Федеральное государственное
бюджетное образовательное учреждение высшего образования
«Юго-Западный государственный университет»

На правах рукописи

Пивнева Людмила Валерьевна

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

Специальность 5.1.4. Уголовно-правовые науки

ДИССЕРТАЦИЯ
на соискание ученой степени кандидата юридических наук

Научный руководитель:
доктор юридических наук, доцент
Баумштейн Антон Борисович

Курск – 2026

СОДЕРЖАНИЕ

Введение 3
Глава 1. Теоретические основы хищений, совершаемых дистанционно 21
1.1. Понятие и юридическая природа хищений, совершаемых дистанционно 21
1.2. Формы и способы хищений, совершаемых дистанционно 50
Глава 2. Уголовно-правовые средства противодействия хищениям, совершаемым дистанционно 73
2.1. Система уголовно-правовых средств противодействия хищениям, совершенным дистанционно 73
2.2. Наказуемость хищений, совершённых дистанционно 114
Глава 3. Криминологические основы предупреждения дистанционных хищений 137
3.1. Криминологическая характеристика лиц, совершающих дистанционные хищения 137
3.2. Мотивация и вербовка лиц, совершающих хищения дистанционно 159
3.3. Система предупреждения дистанционных хищений 180
Заключение 211
Список литературы 220
Приложение 1 255
Приложение 2 259
Приложение 3 263
Приложение 4 270
Приложение 5 271

Введение

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 преступности остаётся значительным. Кроме того, почти две трети

[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).

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 необходимость уточнения содержания и признаков дистанционного хищения, определения

[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).

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 разъяснений 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.

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.

Глава 1. Теоретические основы хищений, совершаемых дистанционно

1.1. Понятие и юридическая природа хищений, совершаемых дистанционно

Понятие хищения в отечественной уголовно-правовой науке имеет нормативно закреплённое содержание. Согласно Примечания 1 к ст. 158 УК РФ, под хищением понимаются совершённые с корыстной целью противоправные безвозмездное изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, причинившие ущерб собственнику или иному владельцу этого имущества. Из приведённого законодательного определения вытекают обязательные признаки хищения, например, корыстная цель, противоправность изъятия, безвозмездность завладения и т.д.

Вместе с тем развитие информационно-телекоммуникационных технологий обусловило существенную трансформацию способов совершения хищений, при которой традиционные элементы данного состава реализуются в условиях пространственной удалённости участников имущественных отношений. В связи с этим в научном обороте обоснованно выделяется дистанционный характер хищений, предполагающий территориальную разобщённость потерпевшего и субъекта преступления, а также отсутствие непосредственного физического контакта между ними (понятие «дистанционный» образовано от латинского слова *distantia* – расстояние[9]).

В то же время следует отметить, что в научной литературе при характеристике хищений, совершаемых с использованием цифровых технологий, используется значительное количество смежных и частично пересекающихся понятий.

[9] Скворцов Л.И. Большой толковый словарь правильной русской речи: 8000 слов и выражений. М.: ООО «Издательство Оникс»: ООО «Издательство «Мир и образование», 2009. С. 179.

Часть исследователей в настоящее время дистанционные хищения называют интернет-мошенничеством[10], другие – компьютерным мошенничеством[11], некоторые – мошенничеством в сфере компьютерной информации[12], а также онлайн-хищениями[13], хищениями с использованием мобильных средств связи и сети интернет[14], кибермошенничеством, кражей с использование электронных средств платежа[15] и т.д. Вместе с тем, соглашаясь с мнением отдельных исследователей, также заметим, что данные понятия трактуются научным сообществом правоведов и криминологов достаточно вольно и нередко используются как синонимы[16]. Подобная терминологическая множественность обусловлена, прежде всего, спецификой цифровой среды совершения преступлений и многообразием используемых информационно-технологических средств воздействия на имущественные отношения, реализуемых в рамках цифровой инфраструктуры[17]. Между тем, указанные понятия, несмотря на широкое распространение, не обладают достаточной степенью юридической определённости и, как правило, отражают лишь отдельные технологические или средовые характеристики преступного поведения, не охватывая всего спектра способов совершения посягательств. Так, термины «интернет-мошенничество» или «интернет-хищения» ограничивают анализ

[10] Теплова Д.О. Криминологические основы противодействия организованному мошенничеству: монография. М.: РГУП, 2017. С. 116; Дворянкин О.А. Интернет мошенничество – это новая интернет технологии или жадность и алчность неистребимы...? // НАУ. 2021. № 64-1. С. 14-20; Маилян А.В. О криминалистической характеристике отдельных видов интернет мошенничества // Право и государство: теория и практика. 2019. № 3 (171). С. 98-100; Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2010. С. 58 и др.

[11] Богданчиков С.В. противодействие преступным посягательствам на абсолютные права собственности (хищения): монография. – М.: ЮНИТИ-ДАНА: Закон и право, 2017. С. 26.

[12] Энгельгардт А.А. О понимании мошенничества в сфере компьютерной информации // Вестник Московского университета МВД России. 2016. № 8. С. 84-90.

[13] Полстовалов О.В., Галяутдинов Р.Р. Организованные формы онлайн-мошенничества: виды, содержание и элементы криминалистической характеристики // Вестник КГУ. 2023. № 4. С. 205-211.

[14] Левашова О.В., Сурнова Е.Ю. Понятие мошенничества с использованием мобильных средств связи и сети интернет // Государственная служба и кадры. 2021. № 2. С. 114-117.

[15] Красовская Н.Р., Гуляев А.А. К вопросу о кибермошенничестве // Вестник Удмуртского университета. Социология. Политология. Международные отношения. 2022. № 1. С. 133-138.

[16] Барчуков В.К. Терминология мошенничества в сфере компьютерной информации // Пробелы в российском законодательстве. 2017. № 4. С. 163-165.

[17] В рамках настоящего исследования под цифровой инфраструктурой надлежит понимать совокупность информационно-телекоммуникационных сетей, электронных платежных систем, программно-аппаратных комплексов, устройств связи, банковских цифровых сервисов, электронных кошельков, онлайн-платформ и иных технических средств, обеспечивающих удалённое совершение имущественных операций.

исключительно сетью Интернет, исключая иные дистанционные каналы воздействия (мобильная связь, банковские платёжные системы, офлайн-цифровые интерфейсы, банкоматные и терминальные сети), которые активно используются в преступной практике.

Понятие «киберхищения» носит преимущественно криминологический характер и объединяет широкий круг деяний, связанных с использованием цифровых технологий, однако не отражает юридико-структурной специфики хищения как уголовно-правовой категории. Категория «компьютерное мошенничество» или «компьютерное хищение», в свою очередь, неоправданно сужает сферу анализа до взаимодействия с компьютерной техникой, не учитывая многоуровневую цифровую инфраструктуру современных финансовых и коммуникационных систем. В этой связи представляется обоснованным использование термина «дистанционное хищение». Его преимущество состоит в том, что он характеризует не используемую при совершении преступления технологию, а способ взаимодействия виновного с потерпевшим. Определяющим является отсутствие непосредственного физического контакта между ними при направленности действий виновного на безвозмездное завладение чужим имуществом. Такой подход позволяет рассматривать в рамках одного понятия различные способы совершения хищений, если их объединяет дистанционный характер взаимодействия участников. При этом использование информационно-телекоммуникационных технологий не выступает обязательным признаком самого понятия, поскольку соответствующие средства могут выполнять различную функцию в механизме преступления, например, обеспечивать связь с потерпевшим, передачу информации, получение доступа к имуществу либо совершение иных действий, необходимых для реализации преступного умысла. Выбор термина «дистанционное хищение» имеет значение и с точки зрения его дальнейшего применения. Понятие не связано с определённой технологией или конкретным каналом коммуникации, поэтому его содержание не зависит

от сохранения существующих интернет-сервисов, компьютерных систем или иных технических решений. При изменении способов дистанционного взаимодействия квалифицирующим для предлагаемой категории остаётся характер отношений между виновным и потерпевшим, а не конкретное техническое средство, посредством которого осуществляется преступная деятельность.

Указанные обстоятельства обусловливают необходимость выработки более точного и универсального понятийного обозначения, в качестве которого представляется целесообразным использование категории «дистанционное хищение», позволяющей охватить все формы противоправного безналичного и цифрового завладения имуществом без непосредственного физического контакта с предметом посягательства. В связи с этим далее представляется необходимым обратиться к анализу классических признаков хищения и выявить особенности их трансформации при совершении хищений дистанционным способом, что позволит впоследствии сформулировать авторское определение рассматриваемого понятия.

Как отмечалось ранее, в условиях цифровизации имущественного оборота корыстная цель как обязательный субъективный признак хищения сохраняет своё фундаментальное значение и в дистанционных формах преступного посягательства, однако способы её реализации приобретают качественно иные, более сложные и опосредованные характеристики. По своей правовой природе корыстная цель в дистанционных хищениях тождественна корыстной цели при «классических» формах хищения и выражается в стремлении виновного к противоправному безвозмездному извлечению имущественной выгоды за счёт другого лица. Вместе с тем специфика дистанционного формата существенно усиливает и трансформирует механизм её достижения. Так, в традиционных хищениях корыстная цель реализуется через непосредственное физическое изъятие имущества либо прямое воздействие на потерпевшего. В дистанционных же

хищениях корыстная цель достигается опосредованно. В результате корыстная цель не ослабевает, а, напротив, реализуется в более «усиленной» форме, поскольку позволяет извлекать имущественную выгоду без физического контакта, с минимальными затратами и при значительно более высоком уровне латентности. Определённое «усиление» корыстной цели в дистанционных хищениях проявляется также в их серийности, масштабируемости и высокой экономической эффективности. Использование автоматизированных алгоритмов, вредоносного программного обеспечения, фишинговых и социально-инженерных технологий позволяет преступнику многократно воспроизводить преступный результат, одновременно причиняя ущерб неограниченному кругу потерпевших. При этом субъективная сторона преступления сохраняет классическую направленность на извлечение материальной выгоды, но дополняется расчётом на анонимность, трансграничность и затруднённость выявления преступника[18].

Следовательно, корыстная цель в дистанционных хищениях по своему содержанию полностью совпадает с корыстной целью в традиционных формах хищения, однако отличается более высоким уровнем рационализации, технологической опосредованности и интенсивности реализации. Данное обстоятельство требует учета при уголовно-правовой оценке дистанционных посягательств и подтверждает необходимость сохранения единого подхода к пониманию корыстной цели как системообразующего признака хищения, независимо от формы его совершения.

При дистанционном хищении противоправное «изъятие» происходит не физически, а посредством нарушения законного режима владения, пользования и распоряжения имущества потерпевшего. Так, неправомерный доступ к банковскому счету, использование украденных реквизитов,

[18] Семенов А.В. Ст. 159[3] УК РФ «Квалификация мошенничества, совершенного с использованием электронных средств платежа» // Вестник науки. 2025. № 3 (84). С. 198-203.

подделка платежных карт, фишинг, взлом онлайн- банкинга и многое другое – это своеобразные формы цифрового воздействия, лишённые физического контакта, но обладающие точно такой же противоправностью, как и «традиционные» действия, направленные на изъятие имущества.

Следующий признак – безвозмездность – отсутствие встречного предоставления – при дистанционном хищении выражается в фактическом лишении потерпевшего имущественного блага без какого-либо эквивалентного возмещения, несмотря на внешнюю «добровольность» совершаемых им действий. В дистанционных хищениях безвозмездность приобретает особенно завуалированный характер, поскольку противоправное изъятие имущества осуществляется не путём открытого физического изъятия, а посредством введения потерпевшего в заблуждение, злоупотребления доверием либо скрытого вмешательства в цифровые механизмы распоряжения имуществом. В отличие от «классических» форм хищения, где отсутствие встречного предоставления, как правило, очевидно и объективно фиксируемо (например, изъятие вещи без передачи эквивалента), при дистанционном хищении создаётся определённая иллюзия возмездности. Потерпевший нередко полагает, что совершает правомерную имущественную операцию, например, оплачивает товар или услугу, переводит денежные средства в целях «обеспечения безопасности счёта», «подтверждения операции», «инвестирования» и т.п., однако в действительности никакого встречного предоставления не предполагается и не осуществляется, а действия потерпевшего направлены исключительно на незаконное обогащение виновного. Так, безвозмездность в дистанционных хищениях выражается не столько в отсутствии формального основания для передачи имущества, сколько в отсутствии реального экономического эквивалента, поступающего потерпевшему. Даже если преступник имитирует наличие обязательства (фиктивный договор, поддельный сайт, ложная инвестиционная платформа и т.п.), такая «возмездность» носит мнимый

характер и не устраняет безвозмездности как обязательного признака хищения.

