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 ХИЩЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ (ПО МАТЕРИАЛАМ ТЕРРИТОРИАЛЬНОГО ОРГАНА ВНУТРЕННИХ ДЕЛ)»**

Выполнил
Минигалиев Ирек Радиевич,
обучающийся по специальности
40.05.01 Правовое обеспечение
национальной безопасности
2017 года набора, 7101 учебной группы

Руководитель
Старший преподаватель кафедры
Еркеев Ильшат Хамитович

К защите _____
рекомендуется / не рекомендуется
Начальник кафедры _____ Э.Д. Нугаева
подпись
Дата защиты «___» _____ 2023 г. Оценка _____

ПЛАН

ВВЕДЕНИЕ

Актуальность выпускной квалификационной работы. С развитием науки и техники условия для жизнедеятельности человека меняются в сторону повышения комфорта. Однако, криминальный мир также подстраивается к общественным переменам, что приводит к появлению новых способов совершения преступлений.

Всю историю человечества самыми распространёнными преступлениями являлись хищения. В настоящее время одним из динамично растущих по количеству совершенных преступлений являются хищения, совершенные с помощью информационных и телекоммуникационных технологий. Мы согласимся с мнением тех ученых, которые указанную группу преступлений именуют дистанционными хищениями[1].

Так, за последние пять лет наблюдений с 2018 по 2022 год масштабы указанной группы преступлений демонстрируют рост в среднем, на 33,38 % в год (Приложение 1). Кроме того, раскрываемость хищений, совершенных с помощью информационных технологий, с 2018 по 2022 год остается на низком уровне – 18,01 %[2]. Следовательно, только каждое пятое уголовное дело в исследуемой группе хищений предварительно расследуется с направлением материалов в суд. Значит в четырех из пяти уголовных дел о хищениях с помощью информационных технологий в Российской Федерации преступники остаются безнаказанными.

В свете сказанного, важно понимать, что повышение качества предварительного расследования зависит не только от профессионализма следователя, но и качества и оперативности сбора доказательственной базы. Кроме того, на профессионализм следователя, расследующего хищения,

---

[1] Евтушенко И.И., Венедиктов А.А. Дистанционные хищения: понятие и признаки // Гуманитарные, социально-экономические и общественные науки. 2020. № 12-2. С. 65-67.

[2] Состояние преступности в Российской Федерации: [Электронный ресурс]: статистические сборники за 2018, 2019, 2020, 2021, 2022 года. URL:// https://xn--b1aew.xn--p1ai/dejatelnost/statistics (дата обращения: 28.01.2023).

совершенные с помощью информационных технологий, влияет тот факт, что у современных следователей еще не наработан должный следственный опыт для высокого уровня раскрываемости и, соответственно, обмена опытом между собой.

Выявление особенностей расследования хищений, совершаемых с использованием информационных технологий, основывается на криминалистической характеристике обозначенной группы преступлений. Выявив виды и объемы совершаемых преступлений, личность преступника, личность жертвы, способы и обстановку совершения дистанционных хищений на примере деятельности территориального органа внутренних дел, а именно ОМВД России по Ашинскому району, возможно исследовать организационно-тактические особенности в рамках расследования указанной группы преступлений.

Несомненно, низкие уровни раскрываемости требуют немедленного реагирования со стороны научного сообщества и руководства страны с целью внедрения предложений по модернизации процесса предварительного расследования дистанционных хищений. Так, одной из практических проблем, влияющих на качество предварительного расследования хищений, совершенных с помощью информационных технологий, является низкий временной показатель предоставления провайдерами финансовых услуг необходимых данных по запросам правоохранительных органов в рамках досудебного производства. Безусловно, основы правового российского государства не позволяют требовать от указанных организаций предоставления сведений в правоохранительные органы в кратчайшие сроки. Поэтому необходима система выстраивания отношений взаимодействия между указанными субъектами с целью достижения безопасности счетов с электронными денежными средствами.

Другим проблемным вопросом является отсутствие у следователей, расследующих дистанционные хищения, достаточной компетенции в области информационных технологий, банковского и бухгалтерского дела. Данная

проблема должна решаться привлечением специалистов в указанных сферах при планировании расследования и непосредственном производстве следственных действий.

Кроме того, достаточно перспективными для расследования дистанционных хищений являются предложения по модернизации таких следственных действий, как допрос, осмотр и производство экспертиз.

В свете сказанного, цель выпускной квалификационной работы заключается в комплексном изучении особенностей расследования хищений, совершаемых с использованием информационных технологий.

Названная цель предопределила решение следующих задач:

– проанализировать понятие и сущность криминалистической характеристики хищений, совершаемых с использованием информационных технологий;

– исследовать динамику и способы совершения хищений с использованием информационных технологий, как ключевой элемент, составляющий криминалистическую характеристику;

– проанализировать факультативные элементы криминалистической характеристики хищений, совершаемых с использованием информационных технологий;

– рассмотреть производство доследственной проверки и возбуждение уголовных дел о хищениях, совершаемых с использованием информационных технологий

– определить характерные следственные ситуации и составление плана расследования хищений, совершаемых с использованием информационных технологий;

– выявить тактические особенности производства отдельных следственных действий при расследовании хищений, совершаемых с использованием информационных технологий.

Объектом выпускной квалификационной работы следует обозначить систему общественных отношений, которые возникают в процессе расследования

хищений, совершаемых с использованием информационных технологий.

Предмет выпускной квалификационной работы составляют: система законодательства по вопросам расследования хищений, совершаемых с использованием информационных технологий, научная и учебная криминалистическая литература по рассматриваемой проблематике, различные статистические и аналитические данные Министерства внутренних дел Российской Федерации, отдельных территориальных органов внутренних дел, судебная практика, а также иные материалы.

При выполнении исследования применялась система общенаучных методов познания, важное место среди которых заняли анализ, синтез, формально-логический метод, индукция и другие. Кроме того, в работе применялись частно-научные методы познания, среди которых сравнительно-правовой, статистический, обобщение и другие. Названные методы научного познания позволили глубоко проработать тематику исследования, выявить дискуссионные аспекты и проблематику расследования хищений, совершаемых с использованием информационных технологий.

В структуру выпускной квалификационной работы следует включать введение, две главы, которые объединяют в себе шесть параграфов, заключение, список использованной литературы, а также приложения.

ГЛАВА 1. КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА ХИЩЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

§ 1. Понятие и сущность криминалистической характеристики хищений, совершаемых с использованием информационных технологий

Для того, чтобы изучить особенности расследования хищений, совершаемых с использованием информационных технологий, необходимо исследовать понятие указанной группы преступлений, способы и обстановку их совершения, личность преступника. Обозначенные данные позволят сформировать представление о наиболее и менее вероятных следственных ситуациях, а также сформировать следственные версии для планирования расследования. Результаты теоретического анализа криминалистической характеристики указанной группы преступлений, а также эмпирическое исследование конкретных уголовных дел позволят выявить проблемные вопросы, влияющие на их низкую раскрываемость, а также спроектировать алгоритмы действий органов предварительного расследования в целях достижения основного предназначения уголовного судопроизводства. В данном параграфе изучим понятие и сущность криминалистической характеристики хищений, совершаемых с использованием информационных технологий.

Криминалистический аспект исследования комплекса свойств, типичных для конкретной группы преступлений, влияет на эффективность выработки решений органов предварительного расследования на всей досудебной стадии. Такой комплекс свойств группы преступлений составляет категорию их криминалистической характеристики.

Не смотря на значительное количество исследований категории криминалистической характеристики, в настоящее время единого подхода к ее пониманию в научном сообществе нет. Рассматривая несколько подходов к определению и структуре этой категории, мы пришли к выводу, что их

определяющим отличием является количество тех элементов, которые криминалистическая характеристика в себя включает. Вместе с тем, важно обозначить научное мнение, согласно которого ключевые элементы криминалистической характеристики взаимосвязаны с криминологическим и уголовно-правовым аспектами[1].

Итак, разбирая конкретные элементы криминалистической характеристики, следует обозначить их важнейший признак, который заключается в регулярности и постоянстве при совершении исследуемой группы преступлений. Соответственно, считаем, что отсутствие такого постоянства как признака элемента лишает нас возможности рассматривать его в качестве элементов криминалистической характеристики, т.к. это усложнит восприятие сущности группы таких преступлений, а также негативно скажется на эффективности предварительного расследования.

Ряд ученых относят к элементам криминалистической характеристики механизм, метод и обстоятельства совершенного преступления[2]. Иные ученые раскрывают сущность указанных элементов, конкретизируя подструктуры: способ совершения преступления, предмет преступного посягательства, условия совершения преступления, личность преступника и личность жертвы, а также криминалистически значимые связи между указанными элементами[3]. Сказанное подтверждает сущность криминалистической характеристики во взаимосвязи с криминологическим и уголовно-правовым аспектами, указанными ранее.

Рассмотрим понятие исследуемой группы преступлений. Согласно Перечня № 25 указания Генеральной прокуратуры Российской Федерации и

---

[1] Караева А.А., Панченко О.В. Криминалистическая характеристика преступления: терминологические подходы, содержание понятия // Молодой ученый. 2020. № 41 (331). С. 103-105.

[2] Борисова Ю.А. Возникновение и становление понятия криминалистической характеристики преступления // StudNet. 2020. Т. 3. № 3. С. 467-472.

[3] Кочеткова А.А. Криминалистическая характеристика преступления: актуальные проблемы понятия // Юность. Наука. Культура:материалы VII Всероссийской научно-практической конференции. Средне-Волжский институт (филиал) ВГУЮ (РПА Минюста России). 2020. С. 344-346.

Министерства внутренних дел Российской Федерации «О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности» от 29 декабря 2021 г. № 790/11/1 (далее – Перечень)[1], к хищениям, совершенным с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, относятся мошенничества, квалифицируемые по ст. 159 УК РФ, мошенничества с использованием электронных средств платежа, квалифицируемые по ст. 159.3 УК РФ, мошенничества в сфере компьютерной информации, квалифицируемые по ст. 159.6 УК РФ, а также кражи, совершенные с банковского счета, а равно в отношении электронных денежных средств, квалифицируемые по п. «г» ч. 3 ст. 158 УК РФ.

Одной из особенностей данных преступлений являются разные их наименования, такие как хищения в сфере информационных технологий, киберхищения[2], хищения в сфере IT-технологий[3], интернет-хищения[4]. Вместе с тем, в научной литературе есть, на наш взгляд, удачное наименование всех хищений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, – это дистанционные хищения[5].

Рассмотрим основные признаки, которые позволяют выделять дистанционные хищения с уголовно-правовой точки зрения, и объединять их в

---

[1] О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности: указание Генпрокуратуры России № 11/11, МВД России № 1 от 17 января 2023 г. (Перечень № 25) [Электронный ресурс]. URL:// http://www.pravo.gov.ru (дата обращения: 10.02.2023).

[2] Старостенко О.А. Меры специальной профилактики киберхищений // Молодежь и наука: актуальные проблемы фундаментальных и прикладных исследований: материалы V Всероссийской национальной научной конференции молодых учёных. В 4-х частях. Редколлегия: А.В. Космынин (отв. ред.) [и др.]. Комсомольск-на-Амуре, 2022. С. 212-214.

[3] Ижунинов М.А. Процесс предупреждения хищения с помощью IT-технологий на настоящий момент // Интеграция наук. 2019. № 2 (25). С. 97-98.

[4] Грунина В.А., Новичкова Ю.Г., Ананьина Ю.А. Теоретические основы регулирования юридической ответственности за новые формы интернет-мошенничества в сети «Интернет» // Современная наука: актуальные проблемы теории и практики. Серия: Экономика и право. 2021. № 9. С. 79-84.

[5] Евтушенко И.И., Венедиктов А.А. Дистанционные хищения: понятие и признаки // Гуманитарные, социально-экономические и общественные науки. 2020. № 12-2. С. 65-67.

одну группу преступлений.

Считаем важнейшим признаком исследуемой группы преступлений их совершение в условиях неочевидности, т.е. преступник и жертва не видят друг друга, чаще всего находятся на расстоянии.

Важно также выделить такой существенный признак как применение средств и устройств, позволяющих в отсутствие личного физического контакта с жертвой и ее деньгами завладеть последними.

Предметом дистанционных хищений всегда являются электронные денежные средства, однако, они обезличены и передаются жертвой (или захватываются преступником) в безналичной или наличной форме.

Определяя общность предметов дистанционных хищений, мы согласимся с мнением тех ученых, которые среди таких предметов выделяют: безналичные денежные средства, электронные денежные средства и иные имущественные права, в том числе цифровые права[1].

