

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

Кафедра криминалистики

Специальность 40.05.01 Правовое обеспечение национальной
безопасности (специализация Уголовно-правовая, профиль
образовательной программы – Предварительное следствие в
органах внутренних дел), очная форма обучения, набор 2021 года

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

по теме:

**Криминалистическая характеристика хищений, совершенных
с использованием информационно-телекоммуникационных технологий или
в сфере компьютерной информации**

Выполнил:

слушатель группы НБ2101

младший лейтенант полиции

Артомохин Даниил Денисович

Руководитель:

доцент кафедры криминалистики

кандидат юридических наук

подполковник полиции

Харина Елена Алексеевна

Дата защиты:

« 29 » июня 2026 г.

Оценка: хорошо

Председатель ГЭК

полковник Котляков
(специальное звание)


(подпись)

В. В. Знак
(инициалы, фамилия)

Красноярск 2026

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

Кафедра криминалистики

Направление подготовки (специальность) 40.05.01 Правовое обеспечение
национальной безопасности (специализация Уголовно-правовая,
профиль образовательной программы – Предварительное следствие
в органах внутренних дел)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

по теме:

Криминалистическая характеристика хищений, совершенных
с использованием информационно-телекоммуникационных технологий или
в сфере компьютерной информации

Выполнил:

Руководитель:

Дата защиты:

« ____ » _____ 2026 г.

Оценка: _____

Председатель ГЭК

(специальное звание)

(подпись)

(инициалы, фамилия)

Красноярск 2026

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ	3
ГЛАВА 1. КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА КАК ОСНОВА ДЛЯ ФОРМИРОВАНИЯ МЕТОДИКИ РАССЛЕДОВАНИЯ ХИЩЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО- ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ ИЛИ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ	
1.1 Современные подходы к пониманию криминалистической характеристики, ее структуре и значению в раскрытии и расследовании преступлений	8
1.2 Соотношение криминалистической характеристики преступлений с уголовно-правовой и криминологической характеристиками	17
ГЛАВА 2. СОДЕРЖАНИЕ ОТДЕЛЬНЫХ ЭЛЕМЕНТОВ КРИМИНАЛИСТИЧЕСКОЙ ХАРАКТЕРИСТИКИ ХИЩЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО- ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ ИЛИ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ	
2.1 Предмет преступного посягательства по делам о хищениях, совершенных с использованием информационно- телекоммуникационных технологий или в сфере компьютерной информации	25
2.2 Способы хищений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации	35
2.3 Обстановка и следы хищений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации	48
2.4 Личность преступника, совершающего хищения с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации	57
ЗАКЛЮЧЕНИЕ	65
СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ	69

ВВЕДЕНИЕ

Актуальность темы исследования. Явлением, существенным образом повлиявшим на развитие современного общества в XXI в., стало интенсивное развитие и внедрение во все сферы жизнедеятельности человека дистанционных технологий. Это не только способствовало улучшению качества жизни общества, но и обусловило возникновение нового вида преступлений.

Произошел беспрецедентный рост хищений, совершаемых с использованием дистанционных технологий, и в сфере информационно-коммуникационных отношений: с 2015 г. наблюдалось постоянное увеличение количества данных преступлений, однако заметный их рост отмечается именно в последние годы. Так, в 2021 г. было зарегистрировано 406 041 анализируемое преступление, в 2022 г. – 371 171, в 2023 г. – 475 291, в 2024 г. – 486 281, в 2025 г. – 428 991¹. Как видим, неотъемлемой частью современного общества являются информационные технологии, которые влияют не только на повышение ценности информации, но и на появление новых видов преступлений.

Хищения, совершаемые с использованием дистанционных технологий, наносят значительный вред как отдельно взятым гражданам и организациям, так и всему государству. В 2025 г. данными преступлениями был причинен ущерб на общую сумму 557 млрд рублей, что на 54 млрд больше, чем в 2024 г.². О масштабах существующей проблемы свидетельствуют не только постоянное обсуждение ее на высоком государственном уровне, но и то, что в новой Стратегии национальной безопасности Российской Федерации

¹ Краткая характеристика состояния преступности 2021-2025 гг. URL: <https://мвд.рф/reports/item/19655871/> (дата обращения: 24.02.2026).

² Статистические данные о преступности. URL: <https://genproc.gov.ru/search/tags/?tags=Статистические%25данные>. (дата обращения: 24.02.2026).

преступления, совершаемые с использованием информационных технологий, отнесены к угрозам национальной безопасности Российской Федерации¹.

Об актуальности исследования данного вида криминальных деяний свидетельствует и тот факт, что они в настоящее время проникают во все новые сферы и отрасли деятельности общества, неизбежно следуя за устойчивым развитием и совершенствованием информационных технологий, увеличением численности пользователей электронно-вычислительных машин, способных подключиться к глобальной сети Интернет.

Наряду с беспрецедентным ростом количества хищений, совершаемых с использованием дистанционных технологий, и расширением сферы их преступного воздействия, еще одной значимой стороной общественной опасности данных преступлений является то, что сегодня происходит их качественное изменение, что затрудняет борьбу с ними. Большинство таких преступлений совершается в информационно-телекоммуникационном пространстве, в котором злоумышленники продолжают оставаться вне поля зрения правоохранительных органов, поскольку используют современные технологии и передовые методы шифрования, обеспечивающие децентрализацию и практически полную анонимность. Данную проблему подтверждают статистические показатели: за последние годы раскрываемость хищений, совершаемых с использованием информационных технологий, в среднем составляет 22%².

Таким образом, новизна возникающих проблем борьбы с хищениями, совершаемыми с использованием дистанционных технологий, недостаточная разработанность путей их разрешения, масштабы данной криминальной угрозы определяют актуальность темы исследования.

¹ Актуальные киберугрозы: итоги 2025 г. URL: <https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2024/> (дата обращения: 13.02.2026).

² Иванова О.М. О проблемах квалификации кражи, совершенной с банковского счета, а равно в отношении электронных денежных средств, как единичного сложного преступления // Судья. 2026. № 1 (181). С. 26.

Степень разработанности темы исследования. Теоретической основой исследования послужили труды А.Ю. Арефьева, Л.Н. Башкатова, Б.Т. Безлипкина, Р.С. Белкина, В.В. Вандышева, А.Ф. Волынского, А.В. Дулова, Н.А. Колесниченко, В.Н. Григорьева, А.Н. Гущина, В.И. Диденко, Л.Я. Драпкина, В.И. Зажицкого, С.И. Захарцева, А.В. Земсковой, Н.В. Изотовой, А.В. Коршунова, А.С. Косенко, М.П. Котухова, В.Ф. Луговика, А.Л. Осипенко, Н.М. Попова, А.А. Фальченко, Н.П. Яблокова, И.Н. Якимова.

Объектом исследования является преступная деятельность в форме хищений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, а также деятельность правоохранительных органов по выявлению, раскрытию и расследованию данных преступных деяний.

Предметом исследования являются закономерности хищений, совершенных с использованием информационно-телекоммуникационных технологий, а также связанные с ними закономерности деятельности правоохранительных органов по выявлению, раскрытию, расследованию указанных преступлений.

Цель исследования – выявление криминалистически значимых характеристик хищения, совершенного с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации.

Для достижения поставленной цели необходимо решить ряд задач:

- проанализировать современные подходы к пониманию криминалистической характеристики, ее структуре и значению в раскрытии и расследовании преступлений;
- осуществить соотношение криминалистической характеристики преступлений с уголовно-правовой и криминологической характеристиками;
- рассмотреть предмет преступного посягательства по делам о хищениях, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации;

- определить способы хищений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации;

- проанализировать особенности обстановки и следов хищений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации;

- рассмотреть особенности личности преступника, совершающего хищения с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации.

Методологической основой исследования явились – всеобщий диалектический метод научного познания, общенаучные методы эмпирического и теоретического познания, а также частно-научные методы: статистический, социологический, кибернетический, психологический.

Нормативной базой исследования выступили Конституция РФ, федеральные законы РФ, постановления Пленумов Верховного Суда РФ, ведомственные нормативные правовые акты МВД России и другие нормативные правовые акты.

Теоретическую основу исследования составляют фундаментальные и прикладные научные труды в области криминалистики, уголовного права, криминологии и уголовного процесса, посвященные проблемам расследования преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. В работе критически осмыслены и систематизированы положения, содержащиеся в работах таких ученых, как Р.С. Белкин, А.А. Бессонов, А.Ю. Головин, В.К. Гавло, О.П. Грибунов, Л.Я. Драпкин, Н.П. Яблоков, а также современных исследователей киберпреступности и цифровых следов – А.В. Белоусова, К.А. Мира, Е.В. Смахтина, Д.И. Шнейдеровой.

Эмпирическую базу исследования составили несколько групп источников, обеспечивающих репрезентативность и достоверность полученных выводов: 1) судебно-следственная практика: проведен анализ

50 приговоров о хищениях, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, вынесенных судами различных регионов Российской Федерации в период с 2020 по 2025 год. В работе использованы определения и постановления Верховного Суда РФ и кассационных судов общей юрисдикции;

2) статистические данные: использованы официальные сведения ГИАЦ МВД России о состоянии преступности, уровне зарегистрированных хищений рассматриваемой категории за 2021–2025 годы.

Теоретическая значимость исследования заключается в развитии положений криминалистической науки применительно к качественно новому виду преступной деятельности – хищениям, совершаемым с использованием информационно-телекоммуникационных технологий. Предложено авторское определение криминалистической характеристики данных хищений, раскрыто ее содержание как системной информационной модели, отражающей сущность преступления и закономерные связи между ее структурными элементами. Определен и детально проанализирован перечень криминалистически значимых сведений: предмет преступного посягательства, способы совершения и сокрытия преступления, механизм следообразования, обстановка преступления, личность преступника.

Практическая значимость исследования определяется направленностью полученных результатов на совершенствование деятельности органов внутренних дел по раскрытию, расследованию и предупреждению хищений, совершаемых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации.

Структура работы обусловлена ее содержанием и включает в себя введение, две главы, объединяющие шесть параграфов, заключение, список использованной литературы.

ГЛАВА 1. КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА КАК ОСНОВА ДЛЯ ФОРМИРОВАНИЯ МЕТОДИКИ РАССЛЕДОВАНИЯ ХИЩЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ ИЛИ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

1.1. Современные подходы к пониманию криминалистической характеристики, ее структуре и значению в раскрытии и расследовании преступлений

Сущностным началом подготовки деятельности по изобличению фактов и лиц, совершивших или совершающих хищения с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, должны быть данные о событии деяния, системе действий по его совершению, методах сопротивления всестороннему производству по уголовным делам, специфики поведения представителей криминальной среды при совершении конкретного преступления. Все выше перечисленные данные, характеризующие то или иное преступное событие, имеют свое определение – это «криминалистическая характеристика преступлений».

А.С. Усенко и С.П. Казакова отмечают, что «в криминалистике общепризнанным является высокое значение криминалистической характеристики преступления, которая представляет собой некоторую информационную модель преступления»¹. Вместе с тем, необходимо обращать внимание на то, что «любые рекомендации методического характера приобретают познавательную суть только тогда, когда они имеют адаптацию к конкретным, новейшим требованиям, исходящим от судебно-следственной

¹ Усенко А.С., Казакова С.П. Понятие и элементы криминалистической характеристики кражи // Юриспруденция: теория и практика. 2025. № 5. С. 104.

практики»¹, что будет особо актуальным для хищений с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. Также многие современные исследователи, по справедливому мнению О.П. Грибунова, «воспринимают криминалистическую характеристику преступления как обязательный элемент частной криминалистической методики»².

В криминалистической литературе приводится многообразие подходов к определению криминалистической характеристики преступления. В целом их можно разделить на две основные группы. Первая включает в себя определения, заостряющие внимание на перечислении элементов криминалистической характеристики преступления.

Изложенная концепция использована в трудах Р.С. Белкина³, Л.Л. Каневского⁴, В.К. Гавло⁵, Л.Я. Драпкина⁶, Н.П. Яблокова⁷ и некоторых других авторов. В качестве примера рассмотрим понятие, приведённое А.Ю. Головиным, который предлагает определить криминалистическую характеристику преступления как «систему типовых данных (сведений) об элементах отдельного вида преступления и его механизме»⁸.

Также хотелось бы выделить определение криминалистической

¹ Грибунов О.П., Назырова Н.А. Эволюция взглядов на понятие и структуру криминалистической характеристики преступлений // Известия Тульского государственного университета. 2020. № 2. С. 14.

² Грибунов О.П., Назырова Н.А. Указ. соч. С. 14.

³ Белкин Р.С. Криминалистика: проблемы, тенденции, перспективы. От теории – к практике. М.: Юридическая литература, 1988. С. 181.

⁴ Каневский Л.Л. Криминалистические проблемы расследования и профилактики преступлений несовершеннолетних. Красноярск: Красноярский государственный университет, 1991. С. 74.

⁵ Гавло В.К. Теоретические проблемы и практика применения методики расследования отдельных видов преступлений. Томск: Томский государственный университет, 1985. С. 167.

⁶ Драпкин Л.Я. Предмет доказывания и криминалистические характеристики преступлений // Криминалистические характеристики преступлений. Свердловск: Уральский государственный университет, 1978. С. 17.

⁷ Яблоков Н.П. Криминалистика: учебник. М.: Проспект, 2005. С. 64.

⁸ Головин А.Ю. Криминалистическая характеристика преступлений как категория современной криминалистики // Известия Тульского государственного университета. 2012. № 1-2. С. 48.

характеристики, данное Р.С. Белкиным, в соответствии с которым под таковой можно понимать «систему информации, включающую данные о преступлении и связанных с ним обстоятельствах, имеющих значение для расследования»¹.

Однако стоит отметить, что, с учетом научно-технического прогресса, возможно возникновение новых элементов криминалистических характеристик, что может сделать часть определений неактуальными в отношении конкретных видов преступлений, либо, напротив, добавить потребность в выявлении новых элементов.

Во вторую группу входят определения, раскрывающие сущностный, смысловой компонент криминалистической характеристики.

В связи с этим можно заявить о востребованности определений авторов, раскрывающих понятие криминалистической характеристики преступления через смысловой, сущностный аспект. Приведем примеры таких определений.

А.А. Бессонов указывает на то, что «криминалистическая характеристика представляет собой отражение сущности преступления, которое предстает как системное явление объективной реальности, его структуру, а также закономерности, существующие между ее элементами»².

С.Ю. Бирюков считает целесообразным определение криминалистической характеристики, согласно которому «она предстает как вероятностная либо информационная модель типичных характеристик отдельной категории общественно опасных деяний, а также закономерных связей между ними»³. Схожие позиции можно встретить в работах О.Я. Баева⁴,

¹ Белкин Р.С. История отечественной криминалистики: монография. М.: Норма, 1999. С. 274.

² Бессонов А.А. Частная теория криминалистической характеристики преступлений: автореферат дис. ... д-ра юрид. наук. М., 2017. С. 11.

³ Бирюков С.Ю., Кушпель Е.В. Методика расследования организации незаконной миграции: учеб. пособие. Волгоград: Волгоградская академия МВД России, 2007. С. 19.

⁴ Баев О.Я. Основы криминалистики: курс лекций. М.: Проспект, 2001. С. 230.

А.Н. Басалаева¹, И.Ф. Герасимова², В.Ф. Ермоловича³, В.В. Ключкова⁴, А.Ю. Головина⁵, В.С. Ишигеева⁶, В.Я. Колдина, Е.П. Ищенко⁷ и др. и иных авторов.

На наш взгляд, достоинство определений второй группы авторов заключается в том, что они позволяют варьировать структурно-элементный состав криминалистических характеристик различных категорий преступлений. А.Ю. Головин отмечает, что «весьма востребованной такая позиция является в связи с возникновением качественно новых характеристик преступлений. Помимо прочих преступлений, это касается рассматриваемой категории преступлений. Одновременно с этим, такие определения отражают сущность криминалистической характеристики преступления, подчеркивают ее значение для методик расследования преступлений»⁸.

Для определения структуры криминалистической характеристики хищений с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации востребованным являются мнения Е.В. Смахина и А.В. Белоусова, которые отметили распространенное мнение в криминалистике, согласно которому «отдельные элементы криминалистической характеристики преступления могут

¹ Басалаев А.Н., Гуняев В.А. Криминалистическая характеристика преступления (Общее понятие и практическое значение) // Методика расследования преступлений. Общие положения. М.: Юридическая литература, 1976. С. 100.

