На правах рукописи



Пивнева Людмила Валерьевна

ПРОТИВОДЕЙСТВИЕ ХИЩЕНИЯМ, СОВЕРШЕННЫМ ДИСТАНЦИОННО: УГОЛОВНО-ПРАВОВОЙ И КРИМИНОЛОГИЧЕСКИЙ АСПЕКТЫ

5.1.4. Уголовно-правовые науки (юридические науки)

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата юридических наук

Курск – 2026

Работа выполнена в ФГБОУ ВО «Юго-Западный государственный университет»

Научный руководитель доктор юридических наук, доцент
Баумштейн Антон Борисович

Официальные оппоненты: **Рогова Евгения Викторовна,**
доктор юридических наук, профессор,
Иркутский юридический институт (филиал)
ФГКОУ ВО «Университет прокуратуры Российской Федерации»,
директор института

Соловьев Владислав Сергеевич,
кандидат юридических наук, доцент,
ФГКОУ ВО «Московский ордена Почета университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя»,
факультет подготовки научно-педагогических и научных кадров, докторант

Ведущая организация ФГБОУ ВО «Ярославский государственный университет им. П.Г. Демидова»

Защита диссертации состоится «26» декабря 2026 года в 16 часов 00 минут на заседании диссертационного совета 24.2.435.03 на базе ФГБОУ ВО «Юго-Западный государственный университет» по адресу: 305040, г. Курск, ул. 50 лет Октября, 94, конференц-зал.

С диссертацией можно ознакомиться в библиотеке ФГБОУ ВО «Юго-Западный государственный университет» и на сайте https://swsu.ru/upload/iblock/a32/ydeyn8lvm1h9m7ilruhc6epw6zlhnqzh/Dissertatsiya-L.V.-Pivneva.pdf

Автореферат разослан «___» _____ 2026 г.

Ученый секретарь
диссертационного совета Позднякова Елена Владимировна

I. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. По данным отчёта Global Digital 2025, сегодня в мире сетью Интернет пользуются 5,56 млрд человек, что составляет 67,9% населения Земли[1]. В России доступ к сети Интернет имеют 92,2% населения[2]. При этом цифровая среда используется не только для коммуникации и получения информации, но и для совершения имущественных и финансовых операций. Так, по данным Банка России, в 2022 г. доля граждан, пользовавшихся различными цифровыми финансовыми услугами, составила 66%, а в 2024 г. – уже 72%. Среди молодёжи в возрасте 14–22 лет этот показатель вырос с 91 до 96%[3]. Кроме того, по сообщению Сбербанка России, более 50% расходных операций по банковским картам граждане совершают в безналичной форме[4]. Это свидетельствует о том, что экономические отношения всё активнее перемещаются в цифровую среду. Одновременно расширение цифровых возможностей создаёт благоприятные условия и для преступников, использующих информационно-телекоммуникационные технологии (далее – ИКТ) для совершения имущественных посягательств.

Согласно официальной статистике МВД России, в 2023 г. каждое третье преступление было совершено с использованием информационно-телекоммуникационных технологий[5]. В 2024 г. доля таких деяний возросла до 40%[6]. Несмотря на то, что в 2025 г. отмечено некоторое снижение их количества (на 11,8%), удельный вес этих преступлений в общей структуре

---

[1] Статистика интернета и соцсетей на 2025 год – цифры и тренды в мире и в России [Электронный ресурс]. – URL: https://www.web-canape.ru/business/statistika-interneta-i-socsetej (дата обращения: 02.02.2026).

[2] Сколько россиян не пользуются интернетом [Электронный ресурс]. – URL: https://www.connect-wit.ru/skolko-rossiyan-ne-polzuyutsya-internetom.html (дата обращения: 03.02.2026).

[3] Исследование уровня финансовой грамотности [Электронный ресурс]. – URL: https://cbr.ru/analytics/szpp/fin_literacy/research/fin_ed_5/ (дата обращения: 04.02.2026).

[4] Результаты работы Группы Сбер по МСФО за 2025 год [Электронный ресурс]. – URL: https://www.sberbank.ru/ru/sberpress/vazhnoe/ (дата обращения: 05.02.2026).

[5] Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2023 года [Электронный ресурс]. – URL: https://xn--b1aew.xn--p1ai/reports/item/47055751/ (дата обращения: 06.02.2026).

[6] Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2024 года [Электронный ресурс]. – URL: https://xn--b1aew.xn--p1ai/reports/item/60248328/ (дата обращения: 07.02.2026).

преступности остаётся значительным. Кроме того, почти две трети преступлений, совершаемых с использованием информационно-телекоммуникационных технологий (63,5%), составляют кражи и мошенничества[7]. Эти данные характеризуют масштаб имущественных посягательств с использованием ИКТ, однако не позволяют отождествлять их с дистанционными хищениями. Использование таких технологий описывает применяемые средства, тогда как дистанционный характер хищения связан со способом завладения имуществом без непосредственного взаимодействия виновного с потерпевшим при передаче имущества.

Особую обеспокоенность вызывает масштаб материального ущерба, причиняемого дистанционными хищениями. По данным Следственного департамента МВД России, за десять месяцев 2025 г. общий ущерб от дистанционных хищений превысил 154 млрд руб.[8] Этот показатель свидетельствует не только о высокой распространённости рассматриваемых деяний, но и об эффективности используемых преступниками схем незаконного завладения имуществом с применением современных цифровых технологий. Столь значительный ущерб негативно влияет на имущественную безопасность граждан, устойчивость финансовых отношений и функционирование цифровой экономики.

