Министерство внутренних дел Российской Федерации
Барнаульский юридический институт МВД России

Расследование хищений, совершенных с использованием информационно-телекоммуникационных технологий

Учебное пособие

Барнаул
2023

УДК 343.7:004(075.8)
ББК 67.408.121.9с51я73
Р 244

Авторы:
канд. юрид. наук, доцент Н.А. Архипова (§ 2.4, 2.5, 3.1, 3.2),
канд. юрид. наук, доцент О.В. Кругликова (введение, заключение),
канд. юрид. наук, доцент А.В. Шебалин (§ 1.1, 2.1, 2.2),
канд. юрид. наук М.О. Янгаева (§ 1.2, 1.3, 2.3, 3.3)

Рецензенты:
начальник отдела организации дознания ГУ МВД России
по Алтайскому краю *В.В. Говорухин*;
доцент кафедры уголовного процесса Санкт-Петербургского
университета МВД России канд. юрид. наук, доцент *Н.В. Шепель*.

Р 244 **Расследование** хищений, совершенных с использованием информационно-телекоммуникационных технологий : учебное пособие / Н.А. Архипова, О.В. Кругликова, А.В. Шебалин [и др.]. – Барнаул : Барнаульский юридический институт МВД России, 2023. – 91 с.

ISBN 978-5-94552-562-7

В учебном пособии проведено исследование проблемных вопросов расследования хищений, совершенных с использованием информационно-телекоммуникационных технологий. На основе изучения судебно-следственной практики сформулированы криминалистические рекомендации, направленные на совершенствование расследования данной группы преступлений.

Пособие предназначено для курсантов и слушателей образовательных организаций МВД России, может быть использовано в служебной деятельности сотрудниками правоохранительных органов. Оно также может представлять интерес для научных и практических работников, преподавателей и адъюнктов.

УДК 343.7:004(075.8)
ББК 67.408.121.9с51я73

ISBN 978-5-94552-562-7

Введение

В современном обществе быстро развивается цифровизация, в т.ч. за счет применения технологий искусственного интеллекта, биометрической идентификации, работы с большими данными, облачного хранения информации и дистанционного банковского обслуживания. Данные технологии стали неотъемлемой частью повседневной жизни человека. Граждане активно открывают банковские счета, оформляют пластиковые карты и используют интернет-банкинг для оплаты покупок в интернете.

Активное развитие информационных технологий и их широкое применение, растущий интерес населения к информационным системам и в то же время отсутствие навыков, необходимых для безопасной работы с ними, привели к возникновению объективных предпосылок для стремительного роста преступлений в данной сфере. Сегодня совершается большое количество преступлений с использованием средств мобильной связи, сети Интернет, широкого спектра возможностей информационной и коммуникационной инфраструктуры. С развитием высоких технологий неизбежно меняются механизмы совершения преступлений, личность преступника и характер взаимоотношений между жертвой и преступником.

Хищения в сфере информационно-телекоммуникационных технологий разнообразны, прежде всего к ним относятся преступления, предусмотренные ст. 158, 159-159.3, 159.5, 159.6 УК РФ. Анализ состояния преступности в Российской Федерации за январь – сентябрь 2023 г. позволил сделать вывод, что с использованием информационно-телекоммуникационных технологий совершается каждое третье преступление. В этой сфере зарегистрировано на 29,2% преступлений больше, чем в январе – сентябре 2022 г.[1]

Выявить и раскрыть хищения, совершаемые с использованием информационно-телекоммуникационных технологий, сегодня крайне сложно, поскольку преступники имеют хорошее техническое оснащение, объединяются в преступные сообще-

[1] Краткая характеристика состояния преступности в Российской Федерации за январь – сентябрь 2023 г. URL: https://xn--b1aew.xn--p1ai/reports/item/42989123/

ства, которые порой взаимодействуют на международном уровне. Поэтому данный вид преступной деятельности представляет собой мировую проблему, отличается высокой степенью латентности и сложностью в организации расследования, в связи с чем необходимо его детальное и всестороннее изучение. Вместе тем, как показывает следственная практика, многие уголовные дела расследуются на низком профессиональном уровне, не обеспечивается полнота расследования, имеет место некачественное проведение следственных действий.

Поэтому перед авторами работы стояла цель – разработать и предложить комплекс тактико-криминалистических рекомендаций, направленных на повышение эффективности раскрытия, расследования и предупреждения хищений, совершенных с использованием информационно-телекоммуникационных технологий.

В данном учебном пособии предпринята попытка комплексного рассмотрения организационно-правовых вопросов расследования преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. При этом особое внимание уделено порядку проведения проверки сообщений о преступлении, алгоритму действий следователя на первоначальном и последующем этапах, а также тактике производства отдельных следственных и иных процессуальных действий. Также в работе рассмотрены особенности организации взаимодействия органов предварительного расследования с сотрудниками других ведомств и подразделений.

В учебном пособии проанализирован имеющийся опыт расследования уголовных дел о преступлениях, совершаемых с использованием информационно-телекоммуникационных технологий; рассмотрены проблемные вопросы проведения предварительного расследования.

Издание предназначено для использования в образовательном процессе курсантов и слушателей образовательных организаций Министерства внутренних дел Российской Федерации, обучающихся по специальности 40.05.01 Правовое обеспечение национальной безопасности, 40.05.02 Правоохранительная деятельность, по направлению подготовки 40.03.01 Юриспруденция (уровень бакалавриата), по направлению подготовки 40.03.02 Обеспечение законности и правопорядка и может быть рекомендовано для изучения в рамках прохождения обучения по

дополнительным профессиональным программам повышения квалификации, в частности, старших следователей (следователей), старших дознавателей (дознавателей), оперативных сотрудников и сотрудников экспертно-криминалистических подразделений территориальных органов МВД России, осуществляющих функции по противодействию преступлениям, совершенным с использованием современных информационно-коммуникационных технологий, с целью закрепления теоретических и практических навыков организации расследования преступлений данной категории. Пособие дополняет учебный материал дисциплин «Расследование преступлений в сфере экономической деятельности», «Расследование преступлений против личности и собственности», «Криминалистика» по темам, связанным с особенностями расследования преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. Оно также может представлять интерес для научных работников, преподавателей и адъюнктов.

Учебное пособие направлено на дальнейшее развитие таких компетенций, как:

- умение применять теоретические знания и практические навыки в области расследования хищений, совершенных с использованием информационно-телекоммуникационных технологий;
- способность анализировать и оценивать полученные доказательства, формулировать выводы и предложения по результатам расследования;
- владение методами и средствами криминалистической техники, используемыми в процессе расследования хищений, совершенных с использованием информационно-телекоммуникационных технологий;
- умение использовать современные информационные технологии и базы данных для сбора и анализа информации, необходимой для расследования указанной категории преступлений;
- владение навыками работы с криминалистическим оборудованием и инструментами, необходимыми для проведения следственных действий;
- умение взаимодействовать с другими специалистами и сотрудниками правоохранительных органов в процессе расследования преступлений, а также при назначении и производстве судебных экспертиз.

Глава 1. Организационно-правовые основы расследования хищений, совершенных с использованием информационно-телекоммуникационных технологий

1.1. Правовые основы расследования хищений, совершенных с использованием информационно-телекоммуникационных технологий

Федеральный закон от 23 апреля 2018 г. № 111-ФЗ ввел в Уголовный кодекс РФ новые статьи, а также усовершенствовал некоторые положения уже действующих уголовно-правовых норм, изложив наименования рассматриваемой нами группы деяний следующим образом: п. «г» ч. 3 ст. 158 УК РФ – кража, совершенная с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного ст. 159.3 УК РФ); ст. 159.3 УК РФ – мошенничество с использованием электронных средств платежа, п. «в» ч. 3 ст. 159.6 УК РФ – мошенничество в сфере компьютерной информации, совершенное с банковского счета, а равно в отношении электронных денежных средств[1]. Вместе с тем противоречивость судебно-следственной практики по рассматриваемым преступлениям, неоднозначный характер некоторых положений законодательства, регулирующего электронный денежный оборот, дискуссионность целого ряда правовых норм, регламентирующих процедуры выявления и расследования указанных деяний, не способствуют успешной правоприменительной практике их расследования.

Для оптимизации борьбы с кражами с банковского счета, а равно совершенных в отношении электронных денежных средств, мошенничествами с использованием информационно-телекоммуникационных технологий следователю необходимо

[1] О внесении изменений в Уголовный кодекс Российской Федерации [Электронный ресурс]: федеральный закон от 23 апреля 2018 г. № 111-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

знать особенности правовой регламентации расследования подобных преступлений.

Нормативное регулирование процесса расследования краж с банковского счета, а равно совершенных в отношении электронных денежных средств, мошенничеств с использованием информационно-телекоммуникационных технологий имеет свою специфику, определяемую способом преступления. В связи с этим необходимо указать на многочисленные нормативные правовые акты, регулирующие деятельность в этой сфере, а также судебную практику.

В Уголовном кодексе Российской Федерации от 13 июня 1996 г. № 63-ФЗ в связи с этим необходимо обратить внимание на следующие статьи: п. «г» ч. 3 ст. 158 – кража с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного ст. 159.3 УК РФ); ст. 159 – мошенничество; ст. 159.3 – мошенничество с использованием электронных средств платежа; ст. 159.6 – мошенничество в сфере компьютерной информации.

В связи с тем, что рассматриваемые преступления могут совершаться путем кражи, необходимо в ходе расследования руководствоваться положениями постановления Пленума Верховного Суда РФ от 27 декабря 2002 г. № 29 «О судебной практике по делам о краже, грабеже и разбое»[1].

Особое внимание стоит уделить содержанию постановления Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» (пунктам 17, 20, 21)[2], а также определению Судебной коллегии по уголовным делам Верховного Суда РФ от 29 сентября 2020 г. № 12-УДП20-5-К6, в котором рассматриваются особенности квалификации краж с банковского счета, а равно

[1] О судебной практике по делам о краже, грабеже и разбое [Электронный ресурс]: постановление Пленума Верховного Суда РФ 27 декабря 2002 г. № 29. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] О судебной практике по делам о мошенничестве, присвоении и растрате [Электронный ресурс]: постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48. Доступ из справ.-правовой системы «КонсультантПлюс».

совершенных в отношении электронных денежных средств, мошенничеств с использованием информационно-телекоммуникационных технологий[1].

Также непосредственно к рассматриваемой теме относятся положения ст. 152 Уголовно-процессуального кодекса Российской Федерации, где регламентируются правила определения места производства предварительного расследования. Кроме того, в приказе МВД России от 3 апреля 2018 г. № 196 «О некоторых мерах по совершенствованию организации раскрытия и расследования отдельных видов хищений» говорится, что в порядке статьи 144 УПК РФ проведение проверки сообщения о преступлениях, предусмотренных ст. 158, 159, 159.3, 159.6 УК РФ, совершенных с использованием платежных карт, средств мобильной связи и информационно-телекоммуникационной сети Интернет, следует незамедлительно принимать исчерпывающие меры к раскрытию преступлений и установлению лиц, их совершивших, направлять в установленном порядке запросы в кредитные организации, организации, оказывающие услуги связи, в т.ч. по передаче данных и предоставлению доступа к информационно-телекоммуникационной сети Интернет, получать объяснения от заявителя и возможных очевидцев преступления. При наличии достаточных данных, указывающих на признаки преступлений, указанных в подп. 1.1 ведомственного приказа[2], принимается решение о возбуждении уголовного дела в органе внутренних дел Российской Федерации, в который поступило сообщение о преступлении. только после получения достаточных доказательств о совершении преступления на территории обслуживания другого территориального органа МВД России и выполнения всех возможных процессуальных действий по месту возбуждения уголовного дела уголовное дело направляют в порядке, предусмотренном ст. 152 УПК РФ.

---

[1] Определение Судебной коллегии по уголовным делам Верховного Суда РФ от 29 сентября 2020 г. № 12-УДП20-5-К6 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] О некоторых мерах по совершенствованию организации раскрытия и расследования отдельных видов хищений [Электронный ресурс]: приказ МВД России от 3 апреля 2018 г. № 196. Доступ из справ.-правовой системы «КонсультантПлюс».

Понятия «кредитная организация», «банк», «небанковская кредитная организация» содержатся в Федеральном законе от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности»[1]. К кредитным организациям, в соответствии с этим законом, относятся также и небанковские кредитные организации. И многие российские операторы по переводу электронных денежных средств (т.е. компании, оказывающие услуги по управлению электронными деньгами посредством электронных кошельков) являются именно небанковскими кредитными организациями. Так им проще вести бизнес, находясь при этом полностью в рамках закона: небанковские кредитные организации имеют право выполнять только отдельные виды финансовых операций, поэтому требования регулятора к ним не такие строгие, как к классическим банкам.

В Федеральном законе от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе» говорится об операторе по переводу денежных средств, операторе электронных денежных средств, электронных денежных средствах, электронном средстве платежа, банкомате[2]. В роли оператора электронных денежных средств в равной степени могут выступать банковские и небанковские кредитные организации. Электронное средство платежа – это средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в т.ч. платежных карт, а также иных технических устройств. К ним можно отнести электронный кошелек, онлайн-банкинг, банковскую пластиковую карту, банкомат. Не являются электронными средствами платежа такие вещи, которые хотя и используются для передачи распоряжений о переводе денеж-

[1] О банках и банковской деятельности [Электронный ресурс]: федеральный закон от 2 декабря 1990 г. № 395-1. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] О национальной платежной системе [Электронный ресурс]: федеральный закон от 27 июня 2011 г. № 161-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

ных средств, но созданы не специально для этого (например, компьютер, сотовый телефон и др.).

Вышеизложенное позволяет предложить следующее определение электронного средства платежа – это компьютерные программы и их совокупность, а также специальные технические устройства, в т.ч. электронные носители информации, предназначенные для дистанционной выдачи распоряжений о переводе денежных средств, зачисления на счет и выдачи наличных денежных средств.

Электронный кошелек как электронное средство платежа позволяет лицу, предоставившему денежные средства, составлять, удостоверять и передавать распоряжения относительно их перевода третьим лицам для исполнения перед ними денежного обязательства. Электронный кошелек может быть в форме либо пластиковой карты, либо специального приложения на мобильном устройстве (или компьютере), которое позволяет хранить и использовать деньги в электронной системе. Функциональные возможности электронных кошельков позволяют использовать их не только для оплаты товаров и услуг в онлайн-пространстве, но и для совершения иных расчетных операций.

В Федеральном законе от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе» дается определение электронным денежным средствам. Под ними понимаются денежные средства, которые предварительно предоставлены одним лицом (лицом, предоставившим денежные средства) другому лицу, учитывающему информацию о размере предоставленных денежных средств без открытия банковского счета (обязанному лицу), для исполнения денежных обязательств лица, предоставившего денежные средства, перед третьими лицами, и в отношении которых лицо, предоставившее денежные средства, имеет право передавать распоряжения исключительно с использованием электронных средств платежа. При этом не являются электронными денежными средствами денежные средства, полученные организациями, осуществляющими профессиональную деятельность на рынке ценных бумаг, клиринговую деятельность, деятельность оператора финансовой платформы, деятельность по организации привлечения инвестиций, деятельность по управлению инвестиционными фондами, пае-

выми инвестиционными фондами и негосударственными пенсионными фондами, деятельность операторов информационных систем, в которых осуществляется выпуск цифровых финансовых активов, и (или) деятельность операторов обмена цифровых финансовых активов и осуществляющими учет информации о размере предоставленных денежных средств без открытия банковского счета в соответствии с законодательством, регулирующим деятельность указанных организаций.

Говоря об электронных денежных средствах, нельзя не упомянуть нормативные правовые акты, которые закрепляют понятие «безналичные денежные средства». Гражданский кодекс Российской Федерации не объясняет, что такое электронные денежные средства, а лишь закрепляет, что к объектам гражданских прав относятся имущественные права, включая безналичные денежные средства[1]. В то же время Конституционный Суд РФ в своем определении указывает, что «…по своей природе безналичные денежные средства, существующие в виде записи на банковском счете кредитора (их обладателя), представляют собой его обязательственное требование на определенную сумму к кредитной организации, в которой открыт данный счет»[2].

В Федеральном законе от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – Закон об информации) содержатся определения таких понятий, как «информация», «коммуникация» и «информационные технологии»[3]. При этом под информацией следует понимать сведения (сообщения, данные) независимо от формы их представления (п. 1 ст. 2 Закона об информации), под коммуникацией – операционные системы, повседневно обеспе-

[1] Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] По делу о проверке конституционности частей шестой и седьмой статьи 115 Уголовно-процессуального кодекса Российской Федерации в связи с жалобой закрытого акционерного общества «Глория»: постановление Конституционного Суда РФ от 10.12.2014 № 31-П // Вестник Конституционного Суда РФ. 2015. № 2.

[3] Об информации, информационных технологиях и о защите информации [Электронный ресурс]: федеральный закон от 27 июля 2006 г. № 149-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

чивающие единство и преемственность человеческой деятельности, под информационными технологиями – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов (п. 2 ст. 2 Закона об информации).

Федеральный закон «О связи» от 7 июля 2003 г. № 126-ФЗ нормативно определяет следующие, часто встречающиеся при составлении процессуальных документов по рассматриваемым преступлениям, термины:

- *абонент* – пользователь услугами связи, с которым заключен договор об оказании таких услуг при выделении для этих целей абонентского номера или уникального кода идентификации;

- *база данных перенесенных абонентских номеров* – информационная система, содержащая сведения об абонентских номерах, которые сохраняются абонентами при заключении новых договоров об оказании услуг связи с другими операторами подвижной радиотелефонной связи, и об указанных операторах связи, заключивших такие договоры;

- *идентификационный модуль* – электронный носитель информации, который устанавливается в пользовательском оборудовании (оконечном оборудовании) и с помощью которого осуществляется идентификация абонента, и (или) пользователя услугами связи абонента – юридического лица либо индивидуального предпринимателя, и (или) пользовательского оборудования (оконечного оборудования) и обеспечивает доступ оборудования указанных абонента или пользователя к сети оператора подвижной радиотелефонной связи;

- *оператор связи* – юридическое лицо или индивидуальный предприниматель, оказывающие услуги связи на основании соответствующей лицензии;

- *сеть связи* – технологическая система, включающая в себя средства и линии связи и предназначенная для электросвязи или почтовой связи[1].