² Герасимов И.Ф. Криминалистические характеристики преступлений в методике расследования // Там же. С. 97.

³ Ермолович В.Ф. Криминалистическая характеристика преступлений: законы и законодательные акты. Минск: Дрофа, 2001. С. 19.

⁴ Ключков В.В. Криминалистическая характеристика преступлений: состояние и перспективы исследований // Криминалистическая характеристика преступлений. М.: Полиграфист, 1984. С. 24.

⁵ Головин А.Ю. Криминалистическая характеристика преступлений как категория современной криминалистики // Известия Тульского государственного университета. 2012. № 1-2. С. 48.

⁶ Ишигеев В.С., Авдеев М.В. Междисциплинарный характер криминалистической характеристики преступлений // Криминалистика: вчера, сегодня, завтра. 2020. № 4 (16). С. 34.

⁷ Колдин В.Я., Ищенко Е.П., Крестовников О. А. Типовая информационная модель или криминалистическая характеристика преступления? // Академический юридический журнал. 2006. № 4. С. 10.

⁸ Головин А.Ю. Указ. соч. С. 48.

трансформироваться»¹. А.Ю. Головин в своей диссертации также подчеркнул «наличие объективной потребности в последующей систематизации криминалистических научных знаний»².

Криминалистическая характеристика преступлений является важнейшим инструментом применения криминалистических знаний в практической деятельности должностных лиц по раскрытию и расследованию преступлений. Данной научной категории посвящены сотни научных работ советских и российских ученых-криминалистов. Не вдаваясь в дискуссию относительно понятия и содержания отдельных ее элементов, отметим, что практически все ученые сходятся во мнении, что криминалистическая характеристика является неотъемлемым структурным элементом любой частной методики расследования.

Несмотря на огромное количество научных работ о криминалистической характеристике преступлений (включая отдельные параграфы и главы в диссертационных исследованиях), непосредственно вопросам формирования³ криминалистической характеристики преступлений уделено крайне незначительное внимание. В большинстве работ констатируется «наличие данной категории в частной методике расследования, обозначаются ее элементы и их содержание, в редких случаях демонстрируется взаимосвязь между ее отдельными элементами»⁴. Ведь в свое время Р.С. Белкин говорил, что «максимальная польза криминалистической характеристики преступлений проявляется только тогда,

¹ Смахтин Е.В., Белоусов А.В. Значение предмета и объекта преступления в структуре криминалистической характеристики деяний в сфере компьютерной информации // Материалы национальной науч.-практ. конф. Иркутск: Восточно-Сибирский институт МВД России, 2021. С. 228.

² Головин А.Ю. Теоретические основы и актуальные проблемы криминалистической систематики на современном этапе развития криминалистики: автореф. дис. ... канд. юрид. наук. М., 2003. С. 20.

³ Под формированием автор имеет ввиду процесс, технологию построения криминалистической характеристики.

⁴ Тебиев Р.Р. Технология построения криминалистической характеристики преступлений на примере жестокого обращения с животными // Вестник Сибирского юридического института МВД России. 2023. № 2 (51). С. 30.

когда выявлены те самые пресловутые закономерные связи между отдельными ее элементами»¹.

Одним из современных комплексных исследований криминалистической характеристики преступлений является докторская диссертация А.А. Бессонова «Частная теория криминалистической характеристики преступлений». В ней автор подробно рассматривает «вопросы формирования данной научной категории и предлагает технологию построения криминалистической характеристики, состоящую из 7 этапов»². Именно данная технология была адаптирована и применена при построении криминалистической характеристики хищений с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. Рассмотрим более подробно данную технологию.

Первый этап включает в себя изучение теоретического материала, а также ранее проведенных исследований. Относительно хищений с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации были изучены работы авторов, занимавшихся методическими вопросами указанных преступлений, выявлен ряд недостатков. В частности, в них не учитывались серьезные законодательные преобразования последних лет.

Кроме того, на данном этапе решался вопрос относительно эмпирического материала, подлежащего изучению, и его объема (материалы архивных уголовных дел за период с 2020 по 2025 г., статистические данные ГИАЦ МВД России, анкетирование сотрудников органов внутренних дел).

Второй и третий этап заключаются в непосредственном изучении эмпирического материала, его анализе и систематизации. Сущность данного этапа заключается в установлении и описании закономерных связей между криминалистически значимыми признаками хищений с использованием

¹ Белкин Р.С. Курс криминалистики: в 3 т. Т. 3: Криминалистические средства, приемы и рекомендации. М.: Норма, 1997. С. 116.

² Бессонов А.А. Указ. соч. С. 21.

информационно-телекоммуникационных технологий или в сфере компьютерной информации, впоследствии устанавливаемых между элементами криминалистической характеристики.

При выполнении указанных действий были выявлены закономерные связи между содержанием и характером способа преступления и фактом знакомства субъекта преступления с потерпевшим; между способом преступления и личностью преступника и др.

Четвертый этап заключается в определении элементного состава криминалистической характеристики преступлений. Нами была выявлена следующая структура: непосредственный предмет преступного посягательства, способ преступления, данные о следах преступления, обстановка преступления и личность преступника.

Пятый этап формирования криминалистической характеристики хищений с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации состоит в ее апробации. Решение данной задачи предопределяет качество как самой характеристики, так и в целом частной методики расследования.

Шестой и седьмой этапы заключаются в использовании криминалистической характеристики, ее мониторинге, анализе эффективности в практической, научной и образовательной деятельности. При этом использоваться она может как при создании новой частной методики расследования хищений с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации либо совершенствовании уже имеющейся; в деятельности по раскрытию и расследованию преступлений; в образовательной деятельности и т.д. А.А. Ермолаев отмечает, что «оценка эффективности сформированной криминалистической характеристики должна производиться спустя некоторое

время после ее внедрения»¹.

Таким образом, указанная технология позволила сформировать обоснованную, актуальную и востребованную в практике криминалистическую характеристику хищений с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. Данная технология является универсальной, она может быть использована при создании криминалистических характеристик других преступлений.

С учетом проанализированных научных точек зрения, полагаем, что в перечень криминалистически значимых сведений о хищениях с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации должны входить следующие:

1. Сведения о способе преступления.
2. Сведения о предмете преступного посягательства.
3. Сведения о следовой картине преступного посягательства.
4. Сведения об обстановке преступления.
5. Сведения о личности преступника.

Таким образом, в рамках обоснования авторской позиции представляется возможным сформулировать следующие выводы, раскрывающие сущность и значение криминалистической характеристики хищений, совершаемых с использованием информационно-телекоммуникационных технологий либо в сфере компьютерной информации:

1. Несмотря на множественность доктринальных подходов к определению содержания и сущности преступного деяния, криминалистическая характеристика преступления сохраняет статус общепризнанной научной категории в системе криминалистического знания. Более того, она выступает в качестве обязательного структурного элемента

¹ Ермолаев А.А. Количественные корреляционные связи между элементами криминалистической характеристики преступления // Мониторинг правоприменения. 2025. № 1 (54). С. 51.

частной методики расследования, выполняя функцию технико-криминалистического инструментария, предназначенного для раскрытия отдельных видов преступлений и преступных групп.

2. Криминалистическая характеристика хищений, совершаемых с применением информационно-телекоммуникационных технологий или в сфере компьютерной информации, представляет собой обобщенное (типовое) описание соответствующего вида преступной деятельности. Данное описание базируется на анализе правоприменительной практики, статистических данных, криминалистически значимых сведений и нормативных положений уголовного закона. Целевым назначением такой характеристики выступает формирование общих и специальных методических рекомендаций по расследованию указанных деяний, обоснованный выбор криминалистических средств, приемов и тактических решений применительно к различным этапам расследования.

3. Криминалистическая характеристика является формой отражения сущности преступления как системного явления объективной действительности, фиксирующей его структуру, а также закономерные связи, существующие между элементами этой структуры. В данном качестве она признаётся важнейшим инструментом трансформации теоретического криминалистического знания в практическую деятельность уполномоченных должностных лиц по выявлению, раскрытию и расследованию преступных деяний.

4. Система криминалистически значимых сведений о хищениях, совершаемых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, должна включать следующие элементы: сведения о способе совершения преступления; сведения о предмете преступного посягательства; сведения о следовой картине; сведения об обстановке (обстоятельствах) совершения преступления; сведения о личности субъекта преступной деятельности.

1.2. Соотношение криминалистической характеристики преступлений с уголовно-правовой и криминологической характеристиками

Преступление как многоаспектное явление исследуется науками криминального цикла с разных сторон, в зависимости от поставленных ими целей, вследствие чего оно имеет разные понятия. По мнению отдельных исследователей, «неоднозначность результата исследований этих наук данной правовой категории объясняется следующими причинами: постановкой разных задач, включением в оборот разных сведений, использованием своих источников этих сведений, рассмотрением проблем в узком аспекте без осуществления системного сравнительного анализа и т.п.»¹.

Научный анализ трудов различных авторов свидетельствует, что «в настоящее время в науках криминального цикла нет единого подхода к структуре и содержанию уголовно-правовой, криминологической и криминалистической характеристик, их соотношению между собой. Некоторые ученые вообще ставят под сомнение целесообразность существования отдельных из указанных категорий»².

Целью является совершенствование методов частного расследования, и следователи непосредственно используют эти характеристики для определения методов решения следственных задач. Они являются руководством по поиску, сбору и рассмотрению доказательств по расследуемым уголовным делам.

¹ Халиуллина А.Ф. Криминалистическая характеристика насильственных действий сексуального характера, совершенных в отношении малолетних и несовершеннолетних // Правовое государство: теория и практика. 2017. № 1 (47). С. 161.

² Так, в криминалистике долгое время существует спор относительно существования понятия «криминалистическая характеристика преступления». (Белкин Р.С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики: монография. М.: Проспект, 2001. С. 220-224).

Л.Е. Чистова отмечает, что «криминалистическая характеристика, формируясь в тесном взаимодействии с криминологической, уголовно-правовой и психологической характеристиками преступлений, позволяет выдвигать версии относительно неустановленных обстоятельств совершенного преступления, а также оказывать значительное влияние на такой вид следственной деятельности как профилактика и предупреждение преступлений»¹.

Знание криминалистической характеристики преступления как одного из элементов любой частной криминалистической методики расследования преступлений, по мнению А.Ф. Халиуллиной, позволяет своевременно определить правильное направление расследования, круг вопросов, требующих первоочередного решения, выдвинуть версии о личности преступника, а также выбрать комплекс необходимых следственных действий².

Л.Е. Чистова, сопоставляя уголовно-правовую и криминалистическую характеристики, полагает, что «система выраженных в законе признаков, позволяющих охарактеризовать конкретное общественно опасное деяние как преступление, то есть виновное и наказуемое деяние, и отличить данный состав преступления от другого, составляет его уголовно-правовую характеристику»³. По сути, автор понимает под уголовно-правовой характеристикой преступления его состав, что, на наш взгляд, не совсем правильно. Система признаков деяния, выраженных в уголовном законе, – это конкретный вид преступления, но никак не его уголовно-правовая характеристика. Уголовно-правовая характеристика преступления – это прежде всего научная категория. Как справедливо отмечает И.В. Александров, «уголовно-правовая характеристика имеет своей целью изучение вопросов квалификации преступления. Поэтому она конструируется не в законе

¹ Чистова Л.Е. О соотношении уголовно-правовой и криминалистической характеристик // Вестник криминалистики. 2006. №1. С. 36.

² Халиуллина А.Ф. Указ. соч. С. 161.

³ Чистова Л.Е. Указ. соч. С. 37.

законодателем в процессе законотворчества, а ученым исходя из закона, в научном труде в процессе научного творчества»¹.

Л.Д. Гаухман, рассматривая уголовно-правовую характеристику, включает в нее исключительно вопросы понятия и квалификации преступления. По мнению указанного автора, «содержанием данной характеристики являются сведения, раскрывающие конкретный состав преступления. На основании их законодатель получает возможность описать преступление как общественно опасное деяние. Состав преступления представлен набором характеризующих его признаков. Их совокупность позволяет привлечь виновного лица к уголовной ответственности»². Отдельные авторы отмечают, что «все признаки, образующие состав преступления, законодательно закреплены в диспозиции статей Особенной части УК РФ, в качестве признаков конкретного его состава. Определенная их часть также содержится в статьях Общей части УК РФ. Например, статьи 14, 29-31, 37-42 УК РФ содержат признаки, характеризующие объективную сторону, статьи 24-28 УК РФ – субъективную сторону, статьи 20, 21, 32-35 УК РФ – субъект преступления»³.

Признаки состава преступления проявляются в группе, образуя такие его элементы, как объект, объективная сторона, субъект и субъективная сторона. В свою очередь эти элементы составляют единую систему. Отсутствие в данной системе хотя бы одного из них приводит к отсутствию самого преступления. Посредством этих элементов, образующих состав преступления, устанавливаются индивидуальные особенности, выделяющие его из ряда других. По этому поводу В.Н. Кудрявцев отмечал следующее: «...состав является информационной моделью преступления определенного

¹ Александров И.В. Теоретические и практические проблемы расследования налоговых преступлений: дис. ... докт. юрид. наук. Екатеринбург, 2003. С. 88.

² Гаухман Л.Д. Расследование по делам о телесных повреждениях и хулиганстве. М.: Юридическая литература, 1975. С. 6.

³ Боровик П.Л., Пилюшин С.В. Хищение имущества путем модификации компьютерной информации: анализ способов и рекомендации по проведению проверочных мероприятий // Юстиция Беларуси. 2024. № 8 (269). С. 54.

вида, закрепленный в уголовном законе. Эта модель образуется в результате обобщения признаков всех преступлений данной разновидности. В результате мы получаем экономное, краткое и достаточно четкое описание их основных свойств»¹.

Представляется, что уголовно-правовая характеристика преступления – это построенная в результате научной деятельности система сведений о признаках элементов состава конкретного вида преступлений. Следуя такой логике, можно сделать вывод, что «в основу уголовно-правовой характеристики преступлений входят сведения об элементах состава преступления. Задача лица, занимающегося научной разработкой уголовно-правовой характеристики, сводится к детализации сведений об элементах состава преступления и описанию корреляционных связей между ними. Однако указанного явно недостаточно для достижения задач по разработке мер предупреждения конкретного вида преступлений, их раскрытия и расследования. Указанные меры разрабатываются лишь на основе криминологической и криминалистической характеристик преступлений»².

О.В. Дамаскин отмечает, что «криминологическая характеристика определенной группы преступлений имеет не только доктринальное, но и практическое значение, поскольку позволяет получить комплексное представление об особенностях таких деяний и личности их субъектов, присущих им детерминантах, механизме осуществления и причиняемых ими социальных последствиях, что способствует повышению эффективности противодействия таким деяниям, включая их профилактику и последующие предупреждение и пресечение»³.

Криминологическая характеристика представляет собой исходный этап, необходимый для оптимизации процесса разработки и последующей реализации мер предупреждения преступлений. Структура криминологической

¹ Кудрявцев В.Н. Общая теория квалификации преступлений. М.: Дрофа, 1972. С. 45.

² Там же. С. 46.

³ Дамаскин О.В. Криминология: учеб. пособие. М.: Юрлитинформ, 2009. С. 9.

характеристики образована следующими основными блоками, содержащими взаимосвязанные элементы и признаки: «1) криминологически значимые признаки преступления (группы преступлений), характеризующие детерминанты и механизм совершения преступления (преступлений), личность субъектов последних, мотив и цель их совершения; социально опасные последствия преступных деяний; 2) сведения, раскрывающие криминологическую ситуацию, включая информацию о социальной среде, в которой проявилось преступное деяние, а также об имеющихся на данный момент социально-экономических условиях; 3) сведения о превентивной деятельности, в том числе об объектах и субъектах предупреждения преступлений, используемых при этом методах и средствах»¹.

По своей гносеологической сущности все элементы и признаки можно также подразделить на три группы: «1) объективные (статистика преступлений, социальные условия преступлений, включая социально-экономическую и геополитическую обстановку, время и географию совершения преступлений); 2) субъективные (свойства личности преступника и потерпевшего, мотивы и цели преступного поведения); 3) комплексные (механизм совершения преступления, детерминанты преступления и его последствия)»².

Криминологическая характеристика преступления или группы преступлений являются первой составной частью системы предупреждения преступлений, а ее второй составной частью – разработка и реализация профилактических и иных превентивных мер. Именно в своем единстве данная система может быть эффективной, при этом «криминологическая характеристика составляет ее информационную основу, без которой невозможно сформировать действенный комплекс мер предупреждения соответствующих преступлений»³.

