МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное казенное образовательное учреждение
высшего образования
«Уфимский юридический институт Министерства внутренних дел
Российской Федерации»

Кафедра криминалистики

ДИПЛОМНАЯ РАБОТА

на тему **«ОСОБЕННОСТИ ПРОИЗВОДСТВА СЛЕДСТВЕННЫХ ДЕЙСТВИЙ В ХОДЕ РАССЛЕДОВАНИЯ МОШЕННИЧЕСТВ В СФЕРЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ (ПО МАТЕРИАЛАМ ТЕРРИТОРИАЛЬНОГО ОРГАНА ВНУТРЕННИХ ДЕЛ)»**

Выполнил
Лебедев Даниил Владимирович
обучающийся по специальности
40.05.01 Правовое обеспечение
национальной безопасности
2021 года набора, 111 учебного взвода

Руководитель
доцент кафедры,
кандидат юридических наук, доцент
Гайнельзянова Венера Равилевна

К защите рекомендуется
рекомендуется / не рекомендуется
Начальник кафедры _____ Э.Д. Нугаева
подпись
Дата защиты «___» _____ 2026 г. Оценка _____

ПЛАН

ВВЕДЕНИЕ

Актуальность исследования обусловлена тем, что в XXI веке, лишь за четверть прошедшего от столетия времени, произошел значительный прогресс в развитии информационных технологий, в связи с чем, изменили свой вектор направления и преступления. Совершенствование способов реализации преступных деяний, методики оказания давления на граждан – то, что является одним из последствий научно-технического прогресса. Опираясь на материалы правоприменительной практики, можно сделать вывод о том, что составы преступлений, связанные с использованием информационно-телекоммуникационных технологий, вызывают сложности при их расследовании. В связи с этим имеется необходимость в разработке алгоритма проведения следственных действий на различных этапах расследования.

Согласно статистике МВД России, преступления против собственности, совершенные с помощью информационных технологий составляют 48,1% от общего количества преступлений за 2025 год. Среди преступлений против собственности лидирующее положение занимает мошенничество, совершенное с использованием информационно-телекоммуникационных технологий, составляющее 28,5%[1].

В настоящее время органы внутренних дел сталкиваются с значительными трудностями, возникающими в ходе раскрытия и расследования мошенничества, совершенного в сфере информационно-телекоммуникационных технологий, которые связаны с отсутствием четкой алгоритмизации осуществления процесса расследования данного вида преступления и специальных знаний в области информационно-телекоммуникационных технологий.

Цель исследования состоит в анализе примеров правоприменительной

[1] Статистические сведения использования системы межведомственного взаимодействия ИСОД МВД России // Единая система информационно-аналитического обеспечения деятельности МВД России.

практики, а также проблем производства следственных действий в ходе расследовании мошенничества, совершенного с использованием информационно-телекоммуникационных технологий.

Задачами выпускной квалификационной работы являются:

– изучение исторического аспекта развития мошенничества в сфере информационно-телекоммуникационных технологий;

– исследование и анализ криминалистической характеристики мошенничества в сфере информационно-телекоммуникационных технологий;

– определение особенностей проведения следственных действий, проводимых на первоначальном и последующем этапах расследования мошенничества в сфере информационно-телекоммуникационных технологий;

– определение проблем, возникающих при расследовании мошенничества, совершенного с использованием информационно-телекоммуникационных технологий.

Объектом исследования является общественные отношения, возникающие в ходе расследования мошенничества в сфере информационно-телекоммуникационных технологий.

Предметом исследования является теоретические и практические аспекты следственных действий, направленных на расследование мошенничества с использованием информационных технологий.

Структура выпускная квалификационная работа включает в себя введение, основную часть, состоящую из двух глав, пяти параграфов, заключения и списка использованной литературы.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ РАССЛЕДОВАНИЯ МОШЕННИЧЕСТВА В СФЕРЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

§ 1. Исторический аспект расследования мошенничества, как состава преступления

Первые упоминания о мошенничестве зафиксированы в нормативно-правовом акте «Артикул воинский» 1715 года, где понятие «мошенничество» не существовало, однако упоминалось под терминами «обмеривание» и «обвешивание».

Согласно вышеуказанному нормативно-правовому акту, лицо, совершившее противоправное действие («ежели кто мерою и весом лживо поступит»), обязуется возместить ущерб, причиненный потерпевшему в троекратном размере, а также выплатить штраф государству и понести телесное наказание, которое проводилось публично, чтобы общественность наглядно понимала, какие последствия за совершение преступления[1].

В годы правления Елизаветы Первой появился новый нормативно-правовой акт, в котором было упомянуто мошенничество в качестве отдельного состава преступления. Отмеченный документ имел название «Общий кодекс законов – Новоуложенная книга», который состоял из пяти глав, посвященых преступным деяниям, направленным против собственности, где совершение мошенничества имело лишь два способа, это обманное завладение чужим имуществом и кража, совершенная с использованием лжедоверия. Анализируя данный нормативный акт, отметим, что в годы правления Елизаветы I были сформированы те признаки мошенничества, которые образуют его объективную сторону и в настоящее время.

В статье 24 «Новоуложенной книги» отмечается: «Если непотребного

[1] Криминалистика: учеб. пособие. Омск, 2023. С. 209.

жития люди ходят по кабакам, играют в карты, обманы чинят или тайно мошенничают, из карманов деньги, табакерки и прочее крадут, и таких мошенников всякие меры стараться искоренять и когда в поимке и в приводе будут, учинять им, по важности их преступления, наказание положено соразмерное ворам», где четко определена объективная сторона мошенничества как преступления, но при этом отсутствовала его субъективная сторона.

Для восполнения пробелов в законодательстве был принят Указ «О суде и наказании за воровство разных родов и о заведении рабочих домов». Устранение недоработок в законодательстве России коснулось и преступлений против собственности. Появилось новое понятие «воровство-мошенничество», которому соответствовали различные преступления, связанные с неправомерным завладением чужим имуществом (кража чужого имущества посредством обмана или вымысла)[1].

При этом, в Указе отмечалось: «Воровство мошенничество есть, буде кто торгу или в ином многолюдстве у кого из кармана что вынет, или вымыслом, или внезапно у кого что отымет, или унесет, или от платья полу отрежет, или позумент спорет, или шапку сорвет, или купя что не платя денег скроется, или обманом, или вымыслом продаст или отдаст поддельное за настоящее, или весом обвесит, или мерою обмерит, или что подобное обманом или вымыслом себе присвоит ему не принадлежащее, без воли и согласия того, чье оно»[2].

К началу XIX века в Российской Империи была произведена масштабная работа в области систематизации законодательства, по итогам которой были разработаны 45 томов Полного собрания законов Российской Империи. Однако Полное собрание законов существовало недолго из-за неудобства, из-за своих больших объемов. В связи с чем, М. М. Сперанский, на основе Полного

[1] Горшкова М.М. Криминалистические аспекты производства следственных действий: учеб. пособие / под общ. ред. доц. М. М. Горшкова. Омск, 2020. С. 32.

[2] Ищенко Е.П., Топорков А.А. Криминалистика: учеб. для вузов. 2-е изд., испр., доп. и перераб. М., 2023. С. 597.

собрания законов, составил Свод законов Российской Империи, который отличался своей компактностью (он состоял всего из 3 томов), и вся информация была консолидирована из предыдущего нормативного акта в новый.

В Своде законов Российской Империи преступные деяния, направленные против собственности, состояли из двух групп: преступления против собственности, преступления против частной собственности. Данный документ выделял три рода мошенничества: мошенничество и кража до 6 рублей серебром; мошенничество и кража от шести до тридцати рублей серебром; мошенничество и кража свыше тридцати рублей серебром. Вместе с тем, мошенничество и кража квалифицировались по повторяемости, то есть, совершенные впервые, второй и третий раз[1].

Однако систематизация законодательства Российской Империи на этом не закончилась и получила свое новое отражение в Уложении о наказаниях уголовных и исправительных, которое было принято в 1845 году.

В Уложении присутствовали и меры, которые как отягчали, так и смягчали наказание за совершение мошенничества и кражи, среди которых существенное значение имел рецидив совершения преступления.

Заключительным этапом кодификации уголовного права Российской Империи стало создание Уголовного уложения, принятое в 1903 году, где выделялась отдельная глава, посвященная мошенничеству. В указанном нормативно-правовом акте к предмету мошенничества относилось не только движимое имущество, но и все имущественные блага и права на них. Также данный нормативный акт вводит виды мошенничества, которые сохранились и в настоящее время, в частности, мошенничество при страховании имущества, мошенничество при продаже и залоге имущества и т.д.

В Уголовном уложении впервые имело отражение полноценного состава преступления, где субъектом являлось лицо, совершившее мошенничество

[1] Белкин Р. С. Криминалистическая энциклопедия. М., 2017. С. 201.

впервые, «учиненное шайкой», мошенничество, совершенное по отбытии виновным двух и более раз наказания за воровство, разбой, вымогательство или мошенничество. Субъективная сторона включала в себя заведомое искажение фактов настоящего или прошедшего.

Далее были приняты Уголовные кодексы РСФСР 1926 г. и 1960 г., в которых менялась лишь санкция за совершение мошенничества. Отметим, что в Уголовном кодексе Российской Советской Федеративной Социалистической Республики 1960 г. формулировка мошенничества как преступления имела вид, знакомый нам из Уголовного кодекса Российской Федерации (далее – УК РФ), то есть мошенничество – завладение чужим имуществом или приобретение права на имущество путем обмана либо злоупотребления доверием.

Заключительной стадией утверждения общепринятого понятия мошенничества, его квалифицирующих признаков и установленной санкцией является УК РФ, принятый Государственной Думой в 1996 году, где присутствует восьмой раздел: Преступления в сфере экономики, который открывает глава двадцать первая – Преступления против собственности, где предусмотрена ответственность за мошенничество.

Исходя из вышеуказанного отметим, что с момента принятия УК РФ в последней редакции прошло практически 30 лет, способы совершения преступлений указанной категории развивались, подстраиваясь под новые тенденции общества, например, используя научно-технический прогресс. Такое совершенствование способов совершения мошенничества привело к появлению мошенничества, совершенного с использованием информационно-телекоммуникационных технологий.

§ 2. Базовые элементы криминалистической характеристики мошенничества, совершенного с использованием информационно-телекоммуникационных технологий

Опираясь на представленное выше исследование и анализ исторического

аспекта мошенничество берет свое начало еще с XVII века, отметим, что данный состав преступления, предусмотренный ныне в УК РФ, существует на протяжении трехсот лет. Особенности его расследования опираются на базовых элементах криминалистической характеристики.

Криминалистическая характеристика – это определенная информационная модель, которая отражает криминалистическую сущность преступлений определенного рода. Суть криминалистической характеристики в том, что в ней находятся сведения о криминалистически значимых признаках и их закономерных связях между собой. Как правило, она строится на основе анализа и обобщения практики расследования и судебного рассмотрения преступлений.

В свою очередь, криминалистическая характеристика имеет следующую структуру: личность потерпевшего; личность преступника; обстановка совершения преступления; способ совершения преступления; механизм следообразования.

Рассмотрим базовые элементы криминалистической характеристики мошенничества, совершенного с использованием информационно-телекоммуникационных технологий.

Важным элементом криминалистической характеристики по указанной категории преступлений является личность потерпевшего. Отмечая ранее, укажем, что на данный момент цифровые технологии присутствует в разных сферах у каждого человека. В связи с этим, потерпевшим по данному составу преступления является лицо, использующее информационно-телекоммуникационные технологии. Как правило, это мобильный телефон, который всегда «под рукой» у любого человека.