Постановление Правительства РФ от 9 декабря 2014 г. № 1342 «О порядке оказания услуг телефонной связи» (вместе

[1] О связи [Электронный ресурс]: федеральный закон от 7 июля 2003 г. № 126-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

с «Правилами оказания услуг телефонной связи») дает легальное определение термина «абонентский номер», под которым понимается телефонный номер, однозначно определяющий (идентифицирующий) оконечный элемент сети связи или подключенную к сети подвижной связи абонентскую станцию (абонентское устройство) с установленным в ней (в нем) идентификационным модулем[1].

В приказе Министерства информационных технологий и связи РФ от 2 июля 2007 г. № 73 «Об утверждении правил применения автоматизированных систем расчетов» даются определения сим-карты, автоматизированной системы расчетов[2].

Необходимо отметить, что большое количество хищений, совершенных с использованием информационно-телекоммуникационных технологий, привело к изданию нормативных правовых актов, регулирующих отношения в области организации работы по расследованию рассматриваемых преступлений. Это некоторые положения приказа МВД России от 3 апреля 2018 г. № 196 «О некоторых мерах по совершенствованию организации раскрытия и расследования отдельных видов хищений». В системе Следственного комитета РФ действует приказ от 30 января 2023 г. № 19 «Об организации работы по расследованию преступлений, совершенных с использованием информационно-телекоммуникационных технологий», который достаточно подробно регламентирует не только процедуру производства предварительного расследования по названным преступлениям, но и предусматривает организацию на постоянной основе мероприятий по повышению квалификации следователей и получению ими навыков применения знаний при расследовании преступлений, совершенных с использованием информационно-телекоммуникационных технологий, а также проведение систе-

[1] О порядке оказания услуг телефонной связи [Электронный ресурс]: постановление Правительства РФ от 9 декабря 2014 г. № 1342. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Об утверждении правил применения автоматизированных систем расчетов [Электронный ресурс]: приказ Министерства информационных технологий и связи Российской Федерации от 2 июля 2007 г. № 73. Доступ из справ.-правовой системы «КонсультантПлюс».

матических теоретических и практических занятий по тактике и методике расследования преступлений данного вида.

Федеральный закон от 20 октября 2022 г. № 408-ФЗ «О внесении изменений в статью 26 Федерального закона “О банках и банковской деятельности” и статью 27 Федерального закона “О национальной платежной системе”» и Федеральный закон от 24 июля 2023 г. № 369-ФЗ «О внесении изменений в Федеральный закон “О национальной платежной системе”» определили новые правила обеспечения защиты информации в платежной системе и особенности взаимодействия Банка России и МВД России, указав, что «Банк России предоставляет федеральному органу исполнительной власти в сфере внутренних дел информацию, содержащуюся в базе данных, о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента, на основании полученных от указанного федерального органа исполнительной власти сведений о совершенных противоправных действиях. Порядок информационного обмена, форма и перечень предоставляемых сторонами сведений закрепляются в соглашении, заключаемом между Банком России и федеральным органом исполнительной власти в сфере внутренних дел». Данные правила вступят в силу с 25 июля 2024 г.

Таким образом, можно сделать вывод о том, что нормативно-правовое регулирование расследования краж с банковского счета, а равно совершенных в отношении электронных денежных средств, мошенничеств с использованием информационно-телекоммуникационных технологий, имеет свою специфику, определяемую способом преступления.

1.2. Современные способы совершения хищений с использованием информационно-телекоммуникационных технологий

В криминалистике под способом совершения преступления целесообразно понимать объективно и субъективно обусловленную систему поведения субъекта до, в момент и после совершения преступления, оставляющую различного рода характерные следы, позволяющие с помощью криминалистических приемов и средств получить представление о сути произошедшего, своеобразии преступного поведения правонарушителя, его отдельных личностных данных и, соответственно, определить наиболее оптимальные методы решения задач расследования преступления[1].

Г.Г. Зуйков под способом совершения преступления подразумевает «систему действий по подготовке, совершению и сокрытию преступления, детерминированных условиями внешней среды и психофизиологическими свойствами личности, могущих быть связанными с избирательным использованием соответствующих орудий, средств и условий места и времени и объединенных общим преступным замыслом»[2]. Думается, что данное определение верно для тех случаев, когда все действия (подготовка, совершение и сокрытие преступления) связаны между собой в единую систему и происходят по единому замыслу. Однако так бывает не всегда, т.к. такие элементы способа совершения преступления, как подготовка или сокрытие, вообще могут отсутствовать.

Итак, выделим несколько типичных способов хищений, совершенных с использованием информационно-телекоммуникационных технологий.

---

[1] Мохоров Д.А. Понятие способа совершения преступления // Юридическая мысль. 2006. № 5 (36). С. 76.

[2] Зуйков Г.Г. Криминалистическое учение о способе совершения преступления: автореф. дис. … д-ра юрид. наук. М., 1970. С. 10.

Способ 1. Хищение безналичных или электронных денежных средств, совершаемое при непосредственном контакте со смартфоном потерпевшего или его банковской картой.

Данный способ может характеризоваться подготовкой к совершению преступления, выбором времени и места совершения преступления (когда смартфон или банковская карта потерпевшего останется без присмотра), планом, куда будут переводиться безналичные или электронные денежные средства и как обналичиваться.

Далее происходит непосредственное совершение преступных деяний, например, с помощью смартфона или банковской карты потерпевшего похищаются безналичные или электронные денежные средства.

Преступник пытается скрыть следы преступного деяния путем перевода безналичных или электронных денежных средств на электронные кошельки, зарегистрированные на подставных людей, или банковские карты, зарегистрированные на дропперов[1], использует VPN[2] при преступной деятельности в сети Интернет и т.д.

*22 сентября 2018 г. около 03:00 Л. находился по адресу *** у С., где решил совершить тайное хищение электронных де-*

[1] Дроппер – это человек, которого используют преступники для достижения своих целей. Он не является инициатором преступления, а выполняет указания, получая за это деньги. Дропперы участвуют во всех схемах по незаконному обналичиванию чужих денег. Схема довольно проста: дроппер предоставляет данные своей банковской карты, на которую переводят средства, добытые преступным способом. Затем он обналичивает сумму в банкомате, передает другим лицам и получает определенный процент со сделки. URL: https://journal.sovcombank.ru/umnii-potrebitel/kto-takie-dropperi-i-chto-znachit-oformit-na-dropa.

[2] VPN, или виртуальная частная сеть, создает частное сетевое подключение между устройствами с помощью сети Интернет. Сети VPN используются для безопасной и анонимной передачи данных по публичным сетям. Принцип их работы заключается в маскировании IP-адресов пользователей и шифровании данных, в результате чего пользователи, не имеющие разрешения на получение таких данных, не смогут их прочесть. URL: https://aws.amazon.com/ru/what-is/vpn/

*нежных средств с электронного средства платежа № *** платежного сервиса «Яндекс.Деньги», принадлежащего С. Для реализации своего преступного умысла Л. через социальную сеть *** попросил разрешения М. воспользоваться банковской картой ПАО «Сбербанк», имеющей лицевой счет № ***, принадлежащий последнему, для осуществления перевода денежных средств с электронного платежного сервиса «Яндекс.Деньги», принадлежащих С., чтобы потом обналичить их, о чем М. не был поставлен в известность. Л., находясь в комнате, воспользовавшись тем, что С. уснул, достоверно зная, что к смартфону, принадлежащему С., подключено приложение «Яндекс.Деньги», а также пароль от него, взял указанный смартфон и покинул комнату. Затем Л. проследовал к зданию ФГУП «Почта России», где встретился с М., и тот сообщил ему номер своей банковской карты для перевода*[1].

Способ 2. Хищение безналичных или электронных денежных средств, совершаемое с использованием вредоносного программного обеспечения или с помощью программ удаленного доступа.

Данный способ может характеризоваться подготовкой к совершению преступления, а именно формированием умысла, приисканием орудий, средств совершения преступления. Это может выражаться в самостоятельном создании преступником вредоносного программного обеспечения или его приобретении у иных лиц, рассылке фишинговых писем, в которых скрывается вредоносное программное обеспечение, приискании сообщников, а также лиц для обналичивания похищенных электронных денежных средств, а также подготовке приемов социальной инженерии для убеждения потерпевшего установить на свое устройство программу удаленного доступа.

Далее происходит непосредственное совершение преступных деяний, например, при помощи вредоносного программного обеспечения похищаются логины и пароли от личных кабинетов финансово-кредитных организаций и используются пре-

[1] Приговор Собинского городского суда Владимирской области № 1-1-25/2020 1-1-252/2019 от 28.01.2020 по делу № 1-1-25/2020. URL: https://sudact.ru.

ступниками с целью перевода денежных средств со счета потерпевшего на заранее подготовленный счет, взлом электронных кошельков, мобильных приложений банков, расположенных на устройствах потерпевшего путем установки программы удаленного доступа потерпевшим, и т.д.

Преступник пытается скрыть следы преступного деяния путем вывода безналичных или электронных денежных средств малыми суммами на несколько электронных кошельков, зарегистрированных на подставных людей, или банковские карты, зарегистрированные на дропперов, использует VPN при преступной деятельности в сети Интернет и т.д.

Так, Д., имея умысел на хищение электронных денежных средств с электронных средств платежа граждан, оплачивал доступ к интернет-ресурсам, где размещались учетные данные, неустановленному лицу, который осуществлял создание, использование и распространение вредоносного программного обеспечения, предназначенного для несанкционированного копирования компьютерной информации и нейтрализации средств ее защиты с электронных устройств граждан. Д. также установил на свой компьютер специальное программное обеспечение, позволяющее подключиться по протоколу безопасности RDP. Кроме того, Д. подыскал неустановленных лиц, готовых за денежное вознаграждение принимать на банковские счета похищаемые Д. электронные денежные средства и обналичивать их в банкоматах.

Если говорить о программах удаленного доступа, то они могут быть не вредоносными, поэтому часто на персональных компьютерах, ноутбуках потерпевших эксперт, производящий экспертизу, не обнаруживает следы (коды) вредоносного программного обеспечения, однако находятся следы использования программы, например AnyDesk, предназначенной для удаленного управления устройством.

Способ 3. Хищение безналичных или электронных денежных средств, совершаемое с использованием приемов социальной инженерии.

Данный способ может характеризоваться подготовкой к совершению преступления, а именно формированием умысла, приисканием средств совершения преступления, это может вы-

ражаться в создании «зеркальных» сайтов, размещении на торговых площадках фейковых объявлений о продаже товаров, поиске и приобретении баз персональных данных, утекших в сеть Интернет, или вербовке лиц, которые работают с персональными данными и согласны продавать персональные данные граждан, а также используют приемы OSINT.

Далее происходит непосредственное совершение преступных деяний. Данный способ отличается от вышеописанных, т.к. у преступников происходит контакт с потенциальным потерпевшим (чаще по телефону), цель преступника – используя психологические методы, в т.ч. нейролингвистического программирования, убедить потерпевшего в необходимости перевести денежные средства на счет преступника или сообщить конфиденциальную информацию о своей банковской карте и т.д.

Преступник пытается скрыть следы преступного деяния путем вывода безналичных или электронных денежных средств малыми суммами на несколько электронных кошельков, зарегистрированных на подставных людей, или банковские карты, зарегистрированные на дропперов, использует VPN в преступной деятельности в сети Интернет, SIP- или IP-телефонию, боты для рассылки писем и т.д.

Так, часто преступники распространяют в сети Интернет и среди абонентов сотовой связи ложные сведения относительно возможности наступления негативных последствий как для получателя сообщения, так и для его близких, активно воздействуя на эмоции абонентов. Преступники предлагают перечислить денежные средства на указанный счет, например, за решение вопроса о непривлечении к уголовной ответственности, на лечение тяжелой болезни, «снятие сглаза» и пр. Данные действия также могут быть сопряжены с неправомерным использованием учетной записи лица, для нужд которого якобы и требуются денежные средства.

Следующая разновидность указанного способа – это размещение на электронных торговых площадках (таких как «Авито», «Юла», «Из рук в руки» и пр.) заведомо ложных объявлений о продаже товаров либо предоставлении услуг с условием обязательной предоплаты.

После чего обманутые потерпевшие перечисляют сумму первоначального взноса на указанные реквизиты банковских карт, как правило, оформленных на подставных лиц.

Таким образом, изучение судебно-следственной практики позволило выявить способы совершения преступлений, которые объединены в три группы по схожему механизму совершения хищений: хищение безналичных или электронных денежных средств, совершаемое при непосредственном контакте со смартфоном потерпевшего или его банковской картой; хищение безналичных или электронных денежных средств, совершаемое с использованием вредоносного программного обеспечения или с помощью программ удаленного доступа; хищение безналичных или электронных денежных средств, совершаемое с использованием приемов социальной инженерии. Своевременное определение способа совершения хищений безналичных или электронных денежных средств поможет определению направления поисково-познавательной деятельности следователя, формулированию общих и частных версий, организационных, тактических и управленческих задач, выбору оптимальных методов и средств их решения.

1.3. Получение информации о личности преступника, совершающего хищения с использованием информационно-телекоммуникационных технологий, путем мониторинга интернет-ресурсов

В последние годы наблюдается значительное увеличение количества преступлений, совершенных в сфере информационных технологий, по причине их интеграции в повседневную и деловую жизнь граждан.

Количество пользователей социальных сетей, а также устройств Интернета вещей (IoT) с каждым годом становится все больше, это приводит к увеличению объема цифровых данных.

При раскрытии и расследовании преступлений необходимо оперативно получать данные для их своевременного анализа и использования в служебной деятельности. При этом могут

применяться специальные средства и методы с целью получения информации о замыслах, планах и действиях преступника, а также для изучения его (их) личности. К таким методам относится интернет-разведка (OSINT).

OSINT (Open Source Intelligence) – это разведывательная дисциплина, включающая в себя поиск, выбор, сбор разведывательной информации из общедоступных источников, а также ее анализ. Источники OSINT отличаются от других форм разведки, поскольку они должны быть легально доступны общественности без нарушения каких-либо законов или конфиденциальности.

90% полезной информации, получаемой спецслужбами, поступает из открытых источников. Сегодня социальные сети и иные сайты, содержащие персональные данные, открывают большие возможности для сбора информации о лице. Например, можно получить много данных о человеке по всему миру, просто проверив личную страницу этого человека в «Фейсбуке», «ВКонтакте», «Одноклассниках» и других социальных сетях.

С помощью OSINT можно не только проводить сбор данных в социальных сетях, но также использовать расширенные запросы поисковых систем для предоставления наиболее точных результатов поиска, осуществлять поиск удаленных версий веб-сайтов, отслеживать людей и их деятельность в интернете с помощью общедоступных баз данных и эффективных инструментов поиска, просматривать спутниковые изображения любой улицы мира, искать геолокацию лица и многое другое.

OSINT включает в себя все общедоступные источники сбора данных. Для сбора данных могут использоваться:

- поисковые сайты с грамотным формированием запросов (Google, «Яндекс», Opera, Firefox и пр.);
- средства массовой информации, статьи-компроматы, сайты-«отзовики» и т.д.;
- социальные сети, Telegram, включая боты (например, @EmailPhoneOSINT_bot), DarkNet;
- специализированные сайты (Shodan, Whols, «Глазбога.рф», YaSeeker, подсчет лайков, выявление общих связей в социальных сетях (например, 220vk.com) и т.д.);
- различные реестры, включая официальные сайты государственных служб (например, официальные сайты ГИБДД, ФССП и т.д.);
- специализированное программное обеспечение.

Необходимо помнить, что новые ресурсы для разведки по открытым источникам появляются ежедневно, но нельзя полагаться только на автоматизированные ресурсы. OSINT предполагает непосредственную работу аналитика, ручную проверку данных об изучаемом объекте, анализ выявленной информации, а также выводы по ней.

Достаточно большое количество данных находится в открытых источниках, которые сосредоточены в веб-пространстве. При поиске данных в интернете можно использовать:

1. Поисковые машины. Google является лидером среди поисковых машин и имеет наибольшую долю рынка потребителей (более 77%).

Поисковая система Google, помимо стандартного поиска, осуществляет поиск по изображению, группе новостей и т.д. Также можно воспользоваться техникой Google Dorks[1], которая представляет собой поисковые запросы для обнаружения скрытой информации на общедоступных серверах. Например, используя оператор allinurl, поисковая система Google выдаст результат со всеми страницами, которые были введены после оператора allinurl (allinurl:OSINT intelligence) (рис. 1).

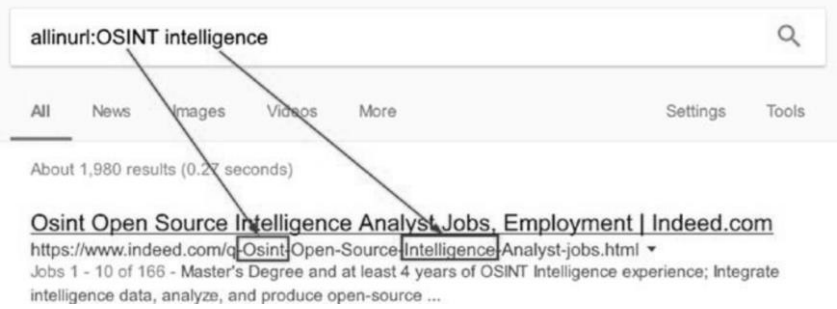

Рис. 1. Пример использования оператора allinurl

[1] Более подробно с поисковыми операторами можно ознакомиться по ссылке URL: https://habr.com/ru/post/437618/

Для тех, кто не желает прибегать к Google Dorks, поисковая система Google дает возможность использовать расширенные функции для поиска данных (https://www.google.com/advanced_search).

Для поиска устройств (IoT), подключенных к сети Интернет, существует поисковая система Shodan (https://www.shodan.io) (рис. 2).

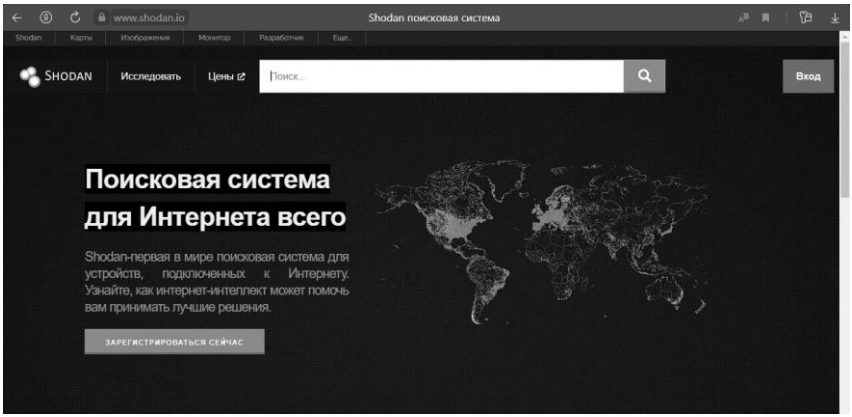

Рис. 2. Поисковая система Shodan

2. Историю веб-сайтов. Существуют интернет-сервисы, предоставляющие услуги по созданию точных копий веб-сайтов. Суть их работы заключается в том, что при удалении и иной модификации оригинальной веб-страницы созданная копия веб-сайта будет оставаться в сети Интернет. Одним из таких интернет-сервисов является Internet Archive (https://archive.org/web/web.php). Данный сервис сохранил более 308 миллиардов веб-страниц (рис. 3).

