

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«УФИМСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ»

Э. Д. Нугаева, З. И. Харисова, О. В. Евдокимова

**ОРГАНИЗАЦИЯ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ
ДИСТАНЦИОННЫХ МОШЕННИЧЕСТВ, СОВЕРШАЕМЫХ
С ИСПОЛЬЗОВАНИЕМ ИНТЕРНЕТ-СЕРВИСОВ**

Научно-практическое пособие

Уфа 2026

УДК 343.985.7:[343.72]:004.77(470)(076.5)

ББК 67.523.12(2Рос)я73-5

Н87

*Рекомендовано к опубликованию
редакционно-издательским советом Уфимского ЮИ МВД России*

Рецензенты:

кандидат юридических наук, доцент В. Н. Чаплыгина
(Орловский юридический институт МВД России
имени В. В. Лукьянова);

кандидат юридических наук, доцент А. Ш. Габдрахманов
(Казанский юридический институт МВД России)

Н87

Нугаева, Э. Д.

Организация раскрытия и расследования дистанционных мошенничеств, совершаемых с использованием интернет-сервисов : научно-практическое пособие / Э. Д. Нугаева, З. И. Харисова, О. В. Евдокимова. – Уфа: Уфимский ЮИ МВД России, 2026. – 96 с. – Текст : непосредственный.

В научно-практическом пособии на основе комплексного анализа теоретических источников, судебно-следственной практики и статистических данных предложена структура криминалистической характеристики дистанционных мошенничеств на интернет-сервисах; представлена классификация способов дистанционных мошенничеств, совершаемых с использованием интернет-сервисов; показаны особенности тактики производства отдельных следственных действий; рассмотрены особенности криминалистического исследования цифровых следов; описаны возможности технико-криминалистического обеспечения.

Издание предназначено для профессорско-преподавательского состава, обучающихся образовательных организаций МВД России, сотрудников органов, организаций, подразделений МВД России.

УДК 343.985.7:[343.72]:004.77(470)(076.5)

ББК 67.523.12(2Рос)я73-5

© Нугаева Э. Д., 2026

© Харисова З. И., 2026

© Евдокимова О. В., 2026

© Уфимский ЮИ МВД России, 2026

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ	4
ГЛАВА I. ОРГАНИЗАЦИОННО-ТАКТИЧЕСКИЕ ОСОБЕННОСТИ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ДИСТАНЦИОННЫХ МОШЕННИЧЕСТВ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНТЕРНЕТ-СЕРВИСОВ	7
§ 1. Особенности криминалистической характеристики дистанционных мошенничеств, совершаемых с использованием интернет-сервисов	7
§ 2. Классификация способов дистанционных мошенничеств, совершаемых с использованием интернет-сервисов	20
§ 3. Особенности производства доследственной проверки	27
§ 4. Тактические приемы производства отдельных следственных действий	42
ГЛАВА II. КРИМИНАЛИСТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ОРГАНИЗАЦИИ И РАССЛЕДОВАНИЯ ДИСТАНЦИОННЫХ МОШЕННИЧЕСТВ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНТЕРНЕТ-СЕРВИСОВ	63
§ 1. Особенности криминалистического исследования цифровых следов	63
§ 2. Техничко-криминалистическое обеспечение, используемое при расследовании дистанционных мошенничеств	66
§ 3. Совершенствование криминалистических учетов при раскрытии и расследовании дистанционных мошенничеств, совершаемых с использованием интернет-сервисов	75
ЗАКЛЮЧЕНИЕ	84
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	86

ВВЕДЕНИЕ

В условиях стремительной цифровизации и повсеместного распространения информационных технологий Интернет-сервисы стали неотъемлемой частью нашей жизни. Они используются для общения в социальных сетях, совершения покупок на маркетплейсах, управления финансами через интернет-банкинг, поиска информации, развлечений и многого другого. Эта интеграция онлайн-сервисов во все сферы нашей деятельности, к сожалению, создала благоприятную среду для развития мошенничества. К распространенным интернет-сервисам, на которых совершается мошенничество, относятся: сайты объявлений («Юла», «Авито», «Циан»); платформы онлайн-знакомств (Pure, Mamba, «Леонардо Дайвинчик»), социальные сети и мессенджеры («ВКонтакте», «Одноклассники», WhatsApp¹, «Телеграмм»), интернет-магазины и т. п.

Структура и динамика преступлений, квалифицированных по ст. 159 Уголовного кодекса Российской Федерации (далее – УК РФ) («Мошенничество»), совершаемых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, за 2022–2025 гг. выглядит следующим образом (табл.).

Таблица

**Структура и динамика мошенничеств, предусмотренных
ст. 159 УК РФ за 2022–2025 гг.**

№ п/п	Год	Зарегистрировано	Раскрыто	Не раскрыто
1	2022	249 984	29 751	214 225
2	2023	353 201	37 128	304 393
3	2024	379 762	37 749	340 295
4	январь – июнь 2025 г.	183 508	20 099	147 232

Таким образом, анализ данных показывает, что уровень мошенничеств, совершаемых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, за 2022–2025 гг. остается высоким и ежегодно увеличивается. При этом раскрываемость преступлений продолжает оставаться на низком уровне. В период с 2022 по 2025 год уровень раскрываемости преступлений в среднем составил около 11 % от общего числа зарегистрированных преступлений².

¹ WhatsApp принадлежит корпорации Meta, которая признана экстремистской организацией и запрещена на территории России.

² Краткая характеристика состояния преступности в Российской Федерации за январь – июнь 2025 года // МВД России. URL: <https://мвд.рф/reports/item/67755056/> (дата обращения: 10.07.2025).

В 2024 г. у россиян было похищено рекордные 27,5 млрд руб. с банковских счетов, что на 74,4 % больше, чем в 2023 г. Основной объем средств (26,9 млрд руб.) был украден у физических лиц. По оценке Сбербанка, ущерб от телефонного мошенничества в 2024 г. составил не менее 295 млрд руб.¹ Мошеннические схемы, реализуемые посредством интернет-сервисов, отличаются значительным разнообразием и непрерывной адаптацией к новым технологиям и поведению пользователей.

Отсутствие рекомендаций по организации и осуществлению расследования на первоначальном этапе, методики раскрытия и расследования мошенничеств, совершаемых на интернет-сервисах, являющейся оптимальной формой современных научных разработок в данной области, несовершенство тактики производства отдельных следственных действий отрицательно сказывается на эффективности научного обеспечения борьбы с данным видом преступной деятельности. Преступления этой категории оказывают значительное влияние на общество: жертвы не только теряют личные средства, но и могут испытывать психологические травмы, что подчеркивает важность эффективного раскрытия, расследования и предотвращения таких преступлений.

Объектом исследования является преступная деятельность, осуществляемая с использованием интернет-сервисов, а также деятельность органов предварительного следствия и дознания по раскрытию и расследованию данного вида преступлений.

Предметом исследования выступают закономерности осуществления преступных посягательств в мошенничестве с использованием интернет-сервисов, а также обусловленные ими закономерности собирания, исследования, оценки и использования доказательств в процессе борьбы с этими преступлениями.

Цель исследования заключается в разработке организационно-тактических мероприятий раскрытия и расследования дистанционных мошенничеств, совершаемых с использованием интернет-сервисов, направленной на повышение эффективности деятельности органов предварительного расследования по расследованию преступлений данного вида.

Обеспечивая достижение поставленной цели, важно решить следующие задачи:

1. Определить особенности криминалистической характеристики дистанционных мошенничеств, совершаемых с использованием интернет-сервисов.
2. Систематизировать классификацию способов мошенничеств, совершаемых с использованием интернет-сервисов.
3. Раскрыть особенности производства доследственной проверки.

¹ Топ-10 актуальных схем мошенников. URL: <https://www.sberbank.ru/ru/person/kibrary/articles/top-10-aktualnykh-skhemmoshennichestva> (дата обращения: 11.07.2025).

4. Сформулировать тактические приемы производства отдельных следственных действий.

5. Выявить проблемные аспекты организации взаимодействия следственных, оперативных и иных государственных органов в раскрытии и расследовании дистанционных мошенничеств, совершаемых с использованием интернет-сервисов.

6. Сформировать рекомендации по применению криминалистических тактических комбинаций.

7. Определить эффективные методы использования криминалистических учетов при раскрытии и расследовании дистанционных мошенничеств, совершаемых с использованием интернет-сервисов.

Теоретическая значимость исследования состоит в анализе криминалистической характеристики дистанционных мошенничеств на интернет-сервисах, описании организационно-тактических особенностей расследования данной категории дел.

Практическая значимость исследования заключается в выработке конкретных предложений в виде выводов и рекомендаций с целью повышения выявления, раскрытия и расследования органами предварительного расследования и органами дознания дистанционных мошенничеств, совершаемых с использованием интернет-сервисов.

Материал, изложенный в научно-практическом пособии, может быть применен в образовательном процессе образовательных организаций Министерства внутренних дел Российской Федерации (далее – МВД России) у обучающихся по специальностям 40.05.01 Правовое обеспечение национальной безопасности, 40.05.02 Правоохранительная деятельность, 40.03.02 Обеспечение законности и правопорядка при изучении отдельных тем дисциплин «Криминалистика», «Практикум по проведению отдельных следственных действий», «Расследование преступлений против личности и собственности».

ГЛАВА I. ОРГАНИЗАЦИОННО-ТАКТИЧЕСКИЕ ОСОБЕННОСТИ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ДИСТАНЦИОННЫХ МОШЕННИЧЕСТВ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНТЕРНЕТ-СЕРВИСОВ

§ 1. Особенности криминалистической характеристики дистанционных мошенничеств, совершаемых с использованием интернет-сервисов

Дистанционные мошенничества, совершаемые с использованием интернет-сервисов, представляют собой одну из наиболее динамично развивающихся и трудно раскрываемых форм преступной деятельности. Стремительное распространение глобальной сети, развитие цифровых технологий и онлайн-сервисов создают благоприятную почву для совершения преступлений, отличительной особенностью которых является отсутствие прямого контакта между преступником и жертвой.

Анализируя дистанционное мошенничество, важно учитывать его криминалистическую характеристику. В работе по смежной теме А. А. Протасевич, Л. П. Зверьянская среди ключевых элементов называют способ совершения преступления, особенности следовой информации, обстановки совершения преступления (место и время его совершения и др.), личностную характеристику преступника, особенности непосредственного предмета преступного посягательства¹. А. И. Маилян полагает, что в криминалистическую характеристику хищений, совершенных в отношении электронных денежных средств, необходимо включить сведения о способах приготовления, совершения, сокрытия преступлений, об орудиях и средствах совершения преступлений, предмете преступного посягательства, следах преступления, об особенностях личности преступника и потерпевшего².

Данный вид мошенничества характеризуется широким использованием разнообразных интернет-платформ: от социальных сетей и мессенджеров до фишинговых сайтов и онлайн-магазинов.

По мнению авторов, криминалистическая характеристика таких преступлений требует комплексного анализа, включающего изучение способов приготовления, совершения, сокрытия преступлений, средств и орудий совершения мошенничества данного вида, обстановки совершения преступления, предмета преступного посягательства, особенностей личности пре-

¹ Протасевич А. А., Зверьянская Л. П. Криминалистическая характеристика компьютерных преступлений // Российский следователь. 2013. № 11. С. 45–47.

² Маилян А. В. Общие положения криминалистической характеристики хищений, совершенных с банковского счета, в отношении электронных денежных средств и/или с помощью электронных средств платежа // Известия Тульского государственного университета. 2020. № 3. С. 125.

ступников и потерпевших, механизма слеодообразования. Понимание этих особенностей является ключевым для разработки действенных мер раскрытия, расследования и предупреждения данного вида преступлений.

Особенности способов приготовления, совершения и сокрытия дистанционных мошенничеств, совершаемых с использованием интернет-сервисов

Анализ эмпирических материалов показывает, что способы дистанционного мошенничества, совершаемые с использованием интернет-сервисов, являются полноструктурными (подготовка к совершению преступления, реализация преступного умысла и сокрытие). Подготовительный этап характеризуется как ключевой для формирования преступной деятельности. Его значение заключается в том, что без комплексной подготовки значительная часть мошеннических схем, реализуемых посредством интернет-сервисов, не могла бы быть осуществлена. На этапе реализации преступного умысла происходит непосредственное взаимодействие с объектом преступного посягательства (жертвой) с целью осуществления обмана и получения противоправной выгоды. На этапе сокрытия следов преступления задачей мошенника является избежать ответственности. После хищения денежных средств необходимо максимально затруднить расследование и уничтожить следы своей деятельности¹.

Способы приготовления к дистанционным мошенничествам на интернет-сервисах разнообразны. Для организации своих действий преступники используют различные устройства, такие как компьютеры, планшеты и смартфоны. Стабильный доступ в Интернет выступает основным ресурсом для создания поддельных веб-сайтов, рассылки электронных писем и общения с жертвами через мессенджеры и социальные сети. Мошенники создают фальшивые профили в социальных сетях или на платформах для знакомств, чтобы обмануть жертву. Размещают ложную информацию о товарах или услугах на популярных платформах, что напрямую приводит к финансовым потерям пользователей. Кроме того, злоумышленник имеет банковский или другой счет, электронный кошелек, на который жертва переводит деньги под воздействием обмана.

Расследование дистанционных мошенничеств представляет объективную сложность в связи с тем, что, как правило, исключается непосредственный личный контакт с мошенником, преступник может находиться в любом месте на территории страны и за ее пределами, регистрировать доменные имена за границей, в короткий промежуток времени совершить значительное число хищений, а установление его личности в данном случае крайне затруднительно. На этапе подготовки мошенник обдумывает

¹ Изучено и проанализировано 78 уголовных дел о мошенничестве на интернет-сервисах Республики Башкортостан, Челябинской, Оренбургской и Московской областей (ст. 159 УК РФ).

способы сокрытия своих следов, поскольку успешное мошенничество часто зависит от того, насколько хорошо он может скрыть свою идентичность и действия. С целью сокрытия следов преступления они используют такие анонимайзеры, как VPN-сервисы (Virtual Private Network – виртуальная частная сеть), обеспечивающие шифрование трафика и сокрытие реального IP-адреса преступника, системы прокси-серверов, построенные на базе многослойного шифрования данных, и пр.¹ На стадии получения денежных средств, мошенники не участвуют в процессе лично, а используют современные технологии, позволяющие получить деньги. Следы совершения преступления в этом случае блокируются за счет возможности анонимного обналичивания денежных средств либо их иного использования, например для оплаты товаров, заказываемых из-за рубежа, когда идентификация покупателя не осуществляется либо крайне затруднена, потому что покупатель и мошенник – не одно и то же лицо².

По мнению авторов, способ совершения дистанционного мошенничества с использованием интернет-сервисов является центральным элементом. Способы дистанционных мошенничеств, совершаемых на интернет-сервисах, достаточно разнообразны и зависят от изобретательности и интеллектуальных способностей преступника. В связи с этим мы выделили их в отдельный параграф, где более подробно рассмотрим различные методы и схемы, используемые мошенниками.

Обстановка совершения преступления

При выявлении и расследовании преступлений данного вида вызывает сложность установление места совершения преступления. Часто место непосредственного совершения мошенничества и место наступления вредоносных последствий могут не совпадать, поэтому в криминалистической науке принято выделять место обнаружения признаков преступления и место непосредственного совершения преступных действий. Следует учитывать, что эти места могут быть удалены друг от друга на значительные расстояния, находиться в различных учреждениях, регионах и даже странах. В связи с этим местом совершения преступления будет тот участок местности (учреждение, организация, предприятие, территория государства или транспортное средство), где были совершены противоправные деяния, независимо от места наступления вредоносных последствий³. Типичными

¹ Харисова З. И. Криминалистическая характеристика преступлений, связанных с неправомерным доступом к компьютерной информации // Правовое государство: теория и практика. 2025. № 2 (80). С. 99.

² Новые способы совершения преступлений в сфере информационных технологий на территории государств – участников СНГ : аналитический обзор / И. Б. Колчевский, В. М. Журавлев, А. Г. Кузнецов [и др.]. М. : ФГКУ «ВНИИ МВД России», 2018. С. 32–34.

³ Низаева С. Р. Цифровые технологии в криминалистике // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. 2021. № 21 (1). С. 55–56.

местами совершения неправомерного доступа к компьютерной информации являются жилище преступника, место его учебы (работы), общественное место со свободным доступом к информационно-телекоммуникационной сети Интернет, а также со стационарным подключением компьютерного оборудования, имеющего выход в данную сеть, либо жилище потерпевшего (в редких случаях).

Временем совершения неправомерного доступа к компьютерной информации считается период совершения противоправного деяния. По данной категории уголовных дел время практически всегда устанавливается с точностью до минуты. Это обусловлено автоматической регистрацией параметров входа в сеть, действий и событий, произошедших потом. Данное обстоятельство устанавливается следственным путем посредством осмотра компьютерной информации, содержащейся на материальном носителе (флеш-карта, платежный терминал и т. д.), либо виртуальных следов преступления (например, информация о посещаемых интернет-сайтах).

Особенности средств и орудий совершения мошенничеств на интернет-сервисах

К орудиям и средствам дистанционного мошенничества, совершаемого с использованием интернет-сервисов, относятся, прежде всего, смартфоны, ноутбуки, планшеты, а также электронные кошельки и доступ к соответствующим интернет-ресурсам, таким как социальные сети, мессенджеры и банковские приложения. Эти устройства и сервисы служат инструментами для установления контакта с жертвой, сбора необходимой информации и проведения незаконных финансовых операций. Например, с помощью телефона мошенники могут отправлять сообщения, а ноутбук используется для более сложных схем, таких как фишинг или создание поддельных сайтов. Электронные кошельки и банковские приложения, в свою очередь, выступают как каналы для получения украденных денежных средств, делая процесс перевода денег максимально быстрым и часто анонимным.

В случаях о хищениях электронных денежных средств орудиями совершения преступления являются персональные компьютеры, смартфоны и прочие девайсы, электронные носители информации, вредоносное программное обеспечение, средствами – информационно-телекоммуникационная сеть Интернет и средства обеспечения доступа к ней; программное обеспечение операторов электронных платежных средств; мессенджеры, информационные ресурсы торговых площадок; фишинговые сайты; социальные сети¹.

Особенности предмета преступного посягательства дистанционных мошенничеств на интернет-сервисах

Особенностью мошенничества в сфере компьютерной информации является то, что, как правило, большинство преступлений совершается

¹ Голятина С. М. Методика расследования хищений электронных денежных средств : дис. ... канд. юрид. наук. Волгоград, 2022. С. 59.

не в отношении наличных, а в отношении безналичных, электронных денежных средств и т. д.¹ Однако обратим внимание на то, что некоторое время назад суды Российской Федерации практически единогласно отмечали, что электронные деньги не могут рассматриваться в качестве предмета хищения, поскольку не являются вещью материального мира и не существуют в физически осязаемой форме. Таким образом, преступные посягательства в отношении электронных денежных средств квалифицировались по нормам о мошенничестве. В ноябре 2017 г. Пленум Верховного Суда Российской Федерации в постановлении № 48 указал, что «если предметом преступления при мошенничестве являются безналичные денежные средства, в том числе электронные денежные средства, то по смыслу положений пункта 1 примечаний к статье 158 УК РФ и статьи 128 Гражданского кодекса Российской Федерации содеянное должно рассматриваться как хищение чужого имущества. Такое преступление следует считать оконченным с момента изъятия денежных средств с банковского счета их владельца или электронных денежных средств, в результате которого владельцу этих денежных средств причинен ущерб»², то есть с этого времени электронные денежные средства были приравнены к наличным и стали рассматриваться в качестве предмета хищения чужого имущества.

Предметом преступного посягательства могут быть также логины и пароли, которые предоставляют доступ к аккаунтам в социальных сетях, электронной почте, личным кабинетам и онлайн-магазинам, что позволяет злоумышленникам управлять чужими аккаунтами, совершать мошеннические действия и причинять материальный ущерб; персональные данные, такие как паспортные данные, страховой номер индивидуального лицевого счета (СНИЛС) и идентификационный номер налогоплательщика (ИНН), используемые для оформления кредитов, открытия банковских счетов и других незаконных операций; информация о собственности, например документы на недвижимость, автомобили и другие материальные ценности, которые могут использоваться для мошенничества и незаконного распоряжения имуществом.

Механизм следообразования

Использование преступниками средств мобильной коммуникации оставляет специфическую следовую картину. Помимо типичных материальных и (или) идеальных, остаются следы действий – виртуальные следы в памяти электронных устройств. Данное понятие введено в криминали-

¹ Харина Е. А. Особенности методики расследования мошенничества в сфере компьютерной информации : дис. ... канд. юрид. наук. Красноярск, 2024. С. 26.

² О судебной практике по делам о мошенничестве, присвоении и растрате : постановление Пленума Верховного Суда Российской Федерации от 30 нояб. 2017 г. № 48 // ГАРАНТ.РУ : информационно-правовой портал. URL: <https://base.garant.ru/71823288> (дата обращения: 21.07.2025).

стику, поскольку сложившееся в теории традиционное понимание следов не в полной мере относится к преступлениям, связанным с неправомерным доступом к компьютерной информации.

В науке неоднократно предпринимались попытки определить и классифицировать различные следы преступления, оставленные в информационной среде. В. А. Мещеряковым было предложено ввести понятие «виртуальный след», Л. Б. Краснова определяет понятие «электронно-цифровой объект», Г. М. Шаповалова, В. В. Борисов, Ю. В. Гаврилина – «информационный след», Н. Н. Лыткин – «компьютерно-технические следы», В. А. Милашев – «бинарные следы», В. Б. Вехов – «электронно-цифровой след», Е. Р. Россинская – «цифровой след»¹. При наименовании следов, оставляемых в информационном пространстве, нам близка позиция Е. Р. Россинской и И. А. Рядовского, выделяющих понятие «цифровой след» и представляющих его как «...криминалистически значимую компьютерную информацию о событиях или действиях, отраженную в материальной среде, в процессе ее возникновения, обработки, хранения и передачи»².

Применительно к хищениям электронных денежных средств это могут быть операторы электронных платежных систем; электронные торговые площадки; интернет-провайдеры; серверы компаний, предоставляющих услуги пользования той или иной социальной сетью; сервисы электронных сообщений; «облачные» хранилища; компьютерные системы потерпевшего и подозреваемого. На серверах платежных систем остаются данные об операциях с интересующими нас счетами, данные пользователей, конкретное время проведения операций со счетами, следы от дистанционного управления мошенниками своими счетами, их открытия и закрытия, а также многие другие сведения; реквизиты счетов, на которые осуществлен перевод денежных средств³.

Особенности личности преступника и потерпевшего

Следующим важным элементом криминалистической характеристики преступлений является личность преступника, необходимость изучения которой продиктована не только задачами криминалистики, но и требованиями уголовно-процессуального законодательства. Согласно ст. 73 Уголовно-процессуального кодекса Российской Федерации (далее – УПК РФ) «при производстве по уголовному делу подлежат доказыванию... виновность лица в совершении преступления, форма его вины и мотивы; обстоя-

¹ Кулаевский А. В. Нормативно-правовые основания развития программы материнского (семейного) капитала // Вопросы российского и международного права. 2024. Т. 14, № 7А. С. 450.

² Россинская Е. Р. Концепция цифровых следов в криминалистике // Аубакировские чтения : материалы междунар. науч.-практ. конф., Алматы, 19 февр. 2019 г. Алматы, 2019. С. 7.

³ Полещук О. В. Шаповалова Г. М. Криминалистическое исследование следов при расследовании компьютерных преступлений : моногр. Владивосток : Изд-во Дальневост. ун-та, 2006. С. 52.

тельства, характеризующие личность обвиняемого», то есть необходимо установить, что преступление совершено именно этим лицом при наличии умысла или неосторожности, цель и мотив преступления независимо от того, имеют ли они уголовно-правовое значение квалифицирующих признаков, а также формальные данные о личности обвиняемого (фамилия, имя, отчество, год рождения и т. д.) и данные, характеризующие его как члена общества. Ю. Л. Дяблова отмечает, что личностью в криминалистике нужно называть совокупность относительно постоянных свойств, принадлежащих биологической, социальной либо биосоциальной сферам и находящих свою реализацию в признаках, которые важны как для теоретического изучения личности, так и для ее практического познания при расследовании того или иного преступления¹. Д. Н. Балашов, Н. М. Балашов и С. В. Маликов подчеркивают, что криминалистическое изучение личности преступника позволяет следователю создать наиболее благоприятную следственную ситуацию, когда можно принять оптимальное тактическое решение². По мнению авторов, объем такого изучения должен исчерпываться сведениями, которые помогут установить состав преступления и иные обстоятельства, дающие всестороннюю характеристику человека и имеющие значение для правильного разрешения дела.

Не вызывает сомнения, что в психологическом плане мошенники – особая категория. Как правило, это люди, владеющие определенными познаниями в психологии, психиатрии и физиологии человека, обладающие хорошими коммуникативными способностями, навыками установления психологического контакта с потерпевшими, находящимися в сложных жизненных ситуациях. Это стрессоустойчивые личности с располагающим внешним видом. Их отличает решительность, смелость, гибкость мышления, самообладание, склонность к риску, хладнокровие, пониженная тревожность, умение отстаивать свои интересы и свободно держаться, импровизировать, артистизм, способность быстро принимать решения, незамедлительно их осуществлять, льстивость и эгоизм. Способность к обману развивается на фоне природных качеств преступников, таких как внимательность, хитрость, ловкость рук, дерзость, находчивость³.

Исследование установило, что социально-демографические и биологические признаки личности преступников, совершающих дистанционные мошенничества на интернет-сервисах, различаются в зависимости от используемой интернет-платформы. В связи с этим мы считаем необходимым рассмотреть криминалистическую характеристику преступника по отдельным способам дистанционного мошенничества, таким как мошенничество

¹ Дяблова Ю. Л. Понятие и структура личности в криминалистике // Известия Тульского государственного университета. Экономические и юридические науки. 2016. № 2-2. С. 108.

² Криминалистическое изучение личности : науч.-практ. пособие для магистров / отв. ред. Я. В. Комиссарова. М. : Проспект, 2016. С. 7.

³ Нугаева Э. Д. Особенности расследования мошенничества при оказании оккультных услуг : дис. ... канд. юрид. наук. Уфа, 2018. С. 73.

на платформах онлайн-знакомств, в сфере инвестирования, в сфере предоставления государственных услуг и справочной информации.

Личность преступника, совершающего дистанционные мошенничества на платформах онлайн-знакомств

Изучение уголовных дел о мошенничествах на платформах онлайн-знакомств свидетельствует о том, что большинство из них совершаются мужчинами – 58 %, однако наблюдается и значительное количество женщин, участвующих в мошеннических схемах, – 42 %. Это может быть связано с различными ролями, которые они исполняют. Анализ 38 уголовных дел, в которых преступниками выступали мужчины, показал следующие процентные доли по возрастным группам: 18–25 лет – 26 %, 26–35 лет – 45, 36–50 лет – 24, 51 год и более – 5 %. При рассмотрении преступлений, которые совершались женщинами (39 уголовных дел), наблюдается немного иная тенденция. В возрастной категории 18–25 лет женщины составляют 41 %, 26–35 лет – 30, 36–50 лет – 28, 51 год и более – 2 %. Таким образом, можно сделать вывод, что мужчины совершают такие преступления в возрасте от 26 до 35 лет, в то время как женщины – в возрасте от 18 до 25 лет. Рассматриваемое мошенничество совершается гражданами различных стран, и среди них Нигерия и Камерун выделяются как страны, откуда чаще всего исходят преступления такого рода¹.

Анализ уголовных дел показал, что большинство мошеннических действий на платформах онлайн-знакомств (94 %) совершаются единолично. Преступления, осуществляемые группой по предварительному сговору, составляют 4 %, организованной группой – 2 %. Данные свидетельствуют о преобладании самостоятельности совершения преступных деяний при взаимодействии с жертвой. Образовательный уровень мошенников является довольно низким: неполное среднее образование имеют 23,4 %, среднее общее – 38,2, среднее специальное – 27, высшее – 11,4 %².