Однако само по себе распространение рассматриваемых преступлений наряду с высокой степенью общественной опасности не исчерпывают оснований для признания данной проблемы актуальной. Её научная значимость обусловлена прежде всего тем, что распространение дистанционных хищений сопровождается появлением новых способов реализации преступного умысла, которые не всегда находят адекватное отражение в действующих уголовно-правовых конструкциях и сложившихся подходах к их применению. В результате возникает

[7] Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2025 года [Электронный ресурс]. – URL: https://xn--b1aew.xn--p1ai/reports/item/77848182/ (дата обращения: 08.02.2026).

[8] В МВД оценили ущерб от дистанционных хищений [Электронный ресурс]. – URL: https://ria.ru/20251211/uscherb-2061537107.html (дата обращения: 09.02.2026).

необходимость уточнения содержания и признаков дистанционного хищения, определения его соотношения с традиционными способами хищения и выработки единообразных подходов к уголовно-правовой оценке соответствующих деяний.

Необходимость дальнейшего теоретического осмысления обозначенных вопросов подтверждается и развитием судебной практики. Так, Постановлением Пленума Верховного Суда Российской Федерации от 16 июня 2026 г. № 19 внесены изменения в постановление Пленума Верховного Суда Российской Федерации от 27 декабря 2002 г. № 29 «О судебной практике по делам о краже, грабеже и разбое», в том числе затрагивающие вопросы квалификации хищений, совершаемых с использованием современных технологий. Появление новых судебных разъяснений в данной сфере свидетельствует о продолжающемся формировании правоприменительных подходов к уголовно-правовой оценке современных способов хищения и, одновременно, о наличии вопросов, требующих дополнительного теоретического обоснования.

В этой связи актуальной научной задачей является выявление закономерностей противодействия дистанционных хищений, определение особенностей их уголовно-правовой характеристики и установление критериев разграничения с иными формами хищения. Особое значение приобретает разработка научно обоснованного определения понятия дистанционного хищения, отражающего специфику механизма совершения данного преступления и позволяющего установить его место в системе средств противодействия хищениям. Необходимость решения указанных теоретических и прикладных вопросов обусловливает выбор темы настоящего диссертационного исследования.

Цель диссертационного исследования – получение новых научных знаний о закономерностях уголовно-правового противодействия дистанционным хищениям, их криминологической характеристики, а также разработка предложений по совершенствованию системы их предупреждения в условиях цифровой трансформации общественных

отношений.

Для достижения поставленной цели были определены следующие **исследовательские задачи**:

– сформулировать определение понятию дистанционного хищения;

– охарактеризовать формы и способы хищений, совершаемых дистанционно;

– раскрыть действующую систему уголовно-правовых запретов хищений, совершаемых дистанционно;

– определить характер наказуемости хищений, совершённых дистанционно;

– выявить характерные черты личности преступника, совершающего дистанционные хищения;

– раскрыть основные мотивы и способы вербовки лиц, совершающих хищения дистанционно;

– установить основные направления предупреждения современных дистанционных хищений;

– сформулировать предложения, направленные на повышение эффективности предупреждения данной разновидности преступлений.

Объектом исследования является комплекс общественных отношений, возникающих в связи с совершением дистанционных хищений, а также в сфере выявления, расследования и предупреждения данной разновидности преступной деятельности в условиях цифровизации современной экономики.

Предмет исследования – закономерности совершения дистанционных хищений, особенности их уголовно-правовой оценки, состояние и структура данной разновидности преступности, криминологическая характеристика лиц, совершающих указанные преступления, особенности их детерминации, механизма совершения и вовлечения участников преступной деятельности, а также направления совершенствования мер предупреждения дистанционных хищений.

Степень разработанности темы исследования. Проблемы преступлений против собственности, совершаемых с использованием информационно-телекоммуникационных технологий, начали активно изучаться в юридической науке сравнительно недавно, что обусловлено стремительным развитием цифровых технологий и распространением электронных финансовых операций.

Вопросы расследования, уголовно-правовой оценки, квалификации, криминализации, а также криминологического противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий, электронных средств платежа и методов социальной инженерии, получили отражение в диссертационных исследованиях С.М. Голятиной, Г.Р. Григоряна, В.В. Жданович, Е.В. Зотиной, Ю.Б. Имаевой, А.А. Киктенко, И.А. Киселевой, И.Е. Мазурова, А.В. Маилян, И.А. Мусьял, А.П. Перетолчина, М.А. Простосердова, О.А. Старостенко, Н.И. Старостенко и М.Д. Фролова.

Отдельные вопросы уголовно-правовой характеристики дистанционных хищений исследовались в трудах таких учёных, как А.А. Алёхин, А.В. Архипов, А.А. Байбарин, Е.В. Благов, В.К. Барчуков, А.В. Беляков, Л.М. Болсуновская, В.И. Гладких, Г.Р. Григорян, Е.И. Думанская, О.В. Ермакова, М.Г. Иванов, А.В. Иванчин, К.Н. Карпов, А.А. Киктенко, И.А. Клепицкий, Д.И. Крумина, И.Л. Крутиков, В.П. Лещенко, Н.А. Лопашенко, Ю.В. Лукьянова, Е.А. Маркова, Т.И. Матюхина, А.С. Мирончик, Е.П. Новикова, Е.А. Раненкова, Е.В. Рогова, Е.А. Русскевич, М.М. Савченко, Я.В. Самиулина, А.В. Семёнов, В.С. Соловьёв, О.Г. Соловьёв, А.В. Суслопаров, К.Ю. Федоренко, А.Н. Халиков, А.А. Энгельгардт, А.Ф. Юсупова и др.