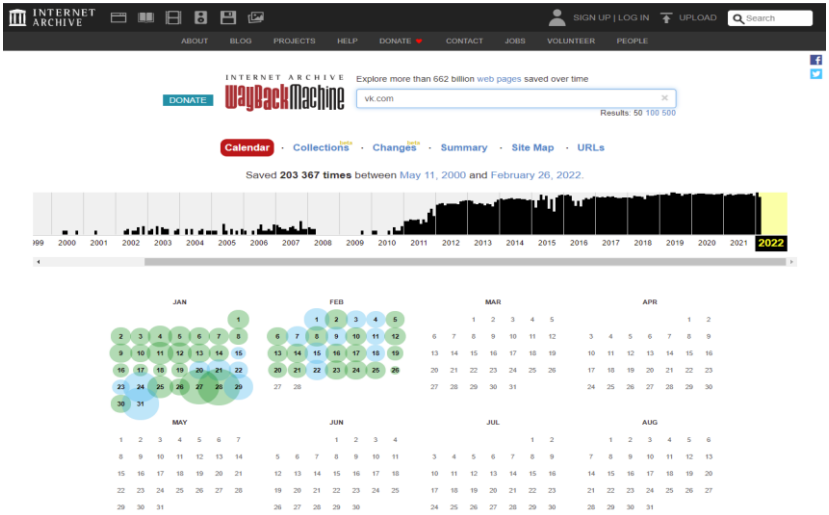

Рис. 3. Архив социальной сети www.vk.com

3. Операционные системы. Например, Trace Labs OSINT Linux Distribution на базе Kali является виртуальной машиной, ориентированной на разведку по открытым источникам, которая обеспечивает безопасность и скрытность ее пользователя (рис. 4).

Рис. 4. Внешний вид Trace Labs OSINT Linux Distribution

4. Утилиты Web Scraping. Существуют автоматизированные инструменты, которые способны помочь в сборе различных типов данных с целевого веб-сайта. Такие инструменты называются web scraping tools или web data extraction tools. Один из таких инструментов – theHarvester (https://github.com/laramies/theHarvester). TheHarvester способна собирать такие данные, как адреса электронных почт, персональные данные пользователей и т.д. из различных открытых источников, например, Google, Bing, LinkedIn, Twitter, Yahoo и др.

5. Онлайн-карты. Почти все портативные устройства (смартфоны, смарт-часы, трекеры) оснащены спутниковыми датчиками слежения для определения их местоположения на карте (Google Maps, «Яндекс.Карты»). Многие приложения, например, App Store, Google Play, используют данные о геолокации смартфона для предложения пользователю контента, анализируя его местоположение.

Существуют онлайн-сервисы, которые могут помочь обнаружить местоположение человека. Например, Tweet Mapper (https://keitharm.me/projects/tweet/), который показывает на карте твиты пользователя. Для обнаружения месторасположения человека необходимо знать его ник (рис. 5).

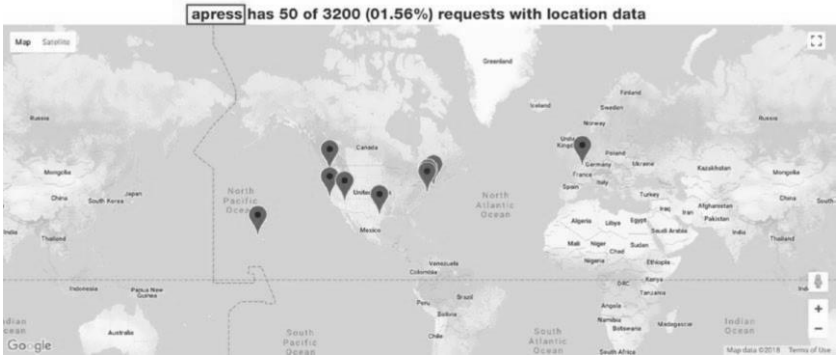

Рис. 5. Отображение на карте твитов пользователя apress

6. Справочные интернет-ресурсы:

6.1. SpravPortal (https://www.spravportal.ru/) (рис. 6), Phonenum (https://www.phonenum.info/) (рис. 7). Благодаря данным ресурсам можно определить оператора сотовой связи, к номерной

емкости которой относится проверяемый абонентский номер, а также получить сведения о смене оператора сотовой связи при сохранении номера телефона.

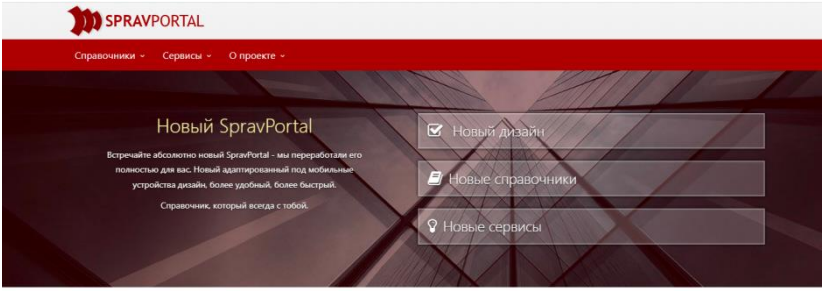

Рис. 6. Справочный интернет-ресурс SpravPortal

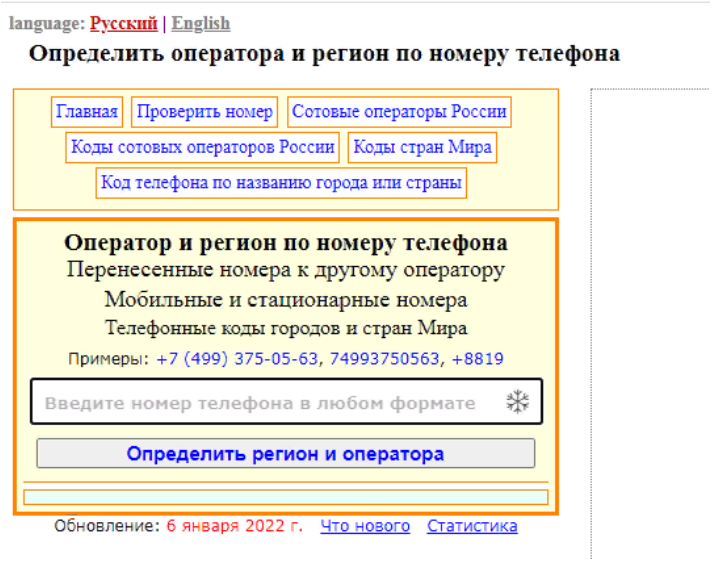

Рис. 7. Справочный интернет-ресурс Phonenum

6.2. IMEI.info (https://www.imei.info) (рис. 8). Благодаря данному ресурсу можно проверить IMEI. На основании данного номера можно узнать некоторую информацию об устройстве, например, марку или модель.

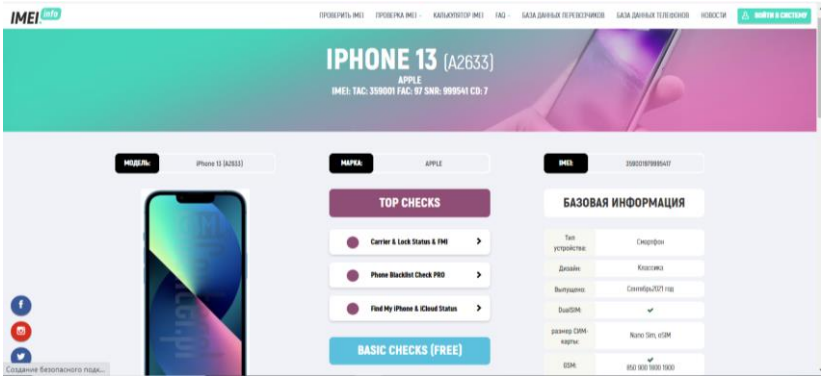

Рис. 8. Определение модели телефона по информации об IMEI-номере через справочный интернет-ресурс IMEI.info

6.3. «Рег.ру» (https://www.reg.ru/) (рис. 9), 2IP (https://2ip.ru/) (рис. 10). Благодаря данному ресурсу можно установить компанию-провайдер, предоставившую IP-адрес.

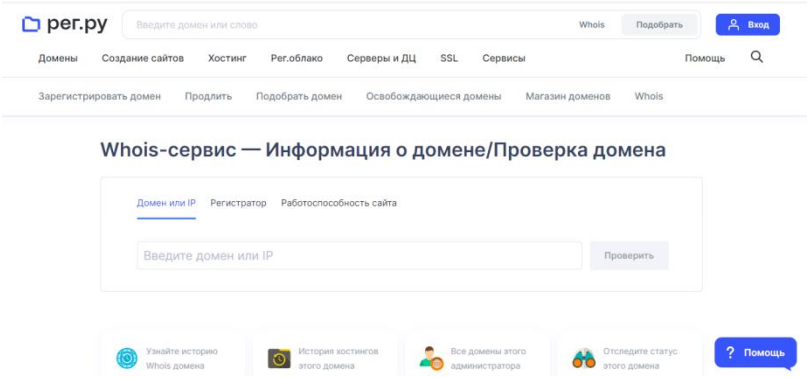

Рис. 9. Справочный интернет-ресурс «Рег.ру»

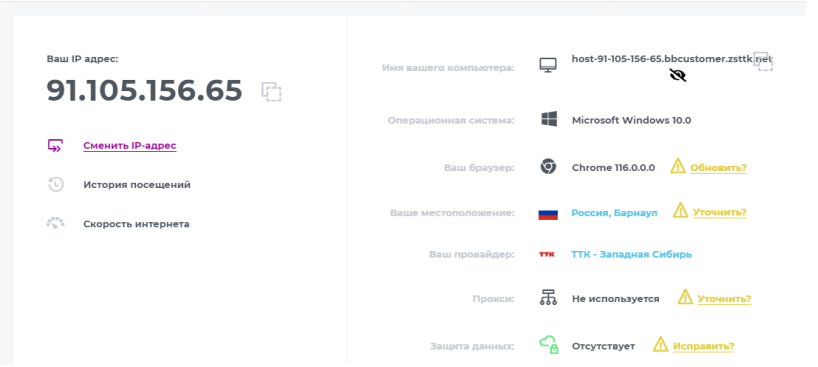

Рис. 10. Справочный интернет-ресурс 2ip.ru

Если раньше, чтобы получить какие-либо данные о лице, необходимо было посетить некоторое количество интернет-ресурсов, то на сегодняшний день для автоматизации OSINT существуют различные интегрированные интернет-ресурсы и программные средства (например, Maltego, FOCA, Creepy, NameChk.com, Yateda.com). Сервисы представляют собой платформы, на которых можно сразу провести комплекс действий: и поиск информации, и анализ результатов, и мониторинг дальнейших изменений.

При работе по открытым источникам необходимо помнить основные правила OSINT:

1) для регистрации (на сайтах-разведчиках, социальных сетях и т.д.) и мониторинга необходимо использовать отдельные номер телефона, электронную почту и аккаунты в социальных сетях;

2) проявлять осмотрительность, поскольку некоторые сервисы, содержащие информацию об объекте мониторинга, отправляют им уведомления с информацией, что данные о них запрашивались;

3) нужно быть готовым к тому, что сегодня какие-то используемые вами сервисы работают, а завтра уже нет;

4) пользоваться двумя-тремя аналогичными сервисами для перепроверки полученных данных об объекте мониторинга;

5) качественные и эффективные ресурсы-разведчики стоят денег – будьте готовы за них платить. Как правило, такие ресур-

сы предлагают оформить подписку на какой-то промежуток времени – месяц, год и т.д.;

6) внимательность, безопасность, критичность и креативность всегда должны сопровождать вас в мире OSINT (используйте VPN в своей работе).

Собирая данные по открытым источникам о физическом лице, необходимо определить ключевые маркеры поиска, они будут зависеть от целей анализа и желаемого результата поиска, также нужно помнить о геометках и поиске по изображениям.

Приведем примеры основных маркеров, которые можно использовать, собирая данные по физическому лицу:

- аккаунты в социальных сетях, проявление активности, на что существенно влияют возраст, сфера деятельности;
- публикации, репосты, размещаемый фото- и видеоконтент, включая фото профиля (-ей);
- друзья в социальных сетях, лайки, сфера интересов (участие в сообществах, пабликах), владение какой-либо собственностью;
- участие в деятельности юридических лиц, места учебы, работы, включая государственный сектор;
- связи с лицами, потенциально представляющими интерес для правоохранительных органов (в зависимости от решаемого кейса), родственные связи, аффилированность;
- анализ дополнительной информации: финансовых реквизитов, перемещений (включая парковочные сессии), различной сетевой активности (продажа товаров, оказание и предоставление услуг и т.д.), участия в конференциях, форумах и т.д.

Сотрудники полиции, особенно подразделений следствия, дознания и уголовного розыска, должны применять в своей профессиональной деятельности приемы и методы OSINT, т.к. благодаря разведке по открытым источникам можно получить криминалистически значимую информацию ориентирующего характера, которая может быть использована для выдвижения версий, определения направлений расследования, планирования следственного действия, прогнозирования возможной линии поведения участников уголовного процесса и возможного противодействия расследованию.

Вопросы для самоконтроля:

1. Какие нормативные правовые акты определяют особенности расследования хищений, совершенных с использованием информационно-телекоммуникационных технологий (ИТТ)?

2. Какими способами чаще всего совершаются хищения электронных денежных средств с использованием информационно-телекоммуникационных технологий?

3. Какова роль дроппера при совершении хищений с использованием ИТТ?

4. Что такое OSINT? Как возможно применять методы OSINT в деятельности правоохранительных органов при расследовании хищений, совершенных с использованием ИТТ?

5. Перечислите основные правила работы с информацией, размещённой в открытых источниках.

Литература

1. О банках и банковской деятельности [Электронный ресурс]: федеральный закон от 2 декабря 1990 г. № 395-1. Доступ из справ.-правовой системы «КонсультантПлюс».

2. О внесении изменений в Уголовный кодекс Российской Федерации [Электронный ресурс]: федеральный закон от 23 апреля 2018 г. № 111-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

3. О национальной платежной системе [Электронный ресурс]: федеральный закон от 27 июня 2011 г. № 161-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

4. О связи [Электронный ресурс]: федеральный закон от 7 июля 2003 г. № 126-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

5. Об информации, информационных технологиях и о защите информации [Электронный ресурс]: федеральный закон от 27 июля 2006 г. № 149-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

6. О порядке оказания услуг телефонной связи [Электронный ресурс]: постановление Правительства РФ от 9 декабря 2014 г. № 1342. Доступ из справ.-правовой системы «КонсультантПлюс».

7. О некоторых мерах по совершенствованию организации раскрытия и расследования отдельных видов хищений [Электронный ресурс]: приказ МВД России от 3 апреля 2018 г. № 196. Доступ из справ.-правовой системы «КонсультантПлюс».

8. Об организации работы по расследованию преступлений, совершенных с использованием информационно-телекоммуникационных технологий [Электронный ресурс]: приказ Следственного комитета Российской Федерации от 30 января 2023 г. № 19. Доступ из справ.-правовой системы «КонсультантПлюс».

9. Об утверждении правил применения автоматизированных систем расчетов [Электронный ресурс]: приказ Министерства информационных технологий и связи РФ от 2 июля 2007 г. № 73. Доступ из справ.-правовой системы «КонсультантПлюс».

10. О судебной практике по делам о краже, грабеже и разбое [Электронный ресурс]: постановление Пленума Верховного Суда РФ от 27 декабря 2002 г. № 29. Доступ из справ.-правовой системы «КонсультантПлюс».

11. О судебной практике по делам о мошенничестве, присвоении и растрате [Электронный ресурс]: постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48. Доступ из справ.-правовой системы «КонсультантПлюс».

12. Определение Судебной коллегии по уголовным делам Верховного Суда РФ от 29 сентября 2020 г. № 12-УДП20-5-К6 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

13. Бельдеубаева Д.Р. Применение OSINT-технологий в качестве повышения эффективности деятельности органов внутренних дел // Правопорядок в России: проблемы совершенствования: сб. ст. XV Всерос. конф-ции. М., 2021. С. 64-70.

14. Гаврилин Ю.В., Аносов А.В., Баранов В.В. и др. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учеб. пособие. В 2 ч. М.: Академия управления МВД России, 2019. Ч. 1. 208 с.

15. Голятина С.М. Методика расследования хищений электронных денежных средств: дис. … канд. юрид. наук. Волгоград, 2022. 196 с.

16. Янгаева М.О. Некоторые способы совершения хищений, совершенных с использованием информационно-телекоммуникационных технологий // Актуальные проблемы борьбы с преступлениями и иными правонарушениями: мат-лы 21-й междунар. научно-практ. конф-ции. В 2 ч. Барнаул: БЮИ МВД России, 2023. Ч. 1. С. 261-263.

17. Янгаева М.О., Павленко Н.О. OSINT. Получение криминалистически значимой информации из сети Интернет // Алтайский юридический вестник. 2022. № 2 (38). С. 131-135.

Глава 2. Особенности проверки сообщения о преступлении и первоначального этапа расследования хищений, совершенных с использованием информационно-телекоммуникационных технологий

2.1. Действия следователя в ходе проверки сообщения о хищениях, совершенных с использованием информационно-телекоммуникационных технологий

Наука криминалистика, исходя из стоящих перед ней задач, разделяет досудебное производство на этапы расследования, первым из которых является этап проверки сообщения о преступлении, хронологически совпадающий со стадией возбуждения уголовного дела. Такое положение рассматриваемого этапа указывает на его важнейшее значение в процессе собирания следов преступления, т.к. именно в этот период следователь и иные лица, осуществляющие уголовное преследование, начинают осуществлять поисково-познавательную деятельность, направленную на установление обстоятельств произошедшего. Кроме того, на этапе проверки сообщения о преступлении «могут быть собраны доказательства вины конкретного лица, т.е. сразу решена задача первоначального этапа»[1]. Указанные обстоятельства позволяют утверждать, что снижение количества нераскрытых преступлений в целом и хищений, совершенных с использованием информационно-телекоммуникационных технологий в частности, неразрывно связано с эффективностью работы следователя на этапе проверки сообщения о преступлении. Стоит отметить, что в различных ведомствах проверку сообщения о преступлении могут проводить не только следователи, но

[1] Кардашевская М.В. Периодизация расследования преступлений как основа для формирования криминалистических методик // Российский следователь. 2020. № 5. С. 17-20.

