27 основание прекращения уголовного преследования;

☐ О передачи сообщения по подследственности, то есть, определяется орган расследования, уполномоченный вести производство по уголовному делу,(ст. 151 УПК РФ Подследственность УПК), по сообщениям частного обвинения в суд (часть 2 статьи 20 УПК РФ).

При проведении процессуальных действий по проверке данного сообщения особое внимание уделяется осмотру места происшествия, осмотру компьютера, устройства потерпевшего. Проведение осмотра с письменного согласия потерпевшего для фиксации всей информации на устройстве потерпевшего, копирование всей информации, для обнаружения признаков преступления по статьям УК 272, 273, 274, 274.1, 159.6. Согласно 3 пункта части 2 статьи 151 УПК РФ «Подследственность» статьи УК 272, 273, 274 , 159.6 со второй части по четвертой – производиться следователями органов внутренних дел, 2 пункта 2 части статьи 151 УПК РФ – по статье УК 274.1 предварительное следствие производится следователями органовфедеральной службы безопасности. В первую очередь фиксация информации, которая может безвозвратно исчезнуть, например информация в оперативной памяти – загруженные страницы сайта в сети Интернет, желательно производить фиксацию на видео или фото аппаратуре во время проведении осмотра места происшествия. Первичное построение части схемы предположительного механизма преступления, то есть, описание схемы по предложенной ранее

классификации обнаруженных электронноцифровых следов. К примеру, если имеется устройство потерпевшего, его уже относим к личному устройству, если другие члены семьи не пользуются данным устройством. Взять письменное согласие на копирование информации с устройства потерпевшего. В случае использования устройством других членов семьи, берется с каждого члена семьи письменное согласие на копирование информации находящейся на устройстве. Далее фиксируем всю компьютерную информацию сначала на энергозависимой части устройства, чтобы безвозвратно не потерять важную компьютерную информацию, затем на жестком диске устройства.

Возбуждение уголовных дел по мошенническим действиям в сфере компьютерной информации обладает рядом особенностей, отличающих данное преступление от преступлений общеуголовной направленности, и требует проведения проверочных мероприятий, предшествующих принятию решения в порядке ст. 144, 145 УПК РФ[1].

Наиболее распространенными поводами для возбуждения уголовных дел о преступлениях, предусмотренных ст. 159.6 УК РФ являются:

I. Заявление о преступлении (п. 1 ч. 1 ст. 140 УПК РФ).

Рассмотрим правоприменительную практику, согласно которой представитель юридического лица ЗАО «…» обратился в органы внутренних дел с заявлением о том, что за последние несколько месяцев у них значительно увеличились ежемесячные платежи за доступ в Интернет. В ходе доследственной проверки было установлено, что используемый трафик в ЗАО «…» меньше выставленного счета провайдера.Проведенный провайдером анализ трафика показал, что большую часть файлов составляют видеофильмы, которые в основном скачиваются с различных сайтов в ночное время. Вследствие чего было выявлено, что под учетным им. ЗАО «…» в информационном пространстве выходить пользователь со следующим абонентским номером «…», который принадлежит гр. «З.С.С.» по адресу: «…».

[1] Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 18.12.2001 № 174-ФЗ // Российская газета. 2001. № 249.

По оперативным сведениям следует, что в квартире по адресу: «…», проживает гр. «Л.К.А.», являющийся инженером компьютерной фирмы «…».

В процессе расследования правоохранительными органами было установлено, что гр. «Л.К.А.» осуществляя свои функции в фирме «…» получал для ремонта системные блоки от ЗАО «…». Также было установлено, что гр. «Л.К.А.» обладая специальными познаниями в системе программирования и имея определенные программные средства, скопировал необходимые данные при проверке внутреннего наполнения системных блоков для получения информации (пароли и учетные записи пользователей). После преступных действий гр. «Л.К.А.» вскрывал учетные записи сотрудников ЗАО «…» и скачивал видеоматериалы в ночное время[1].

До другому делу гр. «С.М.С.» находился по адресу «…» ДД.ММ.ГГ. вступил в преступную группу, которую создан гр. 1 (неизвестных следствию), которая занималась хищением денег посредством обмана в сфере продажи авиабилетов в целях обогащения.

Вовлеченный в преступную группу гр. «С.М.С.» осуществлял поиск участников для открытия банковских карт в кредитных организациях и осуществления безналичных переводов. В процессе осуществления своих полномочий гр. «С.М.С.» вовлек гр. 3, на которого были возложены обязанности по открытию банковских карт и привязыванием в мобильному банку. Реализую свои полномочия гр. 3 обратился к гр. 4, которая оформила банковскую карту «…» посредством Интернета и установила мобильный банк с абонентским номером «…» за обещанное вознаграждение. После чего последняя получила от курьера банковскую карту «…» и передала гр. 3, который в свою очередь передал гр. «С.М.С.».

ДД.ММ.ГГ. для покупки авиабилета в Интернете из «…» в «…», гр. 5, применяя сеть Интернет и ноутбук марки «…» зашел на сайт «…», в которой содержатся ложные данные в сфере приобретения авиабилетов, ввел

[1] Приговор по ст. 159.6 УК РФ // Московский городской суд. URL: https://mos-gorsud.ru/ (дата обращения: 10.12.2022).

персональные данные и данные банковской карты. После чего с банковской карты гр. 5 были списаны деньги в размере «…» рублей на банковскую карту гр. 4, после чего были списаны деньги в размере «…» рублей на банковскую карту гр. 6. Размер похищенных денежных средств для гр. 5 является значительным.

Таким образом, суд квалифицировал действия гр. «С.М.С.» по ч. 2 ст. 159.6 УК РФ – мошенничество в сфере компьютерной информации, то есть хищение чужого имущества путем вмешательства в функционирование информационно-коммуникационных сетей группой лиц по предварительному сговору, с причинением значительного ущерба гражданину[1].

II. Результаты оперативно-розыскной деятельности (абз. 2 ст. 11 Федерального закона от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности»[2].

ДД.ММ.ГГ. сотрудники отдела «К» «…» в ходе производства операции «Сеть…» было приобретена оперативная информация от лиц, оказывающих содействие, о том, что на территории «…» организованная группа «…» занимается созданием вредоносных программ в преступных целях. Сотрудниками было принято решение о производстве оперативно-розыскного мероприятия «проверочная закупка» по адресу «…». Органами предварительного расследования было установлено, что вредоносные программы предназначены для неправомерного доступа к социальным сетям.

В результате чего, действия участников организованной группы были квалифицированы по ч. 2 ст. 159.6 и ч. 3 ст. 272 УК РФ[3].

III. Сообщение о совершенном или готовящемся преступлении, полученное из иных источников (п. 3 ч. 1 ст. 140 УПК РФ).

---

[1] Постановление Вахитовского районного суда г. Казани № 1-413/2020 от 29 июля 2020 г. по делу № 1-413/2020. URL: https://sudact.ru/regular/doc/ftR7s3xLHjHQ/ (дата обращения: 10.12.2022).

[2] Об оперативно-розыскной деятельности: Федеральный закон от 12.08.1995 № 144-ФЗ // Российская газета. – 1995. – № 160.

[3] Уголовное дело № 1-215/2011 // Свердловской областной суд. URL: http://oblsud.svd.sudrf.ru/ (дата обращения: 10.12.2022).

В данной ситуации следует отметить, что информационное пространство в процессе цифровизации на современном этапе развития общества имеет исключительно важное значение для информационно-поисковой и информационно-аналитической деятельности как для сотрудников органов внутренних дел, так и для иных служб и органов, занимающихся борьбой с информационной преступностью.Очевидно, что использование гражданами Интернет-пространства является не только положительным, но и отрицательным явлением в жизни общества, поскольку Интернет-пространство способствует возникновению новых источников общественной опасности в виде преступности.

На этом этапе очень важно настроить плановое и непрерывное взаимодействие со специалистами социальных сетей, в том числе провайдерами, в целях получения информации о сетях, клиентах и их активности; с сотрудниками подразделения «К». Необходимо отметить, что данное подразделение специализируется на раскрытии преступлений в сфере компьютерной информации. Одним из основных направлений работы Управления «К» МВД России и подразделений по регионам является выявление и пресечение фактов неправомерного доступа к компьютерной информации и борьба с изготовлением, распространением и использованием вредоносных программ для ЭВМ.

Подразделения «К» могут с помощью специальных средств перехватить открытую информацию, передаваемую подозреваемым по каналам связи, получить с помощью специальной техники данные, подтверждающие факт мошенничества, и выявить объекты, которые в дальнейшем могут быть изъяты и приобщены к делу в качестве вещественных доказательств, установить сетевой адрес, с которого преступник выходил в Интернет, установить его личность, электронные счета, используемые им в целях обмана, и другую информацию, необходимую для принятия решения о возбуждении уголовного дела. В такой ситуации необходимо проверить сообщение, полученное посредством сети Интернет об обнаруженном мошенничестве в сфере

компьютерной информации, опросив потенциальных потерпевших и выяснив, совершенно ли мошенничество или иное преступление.

Таким образом, особое внимание нужно акцентировать на проблемах, возникающих при обращении к провайдерам финансовых услуг (кредитные организации, платежные системы, где фиксируются данные о владельцах счетов, дате и времени совершения операций, сведения о дате и времени Интернет-соединений и *IP*-адресах, с которых осуществлялись выходы в сеть). От того, насколько хорошо налажено взаимодействие правоохранительных органов с ними, может зависеть ход дальнейшего расследования: несвоевременность обращений с запросами, промедление получения ответов на них могут способствовать безвозвратной утери или уничтожению значимых сведений. Решению данных проблем, по нашему мнению, может поспособствовать проведение регулярных встреч руководителей территориальных органов МВД России с представителями провайдеров финансовых услуг, где будут обсуждаться вопросы взаимодействия.

Совершенствование деятельности по расследованию мошенничеств с использованием сети «Интернет» на основе предложенных нами рекомендаций, несомненно, повысит эффективность работы органов предварительного расследования[1].