Однако характеристика типичной личности мошенника лишь по социально-демографическим и биологическим признакам не дает полного представления о нем. Психологические методы являются ключевым инструментом мошенников на сайтах знакомств, позволяя им манипулировать жертвами и вызывать у них доверие. Они используют их с целью совершения определенных действий или разглашения конфиденциальной информации. К этим методам относятся: демонстрация ложных чувств к своей жертве, чтобы привлечь внимание и войти в доверие; манипуляция

¹ Изучено и проанализировано 38 уголовных дел о мошенничестве на платформах онлайн-знакомств (ст. 159 УК РФ) Республики Башкортостан, Челябинской области, Оренбургской области, Московской области, а также приговоры Республики Марий Эл, Ленинградской области, Республики Саха (Якутия).

² Изучено и проанализировано 38 уголовных дел о мошенничестве на платформах онлайн-знакомств (ст. 159 УК РФ) Республики Башкортостан, Челябинской области, Оренбургской области, Московской области, а также приговоры Республики Марий Эл, Ленинградской области, Республики Саха (Якутия).

ложными обещаниями о совместном будущем, финансовом благополучии; подстраивание под жертву, отражая ее взгляды, интересы и ценности; манипулирование чувством вины и демонстрация обиды; «газлайтинг» – техника манипуляции, с помощью которой один человек заставляет другого сомневаться в собственной нормальности, постепенно подрывая самооценку и доверие жертвы к собственным ощущениям, и адекватном восприятии реальности; создание ложного образа лица с высоким социальным статусом для повышения уровня доверия.

Личность преступника, совершающего дистанционные мошенничества в сфере инвестирования

Мужчины составляют 95 % от числа преступников. Это связано с тем, что они чаще работают в финансовых и технических сферах, что дает им больше возможностей для разработки и реализации мошеннических схем. Преступников в возрасте 25–35 лет – 78 %, они обладают хорошими техническими навыками, склонны к риску, ищут быстрые способы обогащения, могут выступать в роли «технарей» или «активных продавцов». Преступников среднего возраста (35–55 лет) – 22 %, они имеют опыт в сфере финансов, продаж или даже криминальный опыт, часто выступают в роли организаторов, обладают навыками манипуляции и планирования. Лиц с высшим образованием – 57 %, в том числе в сферах экономики, финансов, юриспруденции, с неполным средним – 9, средним общим – 19, средним профессиональным – 21 %. Высшее образование позволяет им понимать финансовые рынки и создавать правдоподобные легенды, использовать сложные юридические и финансовые термины для убеждения, эффективно применять IT-инструменты для реализации схемы. Работают в финансовых организациях 78 %, в других сферах – 22 %¹.

Личность преступника, совершающего дистанционные мошенничества в сфере предоставления государственных услуг и справочной информации

По данным наших исследований, 68 % мошенничеств в сфере предоставления государственных услуг и справочной информации приходится на женщин, оставшиеся 32 % – на мужчин. Это обусловлено несколькими факторами: женщины часто воспринимаются как более мягкие и заслуживающие доверия, что позволяет им легче входить в контакт и убеждать. В 83 % случаев женщины занимают должности, связанные с предоставлением информации или обработкой документов, что дает им представление о механизмах работы государственных служб, 17 % работают в другой сфере. Наиболее активная возрастная группа – от 25 до 55 лет. 67 % – в возрасте 25–35 лет, имеют жизненный опыт, чтобы понимать, как рабо-

¹ Изучено и проанализировано 20 уголовных дел о мошенничестве в сфере инвестирования (ст. 159 УК РФ), находившихся в производстве Управления МВД России по г. Уфе и ГСУ МВД по Республике Башкортостан.

тают государственные структуры и как можно этим воспользоваться, часто обладают навыками общения и убеждения. 33 % – более старшего возраста (40–55 лет), могут иметь опыт работы в государственных учреждениях. Образовательный уровень мошенников является средним. Это означает, что большинство из них имеют среднее или среднее профессиональное образование – 71 %, высшее – 29 %. Ранее работавшие в сфере, связанной с государственными услугами, социальной защитой, пенсионными фондами, многофункциональными центрами (МФЦ), паспортными столами, составляют 64 % из числа преступников¹.

В большей степени способы дистанционных мошенничеств на интернет-сервисах связаны с определенными нравственными характеристиками и психологическими особенностями преступников. Одним из главных психологических свойств такой личности является коммуникабельность. Это обусловлено тем, что ему необходимо убедить гражданина, с которым будет разговаривать, поверить в его слова, ввести в заблуждение, заставив расстаться с некоторой суммой денежных средств. Как верно отмечает Н. Ю. Лебедев, «огромное значение имеет умение установить психологический контакт с потенциальной жертвой»².

Мошенники, как правило, обладают более высоким уровнем интеллекта по сравнению с другими категориями преступников, они быстро адаптируются к меняющимся условиям. Кроме того, их отличает хладнокровие, расчетливость и самоконтроль, умение понимать психологию окружающих, вызывать у них доверие через демонстрацию сочувствия и сопереживания. Актерские способности, наблюдательность и раскрепощенность в поведении позволяют им использовать техники психологического воздействия на других людей. Значительная часть мошенников демонстрирует признаки психопатии, характеризующейся отсутствием эмпатии, склонностью к манипуляциям и обману, поверхностным обаянием и отсутствием чувства вины.

Таким образом, криминалистическое изучение личности преступника – это сбор, анализ и оценка криминалистически значимой информации о нем, куда входят сведения о его биологических, психологических, социальных характеристиках, необходимые для эффективного решения тактических задач расследования и установления картины события преступления. В результате этой деятельности можно определить, какие группы

¹ Изучено и проанализировано 30 уголовных дел о мошенничестве в сфере предоставления государственных услуг и справочной информации (ст. 159 УК РФ), находившихся в производстве Управления МВД России по г. Уфе и ГСУ МВД по Республике Башкортостан, ГУ МВД России по Челябинской, Оренбургской областям.

² Лебедев Н. Ю. Некоторые из признаков, характеризующих личность мошенника // Актуальные проблемы уголовного судопроизводства : материалы III Всерос. науч.-практ. конф., Новосибирск, 18 мая 2023 г. М. : Московская академия Следственного комитета Российской Федерации, 2023. С. 89.

имеют наибольшую преступную активность, мотивы и цели (прежде всего связанные с субъективными данными, социальными установками и взглядами), которыми руководствуются преступники, и в дальнейшем выработать рекомендации по выявлению и расследованию преступлений.

«...На выбор злоумышленниками тех или иных способов совершения деяния существенно влияют особенности личности потерпевшего, прежде всего, степень его виктимизации, наличие социально значимых отношений с субъектами преступлений и др.»¹. Согласимся с приведенной цитатой и отметим, что мошенничества, на которые приходится большая часть хищений электронных денег, от большинства других преступлений отличает важная черта – вовлеченность в преступное деяние жертвы: она должна участвовать в разговоре, переходить по ссылкам в Интернете, предоставлять злоумышленнику персональные данные и др. Однако при этом подчеркнем, что криминалистическая характеристика все же предполагает набор типичных признаков, выявить которые в случае с интернет-мошенничествами применительно к потерпевшему весьма затруднительно, поскольку возрастной и социальный разброс жертв крайне велик.

В структуре криминалистической характеристики дистанционного мошенничества на интернет-сервисах сведения о личности потерпевших имеют немаловажное значение, так как позволяют очертить круг лиц, причастных к совершению данного преступления, охарактеризовать личность мошенника, запланировать мероприятия по обнаружению доказательственной базы по уголовному делу². Мы разделяем мнение Н. П. Яблокова, что «выявление криминалистических особенностей личности потерпевшего и его поведение дают возможность глубже разобраться во многих обстоятельствах преступления, особенно указывающих на своеобразие, направленность и мотивы поведения преступника, его общие (типовые) и индивидуальные свойства...»³.

Анализ данных о жертвах позволяет очертить круг лиц, потенциально подверженных таким преступлениям. Важно отметить, что характеристики потерпевших различаются в зависимости от специфики интернет-платформы, на которой произошло мошенничество. Для более точного анализа мы будем рассматривать потерпевших, разделив их по используемым интернет-платформам. Это позволяет не только выявить общие черты и уязвимости раз-

¹ Маилян А. В. Общие положения криминалистической характеристики хищений, совершенных с банковского счета, в отношении электронных денежных средств и/или с помощью электронных средств платежа // Известия Тульского государственного университета. Экономические и юридические науки. 2020. № (3). С. 124.

² Нугаева Э. Д. Особенности расследования мошенничества при оказании оккультных услуг : дис. ... канд. юрид. наук. Уфа, 2018. С. 84.

³ Криминалистика : учеб. для вузов / отв. ред. Н. П. Яблоков. М. : БЕК, 1995. С. 55–56.

личных категорий пользователей, но и более эффективно разрабатывать меры по предупреждению и расследованию таких преступлений.

Личность потерпевшего на платформах онлайн-знакомств

Потерпевшими по рассматриваемой категории дел чаще всего являются лица женского пола – 70 %. Детерминацией данного явления являются психологические особенности женщин: они по своей натуре гораздо доверчивее мужчин. Как отмечают эксперты, что чаще обманутыми в онлайн-знакомствах оказываются обеспеченные женщины старше 40 лет¹. Чувство одиночества может повышать мотивацию женщин к поиску партнера. Мошенники, используя эту уязвимость, часто целенаправленно выбирают зрелых женщин в качестве жертв, предполагая наличие у них накопленных финансовых средств. Кроме того, Владимир Соболев, член Московской областной коллегии адвокатов, считает, что взрослая женщина склонна скрывать факт обмана или вымогательства в подобных обстоятельствах.

В результате анализа эмпирических данных, характеризующих поведение потерпевших от мошенничества на платформах онлайн-знакомств, нами выделены определенные категории лиц, демонстрирующие повышенную подверженность манипулятивным техникам преступников: доверчивые, одинокие, с низкой самооценкой, пережившие неудачный опыт в отношениях, с ограниченными возможностями, стремящиеся к быстрой финансовой выгоде.

Результаты проведенного исследования позволяют сделать вывод о том, что знание личности потерпевшего играет ключевую роль в эффективном расследовании мошенничества на платформах онлайн-знакомств. Кроме того, понимание психологической уязвимости потерпевших, например склонности скрывать факт обмана, позволяет быстрее установить доверительный контакт, получить исчерпывающую информацию о преступлении и выстроить более эффективную тактику следственных действий, к примеру допрос и очную ставку².

Личность потерпевшего в интернет-магазинах

67 % потерпевших – женщины, так как традиционно считаются более активными покупателями в онлайн-пространстве, особенно в сегментах одежды, косметики, товаров для дома и детей. Оставшиеся 33 % – мужчины. Наиболее уязвимая группа – лица 25–45 лет (70 %), эта группа активно пользуется интернет-магазинами, часто совершает покупки, имеет доступ

¹ Эксперты рассказали, кто чаще всего становится жертвой онлайн-любовников // Москва 24. URL: https://www.m24.ru/articles/obshchestvo/25112020/157421?utm_source=СоруВuf (дата обращения: 25.02.2025).

² Евдокимова О. В. Некоторые особенности личности потерпевших при мошенничестве на платформах онлайн-знакомств // Санкт-Петербургские встречи молодых ученых : материалы III Всерос. конгресса, Санкт-Петербург, 11 июня 2025 г. / сост. М. В. Бавсун, Н. М. Наумова, Е. А. Слюсарева. СПб. : Санкт-Петербургский университет МВД России, 2025. С. 396–399.

к онлайн-платежам и может быть менее осторожной из-за привычки к онлайн-шопингу; в возрасте 18–24 лет – 20 %, активные пользователи Интернета, часто совершают покупки в социальных сетях и маркетплейсах, могут быть склонны к покупке подделок или товаров по слишком низким ценам, менее осведомлены о рисках. Лица старше 45 лет – 15 %. В зависимости от уровня цифровой грамотности жертвы могут быть как более осторожными, так и более уязвимыми из-за недостаточного понимания современных схем мошенничества или доверия к сайтам. Психологические особенности личности потерпевшего:

1. Стремление к выгоде и экономии. Потерпевшие часто ищут товары по максимально низким ценам, ведутся на обещания больших скидок, акций, бесплатных подарков.

2. Склонность к совершению покупок под влиянием эмоций, рекламы или ограниченности предложения, что может привести к недостаточному анализу продавца и условий сделки.

3. Нежелание проверять репутацию продавца, читать отзывы.

4. Доверие к ссылкам, полученным из непроверенных источников (соцсети, мессенджеры, спам-рассылки).

5. Недостаточное понимание принципов безопасности онлайн-платежей (например, ввод данных банковской карты на сомнительных сайтах).

6. Использование слабых паролей, отсутствие двухфакторной аутентификации.

7. Недостаток информации о реальных механизмах мошенничества, жертвы могут не знать, как именно работают мошенники, какие методы они используют (например, создание фейковых страниц известных магазинов, имитация оплаты, «запросы» на дополнительную верификацию).

Личность потерпевшего в сфере государственных услуг и справочной информации

Потерпевшие от мошенничества в сфере государственных услуг и справочной информации – это группа граждан, сталкивающихся с необходимостью получения официальной информации или услуг. Однако пожилые люди (старше 55–60 лет) выделяются как особо уязвимая категория, в 68 % случаев из числа потерпевших чаще сталкиваются с необходимостью получения государственных услуг (пенсии, льготы, медицинское обслуживание, субсидии). У пожилых людей присутствует доверие к «официальным» источникам, таким как сотрудники социального фонда и налоговой службы, оно усиливается, когда мошенники используют специальную терминологию, имена, должности, даже присылают фотографии своих удостоверений. Недостаточная цифровая грамотность проявляется в неспособности отличить поддельный сайт от настоящего. Визуальная схожесть или использование знакомого логотипа могут легко ввести их в заблуждение. Эти факторы делают пожилых людей особенно уязвимыми к мошенничеству и манипуляциям.

О. Р. Онищенко подчеркивает, что «личность потерпевших от мошенничества характеризуется определенными психологическими признаками – это экстравертированность, повышенный уровень тревожности, неудовлетворенность своим социальным статусом и материальным положением, не критичность при восприятии информации, эмоциональная лабильность и т. п.»¹.

На основании проведенной исследовательской работы сделан вывод, что постоянное развитие интернет-сервисов и совершенствование мошеннических схем требуют непрерывного анализа криминалистической характеристики дистанционных мошенничеств, совершаемых с использованием интернет-сервисов. Установление способов подготовки, совершения, сокрытия, обстановки, средств и орудий совершения мошенничества данного вида, предмета преступного посягательства, механизма следообразования, особенностей личности преступника и потерпевшего является основой для разработки эффективной методики расследования этих преступлений. Полученные данные позволяют своевременно принимать целенаправленные меры противодействия и предупреждения преступлений.

§ 2. Классификация способов дистанционных мошенничеств, совершаемых с использованием интернет-сервисов

В современном мире, где технологии стремительно развиваются, мошенничество также претерпевает значительные изменения. Каждый год появляются новые способы обмана, мошенники активно используют интернет-сервисы для достижения своих целей. Анализ способов дистанционных мошенничеств, совершаемых с использованием интернет-сервисов, становится актуальной задачей, позволяющей систематизировать знания о различных методах обмана и разработать эффективную методику раскрытия и расследования преступлений.

Следует согласиться с мнением А. А. Комаровой, которая полагает, что «определяющим признаком любой формы мошенничества является способ совершения преступления: обман или злоупотребление доверием, являющиеся единственным, исключительным способом совершения данного вида преступлений»².

1. Мошенничества через платформы онлайн-знакомств.

Согласно данным компании Mediascope, занимающейся исследованием поведения людей в цифровой среде, совокупная месячная аудитория

¹ Онищенко О. Р. Характеристика личности потерпевших от мошенничества // Проблемы уголовного права, уголовного процесса и криминалистики : сб. науч. работ. Омск : Омский государственный университет им. Ф. М. Достоевского, 2003. Вып. 7. С. 122.

² Комарова А. А. Интернет-мошенничество: проблемы детерминации и предупреждения : моногр. М. : Юрлитинформ, 2013. С. 9.

всех российских сервисов знакомств в феврале 2025 г. достигла 8 млн пользователей. Распределение аудитории по платформам демонстрирует следующую картину: лидирующую позицию занимает сервис Mamba – 2,2 млн пользователей, далее следуют «VK Знакомства» – 4,4 млн, «Друг Вокруг» – 1,9 млн, Tabor – 1,4 млн пользователей, Twinby – 1,1 млн пользователей, из которых 850 тыс. активны, Loveplanet – 741 тыс. пользователей, Beboo – 659,5 тыс., «Мята» – 503 тыс., «Mail.ru Знакомства» – 464 тыс. и Teamo – 427 тыс. пользователей. Суммарная аудитория «VK Знакомств» и «ОК Знакомств» достигает 5,4 млн пользователей, при этом «VK Знакомства» продемонстрировали годовой рост аудитории на 42 %, а недавно запущенные «ОК Знакомства» уже превысили 1 млн пользователей¹.

На официальном сайте МВД России отмечено, что мошенники начали действовать через сайты знакомств². Мошенничество на платформах онлайн-знакомств происходит, когда одна сторона считает, что удалось найти пару, а вторая, на самом деле являясь мошенником, манипулирует, оказывает собеседнику знаки внимания, завоевывает доверие. Конечная цель мошенника – хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.

Схема 1. Доставка цветов.

Данная схема мошенничества наблюдается в преддверии таких праздников, как 14 февраля, 8 марта, а также в случае, если мошенники располагают информацией о дне рождения жертвы. В этих случаях жертва, ожидая получения подарка, становится более уязвимой к манипуляциям. Процесс начинается с того, что мошенник устанавливает контакт с жертвой на сайте знакомств. После непродолжительной беседы проявляет интерес к личным данным жертве, в частности к ее адресу, создавая видимость, что цветы могут отправлены им. Жертве поступает звонок от курьера по доставке цветов, он спрашивает, когда будет удобно доставить букет, и просит сообщить код из СМС для подтверждения доставки. После этого мошенники получают неправомерный доступ к аккаунтам. В некоторых случаях схема может включать реальную доставку цветов. На следующий день после получения букета жертве вновь поступает звонок, на этот раз от «сотрудника магазина», который интересуется, понравился ли ей букет, просит оценить работу курьера и сообщить код из СМС для завершения заказа.

Так, девушке пришло сообщение в мессенджере о доставке цветов, после чего мошенники запросили код из СМС для отказа от заказа. Затем она получила звонок от «сотрудников Центробанка», которые сообщили о взломе ее личного кабинета на «Госуслугах». К разговору присоединился «следователь», показавший удостоверение и убедивший девушку, что мошенники пытаются оформить кредит на ее родственника. Под давлением

¹ Пажитных Ю. А. Аудитория дейтинг-сервисов в России достигла 8 млн пользователей // Russian Business. URL: <https://rb.ru/news/sajty-znakomstv/> (дата обращения: 28.03.2025).

² МВД России : сайт. URL: <https://мвд.рф/> (дата обращения: 25.03.2025).

она взяла кредит на 193 000 руб. и отправила деньги на «безопасный счет» по указанным реквизитам¹.

Схема 2. Приобретение железнодорожных, авиабилетов для встречи.

После некоторого периода общения на сайте знакомств мошенник заявляет, что готов приехать к жертве, но ему не хватает денег на покупку билетов. Он убедительно рассказывает о своей сильной привязанности и желании скорейшей встречи.

Схема 3. Доставка посылки, подарка из-за границы.

Мошенник сообщает о желании сделать дорогой подарок – ювелирное украшение, электронику, брендовую одежду – и отправляет его «курьерской службой или международной почтой». Далее создается ситуация «непредвиденные расходы» – задержка на таможне, страховка, дополнительная оплата доставки, налог на подарок и т. д. Мошенник просит жертву оплатить эти расходы, обещая все компенсировать при встрече.

Гражданин Н. реализовал мошенническую схему, основанную на 23 эпизодах мошенничества с использованием платформы онлайн-знакомств. Схема характеризовалась использованием вымышленных персонажей и легенд, адаптированных под психологический профиль жертв. Преступник устанавливал контакт с мужчинами и женщинами, представляясь военнослужащим, якобы находящимся в зоне боевых действий (Афганистан, Сирия, Ирак), либо отцом-одиночкой, воспитывающим тяжелобольную дочь. В обоих сценариях фигурировали намерение прибыть в Россию и просьба о получении личных вещей, предположительно отправленных через организацию «Красный Крест» или курьерскую службу. Содержание отправок варьировалось от ценных вещей (деньги, золото, бриллианты) до предметов, ассоциируемых с благотворительной деятельностью. После установления первичного контакта и формирования доверительных отношений гр. Н., используя другую вымышленную личность (сотрудника курьерской службы), связывался с жертвами и сообщал о необходимости оплаты расходов, связанных с доставкой груза. В качестве обоснования назывались различные предлоги: таможенные сборы, страхование, хранение, транспортировка, охрана. Для осуществления платежа предоставлялись реквизиты банковских карт или данные поддельных паспортов, находящихся в распоряжении гр. Н.²

Схема 4. Билет в кино.

Мошенник предлагает совместный досуг, например просмотр фильма в кинотеатре. Потерпевшему отправляется ссылка на поддельный сайт ки-

¹ Приговор Центрального районного суда г. Омска. Дело № 1-314/2024 // Судебные решения РФ. URL: <https://судебныерешения.рф/search> (дата обращения: 28.03.2025).

² Апелляционное определение Верховного Суда Республики Марий Эл. Дело № 22-175/2023 // Судебные решения РФ. URL: <https://судебныерешения.рф/search> (дата обращения: 28.03.2025).

нотеатра, визуально похожий на настоящий. Он, ничего не подозревая, переходит по ссылке и пытается оплатить билеты. После ввода банковских данных происходит списание средств, а затем начинаются проблемы, появляются ошибки или он вовсе перестает работать. Мошенник, играя роль заботливого партнера, предлагает помочь и обратиться в «техническую поддержку». Однако такой поддержки, естественно, не существует. Вместо этого мошенник придумывает новый предлог для выманивания денег, например необходимость внести «депозит» для «разблокировки» аккаунта или возврата средств. Эта сумма также перечисляется на счет мошенников.

В ходе расследования уголовного дела было установлено, что гр. А. познакомился с девушкой через мобильное приложение, которая предложила встретиться в кинотеатре. Для покупки билетов она прислала ему ссылку, по которой он перешел и ввел реквизиты своей банковской карты, нажав кнопку «оплатить». После отсутствия подтверждения оплаты он повторил операцию, в результате чего с его счета было списано 21 тыс. руб. Позже связь с девушкой прервалась, и она перестала выходить на связь¹.

Схема 5. Деньги на различные нужды (болезнь, похороны, оплата учебы и т. п.).

Мошенник, устанавливая доверительные отношения с жертвой, впоследствии сообщает о трагическом событии или серьезных финансовых трудностях, таких как болезнь близкого родственника, похороны, необходимость погашения долгов. Такие истории вызывают сильное эмоциональное сопереживание у жертвы, формируют чувства долга и желание помочь.

2. Мошенничества через сайты объявлений.

Схема 1. Мошенник-покупатель.

Мошенник пишет по объявлению, размещенному на сайте («Авито», «Юла», «Циан» и др.), продавцу с предложением купить товар, условием сделки является проведение платежа через «защищенный» сайт. Покупатель говорит, что уже внес свои средства в систему, а продавцу-жертве остается перейти по ссылке, ввести данные своей банковской карты и нажать кнопку «получить деньги», тем самым приводит к хищению доступа к банковской карте. Альтернативный вариант мошенничества предполагает запрос данных банковской карты под предлогом внесения задатка. Будущий потерпевший, не подозревая о преступных намерениях звонящего, сообщает номер своей банковской карты, срок ее действия и CVV-код, расположенный на оборотной стороне карты. Получив эти сведения, мошенник от имени потерпевшего через онлайн-сервисы делает заявку о покупке какого-либо товара или о переводе денежных средств с банковской карты потерпевшего. После этого мошеннику остается только узнать код

¹ Приговор Советского районного суда г. Красноярск. Дело № 1-1913/2024 // Судебные решения РФ. URL: <https://судебныерешения.рф/search> (дата обращения: 28.03.2025).

подтверждения операции, высланный по номеру телефона потерпевшего. Мошенник под каким-либо обманным предлогом выясняет у потерпевшего текст поступившего СМС-сообщения, после чего вводит этот код в онлайн-сервис, подтверждая тем самым покупку или перевод денежных средств потерпевшего; или же мошенник просит подойти к банкомату и выполнить ряд комбинаций, подключая мобильный банк и в последующем похищая денежные средства.

Схема 2. Мошенник-продавец.

Мошенник размещает на сайтах объявлений (сервисах по размещению частных объявлений) информацию о продаже какого-либо товара, сдаче в аренду жилых помещений или же оказании тех или иных услуг. Он просит продиктовать реквизиты банковской карты, поступивший СМС-код или перейти по ссылке, а также задаток путем перевода на его банковскую карту; завладев данными сведениями, получает доступ к мобильному приложению. Так, трое жителей Санкт-Петербурга, используя популярные сайты объявлений, находили продавцов, а затем в мессенджерах отправляли им фишинговые ссылки. Эти ссылки вели на поддельные сайты, где потерпевшие вводили данные своих банковских карт для получения оплаты за товар. В результате мошенники смогли похитить более 700 тыс. рублей у 30 человек из разных регионов России¹.

3. *Мошенничества с использованием интернет-магазинов (Wildberries, Ozon, «Мегамаркет», Lamoda, «Яндекс Маркет» и т. п.).*

Данный вид мошенничества начинается с сообщения в мессенджере о заманчивой скидке на товар, бесплатном подарке и т. п. Переходя по ссылке, он попадает на поддельный сайт, который выглядит как настоящий маркетплейс с личным кабинетом пользователя, предлагает товар по привлекательной цене. После оформления заказа и оплаты обнаруживает, что товар отсутствует, а деньги с его карты были списаны.

Гражданин А. смог осознать мошенническую схему. Так, в январе 2023 г. он хотел приобрести кофемашину на «Мегамаркете» по заниженной стоимости. После оплаты заказа ему пришло уведомление об отмене, но деньги вернулись. На следующий день он повторил попытку заказа и ситуация повторилась. Вскоре пришло сообщение в Telegram от предполагаемого продавца с информацией о его заказе. Продавец утверждал, что товар закончился, но предлагал аналогичную модель на Ozon по более выгодной цене. А. согласился получить предложение на почту, на которую ему пришло письмо с фишинговой ссылкой, маскирующейся под официальный сайт Ozon. При переходе по ссылке пользователь попал на сайт

¹ Зарабатывавшие на фишинговых сайтах предстанут перед судом // Прокуратура Санкт-Петербурга. URL: https://epp.genproc.gov.ru/web/proc_78/massmedia/news?item=100885263 (дата обращения: 28.03.2025).

с доменным именем, отличающимся от настоящего Ozon. Гражданин А. понял мошенническую схему и обратился в правоохранительные органы¹.

4. Мошенничества, совершенные с использованием сервисов для совместных поездок («едем.рф», BlaBlaCar).

Мошенники создают профили и размещают объявления, которые на первый взгляд ничем не отличаются от настоящих. Они указывают цены, соответствующие рыночным условиям, и даже могут использовать фотографии реальных водителей или автомобилей. Когда пользователь проявляет интерес к такому объявлению и откликается на него, мошенники начинают взаимодействие через чат на сайте BlaBlaCar. В ходе общения злоумышленники предлагают жертве «купить билет» по специальной ссылке, утверждая, что это необходимо для подтверждения бронирования. На первый взгляд, адрес сайта может выглядеть правдоподобно и содержать название сервиса BlaBlaCar, что вводит пользователя в заблуждение. Однако на самом деле это поддельный сайт, который сильно отличается от официального адреса платформы. Когда жертва переходит по этой ссылке, она попадает на страницу, которая визуально напоминает оригинал, но предназначена для кражи личных данных и финансовой информации. Мошенники могут запрашивать ввод данных банковской карты или другие финансовые сведения под предлогом оплаты за поездку. После ввода информации жертва осознает, что стала жертвой мошенничества, когда деньги списываются с ее счета, а «водитель» перестает отвечать.

