МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Кафедра криминалистики

ДИПЛОМНАЯ РАБОТА

на тему **«ОСОБЕННОСТИ РАССЛЕДОВАНИЯ КОРЫСТНЫХ ПРЕСТУПЛЕНИЙ СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ (ПО МАТЕРИАЛАМ ТЕРРИТОРИАЛЬНОГО ОРГАНА)»**

Выполнил
Аглетдинова Диана Ильдаровна
обучающаяся по специальности
40.05.01 Правовое обеспечение
национальной безопасности
2020 года набора, 012 учебного взвода

Руководитель
начальник кафедры,
кандидат юридических наук, доцент
Нугаева Эльвира Дамировна

К защите _____
рекомендуется / не рекомендуется
Начальник кафедры _____ Э.Д. Нугаева
подпись
Дата защиты «___» _____ 2025 г. Оценка _____

ПЛАН

ВВЕДЕНИЕ

Согласно данным характеристики состояния преступности в Российской Федерации за январь-декабрь 2024 года зафиксировано увеличение числа преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий (+13,1%, всего – 765,4 тыс.). В общем числе зарегистрированных преступлений их удельный вес увеличился с 34,8% в январе-декабре 2023 года до 40,0%. Почти две трети таких преступлений (63,5%) совершается путем кражи или мошенничества: 486,3 тыс. (+2,3%)[1].

Анализ юридической литературы и эмпирического материала по теме исследования позволил сделать вывод, что сложности при раскрытии и расследовании корыстных преступлений, совершенных с использованием информационно-телекоммуникационных технологий (далее – ИТТ), возникают в вопросах квалификации преступлений и разграничении по со смежными составами, проведении отдельных следственных действий, что в конечном итоге сказывается на эффективности расследования органами предварительного расследования в целом.

Актуальность проведенного исследования заключается в объективной необходимости получения системы научных знаний о структуре и особенностях криминалистической характеристики корыстных преступлений совершенных с использованием ИТТ, выявлению проблем, связанных с раскрытием изучаемого вида преступлений, выработке методических рекомендаций по раскрытию и расследованию рассматриваемых составов преступлений.

Цель исследования – изучение механизма совершения краж и мошенничеств, совершенных с использованием ИТТ, предусмотренных п. «г» ч. 3 ст. 158 и ст. 159.3 (далее – УК РФ), определение эффективных средств,

---

[1] Состояние преступности в России за январь – декабрь 2024 года Министерство Внутренних Дел Российской Федерации / ФКУ «Главный информационно-аналитический центр». URL: https://мвд.рф/reports/item/60248328/ (дата обращения: 26.01.2025).

приемов и методов расследования преступлений, по рассматриваемой категории дел.

В соответствии с целью поставлены к решению следующие задачи.

– изучить и обобщить нормативную базу, криминалистическую и специальную литературу, эмпирический материал, по раскрытию и расследованию преступлений, совершенных с использованием ИТТ;

– проанализировать криминалистическую характеристику корыстных преступлений, совершенных с использованием ИТТ и определить наиболее значимые особенности;

– выявить, исследовать проблемы организации расследования указанных видов преступлений при взаимодействии следователя с органами дознания и другими участниками раскрытия и расследования преступлений;

– обобщая теоретические и практические знания проанализировать наиболее оптимальную тактику производства отдельных следственных действий, осуществляемых при расследовании изучаемой категории дел.

Объектом исследования является корыстная преступная деятельность, совершаемая с использованием ИТТ, а также деятельность сотрудников правоохранительных органов по раскрытию и расследованию преступлений рассматриваемой категории.

Предметом исследования является закономерности осуществления преступных посягательств при совершении корыстных преступлений совершенных с использованием ИТТ, а также конкретные существенные особенности методики и тактики расследования указанных преступлений.

Методология исследования включает в себя анализ нормативно-правовых актов, научной литературы по теме исследования и статистических данных и эмпирического материала.

Структура дипломной работы включает в себя введение, основную часть, состоящую из трех глав, каждая из которых разделена на параграфы, заключение и список использованной литературы.

ГЛАВА 1. УГОЛОВНО-ПРАВОВОЕ РАЗЪЯСНЕНИЕ И КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА КОРЫСТНЫХ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

§1. Уголовно-правовое разъяснение корыстных преступлений, совершенных с использованием информационно-телекоммуникационных технологий

Новые технологии все прочнее входят в нашу повседневную жизнь, уже большое количество простых и сложных процессов автоматизировано и с каждым дне их число растет. Однако с ростом количества пользователей электронных счетов и платежных средств растет и количество корыстных преступлений совершенных с использованием ИТТ в их отношении. Актуальность и распространенность данной группы правонарушений привела к законодательному закреплению в УК РФ различных составов корыстных преступлений в зависимости от способа их совершения.

Согласно п. «г» ч. 3 ст. 158 УК РФ уголовно-наказуемым деянием является кража, совершенная с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного статьей 159.3 УК РФ). Под этой формулировкой, согласно Постановлению Пленума Верховного Суда РФ от 27.12.2002 № 29 понимается тайное изъятие денежных средств с банковского счета или электронных денежных средств, например, если безналичные расчеты или снятие наличных денежных средств через банкомат были осуществлены с использованием чужой или поддельной платежной карты.

Также по п. «г» ч. 3 ст. 158 УК РФ квалифицируются действия лица и в том случае, когда оно тайно похитило денежные средства с банковского счета или электронные денежные средства, использовав необходимую для получения доступа к ним конфиденциальную информацию владельца денежных средств

(например, персональные данные владельца, данные платежной карты, контрольную информацию, пароли)[1].

В данном случае важным является факт тайного хищения денежных средств с банковского счета или электронных денежных средств, а также тайного хищения самой банковской карты или данных о банковской карте, с помощью которых будет произведен перевод денежных средств или их снятие с помощью банкомата.

По данному составу преступления могут квалифицироваться различные варианты поведения преступников. К ним в том числе относятся:

1. Хищение денежных средств со счетов банковских карт, сопряженное с использованием подлинной банковской карты потерпевшего, которая была украдена или случайно найдена на улице или в общественном месте, но по каким-то причинам не заблокирована владельцем;

2. Хищение денежных средств со счетов банковских карт, сопряженное с использованием поддельной банковской карты, содержащей информацию о номере отделения банка, выдавшего карту, номере карты, дате окончания действия карты и сведения о ее владельце, например если эти данные были считаны с помощью специальных электронных устройств (скиммеров), установленных на банкоматах и замаскированных под его детали[2].

Рассмотрим статью 159.3 УК РФ «Мошенничество с использованием электронных средств платежа», под которыми исходя из Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе»[3] понимаются средства и (или) способы, позволяющие клиенту оператора по переводу

---

[1] Постановление Пленума Верховного Суда РФ от 27.12.2002 № 29 (ред. от 15.12.2022) «О судебной практике по делам о краже, грабеже и разбое» / Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru (дата обращения: 17.09.2024).

[2] Попова Т. В. Способы и преступные схемы хищений денежных средств с лицевых счетов банковских карт граждан // Академическая мысль. 2018. №2 (3). URL: https://cyberleninka.ru/article/n/sposoby-i-prestupnye-shemy-hischeniy-denezhnyh-sredstv-s-litsevyh-schetov-bankovskih-kart-grazhdan (дата обращения: 17.09.2024).

[3] Федеральный закон от 27.06.2011 № 161-ФЗ (ред. от 08.08.2024) «О национальной платежной системе» / Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru (дата обращения: 17.09.2024).

денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с ИТТ, электронных носителей информации, в том числе платежных карт, а также иных технических устройств).

По данному составу преступлений следует квалифицировать действия лица, содержащие в себе обман или злоупотребление доверием потерпевшего с целью хищения у него банковской карты либо ее реквизитов или получение доступа к информационно-телекоммуникационным системам, позволяющим осуществлять перевод денежных средств в рамках применяемых форм безналичных расчетов (например, к личному кабинету в «Мобильном банке»). К ним относятся распространенные дистанционные мошенничества, использующие методы социальной инженерии, при которых преступники под видом сотрудников различных служб (банков, полиции и т. д.) связываются с гражданами и просят сообщить реквизиты банковской карты или код доступа к банковскому счету через «Мобильный банк».

Разграничение данных преступлений вызывает немало споров среди правоведов и в правоприменительной практике[1], в том числе о том, является ли обманом и введением в заблуждение оплата различных товаров похищенной у потерпевшего банковской картой. В таком толковании уголовного законодательства данные действия квалифицируются как мошенничество с использованием электронных средств платежа. Однако более распространенной является точка зрения, согласно которой мошенничеством может признаваться только обман или злоупотребление доверием в отношении потерпевшего, а не третьих лиц, поэтому квалификация данного деяния будет проходить по ч. 3 ст. 158 УК РФ.[2]

---

[1] Адмиралова Е. А. Проблемы отграничения преступлений, предусмотренных ст. 159.3 УК РФ и п. «г» ч. 3 ст. 158 УК РФ // E-Scio. 2022. №7 (70). URL: https://cyberleninka.ru/article/n/problemy-otgranicheniya-prestupleniy-predusmotrennyh-st-159-3-uk-i-p-g-ch-3-st-158-uk (дата обращения: 17.09.2024).

[2] Рогова Е. В. Корыстная преступность в условиях информационной глобализации // Вестник Казанского юридического института МВД России. 2022. №2 (48). URL: https://cyberleninka.ru/article/n/korystnaya-prestupnost-v-usloviyah-informatsionnoy-globalizatsii (дата обращения: 21.04.2025).

Верховный суд Российской Федерации в своем определении от 29.09.2020 г.[1] установил единообразное понимание судебной практики по обозначенным вопросам квалификации, в частности, определив, что хищение денежных средств путем бесконтактной оплаты товаров банковской картой, не принадлежащей виновному лицу, подлежит квалификации по п. «г» ч. 3 ст. 158 УК РФ[2].

Развитие в настоящее время новых способов совершения корыстных преступлений, использующих ИТТ приводит к необходимости постоянного мониторинга криминологической обстановки, проведения регулярного анализа оперативной обстановки по линии данных преступлений и своевременного внесения изменений в законодательство и выработке разъяснений, направленных на верную квалификацию судами преступлений.

Таким образом, в ходе рассмотрения составов корыстных преступлений, совершенных с использованием ИТТ, предусмотренных российским законодательством, мы пришли к выводу о существовании некоторых трудностей в их квалификации. В связи с этим следователям необходимо уделять особое внимание верной квалификации данной категории преступлений на этапе доследственной проверки. Кроме того, затрудняет разграничение схожих составов отсутствие более подробных разъяснений в Постановлениях Пленума Верховного Суда РФ от 30.11.2017 № 48 и от 27.12.2002 № 29. Тем не менее, уголовно-правовое законодательство совершенствуется и по возможности охватывает все возможные способы совершения хищения чужого имущества с использованием ИТТ.

---

[1] Савченко М. М. Квалификационные ошибки применения ст. 159.3 и п. «г» ч. 3 ст. 158 Уголовного Кодекса РФ // Право и практика. 2022. №3. URL: https://cyberleninka.ru/article/n/kvalifikatsionnye-oshibki-primeneniya-st-159-3-i-p-g-ch-3-st-158-ugolovnogo-kodeksa-rf (дата обращения: 17.09.2024).

[2] Адмиралова Е. А. Проблемы отграничения преступлений, предусмотренных ст. 159.3 УК РФ и п. «г» ч. 3 ст. 158 УК РФ // E-Scio. 2022. №7 (70). URL: https://cyberleninka.ru/article/n/problemy-otgranicheniya-prestupleniy-predusmotrennyh-st-159-3-uk-i-p-g-ch-3-st-158-uk (дата обращения: 17.09.2024).