Для понимания сущности исследуемой группы преступлений также необходимо изучить, что подразумевает законодатель под электронным средством платежа. Считаем, что главными его признаками является, во-первых, форма выражения, а именно – это технические устройства (мобильные устройства, платёжные карты и терминалы, персональные компьютеры и пр.), а, во-вторых, программное обеспечение или способ, состоящий из определенных последующих действий, направленных на удостоверение права распоряжения денежными средствами.

Учеными не раз высказывались мнения о декриминализации некоторых составов, входящих в исследуемую группу преступлений, с целью их объединения в единый состав Уголовного закона страны, например, «Хищение с использованием информационных технологий»[2] или «Хищение

---

[1] Савченко М.М. Правовая природа безналичных и электронных денег как предмета преступных посягательств // Бизнес. Образование. Право. 2021. № 2 (55). С. 244-250.

[2] Диденко К.В., Зейналбдыева А.В., Свиридов Р.В. Проблемные вопросы квалификации хищений с использованием информационных технологий // Современный ученый. 2020. № 5. С. 306-310.

имущественных прав»[1]. Вместе с тем, в рамках данной выпускной квалификационной работы считаем первостепенным изучить основные и факультативные криминалистические элементы дистанционных хищений. Для этого рассмотрим динамику, структуру указанной группы преступлений, способы и обстановку их совершения, личности преступника и жертвы.

В качестве вывода к первому параграфу выпускной квалификационной работы следует отметить, что не смотря на различность подходов в понимании сущности криминалистической характеристики преступлений, нами поддерживается научное мнение о взаимосвязи уголовно-правового и криминологического аспектов с элементами криминалистической характеристики преступлений или групп преступлений. В качестве группы преступлений в рамках данной выпускной квалификационной работы исследуются хищения, совершенные с помощью информационных технологий. Исследованы и выявлены признаки таких хищений: совершение в условиях неочевидности, т.е. преступник и жертва не видят друг друга; предметом всегда являются денежные средства в безналичной или наличной форме; применение преступником средств и устройств, позволяющих в отсутствие личного физического контакта с жертвой и ее деньгами завладеть последними. При этом, преступник находится «на дистанции» от потерпевшего, поэтому мы согласимся с учеными-теоретиками права о универсальном наименовании таких преступлений – «дистанционные хищения». Мы согласимся с законодателем, который в исследуемую группу преступлений включает составы, квалифицируемые по ст. 159 УК РФ, мошенничества с использованием электронных средств платежа, квалифицируемые по ст. 159.3 УК РФ, мошенничества в сфере компьютерной информации, квалифицируемые по ст. 159.6 УК РФ, а также кражи, совершенные с банковского счета, а равно в отношении электронных денежных средств, квалифицируемые по п. «г» ч. 3 ст. 158 УК РФ. На основе предлагаемых научным сообществом определений хищений, совершаемых с использованием

[1] Евтушенко И.И., Венедиктов А.А. Дистанционные хищения: понятие и признаки // Гуманитарные, социально-экономические и общественные науки. 2020. № 12-2. С. 65-67.

информационных технологий, нами разработано авторское понимание искомого понятия, согласно которому под дистанционными хищениями следует понимать общественно-опасное деяние, совершаемое с помощью средств и устройств, позволяющих преступнику в отсутствие личного физического контакта с жертвой и ее деньгами завладеть последними.

§ 2. Динамика и способы совершения хищений с использованием информационных технологий, как ключевой элемент, составляющий криминалистическую характеристику

Для исследования способов совершения дистанционных хищений необходимо понимать динамику и структуру обозначенной группы преступлений.

Так, всего в Российской Федерации в 2018 году исследуемая группа преступлений составила 143307 преступлений, в 2019 году – 235507 преступлений, в 2020 году – 410490 преступлений, в 2021 году – 406041 преступления, в 2022 году – 389646 преступлений (Приложение 1)[1].

Анализ диаграммы Приложения 1 позволяет сделать вывод о росте количества дистанционных хищений, в среднем, на 33,38 % в год за последние пять лет наблюдений. Причем, наибольшую долю преступлений в структуре хищений с использованием информационных технологий в Российской Федерации за период с 2018 по 2022 года составляют мошенничества, квалифицируемые по ст. 159 УК РФ, – 56,92 %; кражи, квалифицируемые по п. «г» ч. 3 ст. 158 УК РФ, – 38,67 %; мошенничества с использованием платежных карт ст. 159.3 УК РФ – 4,26 %; мошенничества в сфере компьютерной информации ст. 159.6 УК РФ – 0,15 % (Приложение 2)[2].

---

[1] Состояние преступности в Российской Федерации: [Электронный ресурс]: статистические сборники за 2018, 2019, 2020, 2021, 2022 года. URL:// https://xn--b1aew.xn--p1ai/dejatelnost/statistics (дата обращения: 28.01.2023).

[2] Состояние преступности в Российской Федерации: [Электронный ресурс]: статистические сборники за 2018, 2019, 2020, 2021, 2022 года. URL:// https://xn--b1aew.xn--p1ai/dejatelnost/statistics (дата обращения: 28.01.2023).

С учетом территориального аспекта исследования выпускной квалификационной работы важно так же понимать, какова динамика исследуемой группы преступлений на территории, обслуживаемой ОМВД России по Ашинскому району.

Так, на территории Ашинского района в 2018 году исследуемая группа преступлений составила 70 преступлений (из них по ст. 159 УК РФ возбуждено 41 уголовное дело, по п. «г» ч. 3 ст. 158 УК РФ – 29 уголовных дел), в 2019 году – 100 преступлений (из них по ст. 159 УК РФ возбуждено 57 уголовных дел, по п. «г» ч. 3 ст. 158 УК РФ – 43 уголовных дела), в 2020 году – 123 преступлений (из них по ст. 159 УК РФ возбуждено 62 уголовных дел, по п. «г» ч. 3 ст. 158 УК РФ – 61 уголовное дело), 2021 году – 99 преступления (из них по ст. 159 УК РФ возбуждено 56 уголовных дел, по п. «г» ч. 3 ст. 158 УК РФ – 43 уголовных дела), в 2022 году – 130 преступлений (из них по ст. 159 УК РФ возбуждено 76 уголовных дел, по п. «г» ч. 3 ст. 158 УК РФ – 54 уголовных дела) (Приложение 3)[1].

Анализ диаграммы Приложения 3 позволяет сделать вывод о росте количества дистанционных хищений на территории Ашинского района, в среднем, на 61,4 % в год за последние пять лет наблюдений с 2018 по 2022 года. Причем, наибольшую долю преступлений в структуре хищений с использованием информационных технологий на территории Ашинского района за период с 2018 по 2022 года составляют мошенничества, квалифицируемые по ст. 159 УК РФ, – 55,9 %, в тоже время, кражи, квалифицируемые по п. «г» ч. 3 ст. 158 УК РФ, составляют 44,1 %. Спецификой территории Ашинского муниципального района является тот факт, что за последние пять лет наблюдений с 2018 по 2022 года не было возбуждено ни одного преступления, квалифицируемого либо как мошенничество с использованием платежных карт по ст. 159.3 УК РФ, либо

[1] Аналитические справки деятельности ОМВД России по Ашинскому району за 2018, 2019, 2020, 2021, 2022 года, предоставленные ИЦ ГУ МВД России по Челябинской области.

как мошенничество в сфере компьютерной информации по ст. 159.6 УК РФ[1]. Поэтому с учетом территориального аспекта выпускной квалификационной работы целесообразно в рамках данной работы рассматривать элементы криминалистической характеристики, а также организационно-тактические основы расследования применительно к следующим хищениям, совершаемым с помощью информационных технологий, – мошенничество ст. 159 УК РФ и кражи с банковского счета, а равно в отношении электронных денежных средств по п. «г» ч. 3 ст. 158 УК РФ.

Вся деятельность следователя направлена на достижение истины по уголовному делу, чтобы, в конечном итоге, виновные лица были изобличены, а пострадавшим был возмещен причиненный ущерб и восторжествовала социальная справедливость. Поэтому эффективность деятельности органов предварительного следствия, в том числе следователя, как должностного лица, возможно оценить с помощью коэффициента раскрываемости. Для тактического планирования предварительного расследования указанный коэффициент имеет значение с точки зрения наработанного следственного опыта. Действительно, низкий коэффициент раскрываемости свидетельствует не только о проблемах расследования, но и об отсутствии следственного опыта по расследованию конкретной группы преступлений.

Так, в Российской Федерации с 2018 по 2022 года наблюдается различная динамика коэффициента раскрываемости исследуемой группы преступлений. В частности, в 2018 году раскрываемость дистанционных хищений, квалифицируемых по ст. 159 УК РФ, составила 7,9 %, в 2019 году – 8,6 %, в 2020 году – 6,8 %, в 2021 году – 9,1 %, в 2022 году – 12,8 % (Приложение 4)[2].

Раскрываемость дистанционных хищений, квалифицируемых по ст. 159.3 УК РФ, в 2018 году составила 33,4 %, в 2019 году – 33,3 %, в 2020 году –

---

[1] Аналитические справки деятельности ОМВД России по Ашинскому району за 2018, 2019, 2020, 2021, 2022 года, предоставленные ИЦ ГУ МВД России по Челябинской области.

[2] Состояние преступности в Российской Федерации: [Электронный ресурс]: статистические сборники за 2018, 2019, 2020, 2021, 2022 года. URL:// https://xn--b1aew.xn--p1ai/dejatelnost/statistics (дата обращения: 28.01.2023).

31,3 %, в 2021 году – 6,1 %, в 2022 году – 5,3 % (Приложение 4)[1].

Раскрываемость дистанционных хищений, квалифицируемых по ст. 159.6 УК РФ, в 2018 году составила 7,4 %, в 2019 году – 8,7 %, в 2020 году – 14,5 %, в 2021 году – 24,9 %, в 2022 году – 24,8 % (Приложение 4)[2].

Раскрываемость дистанционных хищений, квалифицируемых по п. «г» ч. 3 ст. 158 УК РФ, в 2018 году составила 22,5 %, в 2019 году – 23,7 %, в 2020 году – 16,0 %, в 2021 году – 25,8 %, в 2022 году – 37,3 % (Приложение 4)[3].

Анализ графика, представленного в Приложении 4, позволяет сделать вывод, что на фоне роста общего количества дистанционных мошенничеств с 2018 по 2022 года показатели раскрываемости синхронно растут благодаря накапливаемому следственному опыту. Вместе с тем, раскрываемость дистанционных хищений, квалифицируемых по ст. 159.3 УК РФ демонстрирует тенденцию к падению, что, несомненно, требует реагирования не только со стороны руководящих должностных лиц органов внутренних дел и следственных подразделений, но и юридических лиц, оказывающих банковские, финансовые и денежные услуги. Кроме того, необходимо развивать профилактическое направление дистанционных мошенничеств, т.к. предупредительная работа эффективнее, чем нежели расследование уже случившегося факта противоправного деяния.

С учетом территориального аспекта выпускной квалификационной работы рассмотрим раскрываемость исследуемых преступлений следственными органами ОМВД России по Ашинскому району. При этом, важно обозначить, что по ст. 159.3 УК РФ и ст. 159.6 УК РФ коэффициент раскрываемости отсутствует, т.к. за период с 2018 по 2022 года на этой территории указанные преступления не совершались.

Итак, в Ашинском муниципальном районе в 2018 году раскрываемость

---

[1] Аналитические справки деятельности ОМВД России по Ашинскому району за 2018, 2019, 2020, 2021, 2022 года, предоставленные ИЦ ГУ МВД России по Челябинской области.

[2] Аналитические справки деятельности ОМВД России по Ашинскому району за 2018, 2019, 2020, 2021, 2022 года, предоставленные ИЦ ГУ МВД России по Челябинской области.

[3] Аналитические справки деятельности ОМВД России по Ашинскому району за 2018, 2019, 2020, 2021, 2022 года, предоставленные ИЦ ГУ МВД России по Челябинской области.

дистанционных хищений, квалифицируемых по ст. 159 УК РФ, составила 7,9 %, в 2019 году – 7,0 %, в 2020 году – 11,3 %, в 2021 году – 5,4 %, в 2022 году –0,0 %. Раскрываемость дистанционных хищений, квалифицируемых по п. «г» ч. 3 ст. 158 УК РФ, в 2018 году составила 10,3 %, в 2019 году – 16,3 %, в 2020 году – 3,3 %, в 2021 году – 41,9 %, в 2022 году – 16,7 % (Приложение 5)[1].

Анализ графика, представленного в Приложении 5, позволяет сделать вывод, что на фоне роста общего количества дистанционных мошенничеств с 2018 по 2022 года на территории Ашинского района показатели раскрываемости дистанционных хищений, квалифицируемых по ст. 159 УК РФ демонстрирует тенденцию к падению, а по п. «г» ч. 3 ст. 158 УК РФ – тенденцию к росту. Указанные данные количественно коррелируют с общероссийскими показателями раскрываемости, представленными в Приложении 4.