и оперативные уполномоченные подразделений уголовного розыска, участковые уполномоченные полиции и т.п.

После принятия заявления о преступлении на этом этапе досудебного производства следует незамедлительно приступить к получению объяснения от пострадавшего об обстоятельствах совершенного в отношении него преступления. При этом непосредственно в объяснении следует отразить информацию о способе преступления, а именно о том, какие ложные сведения сообщал преступник, где, когда и каким образом пострадавшим переданы либо отправлены денежные средства. В последнем случае обязательной является фиксация точных данных о способе отправления денежных средств, номерах счетов, данных об интернет-ресурсах, с помощью которых совершено преступление, информации о возможном преступнике, сумме причиненного материального ущерба.

Учитывая дистанционный характер рассматриваемых преступлений, также необходимо произвести иное процессуальное действие в виде представления, направленное на получение документов, содержащих сведения о соединениях по абонентскому номеру пострадавшего, который он использовал для ведения разговоров с преступником, а также на получение выписки о движении денежных средств по банковской карте (расчетному счету), которые использовал пострадавший для перевода денежных средств.

Для сокращения времени получения указанной важной информации возможно попросить пострадавшего использовать непосредственно при получении объяснения онлайн-банкинг или личный кабинет оператора связи.

Указанное процессуальное действие целесообразно оформить зафиксированным в объяснении или на отдельном листе ходатайством пострадавшего и вынесенным следователем постановлением о его полном удовлетворении[1]. Полученные от пострадавшего сведения, содержащиеся в предоставленных до-

[1] См. статью 122 Уголовно-процессуального кодекса Российской Федерации от 18.12.2001 № 174-ФЗ; Балакшин В.С. Иные процессуальные действия как средства уголовно-процессуального доказывания // Вестник Оренбургского государственного университета. 2006. № 3. С. 27.

кументах, целесообразно использовать для пополнения баз данных учетов (например, подсистемы ИБД-Ф «Дистанционное мошенничество»).

При получении сведений об «активности» абонентских номеров телефонов и IMEI-номеров смартфонов, использованных при совершении преступления, следователь дает поручение о проведении оперативно-розыскных мероприятий органу дознания.

Также на этом этапе целесообразно произвести осмотр места происшествия там, где осуществлялось использование потерпевшим смартфона, компьютера для выхода в сеть Интернет (например, жилище потерпевшего, рабочее место), перевод денежных средств (например, банкомат, офис кредитной организации), незаконный доступ к компьютерной информации и т.п.

С целью установления принадлежности абонентских номеров, которые использовались мошенником, конкретному оператору связи и субъекту Российской Федерации, где он распространялся, следует применять возможности, которые предоставляют различные сайты, например, сайт «SMSЦентр» и др. Также справкой фиксируются сведения об эмитенте банковской карты преступника, куда пострадавший перевел денежные средства. Для этого можно использовать многочисленные интернет-ресурсы, позволяющие получить эту информацию по первым шести цифрам, например сайт Finanso. Указанным выше документом также целесообразно оформить сведения об IP-адресе либо домене, организации, зарегистрировавшей доменное имя и оказывавшей услуги хостинга сайту, который использовал преступник при совершении преступления. Для этого можно использовать ресурсы сайта 2ip.ru и других подобных.

На этапе проверки сообщения о преступлении может использоваться такой уголовно-процессуальный инструмент, как направление запросов в порядке ч. 4 ст. 21 УПК РФ. Поэтому следует безотлагательно направить запросы о получении информации в различные организации, такие как «ВКонтакте», «Одноклассники», «Авито», «Мэйл.ру», интернет-провайдерам и т.п.

Нередко преступник в качестве способа получения денежных средств от пострадавшего использует других лиц. При этом следует подробно установить приметы внешности указанного субъекта, составить его субъективный портрет (композиционный, рисованный и т.п.), осуществить действия, направленные

на поиск свидетелей, очевидцев передачи денег пострадавшим, провести мероприятия, направленные на поиск камер видеонаблюдения в месте совершения преступления, а также по ходу движения указанного лица как пешком, так и на автомобиле (в последнем случае предпринимаются меры, направленные на установление транспортного средства и его владельца).

При установлении лица, которое использовал преступник для получения денег от пострадавшего, необходимо истребовать от него объяснение, в котором зафиксировать информацию, аналогичную содержанию сведений, представленных пострадавшим. Также с его письменного согласия лицо, осуществляющее проверку сообщения о преступлении, получает сведения о входящих и исходящих соединениях посредством использования «личного кабинета» абонентского номера мобильного оператора опрашиваемого.

В случае если сбором и исследованием материала проверки сообщения о преступлении занимается следователь, то целесообразно направить в орган, осуществляющий оперативно-розыскную деятельность (в частности, в подразделения уголовного розыска органов внутренних дел) поручение о проведении оперативно-розыскных мероприятий, направленных на установление факта нахождения похищенных денежных средств на банковских счетах конкретных кредитно-финансовых учреждений.

Необходимо отметить, что выполнение указанных выше действий позволит достаточно полно собрать информацию о совершенном преступлении. Но учитывая ограниченный уголовно-процессуальный инструментарий, который возможно применять на этапе проверки сообщения о преступлении, следует при наличии оснований без промедления вынести постановление о возбуждении уголовного дела и перейти к первоначальному этапу расследования, который по временным рамкам находится на такой стадии уголовного судопроизводства, как предварительное расследование. Данное положение позволяет следователю при осуществлении поисково-познавательной деятельности по хищениям, совершенным с использованием информационно-телекоммуникационных технологий, задействовать весь арсенал предусмотренных уголовно-процессуальным законодательством следственных и иных процессуальных действий.

2.2. Действия следователя на первоначальном этапе расследования хищений, совершенных с использованием информационно-телекоммуникационных технологий

Этапность является широко используемым методом структурирования предварительного расследования, целью использования которого является повышение уровня практической эффективности криминалистических рекомендаций. Первоначальный этап расследования начинается с момента возбуждения уголовного дела и длится, как правило, до момента предъявления обвинения, в случае если преступник установлен, или до момента исчерпания следователем возможностей собирания следов преступления, если лицо, его совершившее, неизвестно. Важнейшей задачей этого этапа расследования является «сбор достаточных доказательств и тактико-психологической информации об основных обстоятельствах расследуемого события и виновности в выявленном преступлении конкретных лиц»[1]. Первоначальный этап расследования хищений, совершенных с использованием информационно-телекоммуникационных технологий, имеет несомненную специфику, обусловленную способом совершения преступления и следовой картиной.

После вынесения постановления о возбуждении уголовного дела следователю необходимо без промедления вынести постановление о признании потерпевшим и приступить к его допросу. В ходе этого следственного действия необходимо выяснить информацию о дате, времени звонка, абонентских номерах звонившего и потерпевшего, дословное содержание разговора, описание голоса и речи звонившего, обстоятельств перечисления или передачи денежных средств неизвестному лицу. Если в ходе допроса выяснилось, что хищение совершено с использованием сети Интернет, целесообразно осуществить поиск объявления в сети Интернет и зафиксировать его адрес, сделать скриншот экрана и приобщить его к материалам уголовного дела. Также

[1] Кардашевская М.В., Шипилова Е.С. Этапы процесса расследования и их характеристика // Таврический научный обозреватель. 2015. № 2. С. 9.

в ходе допроса необходимо разъяснить потерпевшему право на возмещение имущественного вреда, причиненного преступлением, и в случае заявления исковых требований в отношении него вынести постановление о признании гражданским истцом. Кроме того, следует разъяснить потерпевшему право обращения в суд в порядке гражданского судопроизводства с целью отмены операции по переводу денежных средств и обратном перечислении похищенных денежных средств со счета получателя на счет потерпевшего.

Также целесообразно истребовать от потерпевшего и приобщить к протоколу его допроса копию паспорта, справки о доходах потерпевшего и членов его семьи, детализацию телефонных переговоров абонентского номера потерпевшего за период переговоров с мошенником.

С участием потерпевшего провести проверку показаний на месте, в которой отразить содержание показаний потерпевшего в совокупности с демонстрацией его действий по переводу денежных средств мошенникам, например, с использованием банкомата.

После производства допроса потерпевшего вполне логично произвести выемку у потерпевшего документов, подтверждающих факт совершения хищения:

- платежные поручения, приходные кассовые ордера, справки, выписки, чеки, подтверждающие факт перевода денежных средств;

- документы, содержащие детализацию соединений по абонентскому номеру потерпевшего;

- листы со скриншотами экрана с перепиской в социальных сетях или посредством электронной почты.

После выемки указанных выше документов целесообразно изъять у потерпевшего смартфон и незамедлительно произвести его осмотр, по возможности с участием специалиста. В ходе осмотра следует обратить внимание на переписку с виновным, содержание сообщений о переводе денежных средств с указанием кредитной организации – получателя денежных средств. Для обеспечения наглядности следует составить приложение к протоколу осмотра предметов и документов, куда включить скриншоты с экрана смартфона. Следует отметить, что после выпол-

нения указанных действий могут возникнуть основания полагать, что хищение денежных средств у потерпевшего было совершено с использованием вредоносного программного обеспечения. Данное обстоятельство требует незамедлительного назначения компьютерной экспертизы изъятого у потерпевшего смартфона.

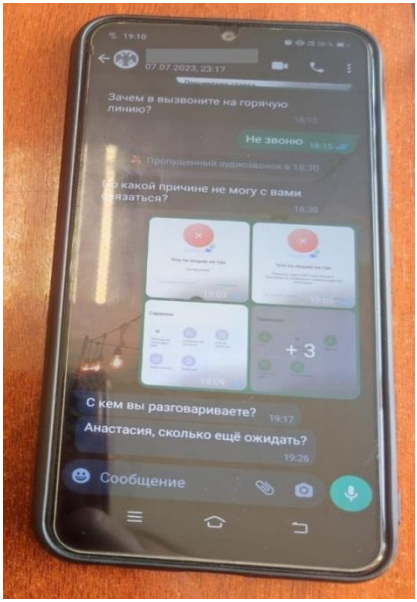

Рис. 11. Смартфон потерпевшего с перепиской с преступником

Кроме осмотра изъятого у потерпевшего смартфона, необходимо также осмотреть ответы из кредитных организаций, от операторов связи, интернет-провайдеров (если запросы в них направлялись ранее на этапе проверки сообщения о преступлении). Необходимо обратить внимание и отразить в протоколе осмотра:

- номера банковских карт, банковских счетов, абонентских номеров, с которых или на которые перечислялись похищенные денежные средства;

- адреса расположения базовых станций и векторов (азимутов) направления сигнала;

- IMEI-номера устройств, в которых была установлена симкарта при регистрации в сети;

- IP-адреса, с которых осуществлялись неправомерный доступ к банковскому счету, создание и администрирование учетной записи (аккаунта в социальных сетях, электронного почтового ящика, электронного кошелька и т.п.), доступ к личному кабинету интернет-ресурса;

- MAC-адреса сетевых карт (встроенных сетевых интерфейсов) компьютерной техники, а также Wi-Fi-роутеров;

- номера объявлений на специализированных сайтах объявлений (досках объявлений);

- черты внешности, поведения, детали одежды подозреваемого лица, а также подробно о производимых им действиях (манипуляциях) с указанием точного времени их осуществления.

В случае если в материалах, отражающих этап проверки сообщения о преступлении, имеются сведения о реквизитах банковского счета, на который были перечислены похищенные у потерпевшего деньги, то следователь незамедлительно должен возбудить перед судом ходатайство о наложении ареста на имущество, направить постановление суда в кредитную организацию и составить протокол наложения ареста на имущество.

Следователь также безотлагательно направляет запросы операторам связи. При получении ответов от операторов сотовой связи об установлении владельцев абонентских номеров, с использованием которых совершено преступление (с которого звонили и на чьи счета переведены денежные средства), также допрашивает данных лиц в качестве свидетелей.

Следователь направляет запросы в кредитные учреждения с целью получения информации о вкладах и счетах граждан в банках и иных кредитных организациях. При получении ответов из кредитных организаций аналогичным образом допрашивает в качестве свидетелей лиц, на чье имя открыты банковские счета, использовавшиеся при совершении преступления. При установлении лиц, обналичивших денежные средства, похищенные у потерпевшего, необходимо допросить их в качестве свидетелей. Также в качестве свидетелей следователь допрашивает всех лиц, осведомленных об обстоятельствах совершения преступления (родственников потерпевшего, соседей и иных

лиц – возможно, они размещали объявление по просьбе потерпевшего, предоставляли ему смартфон, осуществляли перевод денежных средств и т.п.).

Также запросы направляются в организации, владеющие сайтами социальных сетей, почтовых сервисов, с целью установления сведений о лице, которому принадлежат определенный идентификатор, логин, никнейм, почтовый ящик.

После получения ответов из кредитных организаций, от операторов связи, интернет-провайдеров и т.д. необходимо произвести их осмотр, проанализировать на предмет выявления криминалистически значимой информации.

Для установления сведений о соединениях абонентов (о дате, времени, продолжительности, типе соединений, а также об абонентском номере, фамилии, имени, отчестве, адресе регистрации, абонентском устройстве (IMEI, сим-карта) и месте нахождения второго участника соединения (номере, адресе базовой станции, азимуте расположения устройства относительно станции), о маршруте движения абонента в определенный период времени) следователю необходимо возбудить перед судом ходатайство о получении информации между абонентами и (или) абонентскими устройствами, после чего обратиться к оператору связи для получения указанной информации.

С целью истребования содержания текстовых сообщений пользователей услугами связи, голосовой информации, изображений, звуков, видео-, иных сообщений, а также текстовых сообщений пользователей сети Интернет следователю стоит возбудить ходатайство об осмотре и выемке электронных сообщений или иных сообщениях, передаваемых по сетям электросвязи в соответствии со ст. 185 УПК РФ. После получения судебного решения для осмотра и выемки электронных сообщений следователю необходимо прибыть в соответствующие организации.

Помимо этого, для установления лица, подлежащего привлечению в качестве обвиняемого, следователь направляет органу дознания поручение на проведение оперативно-розыскных мероприятий, направленных на установление лица, совершившего преступление.

Таким образом, алгоритмизация процесса расследования является одним из условий его эффективности, что в полной

мере относится и к расследованию хищений, совершенных с использованием информационно-телекоммуникационных технологий. Приведенный нами алгоритм действий будет способствовать повышению уровня раскрываемости преступлений этой категории, их качественному расследованию.

2.3. Тактика производства следственных осмотров

Следственный осмотр – это следственное действие, состоящее в непосредственном восприятии и изучении лицом, уполномоченным на его производство, любых объектов в целях исследования обстоятельств деяния, обнаружения, фиксации и изъятия предметов, документов, следов и веществ, которые имеют или могут иметь значение для раскрытия преступления и расследования уголовного дела.

При проверке сообщения о преступлении и расследовании хищений, совершенных с использованием информационно-телекоммуникационных технологий, могут производиться следственные осмотры:

- места происшествия;
- предметов и документов.

Местом происшествия в рассматриваемых преступлениях может быть:

1) место, где осуществляется обработка компьютерной информации;

2) сервер, сохранивший свидетельства о работе системы за определенный период или о предмете посягательства;

3) место, где осуществлялось использование электронных носителей информации для выхода в сеть Интернет, перевод денежных средств, незаконный доступ к компьютерной информации и пр.;

4) место наступления вредных последствий.

Рассмотрим этапы и стадии осмотра места происшествия. Традиционно выделяют три этапа осмотра: подготовительный, рабочий и заключительный. Каждый из них специфичен и может делиться на стадии.

Подготовительный этап делится на две стадии:

1) действия при получении сообщения о преступлении до выезда на место осмотра;

2) действия следственно-оперативной группы (далее – СОГ) по прибытии на место происшествия.

Как правило, большая часть подготовительных мероприятий, подлежащих выполнению при получении сообщения о преступлении, возложена на сотрудников дежурной части территориального органа внутренних дел.

Для обеспечения незамедлительного выезда на место происшествия в каждом подразделении предварительного следствия в системе МВД России организовано дежурство следователей, согласованное с органом дознания и экспертно-криминалистическими подразделениями.

В рамках данного этапа на основе сбора и анализа ориентирующей информации устанавливаются обстоятельства произошедшего события (способ, место и время); определяются конкретные задачи следственного действия, а также состав СОГ, проводится ее инструктаж.

Считаем, что в состав СОГ, выезжающей на осмотр места происшествия, связанного с информационно-телекоммуникационными технологиями, должны входить следователь, оперуполномоченный уголовного розыска, специалист-криминалист. Также статья 164.1 УПК РФ императивно указывает на необходимость привлечения специалиста в области информационных технологий при изъятии электронных носителей информации и копирования с них информации при производстве следственных действий. Таким специалистом может быть сотрудник отдела «К» БСТМ МВД России по субъекту РФ, эксперт ЭКЦ МВД России по субъекту РФ, производящий компьютерные экспертизы, или иное гражданское лицо, обладающее подобными знаниями, работающее в некоммерческой организации.

Кроме того, до выезда СОГ на место происшествия следователем после консультации со специалистом в сфере информационно-телекоммуникационных технологий принимается решение о целесообразности, а иногда об обязательности использования при осмотре программно-аппаратных средств работы

с электронной информацией (например, «Мобильный криминалист», Cellebrite UFED и др.).

По прибытии на место происшествия следователь должен запретить всем присутствующим лицам работать со средствами вычислительной техники и компьютерной информацией в пределах осуществления следственного действия, удалить с места происшествия всех лиц, которые не вовлекаются в производство осмотра места происшествия. Оптимальным будет нахождение указанных лиц в помещении, где исключена возможность использования средств связи. Необходимо провести инструктажи участникам следственного действия с разъяснением прав, обязанностей, целей и задач следственного действия, а также определить последовательность (очередность) своих действий.

Рабочий этап осмотра места происшествия состоит из двух стадий: общей (статической) и детальной (динамической). Первая предполагает установление границ места, подлежащего осмотру; фиксацию обстановки на момент начала производства следственного действия путем фотографирования; выдвижение типичных общих и частных версий, определение оптимальных способов поиска следов.