Некоторые криминологические и криминалистические аспекты дистанционных хищений нашли отражение в трудах следующих учёных: О.А. Дворянкина, И.Р. Диваевой, С.В. Иванцова, К.А. Ивлева, Н.А. Карповой, Н.Р. Красовской, А.Р. Напсокова, А.Т. Потёмкиной, В.В. Радова, И.П. Родивилина, Б.П. Смагоринского, О.А. Старостенко,

В.Ф. Шаньгина, В.Г. Шумихина и других. В их исследованиях рассматриваются типология и психологические характеристики преступников, совершающих такие общественно опасные деяния, способы совершения преступлений с использованием цифровых технологий, а также вопросы профилактики, виктимологического анализа и предупреждения подобных преступлений.

Вместе с тем представленные научные исследования в основном посвящены отдельным видам преступлений и аспектам их совершения в цифровой среде: вопросам уголовно-правовой оценки мошенничества, краж с использованием электронных средств платежа, особенностям расследования преступлений, совершаемых с применением информационно-телекоммуникационных технологий, а также отдельным криминологическим аспектам противодействия такой преступности. При этом комплексное исследование дистанционных хищений как совокупности современных форм имущественных посягательств, объединённых спецификой дистанционного способа совершения, особенностями личности участников соответствующих преступных схем, механизмами их мотивации и вербовки, а также системой предупреждения, требует научной разработки. Это обусловливает необходимость дальнейшего научного исследования дистанционных хищений.

Нормативную основу исследования составили положения Конституции РФ, международно-правовые акты в сфере защиты имущественных отношений, Уголовный кодекс РФ, Уголовно-процессуальный кодекс РФ, Уголовно-исполнительный кодекс РФ, соответствующие теме исследования федеральные законы, указы Президента РФ, постановления Правительства РФ, нормативные правовые акты федеральных органов исполнительной власти, а также разъяснения высших судебных органов, в том числе постановления Пленума Верховного Суда Российской Федерации, определяющие подходы к квалификации дистанционных хищений.

Эмпирическую базу исследования составили официальные

статистические данные ГИАЦ МВД России за 2019–2025 гг., отражающие состояние, структуру и динамику дистанционных хищений, предусмотренных п. «г» ч. 3 ст. 158, ст. 159, ст. 159.3 и ст. 159.6 УК РФ. В рамках исследования проанализировано 200 уголовных дел 2020–2025 гг., находившихся в производстве подразделений дознания и следствия органов внутренних дел различных субъектов Российской Федерации и содержащих признаки дистанционных хищений, что позволило выявить особенности квалификации рассматриваемых деяний, способы их совершения, структуру преступной деятельности и характеристики личности преступника. Кроме того, проведено анкетирование 250 сотрудников правоохранительных органов Курской и Белгородской областей, представляющих подразделения уголовного розыска, следствия, дознания и подразделения по противодействию преступлениям в сфере ИКТ, результаты которого использованы при анализе проблем предупреждения дистанционных хищений. Эмпирическую основу исследования также составили аналитические и информационные обзоры МВД России, Генеральной прокуратуры РФ, Банка России, характеризующие состояние, динамику и структуру преступлений рассматриваемой категории, а также отдельные эмпирические данные, полученные другими исследователями при изучении смежных вопросов.

Методология и методы исследования. Методологическую основу диссертационного исследования составили общенаучные и частнонаучные методы познания. Выбор конкретных методов определялся характером исследуемой проблемы и необходимостью рассмотреть дистанционные хищения одновременно с позиции уголовного права и криминологии. При исследовании правовой природы дистанционных хищений использовался формально-юридический метод. С его помощью проанализированы положения уголовного законодательства об ответственности за дистанционные хищения, особенности конструирования соответствующих составов преступлений, а также вопросы разграничения отдельных дистанционных способов совершения имущественных посягательств.

Применение данного метода позволило выявить положения уголовного закона, применение которых вызывает затруднения при квалификации хищений, совершаемых дистанционно. Сравнительно-правовой метод применялся для выявления разных правовых подходов к оценке уголовно-правового противодействия дистанционным хищениям. Сопоставление различных подходов использовалось с целью определения возможностей их применения при совершенствовании российского уголовного законодательства и практики его применения в соответствующей сфере. Для изучения механизма совершения дистанционных хищений и состояния рассматриваемого явления в современности использовались анализ, синтез, а также методы индукции, дедукции и обобщения. Статистический метод использовался при обработке и сопоставлении сведений, характеризующих распространённость отдельных видов дистанционных хищений, а также для установления характеристики лиц, привлекаемых к уголовной ответственности по соответствующим составам преступлений. В исследовании также применялся метод анкетирования, результаты которого использовались при оценке отдельных вопросов, связанных с определением состояния указанной разновидности преступной деятельности, а также эффективности мер противодействия им. Сочетание использованных методов позволило сформулировать положения, направленные на уточнение уголовно-правовой оценки рассматриваемых деяний и совершенствование системы их предупреждения.

Научная новизна диссертационного исследования состоит в разработке и обосновании новых положений, раскрывающих уголовно-правовую и криминологическую специфику дистанционных хищений.

Сформулировано авторское определение дистанционного хищения, отражающее его отличительные признаки, связанные с особенностями совершения указанных деяний, и позволяющее отграничить рассматриваемые деяния от иных преступлений против собственности.

Выделены формы и способы совершения дистанционных хищений, дифференциация которых положена в основу адресной профилактики с

учётом характера преступного воздействия, особенностей используемых средств совершения преступления и роли потерпевшего в механизме посягательства.

В отдельных сферах уголовно-правового реагирования выявлены пробелы и противоречия действующей системы средств противодействия дистанционным хищениям и предложены направления её совершенствования.

Сформирован криминологический портрет лиц, совершающих дистанционные хищения, а также выделены типологические портреты организатора, технического исполнителя, социального инженера и номинального участника с учётом различий в выполняемых ими функциях и степени вовлечённости в преступную деятельность.

Раскрыты многофакторная структура мотивации лиц, совершающих дистанционные хищения, и механизм их вербовки, особенности которых учтены при разработке мер криминологического предупреждения.