Определив количественные признаки дистанционных хищений, совершаемых в Российской Федерации и в Ашинском муниципальном районе, нами предлагается рассмотреть основные способы совершения указанных преступлений.

Важность изучения способов совершения дистанционных мошенничеств обусловлена возможностью идентифицировать характерные признаки, которые позволят моделировать типичные следственные ситуации и выбирать тактические особенности при расследовании указанной группы преступлений. На актуальность исследования способа совершения преступлений также указывает и законодатель, т.к. в некоторых составах преступлений способ совершения является квалифицирующим признаком состава и влияет на назначение наказания. С другой стороны, не все составы преступлений предусматривают такой квалифицирующий признак, как способ совершения противоправного деяния. Однако, в рамках криминалистической характеристики данный элемент напрямую может указывать на наличие

[1] Аналитические справки деятельности ОМВД России по Ашинскому району за 2018, 2019, 2020, 2021, 2022 года, предоставленные ИЦ ГУ МВД России по Челябинской области.

нескольких преступников и сложной криминальной сети взаимоотношений в совершении расследуемого преступления и позволить оперативно их установить.

Уголовный закон Российской Федерации не содержит определения искомого понятия. Но и в научной среде нет единого подхода к его пониманию.

По мнению ряда ученых, способ совершения преступления «выражается в определенном плане конкретных действий, направленных, в данном случае, на достижение желаемого для виновного лица (виновных лиц) результата»[1]. Другие считают, что способ совершения преступления рассматривается как форма выражения определенных преступных действий различными приемами и методами, примененными лицом в совершении преступления[2].

Итак, авторское понимание способа совершения преступления сводится к выражению определенной последовательности действий, запланированной для достижения противоправной цели лицом или лицами, реализующими преступный умысел.

Как было выявлено ранее, основным признаком дистанционных хищений является хищение именно электронных денежных средств, находящихся на банковских счетах. Кроме того, из курса особенной части уголовного права известно, что все хищения можно подразделять на открытые и тайные. Исходя из сказанного, необходимо выделять следующие свойства способов совершения дистанционных хищений, которые позволят их дифференцировать по:

1) обеспечение доступа к банковскому счёту потерпевшего;

2) осуществление трансакции.

Устремленность на реализацию банковских операций является фундаментом и отличительной чертой исследуемой группы преступлений.

---

[1] Поддубный И.В., Васюков В.Ф. К вопросу об актуальных способах совершения хищений с банковских счетов граждан, совершаемых с использованием систем дистанционного банковского обслуживания // Шумиловские чтения: сборник материалов Международной научно-практической конференции. Российская таможенная академия. 2021. С. 171-175.

[2] Даминов Д.Ф., Гареева Э.Р. Способ совершения преступления: понятие, виды, характеристика // Юридическая наука в XXI веке: сборник научных статей по итогам работы международного круглого стола. 2018. С. 89-90.

Стержень привлекательности для злоумышленников в осуществлении трансакций составляют такие возможности как: дистанцированность с жертвой, быстрота трансакции, анонимизация трансакции. Для дистанционных хищений характерен особенный вид предмета противоправного деяния, а именно – цифровая информация, которая благодаря системам банковского обслуживания является эквивалентом электронных денежных средств. Соответственно, доминантную задачу преступника в рамках реализации преступного умысла из корыстных побуждений составляют действия по применению этих самых систем. Кроме того, захват электронных денежных средств позволяет в последующем оперативно конвертировать их в наличные денежные средства, иностранную валюту, биткоины и т.д.

Рассмотрим конкретные виды способов совершения дистанционных хищений исходя из выше обозначенных дифференцированных признаков.

Так, при обеспечении доступа к банковскому счету жертвы злоумышленник нацелен либо на самостоятельное управление ее банковским счётом, либо на убеждение жертвы самостоятельно перевести денежные средства злоумышленнику. Начало данных отношений возможно с момента осуществления непосредственного контакта либо с потерпевшим, либо с его банковским счётом. Во втором случае при контакте с банковским счетом нами подразумевается контакт также с физическими носителями, посредством которых возможен такой контакт – сотовый телефон, компьютер, банковская карта и т.д. Исходя из сказанного доступ к управлению банковским счётом может быть получен как посредством хищения носителя, позволяющего осуществить трансакцию, так и путем удаленного программного взлома этих же устройств. Кроме того, в качестве альтернативного пути злоумышленник использует потерпевшего как технического проводника в осуществлении трансакции с помощью прямого убеждения (злоупотребление доверием и т.д.), а также использования закамуфлированных приложений и сайтов. Важно понимать, что преступники отрабатывают специальные алгоритмы диалогов и визуальных маркеров, позволяющих внушить жертве правомерность

реализации трансакции в пользу преступника, либо то, что сайт или приложение являются официальными. Алгоритмы диалогов направлены на снижение способности жертвы ставить под сомнение совершение своих же действий в пользу преступника на основе использования специфического понятийного аппарата, убедительности умозаключений, а также установления психологического контакта с жертвой. Алгоритмы визуальных маркеров концентрируют свое действие на иллюзорность безопасности «поддельных» страниц сети Интернет или программ (приложений).

Теперь стоит рассмотреть, каким образом реализуются трансакции при дистанционных хищениях. В рамках данной операции ключевым действием является факт перевода денежных средств на счет преступника. Реализация трансакции возможна несколькими способами:

1) преступник получил физический доступ к устройству потерпевшего с предустановленным банковским приложением или услугой «Мобильный банк», либо к его банковской карте, после чего осуществил трансакцию со счёта;

2) потерпевший самостоятельно перевел денежные средства со своего счёта, на счёт преступника, введя указанные им реквизиты в банковском приложении или воспользовавшись другим схожим способом (например, обратившись напрямую к сотрудникам банка, или воспользовавшись подключенной услугой «Мобильный банк»);

3) потерпевший предоставил преступникам все необходимые реквизиты своей банковской карты или счёта, а также присланный из банка push-код;

4) преступники похитили необходимые реквизиты банковской карты или счёта потерпевшего, а также код от банка из SMS-сообщения, либо получили удаленный доступ к устройству потерпевшего с предустановленным банковским приложением[1].

Считаем этап подготовки и этап сокрытия следов преступления с

[1] Пудовиков А.С., Ненашев Е.В. Структура типичного способа совершения хищений с банковских счетов в отношении и (или) с помощью электронных денежных средств // Право и государство: теория и практика. 2021. № 12 (204). С. 292-295.

криминалистического аспекта при исследовании дистанционных хищений темой для обособленного научного осмысления, поэтому в рамках данного параграфа рассматривался непосредственно этап совершения преступления.

В качестве вывода к параграфу необходимо отметить, что, исследуя динамику и структуру дистанционных хищений, мы пришли к выводу о росте количества обозначенных преступлений как в Российской Федерации, в целом, так и на территории Ашинского муниципального района, в частности, за период с 2018 по 2022 года. В структуре дистанционных хищений преобладают мошенничества и кражи с банковского счета, а равно в отношении электронных денежных средств. С учетом территориального аспекта исследования выпускной квалификационной работы, важно обозначить, что преступления, квалифицируемые по ст. 159.3 и ст. 159.6 УК РФ, на территории Ашинского муниципального района не совершались за исследуемый период. Кроме того, достаточно низким остается коэффициент раскрываемости исследуемых преступлений. Так, в России, в среднем, раскрываемость дистанционных хищений составляет 18,01 %, а на территории Ашинского муниципального района – 11,94 %. Указанные коэффициенты раскрываемости свидетельствует не только о проблемах расследования, но и об отсутствии следственного опыта по расследованию дистанционных хищений. Понимая, какой объем и какие именно преступления составляют дистанционные хищения, в том числе с учетом территориального аспекта дипломного проектирования, важно понимать, что способ совершения преступления сводится к выражению определенной последовательности действий, запланированной для достижения противоправной цели лицом или лицами, реализующими преступный умысел. Способы совершения дистанционных хищений исследованы на основе характерных свойств этой группы преступлений: обеспечение доступа к банковскому счёту потерпевшего и осуществление трансакции. При обеспечении доступа к банковскому счету жертвы злоумышленник нацелен либо на самостоятельное управление ее банковским счётом, либо на убеждение жертвы самостоятельно перевести денежные средства злоумышленнику.

Доступ к управлению возможен либо через физическое хищение носителя цифровой информации, либо программного взлома этих носителей. Также распространен способ прямого убеждения жертвы в производстве трансакции. Способы реализации трансакции дифференцируются на: физический доступ к устройству потерпевшего, самостоятельный перевод денежных средств преступнику, самостоятельное предоставление жертвой преступникам информации, похищение необходимых реквизитов банковской карты или счёта потерпевшего, либо удаленный доступ к устройству потерпевшего.

§ 3. Анализ факультативных элементов криминалистической характеристики хищений, совершаемых с использованием информационных технологий

Считаем, что для развернутости криминалистической картины дистанционных хищений она должна быть дополнена следующими элементами: личность преступника, личность потерпевшего, обстановка.

Для выявления личности типичного преступника, совершающего дистанционные хищения, нами проанализированы данные ИЦ ГУ МВД России по Челябинской области. Так, за период наблюдения с 2018 по 2022 года следователями указанного территориального органа внутренних дел было выявлен 61 преступник, совершивший дистанционное хищение.

Анализ гендерной характеристики преступников, совершивших дистанционное хищение на территории Ашинского района, показал, что 91,8 % из них были мужчинами[1].

Возрастная характеристика выявила следующую структуру преступников, совершивших дистанционное хищение на территории Ашинского района. Так, доля лиц в дифференцированной возрастной категории от 18 до 24 лет составляет 18,0 %, от 25 до 29 лет – 13,1 %, от 30 до 39 лет –

[1] Аналитические справки деятельности ОМВД России по Ашинскому району за 2018, 2019, 2020, 2021, 2022 года, предоставленные ИЦ ГУ МВД России по Челябинской области.

19,7 %, от 40 до 49 лет – 26,2 %, старше 50 лет – 23 % (Приложение 6)[1].

Таким образом, анализ графика, представленного в Приложении 6, показал, что основной возраст преступников, совершающих дистанционные хищения, составляет группа старше 40 лет – около половины всех преступников. Вместе с тем, самой незначительной группой является возраст от 25 до 29 лет, когда молодые люди находятся в самом работоспособном возрасте.

Рассмотрим структуру социального статуса преступников, совершивших дистанционное мошенничество. Так, почти половину всех преступников составляют лица без определенного источника доходов – 49,2 %, рабочие – 27,9 %, служащие – 3,3 %, предприниматели – 3,3 %, пенсионеры – 4,9 %, иные категории – 11,5 % (Приложение 7)[2].

Таким образом, из анализа диаграммы, представленной в Приложении 7, следует, что каждое второе дистанционное хищение совершают лица без постоянного источника дохода, а каждое третье – рабочие.

Изучая национальность преступников, совершивших исследуемую группу преступлений, с учетом географического расположения Ашинского района Челябинской области в близи Республики Башкортостан и Республики Татарстан нами выделены следующие национальности: русские, которые составляют 78,7 % от общего количества преступников, башкиры – 13,1 % от общего количества преступников, татары – 1,6 %, украинцы, грузины и иные составили 6,6 % (Приложение 8)[3]. Указанные данные позволяют сделать вывод о преобладающей доле русской национальности среди преступников, совершающих дистанционные хищения, что коррелирует с национальной структурой всей Российской Федерации. Кроме того, данный факт позволяет понимать, что злоумышленники хорошо говорят по-русски, умело оперируя

[1] Аналитические справки деятельности ОМВД России по Ашинскому району за 2018, 2019, 2020, 2021, 2022 года, предоставленные ИЦ ГУ МВД России по Челябинской области.

[2] Аналитические справки деятельности ОМВД России по Ашинскому району за 2018, 2019, 2020, 2021, 2022 года, предоставленные ИЦ ГУ МВД России по Челябинской области.

[3] Аналитические справки деятельности ОМВД России по Ашинскому району за 2018, 2019, 2020, 2021, 2022 года, предоставленные ИЦ ГУ МВД России по Челябинской области.

алгоритмами диалогов.