§2. Особенности производства следственных действий и оперативно-розыскных мероприятий на первоначальном этапе

Преступления, совершаемые с использованием современных информационно-коммуникационных технологий, особенно сети Интернет, мобильных средств и систем связи представляет собой серьезную угрозу национальной безопасности Российской Федерации. Потенциал современных

[1] Бондаренко О.С. Особенности расследования мошенничества в сети интернет // Преступность в СНГ: проблемы предупреждения и раскрытия преступлений : сборник материалов, Воронеж, 21 мая 2020 года. Воронеж: Воронежский институт МВД России, 2020. С. 202-204.

информационно-коммуникационных технологий позволяет их использовать в качестве орудий или средств совершения почти всех известных уголовному законодательству преступлений. От способа совершения конкретного преступления зависят ход расследования, степень организованности взаимодействия, алгоритм и очередность следственных действий и оперативно-розыскных мероприятий.

С момента поступления материалов процессуальной проверки о преступлении, совершенном с использованием средств сотовой связи и сети Интернет, следователь (дознаватель) незамедлительно возбуждает уголовное дело и в течение суток проводит следующие следственные и процессуальные действия.

1. Признает лицо потерпевшим и в ходе допроса выясняет у него следующие вопросы:

– дата и время поступления звонка либо SMS-сообщения;

– на стационарный или сотовый телефон совершен звонок, номер телефона звонившего (отправившего сообщение);

– содержание разговора либо сообщения, голос преступника и его характерные особенности (хриплый, высокий или низкий, молодой или старый. Шепелявит, проглатывает окончание, диалект и т. д) с целью дальнейшего опознания по голосу;

– сумма денежных средств, подлежащих передаче;

– способ передачи денежных средств: если блиц-перевод – на чье имя (Ф.И.О), номера сотового телефона;

– если нарочным способом – во сколько и кто (описание внешности по методу словесного портрета и возможность дальнейшего опознания по фотографии или в натуре) подошел, подъехал (марка, модель, цвет, государственный регистрационный знак транспортного средства) за деньгами;

– место передачи и дальнейшие действия преступника после получения денег; если путем перечисления на банковскую карту – реквизиты этой карты[1].

2. Направляет запрос оператору связи о предоставлении полной информации о владельце (в т. ч. период использования, активации, отключения) абонентского номера, с которого совершен звонок.

3. После допроса потерпевшего и получения ответа от оператора связи направляет поручение органу дознания, входящему в состав специализированной следственно-оперативной группы, с целью установления адреса регистрации (фактического проживания) владельца абонентского номера, с которого осуществлялся звонок.

4. На основании полученной информации в соответствии со ст. 186 УПК РФ возбуждает перед судом ходатайство о контроле и записи телефонных переговоров абонентского номера, с которого осуществлялся звонок, и (или) на который перечислялись денежные средства, а также в соответствии со ст. 186.1 УПК РФ ходатайство о получении информации о соединениях абонентского номера, используемого преступником (дата, время, длительность, IMSI, ID и адрес первой и последней вышки сотовой связи абонентов А и Б), после чего истребует данную информацию у оператора связи соответствующего региона.

5. Руководствуясь положениями ст. 183 УПК РФ, на основании полученной информации незамедлительно возбуждает перед судом ходатайство о выемке информации о счетах потерпевшего, а также лиц, на счета которых переведены похищенные денежные средства, и в установленном порядке направляет судебное постановление для реализации в кредитные учреждения[2].

---

[1] Власов С.В. К вопросу об особенностях раскрытия и расследования преступлений, связанных с использованием средств сотовой связи // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2019. № 23. С. 67-72.

[2] Москвичев А. А., Харченко У. А. Особенности проведения первоначальных оперативно-разыскных мероприятий и следственных действий при раскрытии и расследовании преступлений, совершенных с использованием средств сотовой связи // Академическая мысль. 2019. №3 (8). С. 114-116.

Приведенная рациональная, эффективная, построенная в определенной последовательности система первоначальных оперативноразыскных мероприятий и следственных действий позволит правоохранительным органам более точно определить как задачи, возникающие в процессе раскрытия и расследования преступлений, совершенных с использованием средств сотовой связи, так и способы их решения, обеспечить эффективность использования дополнительных сил, средств и времени для выполнения определенного объема работ.

Расследование мошенничества в сфере компьютерной информации на его первоначальном этапе во многом зависит от наличия сведений о преступнике и исходной информации, в том числе механизма следообразования.На основании изученной следственной практики приведем наиболее часто встречающиеся следственные ситуации первоначального этапа расследования мошеннических действий в сфере компьютерной информации:

1. Мошенник обнаружен, задержан и полностью признает свою вину.

Данная ситуация является наиболее благоприятной; программа действий направлена на закрепление доказательств, подтверждающих вину подозреваемого. В этой ситуации необходимо провести следующие следственные действия: допрос потерпевшего, допрос подозреваемого, осмотр места происшествия; осмотр компьютерной техники (в некоторых случаях он может быть составной частью осмотра места происшествия); осмотр предметов или документов; допрос свидетелей, предъявление для опознания; обыски по месту жительства и в иных местах, имеющих отношение к мошенническим действиям; назначение различных видов экспертиз, в том числе компьютерно-технической.

Необходимо также иметь в виду, что в большинстве случаев данные преступления совершаются группой лиц по предварительному сговору или организованной группой лиц. В этом случае, как правило, известны все или некоторые участники организованной группы и есть сведения о некоторых совершенных ими ранее криминальных эпизодах.

Рассмотрим правоприменительную практику. Так, довольно сложных алгоритм прослеживается с действия организованной группу в составе гр.гр. Х., П., Л. и М. По материалам дела следует, что гр. Х. ДД.ММ.ГГ. отбывал наказание в ИК № «…» УФСИН России по «…». В процессе отбывания наказания у гр. Х. возник умысел на создание организованной группы и руководство ею для хищения денег с счетов граждан, которые обслуживаются в банке «…» в корыстных целях (для получения выгоды). Реализую свой умысел гр. Х. сформировал криминальную схему хищения денежных средств. Преступные действия гр. Х. предлагал осуществлять посредством *GSM*-каналов на сайте Авито. Ранее, гр. Х. приобрел *sim*-карты различных операторов страны, которые были зарегистрированы на «подставных» граждан.

Участники организованной группы осуществляли отправку сообщения или звонки посредством *GSM*-каналов с намерениями купить тот или иной товар. Участники организованной группы находя жертв, заявляли им о том, что могут оплатить посредством банковской карты «…». После чего просили жертв отправить им номер карты и копию паспорта владельца, которые без раздумья отправляли данные преступникам. После чего преступники, используя программу, позволяющую изменять номера, звонили в службу поддержки банка «…» и представились от именно других лиц с данными, которые были приобретены ранее, и просили идентификатор для входа в онлайн банка.

Работники банка «…» предоставляли идентификатор и отправляли 5-тизначный код. В последующем участники организованной группы повторно звонили жертвам и представлялись работников банка и просили продиктовать 5-тизначный код в целях оплаты. После получения кода и имеющегося идентификатора, преступники заходили в онлайн банк «…» и осуществляли перевод с карты жертв на другие счета, которые ранее были созданы для «отмывания»[1].

[1] Приговор Засвяженского районного суда г. Ульяновска по делу № 2-1/2018 // Ульяновский городской суд. URL: http://www.uloblsud.ru/ (дата обращения: 10.12.2022).

2. Мошенники завуалировали свои действия под гражданско-правовую сделку.

В данной ситуации после допроса потерпевшего необходимо проверить документооборот той организации, куда потерпевший направил денежные средства, а также наличие лицензии и иных документов, подтверждающих легальность их деятельности; допросить представителей этой организации. Однако основными являются оперативно-розыскные мероприятия, проводимые в целях выяснения сайта-клона, лица, регистрирующего данный сайт, а также сведений, которые помогут обнаружить мошенника. При его выявлении и задержании производится осмотр места происшествия, осмотр компьютерной техники, поддельных документов, допрос подозреваемого, свидетелей, назначение соответствующих экспертиз.

3. Мошенник не обнаружен и не задержан.

В данной ситуации действия сводятся к взаимодействию с сотрудниками подразделения «К», а также специалистами и операторами связи по обнаружению владельца мошеннического сайта и выявлению всех обстоятельств, имеющих значение для обнаружения и доказывания вины подозреваемого. Вышеназванные типичные следственные ситуации первоначального этапа расследования мошенничества в сфере компьютерной информации неявляются исчерпывающим перечнем и могут видоизменяться в зависимости от механизма конкретного преступления, информации, полученной на момент возбуждения уголовного дела, и данных, собранных оперативными сотрудниками.

На первоначальном этапе перед уполномоченным сотрудником (органом) выстраивается ряд основополагающих задач, таких как:

– определение наличия или отсутствия события преступления; способ совершения;

– определение группы лиц, которые имеют отношению к совершению преступления, а также лиц, которые могут быть проинформированы об обстоятельствах подготовки, совершения и сокрытия;

– определение элементов обстановки мошенничества: время, место и др.;

– определение источников и объема документов, в которых отражаются подготовительный механизм, этапы взаимодействия и действия по сокрытию мошенничества;

– определение главных признаков похищенных денег: стоимость, приблизительный размер причиненного вреда;

– пресечение преступной деятельности и использование способности скрыть сведения о преступлении, предотвращение возможного или продолжающегося сопротивления расследованию[1].

Эффективность расследования мошенничеств в сфере компьютерной информации на первоначальном этапе зависит не только от грамотных действий следователя, но и от продуктивного взаимодействия с оперативными сотрудниками подразделения «К», специалистами экспертно-криминалистических подразделений и специалистами в области IT-технологий.

С целью профилактики данного рода преступлений необходимо привлекать средства массовой информации, а также проводить мероприятия, направленные на информирование граждан о новых способах совершения мошенничества, привлекая не только СМИ, но и представителей заинтересованных ведомств и организаций.