Анализируя юридическую литературу, конкретные возрастные критерии отсутствуют, в силу того, что целью посягательства злоумышленника может являться как лицо возраста от 18 до 25 лет, так и лицо, достигшее 50 лет. Данный факт обусловлен тем, что преступники пользуются доверчивостью,

внушаемостью и низким уровнем правосознания населения[1].

При этом, потерпевшими становятся лица, которые не осведомлены о способах совершения мошенничества, совершенного с использованием цифровых технологий. Преступники, совершающие такие преступления постоянно придумывают новые «схемы», с помощью которых будущий потерпевший теряет бдительность и поддается провокациям мошенника. В связи с этим, независимо от количества способов обмана и злоупотребления доверием населения, потерпевшим становится лицо, которое не проверяет полученную информацию из различных источников: мессенджеров, смс-сообщений, аудио- и видеозвонков.

Вместе с тем потерпевшими становятся лица, занимающиеся предпринимательской деятельностью в сфере производства товаров и услуг, то есть, та деятельность, которая связана с покупкой сырья или оборудования. Зачастую такие лица становятся потерпевшими, когда предпринимают попытки приобрести интересующий их товар по очень выгодной цене и в последствии сталкиваются с тем, что деньги отправлены покупателем, а товар не отправлен и продавец исчезает.

Нередкий случай, когда потерпевшими становятся лица, желающие заработать быстро и легко. Как правило, злоумышленники рекламируют себя, как целую компанию, которая занимается прогнозированием каких-либо событий: спорт или криптовалюта. Такие злоумышленники вынуждают людей вложить деньги в «оборот ставок» и пропадают вместе с деньгами.

Основной категорией населения для посягательства мошенников являются лица преклонного возраста, которые в силу доверчивости и отсутствия определенных знаний в области цифровых технологий чаще всего подвергаются кибератаками со стороны злоумышленников[2].

---

[1] Волохова О.В., Егоров Н.Н., Жижина М.В. Криминалистика: учебник. М., 2022. С. 103.

[2] Аносов А.В. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учеб. пособие: М., 2023. С. 172.

Рассматривая такой элемент криминалистической характеристики, как личность преступника, отметим, что последний, совершающий мошенничество с использованием информационно-телекоммуникационных технологий – это лицо, владеющее знаниями в области информационно-телекоммуникационных технологий на высоком уровне, способное организовать систему, приносящую доход незаконным способом.

Большая часть хищений совершается мужчинами в возрасте от 18 до 35 лет, обладающими высокими интеллектуальными способностями, которые позволяют нестандартно мыслить, профессиональными навыками владения современными технологиями. Подобные преступления имеют специфичный механизм совершения, который обусловлен особой сложностью, а именно, необходимостью выполнять преступные действия несколькими лица, т.е. кража, совершенная с ИТТ группой лиц. Например, одно преступное лицо совершает звонок потенциальной жертве хищения, тем самым создает необходимые условия для второго преступника, который получает удаленный доступ к мобильному телефону потерпевшего, а далее осуществляет вход в онлайн-приложения банков и совершает кражу денежных средств со счета.

Данная категория преступников предпринимает всевозможные способы анонимизации в сети Интернет: подключаются к сторонним доменам; приобретают одноразовые сим-карты; банковские карты и др. Они совершают именно ту совокупность действий, которая не позволяет органам внутренних дел обнаружить и идентифицировать личность преступника при расследовании таких уголовных дел.

В дополнение ко всему перечисленному стоит отметить, что преступники, совершающие мошенничество с использованием информационно-телекоммуникационных технологий, имеют способности к психологическому давлению на своих выбранных «жертв», в частности, они понимают, что люди преклонного возраста меньше всех уведомлены об устройстве цифровых технологий, обладают легкой внушительностью и склонны легко поддаваться манипуляциям мошенников.

Следующим немаловажным элементом криминалистической характеристики является обстановка совершения преступления, к которой относится характеристика места и времени совершения преступления, т. е. совокупность всех обстоятельств, образующих обстановку совершения мошенничества с использованием цифровых технологий.

По сравнению с другими составами преступлений, предусмотренных УК РФ, обстановка совершения мошенничества с использованием информационно-телекоммуникационных технологий предусматривает довольно-таки скромную характеристику обстоятельств совершения преступления. Это связано с тем, что такое преступление мошенник может осуществлять абсолютно в любое время суток, для него нет разницы в какой период времени осуществить рассылку смс-сообщений, загрузить на сайт приложение, которое содержит вирус, способный взломать мобильное устройство и предоставить доступ к вашим персональным данным или вовсе внушить своей «жертве» то, что произошло какое-либо событие и вынудить перевести на счет злоумышленнику денежные средства.

Важным элементом криминалистической характеристики является способ совершения мошенничества с использованием цифровых технологий. В названии данного состава преступления уже содержится основное средство его совершения – информационно-телекоммуникационные технологии.

Судебной практике известно два способа совершения мошенничества, совершенного с использованием информационно-телекоммуникационных технологий: непосредственный и опосредованный.

Непосредственный способ указанного вида преступления заключается в том, потенциальный потерпевший напрямую взаимодействует с мошенником, в частности, таким способом совершается: фишинг, рассылка сообщений в мессенджерах или по электронной почте, смс-сообщений по номеру телефона абонента.

Суть опосредованного способа в том, что потерпевший сталкивается с проработанной и сложной системой, которая в совершенстве продумана

злоумышленниками. В данном случае, потерпевшее лицо может взаимодействовать с несколькими лицами (оператор, посредник, курьер и др.). Опосредованным способом совершается смишинг, спуфинг, вишинг и т.д.

Так, в ходе расследования уголовного дела установлено, что в период с сентября 2019 года по апрель 2020 года неустановленное лицо, находясь в неустановленном следствии месте, под предлогом помощи заработать денежные средства в приложении «LBLV» «игровая биржа», путем обмана и злоупотребления доверием гр-на ****, проживающего по адресу: УР, ****, умышленно, из корыстных побуждений, незаконно завладело принадлежащими ему денежными средствами в размере около 6 800 000 рублей 00 копеек, которые **** сам переводил со своего «Киви-Кошелька» на игровую биржу «LBLV». Похищенным имуществом неустановленное лицо распорядилось по своему усмотрению, причинив своими действиями **** материальный ущерб в размере около 6 800 000 рублей 00 копеек в особо крупном размере[1].

В первую очередь, то, с чего началось направление мошенничества, совершаемого с использованием цифровых технологий – фишинг («fishing» с английского «рыбалка»). В данном случае мошенник, отправляет рассылку с ссылкой многим пользователям, и переходит по ссылке, которая либо содержит вредоносный вирус, либо в которой необходимо ввести свои персональные данный для псевдоавторизации.

Фишинговая систеема бывает четырех видов: электронный фишинг; смс-фишинг (смишинг); фишинг через звонки (вишинг); целевой фишинг (спирфишинг).

Электронный фишинг подразумевает под собой рассылку писем по электронной почте или в мессенджере, которое выглядит как сообщение от банка, магазина или другой официальной организации. Сообщение содержит в себе ссылку, перейдя по которой необходимо подтвердить вход в аккаунт и

[1] Уголовное дело №1240194001203**** // Арх. СО МО МВД России «Увинский». Оп. 2. 231 л.

удостовериться в персонализации пользователя. В свою очередь, пользователь вводит свои личные данные, которые попадают в руки злоумышленника. Мошенник, имея в своих руках персонализацию пользователя получает доступ аккаунтам различных систем, например, банковских приложений, личного кабинета портала «Госуслуг» и т.д. В следствие чего на пользователя могут быть оформлены кредиты в микрофинансовых кредитных организациях.

Смишинг происходит аналогично электронному фишингу, при котором приходит смс-сообщение на номер телефона потенциальной жертвы под видом службы доставки или государственных органов. К такому смс-сообщению прикрепляется интернет-ссылка, переходя по которой цифровое устройство абонента «заражается» вирусом, который предоставляет полный доступ к мобильному телефону или компьютеру человека, вплоть до демонстрации экрана и отслеживания его действий. Следовательно, мошенник получает доступ и к учетным записям пользователя устройства, куда входят банковские учетные записи, а также Портала Государственных услуг.

Вишинг – это вид фишинга, где пользователю мобильного устройства поступает входящий вызов, в котором злоумышленник представляется сотрудником банковской организации, сотрудником полиции или почты и просит сообщить данные, чаще всего код, который состоит из определенной комбинации цифр. Свои действия мошенник зачастую обуславливает тем, что учетная запись пользователя подверглась атаке со стороны злоумышленников, пытающихся взломать ее. Получая код, преступник аналогично вышеуказанным способам получает доступ к учетной записи пользователя.

Целевой фишинг заключается в персонализированной кибератаке на конкретного человека или компанию в целях получения данных не учетной записи, а каких-либо сведений, подтверждающих конкретные его действия. Чаще всего такой способ является «заказным», с целью устранения конкурентов на «рыночной арене».

Вторым самым распространенным способом совершения мошенничества с использованием информационных технологий является «спуфинг». Суть

данного способа мошенничества, совершенного с использованием информационно-телекоммуникационных технологий в том, что мошенник создает интернет-сайт, который в точности похож на оригинальный. В судебной практике встречаются частые случаи, когда пользователь, не удостоверяясь в подлинности интернет-ресурса, совершает там покупку каких-либо товаров или услуг, но при этом отправляет свои денежные средства злоумышленнику.

Самым распространенным способом использования спуфинга на данный момент является создание злоумышленником аккаунта от лица девушки, регистрация на сайте знакомств и знакомство с лицом мужского пола. В ходе общения злоумышленник предлагает приобрести билеты в определенный кинотеатр для совместного просмотра, отправляет свой поддельный интернет-сайт, на котором будущая жертва осуществляет покупку билетов, получает потерянные денежные средства, которые были отправлены мошеннику[1].

Исследуя вышеперечисленные способы мошенничества, совершенного с использованием информационно-телекоммуникационных технологий, появляется возможность в разработке рекомендаций и совершенствования алгоритмизации производства следственных действий в целях повышения качества и эффективности расследования указанной категории преступлений.

§ 3. Понятие и сущность следственных действий, как объекта алгоритмизации при расследовании мошенничеств, совершенных в сфере информационно-телекоммуникационных технологии

Принимая уголовное дело к своему производству, следователю рекомендуется в первую очередь установить следственную обстановку и понять, как найти доказательства вины подозреваемого. Для выполнения данной задачи следователем применяются следственные действия.

---

[1] Кузнецова А.А., Мазунина Я.М. Криминалистика (общие положения, техника, тактика): учеб. для вузов / М. М. Горшков [и др.]; М., 2022. С. 297.

Отсутствие понятия следственного действия – один из пробелов действующего уголовно-процессуального законодательства. Изучая юридическую литературу, отмечается, что понятие «следственное действие» рассматривается в нескольких значениях.

В широком смысле следственное действие – процессуальные действия, которые совершаются уполномоченными органами в предварительном расследовании, либо действие следователя или дознавателя, которое регламентировано Уголовно-процессуального кодекса Российской Федерации (далее – УПК РФ), направленное на расследование по конкретному уголовному делу.

По мнению В. М. Лебедева, следственное действие, как регламентированное УПК РФ и выполняемое должностными, ответственными за производство по уголовному делу, процессуальные мероприятия, состоящие из последовательных этапов поискового, фиксирующего и удовлетворяющего характера при соблюдении и обеспечении прав и законных интересов участников процесса, в ходе которых решаются задачи по обнаружению и закреплению доказательств»[1].