Также необходимыми данными для моделирования типичной личности преступника, совершающего дистанционные хищения, необходимо указать, что по данным ИЦ ГУ МВД России по Челябинской области, среди выявленных преступлений в группе совершается 8,2 % дистанционных хищений[1]. Вместе с тем, следует понимать, что указанный признак может быть не объективным в связи с низкой раскрываемостью исследуемого вида преступлений. Действительно выявление групповой и организованной преступности в области дистанционных хищений – сложный и многогранный процесс, который зависит от уровня профессионализма следователя, а, так как дистанционные хищения достаточно молодой вид преступлений, кроме того, динамично развивающийся в способах совершения, то у современных следователей еще не наработан должный следственный опыт для высокого уровня раскрываемости и, соответственно, обмена опытом между собой.

Из выявленных лиц согласно отчету ИЦ ГУ МВД России по Челябинской области каждый второй преступник, совершающий дистанционные хищения, ранее совершал преступления – 55,7 % от общего числа выявленных лиц. Кроме того, понимая, что для совершения дистанционных мошенничеств злоумышленнику нужны навыки работы с техническими и программными средствами, обозначим, что уровень образования большинства исследуемой группы преступников в Ашинском районе Челябинской области средний специальный уровень – 62,3 %[2].

Рассматривая личность жертвы от хищений с использованием информационных технологий, следует их дифференцировать по признаку отношений «преступник-жертва». Так, согласно отчету ИЦ ГУ МВД России по Челябинской области часть дистанционных хищений на территории Ашинского района совершается знакомыми в отношении знакомых, в ряде случаев,

---

[1] Аналитические справки деятельности ОМВД России по Ашинскому району за 2018, 2019, 2020, 2021, 2022 года, предоставленные ИЦ ГУ МВД России по Челябинской области.

[2] Аналитические справки деятельности ОМВД России по Ашинскому району за 2018, 2019, 2020, 2021, 2022 года, предоставленные ИЦ ГУ МВД России по Челябинской области.

родственников в отношении родственников. Другую группу жертв составляют потерпевшие, которые не знакомы с преступником, не видели его, в некоторых случаях даже не разговаривали (например, при хищении данных банковского счета с помощью вредоносного программного обеспечения). Поэтому типичную личность жертвы в первом случае, когда речь идет об отношениях знакомства «преступник-жертва», составляют следующие признаки: женщина, в возрасте старше 40 лет, состоящая в семейных отношениях (супруг, дети, внуки), со средним специальным образованием, злоупотребляющая алкоголем. Типичную личность жертвы во втором случае, когда речь идет о незнакомцах в отношении «преступник-жертва», составляют следующие признаки: мужчина, в возрасте старше 50 лет, состоящий в семейных отношениях (супруг, дети, внуки), со средним специальным образованием, злоупотребляющий алкоголем[1].

Для расследования также важно, какое место считать местом преступления, что позволит не только соблюсти процессуальные требования, но и выполнить организационно-тактические рекомендации производства отдельных следственных действий. Так, кражу, ответственность за которую предусмотрена пунктом «г» части 3 статьи 158 УК РФ, следует считать оконченной с момента изъятия денежных средств с банковского счета их владельца или электронных денежных средств, в результате которого владельцу этих денежных средств причинен ущерб. Исходя из особенностей предмета и способа данного преступления местом его совершения является, как правило, место совершения лицом действий, направленных на незаконное изъятие денежных средств (например, место, в котором лицо с использованием чужой или поддельной платежной карты снимает наличные денежные средства через банкомат либо осуществляет путем безналичных расчетов оплату товаров или перевод денежных средств на другой счет). Местом совершения мошенничества, состоящего в хищении безналичных денежных средств, исходя из особенностей предмета и способа данного преступления, является, как

[1] Аналитические справки деятельности ОМВД России по Ашинскому району за 2018, 2019, 2020, 2021, 2022 года, предоставленные ИЦ ГУ МВД России по Челябинской области.

правило, место совершения лицом действий, связанных с обманом или злоупотреблением доверием и направленных на незаконное изъятие денежных средств[1].

Исходя из выявленного понятия места преступления следует указать, что обстановка совершения исследуемой группы преступлений не существенна при выборе злоумышленником способа совершения дистанционного хищения. Вместе с тем, отметим, что под обстановкой совершения хищения с помощью информационных технологий ученые называют электронную платежную систему или банковскую систему, т.е. фактически место хранения имущества пользователя, обладающее специфическими условиями его хранения[2].

В качестве вывода к параграфу необходимо отметить, что типичная личность преступника, совершающего дистанционные мошенничества в Ашинском районе Челябинской области, состоит из следующих характеристик: мужчина, в возрасте старше 40 лет, без определенного источника доходов, либо рабочий, со средним специальным уровнем образования, по национальности русский, ранее совершавший преступления, не состоящий в зарегистрированном браке, однако, имеющего отношения сожительства.

Типичную личность жертвы дистанционных хищений в Ашинским районе в первом случае, когда речь идет об отношениях знакомства «преступник-жертва», составляют следующие признаки: женщина, в возрасте старше 40 лет, состоящая в семейных отношениях (супруг, дети, внуки), со средним специальным образованием, злоупотребляющая алкоголем. Типичную личность жертвы дистанционных хищений в Ашинским районе во втором случае, когда речь идет о незнакомцах в отношениях «преступник-жертва», составляют следующие признаки: мужчина, в возрасте старше 50 лет, состоящий в семейных отношениях (супруг, дети, внуки), со средним

---

[1] О внесении изменений в некоторые постановления Пленума Верховного Суда Российской Федерации по уголовным делам: постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. № 38 // Российская газета. № 294. 2022.

[2] Кардашевская М.В., Гаврилин Ю.В. Электронная платежная система как элемент обстановки преступления // Академическая мысль. 2020. № 2 (11). С. 21-23.

специальным образованием, злоупотребляющий алкоголем.

Место преступления определено рекомендациями Верховного Суда РФ, которые нами полностью поддерживаются, а именно – место совершения лицом действий, направленных на незаконное изъятие денежных средств, либо связанных с обманом или злоупотреблением доверием с той же целью. Мы также поддерживаем мнение тех ученых-криминалистов, которые под обстановкой совершения дистанционных мошенничеств понимают электронную платежную систему или банковскую систему, т.е. фактически место хранения имущества пользователя, обладающее специфическими условиями его хранения. Механизм следообразования при совершении дистанционных хищений напрямую зависит от специфичности способа совершения противоправного деяния и обусловлен существованием информационных или цифровых следов.

Понимая комплекс признаков и элементов криминалистической характеристики дистанционных хищений на примере Ашинского района Челябинской области, в следующей главе выпускной квалификационной работы мы рассмотрим организационно-тактические особенности расследования исследуемой группы хищений.

ГЛАВА 2. ОРГАНИЗАЦИОННО-ТАКТИЧЕСКИЕ ОСОБЕННОСТИ РАССЛЕДОВАНИЯ ХИЩЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

§ 1. Производство доследственной проверки и возбуждение уголовных дел о хищениях, совершаемых с использованием информационных технологий

Для достижения целей уголовного судопроизводства необходимо качественное производство предварительного расследования, результаты которого создадут основу для обвинения и принятия судом решения о виновности или невиновности обвиняемых лиц. Однако качество самого предварительного расследования во многом зависит не только от профессионализма органов предварительного расследования, но и от производства доследственной проверки и принятия решения о возбуждении уголовного дела или отказе в его возбуждении.

Данный параграф посвящен действиям следователя и органа дознания на стадии возбуждения уголовного дела по факту дистанционных хищений.

Доследственная проверка начинается с момента получения сообщения о происшествии и ее итоговым решением является решение о возбуждении уголовного дела, либо решение об отказе в возбуждении уголовного дела. При получении сообщения о совершенном хищении электронных денежных средств деятельность расследующих органов должна быть направлена на установление не только места совершения дистанционного хищения, но и иных мест, имеющих связь с совершенным противоправным деянием. Так, важно определить:

– место удаленного доступа к ресурсам банка;

– место проживания лица, совершившего преступление;

– место проживания потерпевшего;

– место нахождения подразделения банка, в котором открыт и обслуживается счет потерпевшего;

– место нахождения подразделения банка, в котором обслуживается счет, на который были переведены похищенные денежные средства[1].

Зачастую указанные места, имеющие отношение к дистанционному хищению, не совпадают и могут находится на совершенно разных районах муниципального образования или населенного пункта.

Определение места совершения преступления важно для оперативности принимаемых решений органами внутренних дел «по горячим следам», когда возможна «заморозка» похищенных средств на расчетном счете с последующим возвращением владельцу. Кроме того, установление места преступления позволит избежать волокиты с передачей по территориальной подследственности материалов уголовного дела, что значительно снижает оперативность и эффективность расследования.

Совокупность действий должностного лица, производящего предварительную проверку сообщения о дистанционном хищении, можно представить в следующем алгоритме:

1. Опрос заявителя. В рамках данного действия следует учитывать такие особенности как:

– условия стресса могут стать помехой для жертвы вспомнить все детали произошедшего, в том числе, адреса, приметы и т.д.;

– отсутствие регламентации сроков хранения видеозаписей с камер наблюдения банков и иных финансовых организаций;

– перегруженный по времени механизм предоставления необходимой информации из банка и иных финансовых организаций по запросу следователя. Решением этого проблемного вопроса может быть получение потерпевшим указанных данных самостоятельно с последующим совместным анализом полученной информации со следователем.

---

[1] Ордоков М.Х., Шафиева Э.Т., Карданов А.К. Основные тенденции борьбы с кибермошенничеством // Пробелы в российском законодательстве. 2021. № 4. С. 108-111.

2. Истребование у заявителя мобильного устройства или компьютера с установленными на них программами банковских услуг.

3. Назначение судебной экспертизы. Наиболее информативными могут быть:

– идентификационная автороведческая экспертиза по материалам письменных (печатных) сообщений;

– идентификационная фоноскопическая экспертиза по материалам устных (голосовых) сообщений;

– лингвистическая экспертиза по материалам письменных и устных сообщений;

– компьютерно-техническая экспертиза[1].

Несомненно, круг вопросов по каждому виду экспертиз различается, но вся экспертная деятельность должна быть направлена не только на сбор и анализ первичной информации, но и в условиях, если виновное лицо уже установлено, на проверку выдвинутой версии о вине установленного лица.

Кроме того, на стадии проверки сообщения о преступлении эксперт может ответить на такие вопросы:

1) имеются ли на аппаратных средствах представленного мобильного устройства или компьютера файлы, детектируемые антивирусными программами?

2) имеются ли на аппаратных средствах представленного мобильного устройства или компьютера программы дистанционного банковского обслуживания?

3) имеются ли данные, указывающие на возможные случайные ошибки, связанные с вводом, удалением, блокированием, модификацией информации в работе программного обеспечения представленных на исследование объектов?

---

[1] Грачев С.А., Крюкова А.С. Проверка сообщений о мошенничестве в сети интернет и принятие решения о возбуждении уголовного дела // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2022. № 2 (91). С. 164-171.

Если да, то можно ли установить причину этих ошибок?[1]

4. Направление сотрудниками оперативного подразделения в суд постановления о возбуждении ходатайства об ограничении прав граждан на банковскую тайну. Данное мероприятие необходимо для сбора информации о списании денежных средств, о счетах заявителя и злоумышленника, об IP-адресах злоумышленников или лиц, с ними связанных.

5. Определение IP-адресов злоумышленников и необходимой информации у провайдера, его предоставившего.

6. Наведение справок о лицах, установленных в ходе предыдущего шага.

Результатом проведенной проверки по сообщению о дистанционном хищении является подтверждение повода и основания для возбуждения уголовного дела, либо факты не подтверждаются. В последнем случае выносится отказ в возбуждении уголовного дела, а в первом случае должностное лицо, проводившее проверку, направляет все материалы в следственные органы для возбуждения уголовного дела.

При этом материалы должны содержать всю информацию, перечисленную выше, в том числе:

1) время и место удаленного доступа к данным банка и факта списания денежных средств, их зачисления на другой счет;

2) наименование банков и номера задействованных счетов;

3) данные о заявителе, размер похищенных денежных средств, и значительность их ущерба;

4) IP-адреса злоумышленников и провайдер, их обслуживающий;

5) Лицо, которому выделен IP-адрес, и принадлежит адрес подключения модема или иных технических средств.

Основной организационной проблемой на данном этапе является

---

[1] Бирюкова Ю.В. Проблемы компьютерно-технической экспертизы в процессе расследования хищений, совершенных с использованием компьютерных и телекоммуникационных технологий // Актуальные проблемы экспертно-криминалистической деятельности: сборник научных трудов Международной конференции. Сост. В.В. Бушуев. Москва, 2021. С. 67-70.

временной фактор, не позволяющий оперативно собрать вышеуказанную информацию из запросов юридическим лицам, в том числе, банках, провайдерам и т.д.