¹ Дамаскин О.В. Указ. соч. С. 10.

² Тарасова Н.В. Криминология: учеб.-методич. комплекс. Брянск: Полиграфист, 2010. С. 49.

³ Там же. С. 50.

Часть криминологов выделяет криминологическую характеристику преступлений, которая «систематизирует сведения об особенностях личности лица, совершающего конкретный вид преступлений, причинах и условиях, способствующих указанным деяниям»¹. Другие говорят о криминологической характеристике преступности². По мнению авторов Большого юридического словаря, криминологическая характеристика – это «описание свойств, закономерностей, факторов и последствий преступности (отдельного ее рода или вида), а также свойств личности преступника (отдельного ее типа)»³. В.Е. Эминов формулирует следующее определение криминологической характеристики преступлений: «криминологическая характеристика и есть совокупность данных (достаточная информация) об определенном виде (группе) преступлений либо конкретном особо опасном деянии, используемая для их предупреждения»⁴. Н.В. Тарасова считает, что «дать криминологическую характеристику преступности – означает раскрыть ее состояние, структуру и динамику»⁵.

Научный анализ приведенных определений показывает, что в состав криминологической характеристики преступлений (преступности) включают систему сведений о преступлениях определенного вида (криминологическая характеристика преступлений) либо определенной группы людей (криминологическая характеристика преступности), используемую для их предупреждения и минимизации негативных последствий. Указанная система сведений, в отличие от уголовно-правовой характеристики, содержит в себе информацию о причинах и детерминантах совершения преступления и призвана прежде всего обеспечить теоретико-методологическую функцию для процесса разработки мер по их предупреждению.

¹ Дамаскин О.В. Указ. соч. С. 11.

² См., например: Ваничкин Д.Е. Криминологическая характеристика и предупреждение преступности в регионе (на материалах Ставропольского края): дис. ... канд. юрид. наук. Ставрополь, 2004; и др.

³ Большой юридический словарь / под ред. А.Я. Сухарева. М.: Норма, 2008. С. 356.

⁴ Криминология: учебник / под ред. В.Н. Кудрявцева. М.: Норма, 1997. С. 25.

⁵ Тарасова Н.В. Указ. соч. С. 49.

Все из рассматриваемых категорий достаточно близки между собой. У них один объект – преступление. Их содержание зачастую переплетается между собой, и отличить одно от другого порой и вовсе невозможно. Например, и уголовно-правовая, и криминологическая, и криминалистическая характеристики изучают личность преступника. Каждая из рассматриваемых категорий в своем содержании заимствует что-то из содержания другой. Представляется, что основное отличие одной характеристики от другой заключается в решаемых посредством ее формирования задачах. Достаточно кратко, но в то же время емко по этому поводу высказался И.В. Александров, указав, что «уголовно-правовая характеристика имеет своей целью изучение вопросов квалификации преступления, криминологическая – исследование причин и условий совершения преступления, а криминалистическая – рассматривает обстоятельства преступления, которые связаны с его расследованием»¹. Если же связать воедино все указанные характеристики², то, по существу, решаются все основные задачи борьбы с преступностью: предупреждение, раскрытие и расследование преступлений.

Таким образом, дискуссия относительно самой возможности существования рассматриваемых характеристик в научном контексте представляется лишеной оснований, поскольку их объективное наличие не вызывает сомнений. Вместе с тем отсутствие прогресса в теоретическом осмыслении данных понятий обуславливает их бессистемное применение. Представляется обоснованной позиция тех исследователей, которые полагают, что указанные характеристики образуют единую систему. Возможными вариантами ее наименования могут выступать «социально-

¹ Александров И.В. Указ. соч. С. 88.

² Такое предложение высказал А.М. Кустов, который считал необходимым заменить криминалистическую, уголовно-правовую, криминологическую, оперативно-розыскную, уголовно-процессуальную характеристики социально-правовой характеристикой преступлений. См.: Кустов А.М. Криминалистическая или социально-правовая характеристика преступлений как ориентир в борьбе с преступностью // Роль и значение деятельности Р.С. Белкина в становлении современной криминалистики: материалы Международной научной конференции (к 80-летию со дня рождения Р.С. Белкина). М.: Московский государственный университет, 2002. С. 220-224.

правовая характеристика преступлений» либо «криминальная характеристика (система) преступлений»¹. Последний вариант, с нашей точки зрения, в большей степени согласуется с устоявшимся подходом, учитывая отнесение криминологии, уголовного права и криминалистики к наукам «криминального цикла». В состав данной системы надлежит включать оперативно-розыскную, психологическую и иные разновидности характеристик преступлений. Однако при решении задачи, поставленной в рамках настоящего параграфа, следует отметить, что, по нашему убеждению, уголовно-правовая, криминологическая и криминалистическая характеристики образуют основной «каркас» системы более высокого уровня – «криминальной характеристики преступлений». При этом в иерархической структуре системы базовое положение занимает уголовно-правовая характеристика, которая впоследствии детализируется и дополняется криминологической характеристикой. Криминалистическая же характеристика преступлений использует данные двух вышеназванных характеристик в целях решения частных прикладных задач, связанных с расследованием преступлений.

¹ Кустов А.М. Указ. соч. С. 224.

ГЛАВА 2. СОДЕРЖАНИЕ ОТДЕЛЬНЫХ ЭЛЕМЕНТОВ КРИМИНАЛИСТИЧЕСКОЙ ХАРАКТЕРИСТИКИ ХИЩЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО- ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ ИЛИ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

2.1. Предмет преступного посягательства по делам о хищениях, совершенных с использованием информационно- телекоммуникационных технологий или в сфере компьютерной информации

Традиционное понимание предмета хищения в российском уголовном праве базировалось на триаде признаков: экономическом (стоимостная оценка), юридическом (имущество является чужим для виновного) и физическом (материальная оболочка предмета). Однако стремительная цифровизация экономики и внедрение информационно-телекоммуникационных технологий в финансовую сферу обусловили необходимость пересмотра устоявшихся подходов.

Знаковым этапом эволюции стало принятие Федерального закона от 23 апреля 2018 г. № 111-ФЗ¹, которым УК РФ был дополнен п. «г» ч. 3 ст. 158 и изменена редакция ст. 159.3. Как справедливо отмечает Д.В. Голенко, «включение в предмет имущественных преступлений безналичных денежных средств повлекло за собой переосмысление Верховным Судом РФ момента окончания некоторых форм хищения»². Пленум Верховного Суда РФ в

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

² Голенко Д.В. О проблемах законодательной регламентации уголовной ответственности за преступное использование электронных средств платежа // Юридический вестник Самарского университета. 2025. № 1. С. 68.

постановлениях от 27 декабря 2002 г. № 29¹ и от 30 ноября 2017 г. № 48 связал момент окончания кражи и мошенничества «с моментом изъятия денежных средств с банковского счета их владельца или электронных денежных средств, в результате которого владельцу этих денежных средств причинен ущерб»².

Данная трансформация вызвала оживленную дискуссию в научном сообществе. А.Г. Безверхов обоснованно указывает, что в результате состав кражи, предусмотренной п. «г» ч. 3 ст. 158 УК РФ, «трансформировался из материального в формальный», что фактически означает изменение конструкции состава преступления судебной властью. С одной стороны, такой подход позволяет более эффективно противодействовать хищениям в цифровой среде; с другой – создает риски необоснованного ужесточения ответственности, когда действия, квалифицируемые как покушение, признаются окончанным преступлением³.

Показательным является пример из практики Хабаровского краевого суда. Гр. Г., похитив банковскую карту потерпевшего и оплатив ею товары, была первоначально осуждена по п. «г» ч. 3 ст. 158 УК РФ. Однако Президиум Хабаровского краевого суда переквалифицировал ее действия на п. «в» и «г» ч. 2 ст. 158 УК РФ, указав, что «Г. совершила хищение имущества Б., в том числе принадлежащей ему банковской карты ... и затем в короткий промежуток времени с помощью похищенной карты оплатила товары»⁴. Суд пришел к выводу, что кража карты как предмета, обладающего материальной природой, и последующее распоряжение безналичными денежными средствами образуют единое продолжаемое преступление. Данный пример

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

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

³ Безверхов А.Г. Хищение чужого имущества в условиях становления цифровой экономики // Уголовное право: стратегия развития в XXI веке. М., 2020. С. 329.

⁴ Постановление Президиума Хабаровского краевого суда от 21 октября 2019 г. по делу 44у-139/2019. URL: // <https://kraevoy--hbr.sudrf.ru/>. (дата обращения: 12.04.2026).

иллюстрирует сохраняющуюся в правоприменительной практике неопределенность относительно момента окончания хищения при использовании электронных средств платежа.

Таким образом, эволюция понятия предмета хищения характеризуется переходом от узко-вещественного понимания к широкому, включающему безналичные денежные средства и электронные денежные средства, что потребовало пересмотра традиционных подходов к моменту окончания преступления и породило множество дискуссионных вопросов.

Одной из ключевых проблем является отсутствие четкого законодательного разграничения понятий «безналичные денежные средства» и «электронные денежные средства». Как обоснованно отмечают Н.Ю. Волосова и Е.О. Филиппова, «ни в том, ни в другом приговоре не было указано, что же понимает правоприменитель под электронными денежными средствами. Обусловлено это тем, что и законодательство данных понятий не содержит и не разграничивает их»¹.

Легальное определение *электронных денежных средств* содержится в п. 18 ст. 3 Федерального закона от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе»: это денежные средства, предварительно предоставленные одним лицом другому, осуществляющему учет информации о размере предоставленных денежных средств без открытия банковского счета. *Безналичные денежные средства*, в свою очередь, представляют собой средства на банковских счетах, движение которых осуществляется в рамках обязательственных правоотношений клиента с банком².

Правоприменительная практика демонстрирует различные подходы к разграничению указанных понятий. В одном из приговоров суд приравнял безналичные денежные средства к электронным, указав, что обвиняемый

¹ Волосова Н.Ю., Филиппова Е.О. К вопросу о практической значимости разграничения понятий «безналичные денежные средства» и «электронные средства платежа» как предмета хищения // Аграрное и земельное право. 2025. № 3. С. 18.

² О национальной платежной системе: федеральный закон от 27 июня 2011 г. № 161-ФЗ (в ред. Федерального закона от 23 мая 2025 г. № 105-ФЗ) // Собрание законодательств Российской Федерации. 2011. № 27. Ст. 3872.

путем приобретения товара с помощью похищенной банковской карты совершил кражу «электронных (безналичных) денежных средств»¹. В другом деле суд, напротив, исключил из объема обвинения хищение электронных денежных средств, но так и не конкретизировал, что именно под ними понимается².

Особую сложность представляет разграничение составов преступлений, предусмотренных п. «г» ч. 3 ст. 158, ст. 159.3 и ст. 159.6 УК РФ. По справедливому замечанию А.В. Куликова, «основным критерием разграничения хищения, предусмотренного ст. 159.6 УК РФ, и смежных деяний является прежде всего способ его совершения», тогда как предмет (безналичные или электронные денежные средства) выступает дополнительным дифференцирующим признаком при квалификации по п. «в» ч. 3 ст. 159.6 УК РФ³.

Примером правильного разграничения может служить дело, рассмотренное судом с участием сотрудников банка ФИО18 и ФИО19. Подсудимые изменили данные клиента в банковской системе и оформили фиктивные расходные ордера, похитив денежные средства. Суд отклонил довод о необходимости квалификации по ст. 159.6 УК РФ, указав, что «внесение ФИО19 изменений в профиль клиента ... само по себе не являлось способом завладения денежными средствами», поскольку фактическое хищение было осуществлено посредством оформления подложных документов, известных только обвиняемым. В данном случае компьютерные манипуляции служили не способом хищения, а способом сокрытия уже

¹ Приговор Верхнесалдинского городского суда от 18 октября 2023 г. по делу № 1361/2023. URL: <https://sudact.ru/regular/doc/5MarLTuMgbxh/> (дата обращения: 12.04.2026).

² Приговор Фрунзенского районного суда г.Иваново от 16 октября 2023 г. по делу № 1180/2023. URL: <https://sudact.ru/regular/doc/iu252oJcKBm4/?regular> (дата обращения: 12.04.2026).

³ Куликов А.В. Проблемные вопросы хищения безналичных денежных средств путем мошенничества с использованием компьютерных технологий (п. «в» ч. 3 ст. 159.6 УК РФ) // КриминалистЪ. 2025. № 4 (53). С. 63.

совершенного преступления¹.

В противоположность этому, по делу ФИО1 суд квалифицировал действия по п. «в» ч. 3 ст. 159.6 УК РФ, поскольку подсудимая, являясь специалистом офиса продаж, неправомерно оформила на имя клиента кредитную карту и кредиты, изменяя данные в компьютерной системе и подписывая документы электронной подписью. Суд указал, что «ФИО1 не просто тайно изымала деньги, а активно вводила в заблуждение банковскую систему, изменяя данные, оформляя кредиты от имени потерпевшего», а «обман был направлен не на человека, а на автоматизированную систему»².

Таким образом, проблема разграничения безналичных и электронных денежных средств как предмета хищения требует не только законодательного уточнения дефиниций, но и выработки единообразных подходов к квалификации с учетом способа совершения преступления.

Криптовалюта представляет собой наиболее дискуссионный объект с точки зрения признания ее предметом хищения. Отсутствие легального определения криптовалюты в российском законодательстве, а также ее нематериальная природа порождают множество теоретических и практических проблем.

В Федеральном законе от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» дано определение цифровой валюты как совокупности электронных данных (цифрового кода или обозначения), которые могут быть приняты в качестве средства платежа, не являющегося денежной единицей РФ³. Однако, как справедливо отмечают

¹ Приговор Вельского районного суда (Архангельская область) от 29 июля 2024 г. по делу № 1-107/2024. URL: <https://sudact.ru/regular/doc/Ta6bOG9K6A1p/> (дата обращения: 20.04.2026).

² Приговор Центрального районного суда г. Тольятти (Самарская область) от 14 мая 2020 г. по делу № 1-262/2020. URL: <https://sudact.ru/regular/doc/7A5Kp6LDx6gQ//> (дата обращения: 20.04.2026).

³ О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: федеральный закон от 31 июля

Д.Н. Химеденова и Т.И. Горбачева, «вряд ли представляется возможным говорить о тождественности понятий «цифровая валюта» и «криптовалюта»», поскольку у цифрового рубля, эмитентом которого выступает Банк России, имеется официальный статус национальной валюты, тогда как у криптовалюты аналогичный статус отсутствует¹.

В доктрине сложились четыре основных подхода к правовой природе криптовалюты: 1) как денежного средства (Д.А. Мягков², Ю.И. Овчинникова³); 2) как денежного суррогата (В.И. Тюнин⁴); 3) как имущественного права (М.М. Долгиева⁵); 4) как иного имущества (А.А. Белоусов, Е.В. Сильченко, А.М. Васильев⁶). Наиболее обоснованной представляется последняя позиция, позволяющая квалифицировать криптопреступления по соответствующим статьям УК РФ о хищениях.

С 3 марта 2026 г. действует Федеральный закон от 20 февраля 2026 г. №38-ФЗ «О внесении изменений в статью 104.1 Уголовного кодекса Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации».

2020 г. № 259-ФЗ // Собрание законодательства Российской Федерации. 2020. № 31. Ст. 5018.

¹ Химеденова Д.Н., Горбачева Т.И. Актуальные проблемы нормативного закрепления феномена криптовалюты в Российской Федерации // Полицейская и следственная деятельность. 2025. № 3. С. 17.

² Мягков Д.А. Использование криптовалюты (к вопросу об уголовной ответственности) // Безопасность личности, общества и государства: теоретико-правовые аспекты: сборник научных статей XV международной научной конференции обучающихся, адъюнктов и аспирантов, проводимой в рамках II Санкт-Петербургского международного молодежного научного форума «Северная Пальмира: территория возможностей». СПб., 2022. С. 327.

³ Овчинникова Ю.И. Киберпреступность-новый вид преступности // Актуальные вопросы применения российского права: материалы III научно-практической конференции. Национальный исследовательский Мордовский государственный университет им. Н. П. Огарева. Саранск, 2023. С. 91.

⁴ Тюнин В.И. Криптовалюта - предмет преступления? // Правда и Закон. 2022. № 1 (19). С. 44.

⁵ Долгиева М.М. Противодействие криптопреступности уголовно-правовыми средствами // Актуальные проблемы российского права. 2023. Т. 18. № 2 (147). С. 171.

