ВОРОНЕЖСКИЙ ИНСТИТУТ МВД РОССИИ

МЕТОДИКА РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ ТОРГОВЫХ ПЛОЩАДОК (СЕРВИСОВ)

Методические рекомендации
(электронное издание)

Воронеж 2024

Методика расследования преступлений, совершаемых с использованием электронных торговых площадок (сервисов) : методические рекомендации / А. И. Гайдин, У.Н. Ахмедов, П.Г. Смагин. – Воронеж : Воронежский институт МВД России, 2024. – 47 с.

Материалы методических рекомендаций могут использоваться сотрудниками органов предварительного расследования МВД России в процессе раскрытия и расследования преступлений, совершаемых с использованием электронных торговых площадок (сервисов), в служебной подготовке сотрудников указанных категорий, а также в обучении курсантов и слушателей образовательных организаций МВД России, изучающих дисциплины «Предварительное следствие в ОВД», «Расследование преступлений в сфере компьютерной информации», «Расследование отдельных видов преступлений, совершенных с использованием информационно-телекоммуникационных технологий».

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Современный этап развития экономических отношений характеризуется переходом от традиционной экономики к цифровой, связанный с электронным бизнесом и электронной коммерцией (E-commerce).

Электронная торговля включает рекламу и сбыт товаров с помощью телекоммуникационных сетей. Электронная коммерция объединяет категории, такие как онлайн-продажи, интернет-банкинг, бронирования билетов и отелей, транзакции в платежных системах, онлайн-маркетинг и реклама.

Переход экономических процессов в цифровую сферу привел к адаптации преступных механизмов, действующих в традиционных экономических сферах, к условиям цифровизации. Преступники активно разрабатывают и реализуют схемы хищений, учитывая особенности электронной торговли, и придумывают новые способы совершения преступлений с использованием возможностей сервисов торговых площадок в Интернете.

Количество преступлений ежегодно возрастает, а их способы становятся все более изощренными. В 2021 году их количество увеличилось на 1,4% (517 722) (рост в 2017 году – на 37,4% (90 587); 2018 год – на 92,8% (174 674); 2019 год – на 68,5% (294 409); 2020 год – на 73,4% (510 396)). В настоящее время преступления в сфере компьютерной информации хотя и имеют незначительный удельный вес в общей структуре преступности в сфере ИТТ, однако проявляют стойкую тенденцию к ежегодному росту[1].

В 2022 году отмечается незначительное увеличение числа преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий (+0,8 %, всего: 522 065)[2].

В существующих условиях, формирование навыков организации, и осуществления расследования, фиксации хода и результатов процессуальной деятельности требует от сотрудников органов предварительного расследования обращения к правовым, техническим, методическим и научным источникам, в которых соответствующая информация не всегда систематизирована с учетом потребности. Поэтому для формирования единообразного подхода в расследовании преступлений, совершаемых с использованием электронных торговых площадок (сервисов), необходима подготовка методических рекомендаций.

Увеличение общего числа мошенничеств сопровождалось появлением их новых разновидностей, обусловленных спекуляциями на темы осложнения социально-экономической ситуации в результате санкций, СВО на Украине и

---

[1] Аналитический обзор результатов работы органов предварительного следствия по уголовным дела о преступлениях в сфере компьютерной информации по итогам 2021 года. Новгородская академия МВД РФ. Коллектив авторов под руководством Т.А. Николаевой. 2022 год.

[2] Комплексный анализ состояния преступности в Российской Федерации по итогам 2022 года и ожидаемые тенденции ее развития / М. В. Гончарова, С. А. Невский, М. М. Бабаев, Р. В. Черкасов, Е. Б. Аблиязова, Е. М. Тимошина, Г. Ф. Коимшиди, Г. Э. Бицадзе. – Москва : ФГКУ «ВНИИ МВД России», 2023. – 102 с.

объявленной Президентом Российской Федерации частичной мобилизации. В их числе выделяются мошенничества, осуществляемые:

- при использовании запрещенных в России социальных сетей;
- инвестиционных вложений для проведения операций на международном валютном рынке;
- через «посредничество» при оплате банковскими картами услуг зарубежных сервисов или установку VPN-сервисов;
- через «посредничество» при аренде и купле-продаже по цене ниже рыночной автомобилей, автозапчастей, электронных приборов и оборудования

В связи с представленными данными представляется вполне актуальным проведение комплексного исследования, посвященного особенностям расследования преступлений, совершаемых с использованием электронных торговых площадок (сервисов).

Основной целью данной работы является выявление прикладных проблем методического обеспечения раскрытия и расследования преступлений, совершаемых с использованием электронных торговых площадок (сервисов) и разработка на этой основе системы тактических и методических рекомендаций.

Для достижения поставленной цели необходимо решение следующих задач:

- выявление особенностей механизма преступной деятельности с использованием электронных торговых площадок (ресурсов);
- создание алгоритма проверки сообщений о преступлении;
- рассмотрение вопросов планирования раскрытия и расследования преступлений на первоначальном этапе;
- изучение особенностей производства отдельных следственных и иных процессуальных действий при расследовании указанной категории преступлений.

Разработанные методические рекомендации предназначены для использования в деятельности по раскрытия и расследования преступлений, совершаемых с использованием электронных торговых площадок (сервисов) сотрудниками уголовного розыска, следствия и подразделений дознания. Материалы методических рекомендаций могут быть использованы в рамках служебной подготовки сотрудников указанных категорий.

1. ОСОБЕННОСТИ МЕХАНИЗМА ПРЕСТУПНОЙ ДЕЯТЕЛЬНОСТИ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ ТОРГОВЫХ ПЛОЩАДОК (РЕСУРСОВ)

На сегодняшний день электронная торговля получила широкое распространение как среди компаний разных сфер деятельности, так и частных лиц благодаря массовому распространению информационно-коммуникационных технологий. Под электронной торговлей (коммерцией) понимается деятельность экономических субъектов, по реализации коммерческих операций с использованием электронных средств обмена информацией.

В узком смысле электронная торговля характеризуется как реклама и сбыт товаров с помощью телекоммуникационных сетей. В свою очередь электронная коммерция объединяет такие категории: онлайн-продажи, интернет-банкинг, бронирования билетов и отелей, транзакции в платежных системах, онлайн-маркетинг и реклама.

Переход части экономических процессов в цифровую сферу повлек за собой приспособление преступных механизмов, реализуемых в традиционных сферах экономической деятельности к условиям цифровизации.

Преступники активно разрабатывают и реализуют схемы хищений учитывая особенности электронной торговли и придумывают новые способы совершения различных преступлений, с использованием возможностей сервисов торговых площадок, функционирующих в сети Интернет.

Электронная торговая площадка представляет собой программно-аппаратный комплекс организационных, информационных и технических решений, обеспечивающих взаимодействие продавца и покупателя через электронные каналы связи.

Электронная торговая площадка позволяет объединить в одном информационном и торговом пространстве поставщиков и потребителей различных товаров и услуг и предоставляет участникам ряд сервисов, повышающих эффективность их работы.

Электронной торговой площадкой сегодня можно назвать любой Интернет-ресурс, посредством которого заключаются сделки купли-продажи между покупателями и продавцами. В соответствии с Российским законодательством электронные торговые площадки делятся на несколько видов:

– электронные торговые площадки для размещения государственного заказа;

– электронные торговые площадки для размещения заказов о закупках товаров, работ, услуг отдельными видами юридических лиц;

– электронные торговые площадки по реализации имущества должников (банкротов);

– электронные торговые площадки для коммерческих заказчиков и физических лиц (интернет-магазины, маркетплейсы и т.п.).

Различные виды торговых площадок (сервисов) в разной степени интенсивности используются в преступных схемах. Деятельность первых трех видов достаточно подробно регулируется нормативными актами, в которых прописаны процедуры аукционов и особенности сделок, а также требования к организаторам, участникам торгов и операторам, обеспечивающим функционирование площадок. Чаще они используются в механизме преступлений экономической направленности. Количество преступлений с их использованием, в сравнении с деяниями, при которых используются торговые площадки четвертого вида, незначительно. Однако ущерб при совершении таких экономических преступлений в каждом конкретном случае чаще оценивается как крупный или особо крупный.

Примером такого преступления выступает деяние, совершенное в Оренбургской области. Н совершил хищение чужого имущества путем обмана организованной группой, в особо крупном размере, а также пособничество в совершении растраты, то есть хищения чужого имущества, вверенного виновному. Преступления совершены с использованием электронной торговой площадки.

Н. имея высокие организаторские способности и навыки ведения предпринимательской деятельности в сфере торговли автомобильными деталями, узлами и принадлежностями, являясь учредителем и директором общества с ограниченной ответственностью «АвтоСнаб» зная о том, что на открытой торговой площадке «Сбербанк-АСТ» в единой информационной системе закупок на сайте www.zakupki.gov.ru. размещена заявка на поставку запасных частей для автомобилей для нужд УФПС Оренбургской области в соответствии с Федеральным законом от 18.07.2011 г. № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц», сформировал и реализовал преступный умысел, направленный на хищение денежных средств УФПС Оренбургской области путем обмана, выразившегося в предоставлении недостоверных сведений о наименовании и количестве поставляемых автозапчастей в адрес УФПС Оренбургской области, то есть осуществлять поставку запасных частей на автомобили в меньшем количестве, чем указано в представленных документах, извлекая при этом прибыль от недопоставки в адрес УФПС Оренбургской области автозапчастей. Преступными действиями причинен ущерб на сумму 1650175 рублей[1].

Все многообразие способов совершения преступных деяний с использованием электронных торговых площадок четвертой группы возможно поделить на группы с учетом их значения в механизме преступной деятельности. Легально созданные и функционирующие интернет-магазины, маркетплейсы, доски объявлений в основном используются злоумышленниками для непосредственной реализации способов мошенничества путем введения в заблуждения пользователей сервисов о качестве товара его наличии или путем предоставлений иной ложной информации, под воздействием которой,

[1] См.: Приговор по уголовному делу. URL: https://sudact.ru/regular/doc. / (дата обращения: 11.10.2023).

потерпевший передает денежные средства или осуществляет их перевод злоумышленнику. Также соответствующие сервисы используются как площадка для реализации фишинговых схем, позволяющих обманным путем получить сведения, необходимые для аутентификации клиентов в электронных платежных системах, которые в последующем используются при совершении краж с банковских счетов граждан или их электронных кошельков.

Так, реализуя совместный преступный умысел, направленный на совершение мошенничества, то есть хищение чужого имущества путем обмана, с причинением значительного ущерба гражданину, организованной группой, Н. Ю. и В. разместили объявление о продаже мобильного телефона на сайте Авито с указанием контактных абонентских номеров обратной связи зарегистрированных на подставных лиц. Н., при этом, приискал банковскую карту, зарегистрированную на имя К. неосведомленной о преступных намерениях организованной группы. П. посредством информационно-коммуникационной сети Интернет на интернет-сайте обнаружил объявление о продаже мобильного телефона и с целью его приобретения осуществил звонок по указанному в объявлении контактному номеру телефона В ходе телефонного разговора с П. участники организованной группы от имени продавца подтвердили наличие и возможность приобретения последним указанной модели телефона, а также сообщили условия оплаты. В., действуя согласно разработанному плану, в ходе телефонного разговора с П, проинформировали последнего о необходимости внести предоплату в размере 100 % от стоимости товара в сумме 11 289 рублей, посредством перечисления денежных средств на банковскую карту К. После получения перевода, участники группы обналичили средства со счета карты и обратили в свою пользу[1].

Вторую группу способов преступлений с использованием электронных торговых площадок составляют действия по созданию фиктивных сайтов, повторяющих интерфейс и оформление реально существующих интернет-магазинов, либо создание сайтов, не повторяющих известные, но с фиктивными предложениями реализуемых товаров. Такого рода фиктивные торговые площадки используются и для мошеннического хищения денежных средств, получаемых преступниками от покупателей за мнимые товары, и, при имитации на странице интерфейса сервиса платежных систем, для получения сведений, достаточных для дальнейшего совершения кражи со счетов и электронных кошельков покупателей.

Для осуществления незаконной преступной деятельности, направленной на совершение мошенничества, группой лиц по предварительному сговору, в особо крупном размере П., Ч. и Е. по обоюдному согласию решили использовать квартиру, принадлежащую родственнику Е., в которой разместили приобретенную ранее ими технику: два ноутбука, два модема, мобильные телефоны с сим-картами, которые намеревались использовать для приема звонков от граждан, желающих приобрести в их фиктивном интернет-магазине

[1] См.: Приговор по уголовному делу. URL: https://sudact.ru/regular/doc. / (дата обращения: 11.10.2023).

легковые автомобили. Также на созданном фиктивном сайте ООО «А.» П., Ч. и Е. разместили фотографии легковых автомобилей, технические характеристики автомобилей, сведения о которых скопировали на ресурсах сети Интернет, а также заведомо заниженную стоимость автомобилей, стоимость ввоза автомобилей в РФ, с целью привлечения потенциальных клиентов. Кроме того, П., Ч. и Е. для придания законности совершаемых фиктивных сделок по поставке и продаже легковых автомобилей разместили на указанном сайте интернет-магазина автосалона ООО «А.» номер расчетного счета на которые путем обмана планировали убеждать граждан перечислять денежные средства.