Большинство криминалистов рекомендуют при осмотре места происшествия по факту совершения преступлений с использованием информационно-телекоммуникационных технологий производить осмотр эксцентрическим способом, начиная от устройства, откуда был осуществлен вход в сеть Интернет, перевод денежных средств и пр. Если на подготовительном этапе осмотра следователь так и не смог точно выявить электронный носитель информации, то осмотр необходимо производить концентрическим способом.

В рамках детальной стадии осмотра места происшествия проводится тщательное изучение структуры места происшествия в целом и каждого ее элемента в частности, обнаружение и изъятие предметов и документов, имеющих значение для уголовного дела. Здесь важно использовать помощь и знания специалиста в сфере информационных технологий, который должен быть предельно внимателен и аккуратен.

Сначала выявляются материальные следы преступления. Чаще всего они имеют место, когда речь идет о хищении безна-

личных или электронных денежных средств, которому предшествовал непосредственный контакт преступника с устройством потерпевшего (следы пальцев рук, следы обуви, следы биологического происхождения, устройства, документы, данные банковских карт и др.). Затем следователь и специалист переходят к осмотру устройства и информационно-телекоммуникационной сети, т.е. к поиску цифровых следов. Необходимо помнить о том, что, если на момент начала осмотра устройство находилось в выключенном состоянии, нужно оставить его в таком же, чтобы не потерять важной информации, если было включено, в первую очередь стоит обратить внимание на изображение на экране дисплея, далее выяснить, какая операционная система установлена на компьютере, какие используются протоколы связи, службы доступа к файлам и сети. Именно здесь могут быть выявлены цифровые следы преступления. Важно подчеркнуть, что такие следы имеют высокую скорость трансформации, легко уничтожаются и модифицируются, могут быть представлены бесконечным количеством копий, легко распространяются в компьютерных сетях и доступны в любой точке, где имеется подключение к сети Интернет. Цифровыми следами могут быть следы вывода и ввода денег, хранящиеся на серверах онлайн-банков или платежных систем, следы, связанные с регистрацией доменного имени сайта, IP-адрес и т.д.

В завершение электронные документы и иная значимая для уголовного дела информация (журналы логов) фиксируются и изымаются, при необходимости может быть изъят весь компьютер или системный блок либо мобильный телефон. В качестве иной информации могут выступать, например, документы.

*Так, согласно материалам уголовного дела по обвинению Д. в совершении преступления, предусмотренного п. «в» ч. 2 ст. 158 Уголовного кодекса Российской Федерации, у потерпевшей Р. были изъяты документы, свидетельствующие о несанкционированном списании со счета № ***, открытого в банке «название» денежных средств в сумме 17 000 руб., принадлежащих ей, справка банка «название» и мини-выписка по карте банка «название», а также сотовый телефон Honor (IMEI 1 ***, IMEI 2 ***), содержащий СМС-сообщения о списании денежных средств.*

На заключительном этапе осмотра места происшествия изъятые объекты упаковываются, делается запись об ознакомлении с протоколом всех участников следственного действия, учитываются их замечания.

Осмотр места происшествия необходим для изучения механизма преступления; установления обстоятельств, отражающих объективную сторону преступления; обнаружения и изъятия следов, которые могут служить вещественными доказательствами по уголовному делу.

Тактика производства осмотра предметов и документов

Целью осмотра предметов и документов является обнаружение следов преступления и выяснение других обстоятельств, имеющих значение для уголовного дела. По уголовным делам о хищениях безналичных или электронных денежных средств предметами осмотра обычно выступают устройства, откуда осуществлен вход в сеть Интернет, перевод денежных средств; устройства, с которых запущена вредоносная программа; флешнакопители; внешние жесткие диски; оптические диски; служебные журналы системных и прикладных программ, применяемые для осуществления транзакций; банковские карты; симкарты и пластиковые держатели для них и др. Документами по данным делам являются выписки о движении денежных средств по счетам; сопроводительные письма к оптическим дискам; документы, подтверждающие причинение материального ущербы потерпевшему; документы, подтверждающие получение банковских карт, с которых и на которые осуществлялся перевод денежных средств; документы, свидетельствующие о несанкционированном списании денежных средств со счета, и т.д.

*Так, в рамках уголовного дела по обвинению А. в совершении преступления, предусмотренного ч. 3 ст. 159 Уголовного кодекса Российской Федерации, осмотру подлежало сопроводительное письмо, полученное по запросу № ***, содержащее информацию по переводам денежной системы «Колибри», подготовленное главным специалистом отдела обработки запросов в г. Нижнем Новгороде *** и заверенное оттиском печати ПАО «Сбербанк». В данном письме зафиксированы следующие сведения: по системе денежных переводов «Колибри» счет ***,*

*денежные средств получены в отделении ***. Реквизиты отправителя: М., паспорт ***, место жительства ***, дата заявления ***, сумма перевода 160 000 руб., филиал отправителя перевода ***. Реквизиты получателя: А., иностранный паспорт ***, место жительства ***, дата выплаты ***, дата списания ***, сумма поступивших средств 160 000 руб. Кроме того, осмотру подлежал оптический диск DVD-R торговой марки TDK Life on Record емкостью 4,7 Гб, вставленный в считывающее устройство – дисковод системного блока проигрывателя ноутбука Acer, используемого в качестве технического устройства при производстве описываемого следственного действия. На данном диске в папке «Видеозапись» содержалась запись с камер наружного видеонаблюдения ***, установленных в помещении офиса Сбербанка. В нижней части экрана указаны дата записи *** и время начала записи ***. На видеозаписи с камеры *** видно, как напротив оператора банка сидит молодой человек, одетый в черную куртку, совершающий операции на мобильном телефоне. Со слов участвующего в осмотре подозреваемого А., на видеозаписи изображен он в момент предоставления специалисту банка паспорта гражданина Республики Беларусь и обналичивания денежных средств в сумме 22 000 руб., переведенных ему гр. М.*

Из сути видеозаписи следует, что оператор распечатала на принтере, подключенном к рабочему компьютеру, документ формата А4 и передала его А., который, в свою очередь, взял данный лист бумаги, поставил на нем свою подпись и передал обратно сотруднику банка. Затем оператор передала А. отрывной талон приходного кассового ордера, где А. поставил свою подпись, после чего вернул его обратно. Далее сотрудница банка открыла шкаф, достала оттуда деньги, положила их в счетчик банкнот, затем передала А. Он взял деньги, пересчитал их и убрал в правый карман своей куртки. Таким образом, в результате производства следственного осмотра была получена информацию, доказывающая причастность А. к совершению преступления.

Предметами осмотра также могут быть мобильные телефоны и содержащиеся в их памяти аудиозаписи. Например, *в ходе осмотра мобильного телефона Л., подозреваемого в соверше-*

*нии преступления, предусмотренного ч. 3 ст. 159 Уголовного кодекса Российской Федерации, в папках «Приложения», WhatsApp Messenger.files, «Аудиофайлы» был открыт аудиофайл ***, на котором, по словам подозреваемого Л., он выражает свое недовольство по поводу того, что Н. рассказал сотрудникам полиции о мошеннических действиях, совершаемых Л.*

Осмотр предметов и документов включает в себя три этапа: подготовительный, рабочий и заключительный.

На подготовительном этапе нужно проанализировать имеющуюся в уголовном деле информацию, организовать участие специалиста в сфере IT-технологий, привлечь понятых (в их отсутствие решить вопрос о применении средств фиксации).

На рабочем этапе производства осмотра устройств в первую очередь важно обеспечить неизменность, подлинность и сохранность источника информации (не завершать запущенные ранее программы и не закрывать приложения, не отключать функции «авиарежим», «блокировка экрана», не допускать самостоятельного совершения действий, результат которых сложно спрогнозировать); тщательно изучить предмет осмотра (для этого могут быть использованы упомянутые выше аппаратно-программные комплексы). Большое значение здесь приобретает участие специалиста в сфере информационных технологий.

При решении вопроса о его вызове следователь должен иметь представление о категории доказательств, какие он надеется получить в ходе осмотра, наличии у специалиста необходимой профессиональной подготовки, соответствующей задачам следственного действия, и технико-криминалистических средств, от которых зависит эффективность его работы. Именно с помощью таких средств можно получить доступ к переписке, страницам в социальных сетях, резервным копиям, облачным хранилищам, особенно если на устройстве активирована функция «авиарежим». Кроме того, необходимо удостоверить подлинность обнаруженной информации: отображаемая на устройствах информация должна быть зафиксирована с помощью функции «скриншот» и отражена в фототаблице с соответствующими пояснительными записями.

На заключительном этапе оформляется протокол осмотра, предметы упаковываются в материал, исключающий возможность доступа к содержимому и дистанционного считывания информации, ее модификации или уничтожения.

В результате производства следственного осмотра можно получить информацию, имеющую значение для уголовного дела, а также принять решение о необходимости назначения и производства экспертного исследования.

2.4. Тактика допроса потерпевшего и свидетеля

При расследовании хищений, совершаемых в сфере информационно-телекоммуникационных технологий, представляет интерес допрос потерпевшего, при производстве которого в обязательном порядке должны учитываться особенности личности допрашиваемого. Потерпевшими становятся граждане, которые в силу излишней доверчивости, на фоне страха потерять свои деньги либо желания получить легкие деньги, товары по акции, сообщают мошеннику конфиденциальную информацию о номере карты, паролях, CVV-коде. При допросе, прежде всего, необходимо установить психологический контакт и получить детальную информацию о совершенных преступником и потерпевшим действиях.

Особенностью производства допроса потерпевшего также является использование тактических приемов, способствующих достоверному установлению времени, места, способа совершения преступления, подробных данных о похищенных денежных средствах, размера ущерба, причиненного преступлением, лиц, причастных к совершению преступления, а также дополнительных свидетелей и очевидцев произошедшего.

В ходе допроса потерпевшего им сообщается большой объем цифровой информации: о дате и времени звонка или сообщения, о количестве звонков, об абонентском номере сим-карты, привязанном к банковскому счету, карте, электронному кошельку как потерпевшего, так и преступника, номере подразделения банка, выдавшего карту либо оформившего иное электронное средство платежа, о сумме денежных средств, находившихся на

счете, о сумме списанных денежных средств и пр. Очевидно, что запомнить всю подобную знаковую информацию и воспроизвести ее хронологически и фактически безупречно для большинства лиц невозможно[1].

Согласно ст. 189 УПК РФ потерпевший при допросе может пользоваться документами, подтверждающими факт списания денежных средств, факт общения потерпевшего с неустановленным лицом, совершившим хищение денежных средств. Потерпевший такие сведения может получить самостоятельно при использовании определенных приложений, установленных на мобильном телефоне, или при непосредственном обращении в банк или иную организацию.

При производстве допроса потерпевшего об обстоятельствах хищения денежных средств могут быть поставлены следующие вопросы:

- дата, время поступления звонка (СМС-сообщения) с соответствующим содержанием, с какого номера поступил звонок (сообщение);
- абонентский номер потерпевшего, на который поступил звонок, СМС-сообщение (стационарный, мобильный телефон), на кого он зарегистрирован, как давно пользуется данной симкартой;
- какие были его дальнейшие действия после поступления звонка (СМС-сообщения);
- дословное содержание разговора, кем представился звонивший (сотрудником органов внутренних дел, прокуратуры, Росфинмониторинга, оператора связи и др.), что пояснял, как обратился к потерпевшему, сколько человек разговаривали с ним, что предлагали сделать;
- описание голоса звонившего (дефекты речи – хрипота, картавость, шепелявость, заикание), какова была интонация, разговаривал ли он шепотом или обычным голосом; какие особенности, странности в интонации, произношении звуков, обращении заметил потерпевший; использовал ли в разговоре специальные термины, специфические речевые обороты; может ли

[1] Маилян А.В. Совершенствование методики расследования хищения с использованием электронных средств платежа: дис. … канд. юрид. наук. Ростов н/Д., 2021. С. 111.

определить возраст звонившего, по каким приметам потерпевший сможет опознать голос звонившего;

- качество связи (помехи, пропадала слышимость, разговор прерывался, хорошо или плохо слышен голос и др.);
- что именно (по возможности дословно) сам потерпевший сообщил неизвестному;
- как долго длился телефонный разговор с неизвестным;
- если передача денежных средств происходила при личном контакте, выяснить обстоятельства передачи денежных средств неизвестному (описание внешности и голоса неизвестного курьера, по каким приметам сможет его опознать; если передача денег осуществлялась в жилище, установить: когда неизвестный курьер зашел в квартиру, до каких предметов мебели, иных предметов дотрагивался, как себя вел, что сообщил, задавал ли какие-либо вопросы, задавал ли потерпевший ему какие-либо вопросы, интересовался ли судьбой своего родственника; сообщал ли потерпевший неизвестному точную сумму денег, которую передал ему, для каких целей он передает ему эти деньги; судя по поведению неизвестного, был ли тот осведомлен о содержимом, переданном ему, о причинах (целях) передачи ему денежных средств; как потерпевший упаковал деньги; звонил ли неизвестный в момент получения денег кому-либо, что говорил);
- звонил ли потерпевший своему родственнику, именем которого представился мошенник, или нет; если нет, то почему; кто присутствовал при разговоре с мошенником и может подтвердить слова потерпевшего;
- при осуществлении безадресного перевода необходимо выяснить полные установочные данные получателя, истребовать у потерпевшего квитанцию (чек) о переводе.

Если перевод был осуществлен на лицевой счет абонентского номера или счет банковской карты, необходимо выяснить:

- абонентский номер телефона или номер банковской карты потерпевшего, с которой переведены денежные средства, когда, где (в каком отделении Сбербанка, другого банка) потерпевшим получена банковская карта, ее реквизиты (номер карты, дата и место открытия счета, его номер), пользуется ли в насто-

ящее время данной банковской картой, блокировал ли её после совершения преступления;

- как давно пользуется банковскими картами, известны ли ему правила обращения с ними;
- почему, получив сообщение с неизвестного номера или откликнувшись на телефонный звонок, сам лично не перезвонил в отдел по обслуживанию клиентов Сбербанка либо другого банка, в котором открыт счет;
- какие именно операции им проведены, каким образом, их последовательность (если операции проводились через банкомат – адрес банкомата, какие номера набирал в банкомате, последовательность набора абонентских номеров (желательно воспроизвести), какие суммы перечислены на каждый номер, появлялись ли на дисплее банкомата сообщения о производимых им операциях, если да, то какие именно); осознавал ли он, что переводит денежные средства;
- абонентский номер телефона или номер банковской карты, на которые были переведены денежные средства.

Если хищение совершено с использованием информационно-телекоммуникационной сети Интернет, необходимо также установить:

- дату и время обнаружения объявления (получения ссылки на соответствующий интернет-ресурс), если возможно – найти объявление в интернете и зафиксировать его адрес (еще раз пройти по интернет-ссылке), сделать снимок экрана, приобщить его к материалам уголовного дела;
- с использованием какого технического устройства потерпевший просматривал содержание сайта с размещенным объявлением (переходил по интернет-ссылке): стационарного компьютера, мобильного устройства;
- какие характеристики продаваемого товара были указаны в объявлении о продаже;
- какие условия купли-продажи содержались в объявлении (условия о предоплате, оплате товара, сроках и видах его поставки, ответственности сторон);
- какие контактные данные продавца были указаны в объявлении о продаже;

- имелись ли отзывы, комментарии к объявлению о продаже;
- каким образом, когда (дата, время) потерпевший связался с продавцом;
- отразить подробное содержание разговора с продавцом, как продавец представился, что именно сообщил продавец о продаваемом товаре, об условиях оплаты товара, условиях, сроках и способах доставки покупателю товара;
- каким образом известил продавца товара о перечислении денежных средств на указанную им банковскую карту (электронный кошелек);
- что именно ему сообщил после подтверждения оплаты (перечисления денег на банковскую карту виновного) продавец;
- в какой период времени, куда прибыл для получения приобретенного товара;
- когда он осознал, что в отношении него было совершено мошенничество, в результате которого похищены принадлежащие ему денежные средства;
- сохранилась ли переписка с мошенником;
- кто имел возможность доступа к управлению счетами потерпевшего, в т.ч. к его мобильному телефону;
- подозревает ли кого-либо в совершении преступления;
- какова сумма материального ущерба, причиненного в результате совершения в отношении него преступления, является ли данный ущерб значительным, если да, то почему (состав его семьи, наличие иждивенцев, размер ежемесячного дохода, из чего он складывается, размер общего дохода всех членов семьи, расходы семьи);
- желает ли заявить гражданский иск о возмещении имущественного вреда, причиненного в результате совершения преступления (если да, то истребовать от потерпевшего заявление, в установленном законом порядке признать его гражданским истцом).

На основании соответствующего постановления необходимо произвести выемку у потерпевшего имеющихся у него документов или материальных носителей, содержащих сведения о совершении преступления (платежных поручений, приходных кассовых ордеров, кассовых чеков, скриншотов, фиксирующих

осуществление транзакций, мобильных телефонов, других устройств, содержащих переписку в социальных сетях, текстовые СМС-сообщения, детализацию соединений по его абонентскому номеру и пр.), а также документов, отражающих переписку потерпевшего с лицом, совершившим преступление. После чего необходимо произвести осмотр изъятых объектов, в ходе которого зафиксировать сведения, имеющие доказательственное значение (переписка с лицом, совершившим преступление, сведения о переводе средств в электронных платежных системах, текст СМС-сообщений).

Следует обратить внимание, что осмотр СМС-сообщений, журнала звонков, содержащихся в устройстве, необходимо проводить с разрешения и с участием владельца устройства, в противном случае действия следователя могут быть признаны нарушением конституционного права на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Целесообразно оформлять приложения к протоколу осмотра в виде скриншотов экрана компьютера, мобильного телефона (с целью обеспечения наглядности). После чего при наличии оснований предметы и документы, имеющие доказательственное значение для уголовного дела, необходимо признать и приобщить в качестве вещественных доказательств.

При допросе свидетеля необходимо выяснить:

- приобретал ли он на свое имя сим-карты с интересующими абонентскими номерами, если да, то когда и в каком офисе сотовой компании;

- где в настоящее время находятся сим-карты с интересующими абонентскими номерами (в случае если сим-карта находится при нем, необходимо произвести ее выемку);

- кто пользовался сим-картой в интересующий период времени (когда было совершено преступление);

- какими сотовыми телефонами пользовались в период совершения преступления и пользуются в настоящее время (указать марку, модель и IMEI-коды телефонных аппаратов);

- имеются ли среди родственников и знакомых свидетеля лица, ранее судимые, отбывающие наказание в местах лишения свободы, если да, то указать их полные данные, места, где они отбывают наказание;

- если свидетель никогда не оформлял на свое имя симкарту с абонентским номером, то терял ли свой паспорт, передавал ли его другим лицам, если да, то кому и с какой целью, кто мог использовать его паспортные данные для оформления симкарт.