§2. Особенности криминалистической характеристики корыстных преступлений, совершенных с использованием информационно-телекоммуникационных технологий

Несмотря на то, что в российском законодательстве существуют нормы, регулирующие уголовную ответственность корыстных преступлений совершенных с использованием ИТТ, особенности их расследования все еще затруднительно вследствие их специфических особенностей. Многие исследователи отмечают отсутствие методических рекомендаций, которые бы позволили увеличить эффективность деятельности правоохранительных органов по раскрытию и расследованию рассматриваемых общественно опасных деяний[1].

К общим особенностям, характеризующим рассматриваемую категорию преступлений, относятся:

1) дистанционное совершение преступлений – в большинстве случаев рассматриваемые деяния осуществляются дистанционно, то есть на расстоянии, без непосредственного контакта между преступником и потерпевшим. Это также приводит к невозможности изъятия и исследования дактилоскопических, трасологических, идеальных и других типичных следов;

2) трансграничный характер данных преступлений, также связанный с дистанционным способом, выражается в возможности преступников находится за пределами территории Российской Федерации или любой другой страны во время совершения преступления в отношении граждан РФ. Данный фактор связан с глобализацией сети «Интернет» и использованием злоумышленниками различных маршрутизаторов трафика, препятствующих установлению их местонахождения.

---

[1] Теткин Д. В. Некоторые особенности раскрытия и расследования киберпреступлений в современном мире глобальной цифровизации / Теткин Д. В., Пудовкин А. А., Троицкий А. А. // Право: история и современность. 2022. №2. URL: https://cyberleninka.ru/article/n/nekotorye-osobennosti-raskrytiya-i-rassledovaniya-kiberprestupleniy-v-sovremennom-mire-globalnoy-tsifrovizatsii (дата обращения: 17.09.2024).

3) множество эпизодов преступной деятельности, совершаемых одним лицом до тех пор, пока оно не будет задержано и привлечено к уголовной ответственности, как правило, это обусловлено спецификой используемых способов совершения преступлений и личностью преступника;

4) динамичность способов совершения преступлений заключается в постоянном обновлении схем совершения хищений денежных средств с электронных кошельков. Преступники активно используют различные легенды для введения в заблуждение граждан в преступных целях, а также применяют стремительно развивающиеся ИТТ;

5) сложность в предупреждении и предотвращении преступлений. Несмотря на активную работу по профилактике корыстных преступлений, совершаемых с помощью ИТТ, которая проходит в форме просвещения населения, их количество продолжает расти, в связи с чем можно сделать вывод о необходимости разработки новых методов предотвращения данной категории преступлений[1].

Одним из ключевых факторов при расследовании любых видов преступлений является понимание их криминалистической характеристики, в связи с этим предлагаем рассмотреть ее подробнее.

Криминалистическая характеристика представляет собой наиболее значимые признаки и свойства расследуемого преступного деяния. Существует множество подходов к определению перечня элементов криминалистической характеристики, однако большинство исследователей сходятся на следующих составляющих:

а) личность преступника и потерпевшего;

б) способ совершения преступления;

в) механизм следообразования;

---

[1] Гоголев С. А. Проблемы выявления и расследования киберпреступлений // Скиф. 2021. №11(63). URL: https://cyberleninka.ru/article/n/problemy-vyyavleniya-i-rassledovaniya-kiberprestupleniy (дата обращения: 17.09.2024).

г) обстановка, при которой совершено преступление[1].

Данную точку зрения мы разделяем полностью. Начнем с рассмотрения личности преступника и его типичных особенностей. Одной из таковых является наличие у правонарушителя доступа к информационным системам и технологиям, а также к информационно-телекоммуникационной сети, например «Интернет» или какой-либо локальной сети, с помощью которых преступник совершает преступление. Статистические данные характеризуют личность преступника по рассматриваемой категории дел следующим образом: в 90 % случаев преступником является мужчина, ранее не судимый (более 95 % от общего количества преступников), проживающий в городском населенном пункте, имеющий временную или постоянную регистрацию. Преобладающий возраст – от 16 до 35 лет, причем исследователи отмечают «омоложение»: так, 10 % преступников, совершающих рассматриваемые преступления, в мире – это несовершеннолетние возрасте от 14 до 15 лет, а 90 % преступлений с использованием ИТТ совершается людьми в возрасте до 20 лет[2]. Организаторы преступной группы не редко уже привлекались к уголовной ответственности за аналогичные преступления, в то время как большинство соучастников ранее не судимы. Среди преступников преобладают люди, имеющие высшее или неоконченное высшее образование, зачастую специальность техническая или связанная с компьютерными технологиями, однако среди рядовых исполнителей, которые занимаются, например, снятием или перевозкой похищенных денежных средств, преобладают лица со средним общим или специальным образованием. Семейное положение преступников различно и не показывает какой-либо значительной корреляции.

---

[1] Ищенко П. П. Нужна ли криминалистическая характеристика преступления в криминалистической методике? // Lex Russica. 2020. №3 (160). URL: https://cyberleninka.ru/article/n/nuzhna-li-kriminalisticheskaya-harakteristika-prestupleniya-v-kriminalisticheskoy-metodike (дата обращения: 17.09.2024).

[2] Глазатова С. В. Киберпреступления, совершаемые несовершеннолетними: проблемы расследования // Российский следователь. 2021. № 2. URL: https://elibrary.ru/item.asp?id=44683421 (дата обращения: 17.09.2024).

Психологический портрет лиц, совершающих корыстные преступления с использованием ИТТ включает в себя такие характеристики как высокий уровень интеллекта, завышенная самооценка и чувство собственного превосходства, манипулятивность и умение искусно лгать, им также присуще тщательное планирование, стремление оставаться анонимными и страх перед привлечением к уголовной ответственности, что вынуждает их более тщательно скрывать следы преступления.

Так, гр. У., являющийся одним из соучастников мошенничества в особо крупном размере, уголовная ответственность за которое предусмотрена ч. 4 ст. 159 УК РФ, совместно с соучастниками ввели в заблуждение потерпевшего гр. Б путем осуществления на его мобильный телефон звонков и отправления сообщений, представляясь руководством потерпевшего, сотрудниками ФСБ России и сотрудниками Центрального банка России. Потерпевший по указанию преступников снял со своего банковского счета наличные денежные средства в размере 3 млн. руб. и передал преступникам[1].

Социально-демографическая характеристика личности обвиняемого в данном преступлении гр. У. следующая – это мужчина, 28 лет, среднее-профессиональное образование, имеющий постоянную регистрацию, официально не трудоустроен, ранее не судим.

Наряду с рассмотренными криминалистическими характеристиками личности преступника для полного исследования необходимо также рассмотреть наиболее характерные черты потерпевшего.

Анализ статистики за 2024 год показал, что по половому критерию жертвы мошенничества, совершенного с использованием ИИТ распределились следующим образом: мужчины 9275 или 46,9%, женщины –10 466 или 53,1%.

В исследуемый период жертвами рассматриваемой категории преступления были учтены несовершеннолетних 194 человека или 1,0 %,

---

[1] Ганиева И. А. Личность преступника, совершающего дистанционное мошенничество // Актуальные вопросы борьбы с преступлениями. 2023. №5. URL: https://cyberleninka.ru/article/n/lichnost-prestupnika-sovershayuschego-distantsionnoe-moshennichestvo (дата обращения: 21.04.2025).

представителей молодежи (18-29 лет) 4351 человек или 22,0%; лиц зрелого возраста 9463 (30-49 лет) или 48,0%, лиц старшего и пожилого возраста (50 лет и старше) по 2866 человек или по 14,5%[1].

Основной причиной, по которой люди становятся жертвами данной категории преступлений является неграмотность пользователей, так как они зачастую самостоятельно сообщают информацию, необходимую для доступа к их денежным средствам. Например, жертвы предоставляют свои данные, когда кто-либо звонит и представляется служащим банка или администратором, при этом не проверяя их личность[2]. Преступники, кроме того, умышленно оказывают психологическое давление на потерпевших с целью вызвать у них панику. Как правило, они настаивают, что денежные средства с их счетов прямо сейчас будут списаны или уже списываются. Они могут утверждать, что с близкими потерпевших что-то случилось и им нужна срочная финансовая помощь.

Таким образом при исследовании механизмов совершения преступления можно обнаружить, что немаловажным фактором выступает бдительность потерпевшего и его осведомленность о способах совершения рассматриваемых преступлений. Чем выше осведомлённость населения, тем меньше должно быть преступлений в этой сфере. Самыми незащищенными группами по-прежнему остаются пенсионеры и пожилые люди. В связи с чем необходимо проводить как можно больше профилактической работы конкретно с этой группой населения и с гражданами в целом[3].

---

[1] Кабанов П. А. Жертвы кибермошенничества как один из объектов современной кибервиктимологии: краткий статистический анализ показателей криминальной виктимности 2023–2024 гг. // Виктимология. 2023. №1. URL: https://www.researchgate.net/publication/369559945_Kabanov_P_A_Zertvy_kibermosennicestva_kak_odin_iz_obektov_sovremennoj_kiberviktimologii_kratkij_statisticeskij_analiz_pokazatelej_kriminalnoj_viktimnosti_2023-2024 (дата обращения: 17.09.2024).

[2] Ткачева Н. В., Серова Е. Н. Виктимология и киберпреступность в России // Вестник ЮУрГУ. Серия: Право. 2021. №3. URL: https://cyberleninka.ru/article/n/viktimologiya-i-kiberprestupnost-v-rossii (дата обращения: 17.09.2024).

[3] Стяжкина С. А. Виктимологическая профилактика кибермошенничества // Вестник Удмуртского университета. Серия «Экономика и право». 2022. №3. URL: https://cyberleninka.ru/article/n/viktimologicheskaya-profilaktika-kibermoshennichestva (дата обращения: 17.09.2024).

Одними из ключевых элементов криминалистической характеристики является способ совершения преступления, который включает в себя действия по подготовке, совершению и сокрытию преступления, а также механизм следообразования, позволяющий обнаружить причинно-следственную связь между действиями преступника и их последствиями.

Как правило преступления рассматриваемой категории осуществляются полноструктурным способом, т. е. помимо действий по непосредственному совершению преступлений включает в себя подготовку и сокрытие следов преступления. К подготовке в рассматриваемом случае может относится:

1. Поиск средств и капитала для создание материально-технической базы и привлечения других соучастников.

Стоит обратить внимание, что совершение корыстных преступлений с использованием ИТТ возможно только при тщательной и планомерной подготовке и требует немалых затрат. Исходя из этого можно предположить, что занятие рассматриваемой категорией преступлений может быть привлекательно для организованных преступных сообществ, уже занимающихся совершением противоправной и преступной деятельностью.

2. Привлечение соучастников, создание организованной группы и распределение ролей.

Совершение корыстных преступлений с использованием ИТТ, как правило происходит группой лиц по предварительному сговору, организованной группой или даже преступным сообществом, деятельность которых направлена на получение прибыли. Так как рассматриваемая категория в настоящее время является распространенным видом преступления, а уголовное преследование осложнено дистанционностью способа совершения, небольшим количеством следов и технической сложностью, поиск соучастников для организаторов группы не представляет особых трудностей.

Как правило в состав такой группы входят, помимо организатора, один или несколько человек, обладающие знаниями в области применения ИТТ, которые занимаются непосредственно техническим обеспечением процесса (настройка

используемых технических средств, создание и использование специального программного обеспечения, получение и использование конфиденциальных данных для вывода денежных средств на другие банковские счета, при необходимости удаление данных с электронных носителей информации и других цифровых следов).

Помимо них, как правило в группе участвуют лица, контактирующие с потерпевшим для получения от него информации, необходимой для доступа к денежным средствам (собирание и анализ информации о потерпевшем, осуществление телефонных звонков, в ходе которых с применением методов социальной инженерии выясняются важные сведения или внушается необходимость перевести или отдать денежные средства преступникам). Зачастую такие соучастники хорошо разбираются в психологии людей и могут воздействовать на потерпевшего, использовать его служебное положение, угрожать несуществующими в действительности компрометирующими сведениями, давить на жалость и т.д.)