⁶ Белоусов А.А., Сильченко Е.В., Васильев А.М. Криптовалюта и проблемы в ее законодательном регулировании // Современный ученый. 2022. № 2. С. 231.

Федерации»¹, в соответствии с которым криптовалюта признана имуществом для целей УК РФ и УПК РФ.

Следует отметить, что и до этого судебная практика шла по пути признания криптовалюты имуществом. В определении Восьмого кассационного суда общей юрисдикции от 21 декабря 2023 г. указано, что, «несмотря на отсутствие прямого законодательного регулирования оборота криптовалюты, она обладает признаками имущества, в связи с чем ее хищение влечет уголовную ответственность»². Аналогичная позиция отражена в приговоре от 21 сентября 2020 г., где суд указал, что «биткойны являются виртуальной валютой»³.

Особую сложность представляет определение размера ущерба при хищении криптовалюты. Как указывается в статье Е.В. Ивановой, применяются следующие подходы: оценка по курсу на момент совершения правонарушения; учет упущенной выгоды; привлечение экспертов. В качестве примера приведена схема, где участница преступной группы, получившая оплату в биткойнах за сбыт наркотиков, конвертировала 1,79558113 BTC в 1 831 221,22 руб., что было признано приемлемым для определения суммы ущерба⁴.

Одним из наиболее значимых нововведений в цифровизации финансовой сферы стало внедрение с 2023 г.⁵ в правовое поле Российской

¹ О внесении изменений в статью 104.1 Уголовного кодекса Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации: федеральный закон от 20 февраля 2026 г. №38-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

² Кассационное определение Восьмого кассационного суда общей юрисдикции от 21 декабря 2023 г. № 77-5316/2023. Доступ из справ.-правовой системы «КонсультантПлюс».

³ Приговор Пугачевского районного суда Саратовской области от 21 сентября 2020 г. по делу № 1123/2020. URL: <https://sudact.ru/regular/doc/AvQ1uGGjwD1w>(дата обращения: 20.04.2026).

⁴ Иванова Е.В. Криптовалюта как предмет хищения: теоретический и практический аспекты // Материалы Алтайского филиала РАНХиГС. Барнаул, 2024. С. 123.

⁵ О внесении изменений в статьи 128 и 140 части первой, часть вторую и статьи 1128 и 1174 части третьей Гражданского кодекса Российской Федерации: федеральный закон от 24 июля 2023 г. № 339-ФЗ // Собрание законодательства Российской Федерации. 2023. № 31 (ч. III). Ст. 5765.

Федерации цифрового рубля – третьей формы национальной валюты наряду с наличными и безналичными денежными средствами. В условиях роста киберпреступности и хищений безналичных денежных средств особую актуальность приобретает вопрос о признании цифрового рубля самостоятельным предметом преступных посягательств, в первую очередь – хищений и мошенничества с использованием электронных средств платежа (ст. 159.3 УК РФ).

В соответствии с изменениями, внесенными в ст. 128 ГК РФ, цифровой рубль отнесен к категории безналичных денежных средств. Однако с точки зрения юридической и экономической сущности он обладает рядом специфических характеристик, отличающих его как от классических безналичных денег, так и от иных электронных платежных средств. Согласно разъяснениям Банка России, цифровой рубль является цифровой формой российской национальной валюты, которая эмитируется исключительно Центральным банком и хранится не на банковских счетах в коммерческих банках, а в цифровых кошельках на платформе Банка России. Это принципиально меняет механизм расчетов: оператором платформы выступает мегарегулятор, а не коммерческие кредитные организации¹.

С точки зрения гражданско-правового режима, цифровой рубль, в отличие от криптовалют (биткоин, эфириум), не является децентрализованным активом или денежным суррогатом. Он имеет официальный статус законного платежного средства, обязательного к приему на всей территории Российской Федерации. Вместе с тем, в отличие от безналичных денег на банковских счетах, цифровой рубль не участвует в механизме создания «частичных резервов» коммерческих банков и не может быть объектом кредитования со стороны последних. Данная особенность порождает дискуссию о его природе: некоторые авторы (А.В. Сарнакова, Н.С.

¹ Князькина А.К. Цифровая валюта как предмет хищения (на примере цифрового рубля) // Право и государство: теория и практика. 2025. № 3. С. 196.

Жижин¹) относят цифровой рубль к разновидности электронных денежных средств в смысле Федерального закона от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе», поскольку он существует вне банковской системы в виде записей на специализированной платформе и не требует открытия банковского счета.

Наиболее обоснованной представляется позиция, согласно которой цифровой рубль следует рассматривать в качестве самостоятельного предмета преступного посягательства, обладающего признаками электронных денежных средств².

Несмотря на формальное включение цифрового рубля в перечень объектов гражданских прав, уголовное законодательство не содержит прямого указания на него как на самостоятельный предмет преступления. Это порождает правовую неопределенность и риск судебных ошибок. Представляется необходимым унифицировать понимание цифрового рубля на межотраслевом уровне, закрепив его легальное определение в специальном правовом акте с одновременным дополнением примечания к ст. 158 УК РФ указанием на то, что к «иному имуществу» относятся также безналичные денежные средства, электронные денежные средства, включая цифровой рубль. Такой подход соответствует принципу правовой определенности и позволит правоприменителю единообразно квалифицировать деяния, связанные с хищением цифровой национальной валюты.

При этом важно разграничивать: цифровой рубль как предмет (сами денежные средства, находящиеся в цифровом кошельке) и электронное средство платежа (инструмент доступа к этому кошельку – пароли, биометрические данные, токены).

Как подчеркивает В.П. Лещенко, электронное средство платежа выступает средством (или орудием) удостоверения прав на денежные

¹ Сарнакова А.В., Жижин Н.С. Вопросы соотношения безналичных денежных средств, электронных денежных средств и цифрового рубля // Юрист. 2022. № 5. С. 26.

² Князькина А.К. Указ. соч. С. 198.

средства, в то время как предметом хищения остаются сами цифровые рубли. Ученый подчеркивает, что «анализ действующего законодательства и доктринальных позиций, характеризующих электронное средство платежа как категорию, имеющую уголовно-правовое значение, позволяет утверждать, что понятие электронного средства платежа не ограничивается лишь его физическими качествами – платежными картами, терминалами или мобильными устройствами. Оно включает также программные решения, а в отдельных случаях и совокупность действий клиента, направленных на удостоверение его полномочий»¹.

Проведенный анализ позволяет сформулировать следующие выводы:

1. Традиционное понимание предмета хищения, основанное на физическом (материальном) признаке, утратило исключительный характер в условиях цифровизации экономики. Принятие Федерального закона от 23 апреля 2018 г. № 111-ФЗ и разъяснения Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 фактически расширили предмет хищения за счет включения безналичных и электронных денежных средств, что потребовало пересмотра момента окончания преступления и привело к трансформации формальных составов (например, кражи).

2. Действующее уголовное законодательство не содержит четкого разграничения между «безналичными денежными средствами» и «электронными денежными средствами». Это порождает противоречивую судебную практику, в том числе случаи необоснованного приравнивания указанных понятий либо, напротив, исключения их из объема обвинения без должной мотивировки. Необходимо законодательное уточнение дефиниций на межотраслевом уровне.

3. С введением цифрового рубля (третьей формы национальной валюты) возникла необходимость его унификации как предмета преступления. Обладая

¹ Лещенко В.П. Цифровой рубль как предмет мошенничества с использованием средств электронного платежа (ст. 159.3 Уголовного кодекса Российской Федерации) // *Iuspublicumetprivatum*. 2025. № 3 (31). С. 127-128.

признаками электронных денежных средств, но имея официальный статус законного платежного средства, цифровой рубль не тождественен ни классическим безналичным деньгам, ни децентрализованным криптовалютам. Целесообразно прямое включение цифрового рубля в примечание к ст. 158 УК РФ в качестве разновидности «иного имущества» для обеспечения единообразия правоприменения.

2.2. Способы хищений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации

Способ преступления – «это совокупность действий по подготовке, совершению и сокрытию преступления, объединенная общим замыслом, обусловленная объективными и субъективными факторами и сопряженная с использованием соответствующих орудий и средств»¹. Исходя из определения, данный элемент включает в себя три структурных части, что позволяет выделить две разновидности способа преступления: полноструктурный, включающий в себя подготовку, совершение и сокрытие, и неполноструктурный, когда один из перечисленных элементов отсутствует. При расследовании указанной категории преступлений зачастую сложно определить все три элемента. Например, стадия подготовки будет отсутствовать у преступлений, совершенных с внезапно возникшим умыслом.

Проведенное исследование, выразившееся в изучении научной литературы, а также анализе судебно-следственной практики, позволило выделить следующие наиболее типичные способы осуществления рассматриваемой преступной деятельности.

1. Преступник через систему дистанционного банковского обслуживания перечисляет на счет потерпевшего значительную сумму, после

¹ Шкеле М.В. Способ совершения преступления и его уголовно-правовое значение: дис. ... канд. юрид. наук. СПб., 2001. С. 8-9.

чего обращается к нему с просьбой вернуть денежные средства. Нередко мошенник предлагает потерпевшему лицу оставить «комиссию» от возвращенной суммы. После того, как потерпевший отзывается на просьбу преступника и осуществляет обратный перевод денежных средств, преступник подает в банк заявление о производстве ошибочного перевода. Тем самым, денежные средства списываются с банковского счета потерпевшего повторно и зачисляются на счет мошенника. Как показал анализ приговоров, данный способ совершения преступления встречался в 6% случаев.

2. «Социальная инженерия». Данный способ заключается в том, что потерпевший добровольно сообщает злоумышленнику реквизиты банковской карты либо самостоятельно переводит денежные средства в связи с оказываемым на него психологическим воздействием или обманом¹.

Пандемия коронавируса наглядно показала, как киберпреступники подстраиваются и продолжают подстраиваться под сложившуюся геополитическую ситуацию в стране и в мире. Так, злоумышленники активно использовали социальную инженерию, эксплуатацию темы COVID-19 во вредоносных рассылках, играя на человеческом факторе – интерес, опасение за здоровье, желание быть осведомленным о текущей ситуации, связанной с пандемией и т.д. Кроме того, преступники активно использовали неотъемлемые элементы пандемии: продажа фейковых цифровых пропусков, рассылка сообщений о штрафах за нарушение карантина, липовые сайты курьерских служб, мошеннические рассылки от имени сервиса видеоконференций Zoom и т.д.

Одной из разновидностей социальной инженерии является получение информации об SMS-сообщениях, подтверждающих совершение транзакции в системе дистанционного банковского обслуживания. К примеру, лицо на

¹ Боровик П.Л., Пилюшин С.В. Хищение имущества путем модификации компьютерной информации: анализ способов и рекомендации по проведению проверочных мероприятий // Юстиция Беларуси. 2024. № 8 (269). С. 54.

определенном интернет-ресурсе разместило объявление о продаже автомобиля. Данному лицу поступает телефонный звонок от «потенциального покупателя», в ходе которого он выясняет состояние автомобиля и условия осуществления сделки, после чего покупатель дает согласие на приобретение товара и говорит о том, что переведет денежные средства на банковскую карту в качестве задатка. Для осуществления перевода он просит у лица назвать код авторизации транзакции, указанный в SMS-сообщении, поступившем на телефон продавца. Получив необходимую информацию, мошенники списывают денежные средства с банковского счета¹.

Как показал анализ приговоров, данный способ совершения преступления встречался в 46% случаев.

3. Получение доступа к счету потерпевшего в системе дистанционного банковского обслуживания посредством вредоносных программ, позволяющих собирать данные о реквизитах входа в систему (логин и пароль), а также выполнять иные задачи тайно или открыто от законного пользователя. Такие вредоносные программы зачастую нарушают работу ранее установленного программного обеспечения.

Действительно, одним из излюбленных способов совершения киберкраж у злоумышленников является «фишинг», цель которого состоит в получении логинов и паролей жертвы. Данная цель достигается путем рассылки спам сообщений, содержащих ссылки (зеркала) на вредоносные файлы, замаскированные под официальные сайты известных фирм. Перейдя по ссылке происходит скачивание вредоносного файла либо пользователь вводит данные учетной записи, так как зеркало сайта визуально неотличимо от оригинала.

В последнее время вновь участились случаи атак вредоносных программ ransomware (вымогатели). Суть программ заключается в шифровании данных на ЭВМ пользователя и требования передачи денежных средств для

¹ Приговор Королевского городского суда Московской области от 14 апреля 2021 г. по делу № 1-204/2021. URL: Sudact.ru (дата обращения: 24.02.2026).

разблокировки данных. Данные программы являются вирусом, детектировать которые помогут антивирусные программы и утилиты.

С попаданием вредоносной программы в устройство она отправляет запрос на установление баланса привязанной к номеру банковской карты, после чего денежные средства со счета потерпевшего начинают поступать на банковские счета, подконтрольные злоумышленникам. Данные действия происходят втайне от потерпевшего, поскольку вредоносное программное обеспечение скрывает уведомления, поступающие на принадлежащее потерпевшему устройство.

Преступниками специально создаются банковские счета, к которым они привязывают несколько платежных карт. После поступления денежных средств на карту, «дроп» – лицо, на имя которого оформлена карта, снимает их в банкомате. Исследователи отмечают, что «после снятия денежных средств «дроп» передает их организатору, оставляя себе определенный процент в качестве вознаграждения. В качестве субъекта, на банковский счет которого осуществляется перевод денежных средств потерпевшего, может также выступать подставное юридическое лицо»¹.

Как показал анализ приговоров, данный способ совершения преступления встречался в 8% случаев.

4. Следующий способ основан на использовании вредоносного программного обеспечения для операционных систем современных смартфонов. Данные способы характеризуются высокой опасностью, поскольку на сегодняшний день в смартфонах хранится большой объем конфиденциальной информации, например, реквизиты банковской карты, данные для входа в систему дистанционного банковского обслуживания и др. Например, при использовании вредоносного программного обеспечения «троянского типа» злоумышленники получают практический полный доступ

¹ Боровик П.Л., Пилюшин С.В. Хищение имущества путем модификации компьютерной информации: анализ способов и рекомендации по проведению проверочных мероприятий // Юстиция Беларуси. 2024. № 8 (269). С. 54.

к мобильному телефону, имея возможность перехватывать как входящие, так и исходящие SMS-сообщения, подключать различные услуги посредством USSD-запросов, добавлять контакты в черный список, отображать диалоговое окно или сообщение в соответствии с полученными с управляющего сервера параметрами¹.

Как показал анализ приговоров, данный способ совершения преступления встречался в 6% случаев.

5. Оформление займов или кредитных карт на третьих лиц без их ведома. Поступившие от банка денежные средства обналичиваются либо производится оплата ими различных товаров, работ, услуг. Пособниками при совершении подобного рода хищений выступают, как правило, банковские работники, недобросовестно выполняющие свои служебные обязанности и осуществляющие идентификацию заемщика ненадлежащим образом.

Кроме того, распространенным способом является оформление кредита на третьих лиц с использованием их паспортных данных. В информационную систему банковского обслуживания вносятся недостоверные сведения, подписываются необходимые для оформления кредита документы.

В результате таких действий у потерпевшего появляется обязательство перед банком по выплате кредита, которого он не получал. При этом пострадавшее лицо остается неосведомленным относительно совершенных в отношении него мошеннических действий пока не получит претензию от банка по выплате платежа. Поскольку льготный период у различных банков по времени может быть длительным, время совершения преступления будет значительно отличаться от времени начала расследования.

Как показал анализ приговоров, данный способ совершения преступления встречался в 6% случаев.

¹ Федорова В.С., Лялюк А.В. О мошенничестве с использованием платежных карт // Проблемы развития предприятий: теория и практика: сборник статей VIII Международной научно-практической конференции. Пенза, 2021. С. 213.

6. Одним из способов такого рода преступлений выступает незаконное использование злоумышленником кредитной карты втайне от ее легитимного держателя. Как показал анализ приговоров, данный способ совершения преступления встречался в 4% случаев.

7. Совершение хищения посредством использования поддельных платежных карт. При данном способе с помощью поддельной платежной карты могут оплачиваться товары и услуги, как через Интернет, так и через POS-терминалы, а также может осуществляться перевод денежных средств на другой банковский счет. Среди проанализированных приговоров данный способ совершения преступления не встречался.

8. Хищения, совершенные посредством использования ранее похищенной банковской карты, законный держатель которой своевременно не заблокировал ее¹.