Следует выделить главные признаки, характеризующие следственные действия:

1. Цель следственных действий – сбор и проверка доказательств;

2. Производство следственных действий урегулирована УПК РФ;

3. Следственные действия вправе проводить только определенные должностные лица;

4. В процессе проведения следственных действий возможно применение мер процессуального принуждения;

5. Для следственных действий, которые затрагивают и посягают на

[1] Корчагин А.А. Следственные ситуации и алгоритмы в деятельности по предварительному расследованию и судебному разбирательству уголовных дел об убийствах // Научные ведомости. Серия Философия. Социология. Право. 2023. № 20 (115). Выпуск 18, С. 114–119.

конституционные права и свободы граждан, требуется судебное постановление.

Для расследования преступления следователю необходимо своевременно выбрать необходимое следственное действие, которое позволит в полной мере даст информацию о механизме преступления и виновности лица, его совершившего.

Согласно мнению М. Б. Вандера, следователи нуждаются в вышестоящем руководстве при расследовании сложных следственных ситуаций, отличие которых в дефиците информационного обеспечения, времени, противодействии со стороны заинтересованных лиц, в особенности, их попытки ввести следствие в заблуждение[1].

Исходя из этого, важнейшее значение имеет разработка и использование алгоритмизации следственных действий следователем при расследовании преступлений, что должно повысить уровень эффективности и качества деятельности следователя.

Понятие «алгоритмизация следственных действий» было рассмотрено многими учеными-криминалистами, такими как Р. С. Белкин, В. К. Гавло, Е. П. Ищенко, Г.А. Густов, Н. А. Селиванов, А. А. Корчагин и др.

В свою очередь, В. К. Гавло считает, что алгоритм следственного действия – это научно-обоснованное точное изложение последовательности следственных действий следователя, их комплексов, которые являются наиболее применимыми к конкретным следственным ситуациям, выполнение которых обеспечивает решение поставленных задач по раскрытию и расследованию преступлений[2].

По мнению, А. А. Корчагина, алгоритм – это инструкция, включающая в себя точный и строгий порядок действий для достижения решения

---

[1] Коновалова В.Е. Тактика производства обыска. Харьков, 2025. С. 38.

[2] Ахмедшин Р.Л. Тактика экспериментальных следственных действий: монография. М., 2022. С. 202.

поставленной задачи[1].

В юридической литературе указывают семь этапов процесса построения криминалистических алгоритмов при проведении следственных действий.

На первом этапе следователю необходимо организовать поиск и сбор первичной информации о преступлениях того вида, по которому возбуждено уголовное дело. Это производится путем взаимодействия следователя с другими подразделениями как вербальным, так и невербальным способом, но, как показывает практика, зачастую следователь исследует и анализирует «закрытые» уголовные дела, по которым уже вынесен приговор суда.

На втором этапе следователь, по окончании сбора, исследования и анализа первичной информации о преступлениях должен, на основании полученных данных выделить типичные следственные ситуации и ряд следственных действий, используемых при расследовании таких ситуаций.

На третьем этапе следователю, имея ряд выделенных следственных ситуаций, необходимо поставить задачи, решение которых достигается путем проведения следственных действий, которые характерны для каждой следственной ситуации.

Четвертый этап заключается в определении следователем средств для решения поставленных задач по конкретному алгоритму. Из данного этапа вытекает последующий: следователь должен выбрать подходящие методы для построения алгоритма.

Суть шестого этапа заключается в построении четкого алгоритма действий следователя, которые необходимо провести в отношении конкретного преступления, направленные на его эффективное и качественное раскрытие и расследование.

Заключительный этап построения алгоритма. Следователю необходимо проверить экспериментальным путем, эффективность и качество построенного алгоритма, а также произвести корректировку поставленных им действий,

---

[1] Кузнецова А.А., Муравьева К.В. Криминалистика: учеб.-нагляд. пособие. Омск, 2020. С. 71.

применяемого к конкретной следственной ситуации.

Таким образом, алгоритмизация следственных действий является четкой и пошаговой методической инструкцией следователя, подробное описание всех его действий, направленных на решение задач расследования преступления. Четкое соблюдение такой инструкции следователем позволит достичь требуемого результата: эффективное и качественное расследование преступления с экономией времени и сил.

ГЛАВА 2. ОРГАНИЗАЦИОННО-ТАКТИЧЕСКИЕ ОСОБЕННОСТИ ПРОИЗВОДСТВА СЛЕДСТВЕННЫХ ДЕЙСТВИЙ ПРИ РАССЛЕДОВАНИИ МОШЕННИЧЕСТВ В СФЕРЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

§ 1. Особенности производства следственных действий на первоначальном этапе расследования мошенничеств в сфере информационно-телекоммуникационных технологий

На первоначальном этапе расследования мошенничества, совершенного с использованием информационно-телекоммуникационных технологий, формируются типовые следственные ситуации, которые выступают ориентиром в планировании и выборе проведения тех или иных следственных действий. Исходя из этого, результат глубокого анализа сложившейся ситуации следствия предопределяет верность принятых тактических решений и выстроенной модели следственной версии.

В настоящее время в науке криминалистики понятие следственной ситуации является дискуссионным[1]. На наш взгляд, наиболее полное и точное определение следственной ситуации дает деятель науки Р. С. Белкин, который определяет, что следственной ситуацией является комплекс условий проведения расследования на данный момент времени, то есть, это подразумевает ту обстановку, в которой проходит процесс доказывания[2].

Представленное определение понятия отвечает концепции для разработки алгоритма действий следователя необходимо рассмотреть следственные ситуации, возникающие при раскрытии и расследовании такого преступления, от которых зависит определение действий следователя, а также

---

[1] Лузгин И.М., Муравьева Я.В. Методика изучения, оценки и разрешения исходных следственных ситуаций // Исходные следственные ситуации и криминалистические методы их разрешения. М., 2022. С. 14–16.

[2] Белкин Р.С. Криминалистика: проблемы, тенденции, перспективы. М.: Юридическая литература, 1988. С. 116.

их порядок.

В зависимости от возможности достижения цели расследования, следственные ситуации делятся на благоприятные и неблагоприятные:

Благоприятные следственные ситуации, характеризуется тем, что известно лицо, совершившее преступление, его событие, но при этом необходимо установить обстоятельства преступного деяния. В свою очередь в неблагоприятной следственной ситуации отсутствует лицо, совершившее преступление, нет достаточной информации о событии преступления.

В ходе расследования мошенничества, совершенного с использованием информационно-телекоммуникационных технологий, могут быть сформулированы более конкретные следственные ситуации:

1. Имеется информация о способе совершения преступления, личности преступника, при этом выявлены следы преступления.

При данной следственной ситуации информация об обстоятельствах события преступления могут быть установлены из разных источников:

– самим заявителем, который запомнил признаки, индивидуализирующие лицо, совершившее преступление, а также обстоятельства события преступного деяния.

– информация о лице и событии преступления получена в ходе проведения оперативно-розыскных мероприятий или в результате раскрытия и расследования других преступлений.

– лицо было задержано на месте совершения преступления.

2. Имеется информация о способе совершения преступления, выявлены следы преступления, при этом сведения о личности преступника отсутствуют.

3. Информация о способе совершения преступления известна, при этом объем выявленных следов незначительный, сведения о личности преступника отсутствуют.

4. Информация о способе совершения известна, выявлены следы преступления, имеются следы преступления, имеются сведения о личности преступника, но его местонахождение неизвестно.

В зависимости от конкретной следственной ситуации следователю необходимо составить следственные версии для последующего планирования предварительного следствия.

В криминалистике выделяются общие и частные следственные версии, где общие версии направлены на установление и проверку события или состава преступления, его признаков. Частные версии нацелены на установление обстоятельств, сопутствующих совершению преступления, которые влияют на его квалификацию.

Исходя из правоприменительной практики, общими следственными версиями являются:

1. Отсутствует состав и событие преступления;

2. Было совершено мошенничество, совершенное с использованием информационно-телекоммуникационных технологий, при обстоятельствах, указанных в заявлении потерпевшего;

3. Был совершен иной вид преступления, предусмотренный УК РФ.

4. Помимо мошенничества, совершенного с использованием информационно-телекоммуникационных технологий, был совершен иной состав преступления, предусмотренный УК РФ.

К частным версиям относят:

1. Злоумышленниками были использованы вредоносные программные обеспечения в целях получения доступа к персональным данным потерпевшего.

2. Злоумышленниками использовались поддельные веб-сайты или электронные письма, чтобы потерпевший ввел свои персональные данные.

3. Злоумышленники представились должностным лицом, оказывая психологическое давление на потерпевшего.

4. Преступление было совершено сотрудниками, имеющими доступ к базам персональных данных населения.

5. Злоумышленники получили доступ к персональным данным потерпевшего, используя подмену sim-карт или спровоцированную утечку

данных.

Используя следственные ситуации и следственные версии, следователь планирует процесс предварительного расследования, в котором основным первоначальным следственным действием является осмотр места происшествия.

Осмотр значительно обобщается относительно следственных действий, перечисленных в главе 24 УПК РФ, цель которых состоит в обнаружении следов преступления, выяснении других обстоятельств, имеющих значение для уголовного дела. Исходя из анализа содержащихся в ней правовых норм, представляется возможным сформулировать перечень следственных действий, объединяемых понятием «осмотр».

В части 1 ст. 176 УПК РФ законодателем предусмотрены следующие виды следственного осмотра: осмотр места происшествия, местности, жилища, иного помещения, предметов и документов.

При этом, исследуя и анализируя положения уголовно-процессуального законодательства можно дополнить данный перечень такими видами, как осмотр трупа (ст. 178 УПК РФ) и освидетельствование (ст. 179 УПК РФ)[1].

Применительно к мошенничеству, совершенному с использованием информационно-телекоммуникационных технологий, при проверке сообщений о преступлении и в ходе предварительного расследования производятся различные виды осмотра: осмотр места происшествия, жилища, помещений, предметов и документов. При проведении первоначального следственного действия следователями допускается ряд ошибок, например, проведение осмотра места происшествия в неполной мере, то есть, отсутствует фиксация и изъятие всех материальных следов совершения преступления, отсутствие специалиста, обладающего специальными познаниями в области цифровых технологий.

---

[1] Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 18 декабря 2001 г. № 174-ФЗ // Собрание законодательства Российской Федерации. – 2001. – № 52. Ст. 4921.

Данное следственное действие осуществляется при помощи следующих методов: наблюдение; измерение; описание; сравнение; экспериментальный метод; моделирование.

При проведении данного следственного действия является то, что на место происшествия могут прибыть, помимо следственно-оперативной группы, различные руководители Министерства внутренних дел Российской Федерации (далее – МВД РФ), которые, в свою очередь, дают указания следователю.

В ходе производства осмотра следователю рекомендуется руководствоваться своими знаниями, навыками его проведения.

Осмотр места происшествия – это неотложное следственное действие, которое заключается в непосредственном восприятии следователем обстановки места происшествия и установление, фиксацию, исследование обстановки места происшествия, следов преступления и иных данных, позволяющих в совокупности с другими доказательствами сделать вывод о механизме происшествия и других обстоятельств расследуемого события.

Целями данного следственного действия являются: определение характера осмотра места происшествия; обнаружение, фиксация, изъятие следов преступления; анализ обнаруженного для построения суждений о механизме и обстоятельствах расследуемого события; получение данных для поиска лица, совершившего преступление.