Таким образом, исходя из анализа следственной и судебной практики, наиболее часто проводятся следующие следственные и иные процессуальные действия:

– осмотр места происшествия, осмотр предметов и документов (100% уголовных дел);

– допрос лиц, процессуальное положение которых определено (100% уголовных дел). Подавляющее большинство – это допросы потерпевших и

[1] Чумаков А.В. Типичные ситуации первоначального этапа расследования мошенничества в сфере компьютерной информации // Ситуационный подход в юридической науке и практике: современные возможности и перспективы развития : Материалы Международной научно-практической конференции, посвященной 15-летию научной школы криминалистической ситуалогии БФУ им. И. Канта, Калининград, 20-22 октября 2017 года. Калининград: Балтийский федеральный университет имени Иммануила Канта, 2017. С. 209-212.

свидетелей, и в меньшей степени при установлении виновных лиц – допросы подозреваемых и обвиняемых. Следует отметить, что допрос последней категории лиц может проводиться спустя значительный промежуток времени;

– назначение и производство судебных экспертиз (100% уголовных дел). Компьютерно-техническая экспертиза назначается в 100% случаев; дактилоскопическая – в 60% случаев; технико-криминалистическая – в 55% случаев; трасологическая – 25% случаев; психологическая – в 10% случаев и в 5% иные виды экспертиз;

– получение образцов для сравнительного исследования (80% уголовных дел);

– предъявление для опознания (25% уголовных дел);

– обыск и выемка (90% уголовных дел);

– очная ставка (85% уголовных дел);

– следственный эксперимент и проверка показаний на месте (65% уголовных дел);

– снятие информации с технических каналов связи (25% уголовных дел);

– прослушивание телефонных и иных переговоров (5% уголовных дел) и др.

§3. Последующий этап расследования

На последующем этапе перед субъектами расследования преступлений, предусмотренных ст. 159.6 УК РФ стоят несколько задач:

1) для сотрудников оперативных подразделений: осуществление легализации результатов оперативно-розыскной деятельности и предоставление их в орган следствия, дознания и суда;

2) для сотрудников органов дознания или следствия: составление обвинительного заключения, постановления или акта и направление дела прокурору.

Помимо вышеуказанных задач, на последующем этапе расследования мошенничества в сфере компьютерной информации решаются также общие задачи:

1) определение обстоятельств, которые способствовали совершению преступления;

2) определение круга всех участников преступного посягательства (их роли и отведенные функции);

3) установление цепи перевода похищенных денежных средств;

4) вычисление *IP*-адресов преступников и др. в целях использования данных в качестве доказательств в судебном производстве.

На последующем этапе расследования весьма эффективным является производство повторного допроса и очной ставки.

Одним из эффективных тактических приемов изобличения допрашиваемого во лжи является повторный допрос обвиняемого. Такой допрос должен проводиться для выяснения деталей отдельных обстоятельств в связи с получением следователем новых доказательств. Повторный допрос также рекомендуется проводить по вопросно-ответной системе, которая позволяет выявить противоречия в показаниях самого обвиняемого. При допросе обвиняемого, не признающего вину, целесообразно использовать такой эффективный способ фиксации, как аудио- и видеозапись.

Следующим следственным действием на последующем этапе расследования, подлежащим исследованию в рамках данной дипломной работы, является очная ставка, проводимая при условии, если в показаниях ранее допрошенных участников уголовного судопроизводства имеются существенные различия.

Как свидетельствует судебно-следственная практика, эффективными тактическими приемами при производстве очной ставки являются: предварительное ознакомление правдивого участника с ранее данными им показаниями с целью напоминания ему отдельных обстоятельств преступления; психологическая подготовка правдивого участника, особенно если это

несовершеннолетний, пожилой или больной человек со слабым характером, сильно поддающийся влиянию посторонних лиц. К эффективным тактическим приемам также относится предложение, чтобы первым давал показания правдивый участник. Это тем более целесообразно сделать в случаях, когда у следователя нет уверенности, что данное лицо не изменило своих показаний под влиянием противоположных утверждений другого участника[1].

Наиболее эффективным тактическим приемом при проведении очной ставки является исключение негативного психологического воздействия участника этого следственного действия, дающего ложные показания, на лицо, занимающее позитивную позицию. Для этого необходимо проводить очную ставку таким образом, чтобы до минимума сократить общение ее участников с тем, чтобы они не могли переговариваться между собой. К тактическим приемам проведения очной ставки также относятся: детализация показаний ее участников, предъявление доказательств, использование противоречий в показаниях и некоторые другие.

На последующем этапе в зависимости от ситуации могут проводиться и другие следственные действия: дополнительные допросы потерпевших и свидетелей, назначение отдельных видов судебных экспертиз, следственный эксперимент и др.

На данном этапе расследования преступлений, предусмотренных ст. 159.6 УК РФ возникают вопросы, связанные с легализацией результатов оперативно-розыскной деятельности органу дознания, следователю или в суд, порядок которого регламентируется Инструкцией[2]. Представление результатов

---

[1] Криминалистика. Полный курс в 2 ч.: учебник для бакалавриата и специалитета / В. В. Агафонов [и др.]; под общей редакцией В. В. Агафонова, А. Г. Филиппова. 6-е изд., перераб. и доп. М.: Юрайт, 2019. С.115.

[2] Инструкция о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд: утв. Приказом МВД России № 776, Минобороны России № 703, ФСБ России № 509, ФСО России N 507, ФТС России № 1820, СВР России № 42, ФСИН России № 535, ФСКН России № 398, СК России № 68 от 27.09.2013 // Российская газета. 2013. № 282.

оперативно-розыскной деятельностиоргану дознания, следователю или в суд состоит из нескольких этапов:

1) представление результатовоперативно-розыскной деятельности в виде рапорта (в данной ситуации следует рассмотреть вопрос о целесообразности рассекречивания данных, которые составляют определенную категорию тайны; оформить необходимые документы и передать результаты оперативно-розыскной деятельности);

2) вынесение постановления о рассекречивании сведений, полученных в результате оперативно-розыскной деятельности;

3) вынесение постановления о предоставлении результатов оперативно-розыскной деятельности.

Таким образом, при положительном раскладе последующего этапа расследования по ч. 1 ст. 159.6 УК РФ уполномоченное лицо органа дознания (по ч. 2-4 ст. 159.6 УК РФ уполномоченное лицо следственного органа) выносит обвинительный акт или обвинительное постановление (обвинительное заключение) и направляет документы прокурору. В случае, если органом следствия или дознания не было нарушено процессуального законодательства и иных нормативно-правовых актов при рассмотрение обвинительного заключения (акта или постановления) прокурор принимает решения для передачи материалов в суд для рассмотрения дела в судебном производстве.

ГЛАВА 3. ТАКТИЧЕСКИЕ ОСОБЕННОСТИ ПРОВЕДЕНИЯ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ

§1. Тактические особенности проведения допроса

При расследовании преступлений, предусмотренных ст. 159.6 УК РФ большое значение отводится особенностям тактики проведения допроса участников уголовного дела. Рассмотрим особенности тактики проведения допроса потерпевшего и подозреваемого (обвиняемого).

Разделим на подгруппы и охарактеризуем граждан, которые могут стать жертвами преступлений, предусмотренных ст. 159.6 УК РФ.Согласно исследования, мы пришли к выводу, что исследуемый вид преступления обладает корыстным аспектов, в связи с чем предлагаем следующую классификацию жертв:

а) граждане Российской Федерации и стран зарубежья;

б) организация, осуществляющие связи, в том числе провайдеры Интернета;

в) банковские организации;

г) интернет-магазины (маркетплейсы);

д) иные организации Российской Федерации и стран зарубежья.

Жертвы от преступлений в различных ситуациях обладают рядом особенностей: виктимное поведение; склонность к спиртным напиткам и наркотических средствам; склонность к азартным играм; желание легкой наживы и т.п. Данное обстоятельство следует принимать во внимание, так как такие жертвы склонны отрицать некоторые факты (случайная активация вирусные программ).

Успех предварительногорасследованияпреступлений, предусмотренных ст. 159.6 УК РФ во многом зависит от умения уполномоченных лиц собирать и исследовать доказательства по уголовным делам, в том числе при проведении допроса.Важным источником информации по уголовным делам о преступлениях, предусмотренных ст. 159.6 УК РФ, являются показания

потерпевших (жертв от преступления).Подготовка и проведение допросов потерпевших по уголовным делам имеют существенные особенности, которые должен учитывать следователь (дознаватель).

Основными факторами, определяющими содержание тактического обеспечения допроса потерпевших по уголовным делам о преступлениях, предусмотренных ст. 159.6 УК РФ, можно считать следующее:

– классификация способа совершения преступления;

– позиция жертвы по отношению к уполномоченному лицу ведущемуся расследованию и личность жертвы;

– отношение к подозреваемым (обвиняемым), а также потерпевшим от преступной деятельности мошенника;

– стадия расследования преступления при проведении допроса;

– особенности личности жертвы;

– условия восприятия информации, являющейся предметом доказывания по уголовному делу[1].

Определенные трудности возникают при вызове потерпевших. Тактические особенности допроса определяются количественно-качественнымиданными об обстоятельствах уголовного дела о преступлениях, предусмотренных ст. 159.6 УК РФ, которыми владеет жертва преступления.Показания потерпевших особенно важны для доказательств по делам о преступлениях, предусмотренных ст. 159.6 УК РФ.

Общий план допроса жертвы компьютерного информационного мошенничества можно представить следующим образом:

– обстановка совершения преступления (место и время совершения);

– обстоятельства совершения преступления;

– как представлял себя мошенник, предъявлял ли документы на сайтах, какие услуги или ценности предлагал и т.п.;

---

[1] Тактические особенности расследования мошенничества в сфере компьютерной информации : учебное пособие / М. Н. Кузьмин. Краснодар : Краснодарский университет МВД России, 2019. С. 31.

– какое имущество было похищено, в каком размере;

– когда подозревает потерпевший;

– кто может подтвердить хищения имущества и т.п.

Помимо общих вопросов, следователь (дознаватель) должен установить индивидуальные элементы преступного посягательства. На наш взгляд, каждый способ мошенничества в сфере компьютерной информации и вопросы, которые следует выяснить обладают определенными характерными чертами.