Так, Л. взял не принадлежащую ему банковскую карту С. и, увидев, что карта оснащена функцией бесконтактной оплаты, реализовав внезапно возникший у него умысел на тайное хищение денежных средств, решил совершать хищения суммами до 1 000 рублей до тех пор, пока на счете не закончатся денежные средства. Свой умысел Л. реализовал в нескольких магазинах, осознавая, что карта и денежные средства ему не принадлежат, а окружающие не понимают преступный характер его действий. Всего Л. похитил денежные средства в сумме 7 470 рублей, причинив потерпевшей значительный ущерб². Действия виновного были квалифицированы по п. «г» ч. 3 ст. 158 УК РФ как кража с банковского счета.

Как показал анализ приговоров, данный способ совершения преступления встречался в 4% случаев.

¹ Вирясова Н.В., Землянова А.Н. Проблемы раскрытия и расследования отдельных видов преступлений, совершенных с использованием информационно-телекоммуникационных технологий // Современная научная мысль: материалы VII Всероссийской научно-практической конференции. Чебоксары, 2021. С. 48.

² Приговор Свердловского районного суда г. Иркутска от 26 сентября 2018 г. по делу № 1-700/2018. URL: <https://sudact.ru/regular/doc/WoQc0Xo0IV14/> (дата обращения: 19.02.2026).

9. Скимминг – это негласный способ получения информации, имеющей конфиденциальный характер (реквизиты банковской карты, ПИН-код и т. д.), с помощью специального считывающего устройства – скиммера.

Скимминговые устройства функционируют по двум основным принципам. Одни передают полученную информацию по радиоканалу, другие – записывают данную информацию на встроенный электронный носитель. Вся информация, записанная на магнитной полосе карты, в последующем переносится на магнитные полосы специально заготовленных банковских карт с помощью энкодера. Тем самым злоумышленник получает дубликат банковской карты и может в дальнейшем проводить любые операции с ней.

Как показал анализ приговоров, данный способ совершения преступления встречался в 2% случаев.

10. Разновидностью скимминга является установка поддельных платежных терминалов или банкоматов, которые копируют реквизиты банковской карты и с помощью энкодера отправляют их на дубликат банковской карты для последующего воспроизведения. Среди проанализированных уголовных дел данный способ совершения преступления не встречался.

11. Введение в информационно-коммуникационную систему «банк-банкомат» вредоносного программного обеспечения, основной задачей которого является копирование и передача данных банковской карты законного держателя для их последующего воспроизведения. Как показал анализ уголовных дел, данный способ совершения преступления встречался в 2% случаев.

12. Размещение на интернет-сервисах, таких как «Авито», «Молоток», «Юла», «Из рук в руки» и др. фиктивных объявлений о продаже товаров или оказании услуг, условием которых является обязательная предоплата. Потерпевшие, введенные в заблуждение относительно истинных намерений лица, разместившего объявление, перечисляют на банковскую карту, реквизиты которой указаны в объявлении, сумму предоплаты. Как правило,

банковские карты, используемые злоумышленниками, оформлены на подставных лиц.

Как показал анализ приговоров, данный способ совершения преступления встречался в 4% случаев.

13. Создание злоумышленниками веб-сайтов, дизайн, название и функциональные возможности которых схожи с официальными сайтами организаций, занимающихся торговлей в сети Интернет или оказанием услуг финансового характера. Стоит отметить, что создаваться могут, в том числе и клоны мобильных приложений, функционирующих на современных смартфонах. Чаще всего мошенники подделывают сайты широко известных интернет-магазинов, авиакомпаний, платежных систем и т.п.¹

Среди проанализированных приговоров данный способ совершения преступления не встречался.

14. Использование реквизитов пользователя для осуществления входа в систему дистанционного банковского обслуживания злоумышленниками, которым эти данные стали известны в силу недостаточной осмотрительности потерпевшего. Поскольку сотрудниками организации или членами семьи может использоваться один персональный компьютер, логин и пароль, используемые определенным лицом для входа в «Личный кабинет» в системе дистанционного банковского обслуживания, могут стать известны остальным пользователям. При первом введении реквизитов, система предлагает их сохранить для последующего упрощенного входа, в результате чего другой пользователь получает беспрепятственный доступ в личный кабинет владельца банковского счета.

М.А. Бугера отмечает, что «одним из видов данного способа является получение доступа преступником к мобильному телефону, к абонентскому номеру которого привязана банковская карта. Воспользовавшись тем, что

¹ Бугера М.А. Особенности использования специальных знаний при расследовании преступлений, связанных с хищением денежных средств с банковских счетов, с использованием вредоносных компьютерных программ // Форум. 2023. № 1 (30). С. 145.

действия мошенника никто не отслеживает, он переводит денежные средства от имени легитимного владельца на счет своей банковской карты или банковской карты третьего лица»¹.

Как показал анализ приговоров, данный способ совершения преступления встречался в 2% случаев.

15. Распространение в сети Интернет и среди абонентов сотовой связи ложных сведений относительно возможности наступления негативных последствий. Например, сообщение о госпитализации родственника либо привлечении близкого лица к уголовной или административной ответственности. Для оказания помощи мошенники уговаривают перечислить денежные средства на указанный ими счет.

Приведем примеры некоторых подобных преступлений. Так, в ходе следствия был задержан В., который, находясь по месту жительства, осуществлял звонки потерпевшим, представлялся сотрудником службы безопасности банка, под различными предложениями выяснял у потерпевших реквизиты банковских карт, после чего тайно похищал со счетов денежные средства. В ходе следственных действий у В. изъяты телефоны и сим-карты, используемые им при совершении преступлений².

В другом случае в ходе следствия был задержан П., который совместно с группой неустановленных лиц с банковских счетов потерпевших тайно похищал денежные средства путем совершения звонков по средствам IP-телефонии. Роль У. заключалась в обналаживании похищенных денежных средств. В ходе следственных действий у П. были изъяты банковские карты, оформленные на номинальных лиц, компьютерная техника и мобильные устройства³.

¹ Бугера М.А. Указ. соч. С. 145.

² Приговор Железнодорожного районного суда г. Пензы от 19 ноября 2019 г. по делу № 1-405/2019. URL: Sudact.ru (дата обращения: 19.02.2026).

³ Приговор Промышленного районного суда г. Ставрополя от 25 августа 2022 г. по делу № 1-724/2022. URL: Sudact.ru (дата обращения: 19.02.2026).

Как показал анализ приговоров, данный способ совершения преступления встречался в 10% случаев.

Необходимо отметить, что представленный нами перечень способов хищений не является исчерпывающим и постоянно обновляется в силу появления усовершенствованных программных и технических средств, а также изменяющейся политической, социальной обстановке в стране и мире.

Далее необходимо проанализировать существующие способы сокрытия следовой картины рассматриваемой преступной деятельности. При этом одной из особенностей таких действий является их преимущественное осуществление еще на стадии подготовки к совершению преступлений.

1. Одним из самых распространенных способов сокрытия преступлений, совершаемых в сфере дистанционных банковских технологий, является обналичивание денежных средств, добытых преступным путем, через электронные кошельки и электронные платежные системы, зарегистрированные на подставных лиц.

2. Осуществление криминальных взаиморасчетов криптовалютой. Данный способ также пользуется большой популярностью среди ИТ-мошенников, поскольку операции с криптовалютой не требуют ведения специальной отчетной документации и обеспечивают относительную анонимность сторон. При регистрации транзакции ей присваивается уникальный номер, который привязывается не к лицу, а к электронному кошельку. Зачастую данные кошельки открыты на третьих лиц.

Существует множество специальных сайтов, позволяющих выводить криптовалюту и обменивать ее на фиатные деньги. Кроме того, денежные средства с электронных кошельков могут переводиться в другие страны, т.е. за пределы национальной юрисдикции, что объясняет распространенность

данного способа в схемах по легализации доходов, полученных преступным путем¹.

3. Соккрытие подлинных персональных данных от провайдера при подключении к сети Интернет. По-прежнему можно получить SIM-карту, не проходя процедуру идентификации.

4. Осуществление входа в сеть Интернет через серверы, предоставляющие пользователю зарубежные IP-адреса, находящиеся вне юрисдикции Российской Федерации.

5. Использование ремейлеров. Посредством данного сервера отправитель электронного сообщения остается неизвестным, поскольку в процессе переправления почтового сообщения адресату вся информация об отправителе уничтожается.

6. Использование анонимайзеров – таких средств, посредством которых можно изменить электронный адрес отправителя сообщения. Необходимо отметить, что при использовании анонимайзеров остается возможным установить IP-адрес компьютера.

7. Отправка электронных сообщений через почтовый ящик, при регистрации которого указывались вымышленные данные.

8. Использование Rootkit – набора программных средств, устанавливаемого злоумышленником на взломанную им информационную систему и обеспечивающего маскировку объектов (процессов, драйверов, файлов и т.д.).

9. Использование сети – бесплатного и открытого программного обеспечения, которое дает пользователям анонимный доступ в Интернет. Название Tor – TheOnionRouter – «луковый маршрутизатор» отсылает к принципу его работы. Пользователь, соединяется с сетевыми ресурсами через

¹ Макаров Р.А. Расследование хищений, совершенных с использованием информационно-телекоммуникационных технологий: обзор криминалистических методик и направления изучения // Юридическая наука и практика. 2023. № 1. С. 68.

цепочку прокси-серверов, каждый из которых видит лишь предшествующий и последующий маршрутизатор цепочки.

Как правило, такая цепочка состоит из трех случайных узлов, каждому из них не известны IP-адрес пользователя и адрес конечного веб-ресурса. Дойдя до конечного узла сети Tor, данные вновь попадают в сеть Интернет. Кроме того, благодаря шифрованию неизвестно содержимое передаваемой информации. Технология Tor также обеспечивает защиту от механизмов анализа трафика пользователя.

10. Использование VPN (Virtual Private Network). VPN – это виртуальная частная сеть, в названии которой отражена суть этой технологии. Она позволяет установить виртуальное соединение (туннель) поверх другой сети (например, сеть Интернет). Использование VPN повышает уровень приватности. Защита заключается в том, что вся передаваемая с технического устройства информация по VPN-туннелю шифруется тем или иным алгоритмом шифрования, за счет чего другие пользователи не могут получить доступ к этой информации для ее прочтения или модификации¹.

Проведенный анализ способов хищений в сфере информационно-телекоммуникационных технологий и компьютерной информации позволяет сформулировать ряд ключевых выводов:

1. В работе обоснованно выделено 15 конкретных способов совершения преступлений и 10 способов их сокрытия. Данная классификация наглядно демонстрирует высокую степень адаптивности преступной среды к развитию цифровых технологий. Способы варьируются от простых (хищение с незаблокированной карты) до сложных технических решений (использование вредоносного программного обеспечения, скимминг, фишинг) и методов социальной инженерии.

2. Анализ приговоров, приведенный в тексте, показывает, что наиболее

¹ Челпанов Е.С. Хищение с банковского счета и равно в отношении электронных денежных средств // Актуальные научные исследования в современном мире. 2021. № 1-9 (69). С. 319.

распространенным способом является «социальная инженерия» (46% случаев). Это подтверждает тезис о том, что основным уязвимым звеном в системах безопасности остается человек, а не техника. Преступники эффективно эксплуатируют базовые человеческие чувства (страх, доверие, жадность, желание помочь), что позволяет им получать конфиденциальные данные добровольно.

3. Значительная доля хищений совершается с использованием специализированного программного обеспечения (8% – вредоносные программы для персональных компьютеров, 6% — для смартфонов, а также скимминг и атаки на банкоматы). Это указывает на профессионализацию киберпреступности, требующую от злоумышленников навыков программирования и знания уязвимостей операционных систем и банковского оборудования. Особую опасность представляют трояны для мобильных устройств, дающие практически полный контроль над телефоном жертвы.

4. Выявленные способы можно классифицировать в зависимости от объекта преступного посягательства: а) непосредственно денежные средства жертвы (социальная инженерия, хищение карт); б) персональные данные и реквизиты доступа (фишинг, вредоносное программное обеспечение); в) кредитные средства (оформление займов на третьих лиц). Последняя категория представляет повышенную общественную опасность, так как потерпевший длительное время может не знать о возникших у него долговых обязательствах, что существенно затрудняет своевременное начало расследования.

5. Преступники активно используют современные технологии для сокрытия следов: обналачивание через криптовалюты и электронные кошельки (обеспечивающие анонимность), использование VPN, Tor, анонимайзеров и подмену IP-адресов. Это создает серьезные препятствия для правоохранительных органов при установлении личности преступника и маршрутов движения похищенных средств, требуя от следователей и криминалистов глубоких знаний в области цифровой гигиены и методов

деанонимизации.

2.3. Обстановка и следы хищений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации

В структуре криминалистической характеристики преступления обстановка его совершения представляет собой систему взаимосвязанных элементов окружающей среды (объектов, явлений, процессов), оказывающих влияние на механизм преступления и следообразования. Как справедливо отмечает А.А. Бессонов, «обстановка имеет пространственно-временные границы, обусловленные совершенным деянием, а изучение закономерностей связей между элементами этой системы и следами механизма преступления служит основой для разработки частных методик расследования»¹.

Хищения, совершаемые с использованием информационно-телекоммуникационных технологий, обладают существенной спецификой обстановки, обусловленной удаленностью взаимодействия субъектов, использованием виртуальной среды и технических устройств, находящихся в различных юрисдикциях. Традиционное понимание места и времени преступления, разработанное в рамках общей криминалистики, требует существенной адаптации применительно к данной категории дел.

Определение места совершения хищения с использованием информационно-телекоммуникационных технологий является одной из наиболее сложных задач первоначального этапа расследования.

¹ Бессонов А.А. Обстановка преступления как элемент его криминалистической характеристики // Вестник Саратовской государственной юридической академии. 2014. № 6. С. 158.

В классическом понимании место преступления – это конкретный географический пункт, где было совершено общественно опасное деяние¹. Однако при использовании сети Интернет, удаленного доступа и распределенных информационных систем данное понятие трансформируется.

В криминалистической литературе обоснованно ставится вопрос «о введении показателя «множественность мест» применительно к хищениям, совершаемым с использованием информационно-телекоммуникационных технологий»². В механизме одного преступления может быть задействовано от двух и более географических точек: местонахождение преступника (преступников), место нахождения серверов, место нахождения устройства потерпевшего, место, где было фактически изъято имущество (например, банкомат для обналичивания).

Как указывает Д.И. Шнейдерова, «местом совершения преступления следует признавать фактическое местонахождение преступника в момент реализации объективной стороны хищения (например, ввода неправомерных команд в информационную систему). При наличии нескольких соисполнителей, находящихся территориально отдаленно друг от друга, местонахождение каждого из них в момент совершения объективной стороны следует считать самостоятельным местом совершения хищения, что и образует показатель множественности мест»³.

Так, приговором Уссурийского районного суда Приморского края от 6 июня 2017 г. по делу № 1-513/2017 установлено, что подозреваемый З., находясь на территории одного субъекта РФ, приобрел вредоносную

¹ Старостенко Н.И. Совершенствование криминалистического взаимодействия при расследовании хищений, совершенных с использованием методов социальной инженерии, реализуемых при помощи информационно-телекоммуникационных технологий // Российский следователь. 2023. № 1. С. 11.

² Баранов С.А. Проблемы противодействия мошенничествам, совершаемым с использованием средств мобильной связи // Противодействие преступлениям в сфере информационных технологий: материалы международной научно-практической конференции. Белгород, 2022. С. 22-23.

³ Шнейдерова Д.И. Пространственный элемент обстановки совершения хищений в сфере оборота криптовалют: криминалистический аспект // Правовая культура в современном обществе. 2024. С. 307.

программу, позволяющую удаленно подключаться к мобильным устройствам, находившимся на территории другого региона, и управлять их функциями. Путем удаленного доступа он проверял баланс счетов и инициировал переводы денежных средств. Суд признал местом преступления как место нахождения самого подозреваемого (его компьютерного устройства), так и место нахождения серверов оператора сотовой связи, через которые проходили команды, хотя непосредственного контакта с имуществом потерпевшего у него не было¹.

Значительную сложность представляет установление реального места нахождения преступника при использовании сервисов-анонимайзеров (VPN, TOR, SOCKS и др.). Исследователи отмечают, что «данные технологии позволяют скрыть истинный IP-адрес и выходить в сеть под IP-адресом стороннего узла, который может находиться на территории иного государства. Выявленные в ходе оперативно-розыскной деятельности анонимизированные IP-адреса зачастую ведут к серверам, зарегистрированным в иностранных юрисдикциях, получение криминалистически значимой информации от которых затруднительно в силу корпоративной политики или международно-правовых ограничений»².