Зачастую при совершении преступления привлекаются так называемые «дропперы» - лица, которые используются для сокрытия и запутывания следов банковских операций с похищенными денежными средствами.

Выделяют различные виды «дропперов», среди которых лица, получающие наличные денежные средства и кладущие их на условленный банковский счет, лица чьи банковские счета и карты используются для проведения промежуточных операций с похищенными деньгами и лиц, которые снимают денежные средства с счета и передают их организаторам.

Нередко встречается в современной практике, когда «дропперы» не знают, что участвуют в преступлении и выполняли указанные действия под различными предлогами за небольшое (относительно похищенных денежных средств) вознаграждение.

К указанным участникам могут добавляться и другие участники по мере расширения преступной деятельности.

3. Создание необходимых условий для деятельности соучастников преступления.

Если для совершения корыстных преступлений, с использованием ИТТ, организатору необходимо привлечение большого количества лиц, которые будут, например, совершать звонки потерпевшим или пытаться войти в систему мобильного банка от имени потерпевшего. то одним из этапов подготовки будет являться в том числе поиск и аренда помещений, их обустройство и обеспечение соответствующей техникой.

4. Поиск и покупка подходящего оборудования.

Использование ИТТ является обязательным элементом объективной стороны рассматриваемых преступлений, исходя из чего нельзя переоценить важность оборудования для преступников. Как правило, лицо, отвечающее за техническую сторону совершения преступления, самостоятельно занимается подбором и настройкой необходимой технической аппаратуры, так как обладает соответствующими знаниями и навыками. Если выбранная схема совершения преступления является сложной по методам и организации, то необходимое оборудование докупается.

5. Создание или приобретение соответствующего программного обеспечения.

В случае, когда для совершения преступления необходимо использовать специальное программное обеспечение (например, подставной сайт или вредоносную программу) оно может создаваться участниками группы, которые обладают соответствующими навыками программирования, но также преступники могут приобрести его, например, в Даркнете или через знакомых, не раскрывая целей его дальнейшего применения. Кроме того, сюда относится поиск и приобретение возможности использовать легальное программное обеспечение, например искусственный интеллект, генерирующий голос или изображение близких потерпевшего или VPN-сервисы. В таком случае в качестве приготовления следует также понимать покупку дополнительных подписок, улучшающих работу указанных приложений и т.д.

6. Получение персональных данных о потерпевшем и его близких из открытых источников или другими способами.

При необходимости в ходе совершения преступления взаимодействовать с потерпевшим и различными способами оказывать на него давление, как правило лица, роль которых как раз состоит в таком взаимодействии, собирают и анализируют как можно больше доступной информации о потерпевшем, его близких и родственниках, его имуществе и денежных средствах на банковских счетах с целью использования данной информации для составления правдоподобной легенды и манипулирования с целью хищения денежных средств.

Одним из самых распространенных способов совершения корыстных преступлений с использованием ИТТ является «фишинг». Фишинг может иметь различные формы, но в конечном счете, он всегда направлен на манипуляции человеком с целью получения от него каких-либо данных, либо доступа к денежным средствам, хранящимся на электронном кошельке. В настоящее время злоумышленниками часто используется такой подвид как «вишинг», главным отличием которого является то, что преступник звонит на сотовый телефон потерпевшему и с использованием методов социальной инженерии и различного рода предлогов просит сообщить ему информацию, которая в последующем используется для хищения денежных средств с электронного банковского счета данного гражданина.

Основные характеристики фишинговой атаки:

– использование электронной почты, сотовой связи, мессенджеров и т.д.

– получение конфиденциальной информации;

– использование социальной инженерии.

В последние годы развитие технологий искусственного интеллекта приводит к тому, что они становятся доступны каждому, в том числе их могут использовать преступники для обмана потерпевшего при мошенничестве. В частности, с помощью искусственного интеллекта они могут на основе уже имеющихся аудиофайлов с голосовыми сообщениями потерпевшего создать

аналогичное только с просьбой о помощи, голос и манера речи при этом будет почти неотличима для простого гражданина от настоящего голоса потерпевшего. Аналогичным способом преступники могут создать видеофайл с изображением потерпевшего, материалы для таких файлов, как правило, есть в аккаунтах в социальных сетях и мессенджерах потерпевших.

Люди, которым приходят такие правдоподобные просьбы о помощи, сложно не поверить в то, что это действительно их близкий человек нуждается в помощи, это приводит к тому, что они выполняют все требованиях преступников и переводят денежные средства.

К действиям по сокрытию следов преступления относится в данном случае будет относится противодействие по обнаружению цифровых следов и вывод денежных средств через сторонние банковские счета.

К мерам по сокрытию цифровых следов будут относится такие действия как удаление переписки с потерпевшим, использование VPN-технологий и прокси-серверов. приобретение и использование одноразовых телефонных номеров, создание одноразовых почтовых ящиков и т.д.

Для вывода денежных средств, как правило используется заранее приготовленная схема, включающая несколько банковских счетов, которые зачастую принадлежат лицам, не имеющим отношения к расследуемому преступления, потерявшим или продавшим свои банковские карты с привязанными к ним счетами. Проводя денежные средства по цепочке через несколько сторонних счетов, преступники преследуют цель предотвращения их утери в случае, если на банковский счет в ходе предварительного расследования судом будет наложен арест.

Все операции, которые предполагают личное участие в зачислении или снятии наличных денежных средств с банковских счетов через банкоматы, почти всегда осуществляют специальные лица, «дроппы», которые были упомянуты и описаны ранее.

Механизм следообразования и его характерные черты. Одной из особенностей криминалистической характеристики данного состава

преступлений является наличие не только материальных и идеальных следов, оставляемых преступником, но и виртуального следа, который фиксируется ИТТ при вмешательстве в их работу. Однако большинство злоумышленников также знают о таком аспекте своей деятельности, что отражается в их поведении: они зачастую принимают активные меры по противодействию раскрытия и расследования преступления посредством уничтожения компьютерных следов. В преступных группах могут присутствовать даже специальные лица, которые работают именно над сокрытием преступных компьютерных следов. Преступники, как правило, используют средства и технологии, которые применяются и в других преступлениях совершаемых с использованием ИТТ, в том числе программное обеспечение для гарантии собственной анонимности с помощью VPN-технологии или средства для уничтожения цифрового следа присутствия на компьютере жертвы.

К материальным следам, которые можно обнаружить при расследовании рассматриваемой категории преступлений относятся:

– кассовые чеки, платежные поручения, находящиеся у потерпевшего и подтверждающие факт внесения им денежных средств на электронный банковский счет;

– фальшивые документы, направляемые потерпевшему в целях ввести его в заблуждение (судебные извещения и т.д.);

– дактилоскопические следы на компьютерном оборудовании, мобильных устройствах и SIM-картах, изъятых при обыске преступников или в их жилище;

К идеальным следам можно отнести:

– показания свидетелей – очевидцев снятия средств с электронного счета. Как правило, такими свидетелями являются сотрудники банка.

– показания свидетелей, которые помогали снимать денежные средства, перевозить их, не причастных к совершению преступления.

Электронно-цифровые следы:

– сведения о соединениях между абонентами и абонентскими устройствами потерпевшего и преступника, а также преступников между собой, если они действовали в группе;

– сведения, отражающие информацию о том, когда, сколько и на какой счет были внесены потерпевшим денежные средства, а также на какие счета они были переведены в дальнейшем, в случае если они были сняты с банкомата, то когда, кем и где;

– переписки в социальных сетях, мессенджерах между потерпевшим и преступником, а также между преступниками, если они действовали в группе;

– записи с камер видеонаблюдения, если они могли зафиксировать преступника и т.д.

При расследовании преступлений рассматриваемой категории особое внимание уделяется поиску и изъятию электронно-цифровых следов, однако нельзя также упускать наличие других материальных и идеальных следов, не менее значимых для установления истины по уголовному делу. Как правило большинство дактилоскопических и потожировых следов, имеющих значение для расследования, находятся на орудии преступления, которым в данном случае выступает персональный компьютер преступника или другая компьютерная аппаратура. Изъятие отпечатков пальцев необходимо для доказывания принадлежности устройства конкретному владельцу.

Обстановка совершения преступления. При выявлении и расследовании корыстных преступлений совершенных с использованием ИТТ вызывает сложность установление места совершения преступления. Вследствие дистанционного характера совершения рассматриваемых деяний 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 последствий.

Типичными местами совершения данной категории преступлений 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 (мобильном телефоне, персональном компьютере и т. д.), либо виртуальных следов преступления (например, информация о посещаемых интернет-сайтах).

Таким образом, нами были рассмотрены наиболее важные особенности расследования корыстных преступлений совершенных с использованием ИТТ, а также подробно описаны основные элементы криминалистической характеристики, которые могут быть использованы в раскрытии и расследовании преступления в установлении источников доказательственной информации путем анализа коррелирующих элементов криминалистической характеристики, выдвижении следственных версий и их анализе, планировании проведения следственных действий и оперативно-розыскных мероприятий и т.д.

ГЛАВА 2. ОСОБЕННОСТИ ОРГАНИЗАЦИИ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ КОРЫСТНЫХ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

§1. Взаимодействие следователя с органами дознания и другими участниками раскрытия и расследования преступлений

На доктринальном уровне подчеркивается, что под взаимодействием следователя с другими органами, осуществляющими содействие в раскрытии преступлений понимается основанная на законодательстве, планируемая, согласованная по целям, месту и времени совместная деятельность автономных по отношению друг к другу органов, обеспечивающих эффективную расстановку сил, комплексное использование методов и средств, направленную на решение задач уголовного судопроизводства, при руководящей и организующей роли следователя и четком разграничении компетенции участников сотрудничества[1].

Формы взаимодействия следователя как субъекта уголовно-процессуальной деятельности в расследовании корыстных преступлений, совершенных с использованием ИТТ, существенно не отличается от общеуголовных преступлений, главным нормативно-правовым актом регламентирующим данную деятельность является приказ МВД России от 21.07.2017 года №495дсп «Инструкция по организации взаимодействия подразделений и служб органов внутренних дел в расследовании и раскрытии преступлений» и приказ от 22.07.2020 года № 478 МВД по Республике Башкортостан, которым был утвержден Алгоритм взаимодействия

[1] Куликова И. Е. Некоторые вопросы взаимодействия следователя с оперативными работниками при раскрытии и расследовании мошенничеств // Криминалистика: вчера, сегодня, завтра. 2022. №2. URL: https://cyberleninka.ru/article/n/nekotorye-voprosy-vzaimodeystviya-sledovatelya-s-operativnymi-rabotnikami-pri-raskrytii-i-rassledovanii-moshennichestv (дата обращения: 17.09.2024).

территориальных ОВД Республики Башкортостан при раскрытии и расследовании уголовных дел по мошенничествам и хищениям, совершенным с использованием ИТТ[1].

При исследовании взаимодействия следователя с органом дознания ученые-криминалисты выделяют различные формы такого взаимодействия, наиболее полный перечень, по нашему мнению, приводит Куликова И.Е.:

1) совместная проверка следователем и оперативными сотрудниками сообщения о преступлении (ст. 144 УПК РФ);

2) вынесение следователем письменного поручения о проведении оперативно-розыскных мероприятий в стадии возбуждения уголовного дела;

3) привлечение должностного лица органа дознания к работе следственной группы;

4) привлечение должностного лица органа дознания к участию в производстве конкретного следственного действия;

5) установление органом дознания лица, подлежащего привлечению в качестве подозреваемого или обвиняемого;

6) розыск подозреваемого, обвиняемого, если местонахождение неизвестно органом дознания по поручению следователя (ч. 1 ст. 210 УПК РФ);

7) создание следственно-оперативный группы;

8) совместное планирование;

9) обмен информацией[2].