П. в сети Интернет увидел рекламу автосалона ООО «А.», размещенную ранее П., Ч. и Е. Зайдя по ссылке на страницу увидел объявления о продаже автомобилей иностранного производства с поставкой из Кореи и других стран. П., желая приобрести автомобиль иностранного производства написал письмо на указанный на сайте электронный адрес, в котором сообщил о своем желании приобрести в данном автосалоне легковой автомобиль Kia Sportage. П., Ч. и Е., получив по электронной почте письмо П., путем обмана стали вводить его в заблуждение и обманывать относительно деятельности ООО «А.», подтверждая ранее размещенную ими ложную информацию о поставке и продаже автомобилей, заверив о возможности продажи и поставки ему автомобиля Kia Sportage, 2013 года выпуска, стоимостью 750000 рублей. Злоумышленники убедили П. подписать договор – поручение по которому ООО «А.» обязуется доставить автомобиль Kia Sportage, 2013 года выпуска, стоимостью 750 000 рублей, а П. должен оплатить первый взнос в размере 420 000 рублей в течение двух банковских дней со дня подписания договора, второй взнос в размере 260 000 рублей в течение двух банковских дней после поступления автомобиля на таможенный склад, и третий взнос в размере 70 000 рублей, не позднее двух банковских дней с момента уведомления З.А.А. о поступлении автомобиля покупателю, затем, убедили П. перевести денежные средства на расчетный счет в счет оплаты за якобы приобретаемый автомобиль. Через некоторое время, продолжая вводить П в заблуждение относительно деятельности ООО «А.», в ходе телефонного разговора сообщили ему, что заказанный им автомобиль поступил на таможенный склад. П. введенный в заблуждение П., Ч. и Е. не подозревая об их преступных намерениях, в счет оплаты приобретаемого автомобиля перечислил на расчетный счет ООО «А.» первый взнос в размере 420 000 рублей, на тот же расчетный счет перечислил второй взнос в размере 272 000 рублей. В результате совместных, согласованных действий П., Ч. и Е. похитили поступившие от П. на расчетный счет 692 000 рублей[1].

Третью группу способов, составляют действия по реализации через электронные торговые площадки предметов, изъятых из гражданского оборота. В таких случаях, действующие маркетплейсы или электронные доски объявлений в большей степени используются в качестве мест рекламы, которая доводится до потребителей маскируясь под разрешенные объекты. При этом

[1] См.: Приговор по уголовному делу. URL: https://sudact.ru/regular/doc / (дата обращения: 11.10.2023).

используются словесные обозначения или изображения, распознаваемые лицами из числа потребителей запрещенных к обороту объектов. Сами сделки совершаются без участия электронной торговой площадки, что обеспечивает сокрытие следов преступления. Для реализации запрещенных предметов могут создаваться отдельные интернет-магазины. они в большей степени распространены в теневом сегменте сети, но с элементами маскировки встречаются и на общедоступных доменах. Такие магазины создаются на непродолжительное время, на иностранных хостингах, поэтому их выявление и документирование деятельности представляет определенную трудность.

С. и Б., для систематического совершения тяжких и особо тяжких преступлений, направленных на незаконный сбыт в течение длительного времени наркотических средств создали устойчивую преступную группу. С. и Б. приискали источник приобретения наркотических средств синтетического происхождения в особо крупном размере у неустановленного лица. С. привлек для создания интернет-сайта «www.robo-gu-n-n-n-market.pw» своего знакомого И., неосведомленного о преступных целях. Для вовлекаемых в организованную группу участников в зависимости от возлагаемых на них обязанностей С. и Б. решили применять условные названия: «диспетчер», «главный склад», «малый склад», «главный закладчик», «рядовой закладчик», что позволяло между участниками группы четко разграничить их роли. С. возложил на себя обязанности по контролю за работой интернет-сайта «www.robo-gu-n-n-n-market.pw», общему руководству организованной группой, координации действий участников организованной группы, приисканию наркотиков, контролю за движением полученных от незаконного сбыта наркотиков денежных средств, распределению преступного дохода, обеспечению безопасности преступной деятельности и оказанию противодействия правоохранительным органам при функционировании организованной группы. Также С. внедрял в деятельность группы технические и тактические меры конспирации, контролировал обеспечение работоспособности и оптимизации интернет-сайта путем интеграции в его структуру новых программных модулей. Обязанностями Б. являлись: приискание наркотиков, общие руководство и координация деятельности нижестоящих (подчиненных) участников организованной группы, подбор и вербовка «закладчиков», их инструктаж и контроль за их деятельностью, направление «закладчиков» в различные регионы России для бесперебойной продажи наркотиков, организация связи «закладчиков» с «диспетчером» и их непрерывной деятельности, перечисление им денежных средств за выполнение преступных обязанностей на счета кредитных учреждений и на баланс учетных записей платежной системы «Visa QIWI Wallet» «КИВИ Банк», распределение наркотических средств между городами России, где осуществлялся сбыт наркотических средств участниками организованной группы.

Созданный сайт «www.robo-gu-n-n-n-market.pw» по замыслу С. и Б. представлял собой интернет-магазин по продаже наркотических средств, в котором был задействован автоматический механизм сбыта наркотиков, позволяющий потребителю (покупателю) наркотических средств, используя

программы обмена сообщениями Icq, Skype, Jabber, Xabber и т.д. самостоятельно подключаться к системе автоматической продажи (программе-роботу), предлагающей для продажи наркотики под видом товара с известными в сфере наркобизнеса законспирированными названиями: «скорость», «скорость в кристаллах», «куреха». После подключения система автоматического сбыта активировала предложение покупателю выбрать из перечня город, где он находился, вид и размер наркотического средства. После выбора наркотика покупатель получал сообщение с информацией о номере «киви-кошелька», размере наркотика и стоимости заказа. На полученный номер «киви-кошелька» покупатель перечислял необходимую сумму денег, после чего сообщал через систему информацию о произведенной оплате (№ чека (квитанции) и (или) его скриншот, время транзакции, комментарий). По зачислению денежных средств за купленный наркотик система продажи направляла заказчику адрес расположения тайника-закладки с наркотическим средством. Адреса расположения тайников-закладок с наркотиками «закладчики» передавали «диспетчеру» через сеть Интернет с использованием сервиса интернет-мессенджеров, учетные записи в которых им создавали С. и Б. Поступившие адреса тайников-закладок обрабатывались «диспетчером», копировались и загружались на сайт «www.robo-gu-n-n-n-market.pw» в подраздел «Адреса» раздела «Админка» для дальнейшей передачи «рядовым закладчикам» и наркопотребителям с использованием системы автоматической продажи[1].

Перечисленные группы способов разделены между собой условно. Действия, которые осуществляют злоумышленники на этапах подготовки, реализации преступного замысла и сокрытия следов преступления достаточно часто пересекаются, имеют много общих черт и, соответственно, схожие следовые картины. Создание фиктивных сайтов, применение способов анонимизации в сетевой среде для сокрытия следов преступления может указывать на высокую криминальную квалификацию в сфере киберпреступлений, а также и на преступную специализацию с разделением преступных ролей.

Говоря о типичных способах совершения преступлений с использованием электронных торговых сервисов, следует выделять типичные действия, характерные для разных их этапов. Именно разнообразие их сочетаний и формирует многообразие способов этих преступлений,

Обязательной составляющей первых двух групп способов совершения преступлений с использованием торговых электронных площадок выступает обман. Он заключается в предоставлении ложной информации, которая возбуждает интерес у потенциальной жертвы и желание воспользоваться выгодным предложением по приобретению товара, или стать клиентом, получив предлагаемую услугу, работу на выгодных условиях. Содержание ложной информации ограничивается лишь фантазией преступников. В определенной мере зависит от сложившейся на конкретный период времени ситуации с

[1] См.: Приговор по уголовному делу. URL: https://sudact.ru/regular/doc. / (дата обращения: 11.10.2023).

наличием товарных дефицитов, сезонных всплесков потребительского интереса на определенные товарные группы и некоторых иных факторов, формирующих временный или постоянный потребительский интерес. Объединяет такого рода фиктивные предложение наличие более выгодных условий чем у остальных продавцов, кадровых агентств, финансовых организаций и т.п., или уникальность предложения в плане выгоды. Криминалистическую значимость при обобщении всего многообразия содержания фиктивных предложений, распространяемых преступниками через электронные торговые ресурсы, имеет прежде всего именно этот признак. По той причине, что позволяет использовать его при выявлении преступных схем оперативными подразделениями органов внутренних дел и в профилактической деятельности с населением.

Обобщение и знание устоявшихся обманных схем в деятельности преступников, имеет ориентирующее значение в деятельности органов внутренних дел по противодействию такого рода преступлениям путем мониторинга рассматриваемых сетевых ресурсов и при установлении отдельных эпизодов многоэпизодной преступной деятельности.

Рассмотрим наиболее распространенные приемы обмана на торговых интернет-ресурсах.

Предложение о продаже товара по цене значительно ниже среднерыночной. В качестве товаров предлагаются брендовая одежда, бытовая техника, украшения, аксессуары, автомобильные запчасти и т.п. Низкая стоимость товаров объясняется различными причинами. Начиная с распродажи «таможенного конфиската», заканчивая реализацией товара, приобретенного за границей в результате легализации средств, полученных преступным путем. Наличие криминальной составляющей в происхождении товаров обеспечивает преступникам объяснение причины, по которой они не представляют полные о себе данные, принимают оплату только на электронные кошельки платежных систем или с использованием криптовалют, обходят предлагаемые торговой площадкой безопасные способы оплаты для участников сделки.

Фейковые (ложные) интернет-магазины. Такой тип обмана требует от злоумышленников значительной подготовки, которая выражается в разработке, регистрации и администрировании сайта интернет-магазина с целью мнимой продажи товаров. Эффективность обмана достигается за счет повторения интерфейса сайтов известных магазинов, использования наименования интернет-адреса, схожего с известным, формирования и поддержания актуального каталога товаров и цен с учетом соответствующих особенностей на сайте повторяемого магазина. Для привлечения будущих жертв обмана, преступники размещают на посещаемых сайтах баннерную и иную рекламу с непосредственным переходом по клику на фейковый сайт или проводят спам-рассылку рекламных писем. Ввиду необходимости вложения значительных финансовых средств на создание ложных копий сайтов известных интернет-магазинов, злоумышленники чаще создают простые фейковые сайты с «дешевым товаром», рассчитанные на непродолжительное функционирование в сети до момента их блокировки, но за счет массовости таких сайтов обеспечивают себе достаточный криминальный доход. Он состоит из средств,

получаемых от потерпевших при непосредственной оплате ими мнимого товара, а также от последующих хищений средств с соответствующих счетов покупателей или продажи преступниками сформированной базы данных компрометированных электронных средств платежа (чаще платежных карт) другим преступным сообществам, специализирующимся на такого рода кражах.

Имитация розыгрыша ценных подарков. Чтобы убедить потенциальных покупателей в необходимости совершить покупку недорогих, но неликвидных товаров злоумышленники организуют покупательский ажиотаж путем объявления розыгрыша ценных подарков среди покупателей определенных групп товаров. Возможность выигрыша толкает доверчивых граждан приобретать вещи по завышенной цене, и предоставлять преступникам свои аутентификационные данные в платежных системах.

Продажа дефектных или иных неликвидных товаров может осуществляться с сокрытием полных сведений о качестве и особенностях товара. Соответствующая информация или утаивается полностью или представляется мелким текстом, а также путем размещения ее в разделах интернет-магазина, на который редко обращает внимание покупатель. Данная информация скрывается в массиве других данных о товаре. Тем самым, недобросовестные продавцы создают условия, при которых юридическая квалификация продажи товара ненадлежащего качества в каждом конкретном случае сводится к гражданско-правовому спору, хотя совокупность таких фактов обмана может рассматриваться в уголовно-правовой плоскости.

Столкнувшись с необходимостью самостоятельно отстаивать свои интересы в гражданско-правовом порядке, большинство неискушенных в юридических особенностях защиты своих прав граждан, отказываются от обращения в суд и ли в правоохранительные органы.

Аналогичным образом интернет-магазины могут реализовывать товар, бывший в употреблении. Здесь ситуация аналогична – товар продается значительно дешевле имеющихся аналогов, а на странице с его описанием мелкими буквами может быть написано, что «товар был в употреблении», «товар продается без гарантии», и т. п.

Часто некондиционный или бывший в употреблении товар доставляется покупателю не курьером, а по обычной почте (например, наложенным платежом, или после совершенной на сайте магазина предварительной оплаты). В такой ситуации покупателю еще сложнее предъявлять претензии.

В достаточной степени распространены интерне-магазины по продаже «чудодейственных» медикаментов. Преступники активно продвигают «волшебные таблетки» «от всех болезней», средства для улучшения мужской силы, пилюли от головной боли, от подагры, мази от радикулита и вообще – любые лекарства от всех известных болезней. Указанные на сайте или в описании к товару сертификаты на продаваемые медикаменты зачастую просто не существуют. Оплаченный в такой интернет-аптеке товар доставляется курьером или отправляется в пункт выдачи, что дополнительно затрудняет установление злоумышленников. Реализация таких поддельных или несуществующих медикаментов, должна получать исчерпывающую

юридическую оценку с учетом имущественного ущерба и ущерба здоровью потерпевшим.