В связи с этим, как обоснованно отмечается в диссертационном исследовании К.А. Мира, «в ходе расследования необходимо разграничивать фактическое местонахождение преступника и техническое местонахождение его устройства, фиксируемое информационной системой. Географическая привязка сетевого адреса не всегда совпадает с реальным местом совершения действий»³.

¹ Приговор Уссурийского районного суда Приморского края от 6 июня 2017 г. по уголовному делу № 1-513/2017. URL: <http://ussuriysky.prm.sudrf.ru/> (дата обращения: 20.04.2026).

² Бондарь М.М., Бочаров А.А. Доказывание по уголовным делам о кражах, совершенных с использованием банковских карт: проблемные аспекты // Актуальные вопросы охраны общественного порядка и административной деятельности полиции: материалы межведомственной научно-практической конференции. М., 2021. С. 87.

³ Мира К.А. Установление механизма хищений чужого имущества с использованием информационных технологий: дис. ... канд. юрид. наук. М., 2022. С. 88-89.

Временной элемент обстановки хищений в сфере информационно-телекоммуникационных технологий также имеет существенные отличия от традиционных преступлений. Они обусловлены использованием различных способов фиксации времени активности пользователя информационными системами, а также возможностью искусственного изменения временных показателей.

Ключевым понятием здесь является различие между локальным сетевым временем (местное время государства, на территории которого находится пользовательское устройство) и универсальным координированным временем (UTC). Большинство сетевых ресурсов, предоставляющих услуги на мировом рынке, используют именно UTC, транслируя пользователю временной показатель с поправкой на его часовой пояс.

Д.И. Шнейдерова приводит следующий пример: «преступник, находясь на территории Екатеринбурга (часовой пояс UTC+5), в 15:00 совершает неправомерную транзакцию. Сервер криптокошелька, расположенный в Берлине (UTC+2), фиксирует данную транзакцию как совершенную в 12:00, а потерпевший в Минске (UTC+3) видит время 13:00. При этом момент совершения хищения един и тот же»¹. Автором обоснованно предлагается фиксировать время совершения преступления по местонахождению преступника с обязательным указанием часового пояса данного региона.

Так, приговором Братского городского суда Иркутской области от 11 января 2017 г. по делу № 1-28/2017 при осмотре компьютерной информации было установлено несоответствие времени совершения транзакций, зафиксированного на жестком диске компьютера подозреваемого, и времени, указанном в электронных журналах банковской системы. В ходе судебной компьютерно-технической экспертизы было выявлено, что локальное время на устройстве подозреваемого было умышленно изменено, тогда как серверное время (UTC) оставалось неизменным. Данное

¹ Шнейдерова Д.И. Указ. соч. С. 308.

обстоятельство позволило точно установить хронологию противоправных действий, несмотря на попытку фальсификации временных показателей¹.

Практическое значение учета часовых поясов становится очевидным при проведении следственных действий на первоначальном этапе. Отдельные исследователи отмечают, что «при осмотре компьютерной информации с устройств потерпевших отображается их локальное сетевое время, которое может не совпадать с локальным временем на устройстве преступника. В целях недопущения путаницы и обеспечения допустимости доказательств в протоколах осмотра (особенно компьютерной информации) необходимо указывать не только абсолютное значение времени, но и часовой пояс, в котором оно зафиксировано»².

Специфика обстановки хищений с использованием информационно-телекоммуникационных технологий тесно связана с действиями по сокрытию следов, которые носят, как правило, «виртуальный» характер. И.В. Поддубный отмечает, что «помимо традиционных способов сокрытия (уничтожение носителей, повреждение техники), преступники активно используют:

- использование анонимайзеров и прокси-серверов (как указывалось выше, это затрудняет установление истинного места совершения преступления);

- искусственное изменение локального времени на устройстве, что влияет на временные показатели фиксации событий в журналах операционной системы и может повлечь ошибочную интерпретацию доказательственной информации;

- использование публичных Wi-Fi сетей – при нахождении нескольких десятков устройств под одним IP-адресом в общественном месте идентификация конкретного устройства преступника существенно

¹ Приговор Братского городского суда Иркутской области от 11 января 2017 г. по делу № 1-28/2017. URL: <http://bratsky.irk.sudrf.ru/> (дата обращения: 28.04.2026).

² Шнейдерова Д.И. Указ. соч. С. 309.

затрудняется»¹.

К.А. Мира в своем исследовании подчеркивает, что при определении времени совершения преступления в случае использования VPN следует исходить из того, что устанавливаемый сервисом временной показатель (обычно соответствующий часовому поясу конечного узла) не может признаваться временем совершения хищения, если доказано использование средств анонимизации. Приоритет имеют данные о реальной активности на устройстве, установленные в ходе судебной компьютерной экспертизы².

Так, приговором Курганского городского суда Курганской области от 22 августа 2023 г. по делу № 1-564/2023 было установлено, что подозреваемый осуществлял отправку SMS-команд с подменного номера, используя услугу переадресации через несколько серверов в разных часовых поясах. Временные метки в журналах операторов сотовой связи различались на несколько часов. Суд, основываясь на заключении экспертизы, принял за точку отсчета время поступления команды на сервер банка, зафиксированное в системе UTC, с последующим пересчетом на местное время по месту нахождения подозреваемого, что позволило доказать его присутствие за компьютером в момент хищения³.

Цифровая трансформация экономических отношений, легализация криптовалют и широкое внедрение систем дистанционного банковского обслуживания детерминировали появление нового поколения криминалистически значимых следов. В структуре хищений, совершаемых с использованием информационно-телекоммуникационных технологий, традиционные материальные следы (дактилоскопические, трасологические) уступают место бинарным данным – следам в сфере компьютерной

¹ Поддубный И.В. К вопросу об использовании фигурантами информационно-коммуникационных технологий в целях сокрытия хищений с банковских счетов граждан // Вестник Удмуртского университета. Серия Экономика и право. 2020. №3. С. 424.

² Мира К.А. Указ. соч. С. 91.

³ Приговор Курганского городского суда Курганской области от 22 августа 2023 г. по уголовному делу № 1-564/2023. URL: <http://kurgansky.krg.sudrf.ru/> (дата обращения: 03.05.2026).

информации. Как справедливо отмечает К.А. Мира, при расследовании данной группы преступлений примерно 20% составляют традиционные следы, тогда как 80% следов образуется в киберпространстве. Указанное обстоятельство требует пересмотра классической теории криминалистического следоведения применительно к виртуальной среде¹.

В криминалистике под следом преступления понимается любое изменение обстановки, возникшее в результате подготовки, совершения или сокрытия деяния². В контексте хищений в сфере оборота криптовалют и компьютерной информации, как обоснованно утверждает Д.И. Шнейдерова, следует вести речь о показателе множественности мест, а, следовательно, и о множественности следовых полей³.

Анализ диссертации К.А. Мира позволяет выделить две крупные группы следов:

- традиционные следы (20%): механические повреждения устройств (скиммеры, накладки на банкоматы), следы пальцев рук на технике, предметы-документы (распечатки, договоры, чеки), следы взлома помещений;
- следы в сфере компьютерной информации (80%): записи в log-файлах, метаданные электронных документов, IP-адреса, временные штампы транзакций, следы модификации кода, дампы оперативной памяти⁴.

Механизм следообразования при ИТТ-хищениях подчиняется закономерностям взаимодействия в системе «преступник – программно-аппаратное средство – информационная система — жертва». Согласно прикладным исследованиям К.А. Мира, наиболее часто фиксируются следующие действия-следствия:

- передача компьютерной информации – 58%;
- создание компьютерной информации (в т.ч. фиктивных платежных

¹ Мира К.А. Указ. соч. С. 93.

² Россинская Е.Р., Рядовский И.А. Концепция цифровых следов в криминалистике // Аубакировские чтения: материалы Международной научно-практической конференции (19 февраля 2019 г.). Алматы, 2019. С. 6.

³ Шнейдерова Д.И. Указ. соч. С. 309.

⁴ Мира К.А. Указ. соч. С. 93.

поручений) – 55%;

- ввод компьютерной информации (команд, реквизитов) – 52%;
- модификация компьютерной информации (изменение остатка на счете) – 48%;
- копирование (скимминг, дампы базы данных) – 34%;
- удаление (логов, сообщений) – 7%.

Особого внимания заслуживает вредоносная компьютерная программа. В механизме слеодообразования вредоносное программное обеспечение оставляет:

- записи о месте размещения (патч, реестр, автозагрузка);
- логи взаимодействия с C&C (CommandandControl) серверами;
- следы инъекта кода в легитимные процессы (например, в svchost.exe или браузеры)¹.

Криптовалюта (биткоин, эфир) обладает свойством псевдоанонимности, что порождает специфические следы в блокчейне. Как уже было отмечено ранее, установление реального IP-адреса затруднено использованием сервисов-анонимайзеров (VPN, TOR, SOCKS). Однако «след» остается в самом распределенном реестре:

- транзакционный след (хэш перевода, адрес отправителя/получателя);
- временной след (метка времени блока – timestamp);
- аппаратный след (MAC-адрес устройства, если доступ к кошельку осуществлялся без VPN)².

Так, О. осуществил перевод 6000 рублей с чужой карты на свой счет посредством SMS-команды. Следовой комплекс включал: 1) традиционный след: запись в логе оператора сотовой связи (отправка сообщения на короткий номер); 2) цифровой след: модификация записи в базе данных банка о балансе счета; 3) предметный след: распечатка детализации звонков и сообщений

¹ Семикаленова А.И. Цифровые следы: назначение и производство экспертиз // Вестник Университета имени О.Е. Кутафина. 2019. № 5 (57). С. 116.

² Шнейдерова Д.И. Указ. соч. С. 309.

(приобщена к делу как вещественное доказательство)¹.

Для признания компьютерных следов допустимыми доказательствами необходимо соблюдение требований УПК РФ и ведомственных стандартов. В ходе осмотра места происшествия следователь должен руководствоваться алгоритмом, предложенным К.А. Мира:

- 1) фиксация состояния техники (включена/выключена);
- 2) сохранение дампа оперативного запоминающего устройства (содержит временные следы);
- 3) изъятие носителя с участием специалиста;
- 4) обязательное указание в протоколе часового пояса.

Проведенное исследование обстановки и механизмов следообразования при хищениях, совершаемых с использованием информационно-телекоммуникационных технологий и в сфере компьютерной информации, позволяет сформулировать следующие ключевые выводы:

1. Обстановка хищений, совершаемых с использованием информационно-телекоммуникационных технологий, характеризуется множественностью географических точек (местонахождение преступника, серверов, устройства потерпевшего, банкомата и др.), что требует отказа от классического понимания единого места преступления. Для целей расследования каждое территориально обособленное место нахождения соисполнителя либо технического узла, задействованного в механизме деяния, признается самостоятельным местом совершения преступления. Использование сервисов-анонимайзеров (VPN, TOR, SOCKS) дополнительно затрудняет установление реального местонахождения злоумышленника.

2. Временной элемент обстановки ИТТ-хищений обладает высокой степенью латентности из-за различий локального сетевого времени, применения универсального координированного времени (UTC) и

¹ Приговор Зуевского районного суда Кировской области от 26 апреля 2022 г. по уголовному делу № 1-38/2022. URL: <http://zuevsky.kir.sudrf.ru/> (дата обращения: 01.05.2026).

возможности искусственного изменения системных часов на устройстве преступника. Практически значимым правилом является фиксация времени совершения деяния по местонахождению преступника с обязательным указанием часового пояса, а при использовании средств анонимизации приоритет отдается данным судебной компьютерной экспертизы о реальной активности на устройстве, а не временным меткам конечного узла VPN.

3. В механизме следообразования по данной категории преступлений преобладают бинарные данные (цифровые следы), составляющие около 80% от общего объема криминалистически значимой информации. Наиболее часто фиксируются действия-следствия: передача, создание (в т.ч. фиктивных платежных поручений), ввод и модификация компьютерной информации. Традиционные следы (дактилоскопические, трасологические, предметы-документы) носят вспомогательный характер и присутствуют примерно в 20% случаев.

4. Использование криптовалют (биткоин, эфир) порождает особые следы в распределенном реестре (блокчейне): транзакционный след (хэш перевода, адреса отправителя/получателя), временной след (timestamp блока) и при отсутствии средств анонимизации – аппаратный след (MAC-адрес). Вредоносное программное обеспечение оставляет записи о месте размещения в реестре и автозагрузке, логи взаимодействия с командными серверами (C&C), а также следы инжекта кода в легитимные процессы.

2.4. Личность преступника, совершающего хищения с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации

Немаловажное значение для раскрытия и расследования рассматриваемой категории преступлений имеет типовой набор личностных характеристик преступника, поскольку он оказывает влияние на характер и

содержание складывающейся следственной ситуации. А.С. Камко отмечает, что «существенные личностные характеристики подозреваемого находятся в зависимости от нескольких факторов, в числе которых способ совершения преступления, а также роль, выполняемая им в составе преступной группы»¹.

Е.С. Никитина подчеркивает, что «помимо трансформации непосредственных форм киберпреступности, происходит смещение акцента на характеристиках личности «хакера». В частности, на современном этапе в качестве основы работы таких лиц лежит преступный бизнес, в то время как еще 15-20 лет назад в основе лежало желание «продемонстрировать» свои умения и навыки при совершении кибератак. Происходит определенное выделение из среды «хакеров» – профессионалов высшей категории, которые самостоятельно обеспечивают себя необходимыми программными средствами и владеют полной информацией о всех процессах при выполнении тех или иных противозаконных операций, и на лиц, которые просто используют приобретенные программные средства в целях обогащения, мести, хулиганства и в иных целях»².

Чаще всего данные преступления совершают лица в возрасте от 18 до 35 лет, что обусловлено большим развитием у данной категории технических навыков и умений работать со средствами и системами связи, в отличие от лиц более зрелого и пожилого возраста. Более 70% преступников, совершающих преступления с использованием информационно-телекоммуникационных технологий, – мужчины.

Для преступников характерна сравнительно высокая образованность – «зачастую это лица, имеющие среднее, среднее специальное и высшее образование, нередко по технической специальности. Совершающий деяние

¹ Камко А.С. Предупреждение мошенничества с использованием телекоммуникационных и компьютерных сетей: дис. ... канд. юрид. наук. Владивосток, 2020. С. 71.

² Никитина Е.С. О некоторых особенностях личности преступника, совершающего хищение цифровой валюты // Преступность в СНГ: проблемы предупреждения и раскрытия преступлений: сборник материалов Международной научно-практической конференции. Воронеж, 2024. С. 189.

данного вида преступник технически подготовлен, обладает комплексом программно-аппаратных методов и навыков, позволяющих не просто облегчить, но и обеспечить сам факт совершения преступления»¹.

Также отметим, что лица, совершающие хищения с использованием информационно-телекоммуникационных систем, имеют высокий уровень интеллекта, который зачастую выше, чем у преступников, совершающих иные преступления. Данные лица стремятся к развитию своих навыков, совершенствуют действия по реализации преступного замысла, осваивают новые схемы совершения преступлений. Лица, совершающие данные виды преступлений, хорошо осведомлены о механизмах раскрытия преступлений, поэтому придумывают новые схемы преступных действий, а также совершенствуют действия по сокрытию преступлений, постоянно развиваются в данной сфере, для того, чтобы быть менее уязвимыми для правоохранительных органов.

Однако, далеко не все преступники, совершающие хищения с использованием информационно-телекоммуникационных систем, имеют техническое образование и высокий уровень навыков обращения с техническим оборудованием. Зачастую это лица, имеющие средние технические навыки, которые узнают о преступных схемах от других людей, являющихся для них «наставниками». Такие лица, как правило, выступают в качестве посредников. Данная тенденция наиболее распространена при совершении преступлений лицами, отбывающими наказание в местах лишения свободы.

Между интеллектуальным и образовательным уровнем и криминальной специализацией преступников, совершающих преступления с использованием информационно-телекоммуникационных систем, имеется тесная взаимосвязь. Чем выше уровень образования и интеллектуальные способности, навыки лица, тем сложнее применяемые схемы преступных действий.

¹ Камко А.С. Указ. соч. С. 72.