---

[1] Соколова Т. С. К вопросу взаимодействия органов предварительного следствия с органами дознания при проведении доследственной проверки по сообщениям о мошенничествах, совершенных с использованием информационно-телекоммуникационных технологий // Право и государство: теория и практика. 2023. №3 (219). URL: https://cyberleninka.ru/article/n/k-voprosu-vzaimodeystviya-organov-predvaritelnogo-sledstviya-s-organami-doznaniya-pri-provedenii-dosledstvennoy-proverki-po (дата обращения: 01.11.2024).

[2] Куликова И. Е. Некоторые вопросы взаимодействия следователя с оперативными работниками при раскрытии и расследовании мошенничеств // Криминалистика: вчера, сегодня, завтра. 2022. №2. URL: https://cyberleninka.ru/article/n/nekotorye-voprosy-vzaimodeystviya-sledovatelya-s-operativnymi-rabotnikami-pri-raskrytii-i-rassledovanii-moshennichestv (дата обращения: 11.01.2025).

Одной из ключевых проблем, с которыми сталкиваются следователи при раскрытии и расследовании мошенничеств, совершенных с использованием электронных средств платежа, является почти полное отсутствие криминалистически значимой информации, по которой можно было бы установить лицо, совершившее преступление. Это следует из особенностей дистанционного мошенничества, которое характеризуется в том числе отсутствием аудиовизуального контакта преступника с потерпевшим.

Во многом поэтому важно при расследовании данной категории преступлений правильно и грамотно изъять и исследовать «цифровые следы», которые могут остаться на электронных носителях потерпевшего и выяснить все обстоятельства произошедшего в мельчайших подробностях. Для этого необходимо установить взаимодействие со специалистом, обладающим техническими знаниями в данной области.

Важно грамотно осуществить организацию первоначального этапа расследования, который при этом является самым сложным и трудоемким. Во избежание допущения ошибок при производстве следственных действий необходимо с самого начала привлечь к расследованию специалиста в сфере компьютерной информации.

Наиболее часто необходимость в привлечении специалистов при расследовании корыстных преступлений, совершенных с использованием ИТТ возникает при проведении таких следственных действий как осмотр места происшествия, допросы подозреваемого, обвиняемого, а также обыски и выемки у подозреваемого, обвиняемого.

При выезде на осмотр места происшествия специалисты, входящие в состав следственно-оперативной группы, оказывают содействие по обнаружению, фиксации, изъятию цифровых следов, а также консультируют следователя по сложившейся следственной ситуации с учетом обнаруженных цифровых следов и предположительного способа совершения преступления. При осмотре места происшествия специалистом фиксируется такая криминалистически значимая информация как переписка преступника

с потерпевшим, данные об исходящих и входящих звонках, факты осуществления переводов через электронные средства платежа и информация о счетах, на которые были осуществлены эти переводы.

Изучение эмпирического материала по рассматриваемой категории дел показывает, что определенные трудности у следователей, особенно с небольшим опытом работы возникают при производстве следственного осмотра, как места происшествия в целом, так и отдельных изъятых предметов. В состав следственно оперативной группы при выезде на осмотр места происшествия рекомендуется включать специалиста, обладающего знаниями в сфере ИТТ для того, чтобы обеспечить правильную фиксацию, исследование и изъятие цифровых следов, которые удаться обнаружить.

Альтернативой привлечения штатных специалистов может являться привлечение в качестве специалистов людей, чье образование либо чья профессиональная деятельность связаны с информационно-коммуникационными технологиями, так как они в силу своих компетенций более осведомлены об особенностях работы тех или иных устройств и могут оказать серьезную ценную помощь при проведении следственных действий. Однако в таком случае следует обратить внимание на оплату труда привлекаемых лиц, обеспечения их необходимыми для работы условиями и по возможности современными техническими средствами.

Анализ оперативной и следственной практики при раскрытии и расследовании дистанционных мошенничеств показывает, что в большинстве случаев отмечается отсутствие необходимого количества специалистов компетентных в области информационно-телекоммуникационных технологий[1].

Наиболее эффективным с точки зрения получение криминалистически важной информации и цифровых следов в данном случае будет использование специалистом специальных программно-аппаратных комплексов («Мобильный

[1] Куликова И. Е. Организационные аспекты использования специальных знаний при раскрытии дистанционных мошенничеств // Пролог: журнал о праве. 2022. №4(36). URL: https://cyberleninka.ru/article/n/organizatsionnye-aspekty-ispolzovaniya-spetsialnyh-znaniy-pri-raskrytii-distantsionnyh-moshennichestv (дата обращения: 17.09.2024).

криминалист», UFED, Belkasoft evidence center и др.). Однако материально-техническая оснащенность территориальных органов не всегда подразумевает такую возможность, тем более значимым становится правильное изъятие различной техники (например, мобильных устройств, компьютеров и т.д.) и направление их на судебную компьютерно-техническую экспертизу.

Кроме того, особенности расследования корыстных преступлений, совершенных с использованием ИТТ предполагают организацию взаимодействия следственных подразделений с банковскими организациями, которые осуществляют финансово-кредитное обслуживание населения.

Как правило, потерпевшие под влияние мошенников переводят денежные средства со своих личных счетов или сообщают конфиденциальную информацию о реквизитах своих счетов, с помощью которой самим преступникам не составляет труда перевести все средства на свои счета. В связи с этим важно как можно более оперативнее получить информацию о счетах и операциях с ними, а также о том куда эти денежные средства переводились дальше, на чьих счетах аккумулировались и через какие банкоматы обналичивались.

Эти и другие предоставляемые банком сведения не только содержат криминалистически значимую информацию, которая ляжет в основу доказательств по уголовному делу, но и может помочь принять меры по обеспечению гражданского иска, конфискации имущества и иные имущественные взыскания в соответствии со ст. 160.1 Уголовно-процессуального кодекса РФ (далее – УПК РФ).

Вместе с тем следует помнить о взаимодействии с компаниями сотовой связи, в случаях, когда преступник звонил потерпевшему и убеждал путем применения социальной инженерии о необходимости совершения тех или иных действий в конечном итоге приводящих к хищению денежных средств со счетов гражданина. Операторы сотовой связи могут предоставить данные о пользователе абонентского номера, с которого осуществлялся звонок жертве мошенничества, и месте его нахождения, времени и длительности разговора,

что может помочь установить сведения о личности преступника, об обстановке совершения преступления и т.д.

Так, при изучении уголовного дела №123-672[1] можно отметить, что следователем были направлены запросы в АО «Национальная система платёжных карт», ПАО «Сбербанк» и ЗАО «Тинькофф Банк», где у потерпевшей Н. имелись открытые банковские счета. В запросах, помимо реквизитов, изложения обстоятельств уголовного дела и данных потерпевшей Н. содержалось указание о предоставить:

«Расширенную выписку по движению денежных средств по банковской карте № 5536 9137 XXXX XXXX ЗАО Тинькофф Банк (ПАО «Сбербанк») за период времени с 06.06.2023 по 10.06.2023 года с указанием суммы, способа, места, даты и времени их списания, полные номера счетов/банковских карт, электронных средств платежей отправителей и получателей денежных средств.

В указанном контексте напрашивается вопрос о возможности сокращения сроков предоставления необходимых сведений банковскими организациями и операторами сотовой связи. В настоящее время получение указанной информации в обоих случаях происходит только при наличии судебного решения, а ответ от организаций должен поступить в течении 10 рабочих дней момента получения соответствующего судебного решения. И, как показывает практика, за такой длительный срок преступники имеют возможность сокрыть следы преступления, осуществить большое количество транзакций и обналичить даже крупные суммы денег. В связи с этим считаем целесообразным упростить указанные процедуры и стремиться к улучшению взаимодействия правоохранительных органов с банковскими организациями и операторами сотовой связи в целях раскрытия и расследования преступлений.

Таким образом, при раскрытии и расследовании корыстных преступлений, совершенных с использованием ИТТ эффективность проводимых оперативно-розыскных мероприятий и следственных действий во многом зависит

[1] Архив Белорецкого районного суда. Уголовное дело № 123-672/2023.

от качества взаимодействия следственных органов в первую очередь со специалистами обладающими техническими знаниями в сфере ИТТ, а также с сотрудниками органа дознания, другими организациями, способствующими расследованию преступления путем предоставления необходимых сведений.

§2. Розыскная деятельность

В настоящее время в юридической литературе, учитывая отсутствие законодательного закрепления понятий розыск и розыскная деятельность существует множество подходов к определению данных терминов, одним из наиболее полных, по нашему мнению, является понятие, данное Буряковым Е.В. в его монографии, посвященной розыску:

«Розыскная деятельность – это базирующаяся на законах и подзаконных актах комплексная система организационных, профилактических, процессуальных, оперативно-розыскных и иных специальных мероприятий, осуществляемых органами внутренних дел, направленных на обеспечение розыска скрывшихся преступников, без вести пропавших лиц и других категорий разыскиваемых граждан, а также на выявление и устранение условий, способствующих длительному укрывательству (пребыванию) разыскиваемых преступников на обслуживаемой территории»[1].

При расследовании уголовных дел в большинстве случаев применяются розыскные меры, осуществление которых определяется в соответствии с тактикой розыскной деятельности.

Тактика розыскной деятельности – это выбор субъектом, осуществляющим розыскную деятельность, наиболее целесообразного в конкретной ситуации правомерного способа (приема) действий, направленного

---

[1] Буряков Е. В. Оперативно-розыскное учение о розыске: монография; Омск : ОмА МВД России, 2011. С. 60.

на обнаружение лиц и предметов, имеющих значение для расследования уголовного дела, с использованием разрешенных законом средств[1].

Тактической основой розыскной деятельности является розыскная версия, которая представляет собой обоснованной предположение об уже предпринятых и последующих действиях разыскиваемого лица, его местонахождении и возможностях, а также других значимых для розыска лица и расследования уголовного дела элементах.

Определяя направление розыска, версия играет роль фактора, детерминирующего поведение субъекта розыска, что составляет психологические основы розыска.

К обязанностям сотрудников уголовного розыска относятся:

– выявление причин, обусловливающих совершение IT-преступлений, а также их устранение в рамках имеющихся полномочий;

– выявление лиц и последующее применение необходимых мер к лицам, имеющим отношение или непосредственно занимающимся приготовлением или покушением на совершение преступлений с использованием ИТТ;

– взаимодействие с участковыми, в том числе в ходе реализации мероприятий по выявлению и предупреждению IT-преступлений, совершаемых лицами, которые раньше уже совершали подобные преступления и были судимы за это;

– участие в совместных комплексных мероприятиях оперативно-профилактической направленности;

– розыск лиц как совершивших, так и подозреваемых или обвиняемых в совершении IT-преступлений, а также лиц, скрывающихся от органов дознания, следствия или суда;

---

[1] Шляхова Ю. Д. Тактические основы розыскной деятельности следователя и оперативно-розыскной деятельности органов дознания // Colloquium-journal. 2022. №34 (157). URL: https://cyberleninka.ru/article/n/takticheskie-osnovy-rozysknoy-deyatelnosti-sledovatelya-i-operativno-rozysknoy-deyatelnosti-organov-doznaniya (дата обращения: 11.01.2025)

– осуществление оперативно-разыскных мероприятий в отношении лиц, представляющих оперативный интерес (например, тех, кто был осужден за совершение IT-преступлений, но при этом наказание не связано с лишением такого лица свободы)[1].

Рассмотрим особенности проведения розыска по рассматриваемой категории преступлений. Одной из основополагающих особенностей корыстных преступлений, совершаемых с использованием ИТТ состоит в том, что преступление, как правило, не связано границами одного региона. Всё это делает необходимым либо осуществление самостоятельных выездов следователя, в производстве которого находится уголовное дело, как правило, соединенное, на основании п. 2 и 3 ч. 1 ст. 153 УПК РФ, и оперативных работников, сопровождающих такое дело, либо направление соответствующих поручений об их производстве и проведении иным должностным лицам в порядке горизонтального ведомственного сотрудничества (ч. 1 ст. 152 УПК РФ)[2].