Вместе с тем, какая-то часть уголовных дел возбуждается лишь по одному заявлению потерпевшего и выписки о движении денежных средств на счете. Это можно объяснить слишком долгими ответами на запросы в организации. В результате эти ответы приходят уже после возбуждения уголовного дела.

В качестве вывода к параграфу необходимо отметить, что объем информации, выявленный и проанализированный на этапе доследственной проверки, позволяет принять решение и наличие повода и основания к возбуждению уголовного дела, либо отказе в таком возбуждении. Итак, по делам о совершенных дистанционных хищениях начало проверки сообщения заявителя начинается с определения места совершения хищения электронный денежных средств, а также тех мест, которые имеют связь с совершенным противоправным деянием. В параграфе последовательно раскрыта совокупность действий должностного лица, производящего предварительную проверку сообщения о дистанционном хищении, которую можно представить в следующем алгоритме: опрос заявителя, истребование у заявителя мобильного устройства или компьютера с установленными на них программами банковских услуг, назначение судебной экспертизы, направление сотрудниками оперативного подразделения в суд постановления о возбуждении ходатайства об ограничении прав граждан на банковскую тайну, определение IP-адресов злоумышленников и необходимой информации у провайдера, его предоставившего, наведение справок о злоумышленниках. Совокупность собранной информации в рамках данного алгоритма действий позволяет передать материалы в следственные органы с последующим принятием решения о возбуждении уголовного дела. При затягивании банками, провайдерами и иными юридическими лицами сроков сбора необходимой информации по выполненным запросам поводом к возбуждению уголовного дела является заявление потерпевшего и выписка о движении денежных средств на счете.

§ 2. Характерные следственные ситуации и составление плана расследования хищений, совершаемых с использованием информационных технологий

Выявленная информация на этапе возбуждения уголовного дела позволяет оценить сложившуюся следственную ситуацию и выдвинуть следственные версии, которые проверяются последовательным выполнением плана расследования.

Анализ данных, представленных ИЦ ГУ МВД России по Челябинской области, по совершенным хищениям с помощью информационных технологий за последние пять лет с 2018 по 2022 года, позволил выделить две исходные следственные ситуации.

Рассмотрим первую следственную ситуацию на примере из следственной практики ОМВД России по Ашинскому району, когда совершено дистанционное хищение, преступник неизвестен.

Так, гр. Н., решил приобрести рыболовные снасти в интернет-магазине. Зайдя на интернет-сайт магазина «Рыболовный *», гр. Н. выбрал необходимый товар и совершил оплату-онлайн в интернет-форме, где ввел данные своей банковской карты и смс-код с подтверждением оплаты. С банковского счета гр. Н. была списана сумма 21560 рублей. По прошествии двух дней, не дождавшись звонка от оператора интернет-магазина по вопросам отгрузки товара, гр. Н. позвонил на горячую линию интернет-магазина, где никто не взял трубку. Гр. Н. обратился в полицию[1].

Вторая следственная ситуация представляет собой совершение дистанционного хищения с последующим установлением и задержанием преступника в результате ОРМ и следственных действий.

Так, у гр. К., находившегося в состоянии алкогольного опьянения, возник корыстный умысел на завладение электронными денежными средствами его

[1] Материалы уголовного дела, возбужденного 27 декабря 2022 г. ОМВД России по Ашинскому району по факту дистанционного хищения денежных средств с банковской карты гр. П.

бабушки гр. П. Имея информацию о том, что банковский счет, принадлежащий гр. П., обслуживается с помощью услуги «Мобильный банк» на мобильном ее телефоне. Действуя тайно, гр. К. взял мобильный телефон гр. П. и совершил перевод денежных средств на банковский счет, принадлежащий гр. К. В результате гр. П. был причинен материальный ущерб на сумму 5500 руб. Потерпевшая гр. П. узнала о похищении электронных денежных средств через сутки и заявила в полицию. В результате проведенных оперативно-розыскных мероприятий гр. К. был установлен и задержан[1].

Сложившаяся следственная ситуация является фундаментом дальнейшего планирования первоначальных и последующих следственных действий. Планирование расследования можно дифференцировать на следующие операции:

– анализ имеющейся информации;

– выдвижение следственных версий и установление задач расследования;

– определение путей и способов решения задач;

– составление письменного плана предварительного расследования.

Итак, анализ информации, которая состоит из данных о предмете преступления, способе хищения, личности потерпевшего, месте и времени совершения преступления, позволяет выдвинуть следственные версии.

Выдвигая следственные версии исходя из объема имеющейся информации, следует комбинировать версии о наличии или отсутствии самого события преступления, личности преступника и его мотивах, об иных обстоятельствах преступления, которые могут иметь значение для расследования.

При производстве предварительного расследования подлежат доказыванию такие обстоятельства, как:

– событие преступления (время, место, способ совершения преступления);

---

[1] Приговор Ашинского городского суда № 1-102/2020 от 22 апреля 2020 г. по делу № 1-102/2020. URL:// https://sudact.ru/ (дата обращения: 28.01.2023).

– виновность лица в совершении преступления, форма его вины и мотивы;

– обстоятельства, характеризующие личность обвиняемого;

– характер и размер вреда, причиненного потерпевшему;

– обстоятельства, исключающие преступность и наказуемость деяния;

– обстоятельства, смягчающие и отягчающие наказание;

– обстоятельства, которые могут повлечь за собой освобождение от уголовной ответственности и наказания;

– обстоятельства, способствовавшие совершению преступления.

Третья операция планирования предназначена в выборе стратегии проверки выдвигаемых следственных версий. Несомненно, при динамичности самого процесса предварительного расследования и результатов последовательно проводимых следственных действий следователь может варьировать комплекс мероприятий и алгоритм основных процессуальных действий. Так, комплекс следственных действий, направленных на проверку выдвинутых версий о дистанционных хищениях, составляют:

– допрос потерпевшего, свидетелей;

– осмотр, выемка и приобщение документов (иных объектов) в качестве доказательств;

– обыск с привлечением специалистов по месту нахождения лиц, возможно имеющих отношение к дистанционному хищению;

– опознание свидетелями держателя карты как лица, имеющего отношение к дистанционному хищению;

– допрос подозреваемого (обвиняемого).

Кроме того, важно план расследования по указанной группе преступлений визуализировать схемой движения денежных средств.

Основное предназначение операции по составлению письменного плана расследования заключается в проверке выдвинутых версий. Каждое действие в указанном плане имеет срок выполнения и ответственное лицо.

Орган дознания должен непосредственным образом взаимодействовать со

следователем в планировании расследования. Это необходимо для повышения эффективности и четкости распределения всех действий.

Нами поддерживается мнение ученых-криминалистов о необходимости экспертного и специального сопровождения расследования с момента получения сообщения о дистанционном хищении до направления материалов уголовного дела в суд[1]. Особенно важна профессиональная роль специалистов в области компьютерных технологий и программ. От их знаний зависит полнота и качество собранной доказательственной базы по уголовному делу. Конкретные задачи, которые ставятся перед специалистом должны быть внесены в план расследования с указанием времени их исполнения.

Особое внимание нужно акцентировать на проблемах, возникающих при обращении к провайдерам финансовых услуг (кредитные организации, платежные системы, где фиксируются данные о владельцах счетов, дате и времени совершения операций, сведения о дате и времени интернет-соединений и IP-адресах, с которых осуществлялись выходы в сеть). Основы правового государства, курса на которые придерживается постсоветская Россия, не позволяют требовать от указанных организаций предоставления сведений в правоохранительные органы в кратчайшие сроки. Поэтому взаимоотношения органов власти и провайдеров финансовых услуг выстраиваются на основе метода убеждения. Налаживание связей способствует повышению оперативности ответов на запросы, снижению промедлений со стороны организаций, которые могут привести к безвозвратной утере или уничтожению значимых сведений[2]. Считаем в качестве предложения налаживания связей между правоохранительными органами и провайдерами финансовых услуг отметить проведение встреч с повесткой о взаимодействии, а

---

[1] Решняк О.А., Ковалев С.А. Организация расследования мошенничеств, совершенных с использованием сети «Интернет», на первоначальном и последующем этапах // Вестник Волгоградской академии МВД России. 2020. № 2 (53). С. 106-111.

[2] Камчатов К.В. Модернизация порядка оперативного получения сведений при раскрытии и расследовании преступлений, совершаемых с использованием информационно-коммуникационных технологий, в целях обеспечения прав потерпевших // Вестник Волжского университета им. В.Н. Татищева. 2022. Т. 1. № 2 (101). С. 206-216.

также межведомственных круглых столов по обмену опытом по установлению связей с указанными организациями.

В результате проведенных процессуальных и следственных действий следователем выбирается та следственная версия, которая подтвердилась. Соответственно, дальнейшие действия следователя направлены на сбор доказательств, которые не проверяют, а утверждают выбранную версию.

В качестве вывода к параграфу отметим, что планирование расследования можно представить в виде совокупности следующих операций: анализ имеющейся информации; выдвижение следственных версий и установление задач расследования; определение путей и способов решения задач; составление письменного плана предварительного расследования. При этом, оценка сложившейся следственной ситуации и выдвижение следственных версий происходят на основе выявленного объема информации, в том числе в рамках доследственной проверки. Анализ данных, представленных ИЦ ГУ МВД России по Челябинской области, по совершенным хищениям с помощью информационных технологий за последние пять лет с 2018 по 2022 года, позволил выделить две исходные следственные ситуации: 1) совершено дистанционное хищение, преступник неизвестен, 2) совершено дистанционное хищение с последующим установлением и задержанием преступника в результате ОРМ и следственных действий. Выдвинув следственные версии на основе вариаций имеющихся данных, следователь приступает к выбору стратегии проверки этих версий. Комплекс следственных действий, направленных на проверку выдвинутых версий о дистанционных хищениях, составляют: допрос потерпевшего, свидетелей; осмотр, выемка и приобщение документов (иных объектов) в качестве доказательств; обыск с привлечением специалистов по месту нахождения лиц, возможно имеющих отношение к дистанционному хищению; опознание свидетелями держателя карты как лица, имеющего отношение к дистанционному хищению; допрос подозреваемого (обвиняемого). Операция по составлению письменного плана расследования заключается в указании каждого действия, его сроков и исполнителя. Нами

поддерживаются предложения ученых-криминалистов о должном специальном обеспечении предварительного расследования в целях повышения эффективности расследования, а также о проведении встреч с повесткой о взаимодействии правоохранительных органов и провайдеров финансовых услуг, а также межведомственных круглых столов по обмену опытом по установлению связей с указанными организациями.

§ 3. Тактические особенности производства отдельных следственных действий при расследовании хищений, совершаемых с использованием информационных технологий

Информация, полученная на стадии возбуждения уголовного дела, представляет собой базу для производства предварительного расследования. Несомненно, от качества этого объема информации зависит понимание следственных ситуаций и выбор направления версий. В предыдущем параграфе на основе анализа данных ИЦ ГУ МВД России по Челябинской области мы выявили две типичные следственные ситуации, которые, как правило, предполагают последовательный набор следственных действий. В данном параграфе раскроем тактические особенности производства некоторых из них, а также проблематику предварительного расследования хищений, совершаемых с использованием информационных технологий.

Итак, по каждому уголовному делу, возбуждаемому в рассматриваемом территориальном органе, производится, как правило, осмотр места происшествия, назначение экспертиз и допрос.

Допрос является одним из важнейших элементов комплекса первоочередных следственных действий, которые проводятся на начальном этапе расследования любого преступления, в т. ч. и расследования хищений денежных средств с электронных счетов.

Носителем значительного количества информации, имеющей существенное значение для расследования хищений электронных денежных

средств, совершаемых в сфере функционирования электронных расчетов, является подозреваемый. Готовясь к проведению допроса этого процессуального лица, следователь должен определить: предмет допроса; доказательства и материалы, которые могут быть использованы для его разоблачения; последовательность проведения допросов при наличии нескольких подозреваемых; сформулировать вопросы и определить их порядок и последовательность.

Определение таких данных, а также успех допроса будет возможен только при условии участия в нем специалиста в области информационных технологий, специалиста-бухгалтера, системного инженера, а также специалиста по банковскому делу. В ходе допроса с разрешения следователя специалисты могут задавать допрашиваемому уточняющие и конкретизирующие вопросы, обращать внимание следователя на замеченные неточности и несоответствия в ответах допрашиваемого на поставленные вопросы.

Организация и проведение допросов по делам о хищениях, совершаемых при осуществлении электронных расчетных операций, с использованием конфиденциальных данных о реквизитах настоящих платежных карточек, требует от следователя не только знания и соблюдения процессуальных норм, но и применения соответствующих тактических приемов допроса. Необходимым условием надлежащей подготовки к проведению допросов по данной категории дел является анализ следственной ситуации, знание психологических особенностей допрашиваемого, создание мысленной модели возможной линии его поведения с целью защиты своих интересов. Содержание вопросов и их форма всегда должны соответствовать интеллектуальному уровню, знаниям и особенностям мышления допрашиваемых, быть краткими, точными и иметь логическую структуру. Полученные ответы требуют всестороннего исследования и тщательной проверки.