Гражданка Б. забронировала поездку у водителя через приложение BlaBlaCar. В процессе общения с водителем ей поступила ссылка на завершение бронирования. При переходе по указанной ссылке гр. Б. попала на сайт, который выглядел идентично официальному сайту BlaBlaCar. Ей было предложено ввести данные своей банковской карты для завершения бронирования. После ввода данных карты и завершения процесса бронирования водитель отменил заказ, но деньги были списаны с карты гр. Б.²

5. Единый портал государственных и муниципальных услуг (функций) («Госуслуги»).

Мошенники рассылают СМС или электронные письма, которые выглядят как официальные уведомления, включая логотипы и шаблоны, схожие с теми, что используются на портале «Госуслуги», о штрафах, начислении выплат и других услугах.

¹ Приговор Октябрьского районного суда г. Екатеринбурга. Дело № 1-210/2023 // Судебные решения РФ. URL: <https://судебныерешения.рф/search> (дата обращения: 28.03.2025).

² Приговор Кузнецкого районного суда Пензенской области. Дело № 1-188/2023 // Судебные решения РФ. URL: <https://судебныерешения.рф/search> (дата обращения: 28.03.2025).

6. Инвестирование.

Существует множество сервисов и платформ для инвестирования, которые могут быть использованы как законно, так и в мошеннических схемах. Приведем некоторые из наиболее распространенных типов сервисов, через которые может происходить мошенничество.

Схема 1. Криптовалютные биржи (BYBIT, MEXC).

Мошенничество в сфере криптовалют часто основано на обмане и манипуляциях доверием инвесторов. Мошенники могут утверждать, что обладают алгоритмами для предсказания цен или предлагают «волшебные» биржи с гарантированной прибылью. Из-за анонимности криптовалюты отследить переводы практически невозможно, что делает возврат средств крайне сложным. Неопытные пользователи легко попадаются на уловки, завуалированные терминами и сложными схемами, например «если вы отошлете криптовалюту на такой-то адрес, ее прогонят через блокчейн, используя миксеры и прокси-протоколы, исполнится смарт-контракт на фьючерсную поставку – и вам вернется в два раза больше денег». В конечном итоге жертвы остаются без своих денег, не имея возможности вернуть их обратно.

Схема 2. Мошенничество на pre-ИРО инвестициях.

Направлено на опытных инвесторов, знакомых с процессом ИРО. Мошенники имитируют инвестиционные сделки, продавая несуществующие акции. Они ждут объявления крупных компаний о выходе на биржу и ищут потенциальных инвесторов. Представляясь брокерами, предлагают купить акции по привлекательной цене до их официального размещения. Инвесторы часто соглашаются из-за заманчивой скидки на акции известных компаний. После получения оплаты мошенники исчезают, оставляя инвесторов ни с чем. Чтобы избежать подобных ситуаций, важно тщательно проверять продавца, запрашивая лицензию и изучая его репутацию на рынке.

Таким образом, можно констатировать, что способ совершения преступления среди данных, составляющих криминалистическую характеристику, являются особо значимым, так как имеет разветвленные корреляционные связи, позволяющие определить комплекс других обстоятельств противоправного деяния. Существует прямая зависимость количества (множественности) способов совершения преступлений в сфере информационных технологий от совершенствования этих самых технологий.

§ 3. Особенности производства следственной проверки

Проверка исходной информации имеет первостепенное значение в уголовно-процессуальной деятельности на стадии возбуждении уголовного дела. Принятие законного решения по сообщению о преступлении

возможно лишь после всесторонней, объективной проверки и оценки собранной информации.

И. В. Александровым верно отмечается, что «роль и значимость стадии возбуждения уголовного дела существенно возросли. По своим характеристикам с точки зрения значимости в структуре расследования она не уступает самому предварительному следствию. На стадии возбуждения решаются вопросы не только законности и обоснованности возбуждения дела, но и задачи последующих стадий судопроизводства. Доследственная проверка стала, по своей сути, формой расследования, и уголовное дело возбуждается лишь тогда, когда установлена судебная перспектива уголовного дела»¹.

Способы проверки сообщения о преступлении – это совокупность законодательно установленных действий, реализуемых уполномоченными лицами в процессуальной форме для установления наличия или отсутствия признаков преступления, оснований отказа в возбуждении уголовного дела, а также для получения и закрепления доказательственной информации.

Особенности производства проверочных действий определяет специфика способов совершения рассматриваемой категории преступлений. На первоначальном этапе необходимо в кратчайшие сроки с учетом допустимых уголовно-процессуальном законом средств получить максимально возможный объем информации о наличии либо отсутствии оснований для возбуждения уголовного дела, об обстоятельствах произошедшего².

На стадии рассмотрения сообщения о дистанционном мошенничестве, совершенном с использованием интернет-сервисов, у заявителя требуется выяснить обстоятельства произошедшего. Объяснения лица или лиц, пострадавших от противоправных деяний, в зависимости от следственной ситуации и обстоятельств события, должны содержать следующие сведения: персональные данные заявителя – подробную информацию о банковском счете и банковской карте заявителя (полное наименование банка и иные его реквизиты, включая юридический адрес, дата, место, цель открытия банковского счета и приобретения банковской карты); о выполнении транзакций с использованием банковского счета и банковской карты потерпевшего (сведения о проводимых финансовых операциях, обстоятельствах использования банковского счета, наименование сервиса дистанционного банковского обслуживания, круг лиц, имеющих доступ к счету (карте)); о неправомерном доступе к банковскому счету (карте) третьих лиц (дата и время обнаружения хищения денежных средств с бан-

¹ Александров И. В. Проблемные аспекты формирования методики расследования современных преступлений, совершаемых в сфере экономики // Вестник Московского университета. Сер.: Право. 2014. № 4. С. 38.

² Валюлин Р. Р., Козлов В. В. Расследование телефонных мошенничеств : учеб. пособие. Барнаул : Барнаульский юридический институт МВД России, 2023. С. 18.

ковского счета, обстоятельства, при которых потерпевшему стало известно о хищении денежных средств).

Подлежит выяснению характеристика электронных устройств и программных средств, используемых заявителем до и в момент совершения в его отношении преступных действий (наименование электронного устройства, модель, марка, серийный номер, наименование программных средств); наименование оператора сотовой связи, абонентский номер, привязанный к банковскому счету (карте) заявителя, Ф. И. О лица, на которого зарегистрирован абонентский номер; каким образом познакомился с преступником, в какой социальной сети; временной промежуток общения в интернет-сервисах, максимально дословное содержание разговора или переписки с мошенником: кем представился, о чем говорил, что предлагал или убеждал сделать; характеристика конфиденциальной информации, которую заявитель сообщил мошеннику, а также обстоятельства, повлекшие предоставление последнему персональных данных или банковских сведений; характеристика требований или дополнительных указаний, поступавших от злоумышленника в момент совершения преступления, психологических приемов воздействия на потерпевшего (условия, которые вызвали доверие и спровоцировали сообщение конфиденциальной информации подозреваемому, описание психологических приемов, которые применил подозреваемый для доступа к информации или денежным средствам потерпевшего); наличие сохранившейся переписки, фотографий в социальной сети или мессенджере, в которых заявитель познакомился с преступником; если поступали звонки с телефона, то абонентский номер этого телефона, описание обстоятельств разговора; пол собеседника; дата (ы), условия и сумма перевода денежных средств; способы перечисления денежных средств (мобильные устройства, платежные терминалы); пароли для доступа в личный кабинет банков через Интернет; наличие документов, подтверждающих перевод денежных средств; конечная сумма причиненного материального ущерба.

В случае совершения хищения в результате телефонного разговора со злоумышленником внимание следует уделить фонетическим и лингвистическим признакам речи (высота, сила, тембр, интонация голоса; общий уровень образования и степень культуры; отсутствие или наличие дефектов речи – хрипота, картавость, шепелявость, заикание; присутствие в разговоре специальных терминов, специфических речевых оборотов, жаргонизма); возможности опознания мошенника по голосу по конкретным приметам, что позволит определить примерный облик человека. С целью сверки в последующем с данными детализации телефонных переговоров необходимо установить качество телефонной связи и длительность разговора между заявителем и мошенником.

Объяснение могут дать и члены семьи заявителя, очевидцы произошедшего, сотрудники банковской организации, компании оператора связи.

При переводе денежных средств мошеннику через банкомат установлению подлежит информация о его наименовании, местонахождении и др. Следует выяснить, кроме того, данные о банковской карте (счете): время и обстоятельства последнего использования карты, месторасположение сервисного предприятия или банкомата, где карта применялась в последний раз, перечень услуг или приобретенных товаров (предметов). Приведенный перечень обстоятельств не считается исчерпывающим. В зависимости от ситуации и способа совершения мошенничества, требующих уточнения, он может быть дополнен.

Следователь в ходе проведения процессуальной проверки в порядке ст. 144 УПК РФ необходимо:

- принять меры к получению от заявителя счетов, чеков, квитанций и иных документов, подтверждающих факт перевода денежных средств, приобщить их к материалам проводимой доследственной проверки;

- инициировать процедуру получения заявителем информации от кредитной организации о движении денежных средств по его банковской карте (счету) с приобщением их к материалам проводимой доследственной проверки;

- рекомендовать заявителю обратиться к оператору сотовой связи о предоставлении детализации соединений его абонентского номера телефона, приобщить данную выписку к материалам проводимой доследственной проверки;

- произвести осмотр места происшествия с целью фиксации обстановки, обнаружения и изъятия следов в виде электронной информации, предметов – носителей такой информации, иных предметов и документов, которые могут иметь значение для раскрытия и расследования преступления.

Если заявитель в рамках общения с мошенником использовал компьютер, в протоколе следует указать расположение компьютера (стационарный компьютер, ноутбук, планшетный компьютер), устройств телекоммуникации (Wi-Fi-роутер, модем), порядок их соединения (сопряжения, связи) между собой (беспроводная связь, организованная компьютерная сеть); назначение каждого устройства, его название, серийный номер, комплектацию (сетевые карты, соответствующие разъемы, наличие дисководов), наличие соединения с сетями телекоммуникации, функциональное состояние устройств на момент осмотра; содержание информации, отображаемой на мониторе (дисплее). При установлении факта функционирования интернет-ресурса, с использованием которого совершены противоправные действия (не удален, не заблокирован), в протоколе осмотра места происшествия следователь указывает представленную на сайте контактную информацию, род деятельности ресурса, наличие отзывов, приобщает распечатки с интернет-сайта, экранную копию (снимок экрана) ресурса се-

ти Интернет, на которой должны быть видны реквизиты: адресная строка страницы, идентификатор страницы.

В случаях и порядке, предусмотренных УПК РФ, в ходе осмотра места происшествия следователь изымает системные блоки персональных компьютеров или установленные в них накопители на жестких магнитных дисках, иные электронные носители информации, а также устройства телекоммуникации. В рамках осмотра места происшествия с письменного согласия заявителя производит осмотр его мобильного телефона с целью отыскания и закрепления следующей информации (в случае хищения с использованием мобильного телефона заявителя): IMEI мобильного устройства заявителя; наличия SIM-карт с абонентскими номерами заявителя; информации, содержащейся в журнале вызовов мобильного устройства, в банке СМС-сообщений, в записной книжке (контактах) внутренней памяти мобильного устройства или SIM-карты; из сохраненных текстов переписки между соответствующими абонентскими устройствами посредством СМС-сообщений или других мессенджеров, например WhatsApp, Telegram; об истории посещения интернет-сайтов; о поиске через установленный на устройстве браузер в сети Интернет сведений, имеющих отношение к исследуемому событию; об использовании соответствующих интернет-сервисов, позволяющих осуществлять виртуальный оборот денежных средств (различные электронные кошельки); о регистрации в качестве пользователя в социальной сети, на личной странице которого могут содержаться данные, представляющие интерес для расследования (социальные сети «ВКонтакте», «Одноклассники» и др.) о сохраненных логинах и паролях (некоторые установленные на персональный компьютер и мобильные средства связи утилиты (программы) позволяют сохранять информацию о логинах и паролях всех когда-либо посещенных сайтов); о типе программного обеспечения мобильного устройства заявителя, наличии в нем собственной антивирусной программы и ее активности¹.

В рамках осмотра следователь детально исследует соответствующие разделы приложения дистанционного банковского обслуживания (далее – ДБО) (мобильного банка) «История платежей», «Последние операции», в которых зафиксировано движение денежных средств по счету (банковской карте), делает снимки экрана мобильного устройства, отображающего данную информацию, с помощью самого устройства (если позволяет его аппаратно-программное обеспечение) или фотографирует экран другим устройством, позволяющим получить фотографическое изображение. Информация, находящаяся в памяти устройства, отражающая переписку с причастным лицом с помощью СМС-сообщений, в WhatsApp, Telegram и иных мессенджерах, сохраненные страницы в браузере из социальных

¹ Старостенко Н. И. Первоначальный этап расследования хищений, совершенных с применением методов социальной инженерии и информационно-телекоммуникационных технологий : дис. ...канд. юрид. наук. Краснодар, 2023. С. 150.

сетей, электронных торговых площадок (и их мобильных приложений) вносятся в протокол и фотографируются.

Информация, полученная в ходе осмотра мобильного устройства, заносит в протокол, а фотоматериалы приобщаются в форме фототаблицы. Осмотр, как правило, проводится с участием специалиста. При рассмотрении сообщения о мошенничестве следователь проводит осмотр места передачи наличных денежных средств, перевода, а при установлении – места зачисления денежных средств. При этом денежные средства заявителем могут быть зачислены на указанный ему номер телефона, на счет электронного кошелька или банковский счет (карту). При использовании для перевода денежных средств как на лицевой счет абонентского номера телефона, так и на счет электронного кошелька заявителем платежного терминала самообслуживания или банкомата, при снятии заявителем с их использованием наличных денежных средств с последующей их передачей непосредственно виновному либо его доверенному лицу следователь осматривает банкомат или платежный терминал, указывает в протоколе их идентификационные номера, которые в дальнейшем используются для направления запроса администратору платежной системы или оператору сотовой связи с целью получения подтверждающей информации о факте перевода (зачисления) денежных средств. Описание таких объектов, как банкомат, терминал, банковская карта, требует использования специальной терминологии, в связи с этим помощь в собирании следов может быть оказана не только специалистом-криминалистом, но и сотрудником кредитного учреждения, знакомым с работой устройств и принципами действия инфраструктуры по обслуживанию держателей банковских карт. Кроме того, для осмотра содержимого банкомата и составления акта по его инкассации целесообразно приглашать бухгалтера, представляющего интересы банка-эквайера¹. При необходимости к осмотру привлекают соответствующих специалистов, в том числе поставщика данной техники или специалиста центра технического обслуживания.

При передаче денежных средств непосредственно виновному либо его доверенному лицу производится осмотр не только места передачи, но и прилегающей территории в целях установления наличия и изучения записи камер видеонаблюдения и домофонов, имеющих функцию видеозаписи, в месте совершения преступления (расположенных на зданиях учреждений, организаций различных форм собственности), а также частных лиц.

Следователь в рамках доследственной проверки дает указание оперативному сотруднику:

– установить анкетные данные владельца абонентского номера связи (посредством ресурсов Бюро специальных технических мероприятий

¹ Рябина И. К., Ряполова Я. П., Чистилина Д. О. Актуальные проблемы выявления и расследования дистанционных хищений с банковского счета // Вестник Белгородского юридического института МВД России имени И. Д. Путилина. 2023. № 4. С. 36–37.

Управления МВД России (далее – БСТМ УМВД) области Единой информационно-телекоммуникационной сети (ЕИТКС)), используемого при совершении преступления: (Ф. И. О абонента, дата рождения, адрес регистрации, паспортные и иные данные, имеющие значение для раскрытия преступления);

- при внесении в подсистему программно-технического комплекса интегрированного банка данных федерального уровня (далее – ПТК ИБД-Ф) «Дистанционное мошенничество» первичных сведений о хищении, совершенном с использованием информационно-телекоммуникационных технологий (ИТТ), проверить наличие совпадений по реквизитному составу с иными дистанционными хищениями;

- отработать информацию о входящих и исходящих звонках (согласно детализации вызовов абонентского номера потерпевшего), по абонентским номерам, использованным при совершении преступления, провести мероприятия по установлению их принадлежности;

- установить получателей денежных средств, похищенных у потерпевшего (согласно выписке о движении денежных средств по счету потерпевшего), провести дальнейшие мероприятия по их проверке на причастность к совершению преступления.

При выявлении совпадений в подсистеме ПТК ИБД-Ф «Дистанционное мошенничество» оперативный сотрудник направляет запросы в территориальные органы внутренних дел МВД России на районном уровне, подчиненные УМВД области, либо в иные территориальные органы МВД России.

Учитывая, что способы совершения мошенничеств с использованием интернет-сервисов имеет свою специфику, рассмотрим алгоритмы по проведению доследственной проверки в конкретных случаях.

При проверке сообщения о хищении под предлогом сделки, связанной с куплей-продажей имущества через сеть Интернет (на площадках бесплатных объявлений «Авито», «Юла» и т. д.):

I. Следователь (дознатель) производит опрос заявителя по следующему примерному перечню вопросов:

- 1) дата (период времени) и на каком сайте, в какой социальной сети, в какой группе социальной сети он нашел объявление о продаже товара; контактные данные продавца в объявлении о продаже; сохранились ли у него данные объявления (№ объявления, ID страницы);

- 2) имелись ли отзывы, комментарии к объявлению о продаже, если да, то какие;

- 3) характеристики продаваемого товара, указанные продавцом в объявлении о продаже, и условия купли-продажи: предоплата, сроки и вид поставки товара, ответственности сторон;

- 4) сохранились ли у потерпевшего фотографические изображения продаваемого товара (при положительном ответе на указанный вопрос по-

сле возбуждения уголовного дела следует выемкой изъять, осмотреть, дать юридическую оценку значимости);

5) каким образом, когда (дата, время) потерпевший связался с продавцом;

6) как продавец представился потерпевшему (назвал Ф. И. О, контактные данные, место своего нахождения, место нахождения товара); что именно сообщил продавец о продаваемом товаре, об условиях оплаты товара, условиях, сроках и способах его доставки покупателю (потерпевшему);

7) описание голоса продавца, сможет его опознать или нет (по каким приметам);

8) связывался ли заявитель с продавцом посредством электронной почты, если да, то какой адрес почтового ящика (аккаунта) заявителя, адрес почтового ящика (аккаунта) продавца;

9) сохранились ли сообщения в его ящике электронной почты (если да, то после возбуждения уголовного дела произвести выемку; в порядке ст. 186.1 УПК РФ обратиться в суд с ходатайством о получении информации о лице, зарегистрировавшем почтовый ящик (аккаунт), содержании переписки за интересующий период времени);

10) когда (дата, период времени), каким образом (через банкомат, посредством услуги «Сбербанк Онлайн», «Мобильный банк»), в каком размере заявитель перечислил на какой счет (№ счета либо банковской карты, открытые на чье имя) денежные средства в счет оплаты за якобы приобретаемый товар;

11) если заявитель осуществил перевод денежных средств со своей банковской карты на банковскую карту неизвестного посредством услуги «Сбербанк Онлайн», через личный кабинет, установить место выхода заявителя в сеть Интернет (с какого компьютера, ноутбука, планшета, с использованием какого модема, Wi-Fi-роутера, их MAC-адреса, логины, пароли, какая компания-провайдер предоставляла в день хищения заявителю услуги связи по выходу в Интернет);

12) дата и место открытия счета (банковской карты), с которой заявитель перечислил денежные средства;

13) каким образом известил «продавца товара» о перечислении денежных средств на указанную им банковскую карту (виртуальный кошелек);

14) что именно ему сообщил после подтверждения оплаты.

II. Подготавливает и направляет запрос в администрации интернет-сайтов «Авито», «Юла», в котором указывает необходимость предоставления сведений об IP-адресах пользователей сети Интернет, просматривавших данное объявление за интересующий период (в случае если заявитель продавец), либо предоставления информации о лице, разместившем объявление о продаже, IP-адресах, используемых в период его размещения (в случае если заявитель покупатель); предоставлении аналогичной ин-

формации об иных объявлениях данных пользователей, установленных при анализе cookie-файлов.

III. Следует отметить, что после принятия решения о возбуждении уголовного дела при установлении адреса электронного почтового ящика (указанного как аккаунт), использованного причастными лицами (путем входа на «персональную страницу» пользователя) в порядке, предусмотренном ч. 7 ст. 185 и ст. 186.1 УПК РФ, следователь возбуждает перед судом ходатайство о производстве выемки информации со страницы пользователя.

IV. В случае если заявителем получен товар, несоответствующий условиям договоренности, через «Почту России» либо курьерской службой, направляет запросы в отделение «Почты России» либо иные почтовые службы о получении информации о почтовом отправлении и наложенном платеже и в курьерскую службу, осуществившую доставку посылки.

При проверке сообщения о хищении, совершенном с использованием фишинговых сайтов в сети Интернет (переход заявителем по ссылке и введение данных банковской карты), вредоносного программного обеспечения (переход по ссылке), а также установки программы для удаленного управления (доступа):

I. Выясняет у заявителя обстоятельства совершенного преступления по примерному перечню вопросов:

1) время, место и обстоятельства хищения денежных средств; реквизиты банковской карты, с которой совершено хищение денежных средств, а также подключенной услуги «Мобильный банк» с указанием номеров телефонов, к которым она привязана; если услуга подключена самим заявителем, то с какого времени и каким способом (посредством заявления о подключении в офисах банковских учреждений или посредством банкоматов);

2) с какого времени заявитель пользуется абонентским номером, к которому данная услуга подключена, так как не исключается перевыпуск номера оператором связи после истечения шести месяцев неиспользования абонентского номера с оформлением номера на иное лицо; модель телефона, подключенного к услуге «Мобильный банк», используемая операционная система в телефоне (Android, IOS или иное);

3) наличие установленных антивирусных программ на мобильном устройстве; какие мобильные приложения устанавливались в последнее время; способ установки (из официальных источников (сайтов) AppStore (Apple), PlayMarket (GooglePlay), с сайта банка-эмитента банковской карты (банковского продукта, в случае, например, открытия банковского счета без выпуска банковской карты);

4) совершались ли операции через мобильное устройство (телефон, планшет) или компьютер, вводились ли иным способом данные банковской карты или хранились ли сведения о ней в устройствах;

5) осуществлялся ли с данного устройства доступ в сеть Интернет, в том числе автоматически (например, при установке графика автоматического обновления приложений, то каких именно приложений);

6) осуществлял ли кто-либо с использованием данных банковской карты (номера, срока действия, данных владельца, CVC / CVC2-кода (три цифры, расположенные на обратной стороне банковской карты)) заявителя покупку товаров, заказ услуг через Интернет;

7) поступали ли на мобильное устройство сообщения, содержащие ссылки на интернет-ресурсы. Если да, то когда, от кого, содержание сообщений; осуществлялся ли переход по данным ссылкам, если да, то каков результат (было установлено приложение, установка приложения неожиданно прервалась, мобильное устройство «зависло», потребовалась перезагрузка, приложение «попросило» ввести определенные данные);

8) производился ли ремонт мобильного устройства до или после обнаружения факта хищения, где и кем;

9) в какое время и с какого номера поступали сообщения о снятии денежных средств, их содержание;

10) местонахождение мобильного телефона в настоящее время, а также желает ли заявитель добровольно предоставить его для производства компьютерной экспертизы с указанием необходимых паролей;

11) обращался ли заявитель в банк, имеются ли у него выписки о движении денежных средств по карте, ответы по обращениям (в случае наличия таковых приобщить их к материалам проводимой проверки);

12) является ли ущерб значительным для заявителя, если да, то обязательно отразить обстоятельства, подтверждающие это; каков состав семьи, близкие родственники, лица, находящиеся на иждивении, размер доходов и расходов заявителя по состоянию на момент совершения в отношении него преступления.

II. В целях установления интернет-ресурсов, которые посещал заявитель, изучает либо поручает сотруднику оперативного подразделения изучить историю интернет-браузеров, устанавливает и сохраняет ссылки на сайты, сведения о регистраторе доменного имени посредством интернет-ресурсов: <https://2ip.ru/whois>, <https://www.reg.ru/whois/>.

III. Определяет целесообразность изъятия компьютера и (или) мобильных устройств в рамках осмотра места происшествия для последующего назначения компьютерной экспертизы в целях установления факта использования вредоносной программы и технических сведений об устройствах, используемых лицом, причастным к совершенному преступлению, для осуществления действий на устройствах заявителя.

IV. В случае использования программного обеспечения (TeamViewer, AnyDesk и др.), предназначенных для удаленного доступа к устройству заявителя, производит его осмотр либо поручает осмотр сотруднику оперативного подразделения с целью выявления наличия log-файлов, установле-

ния ID (идентификаторов) устройств заявителя и лица, причастного к совершенному преступлению, которые хранятся в журнале файлов. Для этого необходимо обнаружить на устройстве заявителя файл `Connexions_incoming`, в котором отображаются логи входящих и исходящих соединений. При наличии этих данных осуществляет их фиксацию, изъятие и приобщение к материалам проверки и (или) уголовного дела в соответствии с требованиями УПК РФ.

V. При переходе потерпевшим по ссылке и введении данных банковской карты, вследствие чего произошло списание денежных средств со счета банковской карты потерпевшего, устанавливает в ходе допроса потерпевшего, а также путем осмотра сотового телефона наличие СМС-сообщения от банка-эмитента (банк, выпускающий и обслуживающий банковские карты) с информацией о платежной системе (сервисе), посредством которой произошло списание денежных средств со счета потерпевшего.

VI. Следователь подготавливает и направляет запрос в банк-эмитент, обслуживающий счет банковской карты потерпевшего, о предоставлении сведений из внутреннего процессингового центра о назначении и подтверждении перевода денежных средств, произведенного с банковской карты потерпевшего, с указанием наименования и географического местоположения мерчанта, MCC-кодов произведенных операций. Запрос направляется во всех случаях списания денежных средств со счета банковской карты потерпевшего посредством национальной платежной системы (сервиса), а также посредством системы или сервиса, не имеющего представительства на территории Российской Федерации (например, PAY2CARD).

VII. При получении сведений из банка подготавливает и направляет запрос в банк-эмитент, обслуживающий банковскую карту, на счет которой поступили похищенные денежные средства.

При проверке сообщения о хищении, совершенном с использованием сети Интернет в социальных сетях, в том числе путем взлома страниц:

I. Выясняет у заявителя обстоятельства совершенного преступления по примерному перечню вопросов:

1) имеется ли по месту его проживания персональный компьютер, ноутбук, планшет и интернет-соединение, если да, то каким провайдером предоставляются услуги связи по выходу в сеть Интернет, под каким логином, паролем; MAC-адрес устройства;

2) кто, кроме заявителя, имеет доступ к компьютеру, ноутбуку, планшету, иному устройству по выходу в сеть Интернет;

3) зарегистрирован ли в социальных сетях; в каких; логины и пароли; идентификационный номер профиля заявителя в социальных сетях;

4) кому известны реквизиты его банковской карты (номер на лицевой стороне, пин-код, номер на оборотной стороне карты (CVC), дата, по которой действительна карта);

5) подключены ли услуги «Мобильный банк» и «Интернет-банк», если да, то к какой сим-карте, с каким номером, у кого находится данная сим-карта, передавал ли он кому-либо ее, терял ли, восстанавливал;

6) осуществлялся ли выход с персонального компьютера по его месту жительства в социальные сети иными лицами;

7) осуществлял ли заявитель сам платежи в пользу данного сайта, имелись ли случаи санкционированного и несанкционированного удаленного доступа к его компьютеру (если да, то когда и при каких обстоятельствах);

8) оснащен ли компьютер заявителя программным обеспечением, препятствующим несанкционированному удаленному доступу (программами-брандмауэрами);

9) осуществлялся ли выход заявителем или иным лицом с телефона в социальные сети и каким образом (через поисковые системы браузера или сразу путем перехода на сайт социальной сети, выяснить возможность выхода на сайты-клоны);

10) какие программы и через какие браузеры были загружены заявителем в сотовый телефон и в какие периоды; оснащен ли сотовый телефон заявителя антивирусным программным обеспечением.