Сформирована дифференцированная система мер предупреждения дистанционных хищений, учитывающая криминологически значимые факторы и предусматривающая комплексное воздействие на всех этапах преступной деятельности (от выявления и предупреждения подготовки хищения до пресечения его совершения, установления участников и минимизации последствий совершённого преступления).

Основные положения, выносимые на защиту:

1. Дистанционное хищение, не являясь самостоятельной уголовно-правовой конструкцией, представляет собой современную форму реализации института хищения в цифровой среде, представляющую собой противоправное безвозмездное изъятие чужого имущества или имущественных прав с корыстной целью, причиняющее имущественный ущерб собственнику или иному законному владельцу и осуществляемое посредством цифровой инфраструктуры без непосредственного физического воздействия виновного на предмет хищения либо без непосредственного очного контакта виновного с потерпевшим при

использовании информационно-телекоммуникационных, электронных платежных или иных технических средств удаленного воздействия.

2. Дистанционные хищения совершаются в форме кражи и мошенничества.

Для адресной профилактики дистанционных хищений дистанционные кражи по способам совершения деяния разделены на две группы: персонализированные (несанкционированный доступ к учётным записям и личным кабинетам потерпевших, включая банковские аккаунты и электронные кошельки, с последующим самостоятельным распоряжением чужими средствами); технические (манипулирование программным обеспечением и платёжными системами, направленное на преодоление или обход установленных технических барьеров). Указанные способы преступного воздействия определяют такие направления адресной профилактики дистанционных хищений, как защита персональных данных и повышение защищённости цифровых систем.

Для совершенствования мер защиты от дистанционных хищений дистанционное мошенничество по способам совершения преступления ранжировано на две группы: мошенничества, совершённые посредством «активного обмана» потерпевшего, реализуемого через методы социальной инженерии (вербально-информационные, психологически-манипулятивные, доверительно-эксплуатирующие и комбинированные), и мошенничества, совершённые посредством технически опосредованного воздействия на цифровую среду, осуществляемого через фишинг, использование подложных интернет-ресурсов и иные формы цифрового воздействия, формирующие у потерпевшего ошибочное волеизъявление (информационно-технологические, эксплуатационно-инфраструктурные, системно-дестабилизирующие и комбинированные методы). Данные способы преступного воздействия обусловливают необходимость одновременного совершенствования мер защиты цифровой инфраструктуры и противодействия психологическим механизмам обмана.

3. Нормы российского уголовного законодательства, применяемые

при квалификации дистанционных хищений (ст. 158, в том числе п. «г» ч. 3, ст. 159, 159.3, 159.6, 172-174 УК РФ), не образуют согласованной системы. Между ними возникает конкуренция, а критерии их разграничения остаются недостаточно определёнными, что способствует формированию противоречивой правоприменительной практики. Признание цифровой валюты и цифровых прав предметом хищения в постановлении Пленума Верховного Суда РФ от 16 июня 2026 г. № 19 устранило одну из существовавших неопределённостей, однако не разрешило все вопросы оценки и квалификации таких деяний. В связи с этим обоснована необходимость конкретизировать порядок определения размера ущерба при хищении цифровой валюты, включая криптовалюту по рыночным котировкам.

В дополнительных разъяснениях Пленума Верховного Суда РФ целесообразно: а) уточнить условия применения ст. 159.3 УК РФ при использовании, разграничив случаи, когда обман потерпевшего или иного лица непосредственно обусловил передачу имущества, и случаи, когда виновный использовал чужое электронное средство платежа или полученные учётные данные для изъятия денежных средств; б) определить критерии разграничения п. «г» ч. 3 ст. 158 УК РФ и ст. 159.6 УК РФ исходя из приоритетного объекта посягательства и направленности цифрового воздействия (при тайном изъятии денежных средств объектом преступного воздействия определить имущественные права потерпевшего, тогда как при вмешательстве в компьютерную информацию – функционирование информационной системы как механизм доступа и распоряжения имуществом); в) разграничить ст. 159.6 УК РФ со ст. 272–274 УК РФ, определив, что неправомерное воздействие на компьютерную информацию с целью хищения имущества охватывается ст. 159.6 УК РФ и не требует дополнительной квалификации по ст. 272–274 УК РФ с приведением санкций данных норм в соответствие.

4. Обосновано, что общая норма о мошенничестве (ст. 159 УК РФ) имеет самостоятельное значение в системе уголовно-правового

противодействия дистанционным хищениям: при отсутствии признаков специальных составов она применяется, когда дистанционный обман либо злоупотребление доверием непосредственно обусловливает волеизъявление потерпевшего или иного уполномоченного лица на передачу имущества либо права на него. Само по себе использование цифрового канала связи не служит основанием для квалификации по ст. 159.3 или ст. 159.6 УК РФ. Разграничение проводится по механизму завладения имуществом: обусловленное обманом имущественное распоряжение необходимо отличать от тайного изъятия с использованием полученных учётных данных и от воздействия на процессы обработки компьютерной информации.

5. В условиях устойчивого роста дистанционных хищений и повышения сложности механизмов их совершения установлена необходимость совершенствования отечественной санкционной политики в части пенализации указанных деяний, включая: нормативное закрепление минимального размера причинённого ущерба по п. «г» ч. 3 ст. 158 УК РФ с целью отграничения дистанционных хищений, имеющих высокую степень общественной опасности от малозначительных посягательств; ужесточение санкций, предусмотренных ст. 159.3 и 159.6 УК РФ, до уровня наказуемости, установленного за кражу, совершённую с банковского счёта (п. «г» ч. 3 ст. 158 УК РФ); уточнение посредством официальных разъяснений высшей судебной инстанции санкций рассматриваемых составов преступлений с учётом степени технологической сложности используемых преступных схем, понимаемой как совокупность объективно устанавливаемых признаков, выражающихся в многоэтапности цифрового воздействия, использовании специализированных программных средств и автоматизированных алгоритмов, применении распределённых цифровых сервисов и платформ для реализации преступного замысла, а также в характере преодоления или обхода средств информационной защиты, что позволяет учитывать повышенную общественную опасность технологически усложнённых

форм дистанционных хищений при назначении наказания.