Осмотр места происшествия проводится по каждому зарегистрированному сообщению о преступлении, при этом, при расследовании мошенничества в сфере информационно-телекоммуникационных технологий объектом осмотра могут являться различные предметы. При осмотре места с конкретным объектом следователь выбирает необходимый порядок проведения следственного действия.

Персональный компьютер и мобильный телефон являются наиболее распространенными объектами осмотра места происшествия при проверке сообщения о мошенничестве, совершенного с использованием

информационно-телекоммуникационных технологий[1].

В случае, если объектом осмотра места происшествия является пользовательский компьютер, то следователю необходимо в первую очередь обратить внимание на подготовку:

1. Обеспечить наличие участников следственного действия.

Следователю в ходе осмотра интересна информация, находящаяся непосредственно на самом пользовательском компьютере. Первоочередно необходимо обеспечить участие собственника компьютера, а также следователь должен сделать отметку в протоколе осмотра места происшествия о том, что собственник дает свое согласие на осмотр компьютера.

Лицо, обладающее специальными познаниями в области цифровых технологий (специалист), обязательно должен участвовать при проведении осмотра любого устройства, а также в случае, когда есть необходимость в изъятие электронного носителя информации (ч. 2 ст. 164 УПК РФ).

Что касается наличия у специалиста специальных знаний, то они необходимы не только в сфере устройства и структурности компьютера, но и в области оборота информационных данных на цифровом устройстве.

К ним относятся следующие специальные знания: по основам работы операционных систем (Microsoft Windows, Linux, MacOS и т. д.) и особенностям хранения данных; по исследованию метаданных файлов; по работе с различными видами баз данных; по исследованию истории сетевых соединений различных интернет-браузеров; по исследованию истории переписки с помощью почтовых клиентов и программ для мгновенного обмена сообщениями; по поиску данных в свободной и неразмеченной области носителя информации; по восстановлению данных; по созданию побитовых копий носителей информации и работе с ними; по корреляции событий по времени; по эмулированию системы; по исследованию журналов и карантина антивирусного программного обеспечения; по исследованию dumpов

[1] Криминалистические аспекты производства следственных действий: учеб. пособие / под общ. ред. М.М. Горшкова. Омск, 2020. С. 89.

оперативной памяти* и сетевого трафика.

2. Использование специального программного обеспечения при осмотре пользовательского компьютера.

Предприняв все необходимые меры к подготовке проведения осмотра места происшествия, объектом которого является пользовательский компьютер, следователь приступает к рабочему этапу осмотра, который включает в себя несколько стадий:

1) Статический осмотр, в ходе которого следователь фиксирует в протоколе осмотра места происшествия общие визуальные признаки цифрового устройства;

2) Детальный осмотр, где следователь фиксирует факт наличия элементов питания, внешних жестких дисков, карт памяти и т. д;

3) «Внутренний» осмотр, в процессе которого следователь осматривает и фиксирует непосредственно информацию, находящуюся на устройстве.

Стоит отметить, что пользовательский компьютер состоит из определенных частей: системный блок и устройства ввода и вывода информации (монитор, клавиатура, компьютерная мышь, принтер, сканер и т. д.). При статическом осмотре в первую очередь необходимо зафиксировать в протоколе наличие следов механического вмешательства или иных повреждений.

В ходе детального осмотра системного блока необходимо зафиксировать в протоколе осмотра места происшествия следующие сведения: какие интерфейсы были использованы при работе устройства, к каким внешним устройствам они были подключены, длина соединений; присутствуют ли внешние физические повреждения (царапины, сколы, загибы и т.д.) на корпусе системного блока и его внутренних составляющих; имеются ли специальные «слоты» для подключения внешних устройств.

После этого, следователь должен зафиксировать в протоколе осмотра места происшествия марку, модель, серийный номер.

В ходе проведения осмотра внутренних составляющих системного блока,

следователь должен уделить внимание комплектующим (материнская плата, оперативная память, блок питания, видеоадаптер, центральный процессор, накопители информации, устройства чтения). Если какая-либо из комплектующих отсутствует, то данный факт необходимо зафиксировать в протоколе осмотра места происшествия.

Так, в ходе расследования уголовного дела по ч. 4 ст. 159 УК РФ Межмуниципального отдела МВД России «Увинский» в протоколе осмотра места происшествия отмечается: «… под столом располагается системный блок в корпусе серого цвета марки «FORMOZA», левая боковая стенка корпуса отсутствует. Системный блок имеет следующие размеры: 43 см высота, 18 см ширина, 42 см длина. Левая боковая крышка отсутствует, внутри имеется блок питания с наклейкой, на которой указано: «MODEL NO: ATX-300 PNR», один жесткий диск марки «Seagate Barracuda 7200.12 320 GB»; одна материнская плата наименование «GIGABYTE GA-P31-S3G»; одна видеокарта с наклейкой, где указано «GT 630 1024M sDDR3 128B CRT DVI HD MI, PIN: NEAT630NHD1-1085F»[1].

Затем необходимо подключить устройство питания пользовательского компьютера и запустить его. Осмотр информационного содержимого компьютера начинается с анализа запущенного программного обеспечения. Полный список работающих служб и приложений можно получить через диспетчера задач, который вызывается в системах на базе: Windows — комбинацией клавиш Ctrl + Shift + Esc; Linux — командой в консоли «Gnome-system-monitor» (в случае, если Linux на Gmone) либо в разделе системных утилит «Диспетчер задач»; MacOS — сочетанием клавиш Cmd + Alt + Esc.

После этого необходимо изучить формат и содержание каждого из обнаруженных файлов. Зафиксированные сведения необходимо учитывать при анализе и исследовании метаданных файлов, которые содержат информацию, необходимую для расследования преступления.

---

[1] Уголовное дело №1210194001201**** // Арх. СО МО МВД России «Увинский». Оп. 1. 152 л.

В случае обнаружения информации, которая имеет значение для расследования уголовного дела, ее необходимо зафиксировать в протоколе осмотра места происшествия одним из способов: зафиксировать их с помощью клавиши «printscreen» на клавиатуре устройства или использовать фотофиксацию экрана монитора компьютера; создать резервную копию сведений на любой внешний носитель (CD-диск, флеш-карта).

По завершении осмотра цифровое устройство необходимо упаковать, опечатать оттиском печати и заверить подписями следователя, а также участвующих лиц, подписав следующим образом: «Пользовательский компьютер, изъятый в ходе осмотра места происшествии. Упаковывая устройство, необходимо использовать такие материалы и инструменты, которые не окажут на компьютер негативного воздействия, приводящего к потере информации. Накопители жестких магнитных дисков следует упаковать в специальные боксы, способные экранизировать воздействие магнитного поля и обезопасить от внешних повреждений.

Допрос – это следственное действие, проводимое следственным органом и направленное на получение сведений о совершении преступления, от допрашиваемого (подозреваемого, обвиняемого, подсудимого, потерпевшего, свидетеля, специалиста и эксперта).

Допрос как следственное действие регламентируется Конституцией Российской Федерации (51 статья), а также УПК РФ (187 – 191 статьи).

Допрос является наиболее распространенным следственным действием, которое присутствует в каждом уголовном деле. При этом, данное следственное действие является эффективным средством для получения новых доказательств и проверке тех, которые уже присутствуют у следователя.

Выделяются следующие цели допроса:

1. Установление наличия/отсутствия обстоятельств, которые подлежат доказыванию по конкретному уголовному делу.

2. Установление источников, которые могут содержать данные, имеющие важное значение для раскрытия и расследования уголовного дела.

3. Проверка достоверности имеющихся доказательств.

При расследовании мошенничества, совершенного с использованием информационно-телекоммуникационных технологий, одним из самых важных следственных действий является допрос потерпевшего. Данный факт обуславливается тем, что следователю крайне необходимо установить четкую последовательность действий потерпевшего, хронологию действий мошенника, для того, чтобы выбрать определенную стратегию расследования уголовного дела.

Следователю при допросе потерпевшего необходимо учитывать следующие особенности. Во-первых, потерпевший – это заинтересованное лицо в уголовном деле. Во-вторых, потерпевший напрямую сталкивается с совершением противоправного деяния и, как правило, теряет либо свои денежные средства, либо свое имущество. Несомненно, данный факт негативно сказывается на психологическое состояние потерпевшего. В-третьих, потерпевший может выйти за пределы вопросов следователя. В-четвертых, показания потерпевшего являются непосредственным средством защиты его прав[1].

Таким образом, допрос потерпевшего целесообразно проводить по следующему алгоритму.

Важная часть проведение данного следственного действия – подготовка следователя к его проведению. На данном этапе следователь должен собрать и изучить сведения о допрашиваемом лице; выбрать нужное время и место; подготовить научно-техническое обеспечение; спланировать ход допроса, то есть подготовить определенный перечь вопросов.

Следователю необходимо заполнить вводную часть протокола допроса с помощью документа, удостоверяющего личность потерпевшего. Далее потерпевший удостоверяет достоверность его личных данных своей подписью.

Следователь должен разъяснить потерпевшему его права и обязанности,

[1] Лурия А.Р. Маленькая книжка о большой памяти. Хрестоматия по общей психологии допроса. Психология допроса. Москва, 2022. С. 68.

а также предупредить об уголовной ответственности за дачу заведомо ложных показаний в соответствии со ст. 308 УК РФ. Потерпевший должен поставить подпись в данной части протокола допроса, чем подтверждает факт ознакомления с его правами, обязанностями и уголовной ответственностью.

В данном случае следователю необходимо предложить потерпевшему в формате свободного рассказа дать показания. При этом, важно отметить, на данном этапе следователь должен применить свои знания криминалистической тактики допроса. (акцентировать внимание на оговорках, не перебивать потерпевшего, выписывать моменты, которые необходимо уточнить или дополнить, а также использовать криминалистические приемы для допроса в бесконфликтной ситуации и т.д.). Потерпевший излагает, как и когда произошло преступление.

После этапа свободного рассказа допрос переходит на другой этап: вопрос-ответ. На данном этапе следователь должен задать потерпевшему уточняющие, дополняющие, контрольные, изобличающие, напоминающие вопросы. Следователю стоит акцентировать свое внимание на обстоятельствах совершения мошенничества и при необходимости уточнить их. Следователь заполняет основную часть протокола допроса от первого лица.

Потерпевшему вновь необходимо ознакомиться с содержанием протокола допроса, прочитав его лично или вслух следователем. На данном этапе потерпевший имеет право уточнить или дополнить свои показания или сделать замечание по содержанию протокола.

Особенностями при проведении данного следственного действия заключается в том, что крайне необходимо установить, как именно общался потерпевший с мошенником (через аудиозвонок, смс-сообщениями, через мессенджер).

При этом, обязательному установлению следователем подлежит конкретная сумма ущерба, которая повлияет непосредственно на квалификацию преступления, предусмотренного Уголовным кодексом Российской Федерации, а также факт неправомерного доступа к компьютерной

информации, повлекший копирование, блокирование, уничтожение и модификацию компьютерной информации потерпевшего. При обнаружении данного факта, следователь должен в последующем составить рапорт об обнаружении признаков состава преступления, предусмотренного Уголовным кодексом Российской Федерации[1].

В случае установления факта неправомерного доступа к компьютерной информации, следователь должен проверить в первую очередь личный кабинет Единого портала «Госуслуги» через онлайн-приложение, которое доступно для всех цифровых устройств, наличие сторонних IP-адресов, с которых выполнена авторизация в личном кабинете потерпевшего.