II. Следует отметить, что в последующем, после решения вопроса о возбуждении уголовного дела при установлении адреса электронного почтового ящика и (или) аккаунта, использованного причастными лицами (путем входа на «персональную страницу» пользователя в социальной сети), в порядке, предусмотренном ч. 7 ст. 185 и ст. 186.1 УПК РФ, следователь возбуждает перед судом ходатайство о производстве выемки информации со страницы пользователя в социальной сети. Направляет запрос администратору социальной сети («ВКонтакте», «Одноклассники») с приложением постановления суда о предоставлении сведений об IP-адресах, с которых осуществлялся доступ к указанной электронной странице с момента регистрации по настоящее время; контактной информации (включая абонентские номера сотовой связи, электронную почту и фамилию, имя, отчество, которые были указаны им при регистрации); геометках или координатах, при помощи которых можно определить его последнее местонахождение; информации со страницы пользователя в социальной сети; аналогичной информации по иным страницам социальной сети данного пользователя, установленных при анализе cookie-файлов.

III. Подготавливает и направляет обязательное для исполнения указание о производстве отдельных следственных действий и оперативно-розыскных мероприятий в Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий МВД России (далее – УБК МВД России) по субъекту в случае хищения, сопровождающегося неправомерным доступом к охраняемой законом компьютерной информации (взломом аккаунтов социальных сетей).

При проверке сообщения о хищении, совершенном под предлогом заказа поездки посредством сервиса «Яндекс.Такси»:

I. Выясняет у заявителя обстоятельства совершенного преступления:

1) с какого времени заявитель работает в такси с использованием приложения «Яндекс.Такси», какие персональные данные содержатся в его аккаунте (абонентский номер, фамилия, имя, отчество, данные автомобиля);

2) каким образом, когда (дата, время) с заявителем связался заказчик поездки; велась ли переписка в приложении, либо сразу поступил звонок от клиента, с какого абонентского номера; как клиент представился (назвал фамилию, имя, отчество, контактные данные, место своего нахождения, конечный адрес поездки), суть разговора;

3) описание голоса клиента, сможет ли его опознать или нет (по каким приметам);

4) после возбуждения уголовного дела выяснить у потерпевшего, сохранились ли сообщения в его ящике электронной почты, если да – произвести выемку и в порядке ст. 186.1 УПК РФ обратиться в суд с ходатайством о получении информации о лице, зарегистрировавшем почтовый ящик (аккаунт), содержании переписки за интересуемый период;

5) какие персональные сведения (номер банковской карты, код из СМС-сообщения, SVC) клиент просил передать для осуществления оплаты поездки;

6) если заявитель передал причастному лицу доступ к своему личному кабинету, то установить место выхода заявителя в сеть Интернет (с какого компьютера, ноутбука, планшета, с использованием какого модема, Wi-Fi-роутера, их MAC-адреса, логины и пароли, какая компания-провайдер предоставляла в день хищения последнему услуги связи по выходу в Интернет).

II. В кратчайший срок подготавливает и направляет запрос в адрес организации, обслуживающей сервис «Яндекс.Такси», о предоставлении сведений о лице, осуществившем заказ поездки, с указанием его абонентского номера, электронного адреса, использованного при регистрации аккаунта (личного кабинета клиента); IP-адресах, используемых для входа в личный кабинет; записи разговора водителя такси либо переписки (при наличии), а также об абонентском номере, при помощи которого осуществлялось соединение; геолокации клиента в момент осуществления заказа согласно данным приложения и конечном адресе заказа; форме оплаты, установленной в приложении (безналичный или наличный), в случае безналичной формы – указать сведения о банковской карте; ранее осуществленных заказах при помощи интересуемого аккаунта с указанием адресов.

При проверке сообщения о хищении, совершенном посредством сети Интернет, путем размещения информации о предоставлении услуг досуга:

I. Выясняет у заявителя обстоятельства совершенного преступления.

II. В целях установления интернет-ресурсов, на которых заявитель нашел объявление о предоставлении услуг досуга, анализирует либо поручает изучение сотруднику оперативного подразделения историю интернет-браузеров, устанавливает и сохраняет ссылки на сайты. Дает обязательное для исполнения указание органу дознания об установлении сведений о регистраторе доменного имени посредством интернет-ресурсов: <https://2ip.ru/whois>, <https://www.reg.ru/whois>.

III. Направляет запрос регистратору доменных имен о предоставлении информации: о лице, на которое зарегистрировано доменное имя, с указанием его паспортных данных и контактных абонентских номеров телефонов; об e-mail-адресе, с которого поступали заявки на регистрацию данного и других доменных имен; о способах оплаты, производимых при регистрации доменного имени; об IP-адресах, используемых для входа в личный кабинет администратора созданного интернет-сайта; о хостинге (размещение файлов сайта на сервере, на котором запущено программное обеспечение); о доменных именах, зарегистрированных данным пользователем, установленным при анализе cookie-файлов.

IV. При получении от регистратора информации об IP-адресах, использованных для входа в сеть Интернет при создании интернет-сайта, а также его администрировании, посредством справочных интернет-ресурсов (www.reg.ru, www.whois-service.ru, www.2ip.ru) устанавливает компанию интернет-провайдера.

V. При установлении принадлежности IP-адреса к интернет-провайдеру направляет в его адрес запрос, в котором указывает о необходимости предоставления следующих сведений: кому в точное время (дата, час, минута, секунда) предоставлен IP-адрес (номер TCP / UDP-порта), о местонахождении абонента, использующего данный IP-адрес, дате регистрации договора предоставления услуг связи в сети Интернет, с кем заключен договор (фамилия, имя, отчество, дата рождения, место регистрации, паспортные данные), о логине, пароле, при помощи которых осуществляется доступ клиента в сеть Интернет, о MAC-адресе устройства (MAC-адрес сетевой карты пользователя), с которого осуществлялся выход в сеть Интернет в момент совершения преступления; если выход в сеть Интернет осуществлялся с мобильных устройств – предоставить информацию об их IMEI-номерах.

При проверке сообщения о хищении, совершенном посредством сети Интернет под предлогом оказания пассажирских услуг через сервис (приложение) по поиску попутчиков BlaBlaCar:

I. Выясняет у заявителя обстоятельства совершенного преступления.

II. В кратчайший срок с момента возбуждения уголовного дела подготавливает и направляет запрос в организацию, обслуживающую сервис BlaBlaCar, в котором в обязательном порядке указывает о необходимости предоставления сведений об IP-адресах пользователей сети Интернет, про-

сматривавших информацию о поездке за определенный период (в случае если потерпевший пассажир), либо предоставления информации о лице, разместившем объявление о предстоящей поездке, IP-адресов, используемых в период размещения объявления (в случае если заявитель водитель); предоставлении аналогичной информации об иных объявлениях данных пользователей, установленных при анализе cookie-файлов.

III. В случае использования лицом, причастным к совершенному преступлению, ссылки для оплаты либо бронирования поездки дает поручение сотруднику оперативного подразделения об установлении сведений о регистраторе доменного имени посредством следующих интернет-ресурсов: <https://2ip.ru/whois>, <https://www.reg.ru/whois>.

IV. Направляет запрос регистратору доменных имен, о предоставлении информации: о лице, на которое зарегистрировано доменное имя, с указанием его паспортных данных и контактных абонентских номеров телефонов; об e-mail-адресе, с которого поступали заявки на регистрацию данного и других доменных имен; о способах оплаты, производимых при регистрации доменного имени; об IP-адресах, используемых для входа в личный кабинет администратора созданного интернет-сайта; о хостинге (размещение файлов сайта на сервере, на котором запущено программное обеспечение); о доменных именах, зарегистрированных данным пользователем, установленным при анализе cookie-файлов.

При проверке сообщения о хищении, совершенном под предлогом оказания брокерских услуг либо предоставления услуг финансового консультанта при инвестировании средств на фондовом рынке (бирже) в сети Интернет:

I. Выясняет у заявителя обстоятельства совершенного преступления:

1) оставлял ли в сети Интернет заявки о возможности инвестирования средств, если да, то на каких интернет-сайтах (приложениях), когда именно, какие данные указывал, сохранились ли контактные сведения, указанные на интернет-сайтах;

2) дата и время, когда заявителю поступило предложение об оказании брокерских услуг либо услуг финансового консультанта при инвестировании средств на фондовом рынке (биржа); каким образом поступило предложение (входящий звонок, сообщение на электронную почту или в мессенджере), с использованием каких абонентских номеров, электронных почтовых ящиков;

3) кем представился собеседник, о чем говорил, какую компанию представлял, какие услуги предлагал, содержание разговора (переписки); какие действия предлагал совершить (установить на компьютер / телефон программное обеспечение, просил ли назвать какую-либо информацию, например персональные данные, данные банковской карты, номер телефона);

4) были ли установлены на устройства заявителя какие-либо программы;

5) посещал ли заявитель интернет-ресурсы, предоставленные собеседником, оставлял ли на данных сайтах свои персональные данные, регистрировался ли, совершал ли какие-либо действия;

6) какие условия заработка предлагал собеседник, предлагал ли приобрести какие-либо акции, цифровые финансовые активы (криптовалюту), приобретал ли их заявитель;

7) способ передачи денежных средств: счета абонентских номеров связи, номера расчетных счетов и банковских карт, если блиц-перевод – через какую платежную систему и на чье имя он совершен, адрес получателя; если путем пополнения счета абонентского номера связи – абонентский номер; если нарочно – время и место передачи, кто подъезжал за деньгами, на каком транспортном средстве, описание человека, которому были переданы денежные средства, возможность опознания и составления фоторобота; если переводом на банковскую карту (расчетный счет) – наличие подтверждающего документа, реквизиты; если путем пополнения кошелька, созданного на сайте, предоставленного собеседником, – сведения о данном кошельке;

8) описание голоса собеседника (хриплый, высокий или низкий, молодой или старый), манеру построения фраз, характерные особенности речи и голоса (шепелявит, проглатывает окончания фраз, говорит скороговоркой), способность опознания голоса звонившего лица.

II. В целях установления интернет-ресурсов, на которых заявитель оставлял заявки об инвестировании средств либо обнаружил объявление об оказании брокерских услуг, в ходе проведения осмотра изучает историю интернет-браузеров, устанавливает и сохраняет ссылки на сайты. Сведения о регистраторе доменного имени устанавливает (поручает исполнение сотруднику оперативного подразделения) посредством следующих интернет-ресурсов: <https://2ip.ru/whois>, <https://www.reg.ru/whois>.

III. Направляет запрос регистратору доменных имен о предоставлении следующей информации: о лице, на которое зарегистрировано доменное имя, с указанием его паспортных данных и контактных абонентских номеров телефонов; e-mail-адресе, с которого поступали заявки на регистрацию данного и других доменных имен; о способах оплаты, производимых при регистрации доменного имени; об IP-адресах, используемых для входа в личный кабинет администратора созданного интернет-сайта; о хостинге (размещение файлов сайта на сервере, на котором запущено программное обеспечение); об иных доменных именах, зарегистрированных данным пользователем, установленных при анализе cookie-файлов.

§ 4. Тактические приемы производства отдельных следственных действий

Процесс расследования преступлений в сфере информационных технологий обуславливает необходимость производства регламентированных УПК РФ следственных и иных процессуальных действий. При следственных действиях нужно соблюдать ряд правил, поскольку они регламентированы уголовно-процессуальным законом и их результаты могут формировать новые доказательства. Тактические особенности их производства на первоначальном этапе расследования находятся в прямой зависимости от специфики слеодообразования и способа совершения преступления.

В результате анализа следственной практики расследования дистанционных мошенничеств, совершаемых с использованием интернет-сервисов, приходим к выводу о том, что при расследовании преступлений этой категории проводятся, в частности, следующие следственные действия:

- 1) осмотр мобильного телефона заявителя;
- 2) допрос потерпевшего;
- 3) допрос подозреваемого;
- 4) обыск;
- 5) назначение производства судебных экспертиз.

При проведении действий, в частности осмотре электронных устройств, с помощью которых совершены преступления, следователь сталкивается с рядом проблем, обусловленных спецификой расследования преступлений данной категории.

При описании мобильного устройства в ходе исследования необходимо определить маркировочные обозначения (модель, серийный номер и т. д.). Они чаще всего указываются производителем на тыльной части корпуса, этикетке под аккумуляторной батареей или лотке для SIM-карты. Кроме того, важной технической характеристикой каждого мобильного устройства является такой уникальный параметр, как IMEI (International Mobile Equipment Identity) – международный идентификатор мобильного оборудования, уникальный для каждого устройства¹. IMEI используется в процедурах обеспечения безопасности связи для идентификации оборудования и предотвращения неавторизованного доступа в сеть. В IMEI закодирована информация о стране происхождения, модели и серийном номере устройства, в связи с чем он выступает одним из основных идентификационных признаков устройства при производстве компьютерных экспертиз и исследований. Сведения об IMEI могут быть представлены в электронном виде во внутренней памяти устройства, в виде маркировки на корпусе или этикетке под аккумуляторной батареей, на лотке для SIM-карты, упа-

¹ Типовая методика исследования информации, содержащейся в мобильных телефонах / О. В. Тушканова, В. М. Щербак, С. Н. Сеницын, С. В. Ермолов М. : ЭКЦ МВД России, 2014. С. 4, 13.

ковке и т. д. В ходе проведения компьютерного исследования или экспертизы необходимо установить соответствие IMEI во внутренней памяти телефона маркировочным обозначениям, находящимся на его корпусе (при их наличии).

В настоящее время мобильные устройства оснащены микропроцессорами с архитектурой системного уровня, применение которых сокращает количество требуемых вспомогательных микросхем и позволяет использовать значительный объем внутренней памяти. Вместе с тем для дополнительного увеличения объема используемой энергонезависимой памяти в мобильных устройствах широко применяются слоты для карт памяти формата Secure Digital (SD), преимущественно форм-фактора microSD, различных поколений, таких как Secure Digital High Capacity (SDHC), Secure Digital eXtended Capacity (SDXC) и Secure Digital Ultra Capacity (SDUC). Съемный накопитель информации может использоваться как отдельный диск для хранения пользовательских данных, так и служить для увеличения объема внутренней памяти, используемой для установки и работы приложений пользователя мобильного устройства.

Современные мобильные устройства могут поддерживать протоколы беспроводной передачи данных. Скорость, тип и объем информации, доступной для передачи по тому или иному протоколу, значительно отличаются. В качестве реализации возможностей для синхронизации и обмена данными, как правило, выступают технологии Bluetooth, Near Field Communication (NFC) и Wi-Fi.

Большинство приложений в современном мобильном устройстве содержат определенные настройки безопасности, которые позволяют скрыть некоторые персональные данные и другую личную информацию. Помимо защиты паролем, применяются различные виды ограничений доступа к информации, хранящейся в памяти мобильного телефона, одним из которых является шифрование.

Чтобы обеспечить конфиденциальность данных, методы шифрования в современных мобильных устройствах реализованы по умолчанию. Традиционно в мобильных устройствах методы шифрования применялись на уровне приложений для защиты индивидуальных пользовательских данных, таких как электронные письма и фотографии. Вместе с тем для обеспечения безопасности и конфиденциальности персональной информации стали использоваться методы шифрования, внедряемые на системном уровне с применением уникальных паролей. Таким образом, данные мобильного устройства по умолчанию хранятся в зашифрованном виде.

В мобильных устройствах используются два типа схем шифрования. Одним из них является полное шифрование диска (FDE – Full Disk Encryption), а другим – пофайловое шифрование (FBE – File Based Encryption). FDE – это метод, при котором весь раздел пользовательских данных шифруется с помощью одного ключа шифрования, в то время как

FBE шифрует данные для каждой файловой базы разными ключами, позволяя файлам шифроваться независимо. Возможна также комбинация указанных схем шифрования.

Помимо шифрования данных, хранящихся в памяти устройств, в современных мобильных устройствах реализованы механизмы по разграничению прав доступа. На всех этапах работы устройства у определенного компонента операционной системы, приложения или пользователя верифицируется наличие прав на доступ к используемым данным или функциям.

На этапе загрузки мобильного устройства выполняется проверка целостности разделов, отвечающих за загрузку операционной системы, и загружаемой операционной системы. В случае обнаружения каких-либо несоответствий заводским параметрам загрузка операционной системы прерывается и устройство не запускается. Практически все производители мобильных устройств дополнительно блокируют модификацию загрузчика для нелегитимных пользователей, делая невозможными любые операции по модификации и изменению загружаемой операционной системы. Доступ к нему возможно получить через производителя либо путем модификации устройства при помощи специального программного обеспечения (наличие данной возможности варьируется в зависимости от производителя и модели мобильного устройства).

После загрузки операционной системы мобильного устройства она также обеспечивает разграничение прав доступа. Низкоуровневые компоненты, отвечающие за работу устройства, такие как ядро операционной системы, системные библиотеки, драйверы, API, функционируют на уровне суперпользователя (root). Для обеспечения их целостности в операционной системе, при сохранении возможности использования устройства, выделяется дополнительный пользователь, обладающий пониженными правами доступа. Этот пользователь может взаимодействовать с операционной системой и управлять устройством через графический интерфейс или функции API. Он не может вносить изменения в компоненты операционной системы или получить доступ к данным, хранящимся в системных разделах устройства. На уровне этого пользователя функционируют и приложения в мобильном устройстве. Таким образом, без прав суперпользователя невозможно получить полный доступ к информации, хранящейся на мобильном устройстве.

В некоторых мобильных телефонах реализованы технологии TrustZone (в мобильных устройствах с операционной системой Android) и Secure Enclave Processor (в мобильных устройствах с операционной системой iOS) для выделения криптографического ключа и обработки конфиденциальной информации, которые даже при получении расширенных прав доступа не позволяют получить доступ к ключевым данным.

Одной из современных технологий, представляющих интерес для криминалистического исследования, является так называемое второе пространство мобильного устройства (наименование может отличаться в зависимости от производителя мобильного устройства). Второе пространство – функция операционной системы мобильного устройства, с помощью которой пользователь может создать второй, независимый от основного, рабочий стол и работать с ним как со вторым устройством. При использовании второго пространства пользователь получает возможность хранения файлов и установки приложений в изолированной среде. Доступ к приложениям и функциям «второго пространства» обычно ограничен паролем, значение которого может не совпадать со значением основного пароля. Криминалистическое исследование информации второго пространства (сообщений переписки, журнала звонков, списка приложений, настроек и др.) следует производить теми же средствами и методами, что используются при исследовании основного пространства операционной системы мобильного устройства, так как файлы и данные приложений могут частично или полностью не совпадать.

Как отмечалось ранее, важной составляющей частью мобильной станции является SIM-карта. SIM-карта (Subscriber Identification Module) – карта, с помощью которой обеспечивается идентификация абонентской станции (абонентского устройства), ее доступ к сети подвижной связи, а также защита от несанкционированного использования абонентского номера. SIM-карта содержит: тип платформы, номер мобильного абонента цифровой сети (MSISDN), название оператора (SPN), международный идентификатор мобильного абонента (IMSI), уникальный серийный номер карты (ICCID), список запрещенных сетей (FPLMN). Также может содержать данные о местонахождении: мобильный код страны (MCC), код мобильной сети (MNC) и временную отметку (TMSI). Поскольку стандарты SIM-карты налагают ограничения на формат и объем данных, пользовательская информация в виде медиафайлов (графических, аудио- и видеофайлов) на ней не хранится.

При осмотре мобильного телефона можем изучить сохраненную текстовую переписку, осуществляемую посредством СМС-сообщений, сообщений на интернет-сервисах, а также с использованием различных мессенджеров (например, WhatsApp); записи о входах и выходах из учетных записей, включая IP-адреса и временные метки; записи о финансовых операциях через онлайн-банкинг или платежные системы. Такой осмотр, согласно ст. 164.1 УПК РФ, следует производить с участием специалиста. Необходимость владения специальными знаниями обуславливает привлечение специалистов из различных областей информационных технологий, в частности инженерии по средствам связи, сетевому обслуживанию, а иногда требуется привлечение нескольких специалистов одновременно. По мнению Ю. Г. Гаврилова, при проведении инструктажа следователь, как

руководитель следственно-оперативной группы, должен убедиться в компетентности специалиста в указанной области знаний¹. Очевидно, что содействие специалиста оказывает следователю существенную помощь в раскрытии преступлений в сфере компьютерной информации, дает возможность эффективно расследовать дела данной категории. Целенаправленные, грамотные и четко спланированные действия следователя, специалиста и оперативных сотрудников, особенно на начальном этапе расследования, обеспечивают успех дальнейшего расследования преступлений, совершенных с использованием средств компьютерной техники.

Одно из самых распространенных следственных действий при расследовании любого преступления – допрос. Не являются исключением дистанционные мошенничества, совершаемые на интернет-сервисах. При производстве допроса следователю необходимо избирать тактику действий в зависимости от механизма совершения преступления данной категории. Р. С. Белкин верно описал допрос как процессуальное действие, заключающееся в получении показаний (информации) о событии, ставшем предметом уголовного судопроизводства, лицах, проходящих по делу, причинах и условиях, способствовавших совершению и сокрытию преступления². Как и иные следственные действия при расследовании преступлений, связанных с интернет-сервисами, допрос обладает определенными особенностями. На выбор тактики производства допроса влияет достаточность объема информации о расследуемом преступлении. Такие сведения следователь получает из различных источников, как процессуальных (результаты иных проведенных следственных действий), так и непроцессуальных (результаты оперативно-разыскных мероприятий). Также при установлении обстоятельств совершения преступлений в сфере информационных технологий необходимы знания об особенностях механизма преступления, возможных орудиях и средствах его совершения. Бесспорно, залогом успешно проведенного допроса является тщательная подготовка к его производству.

На подготовительной стадии обязательно использование полученных в ходе доследственной проверки материалов. Н. Г. Шурухнов отмечает, что «...первоначальный допрос на предварительном следствии лица, от которого во время проведения предварительной проверки были получены объяснения, будет являться повторным изложением события, интересующего следствие. Данное обстоятельство имеет определенное значение, так как предварительная проверка создает благоприятную базу. Что касается недобросовестных участников процесса, оказывающих противодействие рас-

¹ Преступления в сфере компьютерной информации: квалификация и доказывание : учеб. пособие / Ю. В. Гаврилин, А. Ю. Головин, А. В. Кузнецов, Т. В. Толстухина ; под ред. Ю. В. Гаврилина. М. : Книжный мир, 2003. С. 58.

² Белкин Р. С. Криминалистическая энциклопедия. 2-е изд., доп. М. : Мегатрон-XXI, 2000. С. 64.

следованию, то первоначальное получение объяснений от них дает возможность заранее определить позицию, которую займет это лицо на допросе, и соответствующим образом к этому подготовиться»¹. Перечисленные особенности также оказывают влияние на выбор следователем тактических приемов при производстве допроса.

Следственная и судебная практика² показывает, что одним из наиболее распространенных недостатков в проведении допроса потерпевших является его неполнота. Анализ уголовных дел по рассматриваемой категории дел показал, что в процессе проведения следственного действия не выясняется совокупность обстоятельств, имеющих существенное значение для расследования уголовного дела. К таким обстоятельствам можно отнести: отсутствие подробного описания способа совершения преступления, его специфики, особенностей действий злоумышленников при реализации корыстного умысла, участников преступной группы, а также характеристики механизма манипулятивного воздействия, оказываемого на потерпевшего.

С точки зрения Е. С. Шевченко, «чем лучше информационное обеспечение у следователя, безупречное знание и владение им всем собранным по делу материалом и вспомогательной информацией, тем более подконтрольна будет ситуация, которая сложится на допросе»³. Информационное обеспечение включает в себя изучение специальной литературы, в первую очередь в области информационно-телекоммуникационных технологий, интернет-источников, методических рекомендаций по производству следственных действий, нормативной базы. Важным аспектом является консультирование со специалистами в сфере информационных технологий, которые могут разъяснить следователю определенные термины, рассказать о возможных способах совершения рассматриваемых преступлений, а также наметить последовательность вопросов⁴.

Структурно допрос состоит из трех этапов: подготовительного, рабочего и заключительного. В ходе рабочего этапа принято выделять стадии допроса: предварительную, стадию свободного рассказа, вопросно-ответную, заключительную. «Важную роль следует уделять подготовке

¹ Шурухнов Н. Г. Использование при допросе ранее данных объяснений // Тактические приемы допроса и пределы их использования : сб. тезисов теорет. семинара, 14 марта 1980 г. М. : ВНИИ МВД СССР, 1980. С. 52.

² Изучено и проанализировано 78 уголовных дел о мошенничестве на интернет-сервисах (по ст. 159 УК РФ).

³ Шевченко Е. С. Социально-технологические детерминанты следственных действий при расследовании киберпреступлений // Актуальные проблемы российского права. 2016. № 10 (71). С. 161–162.

⁴ Виноградова О. П. Особенности тактики производства невербальных следственных действий при расследовании хищений предметов, имеющих особую ценность // Использование специальных знаний: теоретико-правовая парадигма и проблемы практической деятельности : материалы междунар. науч.-практ. конф., Владивосток, 26–27 сент. 2019 г. Владивосток : ДВЮИ МВД России, 2019. С. 40.

к данному следственному действию, т. е. подготовить перечень вопросов, изучить материалы дела, проанализировать имеющуюся информацию»¹.

Подготовка к допросу включает в себя решение ряда вопросов:

1. Собирая исходной информации и изучения личности допрашиваемого. Это обусловлено тем, что анализ психологического профиля потерпевшего является важным аспектом в расследовании мошенничества данного вида, поскольку позволяет выявить факторы, способствующие виктимизации, и оптимизировать процесс допроса. Потерпевшими в данной категории преступлений чаще всего становятся лица, обладающие определенными психологическими характеристиками и уязвимостями. К ним относятся: повышенная доверчивость, стремление к получению легких денег, поиск отношений, азартность, стремление к выгоде. Существует выраженная тенденция к отрицанию факта виктимизации со стороны потерпевших. Это обусловлено психологическим дискомфортом, чувством стыда, унижения и самообвинения за то, что они стали жертвами обмана. Данное обстоятельство затрудняет получение полной и достоверной информации в ходе следственных действий. По мнению В. Н. Карагодина, объясняется это тем, что многие потерпевшие, стыдясь своего поведения, «стараясь скрывать свои побудительные мотивы при контакте с мошенником»².

2. Выбора момента (времени) и места допроса.

3. О применении технических средств и участии лиц, обладающих специальными знаниями в области информационных технологий (в том числе экспертов в области кибербезопасности, сетевых технологий, цифровой криминалистики).

4. Составления плана допроса.

Рабочий этап начинается с заполнения анкетных данных и разъяснения прав и обязанностей. При проведении допроса первоочередной задачей является установление психологического контакта с потерпевшим. Это позволяет снизить уровень стресса и сопротивления, способствуя получению максимально детальной и объективной информации о всех обстоятельствах совершенного преступления, а также о действиях как самого потерпевшего, так и преступника. Учет психологического состояния потерпевшего и применение эмпатического подхода являются ключевыми для успешного расследования. Как подчеркивает Н. И. Пороубов, психологический контакт в следственной практике представляет собой «особого рода взаимоотношения следователя с участниками уголовного

¹ Грибунов О. П. Отдельные вопросы тактики допроса при расследовании взяточничества // Научный дайджест Восточно-Сибирского института МВД России. 2020. № 4 (7). С. 30.

² Карагодин В. Н. Преодоление противодействия предварительному следствию. Свердловск : Изд-во Урал ун-та, 1992. С. 16.

процесса, характеризующиеся стремлением следователя поддержать в целях получения правдивых, полных и достоверных показаний, имеющих отношение к делу»¹. Потерпевшему предлагается рассказать о произошедшем инциденте в свободной форме. Однако свободный рассказ потерпевшего может быть неполным, в связи с этим следователю рекомендуется по окончании свободного рассказа задать допрашиваемому лицу уточняющие вопросы.