В свою очередь, соглашаясь с мнением отдельных современных исследователей, особенностью дистанционного хищения является также и то, что безвозмездность реализуется через неправомерное использование правомочий распоряжения имуществом потерпевшего. Передача денежных средств или цифровых активов осуществляется самим потерпевшим, однако под воздействием, например, обмана или злоупотребления доверием, вследствие чего утрачивается их экономическое содержание как возмездной сделки[19]. В этом смысле дистанционное хищение демонстрирует расширенное понимание безвозмездности, при котором решающим является не формальный характер передачи имущества, а отсутствие эквивалентного имущественного результата.

Следовательно, признак безвозмездности в дистанционных хищениях сохраняет свою уголовно-правовую сущность, но проявляется в более сложной и опосредованной форме. Он выражается в причинении имущественного ущерба без предоставления потерпевшему реальной экономической выгоды, независимо от того, осуществляется ли передача имущества напрямую либо посредством использования цифровых каналов, что также подтверждает единство уголовно-правовой природы дистанционных и традиционных форм хищения.

Анализируя такой признак, как обращение чужого имущества в пользу виновного или третьих лиц, укажем, что в дистанционных случаях совершения хищений он приобретает специфические формы, обусловленные цифровым характером имущественного оборота и отсутствием непосредственного физического контакта. В дистанционных хищениях обращение чужого имущества в пользу виновного либо третьих лиц осуществляется, по справедливому утверждению некоторых исследователей,

[19] Халиков А.Н. Проблема квалификации дистанционных хищений как отдельного состава преступления // Евразийская адвокатура. 2025. № 4 (75). С. 117–122.

как правило, не через непосредственное завладение вещью, а посредством изменения правомочий распоряжения имуществом, выраженного в переводе денежных средств, цифровых активов на счета, электронные кошельки либо иные подконтрольные виновному инструменты[20]. При дистанционном способе совершения хищения механизм обращения имущества имеет свои особенности. Если при непосредственном завладении имуществом виновный получает возможность фактически овладеть вещью, то при совершении преступления дистанционно предметом воздействия нередко выступают денежные средства, находящиеся на банковском счёте, в электронном кошельке либо в иной форме безналичного имущественного оборота. В таких случаях действия виновного направлены на получение возможности распорядиться чужими денежными средствами и фактически вывести их из сферы контроля потерпевшего. Именно создание такой возможности при наличии остальных признаков хищения имеет значение для определения момента окончания преступления.

Между тем, специфика обращения имущества может проявляться и в том, что после первоначального завладения денежные средства перемещаются через несколько счетов, банковских карт, электронных кошельков или иных платёжных инструментов. Такая последовательность действий затрудняет установление лица, в интересах которого в конечном счёте осуществлялось распоряжение похищенным. Вместе с тем само по себе использование промежуточных счетов и иных участников не меняет направленности преступления. Если перемещение денежных средств осуществляется для обеспечения их последующего использования виновным либо другими лицами, действующими в рамках общего преступного умысла, речь по-прежнему идёт об обращении чужого имущества в пользу виновного или других лиц.

[20] Кирилюк М.А., Литвиненко А.Н. Характеристика способов дистанционных хищений денежных средств как этап ситуационного анализа // Вестник экономической безопасности. 2023. № 1. С. 119-225.

Последствия такого посягательства имеют имущественный характер независимо от того, существует ли предмет хищения в форме вещи. При списании денежных средств со счёта, уменьшении остатка электронного кошелька или ином неправомерном прекращении возможности потерпевшего распоряжаться принадлежащими ему денежными средствами происходит уменьшение его имущественной сферы. Поэтому отсутствие непосредственного физического воздействия на вещь не означает отсутствия имущественного ущерба. Изменяется способ причинения вреда, но не его экономическое содержание.

Таким образом, дистанционный способ совершения хищения сам по себе не изменяет содержания признаков, закреплённых в примечании 1 к статье 158 УК РФ. Корыстная цель, противоправность, безвозмездность, обращение чужого имущества в пользу виновного или других лиц и причинение ущерба собственнику либо иному владельцу сохраняют своё уголовно-правовое значение. При этом особенность заключается в способе их реализации. Преступное воздействие осуществляется опосредованно, а движение имущества и получение возможности распоряжаться им могут быть распределены между несколькими последовательными действиями и участниками. Это значит, что специфика дистанционных хищений не требует изменения законодательного определения хищения. Основная проблема, напротив, состоит в установлении того, каким образом традиционные признаки хищения проявляются при использовании современных способов дистанционного хищения.

В современном УК РФ такие деяния квалифицируются по следующим нормам: п. «г» ч. 3 ст. 158 УК РФ (кража, совершённая с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного ст. 159^3 УК РФ)), ст. 159^3 УК РФ (мошенничество с использованием электронных средств платежа) и ст. 159^6 УК РФ (мошенничество в сфере компьютерной информации). Кроме того, дистанционный способ может использоваться при совершении

мошенничества, предусмотренного общей нормой ст. 159 УК РФ, если содеянное не содержит специальных признаков составов, предусмотренных ст. 159^3 и 159^6 УК РФ. Таким образом, ст. 159 УК РФ также охватывает часть дистанционных хищений, однако выделение их количественных показателей в составе общей статистики мошенничества не совсем корректно, поскольку официальная статистическая отчётность не содержит самостоятельной категории дистанционных хищений и не позволяет разграничить преступления, предусмотренные ст. 159 УК РФ, по способу их совершения, в связи с этим проведение такого разграничения на основании исключительно статистических данных привело бы к недостоверному определению масштабов дистанционного мошенничества. При этом используемая в информационных отчётах МВД РФ статистическая категория мошенничеств, совершённых с использованием информационно-телекоммуникационных технологий, не может быть полностью отождествлена с категорией дистанционных хищений, поскольку использование ИКТ характеризует технологическую сторону совершения преступления, тогда как дистанционный характер хищения отражает способ взаимодействия участников преступления и механизм реализации преступного посягательства. В результате «классические» статьи, по которым привлекают к уголовной ответственности современных преступников, совершающих хищения дистанционно, это п. «г» ч. 3 ст. 158, ст. 159^3 и ст. 159^6 УК РФ. Далее для уточнения признаков дистанционных хищений с целью формулирования определения исследуемого понятия, считаем необходимым кратко рассмотреть данные составы преступлений.

Итак, в первую очередь, кратко проанализируем п. «г» ч. 3 ст. 158 УК РФ (кража, совершённая с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного ст. 159^3 УК РФ)). Данная статья была введения в действие Федеральным законом «О внесении изменений в Уголовный кодекс

Российской Федерации» от 23.04.2018 № 111-ФЗ[21], в пояснительной записке которого указывалось, что число транзакций, совершаемых дистанционно клиентами отдельных банков, достигает 95% и увеличивается ежегодно, вследствие чего в данном финансовом секторе отмечается значительный рост хищений с банковских счетов и прочих преступлений против клиентов банков. Ввиду этого отмечается необходимость усиления уголовно-правовой защиты организаций и граждан путём ужесточения уголовной ответственности за хищение чужого имущества, совершённое в отношении электронных денежных средств посредством дополнения ч. 3 ст. 158 УК РФ соответствующим квалифицирующим признаком. В качестве обоснования необходимости данного изменения также указывается специфика совершения такого рода общественно опасных деяний, исключающая физический контакт преступника и жертвы преступления, а также схожий опыт законодательного регулирования данной сферы общественных отношений в зарубежных странах (в частности, во Франции, КНР, ФРГ и т.д.)[22]. Дифференциация уголовной ответственности в данном случае определяется особым способом, а также особым предметом преступления. Для уточнения предмета преступления определим, что данный квалифицирующий признак кражи имеет место быть только при хищении безналичных и электронных денежных средств путем их перевода[23].

Следующая норма, по которой в современном уголовно-правовом пространстве квалифицируют дистанционные хищения, – это ст. 159^3 (мошенничество с использованием электронных средств платежа) УК РФ. Первоначально данная статья имела другое название и содержание (мошенничество с использованием платежных карт). Указанная норма

[21] Федеральный закон «О внесении изменений в Уголовный кодекс Российской Федерации» от 23.04.2018 № 111-ФЗ [Электронный документ]. – URL: https://www.consultant.ru/document/cons_doc_LAW_296451/ (дата обращения: 16.02.2026).

[22] Законопроект № 186266-7 [Электронный документ]. URL: https://sozd.duma.gov.ru/bill/186266-7 (дата обращения: 17.02.2026).

[23] Федеральный закон от 27.06.2011 № 161-ФЗ (ред. от 08.08.2024) «О национальной платежной системе» [Электронный документ]. – URL: https://www.consultant.ru/document/cons_doc_LAW_115625/4f41fe599ce341751/ (дата обращения: 18.02.2026).

впервые введена в УК РФ Федеральным законом от 29.11.2012 № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации». Данный вид мошенничества определялся законом, как хищение чужого имущества, которое совершено с использованием принадлежащей другому лицу или поддельной расчётной, кредитной или другой платежной карты путем обмана уполномоченного работника торговой, кредитной или иной организации. Также в указанной норме были обозначены такие квалифицирующие признаки как совершение данного деяния группой лиц по предварительному сговору, организованной группой, с причинением значительного ущерба гражданину, с использованием лицом служебного положения, а также в крупном и особо крупном размерах[24].

Позднее Федеральным законом «О внесении изменений в Уголовный кодекс Российской Федерации» от 23.04.2018 № 111-ФЗ в УК РФ указанная норма была изложена в новой редакции. В соответствии с данным нормативным правовым актом этот состав преступлений охватывал мошенничества с использованием электронных средств платежа. При этом квалифицирующие признаки были сохранены, а наказания ужесточены. Так, по ч. 1 ст. 159^3 УК РФ вместо ареста на срок до четырёх месяцев теперь предусматривается лишение свободы на срок до трёх лет. Также изменились крупный и особо крупный размеры ущерба. Если ранее такое мошенничество считалось совершённым в крупном размере в том случае, если было похищено более 1,5 млн рублей, то в действующей редакции нормы – 250 тыс. рублей, особо крупным – вместо 6 млн рублей и более – 1 млн рублей и более[25]. Данные изменения произошли вследствие необходимости расширения сферы применения нормы ввиду более активного развития

[24] Федеральный закон от 29.11.2012 № 207-ФЗ (ред. от 03.07.2016) «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» [Электронный документ]. – URL: https://www.consultant.ru/document/cons_doc_LAW_138322/3d0cac60971a511280cbba229/ (дата обращения: 19.02.2026).

[25] Федеральный закон «О внесении изменений в Уголовный кодекс Российской Федерации» от 23.04.2018 № 111-ФЗ [Электронный документ]. – URL: https://www.consultant.ru/document/cons_doc_LAW_296451/ (дата обращения: 20.02.2026).

информационных технологий и появления таких новых электронных средств осуществления платежей как электронные кошельки, платежные приложения, вследствие чего для обозначения всех возможных способов совершения мошеннических действий в данной сфере в федеральном законодательстве стали использовать обобщающее понятие «электронное средство платежа»[26]. Ужесточение санкции, в свою очередь, обусловлено распространённостью указанной разновидности преступной деятельности и высокой степенью общественной опасности совершаемых деяний. Предметом данного преступления, определяющего наряду со способом совершения данного преступного посягательства его высокую степень и характер общественной опасности, являются электронные средства платежа[27].