Для осуществления обмена информацией между подразделениями уголовного розыска на территории Российской Федерации о совершенных мошеннических действиях используется интегрированный банк данных «Дистанционное мошенничество» (далее – ИБД «Дистанционное мошенничество»). Такой программный комплекс позволяет анализировать информацию относительно номеров телефонов, банковских карт, банковских счетов, электронных кошельков, IMEI-номеров телефонов с целью выявления совпадений на региональном и межрегиональном уровнях. Использование такой

---

[1] Шхагапсоев З. Л. К вопросу о роли органов внутренних дел в предупреждении преступлений, совершаемых с использованием информационных технологий (IT-преступлений) // Государственная служба и кадры. 2020. №2. URL: https://cyberleninka.ru/article/n/k-voprosu-o-roli-organov-vnutrennih-del-v-preduprezhdenii-prestupleniy-sovershaemyh-s-ispolzovaniem-informatsionnyh-tehnologiy-it (дата обращения: 28.10.2024).

[2] Куликова И. Е. Некоторые вопросы взаимодействия следователя с оперативными работниками при раскрытии и расследовании мошенничеств // Криминалистика: вчера, сегодня, завтра. 2022. №2. URL: https://cyberleninka.ru/article/n/nekotorye-voprosy-vzaimodeystviya-sledovatelya-s-operativnymi-rabotnikami-pri-raskrytii-i-rassledovanii-moshennichestv (дата обращения: 11.01.2025).

базы позволяет облегчить процесс получения подразделениями уголовного розыска информации при выявлении совпадений номеров телефонов, банковских карт и других реквизитов, имеющихся в ней. Вместе с тем в практике имеется ряд проблем, снижающих эффективность использования ИБД «Дистанционное мошенничество» в целях выявления и раскрытия мошеннических действий.

Так, при изучении материалов уголовного дела №123-672, возбужденного по признакам состава преступления, предусмотренного ч. 3 ст. 159 УК РФ в рапорте о проделанной работе оперуполномоченного М. указано, что:

«По базе «ИБД-Ф» «Дистанционное мошенничество» по абонентским номерам, а также по банковской карте обнаружены совпадения, раскрытие преступления в настоящее время отсутствуют.

МВД по Республике Бурятия, Управление МВД России по г. Улан-Удэ, ОП№1 УМВД России по г. Улан-Удэ, №КУСП ХХХХХ, Дата КУСП: 27.09.2022, №УД 122-094, Дата УД: 27.09.2022

УМВД России по Ямало-Ненецкому АО, ОМВД России по Надымскому району, №КУСП ХХХХХ, Дата КУСП: 16.11.2022, №УД 122-528, Дата УД: 17.11.2022

УМВД России по Орловской области, МО МВД России Мценский, №КУСП ХХХХ, Дата КУСП: 19.12.2022, №УД 122-702, Дата УД: 19.12.2022…»[1]

Так, у сотрудников оперативных подразделений отсутствует доступ к этой базе. Нужно заметить, что доступ к этому комплексу имеется у руководителя отдела (отделения), а также у сотрудников, закрепленных за линией раскрытия мошеннических действий, совершенных с применением информационно-телекоммуникационных сетей. Однако стоит отметить недостаточное количество времени и сотрудников, закрепленных за этим направлением, поскольку в дежурные части поступает значительное количество сообщений о совершении мошенничества и они просто физически не могут проверять

[1] Архив Белорецкого районного суда. Уголовное дело № 123-672/2023.

все поступившие сообщения, и для этого привлекаются сотрудники, которые ведут другие направления деятельности, и непосредственно у них отсутствует такой доступ. Отсюда такая база может не пополняться своевременно, и для ее пополнения потребуется больше времени, что также может снизить эффективность ее применения. Ввиду этого можно согласиться с мнением Екимцева С.В. о необходимости предусмотреть для всех сотрудников уголовного розыска, независимо от закрепленной за ними линии работы, доступ к ИБД «Дистанционное мошенничество»[1].

Сам механизм совершения рассматриваемых преступлений, оставляющий крайне мало криминалистически значимой информации приводит к сильному затруднению розыска подозреваемого и привлечению его к уголовной ответственности. Принимаемые следователем совместно с органом дознания меры по установлению лица, совершившего преступление недостаточно эффективны, о чем говорит низкая статистика раскрываемости рассматриваемой категории преступлений. По статистике состояния преступности в Российской Федерации за январь-декабрь 2024 года раскрываемость краж, совершенных с использованием ИТТ составляет 35,4% от общего числа зарегистрированных преступлений, а раскрываемость аналогичных мошенничеств всего 10,1%[2].

Таким образом, наиболее актуальной проблемой, связанной с розыскной деятельностью при расследовании корыстных преступлений, совершенных с использование ИТТ является установление непосредственный розыск преступника. Исходя из криминалистической характеристики рассматриваемой категории преступления способ совершения преступления, предполагающий отдаленность субъекта преступления от потерпевшего приводит к необходимости расширения площади розыска лиц до территории всей

---

[1] Екимцев С. В. Проблемы раскрытия мошенничества, совершенного с использованием сети интернет // Научный вестник ОрЮИ МВД России им. В. В. Лукьянова. 2023. №4 (97). URL: https://cyberleninka.ru/article/n/problemy-raskrytiya-moshennichestva-sovershennogo-s-ispolzovaniem-seti-internet (дата обращения: 28.10.2024).

[2] Состояние преступности в России за январь – декабрь 2024 года Министерство Внутренних Дел Российской Федерации / ФКУ «Главный информационно-аналитический центр». URL: https://мвд.рф/reports/item/54040412/ (дата обращения: 26.01.2025).

Российской Федерации, а зачастую и за ее пределами. Успешное выполнение такой задачи не представляется возможным без установления взаимодействия между подразделениями различных субъектов, а также использования технических средств. В частности, поиск по базе данных «ИБД-Ф» «Дистанционное мошенничество» позволяет выявить совпадения по имеющимся данным (таким как банковская карта или номер телефона) и, даже при отсутствии раскрытых уголовных дел определить направления для установления взаимодействия.

Подводя итог всему вышесказанному, можно заключить, что во второй главе нами были рассмотрены такие организационные аспекты раскрытия и расследования корыстных преступлений, совершенных с использованием ИТТ, как взаимодействие следователя с органом дознания, специалистами и экспертами, а также организациями, в которые направляются запросы о предоставлении информации. В связи с особенностями криминалистической характеристики, рассмотренных в первой главе нами было особенна выделена значимость взаимодействия следователя со специалистом, так как применение специальных знаний в процессе расследования и раскрытия исследуемых составов преступлений является неотъемлемой частью уголовного судопроизводства в силу своей специфики. Также нами были изучены вопросы розыскной деятельности, осуществляемой в рамках раскрытия и расследования уголовного дела по вышеуказанным преступлениям и выявлены проблемы, связанные со сложностью установления личности преступника что препятствует его дальнейшему розыску и раскрытию преступления в целом.

ГЛАВА 3. ТАКТИКА ПРОВЕДЕНИЯ ОТДЕЛЬНЫХ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ

§1. Тактика проведения осмотра

При расследовании данной категорий преступлений проведение следственных действий имеет особенности, которые могут вызвать затруднения у следователя, в связи с чем рекомендуем обратить внимание на тактику их производства.

Анализ изученного эмпирического материала показывает, что определенные трудности у следователей, особенно с небольшим опытом работы возникают при производстве следственного осмотра, как места происшествия в целом, так и отдельных изъятых предметов.

Вместе с тем практика показывает, что осмотр автомобилей при раскрытии и расследовании рассматриваемой категории преступлений, как и освидетельствование почти не проводятся.

В состав следственно оперативной группы при выезде на осмотр места происшествия рекомендуется включать специалиста-криминалиста, обладающего знаниями в сфере ИТТ для того, чтобы обеспечить правильную фиксацию, исследование и изъятие цифровых следов, которые удаться обнаружить. Стоит отметить, что при отсутствии возможности специалиста с соответствующими знаниями и навыками, следует привлечь иных лиц, чья профессиональная деятельность непосредственно связана с ИТТ и имеющих специальные компетенции, позволяющие оказывать помощь при проведении следственных действий. Следователю при этом важно заранее согласовать со специалистом порядок действий при осмотре и создать необходимые технические условия для его успешной работы[1].

---

[1]Климова Я. А. Искусственный интеллект и цифровые доказательства в расследовании преступлений, совершенных с использованием современных информационно-коммуникационных технологий // Вестник Волгоградской академии МВД России. 2023. №1 (64). URL: https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-i-tsifrovye-dokazatelstva-v-

Наиболее эффективным с точки зрения получение криминалистически важной информации и цифровых следов в данном случае будет использование специалистом специальных программно-аппаратных комплексов («Мобильный криминалист», UFED, Belkasoft evidence center и др.). Однако материально-техническая оснащенность территориальных органов не всегда подразумевает такую возможность, тем более значимым становится правильное изъятие различной техники (например, мобильных устройств, компьютеров и т.д.) и направление их на судебную компьютерно-техническую экспертизу.

Отметим, что имеется ряд особенностей проведения следственных действий и при осмотре предметов, а именно технических средств, которые были непосредственно задействованы при совершении преступления, как правило

к ним относятся смартфоны потерпевшего и подозреваемого. Рекомендации по проведению осмотра данных предметов включают в себя следующий алгоритм действий:

1) перевести устройство в «Авиарежим» для недопущения удаленного стирания информации с устройства;

2) подключить устройство к сети питания (по возможности);

3) установить (со слов задержанного либо иным способом) и внести в протокол пароль доступа к устройству;

4) провести в присутствии понятых сброс паролевой защиты для обеспечения дальнейшего свободного входа в мобильное устройство (в настройках);

5) проверить наличие на устройстве дополнительных «рабочих пространств», предварительно определив расположение в них мессенджеров и прочих сервисов;

6) осуществить проверку сервисов и мессенджеров, находящихся на момент осмотра во включенном состоянии. Отключить в настройках функцию

---

rassledovanii-prestupleniy-sovershennyh-s-ispolzovaniem-sovremennyh (дата обращения: 17.09.2024).

автоматического удаления сообщений. При обнаружении защищенных паролем сервисов и мессенджеров установить пароль и внести его в протокол;

7) зафиксировать переписку и другую значимую информацию путем создания скриншотов (снимков экрана) или фотосъемки изображений на экране осматриваемого устройства;

8) проверить историю установленных на устройстве браузеров в целях определения посещаемых интернет-ресурсов;

9) осуществить проверку устройств на наличие так называемых программ-шпионов. В случае обнаружения принять меры для их отключения[1].

При описании внешнего вида телефона в протоколе осмотра следует отразить: наименование, марку, размеры, цвет, конструкцию, материал, из которого изготовлен, модель, характеристику клавиатуры, фоновый рисунок, имя владельца на дисплее, наличие повреждений, украшений или наклеек[2]

Поскольку данную категорию преступлений злоумышленники, как правило совершают дистанционно, количество следов, которые можно зафиксировать и изъять (как идеальных, так и материальных) сокращается в разы, во многом поэтому так важно грамотно и наиболее эффективно провести осмотр места происшествия и осмотр изъятых предметов.

Несмотря на то, что особая роль в ходе проведения осмотра места происшествия по исследуемым противоправным деяниям отводится грамотным действиям участвующего в мероприятии специалиста, необходимо учитывать наличие возможных технических мер противодействия. Особенно это важно при проведении следственного действия в связи с совершением

---

[1] Рекомендации по взаимодействию органов предварительного следствия, оперативных и экспертно-криминалистических подразделений при необходимости экспертного исследования материалов, включающих интернет-переписку участников организованных групп, по уголовным делам, связанным с незаконным оборотом наркотических средств, психотропных веществ и их прекурсоров : рекомендации. М. ЭКЦ МВД России, Следственный департамент МВД России, ГУНКМВД России, 2020. 18 с.