Помимо обстоятельств, указанных в ст. 73 УПК РФ, особое внимание необходимо уделить обстоятельствам, требующим обязательной фиксации для обеспечения полноты допроса потерпевшего по делам о мошенничестве на интернет-сервисах.

В зависимости от обстоятельств совершенного преступления следователь должен определить перечень вопросов, которые подлежат выяснению, а именно:

- 1) онлайн-сервис, на котором происходило общение;
- 2) цель использования потерпевшим данного сервиса;
- 3) обстоятельства знакомства со злоумышленником;
- 4) продолжительность общения со злоумышленником;
- 5) данные, сообщенные потерпевшим о себе в момент общения;
- 6) данные, указанные злоумышленником на интернет-сервисе (особенности профиля, фото, наличие голосовых, видеосообщений);
- 7) конкретная история или предлог, использованные злоумышленником для вхождения в доверие и побуждения к действиям (например предложение инвестиций, срочная помощь родственнику и т. п.);
- 8) обещания или угрозы, озвученные злоумышленником;
- 9) суммы и количество произведенных переводов, а также общая сумма причиненного ущерба;
- 10) реквизиты, на которые осуществлялись переводы (номера банковских карт, счета, электронные кошельки, криптовалютные адреса, номера телефонов);
- 11) платежные системы или банки, через которые производились операции (название банка, платежного сервиса, криптобиржи и т. п.);
- 12) факт оформления кредитов или займов по требованию злоумышленника с указанием финансовых учреждений и суммы;
- 13) точная дата, время списания либо перевода самим потерпевшим денежных средств с принадлежащего ему банковского счета, время и дата телефонных звонков, поступивших потерпевшему от злоумышленника. Ошибки при установлении указанных данных, неточное их отражение в протоколе допроса потерпевшего приводят к запросу ненужной инфор-

¹ Порубов Н. И. Тактика допроса на предварительном следствии : учеб. пособие. М. : БЭК, 1998. С. 41.

мации от банков и операторов мобильной связи. Кроме того, необходимо учитывать, что в связи с ежегодным ростом преступности в сфере информационно-телекоммуникационных технологий возросла загруженность работников банковской сферы, а также операторов услуг мобильной связи по представлению сведений о движении денежных средств по банковским счетам граждан, о соединениях между абонентами и абонентскими устройствами, что напрямую влияет на процессуальные сроки по уголовному делу¹;

14) наличие сохранившихся банковских выписок, квитанций, скриншотов транзакций, подтверждающих переводы;

15) устройства, использованные для общения со злоумышленником и совершения действий (смартфон, планшет, персональный компьютер);

16) переход по ссылкам, предоставленным злоумышленником, с указанием полных URL-адресов (по возможности);

17) ввод персональных данных (логины, пароли, банковские реквизиты, коды из СМС или push-уведомлений) на сторонних сайтах;

18) установка программного обеспечения (например, для удаленного доступа, нового приложения банка) по требованию злоумышленника с указанием его названия и источника загрузки;

19) момент осознания потерпевшим факта мошенничества и его причины (например, злоумышленник перестал выходить на связь, невозможность вывода средств, уведомление банка о подозрительных операциях);

20) первые действия потерпевшего после осознания обмана (попытка связаться со злоумышленником, блокировка банковской карты, обращение в свой банк, изменение паролей, обращение в полицию);

21) обращение потерпевшего за помощью к иным лицам (друзьям, родственникам, техническим специалистам);

22) наличие сохранившейся переписки со злоумышленником (текстовые, голосовые, видеосообщения);

23) наличие сделанных скриншотов или фотографий экранов, относящихся к преступлению.

Следует отметить, что приведенный перечень обстоятельств не считается исчерпывающим. В зависимости от конкретной ситуации и способа совершения хищений он может быть дополнен. Такой комплексный подход позволяет не только воссоздать хронологию событий, но и выявить макси-

¹ Лутцева К. В. Особенности проведения допроса потерпевшего при расследовании преступлений в сфере информационно-телекоммуникационных технологий // Проблемы квалификации и расследования преступлений, совершаемых с применением информационно-коммуникационных технологий : сб. науч. трудов междунар. науч.-практ. конф., Москва, 27 мая 2022 г. М. : Московский университет МВД России имени В. Я. Кикотя, 2022. С. 207.

мально возможное количество цифровых следов, которые могут стать ключевыми доказательствами в расследовании¹.

Выслушав свободный рассказ потерпевшего, следователь мысленно фиксирует и приступает к вопросно-ответной стадии, избирательно применяя тактические приемы, разработанные криминалистикой. Если «показания допрашиваемого правдивы, но недостоверны или неполны, а некоторые воспринятые обстоятельства забыты, то следователю, демонстрируя положительное отношение к честной позиции допрашиваемого, необходимо вскрыть возможное добросовестное заблуждение, возникшее при восприятии события, или неполноту восприятия. В случае установления следователем, что правда скрывается умышленно, а показания носят ложный характер, следует изобличить в этом допрашиваемого и добиться от него правдивых показаний»². С этой целью возможно использование следующих тактических приемов:

1) постановки детальных вопросов, активизирующих ассоциативные связи;

2) ознакомления с фрагментами материалов уголовного дела: протоколами допроса потерпевших, сообщников, осмотра места происшествия, обыска и т. п.;

3) прослушивания аудиозаписей отдельных оперативно-розыскных мероприятий или следственных действий;

4) предъявления допрашиваемому материальных вещественных доказательств, а также схем, зарисовок, фотоснимков, выполненных следователем либо другими участниками процесса расследования;

5) совместного просмотра оперативной съемки, на которых запечатлены эпизоды преступной деятельности, анализа звонков и СМС-сообщений на мобильном телефоне допрашиваемого лица;

6) допроса на месте происшествия;

7) воспроизводства фонограмм допросов, проведения очных ставок³.

В некоторых случаях возможно применение тактического приема, основанного на использовании явления реминисценции, описанного

¹ Евдокимова О. В. Особенности проведения допроса потерпевших при расследовании мошенничеств, совершаемых на интернет-сервисах // Актуальные вопросы расследования преступлений в условиях развития цифровых технологий : материалы всерос. науч.-практ. конф., посвящ. 20-летию кафедры криминалистики и кафедры уголовного процесса, Уфа, 17 окт. 2025 г. Уфа : Уфимский ЮИ МВД России, 2025. С. 235–241.

² Нугаева Э. Д. Особенности расследования мошенничества при оказании оккультных услуг : дис. ...канд. юрид. наук, 2019. С. 162.

³ Соловьев А. Б. Допрос на предварительном следствии : метод. пособие / Всесоюз. ин-т по изуч. причин и разраб. мер предупреждения преступности. 2-е изд., перераб. М. : Б. и., 1986. С. 40.

в трудах В. П. Лаврова, А. Б. Соловьева, Е. Е. Центрова, А. А. Хмырова¹. Этому явлению подвержены не только взрослые, но и несовершеннолетние, причем, как подметил К. Сперанский, в последнем случае оно проявляется ярче, чем у взрослых². В связи с этим, как полагают В. С. Бурданова и И. Е. Быховский, «следует считать полезным повторный допрос потерпевшего через 8–14 дней после расследуемого события, если восприятие его носило эмоционально-напряженный характер»³.

В этой ситуации целесообразно повторный допрос начать с ознакомления допрашиваемого с текстом его предыдущего допроса для восстановления в памяти сущности сообщенного им ранее. После следует объяснить допрашиваемому важность конкретизации его показаний и что за это уголовная ответственность как за дачу ложных показаний не наступает, произвести повторный допрос с использованием тактических приемов, разработанных криминалистикой для данных случаев.

Таким образом, в условиях постоянного увеличения числа преступлений в рассматриваемой сфере, а также значительного ущерба, причиняемого потерпевшим в результате противоправных действий, возникает необходимость в качественном проведении допросов сотрудниками органов внутренних дел Российской Федерации. Это является основой для проведения последующих следственных действий, направленных на сбор доказательственной базы по уголовному делу.

Допрос подозреваемого в каждой конкретной ситуации проходит индивидуально. В момент производства допроса лицо, его осуществляющее, должно иметь в виду общепринятые нормы, подбирая их к конкретному преступлению. Рассматривая рамки использования тактических приемов, следует отметить необходимость соблюдения уголовно-процессуального законодательства и условий нормативно-правового регулирования в сфере компьютерной информации.

Учитывая, что содержание рассматриваемого вида преступления связано с алгоритмами различных действий, при получении информации

¹ См.: Лавров В. П. Особенности расследования нераскрытых преступлений прошлых лет : учеб. пособие / Высш. школа МВД СССР. Москва : НИиРИО ВШ МВД СССР, 1972. С. 11 ; Соловьев А. Б. Допрос на предварительном следствии : метод. пособие / Всесоюз. ин-т по изуч. причин и разраб. мер предупреждения преступности. 2-е изд., перераб. М. : Б. и., 1986. С. 43 ; Хмыров А. А. Криминалистическая характеристика преступления и пути доказывания по уголовному делу // Известия высших учебных заведений. Правоведение. 1978. № 3. С. 62.

² Сперанский К. К. Особенности допроса по делам несовершеннолетних // Социалистическая законность. 1968. № 4. С. 51–53.

³ Бурданова В. С. Предъявление для опознания на предварительном следствии / Прокуратура СССР. Ин-т усовершенствования следств. работников органов прокуратуры и М-ва внутр. дел. Всесоюз. ин-т по изучению причин и разработке мер предупреждения преступности. М. : Б. и., 1975. С. 36.

о механизме его совершения от допрашиваемого рекомендуется детализировать действия и события поэтапно. Так как сфера компьютерных технологий обладает своей спецификой, допрашиваемому следует напомнить, чтобы он свои показания выстраивал с использованием общепринятых слов. В случае применения жаргонизмов порекомендовать их сразу расшифровывать.

По делам об интернет-преступлениях могут быть сформулированы дополнительные вопросы для получения новой информации по установленному обстоятельству.

В ходе проведения допроса по указанной категории преступлений у следователя должны быть в распоряжении результаты таких оперативно-розыскных мероприятий, как снятие информации с технических каналов связи, наблюдение, которые в большинстве случаев могут иметь тактическую и изобличающую направленность.

В процессе производства допроса в бесконфликтной ситуации эффективными можно назвать: предложение изложить факты, строго соблюдая прямую или обратную последовательность события; предъявление объектов, способствующих припоминанию (скриншоты, фотографии и т. д.); предложение связать обстоятельство, интересующее следователя, с каким-либо событием (смежность); проведение допроса в месте обнаружения преступного события и др. В конфликтной ситуации эффективными можно назвать: разъяснение допрашиваемому значимости дачи правдивых показаний; выяснение мотивов дачи ложных показаний и устранение этих мотивов; детализацию показаний допрашиваемого; предъявление доказательств; создание у допрашиваемого преувеличенного представления об осведомленности следователя; демонстрацию возможностей расследования, в том числе на современном этапе; отвлечение внимания; инерцию и др.

Известно, что обыск как самостоятельное процессуальное действие имеет свое определенное место среди остальных следственных действий и играет важную роль в расследовании указанной категории преступлений. Решаемые с его помощью задачи во многом обусловлены той или иной следственной ситуацией, складывающейся в ходе предварительного расследования. Своевременное и грамотное проведение обыска способствует достижению целей правосудия. Результаты данного следственного действия могут быть использованы для формирования доказательственной базы обвинительного приговора, так и послужить предпосылкой для исключения факта необоснованного привлечения лица к уголовной ответственности¹. Основанием для его производства является наличие достаточных данных полагать, что в каком-либо месте или у какого-либо лица могут

¹ Низаева С. Р. Тактические особенности производства обыска и выемки документов при расследовании мошенничества на рынке вторичного жилья // Вестник Уфимского юридического института МВД России. 2016. № 3 (73). С. 38–40.

находиться орудия преступления, предметы, документы и ценности, которые могут иметь значение для уголовного дела (ст. 182 УПК РФ).

В зависимости от того, где происходило общение через мобильный телефон или электронно-вычислительную машину (далее – ЭВМ), следует учитывать особенности обыска для каждого устройства. Как правило, выделяют четыре стадии производства обыска: предварительную, обзорную, детальную и завершающую. На первой стадии необходимо собрать информацию о месте производства данного следственного действия (точный адрес, характеристика строения, наличие телефонной связи, локальной и глобальной сети, месторасположение электропитания); определить вид и содержание информации, которая может храниться у преступника, предположить, на какой технике и каких носителях она может содержаться, какие документы и предметы, имеющие значение для уголовного дела, могут находиться на месте обыска; изучить личность подозреваемого, особое внимание уделить его образованию, навыкам работы с информационно-коммуникационными технологиями, платежными системами, финансовыми документами; принять решение о целесообразности использования программно-аппаратных средств работы с электронной информацией («Мобильный криминалист», Cellebrite UFED и др.); очертить круг участников следственного действия (обязательно участие специалиста и понятых). По прибытии на место обыска следователю надлежит ознакомить лицо, в жилище которого проводится обыск, с постановлением и судебным решением о его производстве и предложить добровольно выдать искомые предметы. Если подозреваемый отказывается это делать, нужно собрать всех присутствующих лиц в одном месте, запретить им доступ к устройствам и телекоммуникационным сетям, находящимся на месте производства обыска.

Подготовительный этап обыска играет главенствующую роль во всем процессе реализации замысла следственного действия. Тщательная и глубокая проработка всех нюансов сложившейся накануне обыска следственной ситуации во многом определяет его результативность. Практика показывает, что многое зависит от тесного взаимодействия следователя со специализированным оперативным подразделением – отделом БСТМ МВД России. С его помощью обеспечивается должная оперативная осведомленность следователя об обстоятельствах, связанных с проведением обыска, которая помогает избежать ряда тактических ошибок, а также грамотно решить вопрос о привлечении к его проведению высококвалифицированных специалистов в области компьютерной техники и понятых, имеющих определенные знания в этой сфере. На обзорной стадии обыска в первую очередь нужно провести осмотр всего помещения, вместе с тем сделать акцент на компьютерной технике, находящейся здесь, ее расположении и состоянии, состоянии телекоммуникационных сетей, произвести поиск портативных запоминающих устройств (флэш-карты, внешний

жесткий диск). Детальная стадия обыска предполагает работу с устройством, на котором может храниться информация, имеющая значение для уголовного дела. По мнению А. Л. Осипенко, А. И. Гайдина, прежде всего ее необходимо искать во внутренних накопителях на жестких магнитных дисках¹. Данные, размещенные в них и оперативной памяти, осматриваются, если нет угрозы их потери. В случае обнаружения искомой информации нужно определить, где именно она находится (папка, файл). Затем устройство выключается, упаковывается и изымается. Если компьютер находится в выключенном состоянии, необходимо зафиксировать его местоположение, соединение с телекоммуникационными сетями, периферийными устройствами, разъединить их, упаковать и изъять. В работе с мобильным телефоном существенную помощь может оказать программно-аппаратный комплекс «Мобильный криминалист», предназначенный для извлечения данных с мобильных устройств, из облачных хранилищ, построения маршрутов, выполнения поиска по ключевым словам, выражениям, номерам телефонов и т. д. Если исследовать содержание мобильного устройства на месте обыска не представляется возможным, то принимается решение о его изъятии. В завершении следственного действия проверяется правильность упаковки изъятых предметов, они опечатываются, составляется протокол и опись к нему. В результате производства обыска и выемки можно обнаружить предметы, имеющие значение для правильного разрешения уголовного дела, а также материалы, характеризующие подозреваемое лицо и облегчающие его розыск.

В работе В. Б. Вехова перечислены мероприятия, которые необходимо осуществить следователю на подготовительном этапе обыска:

1. Определить месторасположение и планировку помещения, которое должно быть подвергнуто обыску; выяснить характер охраны объекта; определить пути возможного отхода подозреваемого (обвиняемого).

2. С помощью специалиста в области телекоммуникаций определить расположение в данном помещении узлов связи, локализацию разводки коммуникационных сетей; рассмотреть возможность наличия на объекте средств радиосвязи, используемых подозреваемым (обвиняемым); установить их идентификационные характеристики: абонентский номер, шрифт, позывной, рабочую частоту, логин и пароль доступа для работы в сети Интернет.

3. Выяснить, какие ЭВМ находятся в помещении, в котором предполагается провести обыск (по возможности установить их технические характеристики). Данные сведения могут быть получены у провайдера сети Интернет или оператора электросвязи. При этом во многих случаях требуется консультация с соответствующим специалистом. В дальнейшем полу-

¹ Осипенко А. Л., Гайдин А. И. Правовое регулирование и тактические особенности изъятия электронных носителей информации // Вестник Воронежского института МВД России. 2014. № 1. С. 158.

ченная информация будет использована для определения границ места, подлежащего обыску, и внесет определенность относительно искомых предметов (документов).

4. Установить, какие средства защиты информации и ЭВМ от несанкционированного доступа находятся по месту, где предполагается провести обыск; выяснить источники их питания и рассмотреть возможность их обесточивания до момента начала обыска. Это позволит исключить факты преднамеренного уничтожения искомых документов или предметов.

5. Установить тип источников электропитания ЭВМ и расположение пунктов их обесточивания для предотвращения возможных попыток уничтожения искомой компьютерной информации, содержащейся в оперативной памяти компьютерных устройств.

6. Пригласить специалистов, обладающих достаточными знаниями, умениями и навыками для оказания действенной помощи следователю при подготовке и в ходе производства обыска. Для этих целей больше всего подходят универсальные специалисты в области цифровых средств электросвязи и компьютерной техники.

7. Подготовить соответствующие ЭВМ, специальную аппаратуру и материалы для поиска, осмотра, фиксации и изъятия искомой компьютерной информации, документов и предметов.

8. Определить дату, время и место проведения обыска, его продолжительность, а также меры, направленные на обеспечение его скоротечности и конфиденциальности. Наиболее благоприятной ситуацией является момент отсутствия подозреваемого (обвиняемого) на месте обыска. Это обстоятельство позволяет исключить активное противодействие с его стороны и предоставляет возможность следователю быстро обнаружить и грамотно изъять искомые объекты. При этом следует отметить, что присутствие на месте обыска сослуживцев или близких родственников подозреваемого (обвиняемого), как правило, формирует у них определенное негативное отношение к совершенному преступному деянию. Данное обстоятельство может быть использовано для определения тактики проведения последующих следственных действий, например допросов свидетелей.

9. Провести инструктаж лиц, привлекаемых к участию в обыске, с постановкой персональных задач.

10. Изучить личность подозреваемого (обвиняемого). Особое внимание следует обратить на уровень его профессиональных умений и навыков в области компьютерных технологий.

11. Пригласить понятых, обладающих определенными знаниями в сфере компьютерной информации и телекоммуникаций¹.

¹ Вехов В. Б., Попова В. В., Илюшин Д. А. Тактические особенности расследования преступлений в сфере компьютерной информации : науч.-практ. пособие. Самара : ООО «Офорт», 2003. С. 31.

По прибытии на место проведения обыска специфика действий следователя будет состоять в следующем:

- определить места возможного отхода подозреваемого (обвиняемого) или выноса предметов и документов, имеющих значение для уголовного дела (запасный выход, окна и др.). Принять меры к установлению наблюдения за ними;

- быстро и внезапно войти в обыскиваемое помещение (жилище). Если их несколько – одновременно войти во все. На наш взгляд, нельзя согласиться с доводами отдельных авторов, полагающих, что в некоторых случаях, когда это возможно или целесообразно, непосредственно перед входом в обыскиваемое помещение следует обесточить его. Представляется, что при внезапном отключении электропитания в помещении (жилище) и наличии предположений у преступника о намерении сотрудников правоохранительных органов провести обыск последним могут быть приняты меры по уничтожению следов преступного посягательства. Таким образом, теряется не только фактор внезапности, но и ценные вещественные доказательства;

- в случае оказания активного сопротивления со стороны лиц, находящихся на объекте обыска, принять меры по нейтрализации противодействия и скорейшему проникновению в обыскиваемое помещение (жилище);

- организовать охрану места обыска и наблюдение за ним. Охране подлежат: периметр обыскиваемых площадей; ЭВМ; хранилища машинных носителей информации (далее – МНИ); все пункты (пульта) связи, охраны и электропитания, находящиеся на объекте обыска (в здании, помещении, на производственной площади); специальные средства защиты от несанкционированного доступа; хранилища ключей (кодов, паролей) аварийного и регламентного доступа к ЭВМ, помещениям и другим объектам (пультам, пунктам, стендам, сейфам и т. п.), попавшим в зону обыска.

По поводу дальнейших действий следователя на месте обыска в современной криминалистической литературе рассматриваются различные точки зрения. Так, по мнению Е. С. Шевченко, которая считает, что главной целью производства обыска при расследовании киберпреступления является обнаружение и изъятие компьютерной техники, на которой остались следы киберпреступления, компьютерной информации, касающейся как самого киберпреступления, так и лиц, совершивших его (информация об их нахождении или перемещении), предметы, являющиеся результатом (продуктом) преступления (например, контрафактные компьютерные программы), и (или) документы, содержащие важную информацию для дела (например, квитанции, блокнот с личными записями, документы о переводе, обналичивании денежных средств и прочее)¹. Считаем спра-

¹ Шевченко Е. С. Тактика производства следственных действий при расследовании киберпреступлений : дис. ... канд. юрид. наук. М., 2016. С. 142.

ведливым мнение Г. З. Гаспаряна, который определяет, что по делам исследуемой категории производство обыска целесообразно проводить незамедлительно, по возможности сразу после возбуждения уголовного дела, поскольку своевременное и качественное производство способствует обнаружению и изъятию орудий и средств преступления, а также доказательственной информации¹.

Полагаем, что после реализации вышеуказанных мероприятий следователь должен перейти к обзорной стадии обыска и выполнить следующие действия:

1. Определить местонахождение подозреваемого (обвиняемого) на объекте обыска (если обыск осуществляется в его присутствии). При обнаружении – принять меры к отстранению его от пультов управления техническими устройствами, дистанцировать от них и организовать охрану.

2. Определить и отключить специальные средства защиты информации и ЭВМ от несанкционированного доступа, особенно те, которые автоматически уничтожают компьютерную информацию и электронный носитель информации при нарушении процедуры доступа к ним, порядка их использования и (или) установленных правил работы с ними; принять меры к установлению пароля (кода) санкционированного доступа и ключа шифрования-дешифрования информации.

3. Установить наличие телекоммуникационной связи между ЭВМ и каналами электросвязи. При наличии компьютерной сети любого уровня технической организации осмотреть и обыскать управляющую ЭВМ – сервер, который хранит в своей оперативной и постоянной памяти наибольшую часть компьютерной информации, управляет другими ЭВМ, имеет с ними прямую и обратную связь. Следует учитывать, что у сообщников подозреваемого (обвиняемого) или у него самого (если обыск производится в его отсутствие) имеется возможность уничтожения искомой компьютерной информации дистанционно с помощью ЭВМ, находящихся вне периметра обыскиваемой зоны.

4. Определить ЭВМ, находящиеся во включенном состоянии, характер выполняемых ими операций. Внимание необходимо уделить печатающим и проекционным устройствам. Распечатки информации (листинги) при необходимости должны быть изъяты и приобщены к протоколу следственного действия; изображение на экране монитора – видеограмма изучена и детально описана в протоколе.

При установлении, что на момент обыска на каком-либо ЭВМ происходит уничтожение информации либо ее машинного носителя, необходимо срочно всеми возможными способами приостановить этот процесс и начать обследование с данного места или ЭВМ.

¹ Гаспарян Г. З. Расследование хищений денежных средств, совершенных с использованием информационных банковских технологий : дис. ... канд. юрид. наук. М., 2020. С. 181.

При обследовании персонального компьютера следует: установить последнюю исполненную программу и (или) операцию, а по возможности – все, начиная с момента включения компьютера; произвести экспресс-анализ компьютерной информации, содержащейся на жестком диске и в оперативной памяти с целью получения данных, имеющих значение для следствия (их скорейшее получение позволит скорректировать тактику обыска и порядок производства последующих следственных действий).

5. При совершении преступления с помощью малогабаритной (мобильной) ЭВМ или средства мобильной коммуникации организовать производство личного обыска подозреваемого (обвиняемого), а также лиц, находящихся в обыскиваемом помещении. Это возможно лишь в тех случаях, когда у следователя имеются достаточные основания полагать, что лицо скрывает при себе предметы либо документы, которые могут иметь значение для уголовного дела (ч. 2 ст. 184 УПК РФ). Личный обыск такого лица производится по правилам, изложенным в ч. 3 ст. 184 УПК РФ.

Детальный этап обыска требует слаженной работы всех участников следственного действия. Необходимо четко организовать поисковые мероприятия, направленные на выявление тайников, в которых могут находиться предметы и документы. Ими могут быть и сами компьютерные устройства – аппаратные и программные модули, входящие в состав ЭВМ, системы ЭВМ или их сети.

В процессе обыска и выемки, связанных с изъятием компьютера, носителей информации, возникает ряд общих проблем, обусловленных спецификой изымаемых технических средств. В первую очередь, следует предусмотреть меры безопасности для предотвращения уничтожения компьютерной информации преступниками. Они, например, могут использовать специальное оборудование, в критических случаях образующее сильное магнитное поле, которое выводит из строя магнитные записи. На протяжении обыска все электронные доказательства, находящиеся в компьютере либо в компьютерной системе, должны быть собраны таким образом, чтобы быть признанными судом в качестве вещественных доказательств. Мировая практика показывает, что в большинстве случаев под давлением представителей защиты в суде электронные доказательства не принимаются во внимание. Чтобы гарантировать их признание в качестве доказательств, необходимо строго придерживаться уголовно-процессуального законодательства, а также стандартизированных приемов и методик их изъятия. Обычно компьютерные доказательства сохраняются путем создания точной копии с оригинала (первичного доказательства), прежде чем производится какой-либо их анализ. Но подготовить копии файлов, используя только стандартные программы резервного копирования, иногда недостаточно. Вещественные доказательства могут существовать в виде скрытых или зашифрованных данных, выявить которые возможно только при участии специалиста.

Носители информации, на которые предусматривается запись или копирование информации, должны быть заранее подготовлены и отформатированы. Носители следует сохранять в специальных упаковках либо заворачивать в чистую бумагу – информация может быть повреждена повышенной влажностью, температурным влиянием или электростатическим (магнитным) полем. Большинство пользователей компьютера не осознают важности создания файлов, поскольку обычно они уничтожаются программой в конце сеанса работы. Однако данные, находящиеся внутри этих уничтоженных файлов, могут оказать существенное влияние на ход расследования.

На заключительном этапе обыска составляются: протокол следственного действия и описи к нему; вычерчиваются планы обыскиваемых помещений, схемы расположения ЭВМ относительно друг друга, инженерно-технических коммуникаций, а также схема соединения ЭВМ между собой и с другими техническими устройствами; проводится дополнительная фотосъемка или видеозапись.

При назначении судебных экспертиз принципиально важно профессионально грамотное формулирование требующих своего разрешения вопросов и подготовка материалов экспертного исследования. Хорошо организованные преступные группы и сообщества для достижения корыстных целей активно и высокопрофессионально применяют в своей деятельности новые методы, подходы, специальные программно-аппаратные средства, системы удаленного доступа и криптографического шифрования, высокотехнологичную технику, часто и интеллектуальные комплексы принятия решений¹. В связи с этим особое значение при расследовании киберпреступлений имеют компьютерные экспертизы² (далее – КЭ).

На сегодняшний день сформировалась довольно устойчивая классификация категорий и групп криминалистических инструментов компьютерных экспертиз, которая представлена следующими элементами: устройствами разблокировки машинных носителей информации с аппаратной блокировкой записи на них; устройствами клонирования машинных носителей информации; программными средствами криминалистического исследования содержимого машинных носителей и их образов; мобильными компьютерами с комплексом специализированного программного обеспечения и дополнительных аппаратных средств для проведения исследований компьютерной информации в полевых условиях; набором хэшей для фильтрации содержимого изучаемой файловой системы; специализирован-

¹ Системная модель интеллектуальной предметно-ориентированной профайлинг-системы / В. В. Антонов, З. И. Харисова, З. Р. Мансурова [и др.] // Онтология проектирования. 2020. Т. 10, № 3. С. 338–350.