6. Исследование мотивационной структуры лиц, совершающих дистанционные хищения, показывает, что их поведение определяется многофакторной системой мотивов, состоящей из следующих компонентов: корыстный (ориентация на значительную материальную выгоду), рационально-технологический (ориентация на минимизацию рисков и автоматизацию действий), профессионально-статусный (желание самоутверждения через демонстрацию компетентности в обходе цифровых средств защиты и работе с информационными системами), психологический (иллюзия анонимности и дистанцирования от причиняемого вреда через виртуальное взаимодействие), риско-ориентированный (восприятие низкой вероятности привлечения к ответственности из-за высокой степени анонимизации и сложности отслеживания цифровых операций), ситуативно-оппортунистический (использование случайного доступа к чужим данным или электронным средствам через онлайн-платформы и т.п.). Указанные компоненты мотивационной структуры проявляются в различных сочетаниях и с разной степенью выраженности при формировании преступного умысла, обусловливая специфику преступного поведения в цифровой среде, что предопределяет необходимость их учёта при разработке комплексной системы предупреждения дистанционных хищений.

7. Типичный преступник, совершающий дистанционные хищения – это мужчина в возрасте от 18 до 40 лет, не состоящий в браке, с образованием не ниже среднего специального, официально не имеющий постоянной занятости, ранее не судимый, совершающий мошеннические действия с преимущественно корыстной мотивацией при общей психологической характеристике, включающей рациональность, развитые либо специализированные когнитивные и/или коммуникативные навыки, склонность к манипулятивным формам взаимодействия, эмоциональную дистанцированность от последствий совершаемых действий, сниженный уровень эмпатии, а также преимущественно низкую выраженность

агрессивности и конфликтности при вариативной степени криминальной устойчивости в зависимости от выполняемой роли в преступной схеме.

Вместе с тем, указанный «типичный» образ носит обобщённый характер и включает в себя четыре относительно самостоятельных криминологических типа: организатора, технического исполнителя, социального инженера («звонаря») и номинального участника дистанционного хищения (дроппера), различающихся по возрастной характеристике, уровню образования, профессиональной принадлежности, степени вовлечённости в преступную деятельность, её характеру, функциональной роли в структуре дистанционного хищения, а также по выраженности когнитивных и поведенческих особенностей.

8. В условиях цифровой среды механизм вербовки исполнителей дистанционных хищений приобретает самостоятельное криминологическое значение как элемент, обеспечивающий воспроизводство данной преступной деятельности, и обеспечивает вовлечение участников, различающихся степенью осознания противоправного характера действий и выполняемыми функциями. Вербовка осуществляется в двух формах: латентного вовлечения (маскировка под легальную занятость) и осознанного вовлечения (прямое указание на противоправный характер действий). Это обусловливает необходимость разработки и реализации комплекса мер, направленных на выявление и пресечение каналов вербовки, а также профилактику вовлечения граждан в противоправную деятельность в цифровой среде.

9. Определены приоритетные направления совершенствования системы мер предупреждения данных преступлений.

В правовой сфере – устранение выявленных пробелов и коллизий отечественного законодательства, регулирующего противодействие дистанционным хищениям, формирование единых подходов к их квалификации, а также адаптация уголовно-правовых норм к трансформации цифровых угроз, в том числе с учётом распределения ролей участников преступных схем.

В организационно-управленческой сфере определена необходимость совершенствования системы выявления и пресечения дистанционных хищений, включая повышение уровня специализированной подготовки сотрудников правоохранительных органов в сфере цифровой криминалистики, совершенствование методического обеспечения выявления и пресечения дистанционных хищений с учётом распределённого характера преступной деятельности, а также расширение и актуализацию информационных баз о типичных схемах дистанционных хищений в рамках межведомственного взаимодействия кредитных организаций, органов внутренних дел и операторов связи.

В технической сфере обоснована необходимость внедрения интеллектуального программного обеспечения для многоуровневой защиты устройств клиентов, каналов связи и внутренней инфраструктуры банковских организаций, функционирующего на основе постоянного обновления алгоритмов противодействия дистанционным хищениям.

В культурно-воспитательной сфере предложено расширение охвата профилактических мероприятий посредством использования цифровых платформ, социальных сетей и иных каналов коммуникации для распространения виктимологического контента, ориентированного на уязвимые категории населения для ознакомления с типичными механизмами воздействия социальных инженеров, а также разработка и внедрение интерактивных образовательных модулей и цифровых симуляторов мошеннических ситуаций, формирующих навыки безопасного поведения в цифровой среде и распознавания способов вовлечения в преступную деятельность в качестве номинальных участников, а равно дальнейшее повышение уровня цифровой грамотности населения.

Теоретическая значимость диссертационного исследования определяется тем, что полученные в работе результаты вносят вклад в развитие криминологии и уголовно-правовой науки, способствуют дополнению теоретической базы и методологии предупреждения

дистанционных хищений, дальнейшему научному осмыслению юридической природы и криминологической сущности рассматриваемой разновидности преступной деятельности. Содержащиеся в работе выводы могут быть использованы для дальнейших исследований данной темы.

Практическая значимость диссертационного исследования состоит в том, что полученные выводы и предложения могут быть использованы в соответствующей законотворческой деятельности, практической работе правоохранительных органов, прокуратуры и судов, а также в образовательной деятельности при преподавании курсов «Уголовное право», «Криминология», «Преступления против собственности» и других. Также прикладные результаты исследования использованы при разработке программного решения, направленного на выявление рисков дистанционных хищений с использованием электронных средств платежа.