Более сложные схемы обмана, реализуемые через электронные торговые площадки, связаны с фиктивным предложением удаленной работы. Несмотря на то, что торговые площадки тематически не предназначены для рекрутинга, злоумышленники размещают такие объявления с целью максимального охвата целевой аудитории. В предложениях фриланса (удаленной работы через Интернет) как правило излагаются очень привлекательные условия. Такая работа, исходя из фейковых объявлений, подходит специалистам любых сфер деятельности, которые с технической точки зрения могут работать удаленно: переводчики, программисты, веб-разработчики, тестировщики, журналисты, писатели (в том числе технические писатели), копирайтеры, редакторы, сценаристы, художники, специалисты по работе с графикой и видео, и т. д. Предлагают также виды деятельности и не требующие специальных навыков и знаний: заполнение карточек на товар, переход по ссылкам для увеличения показателя посещаемости сайта и т.п. Чаще такие объявления не содержат важную дополнительную информацию о необходимости внести определенную сумму на счет или электронный кошелек работодателя. Такая информация доводится заинтересованным лицам «представителем работодателя» после того, как клиент свяжется по телефону, указанному в объявлении. Обязательность денежного перевода объясняется необходимостью страхования рисков, оплатой какого-либо информационного пакета, ключа, либо инструкции, либо еще чего-нибудь, необходимого для дальнейшей «работы». Еще злоумышленники могут предлагать купить некие «бизнес-пакеты», в которых содержатся все необходимые инструкции для открытия и успешного развития своего прибыльного бизнеса, который можно вести, не выходя из дома, в удобное время и получать стабильный доход. Получив требуемую оплату, преступники могут некоторое время продолжать имитировать законную деятельность, контактировать с потерпевшим, иногда даже выманивают дополнительные средства за мнимое обучение и т.п. Однако позже, не исполнив «свои обязательства», они перестают выходить на связь с потерпевшим и обращают полученное имущество в свою пользу.

Реализация предметов, запрещенных к обороту, через торговые площадки включает в себя весь комплекс подготовительных действий, обеспечивающих маскировку преступной деятельности; скрытную реализацию наркотических средств, оружия, детской порнографии и т.п.; действий по сокрытию следов преступной деятельности. Уместно говорить, что действия по подготовке к преступлению и действия по сокрытию преступления представляют собой единый комплекс взаимосвязанных и последовательно реализуемых действий, направленных прежде всего на обеспечение анонимности в сети Интернет. Так как реализация запрещенных предметов от момента начала коммуникации продавца и покупателя, до передачи товара и получения оплаты, не предусматривают непосредственных контактов участников, то применение методов анонимизации является наиболее эффективной совокупностью действий по сокрытию преступления в механизме преступной деятельности.

К подготовительным, в рамках рассматриваемой группы способов, относятся действия по созданию и регистрации сайта на ресурсах хостинг-провайдера. Анонимность достигается путем сокрытия реального IP-адреса через VPN-сети и Proxy-серверы, использованием электронных копий поддельных документов, указанием ложной информации о владельце сайта, применением анонимных электронных кошельков, через которые происходит оплата хостинга. Зачастую сами хостинг-провайдеры подбираются из числа находящихся под юрисдикцией недружественных стран, отказывающих во взаимодействии в рамках деятельности Интерпола и оказания международной правовой помощи. Предложение запрещенных к обороту предметов маскируется под схожие разрешенные предметы, дабы минимизировать риск блокирования работы сайта с учетом национального законодательства страны юрисдикции хостинг-провайдера. Подготовка также включает рекламу сайта. Она чаще распространяется в группах социальных сетей. Соответствующие группы создают и администрируют сами же продавцы, указывая ложную информацию о том, что они являются легальными, не запрещенными в гражданском обороте.

Реализация товара осуществляется зачастую через тайники. Диспетчер интернет-магазина после получения подтверждения оплаты направляет покупателю информацию с указанием места тайника. Коммуникация реализуется через мессенджеры, регистрация в которых происходит при использовании номеров телефонов, оформленных на подставных лиц или с использованием SIM-карт операторов сотовой связи иностранных государств. Оплату продавцы принимают на анонимные электронные кошельки небанковских электронных платежных систем, которые администрируют, подключаясь используя средства анонимизации. Так же могут использоваться платежные системы с криптовалютой, что тоже обеспечивает анонимность.

Для сокрытия следов преступники удаляют переписку в мессенджерах мобильных устройств связи и персональных компьютеров, нанимают курьеров и закладчиков, не вступая с ними непосредственно в контакт, меняют используемые для связи технические средства, аккаунты в платежных системах и иных сервисах и ресурсах сети Интернет.

Совершение действий по подготовке, реализации и сокрытию преступного замысла порождает формирование следовых картин, сочетающих материальные и идеальные следы. Среди материальных следов наибольший интерес представляют виртуальные следы, так как они содержат сведения об основной доле обстоятельств преступной деятельности, подлежащих установлению и доказыванию.

Факт соединения компьютерного оборудования преступника с оборудованием сетевого сервиса или ресурса, действия лица по созданию и администрированию сайта, а также иные действия с учетом содержательной и функциональной направленности ресурса отражаются в файлах журналируемой информации, которые создаются автоматически в результате выполнения соответствующих алгоритмов, заложенных разработчиком в работу управляющих программ. Содержащаяся в записях информация разнообразна (дата сеанса связи, информация о времени связи (статические или динамические

IP-адреса, телефонные номера, скорость передачи сообщения, характеристики сеанса связи, включая тип использованных протоколов, сами протоколы, MAC-адрес использованного сетевого оборудования, системное время и др.) Для расследования наиболее значимы сведения об IP- и MAC-адресах, позволяющие установить местонахождение и характеристики используемых технических средств. При использовании злоумышленником распространенных способов анонимизации (VPN, Proxy), в файлах ресурса сохранится не истинный IP-адрес пользователя, а адрес транзитного ресурса. Сведения о принадлежности адреса конкретной стране и относимость к группе адресов, присваиваемых конкретным провайдером, относятся к числу справочной информации и содержатся на ряде открытых ресурсов (например, https://2ip.ru) в удобной поисковой форме. Провайдер располагает информацией о том, кому присваивался динамический IP-адрес в определенное время, и кто из клиентов использует интересующий статический адрес. При установлении пользователя по динамическому адресу у провайдера необходимо учитывать, что сейчас повсеместно применяется технология NAT-адресации, когда один и тот же IP-адрес представляется множеству (до нескольких тысяч) пользователей одновременно. Является ли адрес динамическим или статическим можно установить при проверке его на открытых ресурсах, зачастую там же сразу можно получить сведения о том, что проверяемый адрес относится к VPN.

В виртуальной частной сети (VPN) IP-адреса подразделяются на две группы: внешние и внутренние (белые и серые). Внутренние адреса присваиваются внутри виртуальной сети. Сведения о них через открытые ресурсы установить не представляется возможным. Их можно получить только у администратора соответствующей сети.

MAC-адрес позволяет установить модель сетевого оборудования или идентифицировать его. Передается оператору связи только при непосредственном подключении к его оборудованию. Если для подключения используется промежуточное оборудование (WiFi-маршрутизатор или USB-модем), то MAC-адрес оператору связи не передается. Значение MAC-адреса может принудительно изменяться на произвольное самим пользователем, что предусмотрено настройкой соответствующих параметров в операционной системе. Значение MAC-адреса фиксируется не каждым оператором связи. Некоторые производители присваивают одинаковый MAC-адрес всей партии сетевых адаптеров.

Наряду с данными об IP- и MAC-адресах оборудования, поисковое значение имеют сведения о cookie-файлах, которые регистрируются на сетевых ресурсах. Применяемая при этом технология позволяет управляющей системе ресурса «опознавать» браузер пользователя по совокупности признаков независимо от его IP-адреса. Соответствующие сведения позволяют установить действия пользователя на сайте за интересующий период времени, выявить иную значимую поисковую информацию.

Схожей для «опознания» пользователя в сетевом пространстве по совокупности является технология user-agent (сведения об операционной системе и веб-браузере). Она используется на сайтах и поисковыми системами

для настройки адресной рекламы и может быть использована в поисковой деятельности при применении способов анонимизации в сети Интернет.

Большое количество следовой и ориентирующей криминалистически значимой информации возможно обнаружить на страницах пользователей социальных сетей. Непосредственная связь аккаунта социальной сети с торговой площадкой устанавливается при указании соответствующих данных в процессе регистрации, а также если торговая площадка является одним из сервисов соответствующего ресурса. Кроме того, выход на страничку пользователя возможен в процессе поисковой деятельности при расследовании преступления. Анализ данных, представленных на страничке, позволяет получить ориентирующую информацию о лице и идентификационные сведения при обнаружении фотоснимков лиц. В числе таких сведений необходимо рассматривать данные о контактах пользователя, указанные сведения о месте жительства и перемещениях, состав семьи, сведения о личном автотранспорте. Необходимо помнить, что сведения на странице могут быть вымышленными, чтоб ввести в заблуждение потерпевших от преступления и правоохранительные органы. У владельцев социальной сети можно получить расширенную информацию об учетной записи пользователя (время создания и изменения, какие данные указал о себе пользователь при ее регистрации, активность использования страничкой – частота посещений и администрирования данных, IP-адреса и время когда конкретно пользователь заходил на страницу, адрес электронной почты, номер телефона, данные о платежных инструментах, которые использовал клиент для оплаты сервисов, переписка пользователя).

При использовании злоумышленниками электронной почты, значительный объем доказательственной информации можно обнаружить в файлах журналируемой информации на серверах владельца и администратора соответствующего интернет-сервиса. Кроме содержания самого письма, служебная информация включает данные о маршруте его прохождения от момента отправки до момента получения, IP-адрес отправителя, данные из учетной записи пользователя, сеансы его активности с указанием IP-адресов подключения, переписка пользователя.

Фактически каждое преступление, совершаемое с использованием электронных торговых площадок, в своем механизме включает денежные переводы через электронные платежные системы. Их использование порождает следы, которые могут быть обнаружены на серверах операторов платежных систем. Различаются банковские и небанковские электронные платежные системы, а также криптовалютные. Деятельность первых двух видов урегулирована национальным законодательством, третий вид функционирует в рамках юрисдикции иностранных государств. При этом для криптовалютных платежных систем, основанных на технологии блокчейна, не характерно наличие управляющего центра и оператора как такового. Поэтому получение сведений о транзакциях и данных о пользователях возможно только в рамках оперативно-розыскной деятельности с применением специальных знаний, специального программного и технического обеспечения.

Объем криминалистически значимых сведений у операторов платежных систем отличается. Наибольший объем данных возможно обнаружить в кредитных организациях – операторах банковских электронных платежных систем. К ним относятся исчерпывающие учетные данные на клиентов и сведения о произведенных транзакциях. Операторы небанковских электронных платежных систем располагают значимой информацией в зависимости от вида электронного кошелька, используемого клиентом. Минимальные данные фиксируются относительно анонимных электронных кошельков. Но и в данном случае возможно обнаружение значимых сведений о сеансах доступа к электронному кошельку за определенный период времени с установлением IP-адресов, а также сведения о произведенных транзакциях по переводу средств и пополнению кошелька.

На серверах операторов сотовой связи хранится криминалистически значимая информация о соединении абонентов и абонентских устройств, установочные данные пользователей, сведения о движении средств в связи с оплатой услуг связи и при использовании электронного кошелька, привязанного к абонентскому номеру (оператор связи нередко выступает и оператором небанковской платежной системы). При установлении фактов использования злоумышленниками средств мобильной сотовой связи для коммуникации с потерпевшими и иными соучастниками преступной деятельности (в том числе покупателями запрещенных к обороту предметов), у операторов могут быть получены сведения о паспортных данных лица, на котором зарегистрирован номер, время регистрации, IMEI-номерах устройств с которыми использовалась SIM-карта, сведения о звонках, текстовых сообщениях, о местонахождении устройства с привязкой к базовым станциям в конкретный период времени.

Наиболее потенциально ценными электронными носителями значимой информации об обстоятельствах совершенного преступления являются мобильные устройства сотовой связи его участников. В памяти устройств может быть обнаружены данные об IMEI-номере, звонках, сообщениях SMS и в мессенджерах, сообщения со вложенными фотографиями, видеороликами, голосовыми сообщениями, сведения о посещаемых интернет-ресурсах и сервисах с данными об аккаунтах и паролях доступа, сведения об установленных и ранее использовавшихся программах, данные геолокации (перемещения в пространстве), сохранившиеся на устройстве, а также сведения об аккаунтах в интернет сервисах, использующих данные геолокации (такси, навигаторы и т.п.).

Таким образом, электронной торговой площадкой сегодня можно назвать любой Интернет-ресурс, посредством которого заключаются сделки купли-продажи между покупателями и продавцами. В соответствии с Российским законодательством электронные торговые площадки делятся на четыре вида. Различные виды торговых площадок (сервисов) в разной степени интенсивности используются в преступных схемах. Чаще используются электронные торговые площадки для коммерческих заказчиков и физических лиц (интернет-магазины, маркетплейсы и т.п.). Многообразие способов преступлений, при которых применяются торговые площадки для коммерческих заказчиков, можно сгруппировать в три группы. Первая, когда легально созданные и

функционирующие интернет-магазины, маркетплейсы, доски объявлений в основном используются злоумышленниками для непосредственной реализации способов мошенничества путем введения в заблуждения пользователей сервисов о качестве товара его наличии или путем предоставлений иной ложной информации, под воздействием которой, потерпевший передает денежные средства или осуществляет их перевод злоумышленнику. Вторую группу способов преступлений с использованием электронных торговых площадок составляют действия по созданию фиктивных сайтов, повторяющих интерфейс и оформление реально существующих интернет-магазинов, либо создание сайтов, не повторяющих известные, но с фиктивными предложениями реализуемых товаров. Такого рода фиктивные торговые площадки используются и для мошеннического хищения денежных средств, получаемых преступниками от покупателей за мнимые товары, и, при имитации на странице интерфейса сервиса платежных систем, для получения сведений, достаточных для дальнейшего совершения кражи со счетов и электронных кошельков покупателей. Третью группу способов, составляют действия по реализации через электронные торговые площадки предметов, изъятых из гражданского оборота. Совершение действий по подготовке, реализации и сокрытию преступного замысла порождает формирование следовых картин, сочетающих материальные и идеальные следы. Среди материальных следов наибольший интерес представляют виртуальные следы, так как они содержат сведения об основной доле обстоятельств преступной деятельности, подлежащих установлению и доказыванию.