Установив все вышеуказанные факты, следователю необходимо вынести постановление о производстве выемки цифрового устройства потерпевшего и в последующем составить поручение в отдел по борьбе с киберпреступлениями, который установит факт наличия вредоносных программных обеспечений, а также сторонние IP-адреса.

Подведем итог, проведение следственных действий на первоначальном этапе является ключевым этапом при расследовании мошенничества, совершенного с использованием информационно-телекоммуникационных технологий. На данном этапе органы предварительного следствия собирают цифровые и материальные следы, изучают обстоятельства совершения преступления, проводят мероприятия, направленные на изобличение личности преступника и корректируют последующий план расследования.

§ 2. Особенности производства следственных действий на последующем этапе расследования мошенничеств в сфере информационно-телекоммуникационных технологий

В случае, если правоохранительные органы смогли установить лицо,

[1] Еникеев М.И., Образцов В.А., Эминов В.Е. Следственные действия: психология, тактика, технология: учеб. пособие. М., 2007. С. 39.

совершившее мошенничество в сфере информационно-телекоммуникационных технологий, появляется необходимость в допросе лица в качестве подозреваемого.

В отличии от проведения допроса потерпевшего, проведение допроса подозреваемого гораздо сложнее. Особенность производства допроса подозреваемого заключается в том, что следователю необходимо подобрать индивидуальный подход к подозреваемому лицу, в силу того, что именно этот субъект уголовного дела владеет обладает информацией об всех обстоятельствах совершения преступления.

Алгоритм проведения допроса следующий:

1) Следователю важно понимать, что ему необходимо установить хронологию, средства и способы совершения преступления, куда было сбыто имущество, как реализовано, какими способами и установить соучастников совершения преступления. Учитывая весь вышеуказанный перечень обстоятельств, подлежащих установлению, следователю необходимо основательно подготовиться к проведению данного следственного действия.

2) Также важно помнить, что во время допроса могут присутствовать как его защитник, так и законный представитель. В таком случае следователь должен уведомить их о месте и времени проведения допроса.

3) Как и в любом допросе, перед его началом следователь заполняет вводную часть протокола допроса подозреваемого, опираясь на его документ, удостоверяющий личность.

4) Подозреваемый ставит подпись, подтверждая подлинность данных, заполненных следователем.

5) Следователь разъясняет подозреваемому его права и обязанности, в подтверждение чего подозреваемый ставит свою подпись в протоколе допроса.

6) Вначале допроса следователь должен предоставить подозреваемому право в свободной форме рассказать об обстоятельствах совершенного преступления. Зачастую подозреваемый отказывается давать показания, ссылаясь на статью 51 Конституции РФ или попросту отрицает свою

причастность к совершенному преступлению. В данном случае следователю стоит использовать тактические приемы при допросе: внушить уважение к следователю; вызвать интерес к процессу общения со следователем; проявить заботу о соблюдении прав допрашиваемого; создать спокойную обстановку допроса; проявлять тактичность, выдержку, культуру речи, стимулировать положительные качества подозреваемого и предъявлять доказательства, имеющиеся у органов предварительного следствия, как правило, доказательства предъявляются «по восходящей», то есть от менее значимых к более значимым.

7) В случае, если следователю удалось вызвать желание подозреваемого давать показания, он должен предоставить возможность подозреваемому в форме свободного рассказа повествовать о содеянном. На данном этапе следователю целесообразно использовать хронологический порядок по каждому эпизоду. Соответственно, при отказе давать показания, в протоколе допроса подозреваемого следователю стоит сделать отметку об этом.

8) Далее следователь переходит к следующему этапу допроса: вопросно-ответному. В ходе данного этапа следователь, аналогично предыдущим рассматриваемым допросам, задает уточняющие, дополняющие, изобличающие вопросы и др. Важно отметить, что следователь должен полностью исключить наводящие вопросы, так как защитник может попросить зафиксировать конкретную формулировку вопроса, чтобы использовать это во время судебного разбирательства, ссылаясь на то, что был нарушен порядок проведения следственного действия. В данном случае, есть возможность, что суд признает данное доказательство не допустимым.

9) Следователь заполняет основную часть протокола допроса.

10) Подозреваемому и защитнику необходимо ознакомиться с протоколом допроса лично или с помощью прочтения следователем вслух, в подтверждение чего подозреваемым и защитником ставится подпись в протоколе.

11) Если у подозреваемого или защитника имеются дополнения или

замечания по содержанию протокола, следователь должен сделать об этом соответствующую пометку в протоколе.

12) Подозреваемый и защитник подписывают каждую страницу протокола, а следователь последнюю страницу протокола.

В момент подписания протокола, следователю стоит сохранить бдительность, так как зачастую подозреваемый не справляется с эмоциональной нагрузкой, в связи с осознание того факта, что он понесет уголовную ответственность, и совершит попытку уничтожения или повреждения заполненного протокола допроса, в целях создания трудностей для предварительного расследования.

Бывают и случаи, когда подозреваемый попросту отказывается подписывать протокол допроса. При таком условии следователь должен выяснить причину отказа и сделать соответствующую отметку в протоколе допроса, которая подписывается следователем, а также защитником.

Так, при расследовании уголовного дела №1240194001203**** части 3 статьи 159 УК РФ Межмуниципального отдела МВД России «Увинский» следователем проведен допрос подозреваемого, где в ходе свободного рассказа подозреваемый пояснил, следующее: «В июне 2023 года в мессенджере «Телеграмм» искал работу, и наткнулся на чат «МФО Комьюнити», где общались люди о заработках, а именно: писали как можно оформить микрозаймы на людей, зная их паспортные данные, оформление займов через Госуслуги. Для этого нужно было купить в этом же чате номер телефона ПАО «МТС», который уже не используется клиентом и который до этого был привязан к Госуслугам, далее купить пустую сим-карту ПАО «МТС» с саморегистрацией в интернет-магазине «OZON» (сим-карты с саморегистрацией «пустые», то есть не имеют определенного абонентского номера, его нужно вводить самому). Активировать сим-карту, то есть ввести абонентский номер и указать анкетные данные лица владельца данного абонентского номера, вставить в телефон, зайти на портал Госуслуг, ввести логин – номер телефона этой сим-карты, нажать «забыли пароль», после чего

должно прийти СМС-сообщение с кодом для смены пароля, сменить пароль и зайти в личный кабинет этого человека. Далее нужно было в сети Интернет найти микрокредитные организации, где пройти регистрацию через данные личного кабинета Госуслуг и отправить заявки на интересующие суммы.

06 января 2024 года, в ночное время около 03 часов 40 минут я находился дома у своего друга *** по адресу: ***. В тот момент в моем пользовании находился сотовый телефон марки «Iphone 12 pro» с сим-картой сотового оператора «Теле 2», он был оформлен на мою маму ***. В то время испытывал финансовые трудности, совсем не было денег, тогда решил попробовать оформить микрокредит как читал в чате «МФО Комьюнити», на тот момент понимал, что это неправомерно, но очень нужны были деньги. На тот момент были купленные в интернет-магазине «OZON» пустые сим-карты МТС в количестве 10 штук. Далее зашел в приложение мессенджера «Телеграмм» и в чате «МФО Комьюнити», прочитал подробно всю схему оформления микрозаймов на 3-х лиц, я написал боту «МФО Комьюнити» слово «Старт», далее мне отправили инструкцию как купить номер телефона, выбрал один номер ***, где были указаны серия и номер паспорта человека под именем ***, оплатил около 100 рублей за этот номер, но с какого счета и куда уже не вспомню. После чего я взял одну пустую сим-карту с саморегистрацией, через браузер телефона «Сафари» зашел на сайт ПАО «МТС», где ввел номер ***, активировал его на свое имя по своим паспортным данным. Далее достал из своего телефона сим-карту «Теле 2» и вставил активированную сим-карту МТС с номером ***. После чего через тот же браузер телефона «Сафари» зашел на сайт портала «Госуслуги», нажал вкладку «забыли пароль» и ввел номер телефона ***, после этого на указанный номер пришел цифровой код, который ввел, поменял пароль, тем самым неправомерно вошел в личный кабинет человека с данными ***, **** года рождения, посмотрел его анкетные данные, там были указаны данные паспорта, СНИЛС, ИНН, адрес прописки был г. ***, его данные не изменял, только скопировал их, чтобы в последующем ими воспользоваться для оформления займов. После этого со своего телефона с

браузера «Сафари» нашел микрокредитную организацию «Турбозайм», где авторизировался под скопированными данными с личного кабинета Госуслуг *** на сумму в 8 000 рублей, почти сразу пришел положительный ответ, деньги перевел своему другу ***, которые в последующем снял и потратил на личные нужды. За моими действиями никто не наблюдал, никому об этом не рассказывал»[1].

Получив все необходимые показания в ходе допроса подозреваемого, может появиться необходимость в проведении следственного действия – обыск в жилище подозреваемого.

Обыск как следственное действие подразумевает отыскание и изъятие объектов, имеющих значение для расследования уголовного дела.

На первый взгляд, кажется, что следственное действие простое, но тем не менее, следователи зачастую допускают ряд ошибок при производстве обыска:

– неправильный подбор участников обыска.

– неполноценная подготовка к производству следственного действия.

Для производства данного следственного действия следователю необходимо подготовить постановление о возбуждении перед судом ходатайства о производстве обыска в жилище. В нем следователь аргументирует свое решение о проведении данного следственного действия, так как при его производстве нарушаются права человека и гражданина на неприкосновенность жилища, предусмотренные в Конституции РФ.

Производство обыска в ходе расследования мошенничества в сфере информационно-телекоммуникационных технологий имеет ряд особенностей. Целесообразно установить их содержание, разграничив со смежными следственными действиями.

Стоит отметить, что в ходе осмотра фиксируются материальные следы, которые характеризуют внешние параметры объектов. Но касаемо данного состава преступления, осмотру, фиксации и изъятию подлежат цифровые

[1] Уголовное дело №1240194001203**** // Арх. СО МО МВД России «Увинский». Оп. 2. 231 л.

следы, которые являются разновидностью материальных, к ним относятся сведения о файлах, содержащихся на электронных носителях (место размещения, дата их создания и изменения, объем, расширение и т. п.). Их получение не раскрывает содержания информации, следовательно, не вторгается в охраняемые права и свободы человека.

Учитывая вышеуказанное под обыском при расследовании мошенничества, совершаемого в сфере информационно-телекоммуникационных технологий, понимается следственное действие, состоящее в поиске, обнаружении, фиксации и изъятии материальных следов, в том числе электронных носителей и электронной информации.

Нередко, когда в ходе установления содержания информации непосредственно в ходе обыска может быть затруднено. Данные могут быть скрыты либо защищены программными средствами. В таком следователь изымает все возможные носители электронной информации, после чего привлекает для ее отыскания и изъятия экспертов, назначая судебную компьютерно-техническую экспертизу.

С учетом допущенных ошибок и недостатков при проведении следственных действий, рекомендуется, в первую очередь, выбрать нужного специалиста, обладающего специальными познаниями в области информационно-телекоммуникационных технологий: обладающих данными о типе цифрового устройства, о программном обеспечении, которое используется на устройстве, типе соединений между компьютером одного или разного видов, сведениями о том, является ли это устройство сетевым, находящимся в глобальной либо локальной сети, разбирающегося в организации локальной сети, имеющего навыки работы в режиме удаленного доступа и т. д. Для каждой ситуации подбор специалистов определенного вида может существенно отличаться.

При выборе специалиста следователь может обратиться к экспертно-криминалистическим подразделениям, которые осуществляют производство судебных компьютерно-технических экспертиз; специалистам отдела по

борьбе с киберпреступлениями; специалистам IT-организаций; преподавателей технических высших образовательных заведений.