Результаты допроса потерпевшего, свидетеля отражаются на последующем перечне следственных действий, необходимых для установления всех обстоятельств происшедшего (допросы свидетелей, осмотр предметов и документов, получение информации о соединениях между абонентами и (или) абонентскими устройствами, выемка предметов и документов, содержащих информацию о вкладах и счетах граждан в банках и иных кредитных организациях, осмотр и выемка электронных сообщений и иных передаваемых по сетям электросвязи сообщениях и др.).

2.5. Тактика получения информации о соединениях между абонентами и (или) абонентскими устройствами

В настоящее время одним из основных следственных действий при расследовании хищений, совершенных с использованием информационных-телекоммуникационных технологий, является получение информации между абонентами и (или) абонентскими устройствами.

Получение информации о соединениях между абонентами и (или) абонентскими устройствами позволяет установить сведения о соединениях абонентов в определенное время: о дате, времени, продолжительности, частоте, типе соединений между абонентами; о втором абоненте, с которым производилось соединение (абонентский номер, Ф.И.О., адрес регистрации, информация о его соединениях). Можно также определить абонентское устройство и местонахождение абонентов во время соединения (IMEI, сим-карта, номер и адрес базовой станции), установить маршрут движения абонента в определенный период времени.

Анализ данной информации позволяет установить способ связи с потерпевшим (телефонный звонок, СМС-сообщение

о списании денежных средств или блокировке карты), частоту и продолжительность общения в ходе телефонного звонка (может быть, потерпевший опознает в дальнейшем по голосу звонившего), маршрут передвижения потерпевшего к банкомату, фактическое местонахождение лица в определённый период времени, сведения о пополнении лицевого счета абонентского номера, список абонентов, которые потенциально могут обладать информацией о преступнике, и др.

Следователь может получить информацию о телефонных соединениях, истребовав от потерпевшего детализацию соединений, которую он мог самостоятельно получить в салонах связи. В этом документе будет содержаться информация о всех телефонных соединениях абонента по его абонентскому номеру за определенный период времени. На практике встречались ситуации, когда пострадавшие при самостоятельном обращении в офис оператора связи запрашивали сведения о соединениях за неполный период общения с преступниками, что осложняло установление времени совершения преступления.

В других случаях данная информация о телефонных соединениях устанавливалась при осмотре мобильного телефона. В мобильном телефоне может содержаться информация об абонентском номере преступника, периодичность и продолжительность телефонного разговора с ним, текстовые, голосовые сообщения и другая значимая информация. При осмотре мобильного телефона следователь может не получить необходимую информацию о соединениях, т.к. с течением времени часть информации удаляется.

Таким образом, достоверная и полная информация о входящих, исходящих звонках абонентского номера с указанием сведений о месте расположения базовых станций операторов сотовой связи, через которых обеспечивалось соединение указанного абонента с другими абонентами, с указанием IMEI абонентских устройств, посредством которых осуществлялись соединения, о движении денежных средств по счету абонентского номера, IMEI-номере устройства, в котором использовались сим-карты с определенными абонентскими номерами, других данных, позволяющих идентифицировать абонентов, в т.ч. IP-адресах устройства, используемого для совершения хищения,

следователем может быть получена только в рамках производства следственного действия как получение информации о соединениях между абонентами и (или) абонентскими устройствами (ст. 186.1 УПК РФ).

Производству данного следственного действия может предшествовать направление запросов оператору связи для предоставления сведений об анкетных данных лица, на имя которого оформлена сим-карта, лица, на абонентский номер (номера) которого перечислены денежные средства (Ф.И.О., дата рождения, адрес регистрации, паспортные данные, номер и дата договора об оказании услуг с приложением заверенной копии договора, IMSI-номер сим-карты, дата подключения сим-карты). Изучение следственной практики показало, что сроки исполнения запросов о владельце абонентских номеров, направленных в компании операторов сотовой связи, могут составлять 1-3 месяца. Даже при получении сведений о личных данных лица, на которого зарегистрирован абонентский номер, следователь не мог установить личность преступника, т.к. при совершении данных преступлений чаще всего преступники используют сим-карты, которые зарегистрированы на подставных лиц.

Подготовка к получению информации о соединениях между абонентами и (или) абонентскими устройствами предполагает изучение результатов следующих следственных действий: 1) допрос потерпевшего; 2) допрос свидетелей; 3) выемка и обыск; 4) осмотр предметов и документов. В протоколах этих следственных действий отображается важная информация об абонентских номерах, технических характеристиках абонентских устройств, что позволяет сформировать ходатайство перед судом о получении информации о соединениях между абонентами и (или) абонентскими устройствами.

Содержание постановления о возбуждении перед судом ходатайства о получении информации о соединениях между абонентами и (или) абонентскими устройствами определено частью 2 ст. 186.1 УПК РФ. В данном постановлении указываются: дата и наименование органа, принявшего решение о возбуждении уголовного дела, квалификации преступления; фабула уголовного дела, обстоятельства, подтверждающие необходи-

мость получения информации о соединениях между абонентами и (или) абонентскими устройствами; формулировка задачи производства следственного действия; сведения о номере абонента, абонентского устройства (пользовательского оборудования), приемо-передающей базовой станции и месте ее расположения; период, за который необходимо получить соответствующую информацию, и (или) срок производства данного следственного действия; наименование организации, от которой необходимо получить указанную информацию.

Кроме того, следует учитывать, что в зависимости от времени отображения информации в базе данных операторов связи относительно момента совершения преступления и проведения следственного действия (ст. 186.1 УПК РФ) информацию о соединениях между абонентами и (или) абонентскими устройствами можно разделить: 1) на информацию о телефонных соединениях, которые на момент расследования преступления хранились в базах данных операторов связи; 2) информацию о телефонных соединениях, которые могут состояться в будущем; 3) информацию о телефонных соединениях, сохранившихся в прошлом и которые предположительно должны продолжаться в будущем. Для получения каждого вида информации определен свой порядок производства данного следственного действия.

В пункте 3 ч. 2 ст. 186.1 УПК РФ указывается на необходимость установить «период, за который необходимо получить соответствующую информацию» и «срок производства данного следственного действия». Период всегда связан с событиями, которые имели место в прошлом. Для определения периода следователь должен проанализировать какое-либо событие и определить даты начала и окончания периода. Относительно срока производства рассматриваемого следственного действия необходимо отметить, что он не должен выходить за рамки срока предварительного расследования. Срок производства данного следственного действия не должен превышать шести месяцев. Производство данного следственного действия должно быть прекращено следователем, но не позднее окончания предварительного расследования.

Данное следственное действие может быть направлено для получения информации о соединениях по абонентскому номеру потерпевшего. Ранее у следователя не было возможности проанализировать информацию о базовых станциях, через которые осуществлялось соединение абонентов и абонентских устройств. Результат этого следственного действия позволяет уточнить технические характеристики абонентского устройства потерпевшего, его местонахождение в момент совершения преступления, а также установить все абонентские номера преступников для последующего получения детализации соединения по их абонентским номерам.

Информация о телефонных соединениях потерпевшего связана с событием преступления и отобразилась в прошлом. В этом случае обращение следователя к операторам связи будет носить разовый характер. В таком случае достаточно установить период, за который необходимо получить информацию о соединениях абонентов (дата, время и иные обстоятельства, относящиеся к совершенному преступлению). Срок проведения данного следственного действия определять не нужно.

При получении сведений об абонентском номере преступника необходимо также учитывать, что в настоящее время он может использовать различные способы сокрытия преступной деятельности путем изменения абонентского номера и (или) оператора связи. При обращении к соответствующим сайтам следователь имеет возможность самостоятельно установить предварительную информацию об актуальном операторе связи.

Получение информации о соединениях между абонентами и (или) абонентскими устройствами по абонентскому номеру преступника позволяет собрать информацию о лице, совершившем преступление. Этому способствует анализ документа, содержащего информацию о соединениях между абонентами и (или) абонентскими устройствами, в котором необходимо обратить внимание на детализацию соединений за продолжительный период времени, а также данные о способах пополнения лицевого счета абонентского номера сим-карты.

Детализация телефонных соединений мошенника определяется информацией о соединениях между абонентами и (или) абонентскими устройствами, которые уже состоялись в про-

шлом, и соединениями, которые возможны в будущем. Телефонные соединения между абонентами, которые состоялись в прошлом, – это соединения, которые непосредственно связаны с событием преступления. Кроме того, не следует исключать, что преступник в дальнейшем может продолжить использовать тот же абонентский номер, абонентское устройство для совершения других преступлений. Поэтому при производстве данного следственного действия у операторов связи также можно затребовать сведения о соединениях, которые могут состояться в будущем в течение трех месяцев. Таким образом, при получении информации о соединениях между абонентами и (или) абонентскими устройствами по абонентскому номеру преступника важно получить информацию как о телефонных соединениях, которые состоялись в прошлом, так и о тех, которые, возможно, будут.

Особо следует отметить случаи, когда следователю требуется получить информацию о соединениях, сохранившихся в прошлом, и которые предположительно должны продолжаться в будущем. Получение такой информации требует определить как срок производства данного следственного действия, так и период, за который необходимо получить соответствующую информацию от операторов связи.

Далее постановление согласовывается с руководителем следственного органа. К нему прилагаются: постановление о возбуждении уголовного дела; заявление о преступлении, явка с повинной и т.д.; иные материалы уголовного дела (копия протокола допроса потерпевшего (свидетеля), подозреваемого (обвиняемого), где указаны IMEI-номер абонентского устройства, абонентский номер сим-карты, данные абонента и другие сведения, касающиеся обстоятельств использования средств связи); копия документов, в которых указан IMEI-номер сотового телефона, и другие, которых должно быть достаточно, чтобы у суда не возникало сомнений в даче разрешения на проведение данного следственного действия.

Подписанное руководителем следственного органа постановление о возбуждении перед судом ходатайства с материалами, подтверждающими наличие фактических оснований принятия решения, следователем направляется в суд. В течение

24 часов с момента поступления указанного постановления следователя вместе с поступившими материалами должно быть рассмотрено судьей единолично в судебном заседании с участием прокурора и (или) следователя или без такового.

В случае принятия судом решения о получении информации о соединениях между абонентами и (или) абонентскими устройствами его копия направляется следователем в соответствующую организацию, осуществляющую услуги связи. К копии постановления суда прилагается сопроводительное письмо, в котором следователь должен указать способ обмена информацией, а также свою должность, фамилию, имя, отчество, контактный телефон и адрес, куда нужно направить ответ. Следователь может направить копию постановления суда в соответствующую организацию, осуществляющую услуги связи, любым способом, в т.ч. по почте, нарочным и т.д.

Результатом данного следственного действия является документ, содержащий информацию о соединениях между абонентами и (или) абонентскими устройствами, зафиксированную на любом материальном (бумажном или электронном) носителе. Операторы связи должны предоставлять следователю данные документы в опечатанном виде с сопроводительным письмом, где указываются период, за который она представлена, и номера абонентов и (или) абонентских устройств.

Действия следователя по осмотру содержания документа о соединениях между абонентами и (или) абонентскими устройствами будут складываться в зависимости от того, на каком материальном носителе была предоставлена информация операторами связи.

Если документ представлен организацией, осуществляющей услуги связи, на бумажном носителе, то осмотр данных объектов производится в соответствии с криминалистическими рекомендациями по тактике осмотра документов. В протоколе следственного действия фиксируется информация об упаковке, реквизитах документа, а также та часть информации, которая, по мнению следователя, имеет отношение к уголовному делу.

Осмотр информации, содержащейся на электронном носителе, следователь производит с помощью компьютерной техники. Если объем документа небольшой, то его следует полностью распечатать на принтере. Обычно операторы связи предостав-

ляют электронный носитель в случае, если объем содержащейся в нем информации является значительным. Для удобства изучения электронного документа на принтере распечатывается та часть информации о соединениях между абонентами и (или) абонентскими устройствами, которая, по мнению следователя, имеет отношение к уголовному делу. Следует отметить, что к материалам уголовного дела приобщается не только распечатанный фрагмент текста на бумажном носителе, но и электронный носитель, предоставленный операторами связи. Распечатанный на бумажном носителе документ подвергается анализу и описанию в протоколе следственного действия.

В статье 186.1 УПК РФ определено, что осмотр документов производится для отражения информации о дате, времени, продолжительности соединений между абонентами и (или) абонентскими устройствами, номерах абонентов и других данных.

Анализ правоприменительной практики позволил сделать вывод, что большинство следователей осматривают получаемый от операторов связи документ с целью акцентирования внимания на определенной информации, имеющей значение для уголовного дела, для удобства ознакомления с соответствующей частью данного документа.

В протоколе осмотра документа, содержащего информацию о соединениях между абонентами и (или) абонентскими устройствами, следователь указывает: наименование организации, представившей информацию; состояние и обозначение упаковки; материал, из которого изготовлен носитель; размеры, цвет, внешний вид, идентификационные сведения; дату и время соединений; признак исходящего или входящего вызова абонента; номер абонента (кому или кто звонил) или уникальный код идентификации; продолжительность соединения в секундах, сведения об абоненте из базы данных систем расчета за оказанные услуги связи, в т.ч. и о платежах абонента, информацию о номерах и месте расположения приемо-передающих базовых станций и др.[1]

[1] Васюков В.Ф. Возможности использования информации об абонентской активности лиц, подозреваемых в совершении преступлений // Вестник Академии генеральной прокуратуры Российской Федерации. 2016. № 2 (52). С. 66-70.

После осмотра все объекты заново упаковывают в бумажный конверт, на котором производится пояснительная записка, конверт опечатывают бумажной биркой, и участвующие лица проставляют на нем свои подписи. В протоколе следственного действия фиксируются технические средства, которые использовались для просмотра и распечатывания информации о соединениях между абонентами и (или) абонентскими устройствами на бумажном носителе, а также все действия, произведенные с документами.

Статья 186.1 УПК РФ устанавливает, что представленные документы, содержащие информацию о соединениях между абонентами и (или) абонентскими устройствами, в полном объеме приобщаются к материалам уголовного дела на основании постановления следователя как вещественное доказательство.

В протоколе осмотра документа, содержащего информацию о телефонных соединениях, следователь определяет доказательственное значение определенной части информации о соединениях между абонентами и (или) абонентскими устройствами и использует их для установления обстоятельств совершенного преступления.

Анализ документа, содержащего информацию о телефонных соединениях между абонентами, поможет выяснить следующие обстоятельства: местонахождение мошенника в момент совершения преступления и его дальнейшие перемещения (другой регион), выбор жертв путем подбора номера телефона, сколько у него смартфонов, сим-карт, как часто меняет абонентские номера, IP-адрес, используемый для входа в личный кабинет абонента, и др.

Результаты такого осмотра документа сопоставляются с совокупностью других доказательств. Они могут быть отражены в постановлениях о привлечении в качестве обвиняемого, о прекращении уголовного дела (уголовного преследования), при составлении обвинительного заключения.

В процессе расследования преступлений возможно дальнейшее использование полученной информации о соединениях между абонентами и (или) абонентскими устройствами во время производства других следственных действий, таких как обыск, выемка, осмотр, с целью обнаружения и изъятия сим-карт, мо-

бильных телефонов, коробок от мобильных телефонов, черновых записей, содержащих список номеров.

Если для пополнения баланса преступниками использовался электронный кошелек отечественной платежной системы («Яндекс.Деньги») или банковские карты, эмитированные отечественными банками, то последующие запросы необходимо направить этим субъектам для предоставления сведений о том, кто является владельцем электронного кошелька либо кто является клиентом (держателем) счета банковской карты[1].

Тактические особенности использования осмотра документа, содержащего информацию о телефонных соединениях между абонентами, могут быть использованы следователем при дальнейшем расследовании в качестве основания для повторного производства тех или иных следственных действий, в т.ч. и тех, которые до этого по делу не проводились. После получения информации о соединениях между абонентами и (или) абонентскими устройствами нередко следует повторение данного следственного действия, но уже относительно новых, выявленных в ходе первого, обстоятельств (по иным номерам и абонентам)[2].

Возможность дальнейшего использования результатов рассматриваемого следственного действия в качестве доказательств зависит от вида информации, запрашиваемой от оператора связи, и ее содержания. Степень точности запрашиваемых сведений о телефонных соединениях между абонентами оказывает несомненное влияние на выводы следователя. Изучая результаты следственного действия, следователь делает выводы о том, в какое время в каком месте какой абонент пользовался мобильным телефоном. Правильные выводы формируются в совокуп-

[1] Гаврилин Ю.В., Аносов А.В., Баранов В.В. и др. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учеб. пособие. В 2 ч. М.: Академия управления МВД России, 2019. Ч. 1. 208 с.

[2] Скобелин С.Ю. Расширение границ следственного действия в виде получения информации о соединениях между абонентами // Расследование преступлений: проблемы и пути их решения. 2019. № 4 (26). С. 117.

ности с другими доказательствами, которые имеются в материалах уголовного дела.

Необходимо отметить, что процесс формирования выводов по результатам осмотра документа, содержащего информацию о соединениях между абонентами и (или) абонентскими устройствами, не оканчивается по завершении его осмотра, а продолжается на протяжении всего расследования, в ходе которого результаты поочередно сопоставляются с другими доказательствами по мере их получения.

Следует отметить, что при расследовании хищений, совершаемых с использованием информационно-телекоммуникационных технологий, при получении информации о соединениях между абонентами и (или) абонентским устройствами следователи сталкиваются с различными проблемами: лица, совершающие преступления в данной сфере, продолжают использовать неидентифицируемые технические средства; операторы связи несвоевременно предоставляют истребимую информацию; следователи не располагают достаточным количеством времени, необходимого для анализа документа, содержащего информацию о соединениях между абонентами и (или) абонентским устройствами.

Вопросы для самоконтроля:

1. Назовите основные действия следователя, направленные на установление суммы ущерба, осуществляемые в ходе проверки сообщения о преступлении.
2. Перечислите особенности тактики производства осмотра места происшествия по факту хищения электронных денежных средств, совершенных с использованием информационно-телекоммуникационных технологий.
3. Раскройте основные вопросы, которые подлежат выяснению при допросе потерпевшего.
4. Какие документы, имеющие значение для уголовного дела, могут быть изъяты у потерпевшего?
5. Какие трудности возникают при получении информации о соединениях между абонентами и (или) абонентскими устройствами?