К примеру, жертве мошенничества в сфере компьютерной информации в информационной сети (социальной сети) помимо общих вопрос, следует задавать индивидуальные вопросы, которые относятся к способу совершения преступления, предусмотренного ст. 159.6 УК РФ, которые дают возможность определить такие обстоятельства, как:

– аккаунты в каких социальных сетях был зарегистрирована жертва;

– кем был осуществлен перевод денег (в каком размере);

– сроки совершения мошенничества (возможно, потерпевший несколько раз подвергся преступному обману, но не догадывался об этом ранее);

– какие услуги (товары) должен был обеспечить мошенник;

– какие услуги (товары) были в итоге предоставлены (если были предоставлены, например, они могли быть худшего качества или не в полном объеме);

– какие гарантии предоставлял мошенник, которые позволили убедиться в законности операции, какие документы, возможно, были высланы потерпевшему;

– пытался ли он самостоятельно разыскать мошенника, что удалось выяснить (если удалось);

– каков размер прямого ущерба потерпевшему;

– потерпевшему необходимо предоставить возможность продемонстрировать следователю все обстоятельства совершения преступления в сети Интернет на компьютере с доступом к глобальной сети, это позволит

восстановить детали произошедшего и предоставить следователю ясную картину произошедшего[1].

Тактика допроса подозреваемого мошенника в сфере компьютерной информации имеет свои особенности и, в первую очередь, в аспекте более глубоко продуманной, тщательно подготовленной, наступательной психологической активности следователя. Успешность допроса интернет-мошенника зависит от умелого выбора и эффективного применения тактических приемов допроса.

Необходимо сразу же оговориться, что тактически правильным будет допрос подозреваемого сразу же после его задержания. Это позволит следователю использовать замешательство подозреваемого, его «испуг» и т.д. Кроме того, в данной ситуации подозреваемый не может спокойно придумать себе алиби и т.д.

Использование доказательств при допросе – это тактический прием по реализации находящейся в распоряжении следователя доказательственной информации путем как непосредственного ее предъявления (демонстрации), так и опосредованными способами ознакомления с ней допрашиваемого с целью изменения ошибочной или ложной позиции, а также получения от него показаний о предъявленных доказательствах и связанных с ними обстоятельства расследуемого уголовного дела. При использовании данного тактического приема необходимо исключить демонстрацию подозреваемому протоколов допросов свидетелей и потерпевших, так как в противном случае подозреваемый получает информацию об указанных людях и может оказать на них давление.

Успешность допроса подозреваемого и обвиняемого, а отсюда и значение для дела полученных показаний зависят от умелого выбора и искусного, эффективного применения выработанных теорией и практикой тактических приемов допроса.

---

[1] Кузьмин М.Н. Указ. соч. 2019. С. 33.

При допросе в условиях бесконфликтной ситуации, когда допрашиваемый подтверждает правильность возникшего в отношении его подозрения, а обвиняемый признает себя виновным, основное внимание должно быть направлено на получение полных, подробных, детализированных показаний обо всех обстоятельствах совершенного преступления. Оценивая сообщаемые сведения, следует иметь в виду, что допрашиваемый, даже признавая себя виновным, нередко сознательно, а иногда неосознанно стремится по возможности умалить свою роль в расследуемом событии, представить себя в более выгодном свете, изобразить себя жертвой неблагоприятного стечения обстоятельств. Возможно, также проявление стремления скрыть или преуменьшить участие в преступлении лиц, к которым допрашиваемый испытывает чувство привязанности. Все эти моменты таят угрозу превращения бесконфликтной ситуации в конфликтную. Поэтому, особенно на первом допросе, не следует без необходимости при постановке после свободного рассказа вопросов сразу же акцентировать внимание допрашиваемого на спорных, противоречивых моментах его показаний[1].

В конфликтной ситуации общим правилом является использование возможностей свободного рассказа для установления психологического контакта с допрашиваемым, более глубокого изучения его личностных особенностей и получения как можно более полных показаний по всем обстоятельствам, интересующим следствие[2].

Довольно часто конфликтная ситуация складывается при допросе подозреваемого. Конфликтность подобного допроса обусловлена, прежде всего, позицией допрашиваемого, отрицающего свою причастность к совершенному преступлению. Кроме того, поскольку допрос происходит в начале расследования, следователь обычно не располагает достаточной совокупностью доказательств для полного изобличения допрашиваемого. К тому же еще и нет

---

[1] Горбунов И.Г. Особенности применения специальных знаний по уголовным делам о мошенничестве // Закон и право, 2019. № 4. С. 32.

[2] Криминалистика: учебник для вузов / под ред. А. А. Хмырова, В. Д. Зеленского. Краснодар: 2018. С. 106.

полной уверенности, что подозреваемый – то самое лицо, которое виновно в преступлении. Поэтому первый допрос подозреваемого носит в определенной мере разведывательный характер и направлен на выяснение личностных особенностей допрашиваемого, его позиции, аргументов и получение той информации, которую он намерен сообщить.

При этом нужно учитывать, что подозреваемому свойственны противоречивые психические переживания. С одной стороны, он рассчитывает, что следствие не располагает достаточными доказательствами, и поэтому надеется, что ему удастся уйти от ответственности. С другой же стороны, факт задержания или внезапного вызова на допрос довольно часто оказывается для такого лица неожиданным, ослабляет его уверенность в том, что преступление останется нераскрытым, и способствует формированию в его сознании представления о неизбежности предстоящего разоблачения.

Противоречивость переживаний лица, совершившего преступление, их особая острота, затрудняют правильную оценку ситуации и приводят к грубым просчетам и неверным решениям[1].

Тактика допроса подозреваемого должна быть максимально осторожной, избирательной, поскольку не исключено, что подозрение в отношении определенного лица возникло в результате неблагоприятного стечения обстоятельств, оговора, заблуждения или ошибки. Известно, что фактор задержания или ареста может сломить волю лица, не виновного в совершении преступления, и привести к самооговору. Поэтому особенно важно проверить причастность допрашиваемого к расследуемому событию и получить от него такую информацию, которая может быть известна только лицу, совершившему преступление[2].

О причастности допрашиваемого к расследуемому преступлению чаще всего свидетельствуют характерные умолчания (например, сокрытие факта

[1] Кузьмин М.Н. Указ. соч. 2019. С. 45.
[2] Власов И.Г. Особенности расследования преступлений в области информационных технологий. М.: Принт, 2012. С. 92.

знакомства с лицом, связь с которым допрашиваемого по делу установлена), а также нередко появляющиеся в показаниях проговорки, т.е. невольное сообщение сведений, в которых проявляется осведомленность об отдельных обстоятельствах расследуемого преступления (например, о размерах, приметах похищенного, месте преступления).

С учетом личности допрашиваемого и других обстоятельств на допросе может быть предъявлена вся совокупность уличающих доказательств, чтобы сразу же показать бессмысленность дальнейшего отрицания вины. В некоторых ситуациях изобличение допрашиваемого можно начать с предъявления одного или двух наиболее впечатляющих доказательств. Затем при необходимости используются и другие доказательства.

При проведении допроса обвиняемых должны быть учтены следующие основные тактические правила предъявления доказательств:

– следует обеспечить экономное, целесообразное применение доказательств, собранных по делу. В данном ситуации не следует торопиться предъявить те или иные доказательства; необходимо максимально применять тактику свободного рассказать, дать возможность обвиняемому самостоятельно рассказать о событиях преступления;

– во всех допросных ситуациях следователю (дознавателю) целесообразно сначала показать свою осведомленность о тех или иных обстоятельствах, задав вопросы, а затем использовать соответствующие доказательства;

– не следует предъявлять доказательства допрашиваемому, пока последний не был допрошен по всем обстоятельствам, касательно имеющихся доказательств, за исключением тактики «внезапности».

Подытоживая сказанное, следует отметить, что позитивные изменения в противостоянии мошенникам в сфере компьютерной информации находятся в прямой зависимости от того, насколько адекватен существующим криминальным угрозам арсенал тактических средств следователя. Немаловажной составляющей этого арсенала является тактическое обеспечение

допроса потерпевшего по уголовным делам о мошенничестве в сети Интернет. Своевременное обновление, дополнение и совершенствование данного тактического обеспечения способно заметно повысить эффективность выявления и пресечения фактов интернет- мошенничества, а также расследования уголовных дел о мошенничестве в сети Интернет.

Таким образом, тактика допроса подозреваемого во многом ориентирована на психологическое воздействие на него, особую роль при этом играет оперативность задержания преступника, поскольку он не успевает придумать алиби и тактику ведения следствия по ложному следу. Следователю необходимо убедить подозреваемого в том, что основные доказательства по делу уже есть и смысла отрицать свою вину нет, создать ситуацию, в котором подозреваемый почувствует, что его сообщники или свидетели преступления уже сообщили правоохранительным органам много информации, и если он сейчас не признается, то лишиться смягчающих обстоятельств, связанных с чистосердечным раскаянием и помощи следствию в раскрытии преступления. Подводя итог проведенному в настоящей главе исследованию, отметим, что особенности тактики производства отдельных следственных действий на первоначальном этапе расследования (тактика допроса потерпевшего и подозреваемого, тактика обыска, особенности производства выемки и осмотра электронных документов и соединений пользователя с сетью Интернет) имеют очень важное значение, именно от алгоритма действий следователей в различных ситуациях зависит скорость сбора доказательств и привлечения к ответственности подозреваемого. Следователям на всех этапах проведения расследования по делам о мошенничестве в сфере компьютерной информации следует привлекать специалистов в области информационных технологий и получать профильные консультации специалистов, вся их деятельность должна находиться в рамках действующего законодательства.

§2. Тактические особенности назначения и производства судебных экспертиз

В настоящее время после совершения преступлений уполномоченные лица назначают экспертизы для полноценного сбора доказательств. Специфические свойства цифровых (компьютерных) сведений определяют необходимость соблюдения требований и правил в процессе фиксации и изъятия виртуальных (электронных) доказательств, в том числе экспертное исследование[1].