Факт соединения компьютерного оборудования преступника с оборудованием сетевого сервиса или ресурса, действия лица по созданию и администрированию сайта, а также иные действия с учетом содержательной и функциональной направленности ресурса отражаются в файлах журналируемой информации, которые создаются автоматически в результате выполнения соответствующих алгоритмов, заложенных разработчиком в работу управляющих программ. На серверах операторов сотовой связи хранится криминалистически значимая информация о соединении абонентов и абонентских устройств, установочные данные пользователей, сведения о движении средств в связи с оплатой услуг связи и при использовании электронного кошелька, привязанного к абонентскому номеру (оператор связи нередко выступает и оператором небанковской платежной системы). При использовании злоумышленниками электронной почты, значительный объем доказательственной информации можно обнаружить в файлах журналируемой информации на серверах владельца и администратора соответствующего интернет-сервиса. Фактически каждое преступление, совершаемое с использованием электронных торговых площадок, в своем механизме включает денежные переводы через электронные платежные системы. Их использование порождает следы, которые могут быть обнаружены на серверах операторов платежных систем. Большое количество следовой и ориентирующей криминалистически значимой информации возможно обнаружить на страницах пользователей социальных сетей. Наиболее потенциально ценными

электронными носителями значимой информации об обстоятельствах совершенного преступления являются мобильные устройства сотовой связи его участников.

2. ПРОВЕРКА СООБЩЕНИЙ О ПРЕСТУПЛЕНИИ И ПЛАНИРОВАНИЕ РАССЛЕДОВАНИЯ НА ПЕРВОНАЧАЛЬНОМ ЭТАПЕ

Порядок проверки сообщения о преступлении, совершаемом с использованием электронных торговых площадок, зависит от способа его совершения. Рассмотрим типичные следственные ситуации в зависимости от способа совершения преступления.

Первая ситуация – продажа несуществующего товара. Преступник размещает на сайтах объявлений («Авито», «Юла», «Циан» и др.) информацию о продаже товара по привлекательной цене. Потенциальный покупатель связывается с продавцом, оплачивает частичную или полную стоимость товара, однако сам товар не получает. Данный способ имеет множество разновидностей, однако можно выделить ряд специфических особенностей:

- продавец зарегистрирован на сайте недавно;
- отсутствует номер телефона, по которому можно связаться с продавцом, либо он оформлен на подставное лицо;
- географическое местоположение продавца представляется собой небольшой населенный пункт, расположенный на малонаселенной территории;
- продавец, как правило, не против осмотра товара перед покупкой, однако в силу удаленного расположения предлагает отправить товар «Авито доставкой» или иной транспортной компанией;
- активные предложения продавца перейти в иную диалоговую систему обмена сообщениями (мессенджеры «WhatsApp» и «Telegram»);
- продавец подтверждает отправку товара фиктивной квитанцией (справкой) транспортной компании.

В подавляющем большинстве случаев покупатели обращаются в правоохранительные органы спустя довольно продолжительное время когда либо не получают товар совсем, либо приходит совсем другая посылка (строительный мусор, пустые коробки, отрезки ткани и т.д.).

Так, в Энгельский районный суд Саратовской области направлено уголовное дело по обвинению местного жителя в совершении 9 преступлений, предусмотренных ч. 2–3 ст. 159 УК РФ. Обвиняемый размещал на сайте Avito.ru объявление о продаже автомобильных колес на литых дисках в сборе на автомобиль марки «Мерседес» по низкой цене, но со 100 % предоплатой. После перечисления денежных средств на банковскую карту преступника последний прекращал отвечать на телефонные звонки. Совершенные преступления раскрыты по результатам анализа MAC-адресов, IP-адресов, детализаций телефонных переговоров потерпевших с привязкой к приемопередающим

базовым станциям, а также выемки электронных сообщений с электронных почтовых ящиков[1].

В то же время, несмотря на наличие формальных признаков преступления, принять решение о возбуждении уголовного дела и правильно квалифицировать содеянное бывает затруднительно.

Действия следователя по проверке сообщения.

1) Принятие заявления и объяснения от пострадавшего, в котором необходимо отразить следующую информацию:

- точные дата, время сообщений между продавцом и покупателем;
- канал связи (сервис), с помощью которого отправлялись и принимались сообщения (социальные сети, мессенджеры);
- способ оплаты товара (с помощью банковского перевода или электронных платежных систем);
- предоставить чеки, справки переводов продавцу денежных средств с указанием точной дата и времени, а также наименования платежной системы и реквизитов оплаты;
- если сохранилась переписка, то необходимо попросить пострадавшего сделать скриншоты (снимки экрана) телефона и указать в заявлении просьбу приобщить указанные фотографии к материалам проверки;
- если пострадавший затрудняется предоставить переписку с продавцом – необходимо произвести осмотр мобильного телефона или компьютера с фиксацией даты, времени, наименования аккаунта продавца, привязанного номера мобильного телефона, аватара и т.д.
- отразить в объяснении причины обращения в правоохранительные органы, которые позволили пострадавшему считать сделку купли-продажи преступлением. К таким аргументам можно отнести: продавец перестал выходить на связь или удалил объявление (аккаунт), посылка не пришла, либо в посылке был иной товар, не представляющий материальной ценности.

Если на момент проверки сообщения о преступлении (принятия заявления от пострадавшего) связь с продавцом имеется необходимо отправить поручение по месту его расположения с целью получения объяснения по факту сделку с покупателем и фиксации ответов на вопросы:

- доказательства наличия товара перед его продажей (чеки, фотографии, подтверждение иными лицами);
- факт получения денежных средств от покупателя;
- подтверждение отправки товара транспортной компанией или иным сервисом доставки;
- доказательства отправки именно того товара, который он продавал на сайте объявлений (кому передавал товар для отправки, как упаковывал, кто может подтвердить отправку и т.д.);
- наличие умысла на обман покупателя.

---

[1] Науменко О.А. Проблемы в расследовании уголовных дел о мошенничестве, совершенном с использованием информационно-телекоммуникационной среды // Вестник Краснодарского университета МВД России, – 2019 – №3. – С. 60-64.

Если в ходе получения объяснения от продавца не было получено достаточных данных о совершении им преступлении, то принимается одно из двух решений.

1. Проверка по факту обращения покупателя завершается вынесением постановлением об отказе в возбуждении уголовного дела и сторонам рекомендуется обратиться в суд для разрешения гражданско-правового спора. Данное решение принимается если покупатель товар получил, но, по его мнению, он не соответствует факультативным характеристикам (другой цвет, комплектация, режим работы и т.д.).

2. Возбуждается уголовное дело по факту хищения товара в процессе его транспортировки неустановленными в ходе проверки лицами по ст. 158 УК РФ. Наиболее часто такие случаи наблюдаются при оказании услуг доставки АО «Почта России».

Однако, рассмотренная выше ситуация встречается не так часто. В ряде случаев к моменту обращения пострадавшего в правоохранительные органы, связи с продавцом не имеется. В таком случае проводятся следующие мероприятия.

1. Запрос в банк или иную платежную систему с целью установления факта перевода денежных средств и выяснения персональных данных получателя. Рекомендуется запросить информацию об иных счетах, открытых в банках с целью проверки причастности к совершению других преступлений и добавления информации в автоматизированные базы данных.

Необходимо отметить, что при формировании запросов в рамках ст. 26 Федерального закона от 2 декабря 1990 г. №395-1 «О банках и банковской деятельности»[1] следует четко понимать, в какой организации и какие сведения могут быть запрошены, исключив случаи направления подобных запросов операторам платежных систем, не обладающим необходимой информацией и не относящимся к финансово-кредитным учреждениям.

Следует иметь в виду, что мошенники, с целью ввести в заблуждение потерпевших и сотрудников полиции, зачастую сообщают ложные сведения о принадлежности карты к банку. Например: «Переведите предоплату на счет банковской карты Сбербанка 2245 6145 4353 1354». Не смотря на указание мошенника на принадлежность карты к Сбербанку, фактически указанная банковская карта выпущена и обслуживается банком «ВТБ». Для того, чтобы верно направить запрос и не терять время в ожидании отрицательного ответа, следует проверять банковские карты на принадлежность.

Кроме того, ненадлежащим образом оформленные запросы остаются без ответа, так как операторы платежных систем отвечают лишь за техническую составляющую платежных сервисов, не имеют доступа к персональным данным плательщиков, не аккумулируют запрашиваемые данные, в своей деятельности

[1] О банках и банковской деятельности: Федеральный закон от 2 декабря 1990 г. №395-1 // СПС "КонсультантПлюс" (дата обращения 12.09.2023 г.).

руководствуются положениями Федерального закона от 27 июня 2011 г. №161-ФЗ «О национальной платежной системе»[1].

Многие мошенники принимают денежные средства на счета абонентских номеров. У каждого сотового оператора есть свои особенности по указанному направлению:

- расчетные операции по абонентским номерам «Билайн» проводит ЗАО «Национальная сервисная компания». Поэтому данные о движении денежных средств можно запросить как у самого оператора «Билайн», так и у ЗАО «НСК»;

- расчетные операции по абонентским номерам «МТС» ПАО «Мобильные ТелеСистемы» проводят самостоятельно, поэтому данные о движении денежных средств можно запросить только у самого сотового оператора;

- расчетные операции по абонентскому номеру «Мегафон» проводит ООО «банк Раунд». Данные о движении денежных средств можно запросить только у данной организации;

- у оператора сотовой связи «Теле2» нет устоявшегося корреспондента и для проведения расчетных операций он может использовать много сторонних организаций. Информацию о движении денег нужно запрашивать у самого оператора, а после – у корреспондента[2].

2. Запрос в администрацию сервиса, оказывающего услуги электронной торговой площадки (доски объявлений) с целью установления:

- IP и по возможности MAC адреса абонентского устройства продавца в как период совершения преступления, так и с момента регистрации (для возможности идентификации и физического расположения продавца);

- персональные данные продавца, указанные им при регистрации;

- номер телефона, привязанный к аккаунту продавца;

- связанные аккаунты по данным сетевой активности, поведенческим факторам, номеру телефона, Coockie файлам браузера (текстовые файлы, сгенерированные и установленные в браузер пользователя соответствующими электронными площадками, которые содержат информацию о посещении сайта и нужны для идентификации пользователя), IP и MAC адресам;

- список объявлений и деловая активность на сайте с момента регистрации аккаунта;

- каким браузером пользовался продавец, какие расширения на нем установлены, использовались ли VPN подключения в расширениях браузера, задействовался ли анонимайзер.

Определенную сложность в ходе расследования представляет использование злоумышленниками программного обеспечения, позволяющего избежать (или существенно затруднить) их идентификацию - VPN, TOR, SSL, а

---

[1] О национальной платежной системе: Федеральный закон от 27 июня 2011 г. № 161-ФЗ // СПС «КонсультантПлюс» (дата обращения 16.01.2024 г.).

[2] Методические рекомендации: «Алгоритм раскрытия «дистанционных» мошенничеств и краж с банковских карт, совершаемых с использованием информационно-телекоммуникационных технологий» // Главное Управление Министерства Внутренних дел Российской Федерации по Воронежской области. Управление уголовного розыска. – 2020. С. 10.

также технологий, позволяющих менять IP-адрес пользователя сети Интернет, создавать динамические или нераспознаваемые IP-адреса, применять технологии подменных абонентских номеров посредством IP-телефонии.

Решение проблемы идентификации лиц, использующих программы-анонимайзеры, видится в комплексе законодательных, технических, организационных и научных мер. Например, организация на должном уровне работы по исследованию cookie-файлов, важной особенностью которых является их неизменность. На сегодняшний день существует определенный опыт противодействия анонимным абонентским номерам при входящих и исходящих телефонных вызовах, использующих функцию подмены номера, с помощью создания центров очистки интернет-трафика.

3. Устанавливается провайдер, за которым закреплен установленный ранее через администрацию торговой площадки и выданный в период преступления продавцу IP адрес (сделать это можно, к примеру, на сайте https://2ip.ru).

4. Запрос провайдеру по IP-адресу, который присваивался конечному абонентскому устройству, отправлявшему пакеты данных на сайт электронной торговой площадки. В запросе необходимо указать категории сведений, которые необходимо предоставить правоохранительным органам:

- персональные данные лица в соответствии с договором оказания услуг связи;
- какой тип имеет указанный IP-адрес (динамический, статический, белый или серый);
- какие IP-адреса ранее присваивались указанному абоненту с указанием временных промежутков;
- физическое местоположение коммутационного оборудования (коммутатора, роутера, маршрутизатора);
- сервисы, сайты и иные ресурсы, которые активно посещаются указанным абонентом (с указанием адресов страниц, в которых может содержаться информация о кабинете пользователя, предпочтениях и интересах).

Следует обратить внимание, что имеет место сокрытие подлинных персональных данных от провайдера при подключении к сети Интернет. По-прежнему операторы мобильной связи осуществляют распространение SIM-карт (в переходах метро, возле крупных торговых точек, в иных многолюдных местах) без процедуры идентификации пользователя. Также активно используются для входа в Интернет зарубежные IP-адреса, находящихся вне юрисдикции Российской Федерации через VPN[1].

5. Установка конкретного оператора сотовой связи по номеру мобильного телефона (можно сделать с использованием сервисов https://www.kody.su/check-tel, https://phonenum.info) и определение IMEI номера. IMEI – уникальный номер сотового аппарата. Данный номер состоит из 15 последовательных чисел, из

[1] Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий : учебное пособие : в 2 ч. / [А. В. Аносов и др.]. – М. : Академия управления МВД России, 2019. – Ч. 1. – 208 с. С. 158.