Социально-экономический статус также является значимой детерминантой. Безработные граждане совершают противоправные деяния, направленные против чужой собственности, включая хищение цифровой валюты, чаще других категорий населения. В данном контексте противоправное деяние зачастую выступает в качестве основного источника средств к существованию. Криминалистическая характеристика усугубляется наличием рецидива: примерно 22% лиц, совершающих хищения цифровой валюты, имели судимость ранее, что свидетельствует о высокой степени криминальной зараженности и устойчивости противоправного поведения¹.

Тем не менее, следует отметить, что универсальная модель типичного субъекта хищений с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации не имеет высокой практической значимости, поскольку при ее создании приходится прибегать к высокой абстракции. Таким образом, под такую обобщенную модель попадает широкий круг лиц, что делает невозможным проведение узкой выборки. При расследовании уголовного дела необходимо обратить внимание на поведение подозреваемого, таким образом, лицо, осуществляющее расследование преступлений, должно разбираться во многих сферах, в том числе и психологии, т.к. выбранная тактика поведения может меняться в зависимости от получаемых в ходе расследования доказательств.

На основе анализа следственной практики можно привести пример личности организатора совершения преступления, включающего в себя обширные знания психологии, компьютерной техники, мобильных устройств, способен к самообразованию в сфере IT-технологий, коммуникабельный, расчетливый, может иметь знания в банковской сфере, адаптирован к складывающейся обстановке².

¹ Камко А.С. Указ. соч. С. 73.

² Приговор Ленинского районного суда г. Курска от 28 августа 2019 г. по делу № 1-279/21-2019. URL: Sudact.ru (дата обращения: 19.02.2026).

Хищения денежных средств посредством хищений с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации отличаются тем, что в число их субъектов входит множество различных участников, каждый из которых выполняет отдельные действия, образующие в совокупности механизм совершения преступления. В частности, к таким лицам относятся:

- программисты;
- лица, обеспечивающие распространение вредоносных программ и их эксплуатацию с целью последующего перевода денежных средств;
- «дропы» – лица, которые осуществляют обналичивание поступивших на счет денежных средств;
- «дроповоды» – координаторы «дропов».

Также в научной литературе выделяются специализированные группы, различающиеся по способу совершения преступления, уровню технической оснащенности и психологическим характеристикам. К числу наиболее распространенных категорий относятся: вирусописатели, вирмейкеры, криптоеры, крэкеры и кардеры, осуществляющие тайные хищения чужого имущества (например, с криптокошельков) с использованием специально разработанного программного обеспечения, похищающего коды доступа. Их мотивация, как правило, не ограничивается корыстью и включает в себя стремление к повышению престижа в криминальной среде. Другую значимую группу образуют Фроды, фишеры, спамеры и скамеры, которые преимущественно применяют методы социальной инженерии. Высокий интеллектуальный контроль поведения и профессиональные навыки в области психологии позволяют данным лицам эффективно манипулировать легальными пользователями с целью получения необходимых аутентификационных данных¹.

¹ Никитина Е.С. Указ. соч. С. 190.

Задача «дропа» – снять деньги с банковской карты, рискуя при этом попасть на запись видеокамеры банкомата. Их можно классифицировать на несколько категорий. Первая категория – дилетанты, т. е. лица, которые не осведомлены об истинных намерениях организатора преступления и не подозревающие, что их действия являются противоправными (тем самым, не предпринимают каких-либо мер конспирации).

В большинстве случаев операции по снятию денежных средств совершаются такими лицами однократно. Как правило, это родственники или знакомые участников преступной группы. Они не обладают преступными навыками и характеризуются правовым инфантилизмом.

Вторая категория «дропов» – профессионалы, осознающие правовые последствия своих действий и предпринимающие меры защиты и конспирации. Зачастую они выступают в качестве индивидуальных предпринимателей или учредителей специально создаваемых юридических лиц, фактически не занимающихся предпринимательской деятельностью. Их задачей является снятие денежных средств, добытых преступным путем, под видом заработной платы или дивидендов учредителя.

Период, в течение которого «дропы» играют отведенную им роль, составляет несколько месяцев. Это обусловлено тем, что фиктивная предпринимательская деятельность спустя незначительное время начнет вызывать подозрения у контролирующих органов. Некоторым «дропам» за это время удастся подняться выше в криминальной иерархии и стать «дроповодом» – лицом, руководящим «дропами»¹.

Легализация дохода, добытого преступным путем, возможна и путем перевода денежных средств в зарубежные страны. Стоит отметить, что обязательным участником рассматриваемой категории преступлений является специалист в сфере информационно-коммуникационных технологий, поскольку указанные преступления невозможно совершить, не обладая

¹ Шавалеев Б.Э. Классификация киберпреступлений // Вестник Казанского юридического института МВД России. 2022. № 4. С. 94.

навыками создания программного обеспечения, системного администрирования информационных систем, знаниями алгоритмов работы систем дистанционного банковского обслуживания.

Задачами технических специалистов являются:

- создание специальных интернет-сайтов для совершения мошеннических действий либо продажи изъятых или ограниченных в гражданском обороте предметов;
- защита информационных ресурсов;
- обеспечение анонимности доступа к сайту и безопасности информации на нем;
- обучение членов преступной группы навыкам работы с программным обеспечением и др.

Отличительной особенностью совершения данного вида преступлений является отсутствие непосредственного контакта между преступником и потерпевшим. Как отмечалось ранее, специфической чертой личности преступника является его не нацеленность на личностные ориентиры и качества потерпевшего. При этом преступник, как правило, с жертвой не знаком и его не интересует его личностная характеристика, определяющим моментом является обладание соответствующим имуществом, организация доступа к которому и является главной задачей преступника¹.

Таким образом, проанализировав личность преступника как значимый элемент структуры криминалистической характеристики хищений с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, необходимо сделать следующие выводы:

1. Хищения денежных средств посредством информационно-телекоммуникационных технологий отличаются тем, что в число их субъектов входит множество различных участников, каждый из которых выполняет отдельные действия, образующие в совокупности механизм совершения

¹ Харина Е.А. Особенности методики расследования мошенничества в сфере компьютерной информации: дис. ... канд. юрид. наук. Красноярск, 2024. С. 88.

преступления. В частности, к таким лицам относятся: программисты; лица, обеспечивающие распространение вредоносных программ и их эксплуатацию с целью последующего перевода денежных средств; «дропы» – лица, которые осуществляют обналичивание поступивших на счет денежных средств; «дроповоды» – координаторы «дропов».

2. Обязательным участником рассматриваемой категории преступлений является специалист в сфере информационно-коммуникационных технологий, поскольку указанные преступления невозможно совершить, не обладая навыками создания программного обеспечения, системного администрирования информационных систем, знаниями алгоритмов работы систем дистанционного банковского обслуживания.

ЗАКЛЮЧЕНИЕ

Проведенное исследование позволило сделать следующие выводы:

1. Криминалистическая характеристика хищений, совершаемых с применением информационно-телекоммуникационных технологий или в сфере компьютерной информации, представляет собой обобщенное (типовое) описание соответствующего вида преступной деятельности. Данное описание базируется на анализе правоприменительной практики, статистических данных, криминалистически значимых сведений и нормативных положений уголовного закона. Целевым назначением такой характеристики выступает формирование общих и специальных методических рекомендаций по расследованию указанных деяний, обоснованный выбор криминалистических средств, приемов и тактических решений применительно к различным этапам расследования.

Система криминалистически значимых сведений о хищениях, совершаемых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, должна включать следующие элементы: сведения о способе совершения преступления; сведения о предмете преступного посягательства; сведения о следовой картине; сведения об обстановке (обстоятельствах) совершения преступления; сведения о личности субъекта преступной деятельности.

2. Традиционное понимание предмета хищения, основанное на физическом (материальном) признаке, утратило исключительный характер в условиях цифровизации экономики. Принятие Федерального закона от 23 апреля 2018 г. № 111-ФЗ и разъяснения Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 фактически расширили предмет хищения за счет включения безналичных и электронных денежных средств, что потребовало пересмотра момента окончания преступления и привело к трансформации формальных составов (например, кражи).

Действующее уголовное законодательство не содержит четкого

разграничения между «безналичными денежными средствами» и «электронными денежными средствами». Это порождает противоречивую судебную практику, в том числе случаи необоснованного приравнивания указанных понятий либо, напротив, исключения их из объема обвинения без должной мотивировки. Необходимо законодательное уточнение дефиниций на межотраслевом уровне.

С введением цифрового рубля (третьей формы национальной валюты) возникла необходимость его унификации как предмета преступления. Обладая признаками электронных денежных средств, но имея официальный статус законного платежного средства, цифровой рубль не тождественен ни классическим безналичным деньгам, ни децентрализованным криптовалютам. Целесообразно прямое включение цифрового рубля в примечание к ст. 158 УК РФ в качестве разновидности «иного имущества» для обеспечения единообразия правоприменения.

3. Статистический анализ приговоров, приведенный в тексте, показывает, что наиболее распространенным способом является «социальная инженерия» (46% случаев). Это подтверждает тезис о том, что основным уязвимым звеном в системах безопасности остается человек, а не техника. Преступники эффективно эксплуатируют базовые человеческие чувства (страх, доверие, жадность, желание помочь), что позволяет им получать конфиденциальные данные добровольно.

Значительная доля хищений (8% – вредоносные программы для персональных компьютеров, 6% — для смартфонов, а также скимминг и атаки на банкоматы) совершается с использованием специализированного программного обеспечения. Это указывает на профессионализацию киберпреступности, требующую от злоумышленников навыков программирования и знания уязвимостей операционных систем и банковского оборудования. Особую опасность представляют трояны для мобильных устройств, дающие практически полный контроль над телефоном жертвы.

Выявленные способы можно классифицировать в зависимости от

объекта преступного посягательства: а) непосредственно денежные средства жертвы (социальная инженерия, хищение карт); б) персональные данные и реквизиты доступа (фишинг, вредоносное программное обеспечение); в) кредитные средства (оформление займов на третьих лиц). Последняя категория представляет повышенную общественную опасность, так как потерпевший длительное время может не знать о возникших у него долговых обязательствах, что существенно затрудняет своевременное начало расследования.

4. Обстановка хищений, совершаемых с использованием информационно-телекоммуникационных технологий, характеризуется множественностью географических точек (местонахождение преступника, серверов, устройства потерпевшего, банкомата и др.), что требует отказа от классического понимания единого места преступления. Для целей расследования каждое территориально обособленное место нахождения соисполнителя либо технического узла, задействованного в механизме деяния, признается самостоятельным местом совершения преступления. Использование сервисов-анонимайзеров (VPN, TOR, SOCKS) дополнительно затрудняет установление реального местонахождения злоумышленника.

Временной элемент обстановки ИТТ-хищений обладает высокой степенью латентности из-за различий локального сетевого времени, применения универсального координированного времени (UTC) и возможности искусственного изменения системных часов на устройстве преступника. Практически значимым правилом является фиксация времени совершения деяния по местонахождению преступника с обязательным указанием часового пояса, а при использовании средств анонимизации приоритет отдается данным судебной компьютерной экспертизы о реальной активности на устройстве, а не временным меткам конечного узла VPN.

В механизме следообразования по данной категории преступлений преобладают бинарные данные (цифровые следы), составляющие около 80% от общего объема криминалистически значимой информации. Наиболее часто

фиксируются действия-следствия: передача, создание (в т.ч. фиктивных платежных поручений), ввод и модификация компьютерной информации. Традиционные следы (дактилоскопические, трасологические, предметы-документы) носят вспомогательный характер и присутствуют примерно в 20% случаев.

Использование криптовалют (биткоин, эфир) порождает особые следы в распределенном реестре (блокчейне): транзакционный след (хэш перевода, адреса отправителя/получателя), временной след (timestamp блока) и при отсутствии средств анонимизации – аппаратный след (MAC-адрес). Вредоносное программное обеспечение оставляет записи о месте размещения в реестре и автозагрузке, логи взаимодействия с командными серверами (C&C), а также следы инъекта кода в легитимные процессы.

5. Хищения денежных средств посредством информационно-телекоммуникационных технологий отличаются тем, что в число их субъектов входит множество различных участников, каждый из которых выполняет отдельные действия, образующие в совокупности механизм совершения преступления. В частности, к таким лицам относятся: программисты; лица, обеспечивающие распространение вредоносных программ и их эксплуатацию с целью последующего перевода денежных средств; «дропы» – лица, которые осуществляют обналичивание поступивших на счет денежных средств; «дроповоды» – координаторы «дропов».

Обязательным участником рассматриваемой категории преступлений является специалист в сфере информационно-коммуникационных технологий, поскольку указанные преступления невозможно совершить, не обладая навыками создания программного обеспечения, системного администрирования информационных систем, знаниями алгоритмов работы систем дистанционного банковского обслуживания.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

Нормативные правовые акты и иные официальные документы

1. Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г.) (в ред. Федерального конституционного закона от 4 октября 2022 г. № 8-ФКЗ) // Российская газета. – 1993. – 25 дек. – № 237.
2. Уголовный кодекс Российской Федерации (в ред. Федерального закона от 9 апреля 2026 г. № 100-ФЗ) // Собрание законодательства Российской Федерации. – 1996. – № 25. – Ст. 2954.
3. Уголовно-процессуальный кодекс Российской Федерации (в ред. Федерального закона от 9 апреля 2026 г. № 78-ФЗ) // Собрание законодательства Российской Федерации. – 2001. – № 52. – Ст. 4921.
4. О государственной тайне: закон от 21 июля 1993 г. № 5485-1 (в ред. от Федерального закона от 4 августа 2022 г. № 359-ФЗ) // Собрание законодательства Российской Федерации. – 1997. – № 41. – Ст. 8220.
5. О национальной платежной системе: федеральный закон от 27 июня 2011 г. № 161-ФЗ (в ред. Федерального закона от 23 мая 2025 г. № 105-ФЗ) // Собрание законодательства Российской Федерации. – 2011. – № 27. – Ст. 3872.
6. О внесении изменений в Уголовный кодекс Российской Федерации: федеральный закон от 23 апреля 2018 г. № 111-ФЗ. – Доступ из справ.-правовой системы «КонсультантПлюс».
7. О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: федеральный закон от 31 июля 2020 г. № 259-ФЗ // Собрание законодательства Российской Федерации. – 2020. – № 31. – Ст. 5018.
8. О внесении изменений в статьи 128 и 140 части первой, часть вторую и статьи 1128 и 1174 части третьей Гражданского кодекса Российской Федерации: федеральный закон от 24 июля 2023 г. № 339-ФЗ // Собрание законодательства Российской Федерации. – 2023. – № 31 (ч. III). – Ст. 5765.

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

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

Монографии, учебники, учебные пособия:

11. Антонян Ю.М. Изучение личности преступника / Ю.М. Антонян. – М.: Юридическая литература, 1982. – 180 с.

12. Баев О.Я. Основы криминалистики: курс лекций / О.Я. Баев. – М.: Проспект, 2001. – 340 с.

13. Белкин Р.С. История отечественной криминалистики: монография / Р.С. Белкин. – М.: Норма, 1999. – 480 с.

14. Белкин Р.С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики: монография / Р.С. Белкин. – М.: Проспект, 2001. – 320 с.

15. Бирюков С.Ю. Методика расследования организации незаконной миграции: учеб. пособие / С.Ю. Бирюков, Е.В. Кушпель. – Волгоград: Волгоградская академия МВД России, 2007. – 120 с.

16. Большой юридический словарь / под ред. А.Я. Сухарева. – М.: Норма, 2008. – 858 с.

17. Гавло В.К. Теоретические проблемы и практика применения методики расследования отдельных видов преступлений / В.К. Гавло. – Томск: Томский государственный университет, 1985. – 330 с.

18. Гаухман Л.Д. Расследование по делам о телесных повреждениях и хулиганстве / Л.Д. Гаухман. – М.: Юридическая литература, 1975. – 150 с.

19. Дамаскин О.В. Криминология: учеб. пособие / О.В. Дамаскин. – М.: Юрлитинформ, 2009. – 250 с.

20. Каневский Л.Л. Криминалистические проблемы расследования и профилактики преступлений несовершеннолетних / Л.Л. Каневский. –

Красноярск: Красноярский государственный университет, 1991. – 200 с.

21. Криминология: учебник / под ред. В.Н. Кудрявцева, В.Е. Эминова. – М.: Норма, 1997. – 460 с.

22. Кудрявцев В.Н. Общая теория квалификации преступлений / В.Н. Кудрявцев. – М.: Дрофа, 1972. – 360 с.

23. Тарасова Н.В. Криминология: учеб.-методич. комплекс / Н.В. Тарасова. – Брянск: Полиграфист, 2010. – 150 с.