Степень достоверности результатов диссертационного исследования обеспечивается комплексным междисциплинарным подходом, сочетающим положения уголовного права и криминологии, соблюдением методологических требований указанных научных направлений, а также использованием репрезентативной эмпирической базы.

Апробация результатов диссертационной работы. Исследование проводилось на кафедре уголовного права ФГБОУ ВО «Юго-Западный государственный университет» в соответствии с планом научно-исследовательской работы.

Материалы диссертации были представлены на различных международных и всероссийских научно-практических конференциях (Курск, 2023; Белгород, 2024, 2025, 2026).

Основные положения, результаты и выводы диссертации отражены в 12 публикациях автора (6 статей в изданиях, рекомендованных Высшей аттестационной комиссией при Министерстве науки и высшего образования Российской Федерации).

Дополнительную апробацию результаты исследования получили при использовании сотрудниками правоохранительных органов г. Белгорода программы для ЭВМ, предназначенной для определения рисков дистанционных хищений с использованием электронных средств платежа (Свидетельство о государственной регистрации программы для ЭВМ № 2026667563 от 09.06.2026).

Кроме того, материалы диссертационного исследования внедрены в образовательный процесс Санкт-Петербургского университета МВД России, Белгородского юридического института МВД России имени И.Д. Путилина и Юго-Западного государственного университета при преподавании дисциплин «Криминология» и «Уголовное право».

Структура диссертации определена основными задачами диссертационного исследования. Работа состоит из введения, трёх глав, заключения, списка литературы и приложения.

II. ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обосновывается актуальность темы диссертации, определяются цель, задачи, объект, предмет исследования, его теоретическая, методологическая, нормативная и эмпирическая базы, раскрывается новизна в положениях, выносимых на защиту, теоретическая и практическая значимость сделанных выводов и предложений, отмечены сведения об апробации результатов работы.

Первая глава «Теоретические основы хищений, совершаемых дистанционно» включает два параграфа.

В первом параграфе *«Понятие и юридическая природа хищений, совершаемых дистанционно»* исследуются понятия, относящиеся к термину «дистанционное хищение», их разновидности и особенности использования в научной литературе.

Обосновывается позиция, согласно которой термин «дистанционное хищение» наиболее полно отражает сущность исследуемой категории, поскольку не ограничивается конкретной технологической средой либо

отдельным способом совершения преступления, а фиксирует ключевой признак – отсутствие непосредственного физического воздействия виновного на предмет хищения либо непосредственного очного контакта с потерпевшим.

В работе показано, как классические признаки хищения, проявляются в случае совершения этого преступления дистанционно. Корыстная цель, противоправность, безвозмездность, обращение чужого имущества в пользу виновного или иных лиц и причинение ущерба собственнику – сохраняют своё значение, однако в условиях цифровых технологий имеют свои особенности.

Корыстная цель в дистанционных хищениях по своему содержанию совпадает с корыстной целью в традиционных формах хищения, однако, отличается более высоким уровнем рационализации, технологической опосредованности и интенсивности реализации. Противоправность изъятия проявляется через несанкционированный доступ к банковским счетам, электронным кошелькам, учётным записям, программным системам. Безвозмездность приобретает завуалированный характер, поскольку создаётся иллюзия возмездности. Обращение имущества в пользу виновного осуществляется посредством изменения правомочий распоряжения имуществом. Причинение имущественного ущерба выражается в утрате потерпевшим возможности распоряжаться принадлежащими ему имущественными благами.

Во втором параграфе *«Формы и способы хищений, совершаемых дистанционно»* доказано, что при дистанционном совершении хищения возможны лишь две его формы, выделенные законодателем, – кража и мошенничество. Именно они предполагают опосредованное изъятие имущества без физического контакта между виновным и потерпевшим. Разбой и грабёж требуют непосредственного контакта преступника и потерпевшего. Присвоение и растрата в дистанционной форме практически невозможны, поскольку предполагают нахождение имущества в правомерном владении виновного.

Предлагается авторское видение систематизации форм и способов дистанционных хищений, отражающей как техническую, так и социально-психологическую природу данного феномена.

Вторая глава «Уголовно-правовые средства противодействия хищениям, совершаемым дистанционно» включает два параграфа.

В первом параграфе *«Система уголовно-правовых средств противодействия хищениям, совершенным дистанционно»* исследуются уголовно-правовые нормы, устанавливающие соответствующие запреты.

Выделяются три уровня системы. Основной образуют запреты, непосредственно предусматривающие ответственность за хищение: ст. 159 УК РФ (мошенничество), п. «г» ч. 3 ст. 158 УК РФ (кража с банковского счёта, а равно в отношении электронных денежных средств), ст. 159.3 УК РФ (мошенничество с использованием электронных средств платежа), ст. 159.6 УК РФ (мошенничество в сфере компьютерной информации). Вспомогательный (технологический) включают запреты, обеспечивающие уголовно-правовую охрану цифровой среды, – ст. 272–274 УК РФ. Инфраструктурный – запреты неправомерного оборота электронных средств платежей, аккумулированные в ст. 187 УК РФ.

Выявлены проблемы системы уголовно-правовых средств противодействия дистанционным хищениям. К ним относятся: конкуренция п. «г» ч. 3 ст. 158 УК РФ и ст. 159.6 УК РФ; фактическое поглощение ст. 159.6 УК РФ составов ст. 272–274 УК РФ при рассогласованности санкций; отсутствие единых критериев разграничения смежных составов. Предложены пути их разрешения.

Во втором параграфе *«Наказуемость хищений, совершённых дистанционно»* исследуются санкции рассматриваемой группы преступлений.