В процессе раскрытия и расследования преступлений, предусмотренных ст. 159.6 УК РФ, большое внимание уделяется компьютерной экспертизе[2], которая осуществляется в следующих видах:

1) судебная аппаратно-компьютерная экспертиза, целью которой является изучение технических средств компьютерной системы;

2) судебная программно-компьютерная экспертиза, в рамках которой изучается функционирование программного обеспечения компьютерной системы, структурные особенности и алгоритма деятельности;

3) судебная информационно-компьютерная экспертиза, целью которой является поиск, установление, анализ и оценка данных, которые подготовлены участником или программами в целях осуществления информационных процессов в компьютерной системе;

4) судебная компьютерно-сетевая экспертиза, в рамках которой изучается функционирование компьютерных средств, осуществляющих ту или иную сетевую информационную технологию.

---

[1]Россинская Е.Р., Шамаев Г.П. Криминалистическое исследование компьютерных средств и систем как новый раздел криминалистической техники // Уголовно-процессуальные и криминалистические средства обеспечения уголовного судопроизводства: материалы междунар. науч.-практ. конф., Иркутск, 25-26 сент. 2014 г. Иркутск, 2019. С. 318.

[2] Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации: Приказ МВД России от 29.06.2005 № 511 // Справ.-правовая система «Гарант» (дата обращения: 12.03.2023).

Вышеуказанные виды судебных экспертиз были комплексно исследованы Е.Р. Россинской[1].

Таким образом, следует вывод, что результативность раскрытия и расследования преступлений, предусмотренных ст. 159.6 УК РФ в большей степени зависит от эффективного, оперативного и качественного применения специальных знаний. Производство судебных экспертиз необходимы для приобретения фактических сведений, которые указывают на совершение преступлений. Как ранее уже было отмечено, исследуемая категория преступлений совершается посредством обмана или злоупотребления доверием, с помощью приобретения доступа к компьютерной (электронной) системе[2].

Как правило, по делам о преступлениях, предусмотренных ст. 159.6 УК РФ назначается также судебно-бухгалтерскаяэкспертиза.

Судебно-бухгалтерскую экспертизу целесообразно проводить в тех ситуациях, когда следователь (дознаватель) не может разрешить важнейшие вопросы в процессе исследования без помощи специалиста. Данная экспертиза помогаетустановить величина материального вреда, роль индивидуальныхсубъектов в совершении мошенничества, обстановку, обстоятельства и условия, способствовавшие совершению выявленного преступления.

Производство судебно-бухгалтерской экспертизы дает возможность следователю (дознавателю) определить способ совершения преступлений, предусмотренных ст. 159.6 УК РФ. Данная экспертиза решает вопросы диагностической направленности:

---

[1]Россинская Е.Р. Проблемы использования специальных знаний в судебном исследовании компьютерных преступлений в условиях цифровизации // Вестник университета им. О.Е. Кутафина. 2019. № 5 (57). С. 31-44.

[2] О внесении в Государственную Думу Федерального Собрания Российской Федерации проекта Федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации и иные законодательные акты Российской Федерации: постановление Пленума Верховного Суда РФ от 05.04.2012 № 6 // Справ.-правовая система «КонсультантПлюс» (дата обращения: 10.01.2023).

– установлениеученых несоответствий, их степень, механизм их формирования, воздействия на показатели финансово-хозяйственной деятельности, в том числе отклонений от правил бухгалтерского учета и отчетности;

– создание показателей, связанных с отображением операций поступления, движения и выдачи денежных средств в учетной документации;

– определение соответствия процедуры учета денег с учетом требований и правил[1].

Предметом исследуемого вида экспертизы выступают операции, которые протекают в электронном документообороте. Отсюда следует, что судебно-бухгалтерская экспертиза по уголовным делам о преступлениях, предусмотренных ст. 159.6 УК РФ назначается в следующих ситуациях:

– при возникновении спорных вопросов в отчетных документах, решение которых требует специальных знаний бухгалтерской деятельности;

– при наличии расхождений и несогласованности между итогами проверок;

– при возникновении несогласованности между итогами различных проверок[2].

Большое внимание следует уделять электронным документам, которые представляются эксперту для производства экспертизы (к примеру, бухгалтерская, статистическая или учетная отчетность). Подписи, которые были указаны в данных документах представляются на экспертизу в электронном формате. В правоприменительной практике бывают ситуации, когда подлинность подписей вызывает сомнения. При определении лица, который поставил подписьспециалист должен предоставить подлинники документов и образцы для сравнительного исследования. Согласно материалам

---

[1] Дубоносов Е.С. Судебно-бухгалтерская экспертиза : учебник для бакалавриата и магистратуры / Е. С. Дубоносов. 2-е изд., перераб. и доп. М.: Юрайт, 2019. С. 170.

[2] Звезда И.И. К вопросу о назначении судебной экспертизы при расследовании мошенничества в сфере компьютерной информаци // Известия ТулГУ. Экономические и юридические науки. 2018. №4-2. С. 127.

правоприменительной практики следует, что в ряде ситуациях подлинные документы теряются (уничтожаются). В данной ситуации для производства экспертизы необходимо подписи в электронной форме, после чего их распечатывают для удобства. Согласно правоприменительной практике, следователи (дознаватели) нередко назначают производство почерковедческой экспертизы в целях определения лица, которым была подделана подпись[1].

Проанализированные нами уголовные дела указывают на то, что в 90% случаев следователи (дознаватели) назначают компьютерно-техническую экспертизу, которая имеет большое значение для эффективного раскрытия и расследования преступлений, предусмотренных ст. 159.6 УК РФ.

В производстве данной экспертизы следователь (дознаватель) предоставляет эксперту документы и данные, которые записаны на магнитном носителе и имеют значение для уголовного дела, в том числе которые изъяты в процессе производства иных следственных действия по уголовным делам о преступлениях, предусмотренных ст. 159.6 УК РФ.

На наш взгляд, задачами исследуемого вида экспертизы выступают идентификация и диагностика носителя (устройства), кодов доступа к той или иной компьютерной информации. Опознавательные задачи эксперта заключаются в установлении обстоятельств сходства или общей комплексной принадлежности предъявляемых объектов.

По уголовным делам о преступлениях, предусмотренных ст. 159.6 УК РФ, которые были совершены посредством использования компьютерной техники, возникает нужда в проведении комплексной экспертизы. По мнению Е.Р. Россинской по уголовным делам о преступлениях, предусмотренных ст. 159.6 УК РФ к данной категории экспертиз следует относить: «компьютерно-техническая и бухгалтерская экспертиза; судебная компьютерно-техническая и

[1] См.: Судебный департамент при Верховном суде Российской Федерации. URL: http://cdep.ru/ (дата обращения: 10.01.2023); Судебные и нормативные акты Российской Федерации. URL: https://sudact.ru/ (дата обращения: 10.01.2023).

судебно-техническая экспертиза; судебная компьютерно-техническая и планово-экономическая»[1].

Компьютерно-техническая экспертиза применяется для поиска следов преступлений, совершенных в информационно-коммуникационной сети «Интернет», при выявлении действий злоумышленников, создающих поддельные сайты с реквизитами для перечисления денежных средств. В том числе возможности компьютерно-технической экспертизы позволяют выявлять латентные преступления, информация о которых аккумулирована в различных гаджетах, которые по своей сути выступают объектами экспертного исследования.

Заключение, составляемое экспертом, принципиально для установления обстоятельства по уголовному делу, в связи с чем важно четко и корректно поставить вопросы перед экспертом, который будет проводить компьютерно-техническую экспертизу. Так, к примеру, наиболее уместными вопросами будут выступать следующие:

– является ли исправным представленное на исследование оборудование?

– можно ли данное устройство использовать для удаления, блокирования, модификации компьютерной информации?

– какие сведения зафиксированы в памяти электронных плат?

– может ли представленное на исследование оборудование быть использовано для удаления, блокирования, модификации компьютерной информации? и прочее.

В итоге по своей сущности компьютерно-техническая экспертиза направлена на всестороннее обнаружение, фиксацию и исследование компьютерной информации с точки зрения ее защиты от злоумышленников. Таким образом, важно, чтобы в процессе выявления, раскрытия и предупреждения преступлений в сфере использования компьютерной информации не только присутствовали эксперты соответствующего уровня

[1]Россинская Е.Р. Судебная экспертиза в гражданском, административном, арбитражном и уголовном процессе. М., 2018. С. 185.

подготовки, но и сами действия по получению заключения от него были в максимальной степени легитимны с точки зрения процессуальной экономии проведения экспертных исследований.

Изучение правоприменительной практики показывает, что специалисты, которые принимают участие в производстве следственных действий и понимают, что им необходимо провести экспертизу поуголовным делам о преступлениях, предусмотренных ст. 159.6 УК РФ, будут гораздо инициативнее проводить поисковые мероприятия с целью обнаружения, фиксации и изъятия предметов (документов) и будут проявлять заинтересованность.

Итак, использование следователями (дознавателями) возможностей специальных знаний в процессе раскрытия и расследования преступлений, предусмотренных ст. 159.6 УК РФ заключается в назначении экспертиз, которые способствуют оперативному и эффективному раскрытию и расследованию мошенничеств в сфере компьютерной информации.

ЗАКЛЮЧЕНИЕ

Проведенное исследование позволяет сформулировать следующие выводы:

Во-первых, мошенничество в сфере компьютерной информации – его квалифицированный вид. Совершение данного преступного деяния возможно исключительно посредством использования современных компьютерных технологий. Объект анализируемого преступления полностью совпадает с родовым объектом хищения – это общественные отношения, сложившиеся в сфере электронного документооборота. Как и мошенничество вообще, квалифицированное мошенничество в сфере компьютерных технологий –всегда хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.

Форма объективной стороны содеянного строго ограничена законодателем: хищение чужого имущества, равно приобретения права на него путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Субъект –вменяемоедееспособное лицо, достигшее шестнадцатилетнего возраста. Субъективная сторона – прямой конкретизированный умысел. О наличии умысла, направленного на мошенничество в сфере кредитования, могут свидетельствовать, в частности, заведомое отсутствие у виновного лица права на вторжение в информационные базы потерпевших.