[2] Нугаева Э. Д. Тактика производства отдельных следственных действий по преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий : научно-практическое пособие / Нугаева Э. Д., Харисова З. И., Арипов А. Л. – Уфа : Уфимский ЮИ МВД России, 2022. С. 45.

высокоорганизованного преступления с использованием ИТТ, когда уровень подготовленности к преступлению и сокрытию его следовой картины очень высоки. Одним из вариантов такого противодействия может быть уничтожение компьютерной информации. Так, к примеру, в квартире преступников могут находится электромагнитные устройства для размагничивания жестких дисков.

А. Н. Першиным, М. В. Бондаревой такой вид противодействия именуется как «техническое противодействие расследованию», как правило, планируемое еще на стадии подготовки преступления. Одними из его видов является возможность удаленного доступа к информации, ее размещение на облачных сервисных хранилищах, а также аренда серверов, расположенных за пределами РФ, делающая невозможной процедуру их изъятия[1].

Поэтому, с учетом вышеуказанного, на этапе подготовки следственного действия необходимо предусмотреть готовность к нейтрализации возможного противодействия. В этой связи, одним из эффективных методов «является применение средств радиоподавления, препятствующих возможности дистанционной подачи команд на уничижение (блокирование, модификацию) доказательственной информации с использованием беспроводных компьютерных сетей и сетей мобильной связи. Для целей обнаружения скрытых или замаскированных электронных носителей информации, содержащих электронные компоненты, применяются нелинейные локаторы.

Таким образом, при расследовании преступлений, связанных с ИТТ, следователь неизбежно сталкивается с таким следственным действием как осмотр (места происшествия или предметов), который может вызвать затруднения в связи со спецификой объектов осмотра. Во избежание утери значимой для уголовного дела информации, а также выполнения требований уголовно-процессуального законодательства и признания полученных доказательств допустимыми необходимо в обязательном порядке привлекать

[1] Першин А. Н. «Техническое противодействие» расследованию преступления: понятие и содержание / Першин А.Н., Бондарева М.В. // Российский следователь. 2022. №7. URL: https://www.elibrary.ru/item.asp?edn=uzrsij (дата обращения: 17.09.2024).

специалиста. При проведении осмотра мобильного телефона – наиболее часто осматриваемого по исследуемым статьям вещественного доказательства – необходимо принять меры для защиты содержащейся в нем информации. Также стоит учитывать возможные меры противодействия, совершаемые преступниками как на этапах подготовки к совершению преступления, так и после его совершения для уничтожения данных и сокрытия следов.

§2. Тактика проведения допроса

Следующим следственным действием, которое обязательно проводится и позволяет получить криминалистически значимую информацию является допрос различных субъектов. В зависимости от процессуального статуса допрашиваемого лица определяется тактика и формируется примерный план допроса, зависящий также от того, какую информацию и в каком количестве можно получить от конкретного допрашиваемого лица с соответствующими вопросами.

Учитывая, что содержание рассматриваемого вида преступления связано с алгоритмами различных действий, при получении информации о механизме его совершения от допрашиваемого, рекомендуем детализировать действия и события поэтапно. Данный прием позволит избежать хаотичность изложения сведений и установить причинно-следственные связи действия с процессами, происходящими на технических устройствах. В случае использования жаргонизмов, порекомендовать их сразу расшифровывать предварительным изучением личности носителя искомой информации, продумыванием способа связи с ним, установлением места· и времени встречи, подготовкой перечня вопросов, которые должны быть выяснены, определением того вопроса, с которого планируется начать диалог, подготовкой к использованию по ходу действия необходимых документов, вещественных доказательств, средств аудио- и видеозаписи, а также другими мерами, обеспечивающими результативность диалогового общения и исключающими

нежелательные последствия межличностного контакта. Особое значение имеют четко выверенная линия и манера поведения следователя, его тактическая оснащенность, умение гибко и оперативно реагировать на изменяющуюся ситуацию, криминалистически грамотное использование тактического материала и технико-криминалистических средств[1].

Рассмотрим поподробнее правила проведения допроса при различных обстоятельствах:

1. Бесконфликтная ситуация допроса, как правило, сюда относятся допросы потерпевших и свидетелей, при благоприятной следственной ситуации может быть и подозреваемый. При проведении такого допроса следует заранее определить, основываясь на личности допрашиваемого лица, какую информацию он может дать о субъекте, обстоятельствах, способах и предмете совершения преступления. Рекомендуется попросить изложить известную информацию в хронологическом порядке, задавая в ходе повествования уточняющие вопросы с целью наиболее полной детализации события и установления всех значимых обстоятельств (время и место, номер телефона и т.д.).

Если бесконфликтная ситуация допроса проходит с подозреваемым, то наряду с выше указанной информацией о событии преступления и действиями подозреваемого, начиная с подготовки к преступления и заканчивая сокрытием следов, также важно узнать информацию о возможных соучастниках преступления, их персональные данные и контактную информацию, распределение ролей и т.д.

При допросе в таком случае стоит использовать такие тактические приемы как снятие психологической напряженности лица, вызванного на допрос? создание благоприятной обстановки допроса, проявление такта, внимания к нему, понимание его проблем и т.д.

---

[1] Нугаева Э. Д. Тактика производства отдельных следственных действий по преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий : научно-практическое пособие / Нугаева Э. Д., Харисова З. И., Арипов А. Л. – Уфа : Уфимский ЮИ МВД России, 2022. – С. 47.

Основное значение тактических приемов в бесконфликтной ситуации – помочь допрашиваемому в припоминании, детализации тех или иных сведений об освещаемом им событии. К их числу криминалисты относят приемы смежности, сходности, наглядности, контрастности и другие.

В бесконфликтной ситуации проходил допрос свидетеля С. по уголовному делу №123-126[1] от 10.02.2023, который работая в качестве курьера привез денежные средства, полученные от потерпевшей, к определенному мошенниками банкомату, где положил их на продиктованный преступниками банковский счет. Подробный хронологический рассказ и желание самого допрашиваемого лица помочь расследованию уголовного дела позволили подробно детализировать обстоятельства произошедшего. Из его показаний была получена такая криминалистически значимая информация как телефонные номера, с помощью которых связывались со свидетелем С., сайт, с помощью которого он был нанят, способ связи, адреса банкоматов, с которых зачисление наличных средств на банковские счета, номера банковских счетов и т.д.

Конфликтная ситуация допроса почти всегда проходит с подозреваемым, в таком случае допрашиваемое лицо либо совсем отказывается от дачи показаний, либо намеренно вводит следователя в заблуждение относительно своих действий и роли в совершенном преступлении. При отказе от дачи показаний можно использовать метод предъявления различных доказательств вины данного лица в совершении преступления, описания сложившейся следственной ситуации и т.д.

При проведении допроса в конфликтной ситуации необходимо исходя из личности допрашиваемого применить такие тактические приемы как предъявление доказательств, результатов следственных действий, пресечение лжи, создание у допрашиваемого представления о значительной осведомленности следователя и об имеющихся доказательствах, проведение форсированного допроса, инерционность и т.д.

---

[1] Архив Белорецкого районного суда. Уголовное дело № 123-126/2023.

Кроме того, подозреваемый может умышленно использовать специальные технические термины, значение которых может быть неизвестно следователю, чтобы при описании событий и своего участия в них запутать его и в дальнейшем трактовать это в свою пользу. Для пресечения такого противодействия необходимо заранее в непроцессуальной форме проконсультироваться со специалистом, обладающим специальными техническими знаниями о событии преступления, технологиях, которые были использованы при его совершении, технических средствах и предположительном алгоритме действий преступника, кроме того, можно при наличии такой возможности привлечь специалиста непосредственно присутствовать на допросе.

В целом совокупность приемов логического и эмоционального воздействия, а также тактических комбинаций посредством воздействия на волевую мобилизацию допрашиваемого способствуют созданию благоприятных условий получения правдивых показаний допрашиваемого[1].

Эмоциональное состояние и внешний вид лица, производящего допрос должны излучать и демонстрировать абсолютную уверенность в наличии достаточных доказательств изобличения преступной деятельности допрашиваемого и неотвратимости последующего наказания. Очень важно проведение такой работы с молодыми преступниками, которые, нередко, получили специальные познания в области ИТТ являясь студентами профильных кафедр учебных заведений различного уровня. Разъяснения о потребности и необходимости применения имеющихся у них познаний, не прибегая к нарушению уголовно-правовой границы дозволенного, с учетом происходящих изменений, способны побудить их к раскаянию и дальнейшему сотрудничеству с органами предварительного следствия.

---

[1] Тагиров Р. А. Способ преодоления конфликтных ситуаций допроса подозреваемых (обвиняемых) в совершении мошенничества // Правовое государство: теория и практика. 2021. №3 (65). URL: https://cyberleninka.ru/article/n/sposob-preodoleniya-konfliktnyh-situatsiy-doprosa-podozrevaemyh-obvinyaemyh-v-sovershenii-moshennichestva-v-sfere-kreditovaniya (дата обращения: 12.01.2025).

Совсем иначе обстоит дело с установлением психологического контакта с допрашиваемыми, имеющими устоявшиеся убеждения противоправной направленности, не склонными к раскаянию и активно противодействующие расследованию.

В данной ситуации определенное психологическое преимущество в случае нахождения подозреваемого под стражей может быть получено в результате возможного появления страха быть осужденным к наказанию в виде лишения свободы, что, вероятно, будет способствовать изменению занятой им противодействующей позиции.

Еще одним тактическим инструментом получения правдивых показаний допрашиваемого является предъявление полученных доказательств, изобличающих или указывающих на его виновность. Так, в зависимости от способа преступления, уровня профессиональной подготовленности, классности используемых вредоносных программ, очевидность цифровых следов может быть различной, в связи с этим мы снова должны подчеркнуть важность взаимодействия со специалистами и экспертами, обладающими специальными знаниями в области ИТТ, так как именно их помощь необходима для понимания достаточности имеющихся доказательств для правильного планирования тактики проведения допроса.

Таким образом, допрос также является одним из наиболее частых проводимых следственных действий при расследовании корыстных преступлений, совершаемых с использованием ИТТ. Во многом тактика проведения допроса зависит от допрашиваемого лица и следственной ситуации, в которой проводится данное следственное действие, следователь должен учитывать конфликтность или бесконфликтность сложившегося положения, процессуальный статус, а также настрой и психологическое состояние допрашиваемого.

Поведение следователя и избираемые им тактические приемы в каждой конкретной ситуации индивидуальны, также стоит учитывать, что некоторые

из тактических приемов допроса (как предъявление вещественных доказательств) требуют дополнительной подготовки.

§3. Назначение и производство судебных экспертиз

Следующим наиболее характерным следственным действием, проводимым по рассматриваемой категории дел, является назначение по делу судебной экспертизы. Наиболее распространенными по данной категории преступлений являются судебная компьютерно-техническая, фоноскопическая и психолого-психиатрическая судебные экспертизы. В дальнейшем, при задержании лица, совершившего преступление также возможно проведение дактилоскопической экспертизы.

Качество и полнота проведения судебной компьютерной экспертизы зависят как от квалификации эксперта, так и от правильно поставленных следователем вопросов, выносимых на разрешение. Правильная постановка вопросов в дальнейшем позволит судье (не сведущему в сфере электронно-вычислительных технологий) принять обоснованное решение (вынести законный судебный акт).

Процессуальный алгоритм (гл. 27 УПК РФ), связанный с экспертным исследованием, в целом, и судебной компьютерно-технической экспертизой, в частности, в уголовном процессе условно представлен четырьмя этапами: назначением, производством, составлением заключения эксперта, оценкой заключения эксперта[1].