Важность осмотра заключается в том, что это единственное, неотложное следственное действие, которое проводится незамедлительно и

безотлагательно, как правило, на начальной стадии расследования, и имеет большое значение для раскрытия и расследования преступлений.

Важно отметить, что содержательное наполнение осмотра, по сути, необходимо соотносить с личным восприятием, изучением и фиксацией части определенной окружающей действительности. К таким частям действительности следует относить окружающую обстановку, предметы, вещи, телефоны, персональные компьютеры и их программное содержание. Таким образом, следует согласиться с теми исследователями, которые отмечают, что осмотр при расследовании рассматриваемых преступлений является самым необходимым следственным действием. Именно в рамках него собирается самый значительный массив доказательственной информации по будущему уголовному делу, связанному с хищениями, совершенными с использованием информационных технологий[1].

С учетом мнения ученых, а также анализа следственной практики, считаем возможным предложить следующие рекомендации, направленные на повышения качества расследования по делам данной категории:

– в состав СОГ в обязательном порядке должны входить такие участники как: следователь; оперуполномоченный; специалист-криминалист, а также в качестве специалистов рекомендуется приглашать специалиста в области информационных технологий, специалиста-бухгалтера, системного инженера, а также специалиста по банковскому делу;

– как при подготовке к осмотру места происшествия, так и к осмотру предметов следователь должен предусмотреть целесообразность использования специальных средств и программных продуктов. Как правило, это осуществляется путем проверки их наличия у специалиста. Например, при осмотре банковской карты электронную информацию можно получить при наличии определенного терминала;

– в случае обнаружения каких-либо пластиковых карт, мобильных

[1] Шитикова Ю.И. Особенности криминалистического обеспечения расследования мошенничеств, совершенных дистанционным способом // Альманах молодого исследователя. 2020. № 9. С. 131-134.

устройств, POS-терминалов, принтеров, документов и т.д. обязательным является отражение в протоколе их индивидуальных признаков (цвет, номер, информация о владельце). В случаях обнаружения оборудования для изготовления пластиковых карт рекомендуется обратиться за помощью к специалистам, чтобы правильно и полностью изъять данное оборудование. Рекомендуется бережно относить к слипам, чекам, поддельным документам, обнаруженным в ходе осмотра или обыска, и предпринять соответствующие меры, направленные на обеспечение их целостности и сохранности, так как, возможно, на их поверхности имеются следы пальцев рук лица, совершившего преступление.

– принять меры по своевременному изъятию документов из автоматизированных охранных систем наблюдения при первичном осмотре участниками СОГ.

При расследовании дистанционных хищений назначаются экспертизы в зависимости от объекта исследования: трасологическая, почерковедческая, технико–криминалистическая экспертиза документов, судебная экспертиза полимерных материалов и изделий, судебная компьютерно–техническая экспертиза, которая, например, проверяет наличие и содержание информации на магнитной полосе карты. Судебная портретная экспертиза проводится с целью идентификации человека по признакам внешности, отобразившимся на фотографиях и других носителях изображений. В качестве объектов могут выступать: фотографии и видеозаписи с камер наружного наблюдения или банкоматов. Целью судебной фоноскопической экспертизы будет являться установление факта перезаписи информации с магнитной полосы подлинной кредитной карты на поддельную и исследования звукозаписывающих устройств[1].

В качестве вывода к параграфу необходимо отметить, что проверка

[1] Максименко А.А., Мамичева И.В. Особенности назначения и производства экспертиз по делам о преступлениях, связанных с использованием систем дистанционного банковского обслуживания // Студенческая научная весна: тезисы докладов Всероссийской студенческой конференции, посвященной 175-летию Н.Е. Жуковского. М., 2022. С. 310-311.

выдвинутых версий на этапе планирования расследования осуществляется на основе проведения следственных и иных процессуальных действий. В рамках расследования уголовных дел, возбужденных в ОМВД России по Челябинской области по факту хищений с использованием информационных технологий, наиболее результативными являются такие следственные действия как: осмотр места происшествия, назначение экспертиз и допрос. Допрос представляет собой диалог между следователем и одним из участников уголовного процесса, чаще всего, это потерпевший, свидетели, подозреваемый. С точки зрения тактики производства допроса самым сложным является допрос подозреваемого, т.к. он зачастую проходит в условиях конфликтности и противоборства. В свете сказанного, рекомендовано следователю тщательно готовиться к производству допроса подозреваемых лиц. Одним из определяющих условий эффективности допроса будет участие специалиста в области информационных технологий, а также иные специалисты с учетом способа совершения дистанционного хищения. Осмотр и осмотр места происшествия являются в делах по дистанционным хищениям неотложными следственными действиями, по результатам которых формируется значительная доказательственная база на основе следов, в том числе цифровых следов преступления. В параграфе содержатся предложения по повышению эффективности производства осмотров при дистанционных хищениях. Качество судебных экспертиз напрямую зависит от вопросов, поставленных перед экспертом. Кроме того, оперативность их проведения напрямую влияет на скорость расследования и принятия решений по корректировке плана расследования исходя из полученных результатов. Считаем перспективным направлением в рамках производства судебных экспертиз – их производство во взаимодействии с организациями банковских услуг, т.к. данный субъект напрямую заинтересован в обеспечении безопасности для счетов своих клиентов.

ЗАКЛЮЧЕНИЕ

В заключение выпускной квалификационной работы еще раз остановимся на выводах, которые были достигнуты в процессе ее написания.

Не смотря на различность подходов в понимании сущности криминалистической характеристики преступлений, нами поддерживается научное мнение о взаимосвязи уголовно-правового и криминологического аспектов с элементами криминалистической характеристики преступлений или групп преступлений. В качестве группы преступлений в рамках данной выпускной квалификационной работы исследовались хищения, совершенные с помощью информационных технологий. Исследованы и выявлены признаки таких хищений: совершение в условиях неочевидности, т.е. преступник и жертва не видят друг друга; предметом всегда являются денежные средства в безналичной или наличной форме; применение преступником средств и устройств, позволяющих в отсутствие личного физического контакта с жертвой и ее деньгами завладеть последними. При этом, преступник находится «на дистанции» от потерпевшего, поэтому мы согласимся с учеными-теоретиками права о универсальном наименовании таких преступлений – «дистанционные хищения». Мы согласимся с законодателем, который в исследуемую группу преступлений включает составы, квалифицируемые по ст. 159 УК РФ, мошенничества с использованием электронных средств платежа, квалифицируемые по ст. 159.3 УК РФ, мошенничества в сфере компьютерной информации, квалифицируемые по ст. 159.6 УК РФ, а также кражи, совершенные с банковского счета, а равно в отношении электронных денежных средств, квалифицируемые по п. «г» ч. 3 ст. 158 УК РФ. На основе предлагаемых научным сообществом определений хищений, совершаемых с использованием информационных технологий, нами разработано авторское понимание искомого понятия, согласно которому под дистанционными хищениями следует понимать общественно-опасное деяние, совершаемое с помощью средств и устройств, позволяющих преступнику в отсутствие личного

физического контакта с жертвой и ее деньгами завладеть последними.

Исследуя динамику и структуру дистанционных хищений, мы пришли к выводу о росте количества обозначенных преступлений как в Российской Федерации, в целом, так и на территории Ашинского муниципального района, в частности, за период с 2018 по 2022 года. В структуре дистанционных хищений на территории Ашинского муниципального района преобладают мошенничества и кражи с банковского счета, а равно в отношении электронных денежных средств. Достаточно низким остается коэффициент раскрываемости исследуемых преступлений. Так, в России, в среднем, раскрываемость дистанционных хищений составляет 18,01 %, а на территории Ашинского муниципального района – 11,94 %. Указанные коэффициенты раскрываемости свидетельствует не только о проблемах расследования, но и об отсутствии следственного опыта по расследованию дистанционных хищений. Способ совершения преступления сводится к выражению определенной последовательности действий, запланированной для достижения противоправной цели лицом или лицами, реализующими преступный умысел. Способы совершения дистанционных хищений исследованы на основе характерных свойств этой группы преступлений: обеспечение доступа к банковскому счёту потерпевшего и осуществление трансакции. При обеспечении доступа к банковскому счету жертвы злоумышленник нацелен либо на самостоятельное управление ее банковским счётом, либо на убеждение жертвы самостоятельно перевести денежные средства злоумышленнику. Доступ к управлению возможен либо через физическое хищение носителя цифровой информации, либо программного взлома этих носителей. Также распространен способ прямого убеждения жертвы в производстве трансакции. Способы реализации трансакции дифференцируются на: физический доступ к устройству потерпевшего, самостоятельный перевод денежных средств преступнику, самостоятельное предоставление жертвой преступникам информации, похищение необходимых реквизитов банковской карты или счёта потерпевшего, либо удаленный доступ к устройству потерпевшего.

Типичная личность преступника, совершающего дистанционные мошенничества в Ашинском районе Челябинской области, состоит из следующих характеристик: мужчина, в возрасте старше 40 лет, без определенного источника доходов, либо рабочий, со средним специальным уровнем образования, по национальности русский, ранее совершавший преступления, не состоящий в зарегистрированном браке, однако, имеющего отношения сожительства. Типичную личность жертвы дистанционных хищений в Ашинским районе в первом случае, когда речь идет об отношениях знакомства «преступник-жертва», составляют следующие признаки: женщина, в возрасте старше 40 лет, состоящая в семейных отношениях (супруг, дети, внуки), со средним специальным образованием, злоупотребляющая алкоголем. Типичную личность жертвы дистанционных хищений в Ашинским районе во втором случае, когда речь идет о незнакомцах в отношениях «преступник-жертва», составляют следующие признаки: мужчина, в возрасте старше 50 лет, состоящий в семейных отношениях (супруг, дети, внуки), со средним специальным образованием, злоупотребляющий алкоголем. Место преступления определено рекомендациями Верховного Суда РФ. Механизм следообразования при совершении дистанционных хищений напрямую зависит от специфичности способа совершения противоправного деяния и обусловлен существованием информационных или цифровых следов.

Объем информации, выявленной и проанализированной на этапе доследственной проверки, позволяет принять решение на основе наличия повода и основания к возбуждению уголовного дела, либо отказе в таком возбуждении. Итак, по делам о совершенных дистанционных хищениях начало проверки сообщения заявителя начинается с определения места совершения хищения электронный денежных средств, а также тех мест, которые имеют связь с совершенным противоправным деянием. В работе последовательно раскрыта совокупность действий должностного лица, производящего предварительную проверку сообщения о дистанционном хищении, которую можно представить в следующем алгоритме: опрос заявителя, истребование у

заявителя мобильного устройства или компьютера с установленными на них программами банковских услуг, назначение судебной экспертизы, направление сотрудниками оперативного подразделения в суд постановления о возбуждении ходатайства об ограничении прав граждан на банковскую тайну, определение IP-адресов злоумышленников и необходимой информации у провайдера, его предоставившего, наведение справок о злоумышленниках. Совокупность собранной информации в рамках данного алгоритма действий позволяет передать материалы в следственные органы с последующим принятием решения о возбуждении уголовного дела. При затягивании банками, провайдерами сроков сбора необходимой информации по выполненным запросам поводом к возбуждению уголовного дела является заявление потерпевшего и выписка о движении денежных средств на счете.

Планирование расследования можно представить в виде совокупности следующих операций: анализ имеющейся информации; выдвижение следственных версий и установление задач расследования; определение путей и способов решения задач; составление письменного плана предварительного расследования. Анализ данных, представленных ИЦ ГУ МВД России по Челябинской области, по совершенным хищениям с помощью информационных технологий за последние пять лет с 2018 по 2022 года, позволил выделить две исходные следственные ситуации: 1) совершено дистанционное хищение, преступник неизвестен, 2) совершено дистанционное хищение с последующим установлением и задержанием преступника в результате ОРМ и следственных действий. Выдвинув следственные версии на основе вариаций имеющихся данных, следователь приступает к выбору стратегии проверки этих версий. Комплекс следственных действий, направленных на проверку выдвинутых версий о дистанционных хищениях, составляют: допрос потерпевшего, свидетелей; осмотр, выемка и приобщение документов (иных объектов) в качестве доказательств; обыск с привлечением специалистов по месту нахождения лиц, возможно имеющих отношение к дистанционному хищению; опознание свидетелями держателя карты как лица,

имеющего отношение к дистанционному хищению; допрос подозреваемого (обвиняемого). Операция по составлению письменного плана расследования заключается в указании каждого действия, его сроков и исполнителя. Нами поддерживаются предложения ученых-криминалистов о должном специальном обеспечении предварительного расследования в целях повышения эффективности расследования, а также о проведении встреч с повесткой о взаимодействии правоохранительных органов и провайдеров финансовых услуг, а также межведомственных круглых столов по обмену опытом по установлению связей с указанными организациями.