Ещё одна норма уголовного закона, прямо нацеленная на борьбу с дистанционными хищениями, – это ст. 159^6 (мошенничество в сфере компьютерной информации) УК РФ. Эта норма была так же, как и ст. 159^3 УК РФ введена в действие Федеральным законом от 29.11.2012 № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации». Указанный вид мошенничества определён законом, как приобретение права на чужое имущество или хищение чужого имущества путем ввода, удаления, модификации и блокирования компьютерной информации, либо посредством другого вмешательства в функционирование средств передачи, обработки и хранения компьютерной информации или же информационно-телекоммуникационных сетей. За совершение рассматриваемого общественно опасного деяния назначалось максимальное наказание в виде ареста на срок до четырёх месяцев. Также предусматривались следующие квалифицирующие признаки: совершение деяния группой лиц по

[26] Думанская Е.И., Меньшикова А.Г. Мошенничество с использованием электронных средств платежа: трансформация в законе и практике // Правопорядок: история, теория, практика. 2022. № 3 (34). С. 50-57.
[27] Федеральный закон от 27.06.2011 № 161-ФЗ (ред. от 08.08.2024) «О национальной платежной системе» [Электронный документ]. – URL: https://www.consultant.ru/document/cons_doc_LAW_115625/ (дата обращения: 21.02.2026).

предварительному сговору, организованной группой, а равно с использованием служебного положения, с причинением значительного ущерба гражданину, ущерба в крупном и особо крупном размере[28]. Изменения в данную норму были внесены Федеральным законом от 03.07.2016 № 325-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации» (ужесточена санкция за совершение мошенничества в сфере компьютерной информации группой лиц по предварительному сговору, с причинением значительного ущерба, ущерба в крупном размере и с использованием служебного положения)[29]. Последние изменения в ч. 3 ст. 159[6] УК РФ внесены Федеральным законом «О внесении изменений в Уголовный кодекс Российской Федерации» от 23.04.2018 № 111-ФЗ, где к деяниям, совершённым в крупном размере, а равно с использованием своего служебного положения лицом в качестве квалифицирующего признака также добавилось совершение мошенничества в сфере компьютерной информации с банковского счёта, а равно в отношении электронных денежных средств с назначением наказания до шести лет лишения свободы[30]. Предметом такого преступления признаётся чужое имущество или право на чужое имущество. При этом важнейшим средством совершения преступления (но не дополнительным предметом), по точному замечанию Н.А. Лопашенко, является компьютерная информация, с помощью которой преступник осуществляет мошеннические действия[31].

[28] Федеральный закон от 29.11.2012 № 207-ФЗ (ред. от 03.07.2016) «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» [Электронный документ]. – URL: https://www.consultant.ru/document/cons_doc_LAW_138322/3d0cac60971a511280cbba229d/ (дата обращения: 22.02.2026).

[29] Федеральный закон от 03.07.2016 № 325-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации» [Электронный документ]. – URL: https://www.consultant.ru/document/cons_doc_LAW_200714/3d0cac60971a511280cbba229d9b6329c07731f7/ (дата обращения: 23.02.2026).

[30] Федеральный закон «О внесении изменений в Уголовный кодекс Российской Федерации» от 23.04.2018 № 111-ФЗ [Электронный документ]. – URL: https://www.consultant.ru/document/cons_doc_LAW_296451/ (дата обращения: 24.02.2026).

[31] Лопашенко Н.А. Компьютерное мошенничество – новое слово в понимании хищения или ошибка законодателя? // Пермский юридический альманах. 2019. № 2. С. 598-609.

Так, отнесение анализируемых норм к категории дистанционных хищений предопределяется тем, что преступления совершаются без физического взаимодействия преступника с потерпевшим и зачастую – без непосредственного доступа к материальным носителям информации, при этом осуществление посягательства становится возможным исключительно благодаря использованию электронных средств платежа, информационно-телекоммуникационных технологий и компьютерных систем, что позволяет воздействовать на процесс распоряжения денежными средствами удалённо. В свою очередь, предмет преступления существует в цифровой форме, что делает его уязвимым для удалённого вмешательства, а результат в виде утраты имущества достигается путём изменения, подделки либо манипуляции информацией, а не посредством непосредственного изъятия материальных объектов. Это позволяет квалифицировать указанные деяния как дистанционные хищения, сущность которых раскрывается в удалённом, технически опосредованном завладении денежными средствами или правами на них через воздействие на информационные механизмы, обеспечивающие финансовый оборот. Всё это в совокупности позволяет выделить системообразующие признаки не просто хищения, а дистанционного хищения (по материалам анализа конкретных норм российского уголовного законодательства, криминализующих такие деяния).

В первую очередь, следует отметить корыстную цель как обязательный признак субъективной стороны хищения, которая заключается в стремлении виновного обратить чужое имущество в свою пользу или пользу других лиц. Данный признак закреплён в общем определении хищения, приведённом в Примечании 1 к ст. 158 УК РФ, и лежит в основе квалификации дистанционных хищений по ст. 158 (п. «г» ч. 3), ст. 159^3 и ст. 159^6 УК РФ.

Далее – противоправность изъятия – это нарушение законного порядка владения, распоряжения или контроля над имуществом. В дистанционной среде непосредственного физического контакта нет, однако противоправность проявляется через несанкционированный доступ

к банковским счетам, электронным кошелькам, учетным записям, программным системам и т.п.

Признак безвозмездности завладения при дистанционных хищениях заключается в том, что преступник получает денежные средства или имущественные права без какого-либо встречного предоставления потерпевшему, при полном отсутствии эквивалентного обмена и реального волеизъявления владельца. Так, в п. «г» ч. 3 ст. 158 УК РФ безвозмездность проявляется в тайном и внезапном переводе безналичных либо электронных средств, при котором потерпевший ничего не получает взамен и даже не участвует в операции. Указанный подход получил дополнительное нормативно-разъяснительное развитие в Постановлении Пленума Верховного Суда РФ от 16 июня 2026 г. № 19, которым уточнено, что отсутствие эквивалентного встречного предоставления и реального волеизъявления собственника сохраняется и в случаях, когда обман используется лишь для облегчения доступа к имуществу либо отвлечения внимания потерпевшего, тогда как само изъятие носит тайный характер и фактически осуществляется помимо его воли[32]. В ст. 159^3 УК РФ признак выражен через мнимую возмездность, создаваемую обманом (потерпевший сам перечисляет средства, полагая, что получает товар или услугу, однако фактически никакого встречного исполнения не существует). В ст. 159^6 УК РФ безвозмездность обусловлена незаконным вмешательством в компьютерную информацию, позволяющим виновному распоряжаться средствами потерпевшего без его участия и, разумеется, без какого-либо имущественного эквивалента[33]. Таким образом, во всех трёх составах безвозмездность завладения усиливается дистанционным способом совершения преступления: имущество изымается удалённо, односторонне и

[32] Постановление Пленума Верховного Суда РФ от 16.06.2026 № 19 «О внесении изменений в постановление Пленума Верховного Суда Российской Федерации от 27 декабря 2002 года № 29 «О судебной практике по делам о краже, грабеже и разбое» [Электронный документ]. – URL: https://www.consultant.ru/document/cons_doc_LAW_537044/ (дата обращения: 29.06.2026).

[33] Энгельгардт А.А. О понимании мошенничества в сфере компьютерной информации // Вестник Московского университета МВД России. 2016. № 8. С. 84-90.

без предоставления потерпевшему какого-либо встречного блага, что является типичным признаком дистанционных хищений.

Признак обращения имущества в пользу виновного или третьих лиц при дистанционных хищениях проявляется в особенностях цифрового оборота денежных средств, где результат преступного деяния выражается в переводе безналичных или электронных денег под контроль лица, совершающего хищение, либо связанных с ним субъектов. Так, например, в п. «г» ч. 3 ст. 158 УК РФ изъятие безналичных или электронных денежных средств оканчивается их списанием со счета потерпевшего и поступлением на счет, который контролируется преступником или на транзитные электронные кошельки, используемые для последующего сокрытия настоящего происхождения денежных средств. В результате имущество непосредственно перемещается в сферу фактического распоряжения виновного, что свидетельствует об оконченности кражи в момент изменения учетной записи на стороне банка или оператора электронных платежей. Данный подход также корреспондирует с разъяснениями Постановления Пленума Верховного Суда РФ от 16 июня 2026 г. № 19, согласно которым хищение безналичных денежных средств признаётся оконченным с момента их списания со счёта потерпевшего, поскольку именно в этот момент происходит фактическое выбытие имущества из владения собственника и возникновение у виновного реальной возможности распоряжения похищенными средствами[34]. Тем самым судебная практика акцентирует внимание не на последующих действиях по обналичиванию или перемещению денежных средств, а на моменте изменения баланса на счёте как юридически значимом критерии окончания хищения. В ст. 159^3 УК РФ обращение имущества в пользу виновного или третьих лиц осуществляется посредством совершения потерпевшим операции с использованием

[34] Постановление Пленума Верховного Суда РФ от 16.06.2026 № 19 «О внесении изменений в постановление Пленума Верховного Суда Российской Федерации от 27 декабря 2002 года № 29 «О судебной практике по делам о краже, грабеже и разбое» [Электронный документ]. – URL: https://www.consultant.ru/document/cons_doc_LAW_537044/ (дата обращения: 29.06.2026).

электронного средства платежа, обусловленной обманом или злоупотреблением доверием. Специфика дистанционного совершения такого мошенничества заключается в том, что передача денежных средств осуществляется без непосредственного физического контакта между виновным и потерпевшим, а преступное воздействие реализуется посредством дистанционных каналов коммуникации и электронных средств платежа. При этом юридически значимым для квалификации является не сам факт цифрового характера операции, а использование электронного средства платежа в механизме завладения имуществом. В рамках действия ст. 159^6 УК РФ признак обращения имущества в пользу виновного или третьих лиц проявляется через результаты незаконного вмешательства в компьютерную информацию, обеспечивающую доступ к денежным средствам потерпевшего. При этом специфика данного состава заключается не просто в использовании цифровых средств, а в том, что завладение имуществом обусловлено неправомерным воздействием на компьютерную информацию. Вмешиваясь в функционирование программных средств или информационных систем (ввод, изменение, блокирование данных, вмешательство в работу сетей), злоумышленник получает техническую возможность самостоятельно инициировать перевод средств, изменить реквизиты операций, получить доступ к электронным кошелькам или банковским приложениям. В результате денежные средства зачисляются на счета, виртуальные кошельки или иные электронные ресурсы, контролируемые виновным или его соучастниками.

Таким образом, при внешнем сходстве результата хищения в виде перехода денежных средств в фактическое распоряжение виновного или третьих лиц механизм его достижения в рассматриваемых составах различается. При краже, предусмотренной п. «г» ч. 3 ст. 158 УК РФ, завладение осуществляется тайно и помимо воли потерпевшего, при мошенничестве, предусмотренном ст. 159^3 УК РФ, передача денежных средств осуществляется самим потерпевшим под воздействием обмана или

злоупотребления доверием с использованием электронного средства платежа, при мошенничестве в сфере компьютерной информации, предусмотренном ст. 159[6] УК РФ, завладение имуществом обусловлено неправомерным воздействием на компьютерную информацию. Такое разграничение имеет принципиальное значение для уголовно-правовой квалификации дистанционных хищений.