которых первые 14 определяют происхождение, модель и серийный номер сотового устройства, а 15-ая – контрольная цифра. В предоставляемых сотовыми операторами детализациях последняя контрольная цифра всегда обозначается как «0». Она не имеет целевого значения, поэтому идентификация сотового аппарата при его изъятии всегда происходит по первым 14 цифрам. Зная IMEI, посредством множества онлайн-сервисов можно определить марку и модель сотового телефона (https//imei.info). Информация о конкретной модели и марке телефона облегчит работу при проведении обысков и осмотров, а также позволит определить стоимость телефона. Чем дороже телефон, тем меньше вероятность того, что злоумышленник избавится от него после совершения мошеннических действий, а следовательно будет продолжать его использовать.

6. По запросу оператор сотовой связи предоставляет информацию следующего характера:

- анкетные (персональные) данные лица по договору оказания услуг;
- физическое местоположение абонента в период совершения преступления;
- сведения о посещаемых сайтах в период совершения преступления;
- список установленного программного обеспечения по анализу передаваемого трафика и точек доступа приложений.

Вторая ситуация – обман при покупке товара на сайтах объявлений. Пострадавший размещает объявление в сети Интернет с целью продажи товара или оказания услуги. Предполагаемый преступник звонит по номеру телефона, указанному в объявлении, и предлагает отправить товар с помощью сервисов транспортной доставки. Сценарии возможных способов преступлений могут быть разные, однако следует выделить общие характерные черты:

- покупатель, как правило, находится в ином населенном пункте;
- покупатель очень заинтересован в покупке именно указанного товара, не сильно интересуется состоянием, характеристиками;
- поступают настоятельные предложения перейти для общения в другой мессенджер («WhatsApp», «Telegram» и т.п.);
- покупатель может отправить фотографию паспорта или иного документа для усыпления бдительности продавца, подтверждения своих намерений и честности, однако в большинстве случаев документ не имеет отношения к покупателю;
- покупатель отправляет продавцу ссылки на поддельные страницы об оплате товара, копии фиктивных платежных документов;
- иногда покупатель просит назвать продавца персональные данные, номера банковских карт, сообщить код из СМС;
- для проведения успешного перевода преступник может попросить продавца совершить действия в приложении мобильного банка, подойти к банкомату для идентификации и т.п.

Среди характерных признаков, позволяющих принять решение о возбуждении уголовного дела по факту мошенничества следует отнести:

- отсутствие поступления денег в течении 3 рабочих дней за отправленный транспортной компанией товар;

- связи с покупателем не имеется;

- платежные документы были отправлены пострадавшему с помощью сторонних сервисов и сайтов;

- по номеру транзакции не удается подтвердить перевод денег.

При проведении проверки по данному факту проводятся отдельные уже ранее рассмотренные процессуальные действия, направленные на: установление персональных данных преступника:

- в объяснении (допросе) пострадавшего необходимо отразить информацию о лице, представившемся покупателем: как оно узнало о товаре, где проживает, какие данные о себе сообщило, особенности голоса, шум на заднем фоне, адрес доставки или данные о такси, которое иногда используется в таких целях и иные обстоятельства, имеющие значение для расследования преступления;

- запрос оператору сотовой связи по детализации звонков пострадавшего с целью установления и фиксации номера покупателя. Данную информацию при наличии возможности эффективнее получить самим пострадавшим;

- запрос в компанию, предоставляющей услуги торговой площадки для определения IP-адреса лиц, которое просматривали объявление продавца и активировали просмотр номер телефона. Следует обратить внимание, что отдельные сервисы с целью противодействия спаму не предоставляют реальные номера телефонов продавцов, а предлагают совершить звонок по временному номеру, который периодически меняется. По номеру телефона, полученного от пострадавшего или оператора сотовой связи, можно отфильтровать список IP адресов, которые просматривали и получили указанный номер телефона;

- определяется провайдер, за которым закреплен указанный IP-адрес и по запросу выясняется максимально возможная информация о преступнике: географическое положение, анкетные данные, предпочтения, проводится анализ трафика и т.д.;

- если звонок совершался посредством мессенджеров (VoIP телефония), то следует осмотреть сотовый телефон (или компьютер) с целью фиксации данных звонка, номера телефона, аватара, документов, отправленных покупателем;

- фотографии платежных документов, присланных покупателем, необходимо изучить следователю с привлечением специалиста, а в отдельных случаях можно назначить экспертизу. В фотографии имеются метаданные EXIF (Exchangeable Image File Format) и хранятся в самом начале самих файлов фотографий (до данных фактического изображения). По этим данным можно определить: название и версию программного обеспечения (камеры); дату и время съемки; данные о цифровой среде; географические координаты местоположения; ориентация камеры (вертикальная или горизонтальная); размер матрицы; информация об авторе и многое другое. Наибольший интерес представляют данные о местоположении сделанного снимка. Также отметим, что EXIF легко поддаётся редактированию. Существуют онлайн-сервисы для изменения съёмочных параметров, поэтому данные EXIF могут выступать ориентирующей и справочной информацией;

- если использовались сервисы такси для доставки товара необходимо сделать запрос в диспетчерскую службу или компанию, оказывавшей услуги для установления водителя и подробных данных о заказе (кто и как вызывал, куда и что доставлено и т.д.). Также необходимо получить показания водителя, который осуществлял доставку товара;

- необходимо изъять записи с камер видеонаблюдения, которые имеются в пункте доставки транспортный компании и допросить лиц, выдававшим заказ преступнику;

- сделать запрос к операторам сотовой связи (через поручение органу дознания) для установления лиц, которые находились в районе выдачи товара преступнику по работающим сотовым телефонам (биллинг).

Третья ситуация – преступления с использованием сайтов в форме интернет-магазина.

Мошенник создает (или покупает) интернет-сайт по продаже нескольких товаров (интернет-магазин) различной тематики или один товар (одностраничный сайт - landing). Регистрирует несколько виртуальных номеров (8-800-…, 8- 495-... и др.) у оператора проводной телефонной связи, оператора сотовой связи и IP-провайдера, которые указывает их на сайте в качестве контактов. В последующем покупатели осуществляют на сайте покупки товаров. Преступных схем в таких случаях несколько:

1. Фактическая продажа товаров на сайте не осуществляется – мошенники получают деньги, прилагают фиктивные данные об отправке товаров транспортными компаниями. Сайт работает определённое время до формирования критической массы отрицательных отзывов (заявлений в правоохранительные органы), после чего он ликвидируется и создается новый магазин с другими контактными данными и тем же самым товаром.

2. Товары ненадлежащего качества (подделки), которые выдаются за оригинальные, продаваемые с большими скидками. Часто покупатель получает не те товары, которые рекламируются на сайте, в связи с чем требуется инициировать гражданско-правовые споры со стороны покупателей.

3. На сайте реализуются некачественные товары, не имеющие всех необходимых документов для их законной продажи. В данном случае сайт может существовать продолжительное время, так как привлечь владельцев бывает затруднительно по причине необходимости производства экспертизы товаров, проверки документов на товары и направлении запросов в компанию.

В указанных случаях для принятия решения о возбуждении уголовного дела необходимо выполнить ряд проверочных действий.

Установить владельца сайта путем определения IP адреса хостинга, на котором размещается сайт и владельца доменного имени. Сделать это можно на сайте https://whois.ru.

Провести осмотр сайта с приложением снимков экрана с целью фиксации способов оплаты, вида и способов оплаты на сайте, данных ИНН, юридического адреса и т.п.

Направить запрос и по возможности получить показания от представителей хостинг провайдера, на котором размещается сайт и который регистрировал DNS.

Сведения, которые необходимо запрашивать по доменному имени сайта: информацию о паспортных данных регистратора доменного имени; информацию об использованных для регистрации абонентских номерах и электронной почте; информацию о том, каким образом была произведена регистрация пользователя; информацию об IP-адресах, использованных для регистрации доменного имени; информацию об IP-адресах, использованных для входа в личный кабинет или панель управления для администрирования доменного имени; информацию об оплате услуг регистрации и аренды доменного имени, с указанием полных реквизитов плательщика; аналогичную информацию по иным доменным именам, зарегистрированным данным пользователем, установленным при анализе Cookie-файлов.

Сведения, которые необходимо запрашивать по арендуемому хостингу сайта информацию о паспортных данных арендатора хостинга; информацию об использованных для аренды абонентских номерах и электронных почтах; информацию о том, каким образом была произведена регистрация пользователя; информацию об IP-адресах, использованных для аренды хостинга; информацию об IP-адресах, использованных для входа в личный кабинет или панель управления для администрирования хостинга; информацию об оплате услуг аренды хостинга, с указанием полных реквизитов плательщика; аналогичную информацию по иным хостингам, арендуемым данным пользователем, установленным при анализе cookie-файлов.

Если анкетные и паспортные данные, указанные собственником сайта, были настоящими – необходимо опросить данное лицо или отправить поручение органу дознания об этом. В объяснении необходимо зафиксировать информацию о товаре, где и при каких обстоятельствах он был приобретен, какие документы имеются у продавца и т.д.

Необходимо изъять документы на товар с целью установления его оригинальности, безопасности, наличие сертификатов и т.д.

Определить IP-адреса, с которых осуществлялось администрирование сайта и по возможности установить геолокацию лица.

Направить запрос операторам связи, предоставившим номера владельцу сайта для установления анкетных данных последнего по договору.

- По установленным в ходе осмотра способам оплаты товаров направить запросы в платежные системы для определения данных владельца счета и IP-адресов, с которых он входил в личный кабинет.

По полученным ответам из компаний электронных платежных систем определить способы вывода денег на реальные банковский счета и потом направить запросы в соответствующие банки.

При проведении проверки по указанным фактам необходимо установить умысел лица на совершение преступления, так как в ряде случаев возникают ситуации, разрешаемые в гражданско-правовой сфере путем проведения

судебного разбирательства, либо находящиеся в компетенции органов исполнительной власти (к примеру, Роспотребнадзор).

Четвертая ситуация – продажа товаров, запрещенных к гражданскому обороту.

На территории РФ запрещены к свободному распространению наркотические средства, оружие, материалы порнографического характера и т.д., однако это не исключает существование таких площадок в «темной зоне» Интернета («Даркнет») и сайтов, зарегистрированных на иностранных хостингах. Борьба с такими категориями преступлений представляется особо затруднительной по причине возникновения сложностей, возникающих при деанонимизации продавцов. Как правило, используется браузер Tor (The Onion Router) - свободное и открытое программное обеспечение для реализации так называемой луковой маршрутизации. Это система прокси-серверов, позволяющая устанавливать анонимное сетевое соединение, защищённое от прослушивания и расшифровки трафика. Это анонимная сеть виртуальных туннелей, предоставляющая передачу данных в зашифрованном виде.

С помощью Tor как покупатели, так и продавцы могут сохранять анонимность в Интернете при посещении сайтов, администрировании интернет-магазинов, отправке сообщений и писем, а также при работе с другими приложениями, использующими протокол TCP. Анонимизация трафика обеспечивается за счёт использования распределённой сети серверов (узлов).

Противодействие нелегальным торговым площадкам осуществляется по нескольким направлениям.

1. Проведение оперативно-розыскных мероприятий субъектами ОРД самостоятельно и по поручению следователя. Среди ОРМ, проводимых по данной категории преступлений, можно назвать как традиционные (опрос, наблюдение), так и технические (снятие информации с технических каналов связи, получение компьютерной информации).

2. Активное взаимодействие правоохранительных органов с Роскомнадзором и интернет-провайдерами для выявления лиц, активно использующих алгоритмы анонимизации для проверки их причастности к совершению преступлений.

3. Мониторинг социальных сетей, групп в мессенджерах, рекламирующих продажу запрещенных товаров. Анализ целесообразнее осуществлять с использованием нейронных сетей, позволяющих эффективно анализировать «подозрительные» сообщения пользователей.

4. При выявлении групп в мессенджерах проводится осмотр диалогов или сайта с фиксацией криминалистически значимой информации в протоколе и приложении снимков экрана.

5. В случае установления причастных лиц необходимо получить и зафиксировать информацию по банковским и иным переводам преступника с целью наложения в дальнейшем ареста на денежные средства и иные материальные ценности лица.

6. В связи с большой латентностью исследуемого вида преступлений, совершаемых с использованием нелегальных торговых площадок, следователю

приходится сталкиваться как с противодействием со стороны покупателей таких «товаров», так и техническими трудностями при установлении IP-адресов, анкетных данных лиц. Процесс деанонимизации достаточно трудоемок, так как ряд лиц помимо использования Tor браузера использует и VPN иностранных компаний. Следователь, даже установив IP-адрес интересующего оборудования, с большой вероятностью столкнется с проблемой получения ответа от интернет-провайдера иностранного государства, которое этот адрес выдавало абоненту. В связи со сказанным, процесс выявления и раскрытия преступлений в этой области требует слаженной работы международных организаций, Интерпола, Европола, что в настоящих условиях представляется весьма затруднительным процессом.

Пятая ситуация – хищения с использованием маркетплейсов.

В последние годы большую популярность приобрела дистанционная продажа товара с использованием маркетплейсов («Ozon», «Wildberries», «Яндекс Маркет» и др.). Все схемы мошенничества на маркетплейсах можно свести к нескольким основным направлениям:

1. Классическое мошенничество с хищением денег. Мошенники зачастую просят перейти в отдельный чат в мессенджере и/или провести оплату переводом по фишинговой ссылке. Кроме того, при использовании фишинговых сайтов у пользователей маркетплейсов также могут похитить платежную информацию от их банковских карт.

2. Получением доступа к платежной информации банковских карт. Преступники создают товарное предложение и ждут заказа от клиента на дорогой товар, но после получения оплаты отменяют заказ – деньги возвращаются пользователю. После отмены заказа покупателю пишет продавец и предлагает совершить покупку в обход маркетплейса, аргументируя тем, что это будет дешевле. После этого клиенту предлагают совершить покупку на стороннем ресурсе и отправляют на него фишинговую ссылку.