Во-вторых, криминалистическая характеристика преступлений как информационная база частных методов расследования также должна исследоваться как часть системы криминалистической поддержки при раскрытии и расследовании определенных видов преступлений. Под криминалистической характеристикой преступлений мы понимаем информационную модель, которая отражает криминалистическую природу

конкретного типа преступления, состоящую из информации об их криминалистически значимых свойств и их естественных отношениях друг с другом, на основе анализа и обобщения практики их раскрытия, расследования и судебного разбирательства важна и для развития частных следственных методов.

Способ совершения преступления – это конкретный комплекс в субъективных и объективных аспектах, а также содержание действий и методов, которые используют вымогатели, их цели, подготовительные действия и способы сокрытия преступного деяния. Для подготовки и сокрытия рассматриваемых в данной статье преступлений злоумышленниками используютсяспециальные программно-аппаратные средства для уничтожения значимой для следствия информации при попытке доступа к ней третьих лиц, обеспечения преступником анонимности своих действий в сети Интернет с использованием цепочки прокси-серверов (*VPN*-технологии), подменой номера телефона.

Сходным по способу совершения способ сокрытия следов за счет инсценировки совершения действий самим потерпевшим является и «фарминг». При данном способе используется возможность переадресации с официальных сайтов организации на их мошеннические копии, где преступники и получают необходимые им данные. Нередко подобные способы используются при создании копий сайтов для заказа билетов, предполагающих введение персональных данных пассажира. Взаимодействие с мошенническим сайтом, который может существовать в сети непродолжительное время либо просто больше не использоваться преступниками, не позволяет достоверно установить, кто именно получил запрошенную информацию, а затем воспользовался ею для своих преступных целей.

Отличительным свойством места совершения мошенничества в сфере компьютерной информации выступает удалённость, нередко на значительные расстояния, места совершения общественно опасных деяний от места возникновения последствий. В этой связи 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.

К предмету преступного посягательства могут относится различные элементы: 1) компьютерная информация; 2) имущество; 3) Интернет-трафик и многое другое. В процессе цифровизации на современном этапе развития общества, большое внимание отводится новой «валюте» – криптовалюте. Согласно изученным материалам правоприменительной практики мы можем сделать вывод, что криптовалюту можно считать в качестве собственности (имущества) и она может быть предметом криминального вмешательства.

Основная отличительная черта личности преступника, совершающего преступления, предусмотренные ст. 159.6 УК РФ – это тот факт, что преступников может быть любой человек, начиная от несовершеннолетнего, заканчивая лицом в возрасте до 50 лет. Следует принимать во внимание, что сфера компьютерной информации предоставляет гражданам некую конфиденциальность, раскрепощенность и иллюзию безнаказанности. Согласно изученным материалам уголовных дел и судебно-следственной практики, мы пришли к выводу, что в большинстве случаев, преступники, совершающие преступления, предусмотренные ст. 159.6 УК РФ обладают высоким уровнем интеллектуальных способностей.

В-третьих, на этапе проверки сообщения о преступлении и возбуждения уголовного дела следователю (дознавателю) необходимо:

1. Принять сообщение о преступлении. В данной ситуации следователь (дознаватель) опрашивает жертву преступления по существу, устанавливает первоначальные сведения о «картине» совершения преступления со слов жертвы, регистрирует сообщение в дежурной части.

2. Провести процессуальные действия в целях принятия решение о возбуждении или об отказе в возбуждения уголовного дела или передачи

материалом по подследственности. О передачи сообщения по подследственности, то есть, определяется орган расследования, уполномоченный вести производство по уголовному делу, (ст. 151 УПК РФ Подследственность УПК РФ), по сообщениям частного обвинения в суд (часть 2 статьи 20 УПК РФ).

При проведении процессуальных действий по проверке данного сообщения особое внимание уделяется осмотру места происшествия, осмотру компьютера, устройства потерпевшего.

В-четвертых, на первоначальном этапе перед уполномоченным сотрудником (органом) выстраивается ряд основополагающих задач:– определение наличия или отсутствия события преступления; способ совершения; – определение группы лиц, которые имеют отношению к совершению преступления, а также лиц, которые могут быть проинформированы об обстоятельствах подготовки, совершения и сокрытия; – определение элементов обстановки мошенничества: время, место и др.; – определение источников и объема документов, в которых отражаются подготовительный механизм, этапы взаимодействия и действия по сокрытию мошенничества; – определение главных признаков похищенных денег: стоимость, приблизительный размер причиненного вреда; – пресечение преступной деятельности и использование способности скрыть сведения о преступлении, предотвращение возможного или продолжающегося сопротивления расследованию и др.

После возбуждения уголовного дела перед следователем (дознавателем) открывается целый спектр следственных действий, которые осуществляются именно после возбуждения уголовного делаю. Так, согласно материалам исследуемой правоприменительной практики следует, что по всем делам производится осмотр место происшествия, предметов и документов; допрос; экспертиза. Реже осуществляется получения образцов для сравнительного исследования; обыск и выемка; очная ставка. В 25-40% случаев проводится предъявление для опознания. Нередко при раскрытии и расследовании

преступлений, предусмотренных ст. 159.6 УК РФ осуществляются оперативно-розыскные мероприятия (снятие информации с технических каналов связи и т.п.).

Особенности тактики производства отдельных следственных действий на первоначальном этапе расследования (тактика допроса потерпевшего и подозреваемого, тактика обыска, особенности производства выемки и осмотра электронных документов и соединений пользователя с сетью Интернет) имеют очень важное значение, именно от алгоритма действий следователей в различных ситуациях зависит скорость сбора доказательств и привлечения к ответственности подозреваемого. Следователям на всех этапах проведения расследования по делам о мошенничестве в сфере компьютерной информации следует привлекать специалистов в области информационных технологий и получать профильные консультации специалистов, вся их деятельность должна находиться в рамках действующего законодательства.

В-пятых, на последующем этапе перед субъектами расследования преступлений, предусмотренных ст. 159.6 УК РФ стоят несколько задач:1) для сотрудников оперативных подразделений: осуществление легализации результатов оперативно-розыскной деятельности и предоставление их в орган следствия, дознания и суда; 2) для сотрудников органов дознания или следствия: составление обвинительного заключения, постановления или акта и направление дела прокурору; 3) определение обстоятельств, которые способствовали совершению преступления; 4) определение круга всех участников преступного посягательства (их роли и отведенные функции); 5) установление цепи перевода похищенных денежных средств; 6) вычисление *IP*-адресов преступников и др. в целях использования данных в качестве доказательств в судебном производстве.

В-шестых, в процессе раскрытия и расследования преступлений, предусмотренных ст. 159.6 УК РФ, большое внимание уделяется компьютерной экспертизе, которая осуществляется в следующих видах:судебная аппаратно-компьютерная экспертиза; судебная программно-компьютерная экспертиза;

судебная информационно-компьютерная экспертиза; судебная компьютерно-сетевая экспертиза; судебно-бухгалтерская и компьютерно-техническая.

Изучение правоприменительной практики показывает, что специалисты, которые принимают участие в производстве следственных действий и понимают, что им необходимо провести экспертизу по уголовным делам о преступлениях, предусмотренных ст. 159.6 УК РФ, будут гораздо инициативнее проводить поисковые мероприятия с целью обнаружения, фиксации и изъятия предметов (документов) и будут проявлять заинтересованность.

На наш взгляд, основной проблемой в процессе раскрытия и расследования преступлений, предусмотренных ст. 159.6 УК РФ является латентность данной вида преступления и нехватка технологических (инфраструктурных) возможностей органов внутренних дел. На основе этого предлагаем рассмотреть вопрос о совершенствовании инфраструктуры правоохранительных органов и повышении уровня профессионализма сотрудников правоохранительных органов. По нашему мнению, в борьбе с такого рода преступлениями оперативные подразделения должны использовать все возможности информационно-коммуникационные технологии. Стремительный процесс цифровизации на современном этапе развития общества открывает перспективы совершенствования информационных платформ системы МВД России и внедрения в деятельность оперативных подразделений полиции информационно-коммуникационных технологий в целях эффективной борьбы с мошенничеством в сфере компьютерной информации.

Таким образом, в условиях агрессивных действий криминального мира лишь общественное мнение может положительно повлиять на процесс создания условий и возможностей для правоохранительных органов оперативно использовать современные криминалистические методы, инструменты и рекомендации при выявлении и расследовании преступлений, предусмотренных ст. 159.6 УК РФ.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

I. Законы, нормативные правовые акты и иные официальные документы:

1. Конституция Российской Федерации от 12.12.1993 г.: Принята всенародным голосованием 12 декабря 1993 года с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 года // Официальный интернет-портал правовой информации www.pravo.gov.ru, 04.07.2020.№0001202007040001 (дата обращения: 14.10.2022).

2. Гражданский кодекс Российской Федерации (часть вторая): Федеральный закон от 26.01.1996 № 14-ФЗ // Собрание законодательства РФ.– 1996. – № 5, ст. 410.

3. Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 18.12.2001 №174-ФЗ (ред. от 25.03.2022) // Российская газета. – 2001. – №249.

4. Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 №63-ФЗ (ред. от 01.07.2021) (с изм. и доп., вступ. в силу с 01.12.2021) // Российская газета. – 1996. –№113-115.

5. О банках и банковской деятельности: Федеральный закон от 02.12.1990 № 395-1 // Российская газета. – 1996. – № 27.

6. О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации: Федеральный закон от 18.03.2019 № 34-ФЗ // Российская газета. – 2019. – № 60.

7. О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма: Федеральный закон от 07.08.2001 № 115-ФЗ // Российская газета. – 2001. – № 151-152.

8. Об оперативно-розыскной деятельности: Федеральный закон от 12.08.1995 № 144-ФЗ // Российская газета. – 1995. – № 160.

9. Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд: Приказ МВД России № 776, Минобороны России № 703, ФСБ России № 509, ФСО России № 507, ФТС России № 1820, СВР России № 42, ФСИН России №

535, ФСКН России № 398, СК России № 68 от 27.09.2013 // Российская газета. – 2013. – № 282.

10. Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации: Приказ МВД России от 29.06.2005 № 511 // Справ.-правовая система «Гарант» (дата обращения: 12.03.2023).