Признак причинения имущественного ущерба в дистанционных формах хищений проявляется в утрате потерпевшим возможности распоряжаться принадлежащими ему имущественными благами вследствие воздействия на цифровые инструменты управления имуществом. В п. «г» ч. 3 ст. 158 УК РФ ущерб выражается в фактическом уменьшении остатка безналичных или электронных денежных средств, списанных без согласия владельца, что исключает дальнейшее пользование ими и свидетельствует о реальном экономическом вреде. В ст. 159[3] УК РФ имущественный ущерб возникает как следствие совершённого под влиянием обмана или злоупотребления доверием перевода средств, после чего потерпевший утрачивает доступ к сумме, перемещённой на счета преступника либо третьих лиц. Ущерб здесь носит эквивалентный характер – электронное уменьшение баланса полностью соответствует экономической потере в материальной форме. В ст. 159[6] УК РФ ущерб обусловлен информационно-техническим вмешательством. Результатом противоправных действий становится списание средств, блокировка цифровых кошельков или изменение параметров учетных записей, что делает имущество недоступным владельцу. Нарушение целостности или доступности цифровой финансовой информации выступает непосредственным механизмом причинения вреда[35]. Так, во всех трёх нормах имущественный ущерб возникает в результате удалённого воздействия на цифровую инфраструктуру, управляющую доступом к денежным средствам. Уменьшение электронных балансов,

[35] Журавлева Г.В., Карпова Н.А. Мошенничество в сфере компьютерной информации: спорные вопросы теории и практики // Вестник Московского университета МВД России. 2017. № 5. С. 153-158.

списание средств или блокировка счетов лишают потерпевшего возможности распоряжаться имуществом, образуя реальный экономический вред. Дистанционный характер причинения ущерба подтверждает цифровую природу этих форм хищений[36].

Так, п. «г» ч. 3 ст. 158, ст. 159^3 и ст. 159^6 УК РФ в совокупности с иными характеристиками указанных деяний позволяет выделить следующие ключевые признаки дистанционных хищений:

– корыстная цель (стремление виновного к безвозмездному извлечению имущественной выгоды за счёт другого лица, достигаемое посредством манипулирования сознанием потерпевшего, эксплуатации цифровой инфраструктуры и использования технологических уязвимостей финансовых и платёжных систем);

– противоправное изъятие (нарушение законного режима владения, пользования и распоряжения имуществом потерпевшего, выраженное в списании безналичных средств, переводе электронных денежных средств или установлении контроля над цифровыми активами без физического доступа к ним);

– безвозмездность (отсутствие реального встречного имущественного предоставления, в ст. 159^3 УК РФ, например, маскируемое мнимой возмездностью обманных операций, в ст. 159^6 УК РФ – скрытым вмешательством в компьютерную информацию и цифровые механизмы распоряжения имуществом);

– обращение чужого имущества в пользу виновного или третьих лиц (поступление денежных средств, электронных средств или прав на распоряжение ими на счета, электронные кошельки и иные цифровые ресурсы, контролируемые преступником или его соучастниками);

[36] Шумихин В.Г. Седьмая форма хищения чужого имущества // Вестник Пермского университета. Юридические науки. 2014. № 2 (24). С. 229-233.

– причинение имущественного ущерба (фактическая утрата потерпевшим денежных средств, прав на их использование либо доступа к электронным активам, лишение возможности распоряжаться ими);

– особый предмет преступления (безналичные денежные средства и электронные деньги как имущественные права, электронные средства платежа как инструменты распоряжения денежными средствами, компьютерная информация как средство получения доступа к чужому имуществу, обладающая самостоятельной экономической значимостью);

– особый способ совершения преступления (опосредованное воздействие на имущественные права через электронные средства платежа, информационно-телекоммуникационные сети и цифровые системы, включая обман, злоупотребление доверием и вмешательство в работу компьютерной информации, позволяющее дистанционно и без физического контакта завладеть имуществом).

В результате выявленные особенности трансформации отдельных признаков таких деяний не свидетельствуют об изменении юридической природы хищения как уголовно-правового явления. И именно сочетание традиционной природы хищения и новых технологических механизмов совершения преступления позволяет рассматривать дистанционные хищения как самостоятельную научную категорию, требующую доктринального осмысления в рамках уголовно-правового и криминологического анализа.

В свою очередь, определение признаков дистанционных хищений позволяет перейти к комплексной оценке их общественной опасности, которая носит не только имущественно-ущербный, но и системно-угрожающий характер для цифровой экономики и финансовой безопасности государства. При этом в целом общественная опасность данных деяний определяется совокупностью взаимосвязанных факторов, каждый из которых в условиях цифровой среды приобретает качественно усиленное значение.

Во-первых, дистанционные хищения характеризуются высокой распространённостью и устойчивой тенденцией к росту. Так, по данным

МВД России, в 2024 г. около 40% всех зарегистрированных преступлений были совершены с использованием информационно-телекоммуникационных технологий. При этом количество IT-преступлений увеличилось на 13,1% по сравнению с предыдущим годом[37]. Особую значимость приобретает тот факт, что значительная их часть приходится именно на хищения денежных средств и мошенничества, а общий ущерб от таких деяний в 2024 г. достиг порядка 200 млрд рублей (для сравнения, в 2023 г. этот показатель составлял около 147 млрд рублей), что свидетельствует о резком росте экономических потерь населения и бизнеса[38].

Во-вторых, важным фактором общественной опасности дистанционных хищений выступает их высокая масштабируемость, обусловленная особенностями цифровой среды и возможностью многократного воспроизведения преступных сценариев. В отличие от традиционных форм хищения, при которых увеличение числа потерпевших, как правило, требует совершения отдельных действий в отношении каждого объекта посягательства, дистанционные хищения позволяют использовать единый технологический механизм для воздействия на широкий круг лиц. Так, создание фишингового ресурса, использование вредоносного программного обеспечения, организация массовых SMS- и голосовых рассылок либо применение автоматизированных инструментов социальной инженерии позволяют преступникам одновременно обращаться к значительному числу потенциальных потерпевших[39]. В результате масштабируемость дистанционных хищений проявляется в способности преступника расширять количество объектов посягательства без соразмерного увеличения временных, организационных и материальных

[37] 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).
[38] В МВД оценили ущерб от дистанционных хищений [Электронный ресурс]. – URL: https://ria.ru/20251211/uscherb-2061537107.html (дата обращения: 09.02.2026).
[39] Россияне перевели мошенникам 168 млрд руб. за 11 месяцев 2024 года [Электронный ресурс]. – URL: https://www.kommersant.ru/doc/7421098 (дата обращения: 09.02.2026).

затрат, что качественно отличает их от традиционных форм хищений и повышает степень их общественной опасности.

В-третьих, дистанционные хищения характеризуются высоким уровнем анонимности и латентности. Цифровая среда позволяет преступникам использовать подмену идентификаторов, VPN-сервисы, криптовалютные транзакции, цепочки промежуточных счетов («дроппов») и другие инструменты, что существенно затрудняет установление личности виновного и конечного выгодоприобретателя. На высокий уровень латентности цифровых преступлений указывают и экспертные оценки. Так, по мнению Э.Л. Сидоренко, высказанному на I Международном научно-практическом форуме «Право цифровой безопасности» в МГИМО РФ в 2024 г., количество латентных преступлений в данной сфере по самым скромным подсчётам превышает 60% от числа зарегистрированных деяний[40]. Указанные обстоятельства позволяют сделать вывод, что статистика зарегистрированных дистанционных хищений отражает лишь часть реально существующих преступных посягательств, а фактический масштаб распространения данной разновидности преступности является значительно выше. В итоге сочетание анонимности цифровой среды и высокой латентности дистанционных хищений существенно затрудняет их выявление, расследование и предупреждение, что также повышает общественную опасность рассматриваемых деяний.

Кроме того, повышенная общественная опасность обусловлена трансграничным характером дистанционных хищений, определяемым особенностью функционирования цифровой среды. Общеизвестно, что современные цифровые технологии позволяют осуществлять преступные действия вне зависимости от государственной юрисдикции, используя зарубежные серверы, иностранные платёжные системы и инфраструктуру анонимных сетей. Это приводит к «размыванию» территориального признака

[40] Латентность киберпреступности превысила 60% [Электронный ресурс]. – URL: https://rapsinews.ru/digital_law_news/20240424/309839280.html (дата обращения: 29.06.2026).

преступления и объективно снижает эффективность национальных механизмов уголовного преследования, поскольку установление всех звеньев преступной цепи требует международного взаимодействия, которое не всегда является оперативным и эффективным.

Также важнейшей характеристикой является высокая степень автоматизации преступной деятельности. В отличие от традиционных форм хищений, дистанционные посягательства могут осуществляться с использованием программных средств, позволяющих автоматически генерировать атаки, подбирать пароли, рассылать сообщения или осуществлять фишинговые операции[41]. Это снижает «порог входа» в преступную деятельность и делает возможным совершение хищений лицами, обладающими минимальными техническими навыками, что расширяет криминогенную базу.

И, наконец, особое значение для оценки общественной опасности дистанционных хищений приобретает сложность их выявления и доказывания. Цифровая природа рассматриваемых преступлений обусловливает специфику формирования доказательственной базы. Следы преступной деятельности зачастую имеют нематериальный характер, могут быть распределены между различными информационными системами, изменяться или утрачиваться, а их получение нередко зависит от взаимодействия с банками, операторами связи, владельцами цифровых платформ и иными субъектами, располагающими необходимой информацией Сложность такого процесса подтверждается и развитием специальных механизмов государственного реагирования.

Так, создание государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационно-коммуникационных технологий, предусмотренной Федеральным законом от 1 апреля 2025 г. № 41-ФЗ, направлено, в том

[41] Обзор операций, совершённых без добровольного согласия клиентов финансовых организаций за 2024 год [Электронный ресурс]. – URL: https://cbr.ru/analytics/ib/operations_survey/2024/ (дата обращения: 29.06.2026).

числе, на обеспечение оперативного взаимодействия между правоохранительными органами, кредитными организациями и иными субъектами цифровой инфраструктуры при выявлении и пресечении таких деяний[42]. Необходимость внедрения указанного механизма свидетельствует о том, что расследование дистанционных хищений требует объединения разрозненных цифровых данных и межведомственного обмена информацией, поскольку традиционные способы фиксации и получения доказательств не всегда позволяют эффективно установить обстоятельства совершённого преступления.

Кроме того, указанные особенности находят отражение в показателях работы правоохранительных органов. Так, по итогам 2025 г. в Российской Федерации зарегистрировано 675,4 тыс. преступлений, совершённых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации (большая часть из которых – дистанционные хищения). При этом количество нераскрытых преступлений данной категории составило 494,3 тыс. деяний, то есть значительная часть зарегистрированных преступлений осталась без установленного лица, их совершившего[43]. В результате, несмотря на некоторое улучшение показателей раскрываемости по сравнению с предыдущими периодами, сохраняющийся значительный объём нераскрытых IT-преступлений свидетельствует о наличии объективных трудностей, связанных с установлением виновных лиц, закреплением цифровых доказательств и восстановлением полной картины преступного события. При этом в целом статистика совершения указанных деяний также свидетельствует о повышенной общественной опасности данных деяний (см. рис. 1.).

[42] Федеральный закон от 01.04.2025 № 41-ФЗ (ред. от 31.07.2025) «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации» [Электронный документ]. – URL: https://www.consultant.ru/document/cons_doc_LA (дата обращения: 01.07.2026).

[43] Число IT-преступлений в России в 2025 году сократилось до 675 тыс. [Электронный ресурс]. – URL: https://tass.ru/obschestvo/26385451 (дата обращения: 29.06.2026).