В рамках расследования уголовных дел, возбужденных в ОМВД России по Челябинской области по факту хищений с использованием информационных технологий, наиболее результативными являются такие следственные действия как: осмотр места происшествия, назначение экспертиз и допрос. С точки зрения тактики производства допроса самым сложным является допрос подозреваемого, т.к. он зачастую проходит в условиях конфликтности и противоборства. Одним из определяющих условий эффективности допроса будет участие специалиста в области информационных технологий, а также иных специалистов с учетом способа совершения дистанционного хищения. Осмотр и осмотр места происшествия являются в делах по дистанционным хищениям неотложными следственными действиями, по результатам которых формируется значительная доказательственная база на основе следов, в том числе цифровых следов преступления. В работе содержатся предложения по повышению эффективности производства осмотров при дистанционных хищениях. Оперативность проведения судебных экспертиз напрямую влияет на скорость расследования и принятия решений по корректировке плана расследования исходя из полученных результатов. Считаем перспективным направлением в рамках производства судебных экспертиз – их производство во взаимодействии с организациями банковских услуг, т.к. данный субъект напрямую заинтересован в обеспечении безопасности для счетов своих клиентов.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

I. Нормативные правовые акты и иные официальные документы

1. Конституция Российской Федерации: принята всенародным голосованием 12 декабря 1993 г. [Электронный ресурс]. URL:// http://www.pravo.gov.ru.

2. Уголовный кодекс Российской Федерации: Федер. закон Рос. Федерации от 13 июня 1996 г. № 63-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 24 мая 1996 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 5 июня 1996 г. // Собр. законодательства Рос. Федерации. – 1996. – № 25, ст. 2954.

3. Уголовно-процессуальный кодекс Российской Федерации: Федер. закон Рос. Федерации от 18 декабря 2001 г. № 174-ФЗ принят Гос. Думой Федер. Собр. Рос. Федерации 22 ноября 2001 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 5 декабря 2001 г. // Собр. законодательства Рос. Федерации. – 2001. – № 52, (ч. I), ст. 4921.

4. О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности: указание Генпрокуратуры России № 11/11, МВД России № 1 от 17 января 2023 г. (Перечень № 25) [Электронный ресурс]. URL:// http://www.pravo.gov.ru (дата обращения: 10.02.2023).

5. О внесении изменений в некоторые постановления Пленума Верховного Суда Российской Федерации по уголовным делам: постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. № 38 // Российская газета. № 294. 2022.

II. Учебная, научная литература и иные материалы

1. Бирюкова Ю.В. Проблемы компьютерно-технической экспертизы в процессе расследования хищений, совершенных с использованием компьютерных и телекоммуникационных технологий // Актуальные проблемы

экспертно-криминалистической деятельности: сборник научных трудов Международной конференции. Сост. В.В. Бушуев. Москва, 2021. С. 67-70.

2. Борисова Ю.А. Возникновение и становление понятия криминалистической характеристики преступления // StudNet. 2020. Т. 3. № 3. С. 467-472.

3. Грачев С.А., Крюкова А.С. Проверка сообщений о мошенничестве в сети интернет и принятие решения о возбуждении уголовного дела // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2022. № 2 (91). С. 164-171.

4. Грунина В.А., Новичкова Ю.Г., Ананьина Ю.А. Теоретические основы регулирования юридической ответственности за новые формы интернет-мошенничества в сети «Интернет» // Современная наука: актуальные проблемы теории и практики. Серия: Экономика и право. 2021. № 9. С. 79-84.

5. Даминов Д.Ф., Гареева Э.Р. Способ совершения преступления: понятие, виды, характеристика // Юридическая наука в XXI веке: сборник научных статей по итогам работы международного круглого стола. 2018. С. 89-90.

6. Диденко К.В., Зейналбдыева А.В., Свиридов Р.В. Проблемные вопросы квалификации хищений с использованием информационных технологий // Современный ученый. 2020. № 5. С. 306-310.

7. Евтушенко И.И., Венедиктов А.А. Дистанционные хищения: понятие и признаки // Гуманитарные, социально-экономические и общественные науки. 2020. № 12-2. С. 65-67.

8. Ижунинов М.А. Процесс предупреждения хищения с помощью IT-технологий на настоящий момент // Интеграция наук. 2019. № 2 (25). С. 97-98.

9. Камчатов К.В. Модернизация порядка оперативного получения сведений при раскрытии и расследовании преступлений, совершаемых с использованием информационно-коммуникационных технологий, в целях обеспечения прав потерпевших // Вестник Волжского университета им.

В.Н. Татищева. 2022. Т. 1. № 2 (101). С. 206-216.

10. Караева А.А., Панченко О.В. Криминалистическая характеристика преступления: терминологические подходы, содержание понятия // Молодой ученый. 2020. № 41 (331). С. 103-105.

11. Кардашевская М.В., Гаврилин Ю.В. Электронная платежная система как элемент обстановки преступления // Академическая мысль. 2020. № 2 (11). С. 21-23.

12. Кочеткова А.А. Криминалистическая характеристика преступления: актуальные проблемы понятия // Юность. Наука. Культура:материалы VII Всероссийской научно-практической конференции. Средне-Волжский институт (филиал) ВГУЮ (РПА Минюста России). 2020. С. 344-346.

13. Максименко А.А., Мамичева И.В. Особенности назначения и производства экспертиз по делам о преступлениях, связанных с использованием систем дистанционного банковского обслуживания // Студенческая научная весна: тезисы докладов Всероссийской студенческой конференции, посвященной 175-летию Н.Е. Жуковского. Москва, 2022. С. 310-311.

14. Ордоков М.Х., Шафиева Э.Т., Карданов А.К. Основные тенденции борьбы с кибермошенничеством // Пробелы в российском законодательстве. 2021. № 4. С. 108-111.

15. Поддубный И.В., Васюков В.Ф. К вопросу об актуальных способах совершения хищений с банковских счетов граждан, совершаемых с использованием систем дистанционного банковского обслуживания // Шумиловские чтения: сборник материалов Международной научно-практической конференции. Российская таможенная академия. 2021. С. 171-175.

16. Пудовиков А.С., Ненашев Е.В. Структура типичного способа совершения хищений с банковских счетов в отношении и (или) с помощью электронных денежных средств // Право и государство: теория и практика. 2021. № 12 (204). С. 292-295.

17. Решняк О.А., Ковалев С.А. Организация расследования мошенничеств, совершенных с использованием сети «Интернет», на

первоначальном и последующем этапах // Вестник Волгоградской академии МВД России. 2020. № 2 (53). С. 106-111.

18. Савченко М.М. Правовая природа безналичных и электронных денег как предмета преступных посягательств // Бизнес. Образование. Право. 2021. № 2 (55). С. 244-250.

19. Старостенко О.А. Меры специальной профилактики киберхищений // Молодежь и наука: актуальные проблемы фундаментальных и прикладных исследований: материалы V Всероссийской национальной научной конференции молодых учёных. В 4-х частях. Редколлегия: А.В. Космынин (отв. ред.) [и др.]. Комсомольск-на-Амуре, 2022. С. 212-214.

20. Шитикова Ю.И. Особенности криминалистического обеспечения расследования мошенничеств, совершенных дистанционным способом // Альманах молодого исследователя. 2020. № 9. С. 131-134.

III. Эмпирические материалы

1. Аналитические справки деятельности ОМВД России по Ашинскому району за 2018, 2019, 2020, 2021, 2022 года, предоставленные ИЦ ГУ МВД России по Челябинской области.

2. Материалы уголовного дела, возбужденного 27 декабря 2022 г. ОМВД России по Ашинскому району по факту дистанционного хищения денежных средств с банковской карты гр. П.

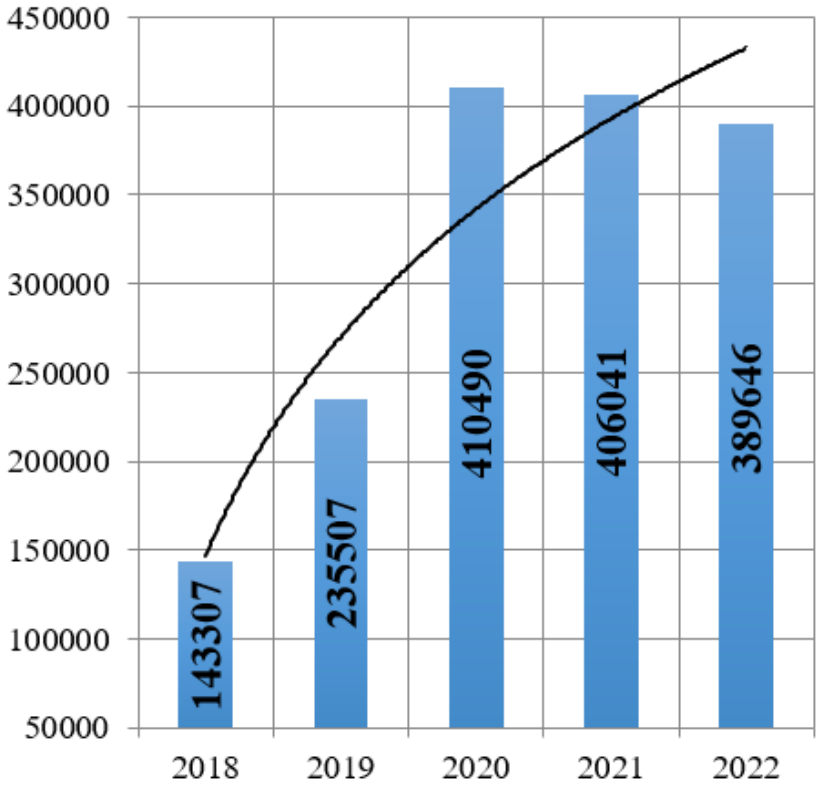
3. Приговор Ашинского городского суда № 1-102/2020 от 22 апреля 2020 г. по делу № 1-102/2020. URL:// https://sudact.ru/ (дата обращения: 28.01.2023).

4. Состояние преступности в Российской Федерации: [Электронный ресурс]: статистические сборники за 2018, 2019, 2020, 2021, 2022 года. URL:// https://xn--b1aew.xn--p1ai/dejatelnost/statistics (дата обращения: 28.01.2023).

Материал вычитан, цифры, факты, цитаты сверены с первоисточником. Материал не содержит сведений, составляющих государственную и служебную тайну. И.Р. Минигалиев

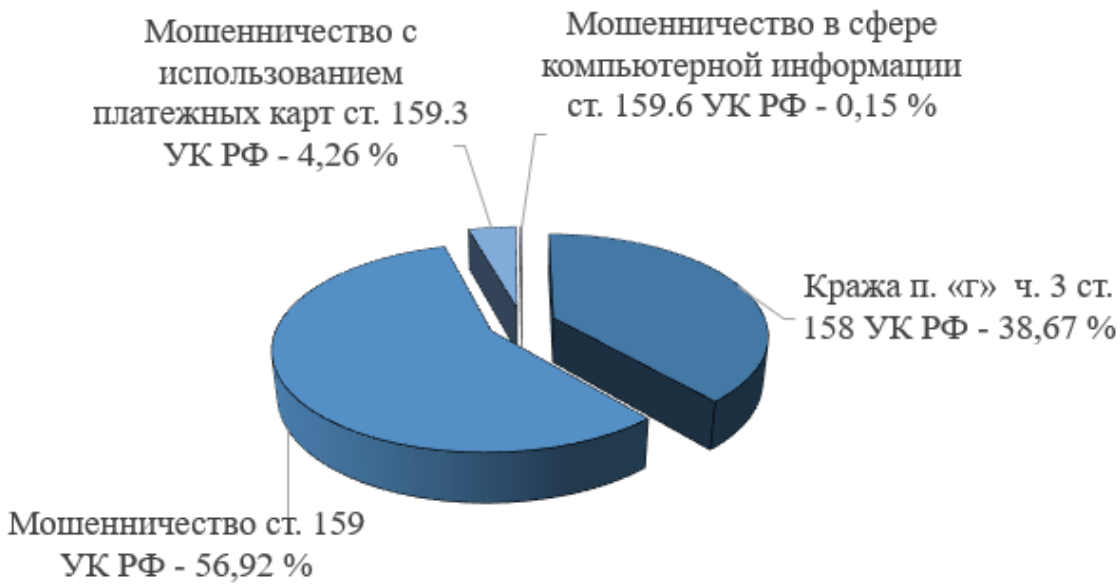
ПРИЛОЖЕНИЕ 1

Динамика хищений, совершенных с использованием информационных и телекоммуникационных технологий, в Российской Федерации с 2018 по 2022 года