В условиях отсутствия конфликта между подозреваемым лицом и следователем, лицо, в жилище которого производится обыск, беспрепятственно впускает участников следственного действия для его производства[1].

После совершения вышеуказанных действий обстоятельства могут сложиться в трех вариантах: лицо добровольно выдает объекты, имеющие значение для расследования уголовного дела; лицо не выдает, но не препятствует производству обыска; лицо препятствует производству следственного действия (создает конфликтную ситуацию).

Если при производстве обыска следователь понимает, что лицо, в жилище которого необходимо произвести обыск, настроено агрессивно по отношению к правомерным действиям сотрудников полиции (попытки скрыться, напасть на сотрудника и т.д.). То следователь должен был на этапе подготовке предусмотреть и задействовать оперуполномоченных для обеспечения физической защиты, а также предотвращения попыток лица скрыться.

Рабочий этап обыска дифференциируется на две стадий – обзорная и детальная. В ходе производства обзорной стадии следователь проводит визуальный осмотр помещения, убеждается в безопасности условий производства следственного действия, а также отстраняет всех лиц, взаимодействующих с пользовательскими компьютерами любым образом. После этого он дает команду участникам на начало обыска.

В процессе проведения детальной стадии осуществляется деятельность, направленная на обнаружение объектов, находящихся не на цифровых устройствах. Позволяется применять криминалистические средства и тактические приемы, а также фиксировать факт поисковых действий и обнаруженные объекты, отражая их в протоколе обыска.

---

[1] Мазунин Я.М. Тактика обыска: учеб. пособие. Омск, 2024. С. 12.

Поиск информации на электронных носителях имеет ряд особенностей. Не стоит забывать о том, что обыск от осмотра места происшествия отличается тем, что позволяет установить не только внешние визуальные признаки файлов (наименование, расширение, размещение, дату образования, дату изменения, объем), но и внутреннее содержимое электронных файлов, то есть, находящуюся в них информацию, используя различные приложения.

Специалист, как и все участники следственного действия, осуществляет поисковые действия и, по сути, является ключевым участником. Обнаруженная информация должна быть изъята по правилам, установленным в ст. 164.1 УПК РФ, при обязательном присутствии специалиста.

На заключительном этапе следственного действия, объекты, имеющие значение для дела, подлежат изъятию. Это касается и самой цифровой информации, и ее носителей.

Фиксация факта, хода, содержания и результатов обыска по уголовным делам, где фигурируют электронные носители, производится по общим правилам, установленным уголовно-процессуальным законодательством. Следователь составляет протокол, соблюдая требования уголовно-процессуального законодательства Российской Федерации. В протоколе следственного действия необходимо отразить сведения о проведенных поисковых действиях, задействованных устройствах, о вспомогательном программном обеспечении, которое было использовано при производстве обыска и его результатах.

В случае, если при производстве обыска было изъято несколько объектов, необходимо отметить в протоколе их индивидуальные признаки. Детальный осмотр изъятых объектов можно будет осуществить позже, в рамках осуществления осмотра предметов или документов. В остальном обнаруженные и изъятые объекты необходимо описать по правилам производства осмотра.

В качестве приложения к протоколу обыска следователь должен подготовить схему обнаружения изъятых объектов, а также составить таблицу

изображений, которая будет содержать узловые и детальные фотоснимки обнаруженных объектов и дополнительно приобщить скриншоты с монитора цифрового устройства.

В ходе изъятия объектов следователю необходимо позаботиться о безопасной их транспортировке и их упаковке. Изымаемые объекты упаковываются аналогично изъятию в ходе осмотра места происшествия.

Зачастую при расследовании мошенничества, совершенного в сфере информационно-телекоммуникационных технологий, назначение судебной экспертизы является ключевым и решающим фактором, который определяет дальнейшее направление деятельности органа предварительного следствия.

Судебная экспертиза является особым процессуальным действием, которое проводится, когда возникают вопросы в рамках уголовного дела, ответы на которые требуют специальных познаний в области науки, техники, искусства или ремесла. При этом, заключение эксперта в ходе проведения судебной экспертизы признано отдельным и самостоятельным вид доказательства, которое имеет равнозначную доказательную силу по сравнению с другими доказательствами.

Результаты назначенной судебной экспертизы во многом зависят от правильности и грамотности ее назначения следователем. В ходе расследования мошенничества, совершенного с использованием информационно-телекоммуникационных технологий следователь сталкивается со специфическими объектами, работать с которыми способен лишь эксперт, обладающий специальными познаниями в области цифровых технологий. Примером таких объектов является информация, которая зафиксирована в электронной форме; программные обеспечения; средства компьютерной техники и сетевых технологий. Исследование и анализ экспертно-криминалистическим центром вышеуказанных объектов позволяет предоставить в распоряжение следователя сведения в формате заключения эксперта, в котором отражен механизм совершенного преступления, а также определение параметров средств компьютерной техники, их отношение к обнаруженной информации и друг другу и т.д.

Компьютерно-техническая экспертиза – это самостоятельный вид среди судебных экспертиз. Она относится к классу инженерно-технических экспертиз. Данная экспертиза проводится в целях определения статуса объекта как компьютерного средства, выявления и изучения его следовой картины в расследуемом преступлении, получения доступа к информации на носителях данных с последующим всесторонним ее исследованием[1].

Деятельность следователя по назначению судебной компьютерно-технической экспертизы можно представить в виде нескольких стадий: установление наличия основания для ее назначения; определение предмета и подготовка объекта, подлежащего направлению на экспертное исследование; формулирование вопросов для разрешения их экспертом; вынесение постановления о назначении судебной экспертизы; ознакомление подозреваемого, обвиняемого, его защитника, по терпевшего, его представителя с постановлением о назначении судебной экспертизы; направление постановления о назначении судебной экспертизы в государственное экспертное или иное учреждение; производство судебной компьютерно-технической экспертизы; оформление заключения компьютерно-технической экспертизы и передача его следователю; ознакомление с заключением компьютерно-технической экспертизы заинтересованных лиц.

Основанием для назначения судебной компьютерно-технической экспертизы выступает необходимость обращения к специальным познаниям экспертов экспертно-криминалистического центра с целью определения наличия сведений на электронных носителях информации и установления механизма совершения преступления[2].

В качестве предмета, который исследуется экспертом выступает цифровая информация, которая обусловливает определение ее объекта, то есть

---

[1] Кондратьев М.В. Оперативно-разыскное обеспечение выявления, предупреждения, пресечения и раскрытия преступлений, связанных с незаконным оборотом наркотических средств // Оперативник (сыщик). М., 2012, № 2 (31). С. 21–24.

[2] Филиппова А.Г. Криминалистическая тактика: учеб. пособие для академического бакалавриата. М., 2019. С. 73.

электронного носителя цифровой информации.

На значимость, эффективность проведения экспертизы, ее качество и полноту влияет непосредственно постановление о назначении судебной компьютерно-технической экспертизы, а если быть точнее, то вопросы, поставленные следователем в нем. Постановка данных вопросов очень тяжелый процесс, так как для того, чтобы поставить вопрос, касаемый объекта, его функционирования, предназначения и т.д., следователь должен иметь познания в области цифровых устройств и технологий. В том случае, если следователь поставит перед экспертом неправильный или некорректный вопрос, то эксперт либо не сможет на него ответить, либо ответ не будет иметь никакого значения для расследования уголовного дела. Частой ошибкой является поставка вопросов правового характера, на которые эксперт не компетентен ответить[1].

При подготовке постановления о назначении судебной компьютерно-технической экспертизы следователь обязан соблюдать ряд требований, следователю рекомендуется: использовать всеобщие, установленные термины, понятия и аббревиатуры (за исключением жаргонизмов, полупрофессиональных терминов); формулировать вопросы таким образом, чтобы они не затрагивали исследовательскую часть предоставляемых объектов. То есть должны быть исключены вопросы, касающиеся характеристик объектов, содержащейся на них информации и т.д.; не ставить вопросы, которые имеют правовой или справочный характер, а также которые выходят за пределы компетенции эксперта; формулировать вопросы, которые касаются только объектов, которые представленных на исследование эксперту.

Предлагаем примерный перечень вопросов, выносимых на судебную компьютерно-техническую экспертизу:

1. Если необходимо обнаружить файлы, которые содержат интересующий органы предварительного расследования текст:

[1] Сорочкин А.С. Криминалистическая тактика: учеб. для вузов. М., 2023. С. 117.

– имеются ли на представленных для исследования объектах (дать их перечень: ПК, ноутбук, мобильные устройства, носители информации) файлы, содержащие следующие ключевые слова: … (дать перечень ключевых слов). Если да, то записать обнаруженные файлы на представленный инициатором назначения судебной экспертизы оптический диск.

2. Если необходимо обнаружить файлы офисных приложений, а также сведения о них:

– имеются ли на представленных для исследования объектах (дать их перечень: ПК, ноутбук, мобильные устройства, носители информации) файлы, созданные в офисных программах (*.doc; *.docx; *xls; *.xlsx; *.odt и т. д.) и содержащие сведения о датах и времени создания, изменения и вывода на печать документа. Если да, то каковы показания даты и времени создания, изменения и вывода на печать документа.

3. Если необходимо обнаружить файлы баз данных приложения «1С: Предприятие»:

– имеются ли на представленных для исследования объектах (дать их перечень: ПК, ноутбук, носители информации) базы данных программы «1С: Предприятие». Если да, то записать обнаруженные файлы на представленный инициатором назначения судебной экспертизы оптический диск.

4.Если необходимо обнаружить вредоносное программное обеспечение:

– имеются ли на представленных для исследования объектах (дать их перечень: ПК, ноутбук, мобильные устройства, носители информации) программы, детектируемые антивирусным программным обеспечением как вредоносные.

5. Если необходимо обнаружить какое-либо программное обеспечение, а также программы для обхода защиты данного программного обеспечения («кряк»):

– имеются ли на представленных на исследование объектах (дать их перечень: ПК, ноутбук, носители информации) программный продукт, атрибутирующий себя как … (дать название). Если да, то имеются ли на

представленных на исследование объектах (дать их перечень) программы, предназначенные для обхода средств защиты от несанкционированного использования программного продукта, атрибутирующего себя как … (дать название).

6. Если необходимо обнаружить факт установки даты записи файлов на компакт-диск:

– имеются ли на представленном на исследование оптическом диске сведения о дате записи файлов, содержащихся на нем. Если да, то каковы показания даты и времени записи[1].

7. Если необходимо обнаружить историю переписки в мессенджерах, а также SMS/MMS сообщений и электронной почты, историю посещения интернет-сайтов:

– имеется ли на представленных на исследование объектах (дать их перечень: ПК, ноутбук, мобильные устройства, носители информации) установленная программа для общения (Telegram, Skype, iMessage, Viber, Line, WhatsApp, Threema, Confide, Wickr, Signal и др.). Если да, то какие пользователи зарегистрированы? Имеются ли сообщения в переписке?

– имеется ли на представленных на исследование объектах (дать их перечень: ПК, ноутбук, мобильные устройства, носители информации) переписка в программах электронной почты и обмена сообщениями (ICQ, Brosix, Skype и т. д.) между … (указать названия адресатов) за … (указать период). Если да, то записать переписку на представленный инициатором назначения судебной экспертизы оптический диск;

– имеются ли на представленных на исследование объектах (дать их перечень: ПК, ноутбук, мобильные устройства, носители информации) сведения о посещении интернет-ресурсов (дать перечень интернет-сайтов) за… (указать период);

– имеются ли на представленных на исследование объектах (дать

[1] Информатика для юристов и экономистов: учеб. для вузов. Стандарт третьего поколения / под ред. С. В. Симоновича. СПб.: Питер, 2014. С. 279.