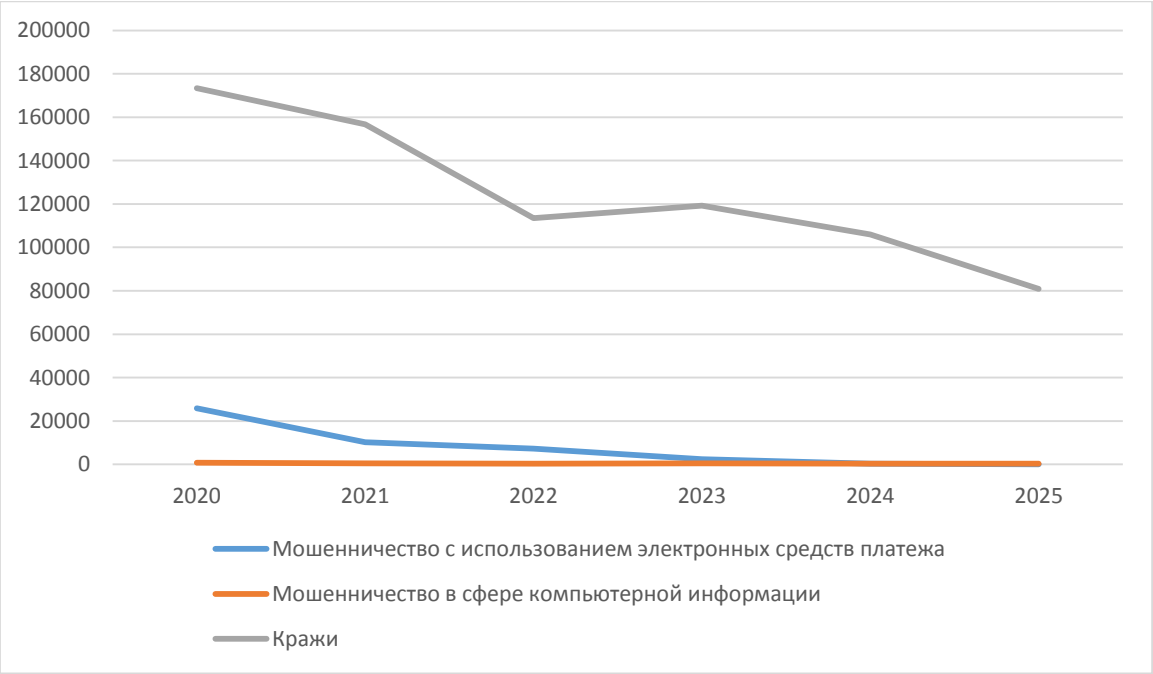


Рисунок 1. Хищения, совершённые с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации в Российской Федерации в 2020–2025 гг.[44]

Анализ представленных статистических данных за 2020–2025 гг. осуществлён в отношении составов преступлений, наиболее репрезентативно отражающих дистанционные хищения в цифровой среде. При этом количественная оценка дистанционных хищений, квалифицированных по общей норме ст. 159 УК РФ, на основании официальных статистических данных не приведена, поскольку представляется не совсем корректной для целей настоящего исследования. Как указывалось ранее, статистическая отчётность МВД России учитывает преступления по иным классификационным основаниям и не выделяет дистанционные хищения как самостоятельную категорию, в связи с чем показатели преступлений, совершённых с использованием информационно-телекоммуникационных технологий, не могут быть непосредственно отождествлены с количеством дистанционных хищений. Соответственно данные о преступлениях, квалифицированных по ст. 159 УК РФ, не позволяют отделить

[44] Состояние преступности в РФ [Электронный ресурс]. – URL: https://мвд.рф/ (дата обращения: 09.05.2026).

дистанционные формы мошенничества от иных деяний, предусмотренных данной статьёй. В связи с этим показатели по ст. 159 УК РФ не используются в настоящем параграфе в качестве самостоятельного количественного показателя распространённости дистанционных хищений.

В целом за рассматриваемый период в структуре цифровой преступности, общий объём которой составляет 510 366 таких преступлений в 2020 г., 517 722 – в 2021 г., 522 065 – в 2022 г., 676 951 – в 2023 г., 765 365 – в 2024 г. и 675 372 – в 2025 г.[45], прослеживается неоднородная динамика с выраженным ростом до 2024 г. и последующей коррекцией показателей в 2025 г., что свидетельствует о расширении «цифрового сегмента» преступности при сохранении его высокой волатильности. На этом фоне динамика исследуемых составов демонстрирует существенные структурные различия.

Мошенничество с использованием электронных средств платежа сокращается с 25 820 случаев в 2020 г. (около 5,06% общего массива цифровой преступности) до 99 в 2025 г. (менее 0,02%). Столь резкое изменение показателя не может быть однозначно интерпретировано как фактическое многократное сокращение соответствующего способа дистанционного хищения. Оно обусловлено в том числе изменением подходов к уголовно-правовой квалификации соответствующих деяний и разграничению составов мошенничества, что отражается на их статистическом учёте (данные вопросы подробно рассмотрены в § 2.1 настоящего исследования). Поэтому приведённые показатели следует оценивать с учётом изменений в правоприменительной практике, а не как прямое отражение динамики фактической распространённости данного способа хищения.

Мошенничество в сфере компьютерной информации характеризуется относительной стабильностью с незначительными колебаниями (761 в 2020 г. –

[45] Состояние преступности в РФ [Электронный ресурс]. – URL: https://мвд.рф/ (дата обращения: 09.05.2026).

около 0,15%; 319, в 2025 г. – около 0,05%), что свидетельствует о его устойчивом характере в структуре цифровых преступлений.

Кражи сохраняют доминирующее положение, оставаясь наиболее массовой категорией (173 416 случаев в 2020 г. (около 33,98%) и 80 956 в 2025 г. (около 11,99%)), несмотря на общее снижение абсолютных значений.

Соотношение краж и мошенничеств в анализируемый период указывает на устойчивое количественное преобладание краж, при одновременном усложнении и диверсификации дистанционных мошенничеств. При этом наблюдается постепенное смещение криминальной активности в сторону более технологически сложных и латентных способов совершения хищений, связанных с использованием информационно-коммуникационных технологий. Так, структура по способам совершения преступлений отражает трансформацию цифровой преступности в целом. Общий анализ представленных статистических данных за 2020–2025 гг. в отношении исследуемых составов преступлений, позволяет констатировать наличие устойчивых трансформационных процессов в структуре цифровой имущественной преступности, выражающихся как в изменении количественных показателей, так и в перераспределении способов совершения посягательств.

Общественная опасность дистанционных хищений обусловлена сочетанием нескольких обстоятельств. К их числу относятся возможность совершения значительного числа посягательств при относительно небольших затратах со стороны виновных, использование дистанционных способов взаимодействия, затрудняющих установление личности преступника, перемещение похищенных средств через несколько платёжных инструментов и территорий, а также применение автоматизированных средств при подготовке и совершении преступлений. Эти особенности объективно осложняют выявление преступлений, установление всех участников и восстановление последовательности действий, приведших к завладению

имуществом. При этом последствия дистанционных хищений не ограничиваются имущественными потерями отдельных лиц. Массовое совершение подобных преступлений способно снижать доверие участников экономического оборота к используемым способам дистанционного взаимодействия и создавать дополнительные риски для организаций, обеспечивающих проведение платежей и передачу информации. В результате общественная опасность дистанционных хищений определяется не каким-либо одним признаком, а сочетанием способа совершения преступления, характера взаимодействия виновного с потерпевшим, особенностей перемещения похищенного имущества и возникающих при этом трудностей правоприменения.

Таким образом, термин «дистанционное хищение» наиболее полно отражает сущность исследуемой категории. В отличие от других используемых в научной литературе понятий, он не ограничивается конкретной технологической средой либо отдельным способом совершения преступления, а фиксирует ключевой уголовно-правовой признак рассматриваемых деяний – отсутствие непосредственного физического воздействия виновного на предмет хищения либо непосредственного очного контакта с потерпевшим при использовании цифровой инфраструктуры. В то же время благодаря своей технологической нейтральности указанная категория сохраняет актуальность независимо от дальнейшего развития информационно-коммуникационных технологий и позволяет объединить различные способы совершения имущественных посягательств в рамках единой научной конструкции. С учётом выявленных признаков рассматриваемой разновидности преступной деятельности дистанционное хищение следует определить как современную форму реализации классического 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 доступа. В результате юридическая природа дистанционного хищения определяется сохранением классической уголовно-правовой конструкции хищения при изменении механизма её реализации в цифровой среде.

1.2. Формы и способы хищений, совершаемых дистанционно

В уголовно-правовой доктрине понятия формы и способа хищения не являются тождественными. Их разграничение имеет значение для определения места дистанционного способа совершения преступления в общей системе хищений. Традиционно к формам «классических» хищений, согласно устоявшейся в уголовно-правовой науке точке зрения, относят разбой, грабёж, присвоение, растрату, кражу и мошенничество, что закреплено в действующем уголовном законодательстве РФ. Но в дистанционном формате не все из перечисленных форм хищений возможны. Так, например, разбой и грабёж предполагают наличие непосредственного контакта преступника и пострадавшего, что определяется объективной стороной данных составов преступлений. В первом случае это объясняется необходимостью применения насилия, опасного для жизни или здоровья, либо угрозы применения такого насилия, что априори невозможно без личного контакта преступника и потерпевшего, а во втором – совершением хищения в присутствии собственника или иного владельца имущества либо на виду у посторонних, когда лицо, совершающее это преступление, сознаёт, что присутствующие при этом лица понимают противоправность данных действий, что также исключает возможность совершения такого преступления на удалении. Присвоение и растрату, в свою очередь,

затруднительно совершить в дистанционной форме, поскольку под данным противоправным деянием понимают хищение чужого имущества, вверенного виновному, или, иначе говоря, незаконное безвозмездное обращение в свою собственность или в собственность иного лица имущества, которое находится в правомерном владении виновного, который ввиду должностных обязанностей, специального поручения или договорных отношений осуществлял в отношении данного имущества правомочия по управлению, распоряжению, хранению или доставке, что также обусловливает наличие прямого контакта собственника (потерпевшего) и преступника.

В результате в рамках дистанционного хищения как криминологической категории релевантными остаются лишь две формы – кража и мошенничество, поскольку именно они допускают опосредованное изъятие имущества без физического контакта между субъектами. При этом для каждой из этих форм хищений, совершаемых в том числе в дистанционном формате, характерны собственные способы совершения преступных деяний.

С точки зрения уголовного закона дистанционная кража описывается п. «г» ч. 2 ст. 158 УК РФ (кража с банковского счета, а равно в отношении электронных денежных средств), не исключая возможность привлечения к уголовной ответственности по основному составу преступления – ст. 158 УК РФ – в случае отсутствия соответствующего квалифицирующего признака, но наличия использования различных дистанционных технологий при совершении кражи[46]. При этом отдельно необходимо подчеркнуть, что данная категория преступлений является достаточно распространённой. Так, каждая пятая кража, по данным Генеральной прокуратуры РФ, в настоящее время связана именно с тайными хищениями с банковского счёта[47].

Оценивая способы совершения дистанционных краж, укажем, что в настоящее время совершение дистанционных краж возможно: посредством

[46] Клепицкий И.А. Новое экономическое уголовное право. М.: Проспект, 2021. С. 125.
[47] Байбарин А.А., Садчикова Д.Н. Кража безналичных и электронных денег: об актуальных проблемах правоприменения // Вестник Сургутского государственного университета. 2022. № 1 (35). С. 60-68.

получения доступа к учётным записям, аккаунтам, личным кабинетам и т.п. жертвы (без совершения обманных действий) с целью дальнейшего использования конфиденциальной информации для совершения тайного хищения чужого имущества или посредством осуществления различных манипуляций с самими платёжными системами, применения соответствующих информационных технологий и т.п. В первом случае преступник получает сам «ключ» доступа к чужому имуществу (чаще всего к безналичным денежным средствам), а во втором – ломает «информационный кодовый замок», обеспечивая себе тем самым такой же противоправный доступ к чужому имуществу. Или, другими словами, в данных случаях преступники придерживаются разных «схем» криминального воздействия: в первом – «преступник-жертва», где лицо осуществляет непосредственное воздействие на жертву и получает доступ к чужому имуществу, а во втором – «преступник-техника», где осуществляется воздействие на средства хранения, передачи и обработки соответствующей информации, также позволяющее получить доступ к чужому имуществу[48]. В результате определяющим критерием для разграничения указанных способов является направленность преступного воздействия.