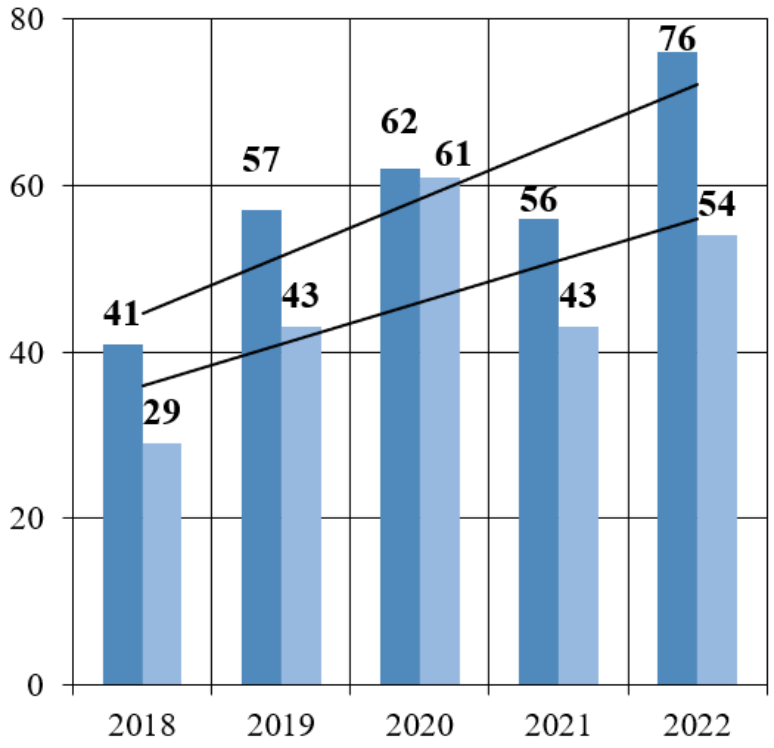
ПРИЛОЖЕНИЕ 2

Структура хищений, совершенных с использованием информационных и телекоммуникационных технологий, в Российской Федерации с 2018 по 2022 года, %



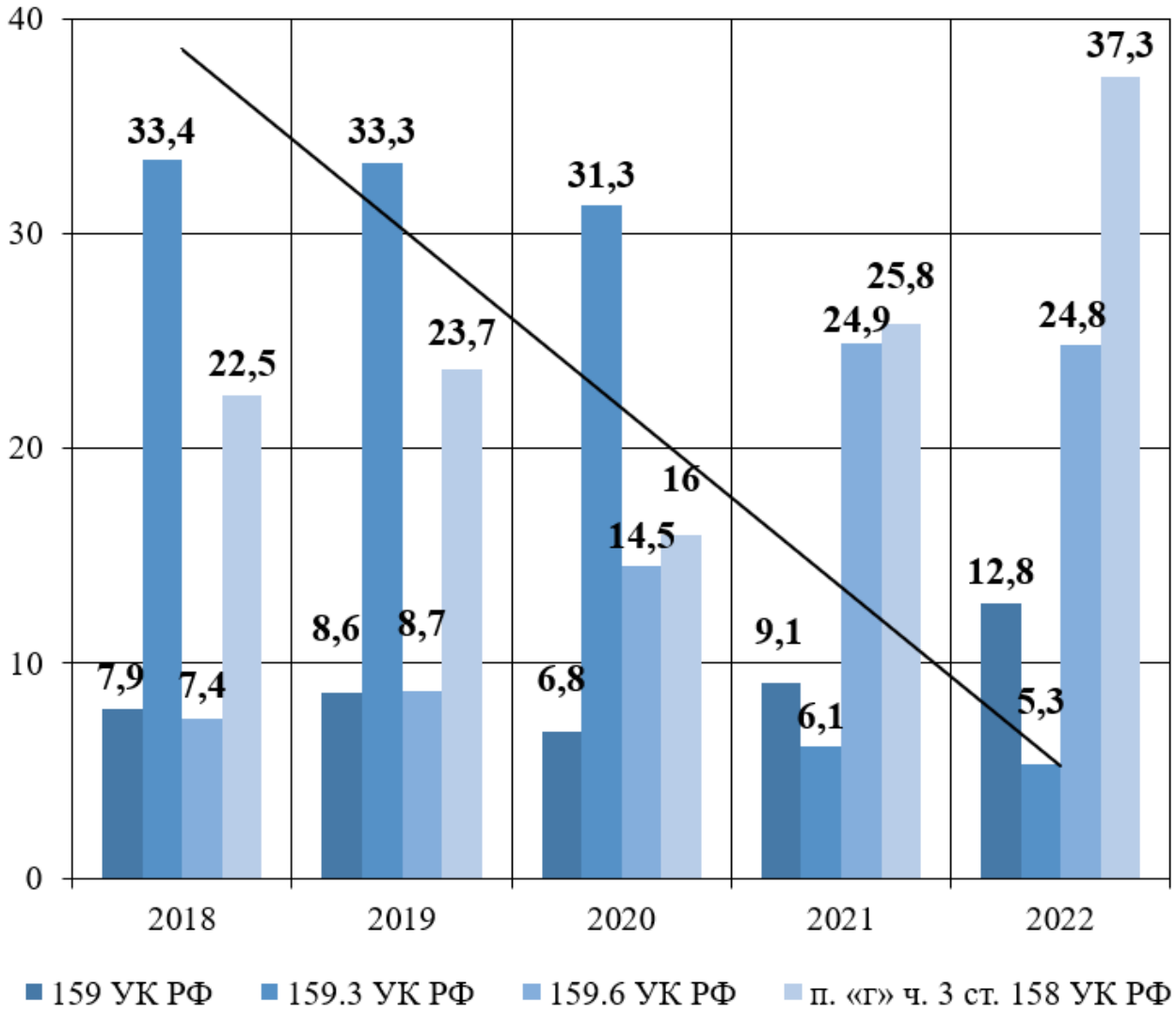
ПРИЛОЖЕНИЕ 3

Динамика хищений, совершенных с использованием информационных и телекоммуникационных технологий, в Ашинском районе Челябинской области с 2018 по 2022 года



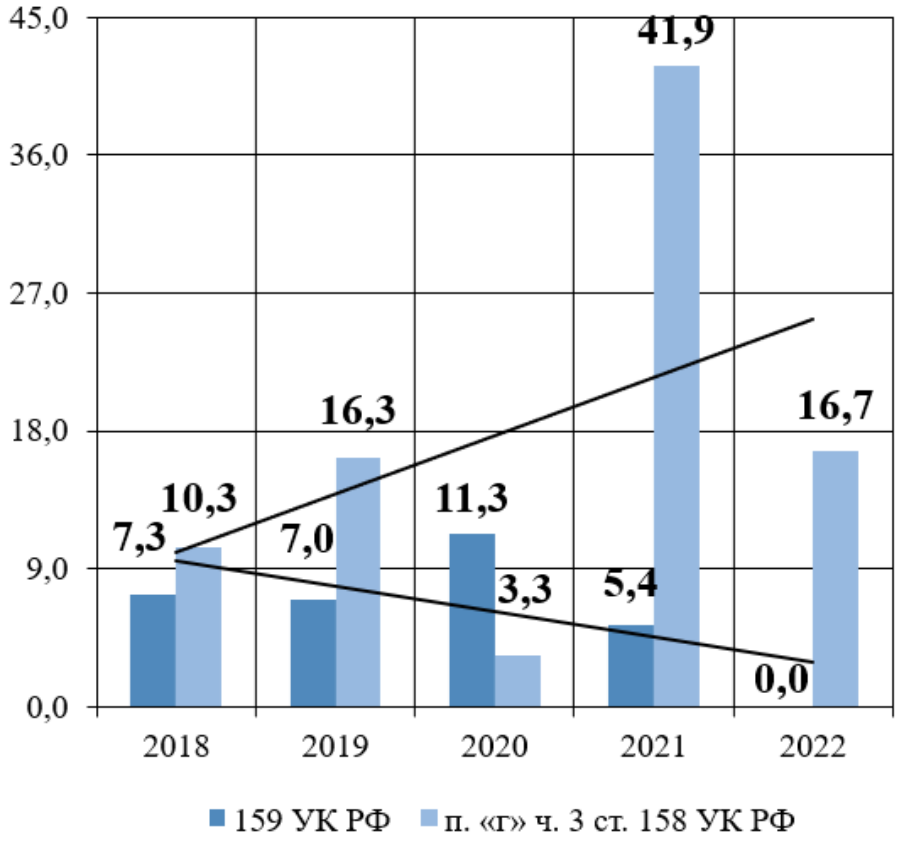
ПРИЛОЖЕНИЕ 4

Коэффициент раскрываемости хищений, совершенных с использованием информационных и телекоммуникационных технологий, в Российской Федерации с 2018 по 2022 года, %



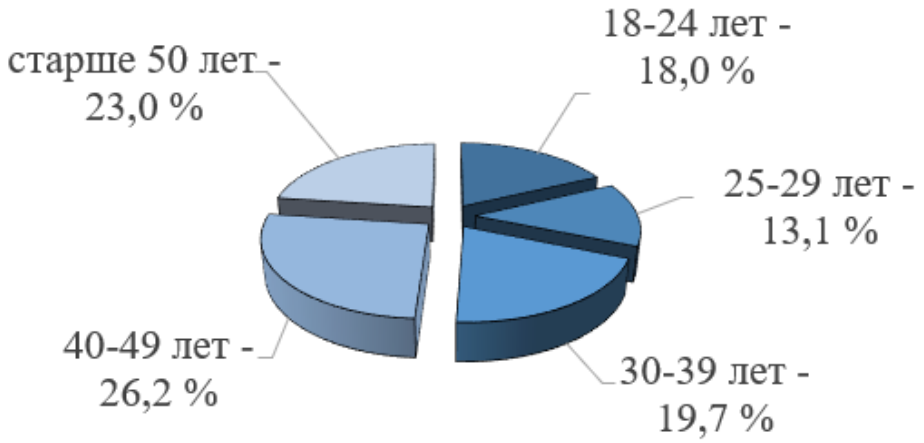
ПРИЛОЖЕНИЕ 5

Коэффициент раскрываемости хищений, совершенных с использованием информационных и телекоммуникационных технологий, в Ашинском районе Челябинской области с 2018 по 2022 года



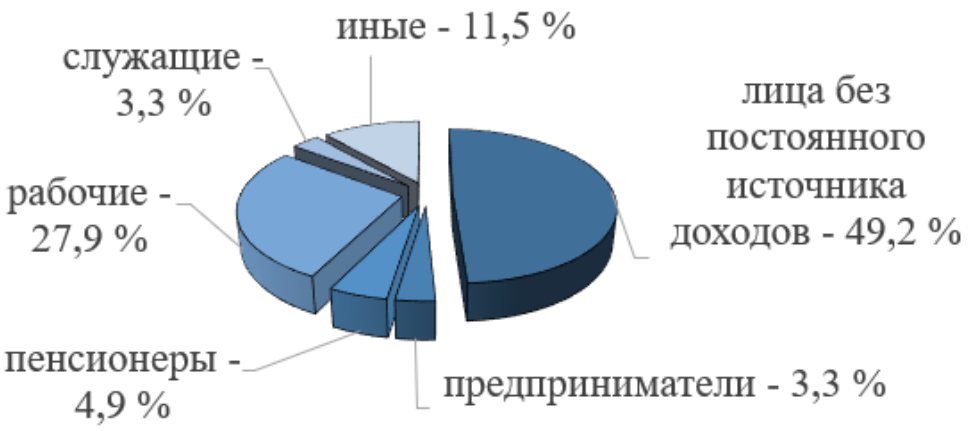
ПРИЛОЖЕНИЕ 6

Возрастная структура преступников, совершивших хищения с использованием информационных и телекоммуникационных технологий,
в Ашинском районе Челябинской области с 2018 по 2022 года, %



ПРИЛОЖЕНИЕ 7

Структура социального статуса преступников, совершивших хищения с использованием информационных и телекоммуникационных технологий, в Ашинском районе Челябинской области с 2018 по 2022 года, %



ПРИЛОЖЕНИЕ 8

Национальная структура преступников, совершивших хищения с использованием информационных и телекоммуникационных технологий, в Ашинском районе Челябинской области с 2018 по 2022 года, %