Назначение судебной компьютерно-технической экспертизы регулируется общими положениями ст. 195 и 283 УПК РФ и предполагает вынесение постановления следователем или определения суда соответственно с обоснованием такового, указанием судебно-экспертного учреждения

[1] Ильяшевич Т. А., Лубяная Н. И. Практические аспекты производства судебной компьютерно-технической экспертизы в уголовном процессе // Юридическая наука. 2023. №12. URL: https://cyberleninka.ru/article/n/prakticheskie-aspekty-proizvodstva-sudebnoy-kompyuterno-tehnicheskoy-ekspertizy-v-ugolovnom-protsesse (дата обращения: 12.01.2025).

или конкретного эксперта, вопросами к лицу, обладающему специальными знаниями и материалами для производства экспертизы. Участников знакомят с постановлением (определением) о назначении экспертизы.

Установив необходимость производства судебной компьютерно-технической экспертизы, следователь должен определить ряд аспектов. Прежде всего, это объекты, которые будут представлены эксперту для производства соответствующего экспертного исследования. Зачастую таковыми объектами выступают компьютерное или иное техническое устройство, с которого производилось подключение и выход в глобальную информационно-телекоммуникационную сеть.

Далее, следователю необходимо сформулировать вопросы, которые будут поставлены перед экспертом для их разрешения.[1] На них стоит обратить особое внимание – при их постановке необходимо учитывать следующие требования:

1) при формулировании вопросов необходимо по возможности использовать понятийный аппарат, закрепленный в нормативно-правовых актах, а в случае отсутствия таких определений, понятия из технической документации. Это обеспечивает правильное понимание и однозначное толкование следователем и экспертом используемых формулировок;

2) поставленные вопросы должны быть направлены на установление конкретной информации, относящейся к расследуемому уголовному делу;

3) вопросы не должны быть направлены на получение общеизвестной или справочной информации, которая не требует индивидуального изучения объекта исследования;

4) вопросы не должны превышать компетенции эксперта;

5) вопросы должны соответствовать методической и технической базе экспертного учреждения, на базе которого проводится экспертиза;

---

[1] Кокорев Р. А. Актуальные аспекты методики расследования преступлений, совершенных с использованием информационных технологий // Общество, право, государственность: ретроспектива и перспектива. 2024. №. 1. С. 56-64. URL: https://vestnik-uyi.editorum.ru/ru/nauka/article/79392/view (дата обращения: 12.10.2024).

6) вопросы должны относится и соответствовать объектам исследования, предоставляемым на экспертизу.

В итоге по своей сущности компьютерно-техническая экспертиза направлена на всестороннее обнаружение, фиксацию и исследование компьютерной информации с точки зрения ее защиты от злоумышленников[1].

Так, можно упомянуть пример из судебной практики, свидетельствующий об эффективном использования компьютерно-технической экспертизы при расследовании уголовных дел. Советский районный суд г. Тамбова рассматривал дело от 28.02.2020 г., в рамках которого подсудимый обвинялся в совершении преступления по ст. 158 УК РФ. В материалах дела содержалось упоминание о том, что у подсудимого после распития алкогольных напитков с незнакомым ему до этого гражданином П. возник преступный умысел на хищение денежных средств с банковской карты в условиях того, что гражданин П. находился в спящем состоянии. Воспользовавшись PIN-кодом карты, действуя из корыстных побуждений, похитил банковскую карту и впоследствии обналичил с нее деньги, потратив их на покупки. В ходе назначенной компьютерно-технической экспертизы было доказано, что с банкомата, с которого были сняты деньги подсудимым, были изъяты денежные средства в сумме, содержащейся изначально на банковской карте гражданина П., в силу чего суд, основываясь на материалах дела, определил наказание в виде лишения свободы сроком 2 года 6 месяцев[2].

Судебная фоноскопическая экспертиза требует от эксперта широкой эрудиции в науке и технике, а также владения различными методами, включая фильтрацию шумов и установление дословного содержания речи.

---

[1] Трошенкова А. И. Роль судебной компьютерно-технической экспертизы в раскрытии преступлений // Международный журнал гуманитарных и естественных наук. 2020. №12-2. URL: https://cyberleninka.ru/article/n/rol-sudebnoy-kompyuterno-tehnicheskoy-ekspertizy-v-raskrytii-prestupleniy (дата обращения: 17.03.2024).

[2] Приговор Советского районного суда г. Тамбова № 1-29/2020 1-364/2019 от 28.02.2020 г. по делу № 1-29/2020 // База судебных актов, судебных решений и нормативных документов URL: https:// sudact.ru (дата обращения: 17.09.2024).

Для анализа цифровых видео- и аудиозаписей проводится судебная видеофоноскопическая экспертиза. При исследовании только звуковой речевой информации необходима комплексная судебно-компьютерная и фоноскопическая экспертиза, что актуально при расследовании дистанционных мошенничеств.

Необходимость в анализе видеофайлов (как и аудиофайлов) может возникнуть в случае, когда преступники отправляли потерпевшему сгенерированные искусственным интеллектом видео- и аудиозаписи с целью ввести его в заблуждение.

В делах о дистанционном мошенничестве, когда есть фонограмма речи злоумышленника, но его личность не установлена (например, отрицание принадлежности голоса), назначается судебно-фоноскопическая экспертиза. Она направлена на идентификацию личности по голосу, выявление признаков изменения фонограммы и установление обстоятельств звукозаписи на основе сопутствующих звуков, что важно для доказывания.

В случаях, когда у следователя имеется фонограмма устной речи преступника, однако принадлежность данной фонограммы подозреваемому не установлена (когда преступник отрицает принадлежность голоса или абонентского номера, с которого осуществлялся звонок, мотивируя это доступом к нему третьих лиц и др.), необходимо назначить судебно-фоноскопическую экспертизу. Данная экспертиза назначается с целью разрешения ряда задач:

а) идентификации и диагностики человека по голосу;

б) установления возможности изменения содержания фонограммы;

в) выявления на основании фонограммы обстоятельств ее звукозаписи (по сопутствующим звукам в фоне), имеющих значение для доказывания, и т.д.

Для установления состояния потерпевшего на момент совершения преступления: мог ли он быть во невменяемом состоянии, легко ли поддается внушению, есть ли какие-либо факторы, которые могли бы повлиять на действия потерпевшего и т.д.

Согласно ч. 4 ст. 196 УПК РФ назначение и производство судебной экспертизы обязательно, если необходимо установить психическое или физическое состояние потерпевшего, когда возникает сомнение в его способности правильно воспринимать обстоятельства, имеющие значение для уголовного дела, и давать показания.

Необходимо обратить особое внимание на производство психолого-психиатрической экспертизы в отношении пожилых людей, ставших жертвами корыстных преступлений совершенных с использованием ИТТ.

Основания для назначения судебной психолого-психиатрической экспертизы в отношении пожилых потерпевших могут включать сомнения в их способности адекватно воспринимать обстоятельства дела. Эти сомнения могут быть вызваны условиями восприятия, такими как быстрота событий, физическое и психическое состояние потерпевшего, а также множественность отвлекающих факторов.

Кроме того, анализ научной литературы показал, что по рассматриваемой категории преступлений может проводиться судебно-бухгалтерскую экспертизу[1]. При проведении судебно-бухгалтерской экспертизы, целью которой является определение поэтапного движения платежных средств, эксперту предоставляются выписки из банковских учреждений по открытым счетам мошенников, справки с реквизитами счетов, гражданско-правовые договоры, на основании которых можно выявить обстоятельства перечисления денежных средств, и др. Кроме того, данные выписки допустимо представлять в электронном виде. При обнаружении электронных следов, указывающих на несанкционированные денежные операции, в качестве объектов судебно-бухгалтерской экспертизы могут выступать персональные компьютеры, сетевые аппаратные средства и пр.). С учетом сложности и многообразия цифровой

[1] Магомедов Г. М. К вопросу об использовании специальных знаний при расследовании мошенничеств, совершаемых при помощи электронных средств платежа // Закон и право. 2024. №4. URL: https://cyberleninka.ru/article/n/k-voprosu-ob-ispolzovanii-spetsialnyh-znaniy-pri-rassledovanii-moshennichestv-sovershaemyh-pri-pomoschi-elektronnyh-sredstv (дата обращения: 22.04.2025).

информации и следов, по мнению А.Н. Халикова, при расследовании дистанционных мошенничеств целесообразнее назначать проведение судебно-бухгалтерских и судебных компьютерных экспертиз в составе комплексной экспертизы, рекомендации по которым имеются в специальной литературе.[1]

С целью изучения информации о движении денежных средств через электронную систему банкинга по имеющимся выпискам целесообразно назначение судебной бухгалтерской экспертизы

Таким образом, нами были рассмотрены особенности назначения и производства судебных экспертиз при расследовании корыстных преступлений, совершенных с ИТТ. Основными являются судебные компьютерно-техническая, фоноскопическая и психолого-психиатрическая экспертизы, а также, в отдельных случаях, дактилоскопическая и бухгалтерская экспертизы. Судебная компьютерно-техническая экспертиза направлена на исследование информации, содержащихся на электронных носителях и, поскольку многие следователи не обладают техническими знаниями, достаточными

для постановки всеобъемлющих и корректных вопросов, необходимо в полной мере обеспечить доступ к межведомственному взаимодействию по данному вопросу.

Подводя итог третьей главы, можно отметить, что специфика данной категории преступлений приводит к необходимости применения специальных знаний и привлечения компетентных специалистов с техническими знаниями при производстве большинства следственных действий, вместе с тем количество аналогичных преступлений и запросов специалистам не позволяет им в полной мере осуществлять сопровождение уголовного дела. В тексте рассматриваются особенности назначения и проведения судебных экспертиз при расследовании

---

[1] Семенихина Т. Н. О некоторых особенностях использования специальных знаний при расследовании дистанционных мошенничеств, совершаемых с использованием информационно-телекоммуникационных технологий // Общество и право. 2022. №2 (80). URL: https://cyberleninka.ru/article/n/o-nekotoryh-osobennostyah-ispolzovaniya-spetsialnyh-znaniy-pri-rassledovanii-distantsionnyh-moshennichestv-sovershaemyh-s (дата обращения: 22.04.2025).

корыстных преступлений, совершённых с использованием ИТТ. В этой связи стоит обратить внимание на возможность улучшения и расширения экспертных учреждений, как штатно и технически, так и научно-методически. Также подводя итог стоит отметить, что при изъятии различных электронных устройств и осмотре данных предметов необходимо придерживаться установленных правил во избежание потери криминалистически значимой информации. В свою очередь тактика и план допроса зависят от процессуального статуса лица, объема информации, которую можно получить от допрашиваемого и сложившейся следственной ситуации. Кроме того, следует принять во внимание особенности назначения судебной компьютерно-технической экспертизы, а именно необходимость точной и правильной формулировки конкретных вопросов по предоставленным объектам исследования, в этом случае также не стоит забывать о непроцессуальном взаимодействии со специалистами и экспертами в области ИТТ.

ЗАКЛЮЧЕНИЕ

В ходе подготовки работы нами были сделаны следующие выводы:

При рассмотрении предусмотренных уголовным законодательством составов корыстных преступлений совершенных с использованием ИТТ выявлены трудности разграничения данных составов преступления, а именно преступлений предусмотренных п. «г» ч. 3 ст. 158, ст. 159.3 и ст. 159.6 УК РФ в силу их схожести и различной правоприменительной практики, а также отсутствия более подробных разъяснений в Постановлениях Пленума Верховного Суда РФ от 30.11.2017 № 48 и от 27.12.2002 № 29. При этом стоит отметить, совершенствование уголовно-правового законодательства в данной сфере, что несомненно является положительной тенденцией.

При рассмотрении криминалистической характеристике были отмечены следующие наиболее значимые черты:

Преступники, совершающие корыстные преступления с использованием ИТТ, характеризуется как правило, как ранее не судимые, молодые люди, имеющий высокий интеллект, высшее образование и специальные технические знания и навыки.