В качестве примера, характеризуя первый способ совершения преступления, приведём дело о тайном хищении гражданином М. с банковского счёта с причинением значительного ущерба потерпевшему 40 тыс. рублей (Приговор № 1-203/2024 1-661/2023 от 28 февраля 2024 г. по делу № 1-203/2024, А. городской суд (Нижегородская область)). Согласно материалам следствия, некто гражданин М. в местном магазине в кассовой зоне обнаружил листок белой бумаги с цифровым кодом от банковской карты и саму карту, оформленную на имя потерпевшей. Осознавая противоправность осуществляемого деяния и возможность вернуть карту с цифровым кодом владельцу, гражданин М. решил обогатиться за счёт

[48] Старостенко О.А. Криминологическая характеристика и основные параметры виктимологического предупреждения дистанционных хищений // Вестник КРУ МВД России. 2022. № 4 (58). С. 22-27.

указанной карты и, реализуя преступный умысел, положил находку в карман куртки, а затем снял в банкомате, используя обнаруженный на бумаге цифровой код, денежные средства в размере 40 тыс. рублей и распорядился ими по своему усмотрению, за что был осуждён приговором А. городского суда по п. «г » ч. 3 ст. 158 УК РФ к лишению свободы на срок 2,5 года[49].

Как видно, приведённый пример относится к первому способу совершения дистанционной кражи, поскольку преступник получил возможность распоряжения денежными средствами не посредством вмешательства в функционирование информационной системы или изменения её параметров, а путём незаконного завладения сведениями, обеспечивающими доступ к имуществу потерпевшего. Иными словами, предметом непосредственного преступного воздействия в данном случае выступала информация, выполняющая роль «ключа доступа» к банковскому счёту, использование которой позволило виновному осуществить тайное изъятие денежных средств. При этом цифровая среда была использована исключительно как средство реализации уже полученного доступа к имуществу, а не как объект технического воздействия. Именно данный критерий позволяет отграничить указанный способ совершения дистанционной кражи от случаев, когда завладение денежными средствами достигается посредством воздействия на информационные системы и механизмы обработки цифровых данных.

Следующий способ совершения дистанционных краж – это кражи, совершаемые по схеме «преступник-техника», посредством осуществления различных манипуляций с самими платёжными системами, применения соответствующих информационных технологий и т.п. Как уже указывалось ранее, в данном случае «ключа», позволяющего получить прямой доступ к чужому имуществу у преступника нет, поэтому «замок», охраняющий это имуществе в виде разнообразных защитных информационных систем

[49] Приговор № 1-203/2024 1-661/2023 от 28 февраля 2024 г. по делу № 1-203/2024, А. городской суд (Нижегородская область) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/iSu7Y2LER5lo/ (дата обращения: 25.02.2026).

технического характера, преступнику приходится целенаправленно «вскрывать», например, перехватывая, необходимую конфиденциальную информацию, что в значительной мере влияет на специфику совершения преступлений такого рода. Среди схем совершения подобных преступлений современные исследователи выделяют скримминг и шимминг (процесс незаконного завладения информацией, которая содержится на магнитной полосе кредитной карты с целью совершения дистанционной кражи), снифферинг (направленный на перехват данных с помощью анализатора проходящего трафика сети) и некоторые другие[50].

В качестве примера совершения таких преступлений приведём дело о хищении денежных средств с банковских счетов граждан-пользователей сети Интернет через получение доступа к конфиденциальной информации о банковской карте жертвы посредством использования фишинговых ссылок, формируемых специальным программным обеспечением. В материалах следствия представлено, что преступник находил потенциальных жертв на сайте объявлений «Авито». Используя виртуальный абонентский номер, с целью конспирации гражданин Н. зарегистрировал аккаунт в мессенджере, затем, следуя обнаруженной в сети Интернет инструкции о совершении преступления таким способом, создавая видимость покупателя, прислал на абонентский номер пострадавшего специально сгенерированную ссылку, якобы необходимую для оформления курьерской доставки. Однако после перехода по этой ссылке пострадавший передал преступнику конфиденциальную информацию о собственной банковской карте, используя которую гражданин Н. похитил имеющиеся на ней денежные средства, «сломав», тем самым, «кодовый замок», защищающий финансы, хранящиеся на расчётном счёте данного клиента банка[51]. Или другой пример – использование для реализации преступного умысла, направленного на тайное

[50] Рябинина Т.К., Ряполова Я.П., Чистилина Д.О. Актуальные проблемы выявления и расследования дистанционных хищений с банковского счета // Вестник БелЮИ МВД России. 2023. № 4. С. 31-38.
[51] Приговор № 1-137/2023 от 12 октября 2023 г. по делу № 1-137/2023, О. районный суд г. Иваново (Ивановская область) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/tijN7saagGZ0/ (дата обращения: 27.02.2026).

хищение денежных средств в дистанционной форме, специального интернет-бота, позволяющего создавать фишинговые веб-страницы и похищать, таким образом, денежные средства удалённо у неопределённого круга лиц[52].

Как видим, приведённые примеры относятся ко второму способу совершения дистанционных краж, при котором преступник не обладает непосредственным доступом к конфиденциальной информации потерпевшего и не получает её напрямую от владельца, а осуществляет целенаправленное воздействие на цифровую инфраструктуру и механизмы защиты платежных систем. В отличие от первого способа здесь предметом непосредственного преступного воздействия выступают не сведения как таковые, а технические средства их передачи, обработки и защиты, что выражается в перехвате, подмене либо незаконном получении данных с использованием фишинговых технологий, скримминга, снифферинга и иных программно-технических методов. Следовательно, данный способ характеризуется активным «взломом» информационно-технологической среды («преступник–техника») и направлен на преодоление цифровых барьеров доступа к имуществу, что позволяет отграничить его от иных форм дистанционных хищений, основанных на добровольной передаче либо непосредственном завладении данными доступа.

Следующая форма хищений, совершаемых дистанционно, это дистанционные мошенничества – наиболее распространённая и активно развивающаяся в современности разновидность киберпреступлений корыстной направленности, видовое разнообразие которых определяется способами совершения преступления, отличающимися друг от друга механизмами воздействия на пострадавших.

Отдельно укажем, что мошенничество само по себе в «классическом» уголовно-правовом понимании включает себя эмоционально-волевой компонент непосредственного воздействия на жертву. Это означает, что

[52] См., например: Приговор № 1-617/2023 от 5 сентября 2023 г. по делу № 1-617/2023, С. городской суд (Республика Коми) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/e82eh3iuUxbK/ (дата обращения: 28.02.2026).

действия обманного характера нацелены именно на личность жертвы, её сознание, мышление, психику, эмоции и т.п. В Постановлении Пленума Верховного Суда РФ от 30.11.2017 № 48 (с изм. и доп.) «О судебной практике по делам о мошенничестве, присвоении и растрате» указано, что обман состоит в сознательном сообщении (представлении) заведомо ложных сведений, не соответствующих действительности, либо же в умолчании об истинных фактах или в умышленных действиях, которые направленны на введение в заблуждение владельца имущества или другого лица. Злоупотреблением доверия признаётся использование с корыстной целью доверительных отношений с владельцем имущества или другим лицом, которое уполномочено принимать решения о передаче данного имущества третьим лицам[53]. Как видим, сознательное сообщение, предоставление заведомо ложных сведений, умалчивание истинных фактов, умышленные действия, направленные на введение в заблуждение, ориентированы именно на личность жертвы.

Развивая данную мысль, укажем, что исследователь В.В. Хилюта, характеризуя сущность мошеннических действий, также отмечает, что мошеннический обман имеет цель введения в заблуждение потерпевшего, и для достижения этой цели преступник стремится фальсифицировать его волю так, чтобы сформировать у жертвы преступления поведение, направленное на передачу имущества виновному. Так, по справедливым оценкам учёного, обман – это интеллектуальное, информационное воздействие одного лица на психику другого, и он возникает только в том случае, если присутствует ситуация психологической оценки[54]. Идентичный механизм действия присутствует при осуществлении злоупотребления доверия для совершения мошеннических действий. Однако в случае с дистанционным мошенничеством это интеллектуально-волевое воздействие

[53] Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 (ред. от 15.12.2022) «О судебной практике по делам о мошенничестве, присвоении и растрате» [Электронный документ]. – URL: https://www.consultant.ru/document/cons_doc_LAW_283918/ (дата обращения: 02.03.2026).

[54] Хилюта В.В. Признаки мошеннического обмана в теории и практике уголовного закона // Всероссийский криминологический журнал. 2009. № 2. С. 13-21.

не всегда связано с той или иной личностью, и преступник нередко обманывает не конкретное лицо, а программное обеспечение или другими словами – технику, что обусловлено спецификой среды, в которой совершаются такие мошеннические действия. В связи с этим возникает логичный вопрос: а можно ли в принципе обмануть технику? И будет ли это являться мошенничеством в традиционном уголовно-правовом понимании?

Отвечая на данные вопросы, отметим, что вопреки устоявшемуся мнению, в результате осуществления подобных действий обман всё же имеет место, однако он не «активный» (далее будем придерживаться указанной терминологии, используемой не в «классическом» уголовно-правовом, а криминологическом смысле), а, скорее, технически опосредованный, поскольку жертва преступления ввиду посредственных знаний о функционировании цифровой среды (а никакими другими знаниями лицо и не должно обладать) не в состоянии обнаружить преступный умысел в совершаемых деяниях, вследствие чего злоумышленник реализует криминальную схему. В подтверждение верности заданного предположения отметим, что представленная точка зрения находит подтверждение в научной литературе. Так, например, А.А. Энгельгарт верно отмечает, что для дистанционных мошенничеств обман человека и передача имущества или приобретение права на чужое имущество с помощью потерпевшего не характерны, поскольку воздействие в данном случае осуществляется на компьютер[55]. Н.Л. Коликов замечает, что нередко компьютерное мошенничество в отношении предпринимателей совершается посредством применения результатов автоматизированной обработки данных сети Интернет, и такие действия в России чаще всего квалифицируются по совокупности ст. 159 и ст. 272 УК РФ. Однако в данном случае об «истинном» мошенничестве, по утверждению исследователя, можно говорить с некоторой долей условности, поскольку неотъемлемым волевым

[55] Энгельгардт А.А. Вопросы квалификации мошенничества в сфере компьютерной информации // Право. Журнал Высшей школы экономики. 2016. № 4. С. 86-94.

признаком любой разновидности мошенничества (по основному составу) является добровольность потерпевшего в осуществлении передачи виновному имущества или права на имущество под влиянием злоупотребления доверием или обмана. Однако в результате различных манипуляций с компьютерными данными указанный признак отсутствует, ведь виновный совершает обман не конкретного лица (владелец имущества может и не знать о совершающихся преступных действиях), а компьютерной системы. Хотя и в этом случае обман (а значит мошеннические действия) присутствует[56]. Также отдельные учёные справедливо подчёркивают, что, когда речь идёт о мошенничестве в сфере компьютерной информации (одного из распространённых хищений, совершаемых дистанционно), имеет место быть обман технического устройства, что находится за гранью понимания психологии, в то время как «классический» обман или злоупотребление доверием является исключительно психологическим явлением (воздействием)[57]. Так, несмотря не некую противоречивость отнесения описываемых преступных деяний именно к мошенническим действиям, стоит отметить, что обман или злоупотребление доверием в данном случае также обнаруживается, хотя и в несколько нетипичном виде, вследствие чего правоприменители справедливо относят данные деяния именно к мошенничеству (хотя это понимание несколько разнится с устоявшейся в уголовном праве точкой зрения, а равно и в определениях высшей судебной инстанции РФ).

В результате это можно заключить, что, когда преступное воздействие при осуществлении мошеннических действий осуществляется по линии «преступник-техника», имеет место технически опосредованный обман потерпевшего – владельца имущества, являющегося предметом преступления, а когда это преступное воздействие осуществляется

[56] Коликов Н.Л. Профессиональная компьютерная преступность и мошенничество // Вестник ЮУрГУ. Серия: Право. 2011. № 40 (257). С. 61-64.
[57] Самиулина Я.В. Мошенничество в сфере компьютерной информации: проблемы законодательной регламентации // Вестник Самарского юридического института. 2023. № 3 (54). С. 62-65.

непосредственно на конкретное лицо с применением дистанционных информационно-телекоммуникационных технологий и технологий социальной инженерии, то данные преступные деяния можно оценивать, как активный обман или злоупотребление доверием.