24. Яблоков Н.П. Криминалистика: учебник / Н.П. Яблоков. – М.: Проспект, 2005. – 470 с.

Научные публикации и статьи в иных периодических изданиях:

25. Александров И.В. Теоретические и практические проблемы расследования налоговых преступлений: дис. ... д-ра юрид. наук / И.В. Александров. – Екатеринбург, 2003. – 420 с.

26. Баранов С.А. Проблемы противодействия мошенничествам, совершаемым с использованием средств мобильной связи / С.А. Баранов // Противодействие преступлениям в сфере информационных технологий: материалы международной научно-практической конференции. – Белгород, 2022. – С. 22-25.

27. Басалаев А.Н. Криминалистическая характеристика преступления (Общее понятие и практическое значение) / А.Н. Басалаев, В.А. Гуняев // Методика расследования преступлений. Общие положения. – М.: Юридическая литература, 1976. – С. 98-102.

28. Безверхов А.Г. Хищение чужого имущества в условиях становления цифровой экономики / А.Г. Безверхов // Уголовное право: стратегия развития в XXI веке. – М., 2020. – С. 326-330.

29. Белоусов А.А. Криптовалюта и проблемы в ее законодательном регулировании / А.А. Белоусов, Е.В. Сильченко, А.М. Васильев // Современный ученый. – 2022. – № 2. – С. 229-233.

30. Бессонов А.А. Обстановка преступления как элемент его криминалистической характеристики / А.А. Бессонов // Вестник Саратовской

государственной юридической академии. – 2014. – № 6. – С. 156-160.

31. Бессонов А.А. Частная теория криминалистической характеристики преступлений: автореф. дис. ... д-ра юрид. наук / А.А. Бессонов. – М., 2017. – 50 с.

32. Бондарь М.М. Доказывание по уголовным делам о кражах, совершенных с использованием банковских карт: проблемные аспекты / М.М. Бондарь, А.А. Бочаров // Актуальные вопросы охраны общественного порядка и административной деятельности полиции: материалы межведомственной научно-практической конференции. – М., 2021. – С. 85-89.

33. Боровик П.Л. Хищение имущества путем модификации компьютерной информации: анализ способов и рекомендации по проведению проверочных мероприятий / П.Л. Боровик, С.В. Пилюшин // Юстиция Беларуси. – 2024. – № 8 (269). – С. 52-56.

34. Бугера М.А. Особенности использования специальных знаний при расследовании преступлений, связанных с хищением денежных средств с банковских счетов, с использованием вредоносных компьютерных программ / М.А. Бугера // Форум. – 2023. – № 1 (30). – С. 143-149.

35. Бугера М.А. Особенности первоначального этапа расследования хищений денежных средств с банковских счетов с использованием вредоносных компьютерных программ / М.А. Бугера // Форум. – 2023. – № 1 (30). – С. 179-184.

36. Ваничкин Д.Е. Криминологическая характеристика и предупреждение преступности в регионе (на материалах Ставропольского края): дис. ... канд. юрид. наук / Д.Е. Ваничкин. – Ставрополь, 2004. – 220 с.

37. Вирясова Н.В. Проблемы раскрытия и расследования отдельных видов преступлений, совершенных с использованием информационно-телекоммуникационных технологий / Н.В. Вирясова, А.Н. Землянова // Современная научная мысль: материалы VII Всероссийской научно-практической конференции. – Чебоксары, 2021. – С. 46-50.

38. Волосова Н.Ю. К вопросу о практической значимости разграничения

понятий «безналичные денежные средства» и «электронные средства платежа» как предмета хищения / Н.Ю. Волосова, Е.О. Филиппова // Аграрное и земельное право. – 2025. – № 3. – С. 17-20.

39. Герасимов И.Ф. Криминалистические характеристики преступлений в методике расследования / И.Ф. Герасимов // Методика расследования преступлений. Общие положения. – М.: Юридическая литература, 1976. – С. 94-97.

40. Голенко Д.В. О проблемах законодательной регламентации уголовной ответственности за преступное использование электронных средств платежа / Д.В. Голенко // Юридический вестник Самарского университета. – 2025. – № 1. – С. 66-72.

41. Головин А.Ю. Криминалистическая характеристика преступлений как категория современной криминалистики / А.Ю. Головин // Известия Тульского государственного университета. – 2012. – № 1-2. – С. 46-54.

42. Головин А.Ю. Теоретические основы и актуальные проблемы криминалистической систематики на современном этапе развития криминалистики: автореф. дис. ... канд. юрид. наук / А.Ю. Головин. – М., 2003. – 30 с.

43. Грибунов О.П. Эволюция взглядов на понятие и структуру криминалистической характеристики преступлений / О.П. Грибунов, Н.А. Назырова // Известия Тульского государственного университета. – 2020. – № 2. – С. 12-19.

44. Давыдов В.О. Значение виртуальных следов в расследовании преступлений экстремистского характера / В.О. Давыдов, А.Ю. Головин // Известия Тульского государственного университета. Экономические и юридические науки. – 2016. – № 3-2. – С. 254-258.

45. Долгиева М.М. Противодействие криптопреступности уголовно-правовыми средствами / М.М. Долгиева // Актуальные проблемы российского права. – 2023. – Т. 18. – № 2 (147). – С. 168-175.

46. Драпкин Л.Я. Предмет доказывания и криминалистические

характеристики преступлений / Л.Я. Драпкин // Криминалистические характеристики преступлений. – Свердловск: Уральский государственный университет, 1978. – С. 15-20.

47. Ермолаев А.А. Количественные корреляционные связи между элементами криминалистической характеристики преступления / А.А. Ермолаев // Мониторинг правоприменения. – 2025. – № 1 (54). – С. 49-55.

48. Иванова Е.В. Криптовалюта как предмет хищения: теоретический и практический аспекты / Е.В. Иванова // Материалы Алтайского филиала РАНХиГС. – Барнаул, 2024. – С. 120-125.

49. Иванова О.М. О проблемах квалификации кражи, совершенной с банковского счета, а равно в отношении электронных денежных средств, как единичного сложного преступления / О.М. Иванова // Судья. – 2026. – № 1 (181). – С. 24-28.

50. Ишигеев В.С. Междисциплинарный характер криминалистической характеристики преступлений / В.С. Ишигеев, М.В. Авдеев // Криминалистика: вчера, сегодня, завтра. – 2020. – № 4 (16). – С. 32-38.

51. Камко А.С. Предупреждение мошенничества с использованием телекоммуникационных и компьютерных сетей: дис. ... канд. юрид. наук / А.С. Камко. – Владивосток, 2020. – 230 с.

52. Карлина Н.Ю. Правовое регулирование расчетов с использованием электронных средств платежа / Н.Ю. Карлина // Вопросы науки и образования. – 2019. – № 18 (30). – С. 28-31.

53. Клочков В.В. Криминалистическая характеристика преступлений: состояние и перспективы исследований / В.В. Клочков // Криминалистическая характеристика преступлений. – М.: Полиграфист, 1984. – С. 22-27.

54. Князькина А.К. Цифровая валюта как предмет хищения (на примере цифрового рубля) / А.К. Князькина // Право и государство: теория и практика. – 2025. – № 3. – С. 195-199.

55. Князьков А.А. Цифровые финансовые активы как предмет преступления: понятие, виды, особенности незаконного оборота /

А.А. Князьков, А.А. Пухов // Аграрное и земельное право. – 2025. – № 3. – С. 350-354.

56. Колдин В.Я. Типовая информационная модель или криминалистическая характеристика преступления? / В.Я. Колдин, Е.П. Ищенко, О.А. Крестовников // Академический юридический журнал. – 2006. – № 4. – С. 8-13.

57. Колосовский Д.Ю. Криминологическая характеристика должностной преступности и борьба с ней (на материалах Карачаево-Черкесской Республики): дис. ... канд. юрид. наук / Д.Ю. Колосовский. – М., 2004. – 190 с.

58. Куликов А.В. Проблемные вопросы хищения безналичных денежных средств путем мошенничества с использованием компьютерных технологий (п. «в» ч. 3 ст. 159.6 УК РФ) / А.В. Куликов // КриминалистЪ. – 2025. – № 4 (53). – С. 61-66.

59. Лещенко В.П. Цифровой рубль как предмет мошенничества с использованием средств электронного платежа (ст. 159.3 Уголовного кодекса Российской Федерации) / В.П. Лещенко // Iuspublicumetprivatum. – 2025. – № 3 (31). – С. 125-130.

60. Макаров Р.А. Расследование хищений, совершенных с использованием информационно-телекоммуникационных технологий: обзор криминалистических методик и направления изучения / Р.А. Макаров // Юридическая наука и практика. – 2023. – № 1. – С. 65-71.

61. Мира К.А. Установление механизма хищений чужого имущества с использованием информационных технологий: дис. ... канд. юрид. наук / К.А. Мира. – М., 2022. – 210 с.

62. Мягков Д.А. Использование криптовалюты (к вопросу об уголовной ответственности) / Д.А. Мягков // Безопасность личности, общества и государства: теоретико-правовые аспекты: сборник научных статей XV международной научной конференции. – СПб., 2022. – С. 326-330.

63. Никитина Е.С. О некоторых особенностях личности преступника,

совершающего хищение цифровой валюты / Е.С. Никитина // Преступность в СНГ: проблемы предупреждения и раскрытия преступлений: сборник материалов Международной научно-практической конференции. – Воронеж, 2024. – С. 187-191.

64. Овчинникова Ю.И. Киберпреступность – новый вид преступности / Ю.И. Овчинникова // Актуальные вопросы применения российского права: материалы III научно-практической конференции. – Саранск, 2023. – С. 90-94.

65. Поддубный И.В. К вопросу об использовании фигурантами информационно-коммуникационных технологий в целях сокрытия хищений с банковских счетов граждан / И.В. Поддубный // Вестник Удмуртского университета. Серия Экономика и право. – 2020. – № 3. – С. 422-428.

66. Савельев А.И. Криптовалюты в системе объектов гражданских прав / А.И. Савельев // Закон. – 2017. – № 8. – С. 130-139.

67. Сарнакова А.В. Вопросы соотношения безналичных денежных средств, электронных денежных средств и цифрового рубля / А.В. Сарнакова, Н.С. Жижин // Юрист. – 2022. – № 5. – С. 24-28.

68. Семикаленова А.И. Цифровые следы: назначение и производство экспертиз / А.И. Семикаленова // Вестник Университета имени О.Е. Кутафина. – 2019. – № 5 (57). – С. 114-119.

69. Смахтин Е.В. Значение предмета и объекта преступления в структуре криминалистической характеристики деяний в сфере компьютерной информации / Е.В. Смахтин, А.В. Белоусов // Материалы национальной науч.-практ. конф. – Иркутск: Восточно-Сибирский институт МВД России, 2021. – С. 226-230.

70. Старостенко Н.И. Совершенствование криминалистического взаимодействия при расследовании хищений, совершенных с использованием методов социальной инженерии, реализуемых при помощи информационно-телекоммуникационных технологий / Н.И. Старостенко // Российский следователь. – 2023. – № 1. – С. 9-13.

71. Тебиев Р.Р. Технология построения криминалистической

характеристики преступлений на примере жестокого обращения с животными / Р.Р. Тебиев // Вестник Сибирского юридического института МВД России. – 2023. – № 2 (51). – С. 28-35.

72. Тюнин В.И. Криптовалюта – предмет преступления? / В.И. Тюнин // Правда и Закон. – 2022. – № 1 (19). – С. 42-47.

73. Усенко А.С. Понятие и элементы криминалистической характеристики кражи / А.С. Усенко, С.П. Казакова // Юриспруденция: теория и практика. – 2025. – № 5. – С. 103-107.

74. Федорова В.С. О мошенничестве с использованием платежных карт / В.С. Федорова, А.В. Лялюк // Проблемы развития предприятий: теория и практика: сборник статей VIII Международной научно-практической конференции. – Пенза, 2021. – С. 211-215.

75. Халиуллина А.Ф. Криминалистическая характеристика насильственных действий сексуального характера, совершенных в отношении малолетних и несовершеннолетних / А.Ф. Халиуллина // Правовое государство: теория и практика. – 2017. – № 1 (47). – С. 160-165.

76. Харина Е.А. Особенности методики расследования мошенничества в сфере компьютерной информации: дис. ... канд. юрид. наук. – Красноярск, 2024. – 248 с.

77. Химеденова Д.Н. Актуальные проблемы нормативного закрепления феномена криптовалюты в Российской Федерации / Д.Н. Химеденова, Т.И. Горбачева // Полицейская и следственная деятельность. – 2025. – № 3. – С. 15-21.

78. Челпанов Е.С. Хищение с банковского счета и равно в отношении электронных денежных средств / Е.С. Челпанов // Актуальные научные исследования в современном мире. – 2021. – № 1-9 (69). – С. 317-321.

79. Шавалеев Б.Э. Классификация киберпреступлений / Б.Э. Шавалеев // Вестник Казанского юридического института МВД России. – 2022. – № 4. – С. 92-97.

80. Шнейдерова Д.И. Пространственный элемент обстановки

совершения хищений в сфере оборота криптовалют: криминалистический аспект / Д.И. Шнейдерова // Правовая культура в современном обществе. – 2024. – С. 306-310.

Интернет-ресурсы:

81. Актуальные киберугрозы: итоги 2025 г. URL: <https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2024/> (дата обращения: 13.02.2026).

82. Краткая характеристика состояния преступности 2021-2025 гг. URL: <https://мвд.рф/reports/item/19655871/> (дата обращения: 24.02.2026).

83. Статистические данные о преступности. URL: <https://genproc.gov.ru/search/tags/?tags=Статистические%25данные> (дата обращения: 24.02.2026).

84. Чистова Л.Е. О соотношении уголовно-правовой и криминалистической характеристик / Л.Е. Чистова // Федеральный правовой портал «Юридическая Россия». URL: <http://law.edu.ru/doc/document.asp?docID=1308705> (дата обращения: 20.11.2025).

Эмпирические материалы:

85. По жалобе граждан С.В. Бородина, В.Н. Буробина, А.В. Быковского и других на нарушение их конституционных прав статьями 7, 29, 182 и 183 Уголовно-процессуального кодекса Российской Федерации: определение Конституционного Суда РФ от 8 ноября 2005 г. № 439-О. – Доступ из справ.-правовой системы «КонсультантПлюс».

86. Кассационное определение Восьмого кассационного суда общей юрисдикции от 21 декабря 2023 г. № 77-5316/2023. – Доступ из справ.-правовой системы «КонсультантПлюс».

87. Постановление Президиума Хабаровского краевого суда от 21 октября 2019 г. по делу 44у-139/2019. URL: <https://kraevoy--hbr.sudrf.ru/> (дата обращения: 12.04.2026).

88. Приговор Вельского районного суда (Архангельская область) от 29 июля 2024 г. по делу № 1-107/2024. URL: <https://sudact.ru/regular/doc/>

Та6bOG9K6A1p/ (дата обращения: 20.04.2026).

89. Приговор Верхнесалдинского городского суда от 18 октября 2023 г. по делу № 1361/2023. URL: <https://sudact.ru/regular/doc/5MarLTuMgbxh/> (дата обращения: 12.04.2026).

90. Приговор Зуевского районного суда Кировской области от 26 апреля 2022 г. по уголовному делу № 1-38/2022. URL: <http://zuevsky.kir.sudrf.ru/> (дата обращения: 01.05.2026).

91. Приговор Королевского городского суда Московской области от 14 апреля 2021 г. по делу № 1-204/2021. URL: Sudact.ru (дата обращения: 24.02.2026).

92. Приговор Курганского городского суда Курганской области от 22 августа 2023 г. по уголовному делу № 1-564/2023. URL: <http://kurgansky.krg.sudrf.ru/> (дата обращения: 03.05.2026).

93. Приговор Промышленного районного суда г. Ставрополя от 25 августа 2022 г. по делу № 1-724/2022. URL: Sudact.ru (дата обращения: 19.02.2026).

94. Приговор Пугачевского районного суда Саратовской области от 21 сентября 2020 г. по делу № 1123/2020. URL: <https://sudact.ru/regular/doc/AvQ1uGGjwD1w> (дата обращения: 20.04.2026).

95. Приговор Фрунзенского районного суда г. Иваново от 16 октября 2023 г. по делу № 1180/2023. URL: <https://sudact.ru/regular/doc/iu252oJcKBm4/> (дата обращения: 12.04.2026).