II. Монографии, учебники, учебные пособия:

11. Власов И.Г. Особенности расследования преступлений в области информационных технологий. – М.: Принт, 2012. – С. 92.

12. Возгрин И.А. Общие положения методики расследования отдельных видов преступлений / под ред. И.А. Возгрин. –М., 2016. –С. 95.

13. Дубоносов Е.С. Судебно-бухгалтерская экспертиза : учебник для бакалавриата и магистратуры / Е. С. Дубоносов. 2-е изд., перераб. и доп. –М.: Юрайт, 2019. –С. 170.

14. Егоров Н.Н. Криминалистика : учебник и практикум для вузов / Н. Н. Егоров, Е. П. Ищенко. –3-е изд., испр. и доп. –М. :Юрайт, 2022. –С. 613.

15. Коломинов В. В. Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа: дисс. … канд. юрид. наук. –Иркутск, 2017. –С. 12.

16. Криминалистика в 5 т. Том 5. Методика расследования преступлений : учебник для вузов / И. В. Александров [и др.] ; под общей редакцией И. В. Александрова. –М. :Юрайт, 2022. –С. 242.

17. Криминалистика : учебник для вузов / А. Г. Филиппов [и др.] ; под редакцией А. Г. Филиппова. –3-е изд., перераб. и доп. –Москва :Юрайт, 2022. – С. 466.

18. Криминалистика : учебник для вузов / И. В. Александров [и др.]; под редакцией И. В. Александрова. –2-е изд., испр. и доп. –М. :Юрайт, 2022. – С. 376.

19. Криминалистика. Полный курс в 2 ч.: учебник для бакалавриата и специалитета / В. В. Агафонов [и др.]; под общей редакцией В. В. Агафонова, А. Г. Филиппова. –6-е изд., перераб. и доп. – М.: Юрайт, 2019. – С.115.

20. Маркушин А.Г. Оперативно-розыскная деятельность полиции в раскрытии и расследовании преступлений : учебное пособие для вузов / А. Г. Маркушин, Н. А. Аменицкая. –М. :Юрайт, 2022. –С. 323.

21. Новые способы совершения преступлений в сфере информационных технологий на территории государств – участников СНГ: аналитический обзор / под ред. И. Б. Колчевский, В. М. Журавлев, А. Г. Кузнецов и [др.]. –М.: ФГКУ «ВНИИ МВД России», 2018. –С. 34.

22. Расследование преступлений в сфере компьютерной информации и электронных средств платежа : учебное пособие для вузов / С. В. Зуев [и др.] ; ответственные редакторы С. В. Зуев, В. Б. Вехов. –М.: Юрайт, 2022. –С. 243.

23. Россинская Е.Р. Судебная экспертиза в гражданском, административном, арбитражном и уголовном процессе. – М., 2018. – С. 185.

24. Тактические особенности расследования мошенничества в сфере компьютерной информации : учебное пособие / М. Н. Кузьмин. – Краснодар : Краснодарский университет МВД России, 2019. – С. 31.

25. Цифровое право: учебник / Егорова М.А., Блажеев В.В., Дюфло А., Андреева Л.В. и др.; под общ. ред. В.В. Блажеева, М.А. Егоровой. – М.: Проспект, 2020.– С. 344.

III. Статьи, научные публикации:

26. Абдульмянова Т.В., Асанова И.П., Данилов В.В. Мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ): понятие, уголовно-правовая характеристика и некоторые особенности расследования // Вопросы российского и международного права. – 2021. – Т. 11. – № 1-1. – С. 134-145.

27. Абдульмянова Т.В., Фролкина И.А. Предупреждение мошенничества в сфере материнского капитала // Вопросы российского и международного права. – 2018. – № 10. – С. 139-144.

28. Азмуханов Р.Р. Проблемные аспекты теоретического и практического характера предмета преступления, предусмотренного ст.159.6 УК РФ «мошенничество в сфере компьютерной информации» // Студент года 2020 : сборник статей Международного научно-исследовательского конкурса, Петрозаводск, 11 мая 2020 года. – Петрозаводск: Международный центр научного партнерства «Новая Наука», 2020. – С. 251.

29. Бондаренко О.С. Особенности расследования мошенничества в сети интернет // Преступность в СНГ: проблемы предупреждения и раскрытия преступлений : сборник материалов, Воронеж, 21 мая 2020 года. – Воронеж: Воронежский институт МВД России, 2020. – С. 202-204.

30. Введенская О.Ю. Особенности следообразования при совершении преступлений посредством сети Интернет // Юридическая наука и правоохранительная практика. – 2015. – № 4 (34). – С. 210.

31. Власов С.В. К вопросу об особенностях раскрытия и расследования преступлений, связанных с использованием средств сотовой связи // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2019. – № 23.– С. 67-72.

32. Влезько Д.А. Значение личности преступника в криминалистике // Вестник Восточно-Сибирского института МВД России. –2018. –№4 (87). – С. 187.

33. Горбунов И.Г. Особенности применения специальных знаний по уголовным делам о мошенничестве // Закон и право. –2019. –№ 4. –С. 32.

34. Дрожжинова А.И. К вопросу о структуре криминалистической характеристики преступлений // Новая наука: От идеи к результату. –2017. –Т. 1. № 2. –С. 227-230.

35. Звезда И.И. К вопросу о назначении судебной экспертизы при расследовании мошенничества в сфере компьютерной информации // Известия ТулГУ. Экономические и юридические науки. –2018. –№4-2. –С. 127.

36. Иващенко Н.Д. Мошенничество в сфере компьютерной информации: проблемные вопросы // Столица науки. – 2020. – № 6 (23). – С. 269-276.

37. Кулешова Н.Н., Христофорова Е.И. Особенности квалификации мошенничества в сфере компьютерной информации // Вопросы науки и образования. – 2014. – № 18. – С. 43.

38. Маазов М.М. Криминалистическая характеристика преступления // Проблемы совершенствования законодательства : сборник научных статей студентов юридического факультета. – Махачкала :ООО «АЛЕФ», 2019. – С. 368-370.

39. Москвичев А.А., Харченко У.А. Особенности проведения первоначальных оперативно-разыскных мероприятий и следственных действий при раскрытии и расследовании преступлений, совершенных с использованием средств сотовой связи // Академическая мысль. – 2019. – №3 (8). – С. 114-116.

40. Родивилин В.А., Коломинов В.В. Криминалистическая характеристика отдельных видов преступлений, совершенных с использованием информационно-телекоммуникационных технологий // Криминалистика: вчера, сегодня, завтра. – 2022. – № 1(21). – С. 117.

41. Россинская Е.Р. Концепция учения об информационно-компьютерных криминалистических моделях как основе методик расследования компьютерных преступлений // Вестник Восточно-Сибирского института МВД России. – 2021. – № 2 (9). – С. 195.

42. Россинская Е.Р. Проблемы использования специальных знаний в судебном исследовании компьютерных преступлений в условиях цифровизации // Вестник университета им. О.Е. Кутафина.– 2019. – № 5 (57). – С. 31-44.

43. Россинская Е.Р., Шамаев Г.П. Криминалистическое исследование компьютерных средств и систем как новый раздел криминалистической техники // Уголовно-процессуальные и криминалистические средства обеспечения уголовного судопроизводства: материалы международной научно-

практической конференци. – Иркутск, 25-26 сентября 2014 года. – Иркутск, 2019. – С. 318.

44. Симанович Л.Н. Криминалистическая характеристика вымогательства // Законность. – 2016. – № 4. – С. 17.

45. Третьякова Е.И. Об актуальных элементах криминалистической характеристики мошенничества в сфере компьютерной // Научный дайджест Восточно-Сибирского института МВД России. – 2019. – № 3(3). – С. 213.

46. Чумаков А.В. Типичные ситуации первоначального этапа расследования мошенничества в сфере компьютерной информации // Ситуационный подход в юридической науке и практике: современные возможности и перспективы развития : Материалы Международной научно-практической конференции, посвященной 15-летию научной школы криминалистической ситуалогии БФУ им. И. Канта, Калининград, 20–22 октября 2017 года. – Калининград: Балтийский федеральный университет им. Иммануила Канта, 2017. – С. 209-212.

47. Ширяев А.В. Способы сокрытия следов мошенничества в сфере компьютерной информации // Проблемы правовой и технической защиты информации. – 2020. – Вып. VIII. – С. 126-127.

48. Шруб М.П. Криминалистическая характеристика преступлений - фантом или информационно-поисковая основа расследования? // Вопросы криминологии, криминалистики и судебной экспертизы. – 2020. – № 2(48). – С. 31-36.

49. Polyakov V. Criminalistics specifics of methods of committing computer crimes and peculiarities of their prevention. Religacion. Journal of Social Sciences and Humanities. – 2019. – Vol. 4 (21). – pp. 90-97.

IV. Материалы следственной и судебной практики:

50. О внесении в Государственную Думу Федерального Собрания Российской Федерации проекта Федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации и иные законодательные акты

Российской Федерации: постановление Пленума Верховного Суда РФ от 05.04.2012 № 6 // Справ.-правовая система «КонсультантПлюс» (дата обращения: 10.01.2023).

51. О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 // Российская газета. – 2017. – № 280.

52. Постановление Апелляционного суда г. Севастополя № 44Г-185/2018 4Г-482/2018 от 30 мая 2018 г. по делу № 2-1155/2017. URL: https://sudact.ru/regular/doc/vSzadn3t6sgj/ (дата обращения: 13.09.2022).

53. Постановление Вахитовского районного суда г. Казани № 1-413/2020 от 29 июля 2020 г. по делу № 1-413/2020. URL: https://sudact.ru/regular/doc/ftR7s3xLHjHQ/ (дата обращения: 10.12.2022).

54. Постановление Девятого арбитражного апелляционного суда от 15 мая 2018 г. № 09АП-16416/2018 по делу № А40-124668/2017. URL: https://www.garant.ru (дата обращения: 20.09.2022).

55. Приговор Железногорского городского суда Курской области от 15.10.2018. Уголовное дело № 1-218/201. URL: https://clck.ru/sJy7P (дата обращения: 30.09.2022).