3. Получение доступа к аккаунтам учетных записей пользователей на маркетплейсах. Доступ к ним обычно пытаются получить при помощи методов социальной инженерии. Покупателю могут позвонить и сказать, что оплата за товар не прошла, а потому данные от личного кабинета маркетплейса нужно ввести в ручном режиме на ином сайте или продиктовать преступнику. Хищение данных аутентификации и иных сведений на маркетплейсах может привести к тому, что преступники, получив доступ к личному кабинету, смогут совершить покупку от имени клиента или подадут заявку на возврат денег за товар, но уже с указанием данных своей карты.

4. Преступления с подменой товара как со стороны покупателя, так и со стороны продавца. Наиболее популярная схема мошенничества на маркетплейсах сегодня заключается в подмене товара. Продавцы вместо оригинальных товаров продают их реплики. Причем если совсем недавно это касалось в основном брендовой одежды и обуви, то сейчас с подделками сталкиваются даже бюджетные марки с хорошими отзывами. Также имеют место ситуации, когда покупатель заказывает товар, но при получении его заменяет другим и возвращает продавцу.

Механизм выявления, документирования, проверки и расследования рассматриваемых преступлений во многом аналогичен указанным выше действиям, связанным с изъятием записей камер видеонаблюдения, направлением запросов в банковские организации, компаниям, осуществляющим дистанционную продажу товаров, взаимодействия с интернет-провайдерами для получения IP-адресов, операторами сотовой связи по номерам телефонам и т.д.

Расследование и раскрытие преступлений о дистанционных хищениях, которые зачастую носят межрегиональный характер, нуждаются в выработке единого алгоритма действий как на этапе проверки заявления и сообщения о преступлении, так и на первоначальном этапе расследования.

Вместе с тем до настоящего времени не сформирован действенный инструментарий быстрого получения от кредитных организаций, интернет-провайдеров, операторов связи, социальных сетей и интернет-сервисов информации, имеющей доказательственное значение по расследуемым преступлениям (сведений о лице, биллинге, движении денежных средств по лицевым счетам абонентских номеров и др.). Длительность получения ответов составляет от одного до нескольких месяцев[1].

Таким образом, в данном разделе предложена рекомендованная последовательность проверочных и процессуальных действий, реализуемых в рамках типовых ситуаций совершения преступлений с использованием торговых площадок (сервисов) для коммерческих заказчиков и физических лиц. Типовые ситуации выделены с учетом их формирования на стадии обращения заявителя о совершенном преступлении или регистрации материала проверки органом дознания. Первая ситуация – продажа несуществующего товара. Вторая ситуация – обман при покупке товара на сайтах объявлений. Третья ситуация – преступления с использованием сайтов в форме интернет-магазина. Четвертая ситуация – продажа товаров, запрещенных к гражданскому обороту. Пятая ситуация – хищения с использованием маркетплейсов.

3. ОСОБЕННОСТИ ПРОИЗВОДСТВА ОТДЕЛЬНЫХ СЛЕДСТВЕННЫХ И ИНЫХ ПРОЦЕССУАЛЬНЫХ ДЕЙСТВИЙ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ ТОРГОВЫХ ПЛОЩАДОК (СЕРВИСОВ)

При расследовании преступлений, совершаемых с использованием электронных торговых площадок (сервисов), необходимо провести комплекс процессуальных (следственных) действий, предусмотренных процессуальным законодательством. Перечень процессуальных действий возможных и допустимых при получении сообщений о преступлении регламентирован ст. 144 УПК РФ. При этом особое значение будет иметь не только непосредственно сами

[1] Орлова А.А., Гончар В.В. Особенности расследования преступлений, совершаемых в сфере информационных технологий // Безопасность бизнеса. – 2021. – №4. – С. 25-29.

процессуальные действия, но и организационные и тактические особенности их проведения. В настоящем разделе нами будут рассмотрены комплекс процессуальных (следственных) действий, которые наиболее часто встречаются при раскрытии и расследовании преступлений, совершаемых с использованием электронных торговых площадок (сервисов).

Предварительное изучение материалов уголовных дел, возбужденных по признакам преступлений, совершаемых с использованием электронных торговых площадок (сервисов) и опрос сотрудников органов внутренних дел позволил нам выделить и рассмотреть перечень процессуальных и следственных действий, результаты которых позволили не только формировать доказательственную базу по уголовным делам, но и провести всесторонне и полное расследование уголовного дела. Ниже указаны перечень таких процессуальных и следственных действий:

– получение письменного объяснения;

– осмотр места происшествия;

– осмотр предметов и документов;

– письменные поручения;

– допрос потерпевшего;

– допрос свидетелей;

– допрос сотрудников банков (кредитных организаций) и других;

– запросы (к оператору сотовой связи; к организации, обслуживающей интернет-ресурс)

– выемка;

– обыск;

– получение сведений о соединениях между абонентами и (или) абонентскими устройствами;

– допрос подозреваемого;

– назначение и производство судебных экспертиз.

Получение письменного объяснения от заявителя требует выполнения следующих этапов. При получении объяснения необходимо: установить дату и время обнаружения объявления, получения ссылки на соответствующий интернет-ресурс. При возможности найти объявление в Интернете и зафиксировать его адрес, повторно пройдя по интернет-ссылке.

Сделать снимок экрана и приложить его к материалам проводимой проверки; определить, с использованием какого технического устройства заявитель заходил на сайт с размещенным объявлением – стационарного компьютера или мобильного устройства; получить абонентский номер и модель телефона, подключенного к услуге «Мобильный банк», уточнить используемую операционную систему в телефоне («Android», «iOS»), а также наличие установленных антивирусных программ; рассмотреть характеристики продаваемого товара или вида оказываемых услуг, указанных в объявлении о продаже; изучить условия купли-продажи или оказания услуг, содержащиеся в объявлении, включая условия предоплаты, способы оплаты, сроки и виды поставки товара или оказания услуг, а также ответственность сторон; записать контактные данные «продавца», указанные в объявлении; проверить наличие

отзывов и комментариев к данному объявлению; уточнить, сохранилось ли у заявителя данное объявление (номер объявления, ID-страницы); выяснить, каким образом и когда (дата, время) заявитель связался с «продавцом»; запросить информацию о том, как «продавец» представился, где, по словам «продавца», он находился, и известно ли ему местонахождение товара; получить информацию о том, что именно сообщил «продавец» о продаваемом товаре или оказываемых услугах, об условиях оплаты, сроках и способах доставки; записать описание голоса «продавца» и уточнить, сможет ли заявитель его опознать, и по каким признакам.

Если заявитель осуществил перевод денежных средств, установить дату, период времени, способ (через банкомат, «Сбербанк Онлайн», «Мобильный банк»), размер и на какой счет (номер счета, банковская карта, открытая на имя кого) произведен перевод.

Если перевод осуществлен со своей банковской карты на карту неизвестного через «Сбербанк Онлайн», через «Личный кабинет», установить место входа заявителя в сеть Интернет (с какого компьютера, ноутбука, планшета, с использованием какого модема, Wi-Fi роутера), их MAC-адреса, логины и пароли, а также уточнить компанию-провайдера, предоставлявшую в этот день услуги доступа в Интернет.

Следует также установить такие сведения, как: место и дата открытия счета (банковской карты), с которого заявитель перевел средства; способ уведомления «продавца» о переводе средств на указанную им банковскую карту (или электронный кошелек); информацию, которую «продавец» предоставил после подтверждения оплаты (перевода средств на банковскую карту); временные рамки и место, куда заявитель явился для получения предполагаемого товара, а также момент осознания им совершенного преступления; действия заявителя после выявления факта мошенничества; обращался ли заявитель в банк, наличие выписок о движении средств по карте, а также ответы на обращения; размер ущерба, нанесенного заявителю.

Дополнительная информация.

В необходимых случаях, следует получить показания от очевидцев, родственников и других лиц с соответствующей информацией; запросить у работников банка о процессах перевода денежных средств и у лиц, обслуживающих платежные терминалы; истребовать документов и предметов, включая запросы дознавателя в учреждения и организации.

Получить от заявителя справки, выписки, чеки, договоры на банковское обслуживание карты, подтверждающих перевод средств, а также другие документы.

Осмотр места происшествия в соответствии с статьей 176 УПК РФ, если есть возможность обнаружения следов преступления и выяснения обстоятельств.

В случае просмотра объявлений на продажу товаров через компьютер в жилом помещении, осмотр жилища с согласия заявителя для проверки компьютерного оборудования и связанных сетевых устройств.
В протоколе осмотра места происшествия необходимо отразить:

1. Расположение компьютера и устройств телекоммуникации (Wi-Fi роутера, модема), а также порядок их соединения (беспроводная связь, организованная компьютерная сеть).

2. Назначение, название, серийный номер и функциональное состояние каждого устройства.

3. Содержание информации, отображаемой на мониторе.

Если интернет-ресурс, использованный для противоправных действий, продолжает функционировать на момент осмотра, следует в протоколе указать контактную информацию, род деятельности ресурса, отзывы, приложить распечатки с сайта и экранный снимок с реквизитами страницы.

При осмотре места происшествия следователь, дознаватель, с письменного согласия заявителя, может осмотреть мобильный телефон для фиксации следующей информации:

1. IMEI телефона и наличие SIM-карт с абонентскими номерами.

2. Информация из журнала вызовов, банка сообщений, записной книжки внутренней памяти мобильного устройства или SIM-карты.

3. Сохраненные текстовые переписки по SMS или мессенджерам («WhatsApp», «Viber», «Авито»).

4. История посещения интернет-сайтов и другие.

В рамках осмотра необходимо тщательно исследовать разделы приложения «Мобильный банк» (например, «История платежей», «Последние операции») и сделать скриншоты мобильного устройства для фиксации информации о движении денежных средств по счету (банковской карте).

При осмотре жилого помещения заявителя возможно изъятие документов и сведений, связанных с хищением, таких как:

1. Детализация входящих и исходящих соединений абонентского номера, использованного для общения с подозреваемым лицом.

2. Выписки по банковской карте (счету), с которого были переведены денежные средства.

3. Договор банковского счета (банковского обслуживания) и документы об оформлении банковской карты и др.

Осмотренные или изъятые предметы и документы подлежат последующему исследованию, если они могут быть использованы в качестве вещественных доказательств по делу (согласно статье 81 УПК РФ).

Осмотр предметов и документов. При проверке сообщения о преступлении в соответствии с частью первой статьи 144 УПК РФ следователь, дознаватель может осмотреть все обнаруженные и изъятые предметы и документы, полученные в результате осмотра места происшествия или истребованные.

Осмотр компьютерных устройств, электронных носителей информации, мобильных телефонов и их содержимого, видеозаписей и документов может входить в состав осмотра места происшествия. Как самостоятельное следственное действие, он проводится, если обнаруженные предметы и документы, имеющие значение для дела, не были сразу осмотрены, или если требуется повторный осмотр с применением специальных знаний и технических средств.

В ходе проверки сообщения о преступлении и расследования уголовного дела следователь, дознаватель могут выдавать органу дознания письменные поручения обязательного исполнения, предписывая проведение оперативно-розыскных мероприятий (часть первая статьи 144 УПК РФ). Поручения могут включать проверку абонентских номеров, банковских карт, счетов подозреваемых на совпадение с другими уголовными делами, совершенными аналогичным способом.

Письменные поручения. Содержание письменных поручений должно быть максимально детализировано, включая всю необходимую информацию для их качественного исполнения, а также указание на проведение конкретных следственных действий, таких как допросы определенных лиц.

При наличии достаточных данных и оснований, указывающих на признаки преступления, следователь или дознаватель может возбудить уголовное дело, вынести соответствующее постановление и незамедлительно уведомить заявителя о принятом решении, разъяснив ему право на обжалование и порядок обжалования.

Допрос потерпевшего (статьи 187-191 УПК РФ). Подлежащие выяснению вопросы при допросе потерпевшего аналогичны тем, которые рассматриваются при получении письменных объяснений от заявителя в процессе проверки сообщений о рассматриваемых преступлениях.

Допрос свидетелей (статья 56 УПК РФ, статьи 187-191 УПК РФ). В ходе предварительного расследования в качестве свидетелей могут быть допрошены лица, обладающие информацией о совершенном преступлении, такие как родственники и знакомые потерпевшего.

Если ответ от оператора сотовой связи получен, лицо, на которое зарегистрирована использованная при преступлении SIM-карта, может быть допрошено в качестве свидетеля. В ходе допроса необходимо установить информацию о приобретении и использовании SIM-карты, ее передаче, а также наличие установочных данных получателя, если таковые имеются.

Если владелец SIM-карты утверждает, что не регистрировал ее, требуется выемка у оператора сотовой связи договора об оказании услуг с использованием данной SIM-карты, а также других документов, послуживших основанием для заключения договора, с последующим проведением почерковедческой судебной экспертизы.

При обнаружении зарегистрированных на вымышленных лицах SIM-карт, в материалы дела следует приложить справку от органа миграции об отсутствии соответствующих данных о лице и протоколы допросов жильцов по указанному адресу, подтверждающих, что лицо с такими персональными данными не проживает там.

При выявлении несоответствия персональных данных фактическим пользователям информации в абонентских договорах, дознаватель в целях прекращения оказания услуг направляет уведомление в соответствующее подразделение органов внутренних дел, осуществляющее оперативно-розыскную деятельность, согласно статье 46 Федерального закона «О связи». Оператор связи обязан прекратить услуги связи по запросу органа в случае

неподтверждения персональных данных в течение пятнадцати суток.