Литература

1. Архипова Н.А. Особенности тактики допроса потерпевшего в ходе расследования мошенничеств, совершенных в сфере информационно-телекоммуникационных технологий // Актуальные проблемы борьбы с преступлениями и иными правонарушениями: мат-лы 20-й междунар. научно-практ. конф-ции. Барнаул: БЮИ МВД России, 2022. С. 200-201.

2. Архипова Н.А. Получение информации о соединениях между абонентами и (или) абонентскими устройствами при расследовании хищений, совершаемых с использованием информационно-телекоммуникационных технологий // Вестник Дальневосточного юридического института МВД России. 2022. № 4. С. 84-88.

3. Бердникова О.П., Дерюгин Р.А. Особенности расследования мошенничества в сфере компьютерной информации: учеб. пособие. Екатеринбург: Уральский юрид. ин-т МВД России, 2021. 84 с.

4. Гаврилин Ю.В., Аносов А.В., Баранов В.В. и др. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учеб. пособие. В 2 ч. М.: Академия управления МВД России, 2019. Ч. 1. 208 с.

5. Гаврилин Ю.В., Гаспарян Г.З. Расследование хищений денежных средств, совершенных с использованием информационных банковских технологий: учеб. пособие. М.: Проспект, 2021. 128 с.

6. Голятина С.М. Криминалистическая теория и практика расследования хищений электронных денежных средств: монография / под науч. ред. А.П. Алексеевой. Волгоград: ВА МВД России, 2021. 184 с.

7. Раскрытие и расследование преступлений, совершаемых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации: учеб. пособие / С.В. Петраков, А.Ю. Ушаков, А.А. Попов [и др.]. СПб.: Изд-во Санкт-Петербургской академии Следственного комитета РФ, 2021. 92 с.

8. Тактические особенности производства отдельных следственных действий: учеб. пособие / под общ. ред. О.В. Кругликовой. Барнаул: БЮИ МВД России, 2021. 116 с.

9. Ушаков А.Ю., Саакян А.Г., Поздышев Р.С. и др. Особенности квалификации и расследования хищений электронных денежных средств, в том числе совершенных посредством использования информационно-телекоммуникационных сетей: учеб. пособие. Н. Новгород: Нижегородская академия МВД России, 2022. 61 с.

10. Эткина А.Д. Актуальные вопросы определения места совершения киберпреступления // Трансформация права в информационном обществе: мат-лы I Всерос. научно-практ. форума молодых ученых и студентов. Екатеринбург: Уральский гос. юрид. ун-т, 2019. С. 125-130.

11. Янгаева М.О. Особенности изъятия электронных носителей информации при расследовании преступлений // Актуальные проблемы борьбы с преступлениями и иными правонарушениями: мат-лы 18-й междунар. научно-практ. конф-ции. Барнаул: БЮИ МВД России, 2020. С. 76-77.

Глава 3. Особенности последующего этапа расследования хищений, совершенных с использованием информационно-телекоммуникационных технологий

3.1. Тактика производства обыска

Последующий этап расследования хищений, совершенных с использованием информационно-телекоммуникационных технологий, характеризуется деятельностью следователя, направленной на доказывание виновности преступника, подтверждение имеющихся доказательств, выявление дополнительных эпизодов преступной деятельности, обеспечение возмещения вреда, причиненного преступлением.

Следователь на этом этапе допрашивает ранее не допрошенных свидетелей, назначает судебные экспертизы, проводит обыск и выемку, предъявление для опознания и другие следственные действия.

Рассмотрим особенности производства обыска, т.к. в процессе указанного следственного действия собираются предметы и документы, имеющие доказательственное значение.

Следует отметить, что при совершении хищений с использованием информационно-телекоммуникационных технологий преступники активно обращаются к развивающимся в обществе услугам банковских и платежных систем, интернет-магазинов, мессенджеров, SIP-телефонии, различным аппаратным и программным средствам. Для достижения преступного результата они используют: компьютерную технику; электронные носители информации, смартфоны, банковские карты; флеш-карты; документы и другие предметы.

Сбор сведений о пользовании преступниками указанными устройствами и установление их местонахождения являются необходимой мерой при расследовании всех хищений, совершаемых в рассматриваемой сфере. Поэтому по данной категории дел обыск является следственным действием, который направлен на поиск объектов, имеющих значение как для установления обстоятельств преступления, так и для поиска и задержания ли-

ца, совершившего преступление. Необходимость производства обыска объясняется тем, что другими средствами получить доказательства просто невозможно.

Каждое преступление имеет свои индивидуальные особенности, однако в действиях преступников, совершающих хищения с использованием ИТТ, есть много общего. Они уверены, что используют продуманный арсенал действий по сокрытию следов совершенных преступлений, который не известен правоохранительным органам. Поэтому производство обыска для этих лиц всегда будет неожиданным. Изучение следственной практики может помочь следователю тщательно подготовиться к обыску и не допустить негативного результата проведенного следственного действия, потому что способы совершения, сокрытия следов в этих преступлениях схожи.

Подготовка к производству обыска состоит из разнообразных организационных мероприятий, подлежащих разрешению еще до выезда к месту производства следственного действия. Следует отметить, что по результатам изучения материалов уголовных дел можно сделать вывод, что обыск часто производился по месту жительства или пребывания обыскиваемого лица, расположенного за пределами места производства предварительного расследования, т.к. такие преступления носят межрегиональный и межнациональный характер. Это обстоятельство, несомненно, сказывается на особенностях подготовки следователя к производству данного следственного действия.

Подготовительные мероприятия до выезда к месту производства обыска включают в себя: изучение материалов уголовного дела и результатов оперативно-розыскной деятельности; сбор сведений о месте производства обыска (точный юридический адрес, пути подхода и проникновения); получение информации о личности обыскиваемого (является ли он участником организованной группы, имеет ли специальные знания в какой-либо сфере, необходимые для совершения преступления); интернет какого провайдера использует; возможные способы изъятия компьютерной информации (копирование на собственные энергонезависимые носители информации, изъятие только компьютерной техники и пр.); перечень поисковых технико-криминалистических средств; определение времени начала

обыска; определение порядка прибытия группы к месту проведения обыска; инструктаж сотрудников, которые будут принимать участие в проведении обыска, в ходе которого довести тактику его проведения.

В подготовке и производстве данного следственного действия немаловажную роль играет взаимодействие следователя с сотрудниками оперативно-розыскных подразделений. Это взаимодействие необходимо, прежде всего, в решении задач по оперативному сопровождению обыска.

Сложность обыска по делам этой категории состоит в некоторой неопределенности поисковых действий по отысканию нужных предметов и документов. Чаще всего предметом преступного посягательства по хищениям, совершенным с использованием ИТТ, являются безналичные и электронные денежные средства, которые, как правило, не хранят в своем жилище преступники. Похищенными денежными средствами преступники распоряжаются путем перевода на другую банковскую карту или электронный кошелек, снятия посредством банкомата, покупки различных товаров в интернет-магазинах.

В связи с этим в ходе обыска необходимо осуществлять действия, направленные на поиск и изъятие компьютерного устройства, посредством которого осуществлялся выход в интернет, электронных носителей информации, в памяти которых содержится информация о событии преступления, различные документы (договоры об оказании услуг связи в сети Интернет, документы, отражающие движение денежных средств, документы, удостоверяющие личность, об образовании и квалификации подозреваемого лица, а также записные книжки, черновые записи, скрипты).

Например, *при расследовании мошенничества, совершенного организованной группой, в ходе обыска были изъяты: смартфоны, сим-карты, банковские карты, пластиковые карты от сим-карт, ноутбуки, переносной аккумулятор, роутеры, заявления на получение банковских карт, заявление об открытии сберегательного счета и предоставлении потребительского кредита, заявления о предоставлении расчетной (дебетовой) карты, заявление на получение моментальной платежной карты в банке, товарные чеки, кассовые чеки о зачислении денежных*

средств на счет банковской карты, печать в пластиковом корпусе, картонные конверты с банковскими картами, конверты с ПИН-кодами для банковских карт, договоры на оказание услуг связи по абонентским номерам, договор аренды нежилого помещения, коробки от мобильных телефонов, картонная упаковка от сим-карты и др.[1]

Готовясь к обыску, необходимо выяснить паспортные данные обыскиваемого, абонентские номера, ICCID-номера симкарт, IMEI смартфонов, технические характеристики компьютерной техники, IP-адрес, MAC-адрес, адрес электронной почты, реквизиты банковских карт и др. Обнаружение, фиксация и изъятие данных объектов возможны с участием специалиста в сфере информационных технологий.

К производству указанного следственного действия могут привлекаться сотрудники ЭКЦ, специализирующиеся на производстве компьютерных экспертиз, или сотрудники Центра информационных технологий, связи и защиты информации (ЦИТС и ЗИ) ГУ МВД России по субъектам Российской Федерации. В исключительных случаях следует привлекать к участию в обысках иных лиц, имеющих основное или дополнительное образование в сфере информационных технологий.

Таким образом, подготовка к обыску способствует эффективной организации следственного действия и получению в дальнейшем ценных доказательств, помогающих раскрытию и расследованию такого преступления.

Анализ материалов уголовных дел позволяет рекомендовать следующие меры тактического характера при производстве обыска, связанного с обнаружением и изъятием технических устройств, используемых при совершении рассматриваемых хищений.

Прибытие к месту производства обыска должно быть внезапным, не оставляющим обыскиваемым время на уничтожение предметов и документов с хранящейся в них важной информацией. Далее следователь предъявляет постановление о производстве обыска либо решение суда, разрешающее его производ-

[1] Приговор Железнодорожного районного суда г. Барнаула № 1-93/2020 от 28 июля 2020 г. по делу № 1-93/2020. URL: https://sudact.ru.

ство. В ходе обыска присутствующим разъясняются их права и обязанности, они уведомляются о применении технических средств. Участникам предлагается добровольно выдать искомые предметы и документы. Обыскиваемый может отказаться это сделать либо выдать не все требуемое, но следователю в любом случае следует организовать поисковые мероприятия при производстве обыска.

В начале производства обыска целесообразно провести личные обыски всех присутствующих в помещении лиц для обнаружения находящихся у них смартфонов и иных средств хранения информации. Личный обыск позволяет отыскать предметы и документы, спрятанные на теле, в одежде, обуви и иных предметах. Прощупывание одежды производится в присутствии обыскиваемого, которому предъявляется результат поисковых действий. В необходимых случаях он даёт пояснения по поводу обнаруженных предметов и документов.

В ходе поисковых действий, особенно связанных с обнаружением электронных носителей информации, необходимо организовать наблюдение за поведением обыскиваемого и других присутствующих. Один из членов группы обыска производит наблюдение за его действиями и незаметно, заранее обусловленным способом, обращает внимание на объекты, которые нуждаются в дополнительном обследовании.

Следует помнить, что приближение к отыскиваемому объекту не может не сказаться на поведении обыскиваемого, так же как и удаление от него. Следователь должен учитывать попытки обыскиваемого лица сорвать или приостановить обыск. Желательно установить с обыскиваемым так называемый речевой контакт, как можно активнее включать его в беседу. На месте обыска следует устанавливать строгую дисциплину, запрещать все посторонние разговоры, ненужное хождение[1].

Учитывая стрессовое состояние лиц, у которых проводится обыск, необходимо принять меры по добровольному получению от них паролей доступа к ресурсам электронно-вычислительной техники. Обнаруженные в ходе обыска предметы и документы

[1] Набиев А.З. Некоторые тактические проблемы производства обыска // Молодой ученый. 2015. № 3 (83). С. 660-661. URL: https://moluch.ru/archive/83/15491/

содержат важную информацию об IMEI-номере мобильного телефона, журнале вызовов мобильного устройства, внутренней памяти мобильного устройства или сим-карты, а также тексты сообщений (в т.ч. и голосовые сообщения) между соответствующими абонентами, объявления о продаже товаров, недвижимости, вакансии интернет-сервисов, истории посещений интернет-сайтов и др. На наш взгляд, изучение содержания мобильных устройств при производстве обыска должно быть в необходимых объёмах, обеспечивающих оперативное пресечение преступления или предотвращение возможного уничтожения доказательств.

Кроме того, в обязательном порядке с целью избежать повторного проведения обыска следует установить наличие и изъять сетевое оборудование беспроводного доступа (Wi-Fi-роутер), т.к. при последующем исследовании протоколов работы (log-файлов) в сети будет указан MAC-адрес беспроводного сетевого оборудования; базы от сим-карт (пластиковая рамка, из которой извлекается сим-карта перед установкой). Как правило, при производстве обысков базы от сим-карт не изымаются, хотя на них содержится ICCID – уникальный серийный номер сим-карты, по которому можно идентифицировать ее абонентский номер. При производстве обыска могут быть изъяты документы на приобретение движимого и недвижимого имущества (необходимы для последующего наложения ареста на данное имущество; свободные образцы почерка и подписи, содержащиеся в письмах, личных дневниках, рукописных договорах, записных книжках; похищенные денежные средства, приобретенные с их помощью товары, документы и предметы, свидетельствующие о месте хранения похищенных денежных средств и товаров (пластиковые карты, товарные и кассовые чеки, выписки движения денежных средств по счетам, ключи от камер хранения и банковских ячеек, квитанции о денежных переводах); фотографии, видеозаписи (особенно важно их изъятие при расследовании преступлений, совершенных организованными группами в целях доказывания наличия устойчивых межличностных связей между их участниками); иные предметы и документы, имеющие

значение для установления обстоятельств совершенного преступления[1].

Важным является соблюдение криминалистических требований при работе с обнаруженными предметами и документами на месте обыска. Понятым и другим лицам, присутствующим при обыске, данные предметы предъявляются, после чего они упаковываются и опечатываются. При производстве обыска в протоколе указываются: место, обстоятельства обнаружения и изъятия предметов и документов. Все изымаемые предметы должны быть перечислены с точным указанием их названия, серийных номеров, функционального состояния устройств, а также информации, содержащейся на мониторе.

При обнаружении включенной компьютерной техники необходимо проверить соответствие текущей даты и времени с установленными датой и временем в момент обыска; если в компьютерном устройстве установлено наличие криптоконтейнеров и возможность доступа к облачным хранилищам, то необходимо осмотреть информацию и скопировать ее; извлечь из компьютерного устройства энергонезависимые носители информации (флеш-накопители, карты памяти, оптические носители информации и т.п.).

При изъятии мобильных устройств необходимо следовать рекомендациям, направленным на предотвращение их разряжения. При последующем выключении устройства может потребоваться применение пароля, а также эти действия могут привести к уничтожению криминалистически значимой информации. Необходимо перевести устройство в режим «автономная работа» или режим «полет».

Следователи и сотрудники оперативных подразделений могут допускать ошибки при изъятии вышеуказанных объектов: их изъятие производится без использования технических средств фиксации, не устанавливаются сведения о паролях, защищающие устройства, логинах и паролях личного кабинета различных

[1] Ушаков А.Ю. Особенности производства обыска при расследовании преступлений, совершаемых с использованием современных электронных технологий // Противодействие киберпреступлениям и преступлениям в сфере высоких технологий: мат-лы Всерос. научно-практ. конф-ции. М., 2021. С. 145-149.

приложений обыскиваемого лица, упаковка изъятого устройства должна быть непрозрачной, не позволяющей производить непроцессуальные действия.

Таким образом, в ходе расследования хищений, совершенных с использованием ИТТ, обыск требует тщательной подготовки, нацеливает на применение особых тактических приёмов и специальных знаний в области информационных технологий.

3.2. Тактика осмотра и выемки электронных сообщений или иных передаваемых по сетям электросвязи сообщений

Содержание электронных сообщений или иных сообщений, передаваемых по сетям электросвязи, подлежит осмотру и выемке следователем после получения судебного решения (ч. 7 ст. 185 УПК РФ). Введением данной нормы законодатель конкретно определил способ получения содержания электронных сообщений. У органов, осуществляющих предварительное расследование, появился дополнительный источник получения доказательств.

Согласно ч. 7 ст. 185 УПК РФ, «при наличии достаточных оснований полагать, что сведения, имеющие значение для уголовного дела, могут содержаться в электронных сообщениях или иных передаваемых по сетям электросвязи сообщениях, следователем по решению суда могут быть проведены их осмотр и выемка».

Анализ понятия «электронные сообщения или иные сообщения, передаваемые по сетям электросвязи» позволяет сделать вывод, что в рассматриваемом случае речь идет не только об электронных сообщениях как носителях информации, переданных или полученных пользователями по информационно-телекоммуникационной сети, но и о других сообщениях, которые пользователь мобильного абонентского устройства отсылает СМС-, EMS-, MMS-сообщениями, через приложения для мобильных операционных систем (мессенджеры), сообщения, пересылаемые посредством электронной почты, и др.

Согласно федеральному закону от 7 июля 2003 г. № 126[1] и постановлению Правительства РФ от 9 декабря 2014 г. № 1342[2], оператор связи – это «юридическое лицо или индивидуальный предприниматель, оказывающие услуги связи на основании соответствующей лицензии».

Кроме того, федеральным законом «Об информации, информационных технологиях и о защите информации» введена новая категория – «организатор распространения информации в сети Интернет», под которым понимается «лицо, осуществляющее деятельность по обеспечению функционирования информационных систем и (или) программ для электронных вычислительных машин, которые предназначены и (или) используются для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети Интернет», например, «ВКонтакте», «Одноклассники» и т.д.

Согласно федеральному закону от 6 июля 2016 г. № 374-ФЗ[3], которым были внесены изменения в федеральные законы[4], на организаторов распространения информации в сети Интернет и операторов связи возлагаются обязанности хранить на территории Российской Федерации текстовые сообщения пользователей услугами связи, голосовую информацию, изображения, звуки, видео-, иные сообщения пользователей услуга-

---

[1] О связи [Электронный ресурс]: федеральный закон от 7 июля 2003 г. № 126. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] О порядке оказания услуг телефонной связи [Электронный ресурс]: постановление Правительства РФ от 9 декабря 2014 г. № 1342. Доступ из справ.-правовой системы «КонсультантПлюс».

[3] О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности [Электронный ресурс]: федеральный закон от 06.07.2016 № 374-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

[4] О связи [Электронный ресурс]: федеральный закон от 7 июля 2003 г. № 126; Об информации, информационных технологиях и защите информации [Электронный ресурс]: федеральный закон от 27 июля 2006 г. № 149. Доступ из справ.-правовой системы «КонсультантПлюс».