56. Приговор Засвяженского районного суда г. Ульяновска по делу № 2-1/2018 // Ульяновский городской суд. URL: http://www.uloblsud.ru/ (дата обращения: 10.12.2022).

57. Приговор Кизилюртовского городского суда Республики Дагестан от 04.07.2019 г. по делу № 1-67/2019. URL: https://clck.ru/sJy8r (дата обращения: 13.09.2022).

58. Приговор Кировского районного суда г. Ростова-на-Дону от 13.09.2019. Уголовное дело № 1-345/2019. URL: https://sudact.ru/regular/doc/LkG0QbZcSoNb/ (дата обращения: 30.09.2022).

59. Приговор Октябрьского районного суда г. Владимира № 1-95/2019 от 4 июня 2019 г. по делу № 1-95/2019. URL: https://sudact.ru/regular/doc/v59eyhN7lzJq/ (дата обращения: 13.09.2022).

60. Приговор по ст. 159.6 УК РФ // Московский городской суд. URL: https://mos-gorsud.ru/ (дата обращения: 10.12.2022).

61. Уголовное дело № 1-215/2011 // Свердловской областной суд. URL: http://oblsud.svd.sudrf.ru/ (дата обращения: 10.12.2022).

V. Иные источники:

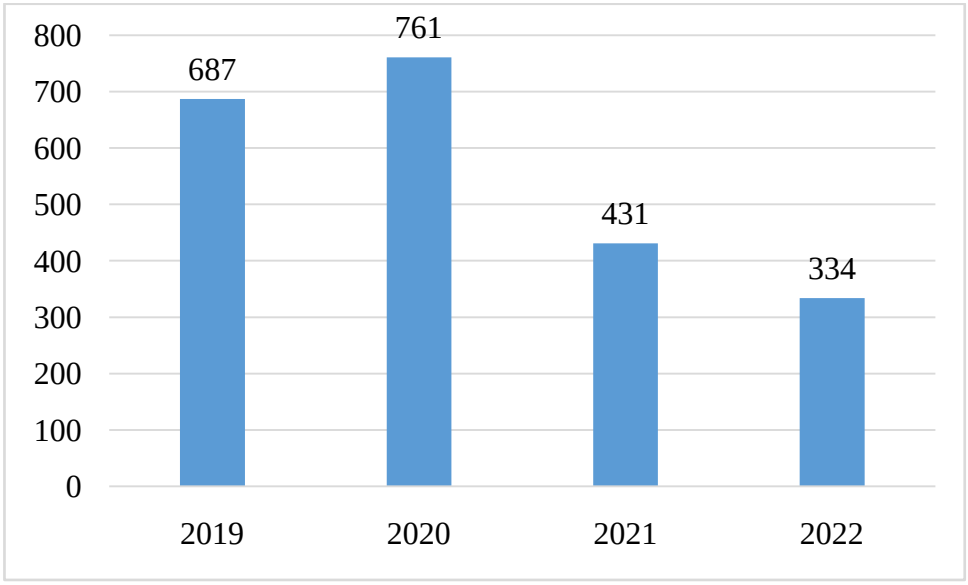
62. Состояние преступности в Российской Федерации. URL: https://xn--b1aew.xn--p1ai/dejatelnost/statistics (дата обращения: 17.09.2022).

63. Судебные и нормативные акты Российской Федерации. URL: https://sudact.ru/ (дата обращения: 10.01.2023).

64. Судебный департамент при Верховном судеРоссийской Федерации. URL: http://cdep.ru/ (дата обращения: 10.01.2023).

ПРИЛОЖЕНИЯ

1. Количество зарегистрированных преступлений, предусмотренных ст. 159.6 УК РФ на территории России за 2019-2022 гг.



2. Показатели, связанные с назначением наказания за совершение преступлений, предусмотренных ст. 159.6 УК РФ

Показатель	Осуждено	Оправдано	Лишение свободы	Условное лишение свободы	Ограничение свободы	Штраф	Исправительные работы	Обязательные работы	Принудительные меры к невменяемым
Статья 159.6 ч. 1	0	0	0	0	0	0	0	0	0
Статья 159.6 ч. 2	5	0	0	4	0	1	0	0	0
Статья 159.6 ч. 3	8	0	0	5	0	2	0	0	0
Статья 159.6 ч. 4	16	0	10	6	0	0	0	0	0

ОТЗЫВ

о работе обучающегося 181 учебного взвода очной формы обучения 2018 года набора, по специальности 40.05.01 - Правовое обеспечение национальной безопасности Кузнецова Аделя Ленаровича в период подготовки дипломной работы на тему:

«Проблемы расследования мошенничества в сфере компьютерной информации»

Содержание

Актуальность выбранной темы не вызывает сомнений. Это подтверждается большим количеством данных преступлений. Мошенники постоянно изобретают новые способы совершения преступлений с целью усложнения их установления и для ухода от уголовной ответственности. Поэтому расследование данной категории преступлений требует научной разработки и постоянного совершенствования.

При выполнении дипломной работы А.Л. Кузнецов показал умение корректно формулировать цели и ставить задачи по своей работе, анализировать, диагностировать причины появления проблем, их актуальность. Слушатель проявил самостоятельность в разработке плана исследования, о чем, свидетельствует логичность и структурированность дипломной работы. Инициативность Кузнецова А.Л. в выборе методов исследования, постановки цели и задач, способах описания результатов исследования проявилась на высоком уровне.

В выполнении структурных элементов работы в установленные научным руководителем сроки слушатель показал пунктуальность. В случае указания научным руководителем недочетов проявил добросовестность, ответственность в устранении недостатков.

В процессе работы над исследовательской частью слушатель проявил навыки работы с материалами следственно-судебной практики, способность и умение анализировать статистические данные, применять их в исследовании, пользоваться научной литературой профессиональной направленности и оперировать криминалистическими терминами и категориями.

Кузнецов А.Л. в процессе написания работы продемонстрировал способность к самостоятельному формулированию выводов и результатов исследования, владению компьютерными методами сбора, хранения и обработки информации, применяемой в сфере профессиональной деятельности, проявил умение и навыки работы с компьютерными программами (Word,

PowerPoint, Excel и т.п.), информационно-справочными ресурсами, работы в системе интернет.

При выполнении дипломной работы слушатель рационально планировал время выполнения работы, определял грамотную последовательность, объем операций и решений при выполнении поставленной задачи, умело анализировал полученные результаты экспериментальных данных и делал самостоятельные, обоснованные и достоверные выводы из проделанной работы.

Проверка по системе «Антиплагиат ВУЗ» показала: оригинальность - 42,93%, цитирование - 21,16%, совпадения - 35,91%.

Таким образом, представленная дипломная работа удовлетворяет всем требованиям Положения об организации подготовки и защите ВКР утвержденного приказом КЮИ МВД России и может быть допущена к защите.

Руководитель
Доцент кафедры криминалистики
кандидат юридических наук, доцент
полковник полиции _____ С.Л. Миролюбов

(ученая степень, ученое звание, должность, специальное звание) (подпись) (инициалы, фамилия)

М.П.
«25» мая 2023 г.

Подпись С.Л. Миролюбова
УДОСТОВЕРЯЕТСЯ
ОД и РКЮИ МВД России

С отзывом ознакомлен А.Л. Кузнецов

«25» мая 2023 г.

РЕЦЕНЗИЯ

на дипломную работу
обучающегося 181 учебной группы очной формы
обучения, 2018 года набора, по специальности 40.05.01
Правовое обеспечение национальной безопасности
Кузнецова Аделя Ленаровича
на тему «Проблемы расследования мошенничества в сфере компьютерной информации»

Содержание рецензии

Рецензируемая дипломная работа выполнена на актуальную тему, поскольку в настоящий момент большое количество преступлений совершаются дистанционно, при помощи компьютера. Данный вид преступления имеет свою специфику, как по механизму его совершения, так и по его способам. Однако, преступления в сфере компьютерной информации характеризуются большой латентностью и низкой раскрываемостью, что способствует увеличению количества деяний и совершенствованию навыков лиц их совершающих.

Дипломная работа состоит из введения, трех глав, включающих в себя семь параграфов, заключения, списка использованной литературы, приложений.

Во введении четко определены предмет, объект исследования, а также цели и задачи.

Первая глава посвящена рассмотрению уголовно-правовой и криминалистической характеристики мошенничества в сфере компьютерной информации. Исследуются вопросы понятия мошенничества, определяются элементы состава преступления, предусмотренного статьей 159.6 Уголовного кодекса Российской Федерации.

Вторая глава посвящена организационно-методическим положениям расследования мошенничества в сфере компьютерной информации. Раскрываются программа действий на этапе проверки сообщения о преступлении и возбуждения уголовного дела, особенности производства следственных и оперативно-розыскных мероприятий на первоначальном этапе, а также раскрывается последующий этап расследования.

Третья глава посвящена тактическим особенностям производства следственных действий. Определяются тактические особенности производства допроса и назначения судебных экспертиз.

В заключении сформулированы научно обоснованные выводы. Достоверность выводов подтверждается внушительным списком использованных НПА и литературы, всего 64 источника.

Автором был проанализирован достаточный объем теоретического

материала, нормативно – правовой базы; для написания работы использованы труды отечественных авторов, проблема раскрыта всесторонне. Весь собранный материал изложен четко, последовательно, с соблюдением логики повествования. Прослеживается тщательная и глубокая проработка вопроса.

Выбранная проблематика раскрыта полно и всесторонне, цель достигнута, задачи решены, выводы правильны и обоснованны.

Дипломная работа соответствует установленным требованиям.

Оценивая научное исследование, проведенное Кузнецовым А.Л. на оценку отлично, необходимо отметить отдельные недостатки и спорные положения.

1. В работе не использовались зарубежные источники законодательства и учебная литература.
2. Исторический аспект проблемы не исследовался.

Рецензент:
Заместитель начальника ГСУ МВД
по Республике Татарстан
полковник юстиции Т.И. Хайруллин

«18» мая 2023 г.

С рецензией ознакомлен А.Л. Кузнецов

«18» мая 2023г.