Обращается внимание на диспропорции в санкционной политике. Отсутствие минимального стоимостного порога причинённого ущерба применительно к п. «г» ч. 3 ст. 158 УК РФ не позволяет последовательно отграничивать общественно опасные деяния от малозначительных

посягательств. Наказуемость мошенничества с использованием электронных средств платежа и мошенничества в сфере компьютерной информации не согласована с ответственностью за кражу, совершённую с банковского счёта. При назначении наказания недостаточно учитываются многоэтапность цифрового воздействия, применение специальных программных средств, автоматизированных алгоритмов и распределённых цифровых сервисов, а также способы преодоления или обхода средств информационной защиты.

Для устранения указанных недостатков обоснована необходимость установления минимального размера ущерба по п. «г» ч. 3 ст. 158 УК РФ, приведения санкций, предусмотренных ст. 159.3 и 159.6 УК РФ, в соответствие с наказуемостью кражи, совершённой с банковского счёта, а также уточнения в разъяснениях Верховного Суда РФ порядка учёта технологической сложности способа совершения дистанционного хищения.

Третья глава «Криминологические основы предупреждения дистанционных хищений» включает три параграфа.

В первом параграфе *«Криминологическая характеристика лиц, совершающих дистанционные хищения»* на основе на основе-изучения 200 уголовных дел формируется криминологический портрет лица, совершающего дистанционные хищения.

Установлено, что для данной категории преступников характерны мужской пол, возраст от 18 до 40 лет, отсутствие постоянной занятости либо занятость в сферах торговли, услуг и логистики, образование не ниже среднего специального, преимущественно корыстная мотивация, рациональность, манипулятивность и эмоциональная дистанцированность от последствий содеянного. Значительная часть лиц ранее не судима, однако для трети из них характерно повторное совершение тождественных преступлений.

Обобщённый портрет конкретизируется посредством типологии участников дистанционных хищений, выделенных по функциональной

роли в преступной схеме: организатор, технический исполнитель, социальный инженер («звонарь») и номинальный участник (дроппер). Организатор осуществляет планирование и координацию преступной деятельности; технический исполнитель обеспечивает несанкционированный доступ к цифровым ресурсам и совершение операций с чужими денежными средствами; социальный инженер воздействует на потерпевшего путём обмана и психологического манипулирования; номинальный участник предоставляет банковские карты, счета или иные реквизиты для легализации похищенных средств.

Выделенные типы различаются возрастом, уровнем образования, профессиональной принадлежностью, степенью вовлечённости в преступную деятельность, характером выполняемых функций и выраженностью криминальной устойчивости. Учёт указанных различий позволяет дифференцировать меры предупреждения дистанционных хищений.

Во втором параграфе *«Мотивация и вербовка лиц, совершающих хищения дистанционно»* рассматривается многофакторная структура мотивации и механизм вербовки.

Обосновывается вывод, что мотивационная структура лиц, совершающих дистанционные хищения, включает шесть компонентов: корыстный (ориентация на значительную материальную выгоду), рационально-технологический (ориентация на минимизацию рисков и автоматизацию действий), профессионально-статусный (желание самоутверждения через демонстрацию компетентности в обходе цифровых средств защиты), психологический (иллюзия анонимности и дистанцирования от причиняемого вреда), риско-ориентированный (восприятие низкой вероятности привлечения к ответственности), ситуативно-оппортунистический (использование случайного доступа к чужим данным). Указанные компоненты проявляются в различных сочетаниях и с разной степенью выраженности в зависимости от функциональной роли лица в преступной схеме.

Раскрыт механизм вербовки, включающий две модели: латентное вовлечение (введение лица в заблуждение относительно истинной сущности выполняемых действий, маскировка преступных задач под социально приемлемые формы занятости) и осознанное вовлечение (прямое информирование потенциального исполнителя о незаконности предполагаемой деятельности, ориентация на лиц, готовых сознательно участвовать в преступлении за вознаграждение). Обосновано, что вербовка выступает не только способом вовлечения новых участников, но и юридически значимым элементом структуры соучастия, определяющим квалификацию действий в рамках ст. 33 УК РФ.

В третьем параграфе *«Система предупреждения дистанционных хищений»* предлагается комплексная система мер их предупреждения.

Под системой предупреждения дистанционных хищений понимается совокупность отношений, выстраиваемых между субъектами предупредительной деятельности и объектами предупреждения, направленных на достижение цели борьбы с дистанционными хищениями. Объектом предупреждения выступают причины, условия и факторы, детерминирующие развитие рассматриваемой разновидности преступной деятельности; сама преступность; группы лиц с повышенной вероятностью совершения таких деяний; жертвы посягательств.

Субъекты предупреждения дифференцированы на специализированные, чья деятельность непосредственно направлена на борьбу с дистанционными хищениями (органы МВД России, ФСИН РФ, Прокуратура РФ, Следственный комитет РФ); факультативные, участвующие в профилактике наряду с выполнением иных задач (органы исполнительной власти, СМИ); субъекты-участники, содействующие предупреждению и профилактике на служебной или добровольной основе (частные предприятия, банки, операторы связи).

Меры предупреждения классифицированы по направленности действия на общесоциальные (минимизация влияния негативных антисоциальных явлений), правовые (обеспечение эффективно

функционирующей нормативно-правовой системы защиты), организационно-управленческие (разработка программно-целевого планирования деятельности субъектов предупреждения и координация их активностей), технические (разработка более совершенных механизмов защиты информационного пространства), культурно-воспитательные (повышение у населения цифровой грамотности). Такая классификация позволяет обеспечить комплексный характер предупредительного воздействия и согласовать усилия государственных органов, кредитных организаций, операторов связи, средств массовой информации и иных участников профилактической деятельности.