В связи с этим логичным при разработке способов совершения дистанционного мошенничества считаем необходимым разделение всех разновидностей исследуемых мошеннических действий на две большие группы: дистанционные хищения посредством персонализированного обмана потерпевшего, либо посредством технически опосредованного воздействия на цифровую среду, когда ошибочное волеизъявление потерпевшего формируется не непосредственным убеждением, а созданием ложной информационной ситуации.

К дистанционным мошенничествам путем технологически опосредованного обмана, основываясь на данных современных исследований в указанной сфере, следует отнести: мошенничества с использованием вредоносного программного обеспечения (фрод), при котором на устройство потерпевшего устанавливаются программы, имитирующие интерфейсы банковских сервисов и запрашивающие ввод логинов, паролей и кодов подтверждения; использование поддельных мобильных приложений, визуально идентичных официальным, формирующих ложные уведомления о необходимости срочной авторизации; атаки с нарушением работы сервисов («отказ в обслуживании»), вынуждающие пользователя повторно вводить данные на подложных ресурсах; траппинг, при котором с помощью технического устройства, удерживающего банковскую карту в банкомате, создаётся ситуация, в которой потерпевший оставляет карту, полагая её неисправной, после чего преступник получает доступ к денежным средствами другие[58].

[58] Алёхин А.А. Теоретические аспекты кибермошенничества: понятие, правовая природа и виды // Государственная служба и кадры. 2024. № 2. С. 17-20; Рябинина Т.К., Ряполова Я.П., Чистилина Д.О. Актуальные проблемы выявления и расследования дистанционных хищений с банковского счета // Вестник Белгородского юридического института МВД России имени И.Д. Путилина. 2023. № 4. С. 31–38.

В обобщённом виде способы совершения таких дистанционных мошенничеств могут быть определены следующим образом:

– информационно-технологические, выражающиеся в непосредственном воздействии на программное обеспечение и информационные системы (внедрение вредоносного программного обеспечения, программных модулей, поддельных приложений, имитирующих банковские сервисы, в результате чего потерпевший самостоятельно вводит идентификационные и платёжные данные, обеспечивая доступ к своим средствам);

– эксплуатационно-инфраструктурные, связанные с неправомерным использованием функциональных и организационно-технических особенностей банковских, платёжных и иных цифровых сервисов без изменения программного кода (использование уязвимостей процедур авторизации, особенностей обработки транзакций и механизмов дистанционного доступа к счетам для последующего неправомерного распоряжения имуществом);

– системно-дестабилизирующие, предполагающие создание искусственных условий нарушения нормального функционирования цифровых сервисов (перегрузка систем, временное ограничение доступа к ресурсам, блокирование операций), при которых потерпевший вынужденно осуществляет действия в контролируемой злоумышленником цифровой среде;

– комбинированные, включающие сочетание указанных механизмов цифрового воздействия.

Предложенная классификация может быть проиллюстрирована материалами судебной практики. Показательным является уголовное дело, рассмотренное в Кемеровской области, по которому в 2016 г. группа лиц по предварительному сговору совершила несколько эпизодов мошенничества в отношении неопределённого круга потерпевших. Для получения доступа к возможностям банковского обслуживания и услугам оператора связи

использовалась вредоносная компьютерная программа, автоматически устанавливавшаяся на мобильное устройство под управлением операционной системы Android после перехода пользователя по соответствующей ссылке. Общая сумма причинённого потерпевшим ущерба составила 299 117,33 рубля. Действия виновных были квалифицированы по ч. 2 ст. 159.6 и ч. 2 ст. 273 УК РФ[59].

Рассматриваемый пример относится к информационно-технологическому способу совершения дистанционного хищения. В данном случае вредоносное программное обеспечение использовалось не как вспомогательное средство, а непосредственно обеспечивало реализацию преступного замысла. После его установки виновные получали возможность воздействовать на используемые потерпевшими сервисы и совершать действия, направленные на завладение денежными средствами. Следовательно, информационная технология в описанном механизме выполняла непосредственную функцию реализации преступного посягательства, что и позволяет отнести данный способ к соответствующей группе предложенной классификации

Другой пример – дело о хищении с сентября по ноябрь 2018 г. во Владимирской области группой лиц по предварительному сговору денежных средств юридических лиц с их банковских счетов посредством распространения и использования специальных вредоносных компьютерных программ. Преступный умысел лиц, состоящих в сговоре, предполагал распространение в сети Интернет специальных компьютерных программ с целью несанкционированного блокирования, копирования, модификации компьютерной информации, а равно и нейтрализации средств защиты такой информации для дальнейшей организации хищения денежных средств через получение с помощью таких вредоносных программ неправомерного доступа

[59] Приговор № 1-573/2020 от 8 сентября 2020 г. по делу № 1-573/2020, Ц. районный суд г. Кемерово (Кемеровская область) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/x4yF5QuhexHV/ (дата обращения: 03.03.2026).

к персональным компьютерам работников коммерческих организаций[60]. Данное деяние также может быть отнесено к информационно-технологическим способам, однако с выраженными элементами эксплуатационно-инфраструктурного воздействия, поскольку преступный результат достигался не только за счёт внедрения вредоносного программного обеспечения, но и посредством его использования для нарушения функционирования информационных систем организаций и обхода средств защиты информации. В результате здесь имеет место комбинированное воздействие на цифровую инфраструктуру, включая как программный, так и организационно-технический уровень.

Рассмотренные примеры подтверждают, что предложенная классификация способов дистанционных хищений (а именно мошенничеств посредством технологически опосредованного обмана) носит условный характер и в практической плоскости нередко проявляется в смешанных формах. При этом ключевым критерием разграничения, как указывалось ранее, остаётся характер технического воздействия на информационные системы, который может варьироваться от точечного внедрения вредоносного программного обеспечения до комплексного воздействия на цифровую инфраструктуру с использованием её эксплуатационных особенностей.

Следующая группа преступлений – это дистанционные мошенничества, совершаемые способом активного обмана или злоупотребления доверием. Характеризуя данную группу общественно опасных посягательств, укажем, что в случае активного обмана или злоупотребления доверием при совершении дистанционно мошеннических действий большое значение, как и при «традиционном» мошенничестве имеют технологии социальной инженерии, поскольку хотя непосредственный физический контакт пострадавшего и преступника

[60] Приговор № 1-12/2023 1-390/2022 от 16 июня 2023 г., К. городской суд (Владимирская область) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/2dMsxJbKfhLR/ (дата обращения: 04.03.2026).

исключён, злоумышленник на расстоянии так же активно виляет на волю и сознание своей жертвы, вынуждая её совершать те или иные действия, позволяющие получить преступнику либо сами денежные средства посредством перевода, либо информацию, которая позволит получить доступ в удалённом формате к этим денежным средствам.

Определяя социальную инженерию как совокупность социальных и психологических приёмов, технологий и методов манипуляции людьми в информационном пространстве с целью вынуждения их совершить определённые действия или разгласить конфиденциальную информацию, необходимую для осуществления последующего хищения денежных средств в дистанционном формате[61], многие современные исследователи справедливо называют её одним из основным инструментов хакеров XXI века и важнейшей угрозой информационной безопасности современности[62]. В настоящее время учёные даже разработали типичную схему преступного воздействия на жертву в социальной инженерии, указывая, что первоначально любой преступник формулирует цель воздействия на жертву, затем собирает информацию об объекте, после обнаруживает наиболее удобные «мишени» воздействия, далее следует этап аттракции (создание нужных для воздействия на жертву условий) и, наконец, следует понуждение к нужному действию и итог (достижение преступного результата)[63]. При этом, как уже отмечалось ранее, преступники используют самые разнообразные механизмы реализации такого воздействия. Среди таких общественно опасных посягательств отечественные исследователи выделяют: «нигерийские письма» (вид мошенничества, где преступник получает денежные средства от жертвы вследствие прямого обмана, например, сообщения о необходимости совершения жертвой преступления перевода денежных средств на заранее предоставленный банковский счёт для

[61] Головин А.Ю., Головина Е.В. Социальная инженерия в механизме преступной деятельности в сфере информационно телекоммуникационных технологий // Известия ТулГУ. Экономические и юридические науки. 2021. № 2. С. 3-13.
[62] Кузнецов М.В. Социальная инженерия и социальные хакеры. – СПб: БХВ-Петербург, 2007. С. 11-12.
[63] Там же. С. 13.

якобы оплаты услуг по получения несуществующего наследства, выигрыша в лотерее, конкурсе и т.п.[64]); смишинг (мошеннические действия, направленные на получение конфиденциальной информации, позволяющей получить доступ к банковским счетам жертвы, осуществляемые посредством рассылки СМС-сообщений с соответствующим содержанием); двойная транзакция (мошеннические действия недобросовестного оператора, сообщающего покупателю о якобы произошедшей ошибке в результате осуществления транзакции денежных средств, вследствие чего лицо повторно оплачивает товар, услуги)[65]; взлом в социальных сетях личной страницы, с последующей рассылкой сообщений с просьбой перевести денежные средства на банковскую карту злоумышленника и другие[66]. При этом отдельно следует подчеркнуть, что количество более узких способов таких преступных воздействий постоянно увеличивается, поскольку типичные схемы дистанционного мошенничества обычно быстро становятся хорошо известными широкой аудитории в результате активной работы СМИ, социальных сетей, прочих медиа, вследствие чего совершать подобные противоправные посягательства злоумышленникам становится всё труднее.

По справедливому замечанию отдельных исследователей, если ранее телефонные мошенники чаще лично звонили своим жертвам, то начиная с конца 2021 г. – начала 2022 г. большая часть таких звонков стала совершаться с использованием специальных голосовых роботов, поскольку использование таких технологий, во-первых, позволяет преступникам охватить большее количество людей, расширяя аудиторию преступного воздействия, а, во-вторых, вызывает большее доверие у граждан, вследствие чего жертвы охотнее делятся с такими роботизированными «помощниками»

[64] Алёхин А.А. Теоретические аспекты кибермошенничества: понятие, правовая природа и виды // Государственная служба и кадры. 2024. № 2. С. 17-20.
[65] Рябинина Т.К., Ряполова Я.П., Чистилина Д.О. Актуальные проблемы выявления и расследования дистанционных хищений с банковского счета // Вестник Белгородского юридического института МВД России имени И.Д. Путилина. 2023. № 4. С. 31–38.
[66] Диваева И.Р. Дистанционное мошенничество: вопросы профилактики // Аграрное и земельное право. 2022. № 11 (215). С. 185-187.

преступников конфиденциальной информацией[67]. Или, например, если на звонки от псевдосотрудников правоохранительных органов с просьбой помочь родственнику якобы попавшему в беду уже практически никто не реагирует, то на звонки от злоумышленников, изменивших свою речь посредством использования технологии deepfake, позволяющей разговаривать практически любым голосом, в том числе и голосом близкого родственника жертвы, по современным данным, откликаются многие[68]. В результате сочетание новых информационно-телекоммуникационных технологий с приёмами и методами социальной инженерии позволяют преступникам посредством активного обмана, злоупотребления доверием эффективно добиваться преступного результата, хотя для получения этого результата злоумышленнику необходимо активно повышать свой криминальный уровень и следить за последними технологическими новинками цифровой среды.

Переходя к анализу более узких способов совершения дистанционных мошенничеств посредством активного обмана или злоупотребления доверием, укажем, что, согласно данным судебной практики, а также современным специальным научным исследованиям отмечается значительное разнообразие применения соответствующих средств совершения преступлений[69]. В связи с этим отдельные исследователи даже классифицируют такие общественно опасные посягательства на: дистанционные мошенничества, совершаемые только с помощью сети Интернет; дистанционные мошенничества, совершаемые с помощью сети Интернет и средств телефонной связи; дистанционные мошенничества, совершаемые с использованием средств сотовой связи и непосредственного

[67] Смагоринский Б.П., Сычева А.В. О некоторых актуальных способах совершения мошенничества в отношении физических лиц в современных условиях // Вестник Волгоградской академии МВД России. 2022. № 2 (61). С. 172-178.
[68] Еремин С.Г., Сычева А.В. О способах мошенничеств без визуального контакта с потерпевшим и методах их предупреждения // Baikal Research Journal. 2022. № 1. С. 23.
[69] Соловьев В.С., Шевчук-Горобец К.Ю. Мошенничество с использованием электронных средств платежа: per motris non lates // Гуманитарные, социально-экономические и общественные науки. 2022. № 12. С. 231–235.