² ГОСТ Р 57429-2017 Национальный стандарт Российской Федерации. Судебная компьютерно-техническая экспертиза. Термины и определения (Forensic information technology examination. Terms and definitions). М. : Стандартинформ, 2018.

ными аппаратными и программными средствами для исследования мобильных телефонов и SIM-карт; программно-аппаратными комплексами для исследования информационных сетей и т. д.¹

На разрешение судебной компьютерной экспертизы в отношении мобильных телефонов могут быть поставлены следующие вопросы:

1. Каково значение IMEI (марка, модель и т.д.) представленного на исследование мобильного телефона? Совпадают ли маркировочные обозначения, представленные на корпусе мобильного телефона, с имеющимися во внутренней памяти устройства?

2. Имеется ли в представленном на экспертизу мобильном телефоне информация об учетных записях пользователя?

3. Имеются ли в представленном на экспертизу мобильном телефоне файлы, содержащие электронную переписку посредством электронной почты, сервисов мгновенных сообщений и социальных сетей?

4. Имеются ли в представленном на экспертизу мобильном телефоне файлы, содержащие историю посещения интернет-ресурсов?

5. Имеются ли в представленном на экспертизу мобильном телефоне файлы, содержащие следующие ключевые слова и/или выражения «...»?

6. Имеются ли в представленном на экспертизу мобильном телефоне сведения об установленном программном обеспечении, атрибутирующем себя как... ?

7. Имеются ли в памяти представленного на экспертизу мобильного телефона телефонная книга (список контактов), входящие, исходящие и пропущенные вызовы, СМС-сообщения в явном либо удаленном виде?

8. Имеются ли в памяти представленного на экспертизу мобильного телефона аудио-, видео- и графические файлы, в том числе и среди удаленных? Если да, то скопировать их на сторонний носитель информации.

На разрешение судебной компьютерной экспертизы в отношении SIM-карт могут быть поставлены следующие вопросы:

1. Каковы значения IMSI (международный код) и ICCID (серийный номер) представленной сим-карты? Имеются ли сведения о номере мобильного абонента цифровой сети (MSISDN) представленной SIM-карты?

2. Имеются ли в памяти сим-карты телефонная книга (список контактов), смс-сообщения и набранные номера?²

В заключение необходимо подчеркнуть, что при проведении следственных действий, связанных с расследованием преступлений в сфере использования компьютерных технологий, целесообразно с самого начала

¹ Особенности первоначального этапа расследования неправомерного доступа к компьютерной информации : учеб.-метод. пособие / Э. Д. Нугаева, С. Р. Низаева, В. Р. Гайнельзянова, З. И. Харисова. Уфа : Уфимский ЮИ МВД России, 2023. С. 55–56.

² Исследование информации, содержащейся в мобильных телефонах : типовая методика / С. В. Ермолов, В. А. Ращупкина, Е. А. Кресан [и др.]. М. : ЭКЦ МВД России, 2023. С. 12–13.

привлечь специалиста в области информационных технологий. До начала следственных действий следует также иметь определенную информацию, касающуюся марки, модели компьютера, операционной системы, периферийных устройств, средств связи, и любые другие сведения о системе, которая является объектом расследования.

ГЛАВА II. КРИМИНАЛИСТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ОРГАНИЗАЦИИ И РАССЛЕДОВАНИЯ ДИСТАНЦИОННЫХ МОШЕННИЧЕСТВ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНТЕРНЕТ-СЕРВИСОВ

§ 1. Особенности криминалистического исследования цифровых следов

Современная реальность требует от правоохранительных органов совершенствования методов расследования рассматриваемых преступлений. Однако существует мнение, что в ходе расследования возникают проблемы, обусловленные двумя основными факторами: технической стороной и сложностью установления лица, подлежащего уголовному преследованию¹.

Особое внимание при расследовании дистанционных мошенничеств следует уделять методам сбора цифровых следов, а именно: изучению программного обеспечения для криминалистического анализа и проведения оперативных исследований на удаленных конечных точках; анализу сетевого взаимодействия средств извлечения информации с исследуемых образцов операционных систем, жестких дисков и энергозависимой памяти средств изучения машинных носителей информации, установленного криптографического программного обеспечения и цифровых устройств, что в настоящее время именуется компьютерной криминалистикой (за рубежом совокупность знаний о методах поиска, исследования и закрепления цифровых следов при расследовании киберпреступлений называют форензикой (от англ. forensic science или forensics – расследование киберпреступлений, судебная наука).

С течением времени и вводом в широкую эксплуатацию все большего количества технологий обработки и передачи информации, с расширением спектра информационных и сетевых услуг, повсеместным развитием рынка цифровых виртуальных активов, удаленной передачи данных, киберфизических систем, нейросетевых технологий и сети Интернет возникают новые виды преступлений.

При назначении всех видов судебных экспертиз принципиально важное значение имеет профессионально грамотное формулирование требующих своего разрешения вопросов и подготовка материалов экспертного исследования.

Организованные преступные группы и сообщества для достижения корыстных целей активно применяют в своей преступной деятельности новые методы, подходы, специальные программно-аппаратные средства, системы удаленного доступа и криптографического шифрования, высокотехнологичное оборудование, а зачастую и интеллектуальные комплексы

¹ Глебова К. В., Воробьев К. В. «Паутина в паутине»: интернет-мошенничество // Молодой ученый. 2017. № 3 (137). С. 28–30.

принятия решений. В связи с этим при расследовании киберпреступлений огромную роль играют КЭ.

В составе КЭ можно выделить четыре вида: аппаратно-компьютерную экспертизу, программно-компьютерную, информационно-компьютерную и компьютерно-сетевую. Выделение этих видов экспертиз обуславливается характером объектов, которые представляются к анализу, и вопросами, решаемыми в рамках каждой конкретной экспертизы.

Аппаратно-компьютерная экспертиза решает вопросы, связанные с исследованием технической (аппаратной) части компьютерных средств. Как правило, эти вопросы носят диагностический характер.

Программно-компьютерная экспертиза направлена на решение вопросов, связанных с исследованием программного обеспечения. В рамках программно-компьютерной экспертизы исследуются процедуры, алгоритмы, принципы разработки программного обеспечения, а также его использование, текущее состояние, структурные особенности, особенности их эксплуатации.

Компьютерно-сетевая экспертиза занимается исследованием обстоятельств и фактов, связанных с применением телекоммуникационных или сетевых технологий.

Ключевым видом КЭ является информационно-компьютерная экспертиза, которая решает задачи, связанные с поиском, обнаружением, оценкой и анализом информации, содержащейся в компьютерной системе. Именно данный вид исследования позволяет обеспечить завершение процесса целостного формирования доказательственной базы в результате формулирования ответов на большинство вопросов, в той или иной степени связанных с цифровыми следами.

Согласно ст. 80 УПК РФ по завершении проведения КЭ эксперт готовит заключение, которое включает в себя результаты судебной экспертизы. Рассматривая указанную категорию преступлений, следователь сталкивается с информацией, зафиксированной в электронной форме, программным обеспечением, средствами защиты информации и сетевыми технологиями, экспертное исследование которых позволяет предоставить в распоряжение сотрудника сведения, отражающие механизм совершенного преступления, дает возможность определить параметры технических средств, их отношение к обнаруженной информации и друг к другу, а также иные важные обстоятельства. При таких обстоятельствах на первоначальном этапе расследования киберпреступлений актуальной задачей является определение уровня защищенности исследуемых информационных систем, общего алгоритма расследования (в зависимости от параметров сложившейся ситуации), от реализации которого, в частности, будет зависеть ход расследования и раскрытия инцидента.

Ведущее место среди судебных экспертиз, назначаемых в комплексе с судебной компьютерной экспертизой (далее – СКЭ), принадлежит техни-

ко-криминалистической экспертизе документов. Именно с необходимостью исследования поддельных документов, ценных бумаг и денежных знаков, оттисков печатей, кредитных и расчетных карт, изготовленных с применением современных информационных технологий, связано большинство комплексных экспертиз в данной области. Объектами такой комплексной экспертизы являются как некоторые объекты СКЭ, предназначенные для создания, хранения и передачи информации, так и некоторые объекты технико-криминалистической экспертизы документов – данные на твердых носителях (в бумажной форме).

Для непосредственного исследования цифровых видео- и аудиозаписей назначается судебная видеофоноскопическая экспертиза. В случае разрешения вопросов, касающихся исследования звуковой речевой информации, то есть файлов со звуковыми форматами, требуется назначение комплексной СКЭ и судебной фоноскопической экспертизы. Такие вопросы часто возникают в связи с широким распространением контрафактной продукции, принадлежности тембра голоса и пр.

При изучении содержимого электронных устройств необходимо учитывать, что источником криминалистически значимой информации могут быть как локальные пользовательские файлы, так и системная информация, а также данные прикладных программ. В зависимости от объектов, представляемых на экспертизу, СКЭ подразделяются на четыре вида: в отношении информации, зафиксированной в электронной форме, технических средств, программного обеспечения и сетевых подключений. На этапе подготовки материалов, предоставляемых в распоряжение экспертов при назначении СКЭ, следователь выбирает объект, подлежащий передаче на экспертизу, и прилагает его к постановлению о ее назначении. Особенностью назначения СКЭ можно назвать тот факт, что эксперту не предоставляются материалы дела (кроме постановления). Ему направляются лишь материальные объекты (например, электронные носители информации, системный блок или комплектующие элементы). С целью обеспечения сохранности информации и гарантии невнесения изменений в их содержимое электронные носители, как правило, должны подключаться к стендовой ЭВМ в режиме защиты от записи. Информация с исследуемого накопителя клонируется на жесткий диск стендовой ЭВМ при помощи специализированного программного обеспечения. Затем производится восстановление удаленных данных на жесткий диск стендовой ЭВМ и отключение исследуемого электронного носителя. Дальнейшее исследование информации проводится на жестком диске стендового компьютера.

В заключение необходимо отметить, что анализ СКЭ и непосредственная беседа с ведущими специалистами Экспертно-криминалистического центра МВД по Республике Башкортостан (равно как и других

регионов Российской Федерации¹⁾) позволили выявить ряд наиболее актуальных проблем в области исследования цифровых следов: сроки производства СКЭ часто увеличиваются в связи с тем, что инициаторы исследования до назначения экспертиз не консультируются по технически выверенной формулировке интересующих их вопросов²⁾. Часто выносятся вопросы, выходящие за пределы компетенции экспертов, решение которых нецелесообразно или занимает продолжительное время; наблюдается острая нехватка специалистов в области производства СКЭ; в рамках одного вынесенного постановления о назначении КЭ направляются на исследование несколько объектов. Вместе с тем рекомендуется на каждый объект выносить отдельное постановление, чтобы впоследствии при производстве экспертизы на каждый объект оформлялось содержательное заключение; нередко имеют место факты несвоевременного назначения КЭ. С момента вынесения следователем постановления до момента поступления материалов в экспертно-криминалистический центр проходит значительное время, что негативно сказывается на процессуальных сроках расследования.

Таким образом, для решения указанных проблем и, соответственно, всестороннего и объективного расследования уголовных дел рассматриваемой категории, эффективности и учета цифровых следов имеется необходимость усиления взаимодействия³⁾ между следственными и экспертными подразделениями⁴⁾ как в период назначения, так и во время производства КЭ.

§ 2. Техничко-криминалистическое обеспечение, используемое при расследовании дистанционных мошенничеств

Развитие информационных технологий (далее – ИТ), стремительная цифровизация социально-экономических процессов, а также широкое использование технических устройств, информационно-телекоммуникационной сети Интернет, мобильных средств связи, развитие дистанционного банковского обслуживания, увеличение безналичного денежного оборота и иные факторы привели к значительным изменениям в способах, средствах и условиях совершения преступлений. Это, в свою очередь, способствовало росту мошенничества, в частности, совершаемого в интернет-

¹⁾ Россинская Е. Р. Проблемы использования специальных знаний в судебном исследовании компьютерных преступлений в условиях цифровизации // Вестник Университета имени О. Е. Кутафина (МГЮА). 2019. № 5 (57). С. 31–44.

²⁾ Сысенко А. Р., Смирнова И. С., Тимошенко С. Е. Проблемы назначения и производства судебной компьютерно-технической экспертизы // Сибирское юридическое обозрение. 2020. Т. 17, № 4. С. 523–533.

³⁾ Cockcroft T., Shan-A-Khuda M., Schreuders M., Trevorrow P. Police Cybercrime Training: Perceptions, Pedagogy, and Policy // Policing: A Journal of Policy and Practice. V. 15. I. 1. 2021. P. 15–33.

⁴⁾ Makhkamov D. International cooperation in the field of forensic computer technical expertise // Journal of Law Research. 2019. V. 9 (1). P. 12.

среде. Однако противодействие таким преступлениям остается затруднительным из-за недостатков в процессе поиска, фиксации, собирания и оценки криминалистически значимой компьютерной информации, а также отсутствия необходимых технико-криминалистических средств (далее – ТКС). Эти проблемы серьезно осложняют расследование дистанционных мошенничеств на интернет-сервисах.

Ключевыми задачами науки криминалистики из числа специальных являются привлечение данных естественных и технических наук в целях оптимизации научно-технического обеспечения, а также совершенствование криминалистических средств, методов, тактических приемов и методических рекомендаций раскрытия, расследования и предупреждения преступлений. Наиболее важные на сегодняшний день сопутствующие задачи заключаются в синергичной адаптации к современным условиям в плане применения ИТ и разработке новейших технических средств в целях своевременного обнаружения, фиксации и исследования следов (в том числе электронных), образующихся в результате совершения преступных деяний.

На сегодняшний день криминалистическая наука оперирует рядом устоявшихся фундаментальных категорий, которые формируют ее основу в виде теоретического аппарата и методологических подходов. К числу основных криминалистических понятий относятся: доказательство, следственная ситуация, способ совершения и сокрытия преступления, криминалистическое средство, криминалистические прием и рекомендация, тактическая комбинация (операция), тактическое решение, криминалистическая характеристика преступного деяния и др.¹ Однако основой предметного поля криминалистики выступает характеристика закономерностей собирания, исследования, оценки и использования доказательств. На основе декомпозиции этих закономерностей наука разрабатывает ТКС, тактические приемы и рекомендации по работе с найденными доказательствами.

Криминалистические методы и средства по источнику происхождения все чаще могут быть результатом междисциплинарного синтеза (в плане использования достижений смежных наук) и по содержанию подразделяются на технические, тактические и методические. Соответственно, надлежащим образом систематизированные совокупности методов расследования и ТКС образуют криминалистическую технику, криминалистическую тактику и криминалистическую методику².

Материально-вещественные объекты (инструменты, устройства или материалы), функционально предназначенные для обнаружения, фиксации, изъятия и анализа доказательственной информации либо создания препятствий к совершению преступного деяния, принято называть ТКС.

¹ Эксархопуло А. А., Макаренко И. А., Зайнуллин Р. И. Криминалистика. Теоретический курс : моногр. Уфа : НИИ ППГ, 2022. С. 28

² Аверьянова Т. В. Криминалистика. М. : Норма, 2023. С. 59.

Условиями применения ТКС и криминалистических приемов являются их допустимость и научная обоснованность, которая означает, что они основаны на положениях той или иной науки, удовлетворяют всем предъявляемым требованиям, а результаты их использования обладают достаточной степенью валидности и достоверности. В первую очередь указанные средства помогают собрать доказательственную базу по уголовному делу, кроме того, именно они применяются для обнаружения, фиксации и изъятия различных следов и иных объектов на месте происшествия, позволяя выявить участников преступления, обеспечивая при этом возможность фиксации обстановки, в которой производится следственное действие¹.

Четвертый этап развития криминалистики (криминалистика 4.0)² связан с активным внедрением ИТ в жизнедеятельность человека и подразумевает цифровизацию применяемых ТКС в целях раскрытия и расследования преступлений, совершаемых в цифровой среде, что соответствует современным научно-исследовательским приоритетам. Правовые основания применения ТКС представляют собой систему закрепленных норм и принципов, определяющих условия допустимости их задействования и порядок процессуального оформления фактов их использования. Применение ТКС осуществляется в строгом соответствии с Конституцией Российской Федерации, нормами УПК РФ и международного права, то есть исключительно при наличии правовых оснований для их использования.

Как уже было указано ранее, глобальная информатизация общества затронула не только способы, средства и условия совершения преступлений, но и правила производства следственных действий. Так, в соответствии со ст. 73 УПК РФ, важнейшее значение имеют поиск, обнаружение, фиксация и изучение различных следов и вещественных доказательств, позволяющих осуществлять доказывание. Соответственно, под цифровым доказательством, исходя из содержания ст. 74 УПК РФ, понимается любая компьютерная информация, на основе которой суд, прокурор, следователь или дознаватель устанавливает наличие или отсутствие обстоятельств, подлежащих доказыванию при производстве по уголовному делу, а также иных имеющих значение обстоятельств.

К основным инструментам, способствующим расследованию дистанционных мошенничеств, относят средства, направленные на выявление, извлечение, анализ и сохранение цифровых доказательств, хранящихся на электронных и машинных носителях информации, в мобильных

¹ Козлов А. Е., Макарова Е. Н., Романова О. Л. Современные технико-криминалистические средства, применяемые в ходе осмотра места происшествия : учеб. пособие. СПб. : СПбУ МВД России, 2024. С. 6.

² Нестеров А. В. Виртуальные следы в криминалистике. М. : Изд-во КноРус, 2024. С. 52.

средствах связи, в сетевой среде, а также в облачных сервисах¹. Средствами являются программные и аппаратные средства анализа цифровых доказательств, хранилища электронных данных, устройства их аппаратного восстановления, комплексы перехвата сетевого трафика и т. п.

Криминалистическое обеспечение расследования и раскрытия преступлений рассматриваемого вида стратегически целесообразно планировать с возможностью автоматизации рутинных задач, что осуществимо исключительно при задействовании ИТ, в том числе современных, на базе технологий искусственного интеллекта (далее – ИИ), анализа больших данных, хранения доказательств в распределенных системах, то есть на базе концепции Web 3.0².

Таким образом, внедрение ИТ в технико-криминалистическое обеспечение расследования рассматриваемых преступлений дает возможность формирования значительного массива криминалистически значимой информации, новых криминалистических учетов, их обработки и использования в профессиональной деятельности следователей, дознавателей, оперативных сотрудников, экспертов и специалистов.

Несмотря на наличие правового регулирования, действующая правоприменительная практика в настоящее время довольно часто сталкивается с проблемами поиска, фиксации и исследования цифровых доказательств, их процессуального оформления, достоверности (неизменяемости) и допустимости их в суде, а также рядом технических трудностей, связанных с последующим хранением данных.

Эффективность поиска и собирания криминалистически значимых объектов часто зависит от уровня использования следователем технических средств, ИТТ, а также специальных знаний. Нередки случаи, когда произвести собирание доказательств без использования специальных знаний либо участия в следственном действии эксперта или специалиста не представляется возможным, что обусловлено, например, применением ультрасовременных технологий при совершении преступлений³. Так, в отсутствие специальных знаний в области собирания и анализа цифровых доказательств или программных ТКС алгоритм действий следователя может привести к утрате или упущению «виртуальных» следов преступного деяния.

Таким образом, эффективность расследования рассматриваемых преступлений в большинстве случаев зависит от качества собирания, фикса-

¹ Tiwari N., Baroniya Y., Bharadwaj V. Cyber and digital forensic // Textbook of forensic science. 2023. No. 25. P. 775.

² Adams T. A. Trends, challenges and opportunities of engaging digital forensics for cybercrime investigations // Advances in multidisciplinary and scientific research journal publication. 2024. No. 15 (1). P. 10.

³ Thakur K. S., Ahuja R. Safeguarding justice employing blockchain-enabled secure chain of custody framework for digital evidence // Innovations in electrical and electronic engineering. 2024. No. 115. P. 3.

ции и оценки цифровых доказательств путем использования ТКС. Например, идентифицировать преступника и определить его причастность к инциденту поможет выявление: IP-адресов и MAC-идентификаторов задействованных устройств; данных лог-файлов, маршрутизаторов и журналов системного программного обеспечения¹; метаданных файлов и реестров сетевой активности; фактов использования виртуальных частных сетей и систем прокси-серверов и пр. Восстановить и реконструировать хронологию событий и в итоге эффективно спланировать дальнейшие следственные действия позволяет анализ временных меток в информационных системах², объективность расследования могут обеспечить данные о местоположении мобильного средства связи, анализ коммуникаций участников уголовного процесса, что, в свою очередь, может подтвердить или опровергнуть показания подозреваемых, свидетелей и пр.

К основным проблемам, связанным с поиском цифровых доказательств, можно отнести фрагментарность и изменчивость цифровой информации (создается риск утраты или искажения криминалистически значимой информации, что особенно актуально при работе с оперативной памятью технических средств и облачных сервисов³), возможность шифрования и анонимизации данных (значительно затрудняет идентификацию и поиск цифровых доказательств и требует специальных средств противодействия для их обхода), разнообразие среды исследования и невозможность стандартизации процесса выявления доказательств (персональные компьютеры с различными видами операционных систем и носителей информации, мобильные средства связи, облачные хранилища данных, сетевая инфраструктура и прочие устройства, каждое из которых предъявляет свои требования к методам поиска данных). Решение проблем поиска, фиксации и исследования цифровых доказательств при расследовании рассматриваемых преступлений преимущественно заключается в автоматизации указанных процессов путем использования программных ТКС, поскольку автоматическую классификацию и детектирование киберугроз, в том числе среди больших массивов сведений, в совокупности с геометрически растущим объемом цифровых данных, возможно охватить исключительно используя программное обеспечение, в частности, построенное на базе технологий ИИ и машинного обучения⁴.

¹ Федотов Н. Н. Форензика – компьютерная криминалистика. М. : Юридический мир, 2007. С. 142.

² Cantelli-Forti A., Longo G., Lupia F. A consistent and tamper-proof methodology for acquisition of automatically verifiable forensic web evidence // International journal of information security. 2025. No. 24 (81). P. 7.

³ Digital rights management scheme based on redactable blockchain and perceptual hash / Yi X., Zhou Y., Lin Y. [et al.]. // Peer-to-peer networking and applications. 2023. No. 16. P. 2640.

⁴ Kreso I. Using blockchain technology for preserving digital evidence in digital forensics // Knowledge international journal. 2025. No. 68 (3). P. 331.

На сегодняшний день информация, являясь одним из наиболее ценных продуктов для мирового сообщества, часто становится объектом преступного посягательства, при этом ИТ служат орудием такого рода правонарушений. В результате «оцифровки» значительного объема пользовательских данных различными интернет-сервисами и веб-приложениями (сведения о пользовательских устройствах и их индивидуальных настройках, логи авторизации, поведенческие, персональные данные и т. п.) появилась возможность использования генерируемой информации в качестве основы для формирования информационно-аналитического кластера распределенных данных с функцией нейросетевого анализа.

Предлагаемый нейросетевой криминалистический кластер на основе общедоступной информации при условии соблюдения установленных нормативными правовыми актами ограничений в отношении распространения такой информации, аналогично криминалистическим учетам в цифровом виде, определил бы возможность гибкой настройки по выдаче отчетов по интересующим следствие направлениям. Необходимость поддержания инфраструктуры предлагаемой системы заключается в плановом и своевременном обновлении сформированных каталогов и инструментов для поиска данных, обеспечения соблюдения требований по обработке общедоступных источников, а также грамотного переобучения системы после обновления баз данных. При этом главной проблемой по формированию интеллектуального нейросетевого криминалистического кластера является отсутствие единых стандартов в подходе к охраняемой информации, в частности персональных данных граждан различных стран. По этой причине актуальной задачей на этапе зарождения проекта являлось бы формирование рассматриваемой информационной системы в рамках реализации для одного государства (национального кластера) либо с возможностью создания массива кластеров данных при условии их обезличивания (путем введения условных идентификаторов объектов исследования). Достоинствами формирования нейросетевого криминалистического кластера данных являются повышение эффективности поиска необходимой для раскрытия или расследования информации за счет алгоритмизации этого процесса, удобство обработки значительного количества данных с применением ключевых слов и фильтров в едином сегменте сети, хранения и использования цифровых доказательств, расширение механизмов оперативного доступа к данным, а также снижение трудозатрат и ресурсов по их поиску.

К проблемам фиксации цифровых доказательств и, как следствие, обеспечения целостности данных и их доказательной силы в суде можно отнести отсутствие единых методологических стандартов по их закреплению, недостаток сертифицированных программных ТКС, а также значительные временные и трудовые издержки неавтоматизированной фиксации криминалистически значимой информации. Непосредственное исследование данных осложняется их разнородностью, величиной массивов инфор-

мации, подлежащих обработке, что требует использования специализированного программного обеспечения и высокопроизводительных вычислительных мощностей, что в совокупности обуславливает увеличение времени, затрачиваемого на анализ. По этой причине целесообразна разработка и активное использование адаптивных программных ТКС, позволяющих в условиях постоянной трансформации и эволюции киберпреступности систематизировать (кодифицировать) преступления в сфере компьютерной информации, в частности дистанционных мошенничеств, в автоматизированном виде обеспечить как поиск, так и фиксацию доказательств в цифровой среде различного генеза.

Достоверность (неизменяемость) и допустимость изъятых цифровых доказательств может обеспечить расчет контрольных сумм файлов. Как известно, основным способом установления дублирования, равно как определения идентичности двух электронных файлов, является дедупликация (тестовая проверка данных, заключающаяся в расчете их контрольных сумм (хеш-функций))¹. По результатам выполнения теста в виде хеширования и установления полного соответствия хеш-функций можно сделать вывод об идентичности сравниваемых файлов. Соответственно, рассчитанная контрольная сумма электронного файла исключает проблему установления достоверности (неизменяемости) цифровых доказательств в процессе ее копирования или исследования. По этой причине необходимо рассмотрение возможности учета контрольных сумм цифровых доказательств в целях последующей допустимости их в суде либо альтернативной возможности в виде внедрения блокчейн-платформ на базе распределенных реестров для обеспечения неизменности выявляемых данных².

Достоверность доказательств в первую очередь оценивается с точки зрения уголовно-процессуального или иного законодательства, относящегося к уголовному судопроизводству, но стоит отметить, что источник получения доказательств должен быть своевременно проверен, должно быть подтверждение существования источника и факт получения доказательства. Относимость доказательств раскрывается применительно ко всем видам доказательств, так как доказательства, которые были получены в ходе проведения следственных действий, должны действительно иметь место и связь с подозреваемым / обвиняемым или же с фактом совершенного преступления.

Помимо исследования, все доказательства нуждаются в оценке. Это также род мыслительной деятельности субъектов расследования, при которой доказательства должны «придерживаться» критериев достоверности,

¹ Medjedovic Dz., Tahirovic E. Algorithms and data structures for massive datasets. N. Y. : Manning Shelter Island, 2024. P. 44.

² Ryu J. H., Sharma P. K., Jo J. H. A blockchain-based decentralized efficient investigation framework for IoT digital forensics // The journal of supercomputing. 2019. No. 75. P. 4380.

относимости и допустимости. Это нужно для того, чтобы при рассмотрении уголовного дела судом не возникло замечаний, отводов и ходатайств со стороны защиты. Все цифровые доказательства должны исследоваться и оцениваться в совокупности, так как отдельно взятое доказательство может противоречить другому, отдельно рассматриваемому, доказательству в деле.