Особое внимание уделено использованию интеллектуальных программных решений, основанных на анализе больших массивов данных, выявлении аномалий финансовой активности, поведенческих паттернов преступников и потенциальных потерпевших. Автором разработана программа для ЭВМ «Программа для определения рисков дистанционных хищений с использованием электронных средств платежа» (Свидетельство о государственной регистрации программы для ЭВМ № 2026667563 от 09.06.2026). В результате использования разработанной программы на синтетических выборках удалось на 23% увеличить полноту обнаружения мошеннических действий и на 32% уменьшить количество ложных срабатываний.

По результатам исследования определены приоритетные направления совершенствования системы предупреждения дистанционных хищений в правовой, организационно-управленческой, технической и культурно-воспитательной сферах. Их реализация должна обеспечивать согласованность правового регулирования, межведомственного взаимодействия, технической защиты цифровой инфраструктуры и профилактической работы с населением.

В заключении представлены результаты диссертационного исследования, включающие теоретические положения, основные выводы,

практические рекомендации и предложения, а также определены перспективы дальнейшего изучения проблематики.

В приложениях содержатся обобщённые эмпирические данные, включающие в себя результаты проведённого анкетирования сотрудников правоохранительных органов Курской и Белгородской областей, формуляр изучения материалов уголовных дел о дистанционных хищениях, описание программы для ЭВМ для определения рисков дистанционных хищений с использованием электронных средств платежа. Также автором проведена систематизация комплекса предложений по совершенствованию нормативно-правовой базы посредством внесения изменений и дополнений в действующие правовые акты.

Основные положения диссертации опубликованы в следующих работах автора:

Статьи в рецензируемых научных изданиях, в которых должны быть опубликованы основные научные результаты диссертаций:

1. Пивнева, Л. В. Проблемы квалификации преступлений по ст. 159.3 Уголовного кодекса Российской Федерации / Л. В. Пивнева // Вестник Белгородского юридического института МВД России имени И.Д. Путилина. – 2024. – № 2. – С. 100–105. (0,4 п.л.).

2. Пивнева, Л. В. Профессиональное компьютерное мошенничество как разновидность профессиональной преступной деятельности в современных условиях развития информационного пространства / Л. В. Пивнева // Вестник Волгоградской академии МВД России. – 2025. – № 1(72). – С. 41–47. (0,4 п.л.).

3. Пивнева, Л. В. Спорные вопросы применения ст. 159.6 УК РФ / Л. В. Пивнева // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. – 2026. – Т. 12, № 2. – С. 501–510. (0,6 п.л.).

4. Пивнева, Л. В. Виртуальная виктимность: методики повышения цифровой грамотности населения как инструмент предупреждения

хищений / Л. В. Пивнева // Право и управление. – 2026. – № 1. – С. 563–566. (0,3 п.л.).

5. Пивнева, Л. В. Уголовно-правовое регулирование дистанционных хищений в России / Л. В. Пивнева // Проблемы правоохранительной деятельности. – 2026. – № 2(64). – С. 58–63. (0,4 п.л.).

6. Пивнева, Л. В. Коллизии и пробелы в системе уголовно-правовых норм о хищениях, совершаемых дистанционно: проблемы квалификации по статьям 158, 159.3 и 159.6 УК РФ / Л. В. Пивнева // Право и государство: теория и практика. – 2026. – № 4. – С. 386–388. (0,2 п.л.).

Публикации в иных изданиях:

7. Пивнева, Л. В. Дистанционное мошенничество: современные способы совершения преступления и проблемы раскрытия / Л. В. Пивнева // Инновационный потенциал развития общества: взгляд молодых ученых : Сборник научных статей 4-й Всероссийской научной конференции перспективных разработок, Курск, 1 декабря 2023 года. – Курск: Университетская книга, 2023. – С. 425–428. (0,3 п.л.).

8. Пивнева, Л. В. Понятие, признаки и проблемы квалификации дистанционного хищения / Л. В. Пивнева // Наука молодых – будущее России : сборник научных статей 8-й Международной научной конференции перспективных разработок молодых ученых, Курск, 12–13 декабря 2023 года. – Курск: Университетская книга, 2023. – С. 221–224. (0,3 п.л.).

9. Пивнева, Л. В. Профессиональное компьютерное мошенничество как современная угроза обществу и государству / Л. В. Пивнева // Белгородские криминалистические чтения : Сборник научных трудов, Белгород, 26 апреля 2024 года. – Белгород: Белгородский юридический институт МВД России имени И.Д. Путилина, 2024. – С. 142–146. (0,3 п.л.).

10. Пивнева, Л. В. Уголовно-правовая и криминалистическая характеристика преступлений, совершаемых с использованием IT-технологий / Л. В. Пивнева // Белгородские криминалистические чтения : Сборник научных трудов, Белгород, 26 апреля 2025 года. – Белгород:

Белгородский юридический институт МВД России имени И.Д. Путилина, 2025. – С. 91-94. (0,3 п.л.).

11. Пивнева, Л. В. Проблемы расследования и доказывания дистанционных хищений: криминалистический аспект / Л. В. Пивнева // Белгородские криминалистические чтения : Сборник научных трудов, Белгород, 20 мая 2026 года. – Белгород: Белгородский юридический институт МВД России имени И.Д. Путилина, 2026. – С. 114-118. (0,3 п.л.).

12. Пивнева, Л. В. О проблемах криминологического противодействия дистанционному мошенничеству при использовании подменных абонентских номеров и технологий социальной инженерии (по материалам Белгородской области) / Л. В. Пивнева// XII Путилинские чтения : сборник материалов Всероссийской научно-практической конференции, 27 марта 2026 г. – Белгород : Белгородский юридический институт МВД России имени И.Д. Путилина, 2026. – С. 79-85. (0,5 п.л.).