перечень: телефонах, смартфонах, планшетах) сведения о контактах, журнале звонков, SMS, MMS? Если да, то записать обнаруженные данные на представленный инициатором назначения судебной экспертизы оптический диск.

8. Если необходимо получить сведения о пластиковых картах, а также данных с их магнитных полос:

– имеется ли на представленных на исследование объектах (дать их перечень: ПК, ноутбук, носители информации) аудиозапись, содержащая сведения о чтении магнитной полосы с пластиковой карты;

– какая информация имеется на магнитной полосе пластиковой карты, представленной на исследование;

9. Если необходимо получить видеоданные с видеорегистратора, а также систем наружного видеонаблюдения:

– имеется ли на представленном на исследование видеорегистраторе видеозапись за … (указать период). Если да, то скопировать ее на представленный инициатором назначения судебной экспертизы оптический диск.

10. Если необходимо получить данные с печатных плат игровых автоматов:

– как атрибутируют себя программы, имеющиеся на представленных печатных платах (для игровых автоматов);

– каковы настройки и статистика работы устройств, из которых изъяты представленные печатные платы (для игровых автоматов);

11. Если необходимо обнаружить графические файлы, а также сведения, содержащиеся в их метаданных (модель и параметры устройства фотосъемки, дате съемки, геолокации и т. д.):

– имеются ли на представленных на исследование объектах (дать их перечень: любые устройства и носители информации) графические файлы, содержащие метаданные (EXIF). Если да, то каковы сведения в обнаруженных графических файлах о … (модели и параметрах устройства, дате съемки,

геолокации и т. д.);

– имеются ли на представленных на исследование объектах (дать их перечень: любые устройства и носители информации) графические файлы, содержание которых соответствует представленным образцам (символики, отсканированных копий документов, денежных билетов).

12. Если необходимо обнаружить сведения о геолокации и координатах:

– имеются ли на представленных на исследование объектах (дать их перечень: навигационные устройства, мобильные устройства, носители информации, GPS-навигаторы) сведения о геолокации и маршрутах следования.

13. Если необходимо обнаружить сведения о различных параметрах, таких как IP и/или MAC адресах, версии программных продуктов, установленных даты и времени, атрибутах файлов и т. п.:

– имеются ли на представленных на исследование объектах (дать их перечень: любые устройства и носители информации) сведения о … (изложить, о чем)[1].

Представленный перечень вопросов, выносимых на судебную компьютерно-техническую экспертизу не исчерпывающий и может быть дополнен, изменен в зависимости от обстоятельств совершенного преступления и требующейся для следователя информации.

Так в ходе расследования уголовного дела №1240194001201**** по части 4 статьи 159 Уголовного кодекса Российской Федерации была назначена судебная компьютерно-техническая экспертиза:

В период времени с сентября 2023 года по апрель 2024 года неустановленное лицо, находясь в неустановленном следствии месте, под предлогом помощи заработать денежные средства в приложении «Liman» «игровая биржа», путем обмана и злоупотребления доверием гр-на ***, проживающего по адресу: ***, умышленно, из корыстных побуждений,

[1] Зубаха В. С. и др. Общие положения по назначению и производству компьютерно-технической экспертизы: метод. рекомендации. М., 2021. С. 27.

незаконно завладело принадлежащими ему денежными средствами в размере около 6 800 000 рублей 00 копеек, которые *** сам переводил со своего «Киви-Кошелька» на игровую биржу «Liman». Со слов потерпевшего *** было установлено, что она в период с сентября 2023 года по настоящее время пользуется системным блоком марки «INTELCORE».

В резолютивной части следователь поставил перед экспертом следующие вопросы:

– «Имеется ли на представленном системном блоке марки «INTELCORE» история посещения интернет ресурсов?»

– «Имеется ли на представленном системном блоке марки «INTELCORE» история работы приложения «Liman»?»

– «Имеется ли на представленном системном блоке марки «INTELCORE» история сообщений программ персональной связи?»[1].

Последующий этап расследования направлен на формирование доказательственной базы, подтверждающей вину подозреваемого лица. На данном этапе следователю необходимо применять тактические навыки при производстве следственных действий, а также привлекать специалистов, имеющих специальные познания для оказания содействия и восполнения пробелов, возникающих в ходе расследования мошенничества, совершенного с использованием информационно-телекоммуникационных технологий.

§ 3. Проблемы, возникающие при производстве следственных действий в ходе расследования мошенничеств, совершенного с использованием информационно-телекоммуникационных технологий

Мошенничество, совершенное с использованием информационно-телекоммуникационных технологий, входит в состав подавляющего большинства преступлений, совершенных за 2025-2026 год. Большая часть

[1] Уголовное дело №1240194001201**** // Арх. СО МО МВД России «Увинский». Оп. 1. 201 л.

указанного вида преступлений является «неочевидными».

Преступления остаются нераскрытыми в силу того, что злоумышленники предпринимают серьезные меры для обеспечения анонимизации своей личности (используют системы VPN-серверов; системы шифраторов и дешифраторов; авторизацию в аккаунтах третьих лиц и т.д.). Комплекс таких действий, предпринимаемых злоумышленниками, позволяет им оставаться в условиях анонимности для органов предварительного следствия. Отметим, что вышеуказанные действия усложняют процесс раскрытия и расследования преступления, но не делают это невозможным. Вышеуказанные сведения являются ключевыми в расследовании уголовного дела, так как, предоставленная информация может способствовать установлению лица, совершившего преступление, но, отправленные следователем запросы зачастую остаются проигнорированы.

Проблемой расследования является и то, что сотрудники органов предварительного расследования, оперуполномоченные не владеют фундаментальными специальными познаниями в области цифровых технологий. Этот факт является ключевым для проведения каждого следственного действия. Отсутствие вышеуказанных знаний негативно сказывается на качестве и эффективности расследования вышеуказанной категории преступлений. Следователь, который специализируется на расследовании данного вида мошенничеств, должен понимать структуру и элементы совершения преступления, уметь взаимодействовать с цифровым устройством, знать его составляющие, в особенности, структуру программного обеспечения и возможности управления им.

Для получения доказательств по делу необходимо изъять устройство - компьютер, ноутбук и иную компьютерную технику - и получить информацию, которую оно содержит. Для достижения этой цели проводятся такие следственные действия, как осмотр, обыск, выемка, следственный эксперимент.

В ходе осуществления данных следственных действий могут возникнуть

технические проблемы. Нередко они связаны с программами защиты информации, установленными пользователем компьютерного устройства. Некоторые системы защиты могут вызвать удаление информации на жёстком диске при попытках взаимодействия с компьютером постороннего лица. Чтобы скрыть следы преступления, злоумышленники могут использовать вредоносные программы, уничтожающие компьютерную информацию, как только доступ к устройству получит третье лицо.

Ещё одна проблема, возникающая в ходе проведения следственных действий, связана с допуском к компьютерной техники её владельца. Данный допуск может быть мотивирован необходимостью оказания помощи в эксплуатации компьютерной техники, однако необходимо понимать, что, преследуя цель сохранения доказательственной базы, сотрудники следственных органов не должны предоставлять такой возможности - исключением являются лишь случаи, когда у следственных органов есть резервные копии необходимой информации. Кроме того, усложнить ситуацию может противодействие сотрудников организации, которой принадлежит техника. Сотрудников, работающих с компьютерами, подключёнными к локальной сети, необходимо допросить, личность каждого нужно установить, а также выявить среди их числа программистов и специалистов по работе с компьютерной информацией - с этой целью необходимо исследовать данные о всех работниках организации, в том числе внештатных. Кроме того, важно истребовать у работающих с нужной компьютерной техникой лиц пароли и коды доступа.

Нередки ситуации, когда в ходе осмотра компьютера он находится во включенном состоянии. В таком случае сотрудникам правоохранительных органов надлежит выключить устройство, однако перед этих необходимо закрыть и сохранить содержимое всех вкладок, открытых на нём, завершить работу действующих программ и, если это представляется возможным, «запаролить» закрытые программы.

Проблемы могут возникать и при проведении допроса подозреваемого.

Сотрудники правоохранительных органов, что вполне закономерно, не просвещены в специфику работы в сфере компьютерной информации. В этой связи велик риск, что сотрудник, проводящий допрос, может быть введён в заблуждение опытным злоумышленником. Для предотвращения подобных негативных последствий представляется разумным обеспечить присутствие специалиста во время проведения допроса.

Ещё одно немаловажное следственное действие, проводимое по данной категории преступлений - судебная экспертиза. Здесь можно столкнуться с двумя основными проблемами - недостаточным уровнем компетенции сотрудников следственных органов при формулировании вопросов эксперту и недостаточностью специализированных экспертных учреждений. Путь решения первой проблемы можно видеть в привлечении специалиста к процедуре составления вопросов, в то время как пути решения второй проблемы найти сложнее, поскольку она требует комплексного подхода, включающего подготовку экспертов соответствующего уровня, дополнительное финансирование, в том числе государственное, и т.д.

Так, по результатам материала проверки сообщения о преступлении КУСП №1389 МО МВД России «Увинский» было возбуждено уголовное дело №125019400120***** по факту совершения мошенничества с использованием информационно-телекоммуникационных технологий, был проведен осмотр места происшествия, который не соответствовал основным принципам УПК РФ. Следственное действие было произведено не в полной мере, поверхностно, в протоколе осмотра места происшествия не было зафиксировано большое количество цифровых следов, изобличающих личность злоумышленника. Содержание осмотра места происшествия было изложено в пяти предложениях, в которых содержалось только описание цифрового устройства.

В ходе проведение оперативно-розыскных мероприятий личность злоумышленника была установлена, после чего уголовное дело перешло в категорию «очевидных». При производстве проверки уголовного дела органами Прокуратуры Удмуртской Республики было выявлено халатное

отношение следователя к производству осмотра места происшествия, вследствие чего, следователь был наказан дисциплинарным взысканием – «строгий выговор».

Возникшая проблема обусловлена тем, что следователь не имел специальных познаний в области цифровых технологий, не исследовал структуру устройства, а также его программного обеспечения, в результате чего множество log-файлов, имеющих значение для расследования уголовного дела, не были зафиксированы и удалены злоумышленником.

Таким образом, специфика расследования мошенничеств в сфере информационно-телекоммуникационных технологий придаёт проведению базовых следственных действий особенный характер. В процессе их проведения возникают дополнительные проблемы, вызванные недостаточным уровнем знаний компьютерной техники у сотрудников правоохранительных органов, спецификой выявления виртуальных следов, возможностью утери и искажения информации, которую можно использовать в качестве доказательства, в связи с использованием вирусных программ и систем защиты на носителях, сложностями в установлении времени и места совершения преступления, а также недостаточным количеством компетентных специалистов и экспертов.

ЗАКЛЮЧЕНИЕ

В заключение выпускной квалификационной работы, опираясь на основные положения организации расследования и тактики отдельных следственных действий мошенничества, совершенного в сфере информационно-телекоммуникационных технологий, необходимо акцентировать внимание следующих выводах.

Мошенничество, которое совершено в сфере информационно-телекоммуникационных технологий, является самым распространенным составом преступления, совершенным за 2025 год. При этом, расследование и раскрытие вышеуказанного киберпреступления представляет особую сложность в связи с неизученным механизмом совершения преступления, а также отсутствием специальных познаний, необходимых для взаимодействия с цифровыми устройствами и получения цифровых следов совершения преступления.