К насущным проблемам процессуального оформления цифровых доказательств можно отнести неопределенность процессуального статуса цифровых данных. Так, в соответствии со ст. 84.1 УПК РФ, электронные носители информации признаются вещественными доказательствами, однако критерии их допустимости не раскрываются. Кроме того, отсутствует четкая регламентация процедуры изъятия таких данных, например, с облачных сервисов и прочих хранилищ. Имеются пробелы в соблюдении правил изъятия и фиксации цифровых доказательств при удаленном доступе к данным, когда согласно ст. 177 УПК РФ для этого требуется участие понятых. Это может привести к оспариванию доказательств в суде. Существенной проблемой является поиск и дальнейшее приобщение к делу криминалистически значимой информации, полученной из открытых источников сети Интернет и сервисов OSINT-разведки¹, деятельность которых признается незаконной и нарушающей права граждан на неприкосновенность частной жизни, личную и семейную тайну, что стало особенно важно в свете дополнения УК РФ ст. 272.1, устанавливающей уголовную ответственность за незаконные сбор и хранение персональных данных, а также создание на их основе информационных ресурсов, предназначенных для распространения личной информации. Указанная коллизия может породить прецеденты, когда полученные цифровые доказательства признаются недопустимыми. С целью устранения данной проблемы возможно развитие систем сертификации специалистов, задействованных в расследовании и раскрытии дистанционных мошенничеств.

Решение проблемы процессуального оформления цифровых доказательств при расследовании рассматриваемых преступлений требует комплексного подхода, включающего не только юридические нормы, но и технические меры, а также усовершенствованные криминалистические методики. В целях соблюдения принципа целостности и аутентичности цифровых доказательств целесообразно придерживаться широко распространенного в настоящее время принципа «цепочка поставок» (chain of custody)², который сможет обеспечить фиксацию всех этапов работы с доказательством. Проблема обеспечения сохранности цифровых доказательств при

¹ Омельченко В. А., Фаниев П. А. Использование программного обеспечения категории Open Source для создания анонимной рабочей среды и проведения разведки OSINT. М. : Изд-во «Перо», 2024. С. 52.

² Nath S., Summers K., Jaejong B. Digital evidence chain of custody: navigating new realities of digital forensics // Intelligent systems, and applications. 2024. No. 6. P. 12.

расследовании данного вида преступлений, безусловно, требует технологических инноваций. Так, предотвратить утрату данных можно путем организации центров обработки данных на основе распределенных баз, облачных или RAID-массивов с возможностью расчета контрольных сумм и контроля версий хранилищ либо внедрения блокчейн-технологий с временными метками, что обеспечит неизменность данных и прозрачность процесса их хранения. При этом защиту цифровых доказательств от посягательств можно обеспечить использованием квантово-устойчивых алгоритмов шифрования¹, что является одним из перспективных направлений реализации подобных систем в будущем.

Таким образом, основными проблемами в деятельности по собиранию цифровых доказательств являются отсутствие средств автоматизации поиска, фиксации и исследования цифровых доказательств, четких регламентов их процессуального оформления, инструкций по обеспечению достоверности (неизменяемости) и их допустимости, а также хранению данных.

В качестве возможного решения указанных проблем предложена система в виде хранилища криминалистически значимой компьютерной информации с функцией нейросетевого анализа данных (нейросетевой криминалистический кластер). Описанное в работе решение может использоваться в целях повышения эффективности поиска необходимых для раскрытия и расследования рассматриваемых преступлений сведений, удобства обработки значительного количества данных с использованием ключевых слов и фильтров в едином сегменте сети, снижения трудозатрат и ресурсов поиска криминалистически значимой информации сотрудниками органов внутренних дел.

Проведенное исследование позволяет сделать вывод о том, что основными направлениями совершенствования деятельности по собиранию цифровых доказательств при расследовании рассматриваемых преступлений являются: подробная регламентация и алгоритмизация процесса собирания, хранения и использования цифровых доказательств, что в условиях постоянной трансформации и эволюции киберпреступности возможно, например, при тщательной классификации способов, средств и условий совершаемых преступлений, а также их универсальной кодификации в целях разработки общей концепции их расследования и выработки соответствующих заданным условиям алгоритмов расследования; введение национальных стандартов по фиксации и анализу цифровых доказательств, а также развитие систем сертификации специалистов, задействованных в расследовании и раскрытии дистанционных мошенничеств; расширение перечня программных ТКС для автоматизированного поиска, фиксации и исследования цифровых доказательств на базе технологий ИИ и анализа

¹ Xiong J., Shen L., Liu Y. Enhancing IoT security in smart grids with quantum-resistant hybrid encryption // Scientific Reports. 2025. No. 15 (3). P. 12.

больших данных; развитие облачных платформ для безопасного и неизменного хранения цифровых доказательств с применением блокчейн-технологий и распределенных реестров; создание единого нейросетевого криминалистического кластера данных с возможностью оперативного доступа к цифровым доказательствам, поиска и обработки криминалистически значимой информации с использованием ключевых слов и фильтров в едином сегменте сети.

§ 3. Совершенствование криминалистических учетов при раскрытии и расследовании дистанционных мошенничеств, совершаемых с использованием интернет-сервисов

В настоящее время насчитываются десятки различных учетов, которые в зависимости от особенностей учитываемых объектов и характеризующих их признаков подразделяются на оперативно-справочные, криминалистические и справочно-вспомогательные учеты. Криминалистическая регистрация является систематизированным научно обоснованным учетом и основой информационного обеспечения органов внутренних дел сведениями об объектах и лицах в сфере уголовного судопроизводства и оперативно-розыскной деятельности. Принимая во внимание, что криминалистическая регистрация определяется перечнем учетных объектов, набор которых диктуется существующим уровнем технического развития, одним из вариантов решения проблем, связанных с поиском, анализом и исследованием цифровых следов, является введение новой системы регистрации цифровых доказательств в виде нейросетевого кластера криминалистически значимой цифровой информации. Формами криминалистических учетов, входящих в указанную систему регистрации цифровых доказательств, могут являться документированная информация, структурированные базы данных со сведениями о технических средствах и их сетевой активности, программное обеспечение, в том числе вредоносное, веб-ресурсы, аудио- и видеозаписи, а также их смешанные варианты, что позволит сформировать глобальную платформу анализа разнородных данных. Предложенная система криминалистического учета цифровых доказательств сможет послужить в дальнейшем основой для реализации программного технико-криминалистического средства с возможностью формирования типовых следственных версий и плана расследования дистанционного мошенничества.

Быстрый темп технологического прогресса, переход к цифровой экономике и, как следствие, обработка значительных массивов данных в электронном виде объясняют недостаточность применения традиционных методов собирания и исследования доказательств при расследовании ряда наиболее распространенных в настоящее время преступных деяний. В этой связи в криминалистической теории наблюдается тенденция изучения так называемых

цифровых следов преступной деятельности¹, что в большей степени обусловлено ежегодным приростом преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, в совокупности составивших за 2024 год более 40 % от числа всех зарегистрированных преступных деяний². Несмотря на широкое применение термина «цифровое доказательство» в зарубежной и отечественной научной литературе, в УПК РФ в настоящее время отсутствует его законодательное определение. Но на международном уровне под цифровым (электронным) доказательством, как правило, понимают любую информацию, обладающую доказательной силой и хранимой (передаваемой) в цифровой форме³.

Анализ способов совершения преступных деяний позволяет сделать заключение о наиболее вероятном расположении следов, оставляемых при том или ином используемом преступником методе⁴. Криминалистическое изучение особенностей совершения преступлений, в частности способов, дает исходные положения для разработки технико-криминалистических средств, при помощи которых следы преступления окажутся зафиксированными наиболее полно и будут пригодными для дальнейшего исследования. Доказывание в понимании познавательной деятельности – это оперирование доказательствами⁵, поэтому процесс доказывания складывается из четырех элементов: поиска (обнаружения, собирания, фиксации), исследования, оценки и использования доказательств, грамотность проведения и правильность процессуального оформления которых способствуют оперативному изобличению участников преступного события и обеспечению надежной доказательственной базы для органов следствия⁶. Обнаружение цифровых следов преступлений является поисковой деятельностью следователя, которая направлена на собирание доказательственной и ориентирующей криминалистически значимой информации, что возможно с использованием различных технических устройств (компьютерных, мобильных и пр.), а также программных технико-криминалистических средств.

¹ Цифровые следы преступлений : моногр. / А. М. Багмет, В. В. Бычков, С. Ю. Скобелин, Н. Н. Ильин. М. : Проспект, 2023. С. 3.

² Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2024 года // МВД России. URL: <https://мвд.рф/reports/item/60248328/> (дата обращения: 25.06.2025).

³ The Practical Guide for Requesting Electronic Evidence across Borders // United Nations Office on Drugs and Crime. URL: <https://sherloc.unodc.org/cld/ru/st/evidence/practical-guide.html> (дата обращения: 25.06.2025).

⁴ Выявление причин преступности и предупреждение преступлений. Общие положения / П. Ф. Гришанин, Г. Г. Зуйков, А. С. Кривошеев [и др.]. М. : НИиРИО МВШ МООП СССР, 1967. С. 117.

⁵ Белкин Р. С. Криминалистика: проблемы, тенденции, перспективы. Общая и частные теории. М. : Юридическая литература, 1987. С. 76.

⁶ Скобелин С. Ю. Цифровая криминалистика: объект и направления развития // Российский следователь. 2020. № 4. С. 44.

Несмотря на динамичное развитие общей теории криминалистики, например, путем ее дополнения частными криминалистическими теориями (исследования компьютерной информации¹, информационно-компьютерного обеспечения криминалистической деятельности² и пр.), релевантные на сегодняшний день обзоры, посвященные выявлению проблем в области расследования³, позволяют сделать вывод о значимости собирания цифровых доказательств и необходимости автоматизации процесса их исследования, что обусловлено сложностями анализа больших массивов данных в электронном виде.

Одним из вариантов обеспечения быстрой и эффективной обработки собранной криминалистически значимой компьютерной информации является внедрение в алгоритмы функционирования программных технико-криминалистических средств технологий ИИ, основанных на математических моделях и реализованных по принципу организации сетей нервных клеток человека. Таким образом, автоматизировать процессы собирания и исследования цифровых доказательств с минимальными трудозатратами позволит специализированное программное обеспечение, разработанное на базе машинного обучения, при этом точность и прозрачность анализа данных смогут обеспечить, например, ХАИ-системы (от англ. explainable artificial intelligence (ХАИ) – объяснимый искусственный интеллект)⁴ и модели, способные объяснять принимаемые нейросетью решения адаптированным для человека языком, что особенно важно для исключения проблем предвзятости алгоритмов.

Наиболее перспективными направлениями применения методов обработки данных на основе технологий ИИ в области расследования преступлений являются проведение криминалистических исследований и выдача заключений по вопросам, разрешение которых требует специальных знаний в области цифровой криминалистики. При этом необходимо соблюдать этическое использование указанных технологий, а также обеспечи-

¹ Цифровая криминалистика / под ред. В. Б. Вехова, С. В. Зуева. М. : Юрайт, 2025. С. 11.

² Теория информационно-компьютерного обеспечения криминалистической деятельности : моногр. / под. ред. Е. Р. Россинской. М. : Проспект, 2022. С. 13.

³ Horsman G., Sunde N. Unboxing the digital forensic investigation process // Science and Justice. No. 62. 2022. P. 176 ; Dunsin D., Ghanem M., Ouazzane K. A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response // Digital Investigation. No. 48. 2024. P. 3 ; Casino F., Dasaklis T. Research trends, challenges, and emerging topics in digital forensics: A review of reviews // IEEE Access. 2022. No. 10. V. P. 25483 ; Машков С. А. Большие данные и криминалистика: возможности и перспективы // Сибирские уголовно-процессуальные и криминалистические чтения. 2024. № 2. С. 81 ; Jian X., Siegel M., Towards a joint semantic analysis in mobile forensics environments // Digital Investigation. 2025. No. 52. P. 2.

⁴ Lundberg E., Mozeliuss P. The potential effects of deepfakes on news media and entertainment // AI & Society. No. 11. 2024. P. 7.

вать строгую регламентацию обучения и переобучения разрабатываемых на его основе систем, что возможно только при соблюдении единых стандартов управления процессами для анализа данных. Таким образом, на сегодняшний день важно принять факт неотвратимости задействования нейросетевых технологий в процесс расследования преступлений. Однако на стадии зарождения и реализации основного функционала рассмотренных систем необходимо заблаговременно определить базовые требования к разработкам и возможности их использования в области противодействия преступлениям с учетом применимости принципов справедливости, подотчетности, прозрачности и объяснимости всех осуществляемых искусственным интеллектом действий и принимаемых решений.

Активное внедрение современных информационных технологий в деятельность правоохранительных органов способствует расширению использования аналитических методов, что значительно влияет на организацию расследования преступлений. Автоматизация процессов сбора, хранения, систематизации и анализа криминалистически значимой информации повышает эффективность следственной, оперативно-розыскной, экспертной и судебной деятельности, способствует научной организации труда и оптимизации процессов расследования¹. Эффективность раскрытия и расследования преступлений в большинстве случаев зависит от качества и количества криминалистически значимой информации, источниками которой могут быть как материальные и идеальные следы, так и следообразующие объекты². К такого рода информации относят находящиеся в причинно-следственной связи с преступлением данные или сведения, которые, например, могут характеризовать способ и средства его совершения, объект, субъект или предмет преступного посягательства и пр. Системы объектов в виде баз данных или хранилищ информации представляют собой криминалистическую регистрацию, которая складывается из подсистем (криминалистических учетов), отличающихся друг от друга учитываемыми данными, способами или формами их систематизации. В связи с этим предлагается ввести новый криминалистический учет, который выступит кластером обучающих данных для информационной системы, используемой в целях систематизации криминалистически значимой компьютерной информации.

Основными источниками информационного обеспечения следственной деятельности в настоящее время являются криминалистические регистрационные системы правоохранительных ведомств, ведомственные учеты правоохранительных органов, не затрагивающие преступную деятель-

¹ Зеленский В. Д., Меретуков Г. М. Криминалистика. СПб. : Юридический центр-Пресс, 2015. С. 704.

² Курс криминалистики / Т. В. Аверьянова, Р. С. Белкин, Ю. Г. Корухов, Е. Р. Россинская. М. : Норма : ИНФРА-М, 2023. С. 382.

ность, различные информационные системы государственных органов власти и управления, учреждений, организаций и предприятий различных форм собственности, информационные ресурсы научно-методического и справочного содержания, а также сведения, размещенные в киберсреде.

Перечисленные ресурсы широко используются следователями, но зачастую бессистемно, эпизодически либо не в полном объеме. Для повышения эффективности их использования необходима систематизация имеющихся данных, обеспечивающая организацию информационных потоков и удобный к ним доступ. Увеличение объема регистрируемых данных и доступных информационных ресурсов, а также создание новых и совершенствование уже существующих криминалистических учетов является перспективным направлением развития информационного обеспечения следственной деятельности.

Таким образом, для более эффективного использования экспертно-криминалистических учетов в раскрытии и расследовании преступлений целесообразно интегрировать различные виды учетов в единую систему, что позволит установить корреляционные связи между объектами разных видов учетов¹. В такого рода системе должен быть предусмотрен функционал для определения связей между следами, оставленными преступником в информационных системах и технических средствах, изъятыми в рамках одного преступного деяния, с другим комплексом следов, изъятым с иного объекта.

Повысить эффективность расследования преступлений, в частности связанных с дистанционным мошенничеством, за счет систематизации, классификации и автоматизированного анализа цифровых следов позволит интегрированная система учета цифровых доказательств, структурными элементами при реализации которой могут выступить подсистемы сбора и агрегации данных, их классификации и структурирования, анализа и оценки, хранения и обмена данными, а также генерации отчетов и визуализации (рис. 1).



Рис. 1. Структура системы криминалистической регистрации цифровых доказательств по преступлениям, связанным с дистанционным мошенничеством

¹Аминев Ф. Г. Актуальные проблемы формирования и использования экспертно-криминалистических учетов в расследовании и раскрытии преступлений : моногр. Уфа.: РИО БашГУ, 2004. С. 155.

Так, подсистема сбора и агрегации данных обеспечит оперативный сбор разнородных цифровых доказательств из множества источников, например с локальных носителей данных, серверов, облачных хранилищ, технических средств, а также элементов (датчиков) интернета вещей, сетевых маршрутизаторов, журналов криптовалютных транзакций, адресов электронных кошельков, межсетевых экранов, прокси-серверов, систем обнаружения вторжений и пр.

Подсистема классификации и структурирования доказательств в зависимости от заданных критериев и способов стандартизации данных обеспечит их систематизацию и разделение по типу, например, на текстовые файлы, бинарные данные, лог-файлы, метаданные, графические данные, аудио- или видеозаписи, а также классификацию по временным меткам и корреляцию событий (создание временных шкал, выявление закономерностей взаимодействия между событиями (например, совпадение времени доступа к информационным системам и осуществление несанкционированного доступа к компьютерной информации)).

Подсистема анализа и оценки доказательств позволит осуществить аналитическую обработку собранных данных, выявить скрытые взаимосвязи между событиями на основе методов машинного обучения, кластеризации, предсказания сценария развития преступления, оценки достоверности цифровых доказательств и их весомости.

Подсистема хранения и обмена данными обеспечит их централизованную сохранность в виде баз данных, которая осуществляется с помощью функций индексирования, шифрования и контроля доступа, интеграцию с национальными и международными реестрами криминалистически значимых данных с возможностью обмена информацией для оперативного реагирования, а также аудит и протоколирование для фиксации изменений и доступа к данным.

Подсистема генерации отчетов и визуализации послужит гибким инструментом для построения отчетов в наглядной форме (дашбордов (от англ. dashboard – панель управления), диаграмм, временных линий, графов связей между событиями, а также статистических сводок с возможностью формирования выводов на основе пользовательских запросов и анализа шаблонов на базе обученных ранее данных).

В систему криминалистического учета по преступлениям, связанным с дистанционным мошенничеством, целесообразно включить:

- 1) подсистему учета зарегистрированных преступлений для сбора и систематизации информации о каждом зарегистрированном преступном деянии, включая дату, время, место, способ совершения преступления, используемые средства, предмет преступного посягательства, размер ущерба;

- 2) подсистему учета лиц, совершивших преступления, для систематизации информации о подозреваемых или обвиняемых лицах, включая анкетные данные, сведения о судимостях, используемые учетные данные,

IP-адреса и MAC-идентификаторы принадлежащих им устройств, адрес электронной почты, аккаунты в социальных сетях и мессенджерах, профессиональные навыки и умения;

3) подсистему учета средств совершения преступлений для сбора информации о задействованных технических средствах и программном обеспечении, включая их характеристики, происхождение, способы задействования;

4) подсистему учета цифровых следов преступлений и мест их расположения для систематизации информации о цифровых следах, оставляемых различными средствами совершения преступлений, а также о местах их наиболее вероятного расположения;

5) подсистему учета криминалистически значимой информации об обстановке совершения преступлений для выявления и систематизации факторов, способствовавших совершению преступления.

Криминалистический учет по преступлениям, связанным с дистанционным мошенничеством, может осуществляться по следующим основаниям:

1) по способу совершения преступления и использованным при этом техническим средствам и программному обеспечению;

2) по способу сокрытия следов преступления и используемым при этом техническим средствам и программному обеспечению;

3) по месту и времени задействования технических средств при совершении преступления;

4) по лог-файлам и журналам событий в информационных системах и программном обеспечении;

5) по сетевому трафику, сетевым артефактам;

6) по сигнатурам распространяемого вредоносного кода и паттернам аномального поведения (коллекции вредоносного программного обеспечения);

7) по учетным записям и идентификаторам в сети Интернет;

8) по цифровым аватарам в метасреде;

9) по идентификаторам в сетях Tor и I2P;

10) по хэш-суммам используемых при совершении преступления файлов и программного обеспечения;

11) по поддельным электронным документам, цифровым подписям и сертификатам;

12) по используемым при совершении преступления веб-ресурсам;

13) по биометрическим данным;

14) по метаданным мультимедиаконтента;

15) по скомпрометированным данным;

16) по синтетически сгенерированному контенту (дипфейк-контент);

17) по идентификаторам криптовалютных транзакций и прочим финансовым операциям.

Таким образом, формирование нового криминалистического учета в виде нейросетевого кластера данных, в частности, по преступлениям, связанным с дистанционным мошенничеством, является важным шагом на пути к повышению эффективности противодействия им. Система учета должна учитывать специфику цифровой среды, обеспечивать сбор, систематизацию и анализ информации о различных аспектах преступных деяний, а также соответствовать требованиям законодательства о персональных данных и информационной безопасности. Предложенная интегрированная система учета цифровых доказательств сможет послужить в дальнейшем основой для формирования модульной и масштабируемой платформы поддержки принятия решений (подбор методики расследования), позволяющей собирать, классифицировать и анализировать цифровые доказательства в режиме реального времени, использовать современные методы анализа на основе ИИ для выявления закономерностей и оценки вероятности развития событий, обеспечить безопасное хранение и обмен данными с возможностью интеграции с существующими национальными и международными системами, а также реализовать комплексное программное технико-криминалистическое средство с возможностью формирования типовых следственных версий и планов расследования преступлений, связанных с дистанционным мошенничеством (рис. 2), с учетом сведений, составляющих базовые элементы криминалистической характеристики преступного деяния.



Рис. 2. Упрощенная модель оптимизации процесса поиска, анализа и интерпретации цифровых доказательств с использованием алгоритмов ИИ:
AI – искусственный интеллект, ML – машинное обучение, CV – компьютерное зрение

Предлагаемый подход к анализу данных, нахождению закономерностей, идентификации связей и корреляций между переменными и построе-

нию моделей с использованием инструментов визуализации по своей сути представляет собой технику EDA-анализа¹ (от англ. exploratory data analysis – разведочный анализ данных) в виде комплекса методик, позволяющих исследовать, нормализовать и стандартизовать данные, определять их качество, структуру и характеристики, а также выявлять аномалии среди них. Таким образом, в эпоху цифровизации и растущего объема данных необходимо применение EDA-техник в криминалистике, которые обладают существенным потенциалом, являясь перспективой в области совершенствования всех имеющихся экспертных систем и криминалистических учетов. Оптимизация процесса поиска, анализа и интерпретации цифровых доказательств возможна с применением алгоритмов ИИ не только в отношении реализации программного технико-криминалистического средства, но и в совокупности с формируемыми цифровой моделью преступления, кластером цифровых доказательств в виде криминалистических учетов и системой поддержки принятия решений.

Подводя итог вышеуказанному, можно отметить, что криминалистика, как наука, изучающая закономерности механизма преступления и возникновения информации о нем, в условиях всеобщей цифровизации и интеллектуализации приобретает новые исследовательские и практико-ориентированные возможности. Технологии ИИ при этом представляют собой дополнительный инструмент, интегрируемый в систему криминалистических средств. Проведенный анализ наиболее значимых исследований в области цифровой криминалистики за последние несколько лет определил возможность реализации гибридной модели анализа электронных доказательств, в основе которой лежит интеграция традиционных методов цифровой криминалистики, машинного обучения и объяснимого искусственного интеллекта, что значительно повысит эффективность расследования преступлений, связанных с дистанционным мошенничеством. Так, существующие методы цифровой криминалистики можно усовершенствовать использованием комбинации современных технологических подходов, основанных на технологиях ИИ и распределенных вычислений, облачных технологиях и технологиях анализа данных, что позволит сформировать полноценный инструмент в целях противодействия дистанционному мошенничеству.

Таким образом, развитие распространенных в настоящее время методов анализа электронных доказательств по принципу глобального нейросетевого кластера цифровых доказательств представляет собой одно из перспективных направлений эволюции цифровой криминалистики и позволяет объединить преимущества отдельно взятых подходов, компенсируя недостатки при их использовании в отдельности.

¹ Тьюки Дж. Анализ результатов наблюдений. Разведочный анализ. М. : Мир, 1981. С. 18.

ЗАКЛЮЧЕНИЕ

В заключение необходимо отметить, что в условиях стремительного развития информационных технологий и увеличения числа преступлений данного вида вопрос разработки научно-практического пособия по организации раскрытия и расследования дистанционных мошенничеств, совершаемых с использованием интернет-сервисов, является особенно актуальным. Президент Российской Федерации В. В. Путин поручил по итогам совещания с членами Правительства Российской Федерации улучшить цифровую грамотность граждан страны¹. И действительно, статистика подтверждает необходимость таких мер: 70 % опрошенных россиян, согласно исследованию Okko и Rambler&Co, сталкивались с кибермошенничеством, при защите от киберпреступников жители страны полагаются на собственные силы. Почти 65% опрошенных считают, что подвергнуться обману не так уж и легко². Начальник УБК МВД России генерал-майор полиции Филипп Немов сообщил³, что преступники все чаще используют виртуальные АТС и мессенджеры.

В результате проведенного исследования предложена структура криминалистической характеристики дистанционных мошенничеств, совершаемых на интернет-сервисах, что послужило основой для выявления организационно-тактических особенностей раскрытия и расследования указанных преступных деяний. На примере наиболее распространенных преступных деяний, связанных с использованием информационно-телекоммуникационных технологий, была установлена взаимосвязь между структурными элементами криминалистической характеристики дистанционных мошенничеств.

Кроме того, в рамках исследования была представлена классификация способов совершения дистанционных мошенничеств с использованием интернет-сервисов, которая может служить практическим инструментом для правоохранительных органов при расследовании данных преступлений. Данная классификация способствует формированию целенаправленных планов (алгоритмов) следственных действий, что повышает эффективность расследований.

Выделены особенности производства проверочных действий, которые определяет специфика способов совершения рассматриваемой категории преступлений. На первоначальном этапе необходимо в кратчайшие

¹ Гапчук С. Владимир Путин поручил повысить цифровую грамотность россиян // Комсомольская правда. URL: <https://www.kp.ru/online/news/6308884/> (дата обращения: 28.03.2025).

² С кибермошенничеством сталкивались 70 % опрошенных россиян // ТАСС. URL: <https://tass.ru/obschestvo/22506821> (дата обращения: 28.03.2025).

³ В России из незаконного оборота изъяли более 1,5 млн sim-карт. URL: <https://dzen.ru/a/aFLJc81k9lrwCJUu> (дата обращения: 28.03.2025).

сроки с учетом допустимых уголовно-процессуальным законом средств получить максимально возможный объем информации о наличии либо отсутствии оснований для возбуждения уголовного дела, обстоятельствах произошедшего.

Особое внимание уделено тактическим аспектам производства отдельных следственных действий при расследовании дистанционных мошенничеств, что может послужить пособием для практикующих специалистов. В результате анализа следственной практики расследования дистанционных мошенничеств, совершаемых с использованием интернет-сервисов, приходим к выводу о том, что при расследовании преступлений этой категории проводятся, в частности, следующие следственные действия: осмотр мобильного телефона заявителя, как основного инструмента коммуникации с мошенником и инструмента осуществления финансовых операций; допрос потерпевшего; допрос подозреваемого; обыск; назначение производства судебных экспертиз. Осмотр места происшествия нецелесообразен в случаях мошенничества на интернет-сервисах, поскольку само преступление совершается в виртуальном пространстве.

Исследованы особенности криминалистического изучения цифровых следов, а также описаны возможности технико-криминалистического обеспечения, используемого при расследовании дистанционных мошенничеств. Программные средства, обеспечивающие поиск, фиксацию, сбор, исследование и оценку цифровых доказательств, играют ключевую роль в процессе раскрытия данных преступлений.

Таким образом, результаты настоящего исследования могут быть использованы для совершенствования практики расследования дистанционных мошенничеств и повышения уровня правоприменительной деятельности в данной области.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

I. Нормативные правовые акты и иные официальные документы

1. **Российская Федерация. Законы.** Конституция Российской Федерации : [принята всенародным голосованием 12 декабря 1993 г.] (с учетом поправок, внесенных Законами Российской Федерации о поправках к Конституции Российской Федерации от 30 декабря 2008 г. № 6-ФКЗ, от 30 декабря 2008 г. № 7-ФКЗ, от 5 февраля 2014 г. № 2-ФКЗ, от 21 июля 2014 г. № 11-ФКЗ, от 14 марта 2020 г. № 1-ФКЗ, от 4 октября 2022 года № 5-ФКЗ, от 4 октября 2022 года № 6-ФКЗ, от 4 октября 2022 года № 7-ФКЗ, от 4 октября 2022 года № 8-ФКЗ). – Текст : электронный // Официальный интернет-портал правовой информации. – URL: <http://www.pravo.gov.ru> (дата обращения: 25.06.2025).