ми связи, а также текстовые сообщения пользователей сети Интернет, голосовую информацию, изображения, звуки, видео-, иные электронные сообщения пользователей сети Интернет до шести месяцев с момента окончания их приема, передачи, доставки и (или) обработки. Изменения вступили в силу с 1 июля 2018 г. Таким образом, можно сделать вывод, что при реализации рассматриваемой нами нормы источником получения электронных или иных сообщений, передаваемых по сетям электросвязи, для следователей могут быть организаторы распространения информации в сети Интернет и операторы связи.

Однако внесенные в ст. 185 УПК РФ положения об осмотре и выемке электронных и иных сообщений, передаваемых по сетям электросвязи, создают сложности для органов предварительного расследования в ее реализации. Так, для проведения осмотра и выемки электронных сообщений должны учитываться форма и содержание следственного действия «наложение ареста на почтово-телеграфные отношения, их осмотр и выемка».

В связи с этим практически сразу обозначились проблемы, связанные с проведением данного следственного действия, при выборе тактики его производства. Тактика следственного действия включает определенные этапы: а) подготовку к проведению следственного действия (подготовительный этап); б) проведение следственного действия (рабочий этап); в) фиксацию хода и результатов следственного действия (заключительный этап); г) оценку полученных результатов проведенного следственного действия. Теперь рассмотрим содержание тактических приемов на каждом этапе осмотра и выемки электронных и иных сообщений, предаваемых по сетям электросвязи.

В ходе подготовки к производству осмотра и выемки электронных сообщений следователь изучает материалы уголовного дела с целью определения фактических оснований для проведения данного следственного действия, которыми являются обстоятельства, указывающие на наличие достаточных данных о том, что в содержание данных электронных сообщений могут быть включены сведения, представляющие интерес для уголовного дела. Фактические основания могут содержаться в протоколах следственных действий (допросов потерпевших, свидетелей, подозреваемых, специалистов, осмотра предметов и докумен-

тов), заключениях экспертов и иных материалах уголовного дела. Анализ материалов уголовного дела целесообразно проводить в тесном взаимодействии с оперативными работниками органов дознания. В рамках такой совместной деятельности оперативными сотрудниками могут быть выяснены сведения о лице, чьи электронные сообщения предполагается осмотреть и изъять, вид электронных сообщений, объем изымаемых сообщений, адрес расположения операторов связи и организаторов распространения информации в сети Интернет. Для получения информации о факте направления и пересылке данных сообщений следователь вправе провести следственное действие, регламентированное ст. 186.1 УПК РФ.

При подготовке к данному следственному действию следователю приходиться взаимодействовать с руководителем следственного органа, с согласия которого возбуждается перед судом ходатайство об осмотре и выемке электронных сообщений или иных сообщениях, передаваемых по сетям электросвязи, о чем выносится постановление. В ходатайстве следователю необходимо отразить обстоятельства, дающие основание для производства данного следственного действия, фамилию, имя, отчество лица, чьи электронные сообщения будут подлежать осмотру и выемке, вид электронного сообщения, наименования операторов связи и организаторов распространения информации в сети Интернет и их юридические адреса расположения.

Подписанное руководителем следственного органа постановление совместно с копиями материалов уголовного дела, подтверждающих необходимость проведения данного следственного действия, направляется в суд. По результатам рассмотрения представленных материалов судья выносит постановление, разрешающее или отказывающее в проведении данного следственного действия.

Рабочая стадия осмотра и выемки начинается с непосредственного прибытия следователя по адресу расположения организатора распространения информации в сети Интернет либо оператора сотовой связи, где предъявляет постановление о производстве рассматриваемого следственного действия представителям службы безопасности данной организации. Они оказывают содействие следователю по обнаружению интересующих

следствие электронных сообщений, применение соответствующих тактических приемов может активизировать работу данных лиц. В протоколе следственного действия описываются отобранные электронные сообщения (вид сообщения, время получения, содержание и т.д.).

Проведенный анализ содержания ч. 7 ст. 185 УПК РФ позволяет сделать вывод, что после осмотра электронных сообщений следует проводить их выемку. Проведение выемки как самостоятельного следственного действия предполагает соблюдение требований Уголовно-процессуального кодекса РФ. В соответствии со ст. 183 УПК РФ при производстве выемки изъятие электронных носителей информации должно производиться с участием специалиста. С учетом специфики проведения данного следственного действия специалистом может выступать работник организации, занимающийся распространением информации в сети Интернет, или оператора связи, который поможет произвести копирование на материальный носитель.

В ходе осмотра и выемки электронных сообщений на следователя возлагается обязанность предупредить участников следственного действия о неразглашении выявленных в ходе выемки обстоятельств частной жизни лица, чьи электронные сообщения изымаются, его личной и семейной тайны, а также сведений о частной жизни других лиц. По результатам осмотра и выемки электронных сообщений необходимо произвести протоколирование данного следственного действия в соответствии со ст. 185 УПК РФ.

В научной литературе указывается мнение о том, что осмотр и выемка электронных сообщений – это два самостоятельных следственных действия, проведение которых предполагает составление двух соответствующих протоколов. По нашему мнению, проведение осмотра электронных сообщений – это необходимое действие, которое позволяет следователю определиться с объемом тех электронных сообщений, которые имеют значение для уголовного дела. Однако на изучение содержания всех сообщений может потребоваться продолжительное время, привлечение соответствующих специалистов и иных участников, поэтому данное следственное действие будет осуществлено недостаточно эффективно. В то же время проведение выемки

предполагает предварительный осмотр изымаемых предметов, документов, сведений и их описание в протоколе данного следственного действия. Таким образом, мы считаем допустимым проведение выемки электронных сообщений, передаваемых по сетям электросвязи, оформив результаты данного следственного действия одним протоколом. Подробный осмотр изъятых сообщений можно будет произвести позже в соответствии с ч. 3 ст. 177 УПК РФ. Указанная норма позволяет следователю производить осмотр предметов и документов, обнаруженных в ходе следственного действия не только в месте производства следственного действия, но и по месту производства предварительного расследования. Таким образом, у следователя будет возможность более подробно ознакомиться с изъятыми электронными и иными сообщениями с целью получения сведений о переписке абонентов, в которых указываются особенности способа совершения преступления, причастность конкретных лиц и другие сведения о событии преступления.

Эта достаточно простая процедура при ее реализации может сопровождаться сложностями, которые могут возникнуть ввиду отсутствия должного взаимодействия правоохранительных органов с операторами связи и организаторами распространения информации в сети Интернет при получении рассматриваемой информации. Кроме того, в ст. 185 УПК РФ указывается на то, что следователю требуется непосредственно прибыть в учреждение связи для проведения осмотра и выемки почтово-телеграфных отправлений, на которые был наложен арест. Для осмотра и выемки электронных сообщений следователю также необходимо прибыть в интересующие организации. Однако организаторы распространения информации в сети Интернет могут находиться в других регионах или за пределами Российской Федерации.

В этих ситуациях возможно в соответствии с п. 4 ч. 2 ст. 38 УПК РФ направить поручение о проведении данного следственного действия совместно с судебным решением оперативным подразделениям с целью его проведения. Однако в электронных сообщениях могут содержаться сведения, относящиеся к личной, семейной и иной охраняемой законом тайне, в т.ч. и к интимной стороне жизни. В связи с этим важно не допустить рас-

пространения сведений, полученных в ходе следственного действия, а также внесения каких-либо изменений в их содержание. Поэтому следователю важно устанавливать взаимодействие с оперативными работниками, добиваясь безусловного и точного выполнения органом дознания письменных поручений и требований следователя при производстве данного следственного действия.

Таким образом, введение в ст. 185 УПК РФ части 7 определило порядок получения содержания электронных и иных сообщений, предаваемых по сетям электросвязи. У следователей появился новый источник доказательственной информации. Однако при наличии обозначенных пробелов в законодательстве вряд ли удастся реализовать весь потенциал данной нормы и не допустить нарушений конституционных прав и свобод граждан.

3.3. Тактика назначения судебных компьютерных экспертиз

Расследование практически любого преступления, совершенного с использованием информационно-телекоммуникационных технологий, не обходится без производства экспертиз.

Приказ МВД России от 29 июня 2005 г. № 511 «Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации» содержит приложение № 2, в котором определен перечень родов (видов) судебных экспертиз, производимых в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации, в число которых входит компьютерная экспертиза.

Обычно судебная компьютерная экспертиза назначается следователем после того, как произведены осмотр места происшествия, предметов и документов, обыск, выемка, но информации для дальнейшего расследования недостаточно.

Цель компьютерной экспертизы – изучение закономерностей функционирования информации в средствах вычислительной техники.

Задачи компьютерной экспертизы:

- обеспечение доступа к информации, содержащейся в компьютерах и на носителях компьютерной информации;
- определение назначения и функциональных возможностей программного обеспечения и компьютерных устройств;
- выявление действий, произведенных с компьютером, и хранящейся на нем компьютерной информации.

Объекты компьютерной экспертизы:

- комплекты ЭВМ в сборе и их системные блоки;
- мобильные ЭВМ: ноутбуки, нетбуки, планшетные ЭВМ;
- носители информации: жесткие магнитные диски, флеш-накопители, флеш-карты, флоппи-диски, оптические диски, магнитооптические диски, магнитные ленты и др.;
- информация (файлы): исполняемые файлы вредоносных программ или программные средства скрытого информационного воздействия, «зеркальные» копии машинных носителей информации и др.;
- периферийные устройства: мониторы, принтеры, дисководы, модемы, клавиатуры, сканеры, манипуляторы и др.;
- коммуникационные устройства ЭВМ и вычислительных сетей: коммутаторы, маршрутизаторы, Wi-Fi-адаптеры и др.;
- мобильные телефонные аппараты сотовой связи.

Вопросы, выносимые на разрешение компьютерной экспертизы, должны удовлетворять следующим **требованиям:**

1) при постановке вопроса необходимо использовать нормативно определенный понятийный аппарат, исключающий сленговые, жаргонные термины (для этого необходимо обратиться к ГОСТам);

2) в случае отсутствия нормативного определения того или иного термина необходимо применять терминологию, используемую разработчиками аппаратных средств и программных продуктов в технической документации, но лучше согласовать этот нюанс со специалистом, который будет проводить исследование;

3) вопрос должен быть четко сформулирован и не допускать неоднозначного толкования;

4) вопросы не должны носить правового характера, т.е. быть направленными на правовую оценку деяния, а также выхо-

дить за пределы компетенции эксперта, т.е. его специальных знаний[1];

5) сформулированные вопросы не должны содержать ошибок (логических, грамматических, синтаксических, речевых и др.);

6) формулируя вопрос, правильнее спрашивать о наличии данных (информации, следов) об осуществлении какой-либо деятельности, а не о факте осуществления этой деятельности.

Не следует задавать вопросов:

- подразумевающих юридическую квалификацию деяния (это должны делать следователи, дознаватели, прокуроры и судьи) (например, «Является ли программа вредоносной?»);

- требующих привлечения эксперта по иной специальности (например, «Имеется ли на носителе конфиденциальная информация или информация, составляющая государственную тайну?»);

- требующих воспроизведения больших объемов информации (например, «Какие файлы находятся на машинном носителе?», «Какое программное обеспечение установлено на компьютере?»);

- на которые в принципе нельзя дать однозначного ответа и ответы на которые могут быть получены другим процессуальным путем, в т.ч. с использованием свидетельский показаний (например, «Удалялась ли информация с машинного носителя? Если да, то какая?», «Является ли автором данного документа конкретное лицо?»).

Наиболее распространенными при назначении компьютерной экспертизы являются информационно-поисковые задачи по исследованию компьютерной информации, содержащейся на носителях информации, соответствующих определенным критериям.

Ниже представлены примерные вопросы, которые можно поставить перед экспертом, при этом всегда необходимо помнить о том, что лучше связаться с экспертом до вынесения постановления о назначении компьютерной экспертизы и согласо-

[1] Гаврилин Ю.В., Аносов А.В., Баранов В.В. и др. Деятельность органов внутренних дел по борьбе с преступлениями... С. 165.

вать вопросы с ним, а также лучше большее количество конкретных вопросов, чем один вопрос общего характера.

Вопросы, решаемые при исследовании компьютерной информации, представленной в виде файловых систем:

1. Имеется ли на представленных на исследование машинных носителях … (перечислить) информация, содержащая следующие ключевые слова … (перечислить)?

2. Имеется ли на представленных на исследование машинных носителях … (перечислить) информация о ... (изложить о чем)?

Вопросы, решаемые при исследовании компьютерной информации, содержащейся на магнитной полосе пластиковых карт:

1. Какая информация имеется на магнитной полосе пластиковой карты, представленной на исследование?

2. Соответствует ли информация, записанная на магнитную полосу пластиковой карты, информации, имеющейся в элементах ее внешнего оформления?

3. Может ли представленная на исследование пластиковая карта быть воспринята в технологии функционирования платежной системы в качестве платежной (при условии использования информации, записанной на магнитную полосу карты) (на определенную дату или период)?

Вопросы, решаемые при исследовании компьютерной информации, содержащейся в мобильных телефонах:

1. Имеется ли в представленном на экспертизу мобильном телефоне, установленных в нем сим-карте и карте памяти информация, вводимая абонентом (номера телефонов, сообщения, аудио-, видео- и графические файлы и др.) или накопленная в процессе работы телефона в сети сотовой связи (последние набранные и полученные звонки, принятые сообщения и др.)? Если да, то какая?

2. Соответствует ли значение IMEI, содержащееся в памяти представленного мобильного телефона, значению IMEI, нанесенному на … (упаковку, этикетку и др.)?

Требования к объектам исследования:

Информация должна быть представлена на подлинных носителях либо в виде посекторных копий.

По возможности должны быть представлены сведения о паролях, кодах доступа, порядке работы с программным обеспечением (если необходимо). Поскольку исследование информации в мобильных устройствах (смартфоны, планшетные компьютеры и т.д.), как правило, проводится во включенном состоянии, необходимо, чтобы в постановлении о назначении экспертизы содержалось разрешение на изменение информации в устройстве в объеме, необходимом для проведения исследований.

Упаковка должна исключать возможность физического доступа к объекту. Целесообразно использовать картонные коробки, полиэтиленовые и бумажные пакеты, которые заклеиваются, завязываются, опечатываются и снабжаются пояснительными надписями. Хранить их необходимо в сухом помещении при комнатной температуре, исключить влияние электромагнитных полей, не допускать штабелирования.

Вопросы для самоконтроля:

1. Назовите основные оперативно-розыскные мероприятия, проводимые при раскрытии хищений, совершенных с использованием ИТТ.
2. Какие процессуальные трудности возникают на последующем этапе расследования хищений, совершенных с использованием ИТТ?
3. Какие объекты чаще всего изымаются при производстве обыска по рассматриваемой категории преступлений?
4. Какие требования предъявляются при получении образцов голоса и речи?
5. Какие объекты направляются на судебную компьютерную экспертизу?

Литература

1. Гаврилин Ю.В., Аносов А.В., Баранов В.В. и др. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учеб. пособие. В 2 ч. М.: Академия управления МВД России, 2019. Ч. 1. 208 с.

2. Гаспарян Г.З. Расследование хищений денежных средств, совершенных с использованием информационных банковских технологий: автореф. дис. … канд. юрид. наук. М., 2020.

3. Голятина С.М. Методика расследования хищений электронных денежных средств: дис. … канд. юрид. наук. Волгоград, 2022. 196 с.

Заключение

Организация расследования преступлений, связанных с информационными технологиями, требует от следователя определенных навыков и знаний. На первом месте стоит знание законодательства и правовых норм, которые регулируют работу с информацией и защиту данных. Также следователю важно понимать принципы работы информационной системы, обладать базовыми навыками работы с программным обеспечением и техническими средствами, применяемыми при расследовании преступлений.

Безусловно, успешное раскрытие и расследование дел данной категории во многом зависит от своевременного принятия решения о возбуждении уголовного дела, поскольку процесс обнаружения, изъятия и фиксации доказательств начинается с момента получения первичных данных о преступном событии, включая всю последующую деятельность, связанную с проверкой информации, решением вопроса о возбуждении уголовного дела, выбором наиболее оптимального алгоритма расследования на всех его этапах.

В данной работе предложен перечень типичных следственных ситуаций, складывающихся на различных этапах расследования, а также выработан примерный алгоритм выполнения следственных и иных процессуальных действий. Отмечено, что учет тактических особенностей производства – осмотра места происшествия, допроса потерпевшего, свидетелей, получения информации о соединениях между абонентами и (или) абонентские устройствами, обыска, выемки – позволит следователю сформировать качественную доказательственную базу по уголовным делам изучаемого вида. Также в работе рассмотрены некоторые аспекты назначения компьютерной судебной экспертизы и особенности подготовки материалов для ее производства, проанализированы особенности проведения вышеуказанных следственных и иных процессуальных действий с целью повышения эффективности их производства.

Таким образом, в результате усвоения материала, предложенного авторами в данном учебном пособии, у обучающихся должно сформироваться представление о хищениях, совершен-

ных с использованием информационно-телекоммуникационных технологий, об особенностях производства проверки сообщений о преступлении, тактике производства отдельных следственных и иных процессуальных действий. Сформулированные в работе предложения могут быть полезными также и для сотрудников правоохранительных органов при осуществлении ими практической деятельности.

Подводя итог, следует отметить, что грамотные действия сотрудников правоохранительных органов играют ключевую роль в раскрытии и расследовании хищений, совершенных с использованием информационно-телекоммуникационных технологий. Использование приведенного в работе алгоритма расследования позволит наиболее эффективно организовать деятельность сотрудников следственных и оперативных подразделений на различных этапах расследования.

Оглавление

Учебное издание

Архипова Надежда Анатольевна
Кругликова Олеся Васильевна
Шебалин Александр Владимирович
Янгаева Марина Олеговна

Расследование хищений, совершенных с использованием информационно-телекоммуникационных технологий

Учебное пособие

Редактор С.В. Калинина
Корректура, компьютерная верстка М.В. Егерь

Лицензия ЛР № 0221352 от 14.07.1999 г.
Лицензия Плр № 020109 от 15.07.1999 г.

Подписано в печать 26.12.2023. Формат 60х84/16.
Ризография. Усл.п.л. 5,8. Тираж 57 экз. Заказ 480.
Барнаульский юридический институт МВД России.
Научно-исследовательский и редакционно-издательский отдел.
656038, Барнаул, ул. Чкалова, 49; бюи.мвд.рф.