Самым распространенным способом совершения корыстных преступлений с использованием ИТТ является «фишинг» в различных формах, к наиболее часто используемым на момент исследования относится «вишинг», осуществляющийся с помощью звонков на сотовый телефон потерпевшего и применяющий методы социальной инженерии.

Одной из особенностей криминалистической характеристики данного состава преступлений является наличие не только материальных и идеальных следов, оставляемых преступником, но и виртуального следа, который фиксируется ИТТ при вмешательстве в их работу. Изъятию таких следов необходимо уделить особое внимание, так как они будут являться ключевыми для доказывания события преступления.

Типичными местами совершения являются жилище преступника, место его учебы (работы), общественное место со свободным доступом к информационно-телекоммуникационной сети Интернет, а время совершения определяется с точностью до минут, благодаря автоматизированности фиксации проводимых операций ИТТ.

Подробный анализ криминалистической характеристики позволяет наиболее эффективно установить источники доказательственной информации путем анализа коррелирующих элементов криминалистической характеристики, выдвигать следственные версии, планировать проведение следственных действий и оперативно-розыскных мероприятий и т.д.

При раскрытии и расследовании корыстных преступлений, совершенных с использованием ИТТ эффективность проводимых следственных и процессуальных действий, оперативно-розыскных мероприятий во многом зависит от качества взаимодействия следственных органов в первую очередь со специалистами обладающими техническими знаниями в сфере ИТТ, а также с сотрудниками органа дознания и другими организациями, способствующими расследованию преступления путем предоставления необходимых сведений, в особенностями банковскими организациями и операторами сотовыми связи.

Также нами была выявлена низкая эффективность принимаемых розыскных мер в рамках раскрытия и расследования изучаемых составов, что обусловлено невозможностью получения сведений о личности преступника, совокупность же этих факторов приводит к низкой раскрываемости данной категории дел в целом.

В том числе нами была отмечена необходимость привлечения специалиста, обладающего знаниями и навыками в сфере ИТТ, при этом следует обязательно согласовать с ним план действий и уточнить все значимые обстоятельства дела. Также подчеркивается эффективность использования специальных программно-аппаратных комплексов, которые оперативно предоставляют доступ к криминалистически значимой информации при их грамотном использовании.

В тексте приведены рекомендации по алгоритму действий в случае осмотра мобильного устройства (смартфона), разработанные Следственным департаментом МВД России и позволяющие предотвратить удаление информации с электронного носителя в ходе его осмотра.

При рассмотрении тактики проведения допроса по корыстным преступлениям, совершенным с использованием ИТТ были выявлены особенности, среди которых отмечается использование специальных технических терминов допрашиваемым лицом, в том числе подозреваемым с целью оказания противодействия расследованию, в связи с чем необходимо на подготовительной стадии проконсультироваться со специалистом, либо пригласить его непосредственно на допрос.

Наиболее часто назначаемой судебной экспертизой является компьютерно-техническая судебная экспертиза, которая направлена на всестороннее обнаружение, фиксацию и исследование компьютерной информации, служащей для установления обстоятельств расследуемого уголовного дела и сбору доказательств по нему. Кроме того, наиболее характерными для корыстных преступлений, совершаемых с использованием ИТТ являются судебная бухгалтерская экспертиза, которую наиболее эффективно проводить в комплексе с компьютерно-технической, а также психолого-психиатрическая. Особое внимание при назначении судебных экспертиз следователю необходимо обратить на формулировку вопросов в их оптимальном количестве.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

I. Нормативно-правовые акты и иные официальные документы

1. Уголовно-процессуальный кодекс Российской Федерации [Электронный ресурс] федеральный закон от 18 декабря 2001 № 174-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 22 ноября 2001 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 5 декабря 2001 г. URL: https://www.consultant.ru/document (дата обращения: 17.02.2025).

2. Уголовный кодекс Российской Федерации [Электронный ресурс] федеральный закон от 13 июня 1996 № 163-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 24 мая 1996 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 5 июня 1996 г. URL: https://www.consultant.ru/document (дата обращения: 17.02.2025).

3. О национальной платежной системе [Электронный ресурс] федеральный закон от 27 июня 2011 № 161-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 14 июня 2011 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 22 июня 2011 г. URL: https://www.consultant.ru/document (дата обращения: 17.02.2025).

4. О судебной практике по делам о мошенничестве, присвоении и растрате [Электронный ресурс]: постановление Пленума Верховного Суда РФ от 30.11.2017 № 48. Текст: электронный. URL: https://www.consultant.ru (дата обращения: 14.02.2025).

II. Учебная, научная литература и иные материалы

1. Адмиралова Е. А. Проблемы отграничения преступлений, предусмотренных ст. 159.3 УК РФ и п. "г" ч. 3 ст. 158 УК РФ // 2022. №7 (70). С. 90-93.

2. Буряков Е. В. Оперативно-розыскное учение о розыске: монография / Е. В. Буряков ; М-во внутренних дел Российской Федерации, Омская акад. - Омск : ОмА МВД России, 2011. – 121 с.

3. Ганиева И. А. Личность преступника, совершающего дистанционное мошенничество // Актуальные вопросы борьбы с преступлениями. 2023. №5. С. 56-59

4. Глазатова С. В. Киберпреступления, совершаемые несовершеннолетними: проблемы расследования // 2021. № 2. С. 23-27.

5. Гоголев С. А. Проблемы выявления и расследования киберпреступлений // Скиф. 2021. №11(63). С. 38-43.

6. Екимцев С. В. Проблемы раскрытия мошенничества, совершенного с использованием сети интернет // Научный вестник ОрЮИ МВД России им. В. В. Лукьянова. 2023. №4 (97). С. 78-82.

7. Ильяшевич Т. А., Лубяная Н. И. Практические аспекты производства судебной компьютерно-технической экспертизы в уголовном процессе // Юридическая наука. 2023. №12. С. 120-127.

8. Ищенко П. П. Нужна ли криминалистическая характеристика преступления в криминалистической методике? // Lex Russica. 2020. №3 (160). С. 91-96.

9. Кабанов П. А. Жертвы кибермошенничества как один из объектов современной кибервиктимологии: краткий статистический анализ показателей криминальной виктимности 2021–2022 гг. // Виктимология. 2023. №1. С. 78-84.

10. Климова Я. А. Искусственный интеллект и цифровые доказательства в расследовании преступлений, совершенных с использованием современных информационно-коммуникационных технологий // Вестник Волгоградской академии МВД России. 2023. №1 (64). С. 15-18.

11. Кокорев Р. А. Актуальные аспекты методики расследования преступлений, совершенных с использованием информационных технологий / Кокорев Р.А. // Общество, право, государственность: ретроспектива и перспектива. 2024. №1 (17). С. 67-71.

12. Куликова И. Е. Некоторые вопросы взаимодействия следователя с оперативными работниками при раскрытии и расследовании мошенничеств // Криминалистика: вчера, сегодня, завтра. 2022. №2. С. 56-60.

13. Куликова И. Е. Организационные аспекты использования специальных знаний при раскрытии дистанционных мошенничеств // Пролог: журнал о праве. 2022. №4(36). С. 180-184.

14. Магомедов Г. М. К вопросу об использовании специальных знаний при расследовании мошенничеств, совершаемых при помощи электронных средств платежа // Закон и право. 2024. №4. С. 89-93.

15. Милованова М. М. Криминалистическая превенция телефонного мошенничества // Правовой альманах. 2025. №1 (41). С. 34-37.

16. Нугаева Э. Д. Особенности первоначального этапа расследования неправомерного доступа к компьютерной информации: учебно-методическое пособие. / Нугаева Э. Д., Низаева С. Р., Гайнельзянова В. Р., Харисова З. И. – Уфа: Уфимский ЮИ МВД России, 2023. 96 с.

17. Нугаева Э. Д. Тактика производства отдельных следственных действий по преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий : научно-практическое пособие / Э. Д. Нугаева, З. И. Харисова, А. Л. Арипов. – Уфа : Уфимский ЮИ МВД России, 2022. 96 с.

18. Попова Т. В. Способы и преступные схемы хищений денежных средств с лицевых счетов банковских карт граждан // Академическая мысль. – 2018. – №2 (3). С. 76-79.

19. Першин А. Н. «Техническое противодействие» расследованию преступления: понятие и содержание // Российский следователь. 2022. №7. С. 67-75.

20. Рогова Е. В. Корыстная преступность в условиях информационной глобализации // Вестник Казанского юридического института МВД России. 2022. №2 (48). С. 123-128.

21. Савченко М. М. Квалификационные ошибки применения ст. 159.3 и п. «г» ч. 3 ст. 158 Уголовного Кодекса РФ // Право и практика. 2022. №3. С. 23-27.

22. Стяжкина С. А. Виктимологическая профилактика кибермошенничества // Вестник Удмуртского университета. Серия «Экономика и право». 2022. №3. С. 90-93.

23. Тагиров Р. А. Способ преодоления конфликтных ситуаций допроса подозреваемых (обвиняемых) в совершении мошенничества // Правовое государство: теория и практика. 2021. №3 (65). С. 45-51

24. Теткин Д. В. Некоторые особенности раскрытия и расследования киберпреступлений в современном мире глобальной цифровизации // Право: история и современность. 2022. №2. С. 34-36.

25. Ткачева Н. В. Виктимология и киберпреступность в России // Вестник ЮУрГУ. Серия: Право. 2021. №3. С. 29-36.

26. Трошенкова А. И. Роль судебной компьютерно-технической экспертизы в раскрытии преступлений Международный журнал гуманитарных и естественных наук. 2020. №12-2. URL: С. 26-31

27. Семенихина Т. Н. О некоторых особенностях использования специальных знаний при расследовании дистанционных мошенничеств, совершаемых с использованием информационно-телекоммуникационных технологий // Общество и право. 2022. №2 (80). С. 97-101.

28. Соколова Т. С. К вопросу взаимодействия органов предварительного следствия с органами дознания при проведении доследственной проверки по сообщениям о мошенничествах, совершенных с использованием информационно-телекоммуникационных технологий // Право и государство: теория и практика. 2023. №3 (219). С. 76-79.

29. Шляхова Ю. Д. Тактические основы розыскной деятельности следователя и оперативно-розыскной деятельности органов дознания // Colloquium-journal. 2022. №34 (157). С. 46-48.

30. Шхагапсоев З. Л. К вопросу о роли органов внутренних дел в предупреждении преступлений, совершаемых с использованием информационных технологий (IT-преступлений) // Государственная служба и кадры. 2020. №2. С. 23-27.

III. Эмпирические материалы

1. Комплексный анализ состояния преступности в Российской Федерации по итогам 2023 года и ожидаемые тенденции ее развития: аналитический обзор. М.: ФГКУ «Всероссийский научно-исследовательский институт Министерства Внутренних Дел Российской Федерации» 2024 г. С. 23-25.

2. Приговор Советского районного суда г. Тамбова № 1-29/2020 1-364/2019 от 28.02.2020 г. по делу № 1-29/2020 [Электронный ресурс]. URL: https:// sudact.ru (дата обращения: 17.03.2025).

3. Рекомендации по взаимодействию органов предварительного следствия, оперативных и экспертно-криминалистических подразделений при необходимости экспертного исследования материалов, включающих интернет-переписку участников организованных групп, по уголовным делам, связанным с незаконным оборотом наркотических средств, психотропных веществ и их прекурсоров : рекомендации. М. : ЭКЦ МВД России, Следственный департамент МВД России, ГУНКМВД России, 2020. 18 с.

4. Архив Белорецкого районного суда. Уголовное дело № 123-126/2023.

5. Архив Белорецкого районного суда. Уголовное дело № 123-672/2023.

Материал вычитан, цифры, факты, цитаты сверены с первоисточниками. Материал не содержит сведений, составляющих государственную и служебную тайну Д.И. Аглетдинова