2. **Российская Федерация. Законы.** Уголовный кодекс Российской Федерации : УК : текст с изменениями и дополнениями на 29 декабря 2025 г. : [принят Государственной Думой 24 мая 1996 г. : одобрен Советом Федерации 5 июня 1996 г.]. – Текст : электронный // Официальный интернет-портал правовой информации. – URL: <http://www.pravo.gov.ru> (дата обращения: 25.06.2025).

3. **Российская Федерация. Законы.** Уголовно-процессуальный кодекс Российской Федерации : УПК : текст с изменениями и дополнениями на 29 декабря 2025 г. : [принят Государственной Думой 22 ноября 2001 г. : одобрен Советом Федерации 5 декабря 2001 г.]. – Текст : электронный // Официальный интернет-портал правовой информации. – URL: <http://www.pravo.gov.ru> (дата обращения: 25.06.2025).

4. **Российская Федерация. Законы.** О полиции : Федеральный закон № 3-ФЗ : [принят Государственной Думой 28 января 2011 г. : одобрен Советом Федерации 2 февраля 2011 г.]. – Текст : электронный // Официальный интернет-портал правовой информации. – URL: <http://www.pravo.gov.ru> (дата обращения: 25.06.2025).

5. **Российская Федерация. Законы.** Об информации, информационных технологиях и о защите информации : Федеральный закон № 149-ФЗ : [принят Государственной Думой 8 июля 2006 г. : одобрен Советом Федерации 14 июля 2006 г.]. – Текст : электронный // Официальный интернет-портал правовой информации. – URL: <http://www.pravo.gov.ru> (дата обращения: 25.06.2025).

6. **ГОСТ Р 57429-2017.** Национальный стандарт Российской Федерации Судебная компьютерно-техническая экспертиза. Термины и определения (Forensic information technology examination. Terms and definitions). – Москва : Стандартинформ, 2018. – 25 с. – Текст : непосредственный.

II. Основная литература

1. **Аверьянова, Т. В.** Криминалистика / Т. В. Аверьянова. – Москва : Норма, 2023. – 928 с. – Текст : непосредственный.
2. **Аминев, Ф. Г.** Актуальные проблемы формирования и использования экспертно-криминалистических учетов в расследовании и раскрытии преступлений : монография / Ф. Г. Аминев. – Уфа: РИО БашГУ, 2004. – 182 с. – Текст : непосредственный.
3. **Белкин, Р. С.** Криминалистика: проблемы, тенденции, перспективы. Общая и частные теории / Р. С. Белкин. – Москва : Юридическая литература, 1987. – 270 с. – Текст : непосредственный.
4. **Белкин, Р. С.** Криминалистическая энциклопедия / Р. С. Белкин. – 2-е издание, дополненное. – Москва : Мегатрон-XXI, 2000. – 334 с. – Текст : непосредственный.
5. **Бурданова, В. С.** Предъявление для опознания на предварительном следствии / В. С. Бурданова, И. Е. Быховский ; Институт усовершенствования следственных работников органов прокуратуры и Министерства внутренних дел, Всесоюзный институт по изучению причин и разработке мер предупреждения преступности при Прокуратуре СССР. – Москва : ВНИИ ПУЗП, 1975. – 80 с.
6. Выявление причин преступности и предупреждение преступлений. Общие положения / П. Ф. Гришанин, Г. Г. Зуйков, А. С. Кривошеев [и др.]. – Москва : НИиРИО МВШ МООП СССР, 1967. – 179 с. – Текст : непосредственный.
7. **Гаспарян, Г. З.** Расследование хищений денежных средств, совершенных с использованием информационных банковских технологий : специальность 12.00.12 «Криминалистика; судебно-экспертная деятельность; оперативно-розыскная деятельность» : диссертация на соискание ученой степени кандидата юридических наук / Гаспарян Гурген Зорикович ; Академия управления Министерства внутренних дел Российской Федерации. – Москва, 2020. – 300 с. – Текст : непосредственный.
8. **Голятина, С. М.** Методика расследования хищений электронных денежных средств : специальность «Криминалистика; судебно-экспертная деятельность; оперативно-розыскная деятельность» : диссертация на соискание ученой степени кандидата юридических наук / Голятина Светлана Михайловна ; Волгоградская академия МВД России. – Волгоград, 2022. – 196 с. – Текст : непосредственный.
9. Исследование информации, содержащейся в мобильных телефонах: Типовая методика / С. В. Ермолов, В. А. Ращупкина, Е. А. Кресан [и др.]. – Москва : ЭКЦ МВД России, 2023. – 29 с. – Текст : непосредственный.
10. **Зеленский В. Д.** Криминалистика : учебник / В. Д. Зеленский, Г. М. Меретуков. – Санкт-Петербург : Юридический центр-Пресс, 2015. – 755 с. – Текст : непосредственный.

11. **Карагодин, В. Н.** Преодоление противодействия предварительному следствию / В. Н. Карагодин. – Свердловск : Издательство Уральского университета, 1992. – 175 с. – Текст : непосредственный.

12. **Козлов, А. Е.** Современные технико-криминалистические средства, применяемые в ходе осмотра места происшествия : учебное пособие / А. Е. Козлов, Е. Н. Макарова, О. Л. Романова. – Санкт-Петербург : СПбУ МВД России, 2024. – 64 с. – Текст : непосредственный.

13. **Комарова, А. А.** Интернет-мошенничество: проблемы детерминации и предупреждения : монография / А. А. Комарова. – Москва : Юрлитинформ, 2013. – 184 с. – Текст : непосредственный.

14. Криминалистика : учебник для вузов / ответственный редактор Н. П. Яблоков. – Москва, 1995. – 689 с. – Текст : непосредственный.

15. Криминалистическое изучение личности : научно-практическое пособие для магистров / ответственный редактор Я. В. Комиссарова. – Москва : Проспект, 2016. – 224 с. – Текст : непосредственный.

16. Курс криминалистики / Т. В. Аверьянова, Р. С. Белкин, Ю. Г. Корухов, Е. Р. Россинская. Москва : Норма : ИНФРА-М, 2023. 928 с. – Текст : непосредственный.

17. **Лавров, В. П.** Особенности расследования нераскрытых преступлений прошлых лет : учебное пособие / В. П. Лавров ; Высш. школа МВД СССР. – Москва : НИиРИО ВШ МВД СССР, 1972. – 87 с. – Текст : непосредственный.

18. **Нестеров, А. В.** Виртуальные следы в криминалистике : учебник / А. В. Нестеров. – Москва : Издательство КноРус, 2024. – 154 с. – Текст : непосредственный.

19. Новые способы совершения преступлений в сфере информационных технологий на территории государств – участников СНГ : аналитический обзор / И. Б. Колчевский, В. М. Журавлев, А. Г. Кузнецов [и др.]. – Москва : ФГКУ «ВНИИ МВД России», 2018. – 76 с. – Текст : непосредственный.

20. **Нугаева, Э. Д.** Особенности расследования мошенничества при оказании оккультных услуг : специальность 12.00.12 «Криминалистика; судебно-экспертная деятельность; оперативно-розыскная деятельность» : диссертация на соискание ученой степени кандидата юридических наук / Нугаева Эльвира Дамировна ; Ростовский юридический институт МВД России. – Ростов н/Д, 2019. – 269 с. – Текст : непосредственный.

21. **Омельченко, В. А.** Использование программного обеспечения категории Open Source, для создания анонимной рабочей среды и проведения разведки OSINT / В. А. Омельченко, П. А. Фаниев. – Москва : Издательство «Перо», 2024. – 69 с. – Текст : непосредственный.

22. Особенности первоначального этапа расследования неправомерного доступа к компьютерной информации : учебно-методическое пособие / Э. Д. Нугаева, С. Р. Низаева, В. Р. Гайнельзянова, З. И. Харисо-

ва. – Уфа : Уфимский ЮИ МВД России, 2023. – 96 с. – Текст : непосредственный.

23. **Полещук, О. В.** Криминалистическое исследование следов при расследовании компьютерных преступлений : монография / О. В. Полещук, Г. М. Шаповалова. – Владивосток : Издательство Дальневосточного университета, 2006. – 161 с. – Текст : непосредственный.

24. **Попов, А. Н.** Преступления в сфере компьютерной информации : учебное пособие / А. Н. Попов. – Санкт-Петербург : Санкт-Петербургский юридический институт Университета прокуратуры Российской Федерации, 2018. – 68 с. – Текст : непосредственный.

25. **Порубов, Н. И.** Тактика допроса на предварительном следствии : учебное пособие / Н. И. Порубов. – Москва : БЭК, 1998. – 196 с. – Текст : непосредственный.

26. Преступления в сфере компьютерной информации: квалификация и доказывание : учебное пособие / Ю. В. Гаврилин, А. Ю. Головин, А. В. Кузнецов, Т. В. Толстухина ; под редакцией Ю. В. Гаврилина. – Москва : Книжный мир, 2003. – 235 с. – Текст : непосредственный.

27. Теория информационно-компьютерного обеспечения криминалистической деятельности : монография / под редакцией Е. Р. Россинской. – Москва : Проспект, 2022. – 254 с. – Текст : непосредственный.

28. **Соловьев, А. Б.** Допрос на предварительном следствии : методическое пособие / А. Б. Соловьев ; Всесоюзный институт по изучению причин и разработке мер предупреждения преступности. – 2-е издание, переработанное. – Москва : Б. и., 1986. – 118 с. – Текст : непосредственный.

29. **Старостенко, Н.И.** Первоначальный этап расследования хищений, совершенных с применением методов социальной инженерии и информационно-телекоммуникационных технологий : специальность 5.1.4 «Уголовно-правовые науки» : диссертация на соискание ученой степени кандидата юридических наук / Старостенко Нина Игоревна ; Краснодарский университет МВД России. – Краснодар, 2023. – 230 с. – Текст : непосредственный.

30. Типовая методика исследования информации, содержащейся в мобильных телефонах / О. В. Тушканова, В. М. Щербак, С. Н. Сеницын, С. В. Ермолов. – Москва : ЭКЦ МВД России, 2014. – 23 с. – Текст : непосредственный.

31. **Тьюки, Дж.** Анализ результатов наблюдений. Разведочный анализ / Дж. Тьюки. – Москва : Мир, 1981. – 696 с. – Текст : непосредственный.

32. **Федотов, Н. Н.** Форензика – компьютерная криминалистика / Н. Н. Федотов. – Москва : Юридический мир, 2007. – 432 с. – Текст : непосредственный.

33. **Харина, Е. А.** Особенности методики расследования мошенничества в сфере компьютерной информации : специальность 5.1.4. «Уголовно-

правовые науки» : диссертация на соискание ученой степени кандидата юридических наук / Харина Елена Алексеевна ; Кубанский государственный аграрный университет имени И. Т. Трубилина. – Красноярск, 2024. – 248 с. – Текст : непосредственный.

34. Цифровая криминалистика / под редакцией В. Б. Вехова, С. В. Зуева. – Москва : Юрайт, 2025. – 490 с. – Текст : непосредственный.

35. Цифровые следы преступлений : монография / А. М. Багмет, В. В. Бычков, С. Ю. Скобелин, Н. Н. Ильин. – Москва : Проспект, 2023. – 168 с. – Текст : непосредственный.

36. Шевченко, Е. С. Тактика производства следственных действий при расследовании киберпреступлений : специальность 12.00.12 «Криминалистика; судебно-экспертная деятельность; оперативно-розыскная деятельность» : диссертация на соискание ученой степени кандидата юридических наук / Шевченко Елизавета Сергеевна ; Московский государственный юридический университет имени О. Е. Кутафина. – Москва, 2016. – 249 с. – Текст : непосредственный.

37. Шурухнов, Н. Г. Использование при допросе ранее данных объяснений / Н. Г. Шурухнов. – Текст : непосредственный // Тактические приемы допроса и пределы их использования : сборник тезисов теоретического семинара, 14 марта 1980 г. – Москва : ВНИИ МВД СССР, 1980. – С. 50–53.

38. Эксархопуло, А. А. Криминалистика. Теоретический курс : монография / А. А. Эксархопуло, И. А. Макаренко, Р. И. Зайнуллин. – Уфа : НИИ ППГ, 2022. – 650 с. – Текст : непосредственный.

III. Дополнительная литература

1. Бахтеев, Д. В. Частные криминалистические теории как источник для разработки прикладных систем искусственного интеллекта в следственной деятельности / Д. В. Бахтеев. – Текст : непосредственный // Сибирские уголовно-процессуальные и криминалистические чтения. – 2020. – № 2 (28). – С. 32–43.

2. Виноградова, О. П. Особенности тактики производства невербальных следственных действий при расследовании хищений предметов, имеющих особую ценность / О. П. Виноградова. – Текст : непосредственный // Использование специальных знаний: теоретико-правовая парадигма и проблемы практической деятельности : материалы международной научно-практической конференции, Владивосток, 26–27 сентября 2019 г. – Владивосток : ДВЮИ МВД России, 2019. С. 35–42.

3. Глебова, К. В. «Паутина в паутине»: интернет-мошенничество / К. В. Глебова, К. В. Воробьев. – Текст : непосредственный // Молодой ученый. – 2017. – № 3 (137). – С. 28–30.

4. **Грибунов, О. П.** Отдельные вопросы тактики допроса при расследовании взяточничества / О. П. Грибунов. – Текст : непосредственный // Научный дайджест Восточно-Сибирского института МВД России. – 2020. – № 4 (7). – С. 28–32.

5. **Дяблова, Ю. Л.** Понятие и структура личности в криминалистике / Ю. Л. Дяблова. – Текст : непосредственный // Известия Тульского государственного университета. Экономические и юридические науки. – 2016. – № 2-2. – С. 99–110.

6. **Евдокимова, О. В.** Методы социальной инженерии, используемые лицами при мошенничестве на сайтах знакомств и их учет при расследовании преступлений / О. В. Евдокимова. – Текст : непосредственный // Проблемы развития криминалистической тактики. – 2025. – № 9. – С. 90–94.

7. **Евдокимова, О. В.** Особенности проведения допроса потерпевших при расследовании мошенничеств, совершаемых на интернет-сервисах / О. В. Евдокимова. – Текст : непосредственный // Актуальные вопросы расследования преступлений в условиях развития цифровых технологий : материалы всероссийской научно-практической конференции, посвященной 20-летию кафедры криминалистики и кафедры уголовного процесса, Уфа, 17 октября 2025 г. – Уфа : Уфимский ЮИ МВД России, 2025. – С. 235–241.

8. **Кулаевский, А. В.** Нормативно-правовые основания развития программы материнского (семейного) капитала / А. В. Кулаевский. – Текст : непосредственный // Вопросы российского и международного права. – 2024. – Т. 14, № 7А. – С. 449–456.

9. **Лутцева, К. В.** Особенности проведения допроса потерпевшего при расследовании преступлений в сфере информационно-телекоммуникационных технологий / К. В. Лутцева. – Текст : непосредственный // Проблемы квалификации и расследования преступлений, совершаемых с применением информационно-коммуникационных технологий : сборник научных трудов международной научно-практической конференции, Москва, 27 мая 2022 г. – Москва : Московский университет МВД России имени В. Я. Кикотя, 2022. – С. 206–211.

10. **Маилян, А. В.** Общие положения криминалистической характеристики хищений, совершенных с банковского счета, в отношении электронных денежных средств и/или с помощью электронных средств платежа / А. В. Маилян. – Текст : непосредственный // Известия Тульского государственного университета. – 2020. – № 3. – С. 120–126.

11. **Машков, С. А.** Большие данные и криминалистика: возможности и перспективы / С. А. Машков. – Текст : непосредственный // Сибирские уголовно-процессуальные и криминалистические чтения. – 2024. – № 2. – С. 78–86.

12. **Низаева, С. Р.** Тактические особенности производства обыска и выемки документов при расследовании мошенничества на рынке вторич-

ного жилья / С. Р. Низаева. – Текст : непосредственный // Вестник Уфимского юридического института МВД России. – 2016. – № 3 (73). – С. 38–40.

13. **Низаева, С. Р.** Цифровые технологии в криминалистике / С. Р. Низаева. – Текст : непосредственный // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. – 2021. – № 21 (1). – С. 55–56.

14. **Онищенко, О. Р.** Характеристика личности потерпевших от мошенничества / О. Р. Онищенко. – Текст : непосредственный // Проблемы уголовного права, уголовного процесса и криминалистики. – 2003. Вып. 7. – С. 115–122.

15. **Осипенко, А. Л.** Правовое регулирование и тактические особенности изъятия электронных носителей информации / А. Л. Осипенко, А. И. Гайдин. – Текст : непосредственный // Вестник Воронежского института МВД России. – 2014. – № 1. – С. 156–163.

16. **Протасевич, А. А.** Криминалистическая характеристика компьютерных преступлений / А. А. Протасевич, Л. П. Зверьянская. – Текст : непосредственный // Российский следователь. – 2013. – № 11. – С. 45–47.

17. **Россинская, Е. Р.** Концепция цифровых следов в криминалистике / Е. Р. Россинская. – Текст : непосредственный // Аубакировские чтения : материалы международной научно-практической конференции, Алматы, 19 февраля 2019 г. – Алматы, 2019. – С. 6–9.

18. **Россинская, Е. Р.** Проблемы использования специальных знаний в судебном исследовании компьютерных преступлений в условиях цифровизации / Е. Р. Россинская. – Текст : непосредственный // Вестник Университета имени О. Е. Кутафина (МГЮА). – 2019. – № 5 (57). – С. 31–44.

19. **Рыжкова, М. В.** Устойчивость феномена финансовой пирамиды / М. В. Рыжкова, Э. Р. Кашапова. – Текст : непосредственный // Terra Economicus. – 2022. – № 20 (3). – С. 22–38.

20. Системная модель интеллектуальной предметно-ориентированной профайлинг-системы / В. В. Антонов, З. И. Харисова, З. Р. Мансурова [и др.]. – Текст : непосредственный // Онтология проектирования. – 2020. – Т. 10, № 3. – С. 338–350.

21. **Скобелин, С. Ю.** Цифровая криминалистика: объект и направления развития / С. Ю. Скобелин. – Текст : непосредственный // Российский следователь. – 2020. – № 4. – С. 42–44.

22. **Сперанский, К. К.** Особенности допроса по делам несовершеннолетних / К. К. Сперанский. – Текст : непосредственный // Социальная законность. – 1968. – № 4. – С. 51–53.

23. **Сысенко, А. Р.** Проблемы назначения и производства судебной компьютерно-технической экспертизы / А. Р. Сысенко, И. С. Смирнова, С. Е. Тимошенко. – Текст : непосредственный // Сибирское юридическое обозрение. – 2020. – № 17 (4). – С. 523–533.

24. **Харисова, З. И.** Криминалистическая характеристика преступлений, связанных с неправомерным доступом к компьютерной информации /

3. И. Харисова. – Текст : непосредственный // Правовое государство: теория и практика. – 2025. – № 2 (80). – С. 96–105.

25. **Хмыров, А. А.** Криминалистическая характеристика преступления и пути доказывания по уголовному делу / А. А. Хмыров. – Текст : непосредственный // Известия высших учебных заведений. Правоведение. – 1978. – № 3. – С. 59–66.

26. **Шевченко, Е. С.** Социально-технологические детерминанты следственных действий при расследовании киберпреступлений / Е. С. Шевченко. – Текст : непосредственный // Актуальные проблемы российского права. – 2016. – № 10 (71). – С. 160–169.

27. **Adams, T. A.** Trends, challenges and opportunities of engaging digital forensics for cybercrime investigations / T. A. Adams. – Text // Advances in multidisciplinary and scientific research journal publication. – 2024. – No. 15 (1). – P. 1–12.

28. **Cantelli-Forti, A.** A consistent and tamper-proof methodology for acquisition of automatically verifiable forensic web evidence / A. Cantelli-Forti, G. Longo, F. Lupia. – Text // International journal of information security. – 2025. – No. 24 (81). – P. 1–14.

29. **Casino, F.** Research trends, challenges, and emerging topics in digital forensics: A review of reviews / F. Casino, T. Dasaklis. – Text // IEEE Access. – 2022. – No. 10. V. – P. 25464–25493.

30. **Dunsin, D.** A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response / D. Dunsin, M. Ghanem, K. Ouazzane. – Text // Digital Investigation. – 2024. – No. 48. – P. 1–22.

31. **Garrie, D. B.** Digital forensic investigations and ediscovery / D. B. Garrie, L. M. Gordon, B. Newman. – Text // Uncovering Digital Evidence. – 2024. – No. 1. – P. 155–191.

32. **Horsman, G.** Unboxing the digital forensic investigation process / G. Horsman, N. Sunde. – Text // Science and Justice. – 2022. – No. 62. – P. 171–180.

33. **Jian, X.** Towards a joint semantic analysis in mobile forensics environments / Jian X., Siegel M. – Text // Digital Investigation. – 2025. – No. 52. – P. 1–26.

34. **Kreso, I.** Using blockchain technology for preserving digital evidence in digital forensics / I. Kreso. – Text // Knowledge international journal. – 2025. – No. 68 (3). – P. 331–336.

35. **Lundberg, E.** The potential effects of deepfakes on news media and entertainment / E. Lundberg, P. Mozelius. – Text // AI & Society. – 2024. – No. 11. – P. 1–12.

36. **Makhkamov, D.** International cooperation in the field of forensic computer technical expertise / D. Makhkamov. – Text // Journal of Law Research. – 2019. – V. 9 (1). – P. 11–15.

37. **Medjedovic, Dz.** Algorithms and data structures for massive datasets / Dz. Medjedovic, E. Tahirovic. – New York : Manning Shelter Island, 2024. – 340 p. – Text.

38. **Nath, S.** Digital evidence chain of custody: navigating new realities of digital forensics / S. Nath, K. Summers, B. Jaejong. – Text // Intelligent systems, and applications. – 2024. – No. 6. – P. 11–20.

39. **Nelufule, N.** Intersection of electronic security and digital forensics: data protecting techniques and uncovering data clues / N. Nelufule. – Text // Towards new e-infrastructure and e-services for developing countries. – 2025. – No. 587. – P. 351–367.

40. **Thakur, K. S.** Safeguarding justice employing blockchain-enabled secure chain of custody framework for digital evidence / K. S. Thakur, R. Ahuja. – Text // Innovations in electrical and electronic engineering. – 2024. – No. 115. – P. 1–11.

41. **Tiwari, N.** Cyber and digital forensic / N. Tiwari, Y. Baroniya, V. Bharadwaj. – Text // Textbook of forensic science. – 2023. – No. 25. – P. 773–803.

42. **Xiong, J.** Enhancing IoT security in smart grids with quantum-resistant hybrid encryption / J. Xiong, L. Shen, Y. Liu. – Text // Scientific Reports. – 2025. – No. 15 (3). – P. 1–15.

43. **Yi, X.** Digital rights management scheme based on redactable blockchain and perceptual hash / X. Yi, Y. Zhou, Y. Lin [et al.]. – Text // Peer-to-peer networking and applications. – 2023. – No. 16. – P. 2630–2648.

IV. Эмпирические материалы

1. Апелляционное определение Верховного Суда Республики Марий Эл. Дело № 22-175/2023. – Текст : электронный // Судебные решения РФ. – URL : <https://судебныерешения.рф/search> (дата обращения: 28.03.2025).

2. Краткая характеристика состояния преступности в Российской Федерации за январь – май 2025 года. – Текст : электронный // МВД России : официальный сайт. – URL: <https://мвд.рф/reports/item/66517593/> (дата обращения: 10.07.2025).

3. Приговор Всеволожского городского суда Ленинградской области. Дело № 1-12/2022. – Текст : электронный // Судебные решения РФ. – URL : <https://судебныерешения.рф/search> (дата обращения: 28.03.2025).

4. Приговор Всеволожского городского суда Ленинградской области. Дело № 1-12/2022. – Текст : электронный // Судебные решения РФ. – URL : <https://судебныерешения.рф/search> (дата обращения: 28.03.2025).

5. Приговор Кузнецкого районного суда Пензенской области. Дело № 1-188/2023. – Текст : электронный // Судебные решения РФ. – URL : <https://судебныерешения.рф/search> (дата обращения: 28.03.2025).

6. Приговор Октябрьского районного суда г. Екатеринбурга. Дело № 1-210/2023. – Текст : электронный // Судебные решения РФ. – URL : <https://судебныерешения.рф/search> (дата обращения: 28.03.2025).

7. Приговор Центрального районного суда г. Омска. Дело № 1-314/2024. – Текст : электронный // Судебные решения РФ. – URL : <https://судебныерешения.рф/search> (дата обращения: 28.03.2025).

V. Иные материалы

1. В России из незаконного оборота изъяли более 1,5 млн sim-карт. – Текст : электронный. – URL: <https://dzen.ru/a/aFLJc81k9lrwCJUt> (дата обращения: 28.03.2025).

2. Гапчук, С. Владимир Путин поручил повысить цифровую грамотность россиян / С. Гапчук. – Текст : электронный // Комсомольская правда. – URL: <https://www.kp.ru/online/news/6308884/> (дата обращения: 28.03.2025).

3. Зарабатывавшие на фишинговых сайтах предстанут перед судом. – Текст : электронный // Прокуратура Санкт-Петербурга : официальный сайт. – URL: https://epp.genproc.gov.ru/web/proc_78/massmedia/news?item=100885263 (дата обращения: 28.03.2025).

4. МВД России : официальный сайт. – URL: <https://мвд.рф/> (дата обращения: 25.03.2025). – Текст : электронный.

5. О судебной практике по делам о мошенничестве, присвоении и растрате : постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48. – Текст : электронный // ГАРАНТ.РУ. – URL: <https://base.garant.ru/71823288> (дата обращения: 21.07.2025).

6. Пажитных, Ю. Аудитория дейтинг-сервисов в России достигла 8 млн пользователей / Ю. Пажитных. – Текст : электронный // Russian Business. – URL: <https://rb.ru/news/sajty-znakomstv/> (дата обращения: 28.03.2025).

7. С кибермошенничеством сталкивались 70 % опрошенных россиян. – Текст : электронный // ТАСС. – URL: <https://tass.ru/obshchestvo/22506821> (дата обращения: 28.03.2025).

8. Топ-10 актуальных схем мошенников. – Текст : электронный // Сбербанк. – URL: <https://www.sberbank.ru/ru/person/kibrary/articles/top-10-aktualnykh-skhem-moshennichestva> (дата обращения: 11.07.2025).

9. Эксперты рассказали, кто чаще всего становится жертвой онлайн-любовников. – Текст : электронный // Москва 24. – URL: https://www.m24.ru/articles/obshchestvo/25112020/157421?utm_source=CopyBuf (дата обращения: 25.02.2025).

10. The Practical Guide for Requesting Electronic Evidence across Borders. – Text : electronic // United Nations Office on Drugs and Crime. – URL: <https://sherloc.unodc.org/cld/ru/st/evidence/practical-guide.html> (accessed on: 25.06.2025).

Научное издание

Нугаева Эльвира Дамировна
(кандидат юридических наук, доцент)
Харисова Зарина Ирековна
(кандидат технических наук, доцент)
Евдокимова Ольга Владимировна
(б/с, б/з)

**ОРГАНИЗАЦИЯ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ
ДИСТАНЦИОННЫХ МОШЕННИЧЕСТВ, СОВЕРШАЕМЫХ
С ИСПОЛЬЗОВАНИЕМ ИНТЕРНЕТ-СЕРВИСОВ**

Научно-практическое пособие

Редактор *Ю. Р. Исмаилова*

Подписано в печать 19.03.2026

Гарнитура Times

Уч.-изд. л. 5,8

Тираж 65 экз.

Выход в свет 30.03.2026

Формат 60×90 1/16

Усл. печ. л. 6

Заказ № 20

*Редакционно-издательский отдел
Уфимского юридического института МВД России
450103, г. Уфа, ул. Муксинова, 2*

*Отпечатано в группе полиграфической и оперативной печати
Уфимского юридического института МВД России
450103, г. Уфа, ул. Муксинова, 2*