Допрос сотрудников банков (кредитных организаций):

В качестве свидетелей могут быть опрошены сотрудники банков, с целью выяснения следующих аспектов:

- должность и функциональные обязанности;
- условия обслуживания банковских счетов и предоставления услуг;
- виды выпускаемых банковских карт и механизм перевода денежных средств;
- наличие договора с потерпевшим, являющимся держателем банковской карты;
- тип программного обеспечения, предоставляемого для удаленного доступа и управления банковским счетом, включая порядок установки и использования;
- операции, доступные через данное программное обеспечение;
- иные обстоятельства, важные для расследования уголовного дела.

В случае, если перевод денежных средств производился в банковских учреждениях, у сотрудников банков следует выяснить:

- какие документы, удостоверяющие личность, предъявил подозреваемое лицо;
- когда и какие действия были совершены;
- присутствие других лиц;
- наличие камер видеонаблюдения в зале обслуживания;
- иные значимые факты.

В роли свидетеля может выступить сотрудник организации, предоставляющей услуги оператора сотовой связи, с целью предоставления информации о характеристиках предоставляемых услуг, включая удаленный доступ к интернету для использования программного обеспечения «Онлайн банк», «Мобильный банк».

Допрос других свидетелей:

В качестве свидетелей могут быть опрошены:

- родственники, знакомые, соседи подозреваемого, для выяснения обстоятельств, характеризующих его личность и образ жизни;
- сотрудники оперативных подразделений, выявившие преступление и установившие личность подозреваемого;
- другие лица, обладающие информацией, важной для расследования уголовного дела.

Запрос сведений. При необходимости разъяснения заключения эксперта, дознаватель вправе допросить эксперта согласно статье 205 УПК РФ.

Для получения информации, имеющей доказательственное значение, могут быть направлены запросы в соответствующие органы, организации и учреждения. В случае установления анкетных данных владельца абонентского номера, используемого при совершении преступления, следователь, дознаватель может направить:

– запрос к оператору сотовой связи. Для направления запроса к оператору сотовой связи, обслуживающему тот регион, где зарегистрирована SIM-карта с

нужным абонентским номером, следует обратиться ко всем операторам, кроме ПАО «ВымпелКом», поскольку у данного оператора единая база данных по всей Российской Федерации;

– запрос к организации, обслуживающей интернет-ресурс. Следователь, дознаватель имеет право направить запрос в организацию, обслуживающую интернет-ресурс, на котором опубликовано объявление. Запрос должен содержать данные о дате и времени регистрации, контактных данных, изменениях в профиле пользователя, точном наименовании ресурса, IP-адресах, а также о других объявлениях с указанным номером телефона.

После получения информации от организации, следует направить запросы провайдерам с указанными IP-адресами для получения данных о клиентах и их местонахождении. Приложение заверенной копии договора об оказании услуг связи также требуется.

Проверка достоверности паспортных данных абонентов. В случае сомнений в достоверности паспортных данных, полученных от оператора сотовой связи или организации, обслуживающей интернет-ресурс, необходимо направить запрос в соответствующее подразделение по вопросам миграции для получения информации о регистрации на территории Российской Федерации и о лицах, зарегистрированных по указанному адресу.

Получение информации о владельце электронной почты. При запросе информации о владельце электронной почты, учитывайте, что сведения о регистрации и администрировании почтовых ящиков @gmail.com, @google.com, @hotmail.com, @yahoo.com и прочих находятся за пределами Российской Федерации. Для получения этой информации, можно обратиться по линии НЦБ Интерпола или отправить запрос о правовой помощи в соответствии со статьями 453 и 454 УПК РФ.

Составление запроса. Для исключения возможности отказа в предоставлении информации, запрос должен быть тщательно подготовлен, включая все необходимые сведения для получения содержательного ответа. Например, при запросе к социальной сети «В Контакте», важно указать ссылку на страницу пользователя, чтобы избежать отказа из-за некорректности запроса.

Выемка. Одним из наиболее распространенных следственных действий на первоначальном этапе расследования является *выемка* (статья 183 УПК РФ).

С целью установления способа хищения денежных средств с банковской карты, места нахождения подозреваемого лица в момент изъятия из законного владения собственника денежных средств с банковской карты, следователю, дознавателю необходимо в соответствии со статьями 182, 183 и частью 1 статьи 165 УПК РФ с согласия прокурора возбудить перед судом ходатайство о производстве выемки информации о вкладах и счетах граждан в банках и иных кредитных организациях, примерно, следующего содержания[1]:

[1] Методические рекомендации «Расследование мошенничеств, связанных с реализацией товаров и оказанием услуг в сети Интернет». URL: https://49.xn--b1aew.xn--p1ai/citizen/Razjasnenija_MVD_Rossii/ методические-рекомендации-расследование (дата обращения 12.10.2023 г.)

«Ходатайствовать перед судом о производстве выемки в ПАО «Наименование банка» (получении) информации о движении денежных средств по банковской карте № ___ (банковскому счету № ___), открытой на имя (потерпевшего) Иванова Ивана Ивановича, __.__.___ года рождения, а именно:

– информации о дате открытия счета, месте открытия счета, дате, времени и месте подключения к банковской карте (счету) услуги «Мобильный банк», услуги «Онлайн банк», идентификационном номере пользователя и пароле, необходимых для входа в «Личный кабинет» заявителя;

– посредством какой услуги («Мобильный банк», через «Личный кабинет», «Онлайн банк», POS-терминал, банкомат) в установленную при производстве дознания дату __.__. 20__ денежные средства в сумме __ рублей перечислены с банковской карты № ___ (банковского счета № __) Иванова Ивана Ивановича, __.__. 19__ года рождения (потерпевшего);

– на какой номер счета (номер банковской карты) __.__. 20__ были перечислены денежные средства в сумме ___ рублей, место открытия счета, кредитной организации, в которой открыт счет, на который перечислены денежные средства, фамилия, имя, отчество, дата рождения, паспортные данные лица, на который данный счет открыт;

– информации о месте обналичивания (снятия) денежных средств, начиная с __ часов __ минут __.__. 20__ (с указанием номера банкомата и места его расположения);

– если перечисление денежных средств осуществлялось посредством услуги «Мобильный банк» с банковской карты № ___ (банковского счета №___) Иванова Ивана Ивановича, __.__. 19__ года рождения, то предоставить информацию: с какого абонентского номера телефона поступило сообщение с кодом подтверждения (поручением/распоряжением на проведение операции по перечислению __.__. 20__ денежных средств в сумме ___ рублей с банковского счета потерпевшего), точном времени (дата, час, минута) поступления в банк сообщения с кодом подтверждения (поручением/распоряжением на проведение операции по перечислению __.__.20__ денежных средств в сумме ___ рублей с банковского счета потерпевшего);

– если перечисление денежных средств осуществлялось посредством услуги «Онлайн банк» (через «Личный кабинет» потерпевшего), то предоставить информацию: в какое точное время (дата, час, минута, секунда) и с какого IP-адреса __.__.20__ осуществлялся вход в «Личный кабинет» «Онлайн банк» в момент перечисления денежных средств в сумме ___ рублей;

– если перечисление денежных средств осуществлялось посредством банкомата, то предоставить информацию: в какое точное время (дата, час, минута, секунда), с какого номера банкомата, место его расположения были перечислены денежные средства (аналогично в отношении POS-терминала).

После получения данных о том, что транзакция была осуществлена через «Онлайн банк» с определенного IP-адреса банка в конкретное время (с точностью до минуты или секунды), следующим этапом является выявление компании-провайдера, предоставившей данный IP-адрес в указанный момент.

Для достижения этой цели дознавателю предоставляется два варианта:

I. Он может направить официальное поручение начальнику органа дознания в соответствии с пунктом 1.1 части третьей статьи 41 УПК РФ, с целью получения специальных технических мероприятий из соответствующего подразделения органов внутренних дел. Таким образом, будет получена информация о компаниях-провайдерах и MAC-адресе устройства, а также дополнительные сведения, такие как логин, пароль и местоположение устройства, с которого был осуществлен доступ в Интернет через указанный IP-адрес в определенный момент времени (дата, час, минута, секунда).

II. В альтернативе, дознаватель имеет возможность самостоятельно выявить компанию-провайдера с использованием справочных интернет-ресурсов (например, «reg.ru», «whois-service.ru», «2ip.ru», включая возможность использования вкладки «IP-LOOKUP»). В этом случае, введя IP-адрес, полученный от банка при предоставлении данных о финансовых операциях, и произведя проверку, можно получить информацию о компании-провайдере. После этого дознаватель создает скриншот данных справочного интернет-ресурса, который впоследствии прилагается к материалам уголовного дела и представляется в рапорте начальнику органа дознания.

Следующим шагом, после выявления компании-провайдера, является направление официального запроса в соответствующую организацию. Запрос отправляется в соответствии с частью четвертой статьи 21 УПК РФ, пунктами 1 и 2 части третьей статьи 41 УПК РФ, пунктом 5 статьи 64 Федерального закона «О связи». В запросе дознаватель запрашивает информацию о том, кому в точное время (дата, час, минута, секунда) был предоставлен IP-адрес, указанный в ответе банка, а также о месте нахождения абонента, использующего этот IP-адрес. В дополнение, запрашиваются сведения о дате регистрации договора предоставления услуг связи в сети Интернет, контрагенте (ФИО, дата рождения, место регистрации, паспортные данные), а также данные о логине, пароле, используемом для доступа клиента в Интернет, и MAC-адресе устройства[1], с которого осуществлялся выход в сеть Интернет в момент совершения преступления.

После получения информации от компании-провайдера о месте (адресе) выхода в Интернет и MAC-адресе устройства, следует провести обыск в указанном помещении или, при необходимости, основываясь на судебном решении, провести обыск в жилище.

---

[1] MAC-адрес (англ. Media Access Control - управление доступом к среде, также Hardware Address) - уникальный идентификатор, присваиваемый каждой единице активного оборудования или некоторым их интерфейсам в компьютерных сетях Интернет (Ethernet). При проектировании стандарта Ethernet было предусмотрено, что каждая сетевая карта (равно как и встроенный сетевой интерфейс) должна иметь уникальный шестибайтный номер (MAC-адрес), прошитый в ней при изготовлении. Этот номер используется для идентификации при появлении в сети нового компьютера (или другого устройства, способного работать в сети). Его еще называют «Физический адрес». Именно поэтому определение MAC-адреса устройства для доказывания места совершения преступления (места нахождения преступника, похитившего денежные средства с банковского счета потерпевшего посредством услуги «Онлайн банка» путем выхода в сеть Интернет), имеет одно из приоритетных значений.

В случае, если банк сообщил о том, что перевод денежных средств произошел через «Мобильный банк» и поступило SMS-сообщение с кодом подтверждения, необходимо принять меры для определения лица, на которое зарегистрирован абонентский номер, с которого было отправлено SMS-сообщение.

Для этого следователь, дознаватель должен, в соответствии со статьей 186.1 УПК РФ, с согласия руководителя следственного органа, прокурора, обратиться в суд с ходатайством о получении информации о соединениях между абонентами и (или) абонентскими устройствами, с привязкой к приемопередающим базовым станциям.

Если банк предоставил информацию о движении денежных средств по счету потерпевшего, включая номер счета, место его открытия, и места обналичивания (снятия) средств, дознавателю необходимо оперативно запросить видеозаписи с камер наблюдения банкоматов, поскольку эти записи обычно хранятся не более 60-90 дней.

С целью установления местонахождения лица, осуществившего обналичивание (снятие) похищенных у потерпевшего денежных средств, дознаватель должен в соответствии со статьями 182, 183 и частью первой статьи 165 УПК РФ, при наличии согласия прокурора, подать ходатайство перед судом о проведении выемки информации о вкладах и счетах граждан в банках и иных кредитных организациях.

В постановлении рекомендуется включить следующую информацию:

Ходатайствовать перед судом о проведении выемки (получении) в ПАО «Наименование банка» данных о движении денежных средств по банковской карте № ___, выданной ПАО «Наименование банка» по адресу: ___ (с указанием реквизитов получателя: ___).

Это включает в себя:

- Дату открытия счета (банковской карты), место (отделение) открытия счета (банковской карты), фамилию, имя, отчество лица, на которое открыт счет (банковская карта), а также данные о дате рождения, месте рождения, серии и номере паспорта гражданина Российской Федерации, и месте регистрации.
- Информацию о подключении к банковской карте № ___ услуги «Мобильный банк», включая абонентский номер телефона, к которому привязана данная услуга, а также дату, время и место подключения.
- Сведения о подключении к счету услуги «Онлайн банк», включая IP-адреса с указанием точного времени входа в личный кабинет клиента данного счета («Онлайн банка») с __ часов __ минут __ секунд __ 20__ по текущее время.
- Десять последних IP-адресов с указанием точного времени входа в «Личный кабинет» услуги «Онлайн банк» банковской карты № ___.
- Информацию о движении денежных средств по банковской карте № ___ с указанием мест обналичивания (снятия) денежных средств, включая номера банкоматов и адреса их расположения с __ часов __ минут __ секунд__ 20__ по текущее время. Если прошло менее 90 суток с момента обналичивания (снятия), запросить видеозаписи с камер наблюдения банкоматов.
- Сведения о статусе банковского счета на данный момент (открыт,

действующий, закрыт). Если закрыт, указать дату и причину закрытия счета.