При расследовании вышеуказанного состава преступления ключевым следственным действием является следственный осмотр и осмотр места происшествия, так как при их производстве есть возможность полноценно и качественно обнаружить и зафиксировать цифровые следы совершения преступления.

Как правило, на поступившее сообщение о преступлении выдвигается следственно-оперативная группа, где на месте совершения преступления проводится осмотр места происшествия. В состав следственно-оперативной группы необходимо включать помимо следователя, оперуполномоченного, специалиста-криминалиста, специалиста в сфере информационно-телекоммуникационных технологий.

Осмотр цифровых устройств включает в себя определенный ряд действий, которые дифференцируются: статический осмотр (наименование устройства, внешние признаки и др.); детальный осмотр (наличие элементов питания, карт памяти, SIM-карт и др.); «внутернний» осмотр (осмотр и

фиксация сведений, содержащихся на электронном носителе информации).

Особенностью проведения допроса потерпевшего является специфика совершенного преступления, в силу малого количества цифровых следов, которые позволяют идентифицировать лицо, совершившее преступление, а также сложность механизма совершения киберпреступления.

Качественное и эффективное расследование мошенничества, совершенного с использованием информационно-телекоммуникационных технологий, зависит непосредственно от обнаружения не только цифровых, но и материальных следов. Кроме фундаментального следственного действия в виде осмотра места происшествия, для достижения выполнения данной функции производится обыск. Эффективность которого напрямую зависит от тщательной и детальной подготовки и организации следователем по данного следственного действия.

Обыск должен быть спланирован следователем очень детально, при этом должны быть учтены следующие аспекты: особенности объекта, который необходимо найти, характеристика личности собственника объекта, действия участников обыска в случае конфликтной ситуации, при попытках лица скрыться или уничтожить искомые объекты, необходимость в использовании поисковых систем и специалистов из определенных областей.

Ключевым аспектом эффективного расследования мошенничества, совершенного в области информационно-телекоммуникационных технологий, является назначение судебной компьютерно-технической экспертизы. Судебная компьютерно-техническая экспертиза при расследовании мошенничества, совершенного с использованием информационно-телекоммуникационных технологий является следственным действием, которое имеет особое значение для расследования такого преступления. Так как эксперт способен ответить на все главные вопросы следователя, на которые ответить самостоятельно он не компетентен. Эксперт сталкивается со специфическими объектами: информацией, зафиксированной в электронной форме; программным обеспечением, средствами компьютерной техники и

сетевыми технологиями. И способен установить факт наличия вредоносного программного обеспечения, факт его распространения, а также скрытые файлы, имеющие значение для расследования уголовного дела.

Организация и назначение судебной компьютерно-технической экспертизы состоит и ряда стадий: определение наличия основания для назначения; определение предмета и подготовка объекта, подлежащего направлению на экспертное исследование; формулирование вопросов для разрешения их экспертом; вынесение постановления о назначении судебной экспертизы; ознакомление подозреваемого, обвиняемого, его защитника, потерпевшего, его представителя с постановлением о назначении судебной экспертизы; направление постановления о назначении судебной экспертизы в государственное экспертное или иное учреждение; производство судебной экспертизы; оформление заключения судебной экспертизы и передача его следователю; ознакомление с заключением судебной экспертизы заинтересованных лиц.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

I. Нормативные правовые акты и иные официальные документы

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Федеральными конституционными законами от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ, от 14.03.2020 № 1-ФКЗ, от 06.10.2022) // Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 6 октября 2022 г. (дата обращения: 10.01.2026).

2. Уголовный кодекс Российской Федерации: федеральный закон от 13 июня 1996 г. № 63-ФЗ // Собрание законодательства Российской Федерации. – 1996. – № 25. – Ст. 2954.

3. Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 18 декабря 2001 г. № 174-ФЗ // Собрание законодательства Российской Федерации. – 2001. – № 52. – Ст. 4921.

4. Постановление Пленума Верховного Суда РФ от 30.11.2017 N 48 (ред. от 15.12.2022) «О судебной практике по делам о мошенничестве, присвоении и растрате» – Текст: электронный // Официальный интернет-портал правовой информации: [сайт]. – URL: http://www.pravo.gov.ru (дата обращения 13.01.2026).

5. О практике рассмотрения ходатайств о производстве следственных действий, связанных с ограничением конституционных прав граждан (статья 165 УПК РФ): постановление Пленума Верховного Суда РФ от 1 июня 2017 г. № 19.

6. О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»: постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37.

II. Учебная, научная литература и иные материалы

1. Аверьянова, Т.В., Белкин, Р.С., Корухов, Ю.Г., Россинская Е.Р. Криминалистика: учебник / Т. В. Аверьянова, Р. С. Белкин, Ю. Г. Корухов, Е. Р. Россинская. 4-е изд., перераб. и доп. – М., 2021. – 971 с.

2. Аносов, А.В. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учебное пособие / Аносов А.В. – М., 2023. – 208 с.

3. Ахмедшин, Р.Л. Тактика экспериментальных следственных действий: монография. – М., 2022. – 320 с.

4. Баев, О. Я. Тактика следственных действий: учебное пособие / О.Я. Баев: – М., 2023. – 440 с.

5. Белкин, Р.С. Криминалистика: проблемы, тенденции, перспективы. –М.: Юридическая литература. 1988. – 304 с.

6. Белкин, Р.С. Криминалистическая энциклопедия. – М., 2017. – 334 с.

7. Бондарева, М. В., Лаврентьева Г. А., Горшков М. М. Организация и тактика осмотра места происшествия: учебно-практическое пособие / М. В. Бондарева, Г. А. Лаврентьева, М. М. Горшков. – Омск, 2024. – 104 с.

8. Вандер, М.Б., Соловьева, О.М. Возможности алгоритмизации следственных действий // Труды Санкт-Петербургского Юридического института Генеральной Прокуратуры Российской Федерации. – Санкт-Петербург, 2024. – С. 72–77.

9. Волохова, О. В., Егоров, Н. Н., Жижина, М. В. Криминалистика: учебник / О. В. Волохова, Н. Н. Егоров, М. В. Жижина. под ред. Е. П. Ищенко. М., 2022. – 501 с.

10. Волчецкая, Т. С. Криминальные и криминалистические ситуации: учебник / Т. С. Волчецкая. – 4е изд., перераб. и доп. –Москва: Норма; ИНФРА-М, 2025. – 752 с.

11. Выявление, пресечение и документирование преступлений, связанных с мошенничеством в сфере компьютерной информации,

предусмотренных статьей 159.6 Уголовного кодекса Российской Федерации : методические рекомендации / С. Н. Миронов [и др.]. – Казань : КЮИ МВД России, 2023. – 65 с.

12. Гайнельзянова, В. Р. Возможности судебной компьютерно-технической экспертизы при расследовании преступлений в сфере компьютерной информации / В. Р. Гайнельзянова // Вестник Уфимского юридического института МВД России. – 2021. – № 1 (91). – С. 144–149.

13. Гавло, В.К. Теоретические проблемы и практика применения методики расследования отдельных видов преступлений. – Томск: Изд-во ТГУ, 1985. – 334 с.

14. Горшкова, М.М. Криминалистические аспекты производства следственных действий: учебное пособие / под общ. ред. доц. М. М. Горшкова. Омск, 2020. 76 с.

15. Григорян, Г. Р. Мошенничество в сфере компьютерной информации: проблемы криминализации, законодательной регламентации и квалификации : дис. … канд. юрид. наук : 12.00.08 / Григорян Гарик Рафикович. – Самара, 2021. – 243 с.

16. Давыдов, В.О. Об актуальных проблемах криминалистического обеспечения раскрытия и расследования мошенничеств, совершенных с использованием информационно-телекоммуникационных технологий / В. О. Давыдов, И. В. Тишутина // Криминалистика: вчера, сегодня, завтра. – 2021. – № 2 (14). – 81–91 с.

17. Еникеев, М.И., Образцов В.А., Эминов В.Е. Следственные действия: психология, тактика, технология: учебное пособие / М. И. Еникеев, В.А. Образцов, В.Е. Эминов. – Москва, 2007. – 214 с.

18. Зубаха, В. С. Общие положения по назначению и производству компьютерно-технической экспертизы: метод. рекомендации. – М., 2021. – 71 с.

19. Информатика для юристов и экономистов: учебник для вузов. Стандарт третьего поколения / под ред. С. В. Симоновича. СПб.:

Питер, 2014. 343 с.

20. Ищенко, Е.П., Топорков А.А. Криминалистика: учебник для вузов. 2-е изд., испр., доп. и перераб. – М., 2023. – 780 с.

21. Кондратьев, М.В. Оперативно-разыскное обеспечение выявления, предупреждения, пресечения и раскрытия преступлений, связанных с незаконным оборотом наркотических средств // Оперативник (сыщик). – М., 2012. – № 2 (31). – С. 21–24.

22. Коновалова, В.Е. Тактика производства обыска. – Харьков, 2025. – 94 с.

23. Корчагин, А.А. Следственные ситуации и алгоритмы в деятельности по предварительному расследованию и судебному разбирательству уголовных дел об убийствах // Научные ведомости. Серия Философия. Социология. Право. – 2023. – № 20 (115). Выпуск 18. – С. 114–119.

24. Кузнецова, А.А., Муравьева, К.В. Криминалистика: учебно-наглядное пособие / Омск, 2020. 110 с.

25. Кузнецова, А.А., Мазунина, Я.М. Криминалистика (общие положения, техника, тактика): учебник для вузов / М. М. Горшков [и др.]. – М., 2022. – 400 с.

26. Криминалистика: учебное пособие. Омск, 2023. 224 с.

27. Криминалистическая тактика: учебное пособие для академического бакалавриата / под общ. ред. А. Г. Филиппова. – М., 2019. – 97 с.

28. Криминалистические аспекты производства следственных действий : учебное пособие / Л. Ю. Аксенова, А. Т. Анешева, Н. И. Герасименко [и др.]; под редакцией М. М. Горшкова. – Омск : Омская академия МВД России, 2020. – 128 с. – URL: https://www.iprbookshop.ru/108817.html (дата обращения: 11.01.2026).

29. Лузгин, И.М., Муравьева Я.В. Методика изучения, оценки и разрешения исходных следственных ситуаций // Исходные следственные ситуации и криминалистические методы их разрешения / И.М. Лузгин. – Москва, 2022. – С. 14–16.

59

30. Лурия, А.Р. Маленькая книжка о большой памяти / О. Б. Гиппенрейтер // Хрестоматия по общей психологии допроса. Психология допроса. – М., 2022. – 96 с.

31. Мазунин, Я.М. Тактика обыска: учебное пособие. Омск, 2024. 123 с.

32. Сорочкин, А.С. Криминалистическая тактика: учебник для вузов. М., 2023. 513 с.

III. Эмпирические материалы

1. Уголовное дело №1210194001201**** // Арх. СО МО МВД России «Увинский». Оп. 1. 152 л.

2. Уголовное дело №1240194001203**** // Арх. СО МО МВД России «Увинский». Оп. 2. 231 л.

3. Уголовное дело №1220194001209**** // Арх. СО МО МВД России «Увинский». Оп. 2. 159 л.

4. Уголовное дело №1240194001201**** // Арх. СО МО МВД России «Увинский». Оп. 1. 201 л.

Материал вычитан, цифры, факты, цитаты сверены с первоисточником. Материал не содержит сведений, составляющих государственную или служебную тайну.

Д.В. Лебедев