Обыск. При наличии достаточных данных о возможном местонахождении предметов, документов и ценностей, имеющих значение для уголовного дела, рекомендуется провести обыск (в соответствии со статьей 182 УПК РФ). Например, обыск в жилище подозреваемого лица может быть осуществлен судебным решением дознавателя с участием компьютерного специалиста с целью обнаружения и изъятия следующих предметов и документов:

- Компьютерной техники, электронных носителей информации, устройств телекоммуникации (Wi-Fi роутера, модема), средств мобильной связи.
- Договоров об оказании услуг связи в сети Интернет, документов, отражающих факты выдачи денежных средств, удостоверяющих личность, образование и квалификацию подозреваемого.
- Дневников, записных книг, черновых записей, а также литературы, содержащей сведения о хищениях денежных средств с использованием сети Интернет.
- Сведения о вкладах и счетах граждан в банках.

Таким образом, если подозреваемое лицо разместило объявление о продаже товара на определенном интернет-ресурсе, есть вероятность, что товар действительно существовал, и его фотография была сделана в его месте проживания. В связи с этим, при проведении обыска в жилище дознаватель может обнаружить сами предлагаемые к продаже товары, их фотографии, а также определить место, где производилась фотосъемка.

Изъятие электронных носителей информации осуществляется в соответствии с процедурой, установленной статьями 164 и 164.1 УПК РФ.

В соответствии с частью первой статьи 176 УПК РФ, осмотр жилища, других помещений, предметов и документов проводится с целью обнаружения следов преступления и выяснения других обстоятельств, имеющих значение для уголовного дела. Процедура осмотра определена статьей 177 УПК РФ.

Следователь, дознаватель может осмотреть ранее изъятые мобильные устройства как потерпевшего, так и подозреваемого. При проведении такого осмотра целесообразно вовлекать специалиста по компьютерным технологиям и при необходимости использовать технические средства, такие как «UFED», «XRY», «Мобильный криминалист» и другие.

Получение информации о соединениях между абонентами и (или) абонентскими устройствами. Согласно части пятой статьи 186.1 УПК РФ, представленные документы от операторов сотовой связи, содержащие информацию о соединениях между абонентами и (или) абонентскими устройствами, подлежат осмотру при участии специалиста (при необходимости). Протокол осмотра должен включать часть информации, которая, по мнению следователя, дознавателя, имеет отношение к уголовному делу, например, такую как дата, время, продолжительность соединений, номера абонентов и другие данные.

В ходе осмотра информации о соединениях между абонентами и (или) абонентскими устройствами подозреваемого, следователю, дознавателю следует обращать внимание на звонки в банковские учреждения, операторов сотовой

связи, а также на другие стационарные телефоны с аудиозаписью телефонных переговоров. При выявлении таких звонков и наличии соответствующей аудиозаписи, следователь, дознаватель должен выполнить ее изъятие. Для последующей идентификации голоса звонившего с голосом подозреваемого может быть проведена фоноскопическая судебная экспертиза.

Получение информации о соединениях между абонентами и (или) абонентскими устройствами допускается по решению суда, если есть достаточные основания полагать, что эта информация имеет значение для уголовного дела (первая часть статьи 186.1 УПК РФ).

В отличие от статьи 186 УПК РФ, для получения согласия суда на получение информации о соединениях между абонентами и (или) абонентскими устройствами не требуется квалификация деяния как преступления средней тяжести, тяжкого или особо тяжкого.

В постановлении о возбуждении ходатайства перед судом в порядке, предусмотренном статьей 186.1 УПК РФ, следователю, дознавателю следует указать конкретную запрашиваемую информацию.

«Ходатайствовать перед судом о получении информации о соединениях между абонентами и (или) абонентскими устройствами с привязкой к приемопередающим базовым станциям, а именно:

– детализации телефонных переговоров с привязкой к приемопередающим базовым станциям абонентского номера ___ за период с __ часов __ минут до __ часов __ минут __.__.20__ с обязательным указанием номеров приемопередающих базовых станций (CID), местах их расположения (адресе), информации о зоне с неповторяющимися частотами, на которых излучает каждая базовая станция (LAC), азимутах и ширине направленности диаграммы антенны каждой базовой станции;

– получении информации в компании сотовой связи ПАО «Наименование организации», с целью установления данных владельца абонентского номера ___ (по состоянию на __.__.20__, даты заключения с ним договора об оказании услуг, imsi-номере[1] (номерах) данной SIM-карты с абонентским номером ____, IMEI-номере (номерах) телефона, выходящему в эфир с абонентского номера ___ с момента начала оказания услуг связи по настоящий момент, а также по состоянию на __.__.20__, обращался ли с __.__.20__ данный владелец с заявлением об изменении абонентского номера телефона (если да, то предоставить информацию о новом абонентском номере телефона, imsi-номере SIM-карты с новым абонентским номером телефона)».

В зависимости от особенностей совершенного преступления, в постановлении о возбуждении ходатайства перед судом для получения информации о связях между абонентами и (или) их устройствами может быть

[1] Imsi-номер - это индивидуальный номер SIM-карты абонентского номера телефона, в случае утери SIM-карты, при обращении клиента в компанию сотовой связи с заявлением о восстановлении номера телефона, ему выдается новая SIM-карта с иным imsi-номером, но тем же абонентским номером телефона. Установление данного imsi-номера позволяет опровергнуть позицию стороны защиты об утере SIM-карты с абонентским номером (на день совершения преступления) и использовании ее не подзащитным, а иным лицом.

также запрошена и иная сведения.

Допрос подозреваемого. В процессе допроса подозреваемого проводится выяснение общих аспектов, таких как наличие у него персонального компьютера с доступом в Интернет, его компетенция в работе с компьютерной техникой и используемым программным обеспечением, а также информация о его должности, месте работы, образовании и профессиональных навыках. Также выясняются момент возникновения умысла совершения мошенничества в Интернете, а также мотивы и цели.

Последующие этапы допроса направлены на уточнение вопросов, связанных с установлением времени создания и действия интернет-магазина, использованных технических средств и программного обеспечения при его создании. Расследуются характеристики товаров или услуг, предлагаемых на сайте, а также методы и ресурсы для рекламы интернет-магазина и привлечения потенциальных клиентов. Также выясняются способы взаимодействия с потенциальными клиентами, используемые абонентские номера телефонов с указанием их владельцев, адреса электронной почты, способы оплаты товаров и банковские реквизиты, на которые поступала оплата. Расследуются обстоятельства совершения преступления, методы его сокрытия, распоряжение похищенными денежными средствами, отношение к последствиям преступления, и прочие сведения, имеющие значение для расследования уголовного дела.

В случае, если лицо, совершившее преступление, возместило ущерб или иным образом компенсировало причиненный вред, следователь, дознаватель может принять решение о возбуждении ходатайства перед судом об окончании уголовного дела и наложении на данное лицо меры уголовно-правового характера в виде судебного штрафа. Такое ходатайство вместе с материалами уголовного дела направляется в суд.

Судебная экспертиза. Также, в уголовных делах может быть проведена судебная компьютерная экспертиза, при необходимости охватывающая различные объекты, такие как персональные компьютеры, мобильные устройства, носители информации и хранящиеся в них данные.

Судебная компьютерная экспертиза может включать в себя различные объекты, помимо персонального компьютера, такие как мобильные телефоны (включая смартфоны), носители информации (например, флеш-карты, жесткие диски, CD и DVD диски), а также информацию, сохраненную в компьютере, отражающую действия пользователя, включая обработку файлов и передачу данных, и отдельные технические средства и устройства компьютера, включая системы обработки информации в целом.

Эксперту могут быть заданы следующие основные вопросы:

1. Существует ли на носителе информации (жестком магнитном диске системного блока персонального компьютера, представленного для исследования) информация о том, что пользователь занимался работой на персональном компьютере в определенный период времени (указываются дата и время)?

2. Если да, то в какие временные отметки и с использованием каких

программ и файлов, а также периферийного оборудования работал пользователь в указанный период времени?

3. Может ли представленное компьютерное устройство осуществлять доступ в Интернет? Если да, то каким образом осуществляется доступ?

4. Есть ли информация о деятельности пользователей представленного компьютерного устройства в Интернете? Каково содержание настроек удаленного доступа и протоколов соединения?

5. Присутствует ли на носителе информации (жестком магнитном диске системного блока персонального компьютера или в памяти мобильного телефона, представленных для исследования) информация об осуществлении сеансов доступа в Интернет за период с ... по ..., включая использование учетных данных ...? Если да, то какие учетные данные использовались для входа в Интернет? Где содержатся сведения о использованных логинах и паролях?

6. Присутствуют ли на носителе информации (жестком магнитном диске системного блока персонального компьютера или в памяти мобильного телефона) логотипы файлов web-сервера, относящихся к обращениям к сайту интернет-магазина «...», и каково содержание этих файлов?

7. Какие MAC-адреса принадлежат сетевому оборудованию представленных для экспертизы объектов?

При назначении судебной компьютерной экспертизы в рамках конкретного уголовного дела могут быть сформулированы дополнительные вопросы, направленные на выявление фактов и обстоятельств, обладающих доказательственной значимостью.

Для совершения обналичивания похищенных у потерпевшего денежных средств, которое может осуществляться с использованием банкоматов, находящихся под видеонаблюдением, назначается портретная судебная экспертиза с целью идентификации личности. В данной экспертизе анализируются фотографические снимки и кадры видеозаписи.

При назначении портретной судебной экспертизы эксперту могут быть предложены следующие вопросы:

1. Могут ли представленные фотографические снимки (кадры видеозаписи) быть использованы для сравнительного идентификационного анализа?
2. Изображены ли на видеозаписи и фотографическом снимке одни и те же лица?
3. Присутствует ли на представленном фотографическом снимке (кадре видеозаписи) изображение конкретной личности?

Если в процессе предварительного расследования обнаруживаются звонки подозреваемого в банковские учреждения, к операторам сотовых компаний и на стационарные телефоны, проводится изъятие аудиозаписей этих разговоров с последующим проведением фоноскопической судебной экспертизы для идентификации голоса звонившего.

При назначении фоноскопической судебной экспертизы эксперту могут быть предложены следующие вопросы:

1. Подходит ли запись (указывается местонахождение на

носителе, описывается тип носителя) для идентификации голоса и речи?

2. Принадлежат ли голос и речь лица (указываются фамилия и инициалы), чьи образцы представлены на диске (описывается тип носителя записи)? Если да, какие реплики, слова или фразы были произнесены?

3. Каково содержание разговора, записанного на носителе (указывается тип носителя и описывается местонахождение записи; указываются границы записи)?

Таким образом в текущем разделе работы предложены тактические рекомендации по организации и производству следственных и иных процессуальных действий с учетом особенностей механизма совершения преступлений с использованием торговых площадок (сервисов) сети Интернет. Рассмотрены особенности получения объяснения у заявителя и иных лиц; осмотра места происшествия; осмотра предметов и документов; подготовки и направления письменных поручений; допроса потерпевшего; допроса свидетелей; допроса сотрудников банков (кредитных и других организаций); подготовки и направления запросов (к оператору сотовой связи; к организации, обслуживающей интернет-ресурс); выемки; обыска; получения сведений о соединениях между абонентами и (или) абонентскими устройствами; допроса подозреваемого; назначения судебных экспертиз.

ЗАКЛЮЧЕНИЕ

Электронной торговой площадкой является любой Интернет-ресурс, посредством которого заключаются сделки купли-продажи между покупателями и продавцами (размещение государственного заказа; размещение заказов о закупках товаров, работ, услуг отдельными видами юридических лиц; электронные торговые площадки по реализации имущества должников (банкротов); электронные торговые площадки для коммерческих заказчиков и физических лиц (интернет-магазины, маркетплейсы и т.п.).

Наиболее распространенными способами совершения преступлений являются: предложение о продаже товара по цене значительно ниже среднерыночной, фейковые (ложные) интернет-магазины, имитация розыгрыша ценных подарков, продажа дефектных или иных неликвидных товаров, фиктивное предложение удаленной работы.

На основе изучения криминалистических, уголовно-правовых и уголовно-процессуальных основ квалификации, раскрытия и расследования преступлений совершаемых с использованием электронных торговых площадок (сервисов) выявлены особенности и типовые проблемы, возникающие в процессе уголовного судопроизводства по данной категории преступлений.

Расследование и раскрытие преступлений о дистанционных хищениях зачастую носят межрегиональный характер и нуждаются в выработке единого алгоритма действий как на этапе проверки заявления и сообщения о преступлении, так и на первоначальном этапе расследования.

Вместе с тем до настоящего времени не сформирован действенный инструментарий быстрого получения от кредитных организаций, интернет-провайдеров, операторов связи, социальных сетей и интернет-сервисов информации, имеющей доказательственное значение по расследуемым преступлениям (сведений о лице, биллинге, движении денежных средств по лицевым счетам абонентских номеров и др.).

В работе рассмотрены особенности механизма преступной деятельности с использованием электронных торговых площадок (ресурсов), алгоритм проверки сообщений о преступлении и планирование расследования на первоначальном этапе, а также особенности производства отдельных следственных и иных процессуальных действий при расследовании указанной категории преступлений.

Предложенные в работе методические рекомендации обеспечивают реализацию обоснованных и эффективных приемов планирования расследования, производства процессуальных действий, точную и единообразную фиксацию их хода и результатов в процессуальных документах. Формирование понятных и доступных в реализации алгоритмов действий способствует более эффективной организации расследования. Это оказывает положительное влияние на скорость расследования и его качество.

Материалы методических рекомендаций могут использоваться сотрудниками органов предварительного расследования МВД России в процессе раскрытия и расследования преступлений, совершаемых с использованием

электронных торговых площадок (сервисов), в служебной подготовке сотрудников указанных категорий, а также в обучении курсантов и слушателей образовательных организаций МВД России, изучающих дисциплины «Предварительное следствие в ОВД», «Расследование преступлений в сфере компьютерной информации», «Расследование отдельных видов преступлений, совершенных с использованием информационно-телекоммуникационных технологий».