контакта с жертвой и т.д.[70] Данные судебной практики также указывают на разнообразие средств совершения таких преступных посягательств, среди которых выделяется использование компьютерной техники[71], программных средств[72], сети Интернет, средств сотовой связи[73], иных технических средств и устройств. Однако чаще всего преобладает использование сразу нескольких технических средств и устройств, необходимых для совершения преступлений, ввиду чего такие общественно опасные деяния нужно относить к комбинированным преступлениям. При этом особо подчеркнём, что в ситуации, когда совершается активный обман, злоупотребление доверием, разнообразные технические средства используются чаще всего именно как средства связи с жертвой для оказания на неё психологического воздействия в удалённой форме.

С учётом всего изложенного следует отметить, что разграничение дистанционных мошенничеств, совершаемых с применением активного обмана или злоупотребления доверием, основывается на характере и доминирующем способе преступного воздействия на потерпевшего, а также на степени опосредованности такого воздействия цифровыми технологиями. При этом определяющим критерием выступает не столько используемый канал связи, а преобладающий механизм формирования у потерпевшего мотивации к совершению имущественных действий – например, преимущественно информационное сообщение, психологическое давление, использование доверительных отношений либо их сочетание. В результате по способам совершения преступления дистанционные мошенничества

[70] Сычева А.В. Некоторые способы совершения «дистанционного» мошенничества // Вестник Волгоградской академии МВД России. 2020. № 4 (55). С. 167-172.

[71] См., например: Приговор № 1-125/2023 1-3/2024 от 22 января 2024 г. по делу № 1-125/2023. О. районный суд г. Новокузнецка (Кемеровская область) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/ULO9JOi7W3oj/ (дата обращения: 05.03.2026).

[72] См., например: Приговор № 1-2/2020 1-2/2021 1-5/2019 1-97/2018 от 21 июня 2021 г. по делу № 1-2/2020. С. районный суд г. Иваново (Ивановская область) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/IifZELYWnygP/ (дата обращения: 06.03.2026).

[73] См., например: Приговор № 1-351/2023 1-8/2024 от 10 января 2024 г. по делу № 1-351/2023.
Л. районный суд г. Саранска (Республика Мордовия) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/6e0BO62jtxm5/ (дата обращения: 07.03.2026).

с применением активного обмана или злоупотребления доверием условно могут быть определены следующим образом:

– вербально-информационные (формирование у потерпевшего ложного представления о фактических либо правовых обстоятельствах путём передачи недостоверной информации через удалённые каналы связи, побуждающее его к добровольному отчуждению имущества или имущественных прав);

– психологически-манипулятивные (целенаправленное воздействие на эмоционально-волевую сферу потерпевшего с использованием приёмов социальной инженерии, направленное на подавление критического восприятия информации и принуждение к совершению имущественно значимых действий);

– доверительно-эксплуатирующие (использование сложившихся либо искусственно сформированных доверительных отношений для побуждения потерпевшего к передаче имущества или раскрытию сведений, обеспечивающих последующее дистанционное завладение им);

– комбинированные (одновременное использование нескольких психологических элементов преступного воздействия, при котором цифровые технологии обеспечивают дистанционность и масштабируемость посягательства, а социальная инженерия – его индивидуализацию).

В качестве иллюстраций использования разных способов совершения дистанционных мошенничеств такого рода приведём несколько уголовных дел. Укажем на Приговор № 1-25/2019 1-377/2018 от 8 декабря 2019 г. по делу № 1-275/2018 С. районного суда г. Томска (Томская область). Согласно материалам уголовного дела, неустановленные лица, действуя совместно и согласованно, осуществили телефонный звонок потерпевшей, представившись сотрудниками банка и службы безопасности финансовой организации. В ходе разговора потерпевшей было сообщено, что в отношении её банковского счёта якобы зафиксированы попытки несанкционированного списания денежных средств, а также оформление

кредитных обязательств третьими лицами. Далее, с целью придания достоверности сообщаемой информации, потерпевшей было предложено продолжить общение в мессенджере, где ей последовательно разъяснялся «алгоритм защиты денежных средств». Под воздействием введения в заблуждение потерпевшая осуществила перевод денежных средств на банковские счета, указанные злоумышленниками, которые были обозначены как «безопасные счета» либо счета «Центрального банка Российской Федерации», подконтрольные преступникам, и обращены ими в свою пользу[74]. Рассмотренное деяние характеризуется психологически-манипулятивным способом совершения дистанционного хищения. Воздействие на потерпевшего осуществлялось посредством телефонной связи и мессенджеров. Виновные сообщали заведомо ложные сведения о возникшей угрозе для денежных средств и тем самым формировали у потерпевшего убеждение в необходимости незамедлительно выполнить их указания. В данном случае телефонная связь и мессенджеры обеспечивали дистанционное взаимодействие, однако сами по себе не определяли способ совершения преступления. Основное значение имело содержание воздействия на потерпевшего, а именно создание тревожного состояния, ограничение времени на принятие решения и формирование ложного представления о необходимости самостоятельно предпринять действия для сохранения денежных средств. Именно такое воздействие побуждало потерпевшего совершить действия, в результате которых виновные получали возможность завладеть его имуществом. Как видим, приведённый пример показывает иной механизм дистанционного мошенничества по сравнению с использованием вредоносного программного обеспечения. Преступный результат достигается здесь не посредством непосредственного воздействия на используемую потерпевшим информационную систему, а через изменение его поведения под воздействием обмана и психологической манипуляции.

[74] Приговор № 1-25/2019 1-377/2018 от 8 декабря 2019 г. по делу № 1-275/2018, С. районный суд г. Томска (Томская область) [Электронный документ]. – URL: https://sudact.ru/regular/doc/hktokOrwZgbO/ (дата обращения: 29.06.2026).

Также для иллюстрации различных способов совершения дистанционных мошенничеств посредством «активного обмана» или злоупотребления доверием приведём дело, рассмотренное в 2025 г. Б. районным судом Республики Крым в отношении нескольких граждан, обвиняемых в совершении преступления, предусмотренного ч. 3 ст. 30, п. «б» ч. 3 ст. 291.1 УК РФ, а также ч. 3 ст. 159 УК РФ. Согласно материалам следствия, подсудимые действовали совместно и согласованно, распределив между собой роли в рамках единого преступного умысла, направленного на незаконное дистанционное получение денежных средств. При этом взаимодействие с потерпевшим осуществлялось опосредованно, без непосредственного личного контакта, посредством передачи информации через удалённые каналы связи. Установлено, что указанные лица осуществляли организационные действия, направленные на обеспечение дистанционного контакта с потенциальными «клиентами», а также доведение до них заведомо ложной информации о возможности решения вопросов имущественного характера за денежное вознаграждение. Однако преступный умысел не был доведён до конца по независящим от виновных лиц обстоятельствам, поскольку противоправные действия были пресечены[75]. Данный способ следует отнести к комбинированным дистанционным мошенничествам, поскольку преступное воздействие на потерпевшего строилось на сочетании нескольких взаимодополняющих способов. Преступный результат предполагалось достичь посредством комплексного сочетания информационного введения в заблуждение и «эксплуатации» доверия потерпевшего.

На основании представленных данных возможно приведение следующей обобщённой систематизации форм и способов совершения дистанционных хищений, отражающей как техническую, так и социально-психологическую природу данного феномена. В первую очередь,

[75] Приговор № 1-178/2025 от 12 ноября 2025 г. по делу № 1-178/2025, Б. районный суд (Республика Крым) [Электронный документ]. URL: https://sudact.ru/regular/doc/GSrqVh21SwmJ/ (дата обращения: 29.06.2026).

дистанционные хищения целесообразно подразделять на две формы – дистанционные кражи и дистанционные мошенничества, внутри которых выделяются устойчивые группы способов.

Для дистанционных краж как формы дистанционного хищения по характеру направленности преступного воздействия свойственны следующие способы совершения преступления: 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).

Дистанционные мошенничества, в свою очередь, могут быть сведены к двум основным способам: посредством персонализированного (активного) обмана потерпевшего либо посредством технически опосредованного воздействия на цифровую среду, когда ошибочное волеизъявление потерпевшего формируется не непосредственным убеждением, а созданием ложной информационной ситуации. При этом для указанных разновидностей обмана характерны собственные более узкие способы совершения преступлений ввиду специфики воздействия на жертву преступления и соответствующие цифровые ресурсы. Так, дистанционные мошенничества, совершаемые посредством активного обмана или злоупотребления доверием, могут реализовываться вербально-информационным, психологически-манипулятивным, доверительно-эксплуатирующим либо комбинированным способом, тогда как мошенничества, основанные на технически опосредованном воздействии на цифровую среду, – информационно-технологическим, эксплуатационно-инфраструктурным, системно-дестабилизирующим либо комбинированным способом.

Таким образом, дистанционные хищения представляют собой категорию имущественных преступлений, в которых традиционные признаки

хищения – корыстная цель, противоправность изъятия, безвозмездность завладения, обращение имущества в пользу виновного или третьих лиц, причинение ущерба – сохраняются, но трансформируются под воздействием цифровой среды. Исследование форм и способов дистанционных хищений показывает сочетание технических и социально-психологических компонентов: кражи реализуются через непосредственный доступ к учётным данным или манипулирование информационно-техническими системами, а мошенничества – посредством активного или технически опосредованного обмана с использованием информационно-телекоммуникационных технологий. Такая дифференциация позволяет обеспечить единообразный подход к систематизации способов совершения дистанционных хищений и формирует методологическую основу для последующего анализа уголовно-правовых и криминалистических механизмов их выявления и расследования. В целом указанные обстоятельства позволяют сделать вывод о формировании в современной уголовно-правовой доктрине устойчивой тенденции к функциональной «цифровизации» института хищения, при которой его традиционная конструкция сохраняется, но наполняется новыми технологическими параметрами, обусловливающими необходимость дальнейшей теоретической систематизации и совершенствования уголовно-правовых средств противодействия. Рассмотренные примеры позволяют увидеть различия не только между формами хищения, но и между конкретными механизмами их совершения. При краже виновный может использовать полученный доступ к сведениям, необходимым для распоряжения денежными средствами, либо непосредственно воздействовать на информационную систему. При мошенничестве возникает иная ситуация. Потерпевший сам совершает необходимые действия, поскольку воспринимает сообщённые ему сведения как достоверные. В одном преступлении оба механизма могут сочетаться. Например, полученные в результате обмана сведения затем используются для доступа к денежным средствам и их перевода. Поэтому при классификации способов

дистанционных хищений имеет значение не наличие информационно-телекоммуникационной технологии как таковой, а выполняемая ею функция. В результате дистанционный характер преступления не меняет его уголовно-правовой формы, а дистанционность характеризует способ реализации преступного умысла. Такое разграничение имеет значение для последующей оценки конкретного деяния, поскольку позволяет не смешивать признаки формы хищения с особенностями использованного виновным способа.

Таким образом, развитие цифровых технологий не изменило юридической природы хищения как уголовно-правовой категории, однако существенно трансформировало механизм совершения имущественных посягательств такого рода. В результате дистанционные хищения в настоящее время представляют собой категорию имущественных преступлений, в которых традиционные признаки хищения – корыстная цель, противоправность изъятия, безвозмездность завладения, обращение имущества в пользу виновного или третьих лиц, причинение ущерба – сохраняются, но трансформируются под воздействием цифровой среды. Вместе с тем дистанционные хищения характеризуются внутренней неоднородностью, находящей своё выражение в различных формах их совершения и присущих им способах преступного воздействия, отражающих особенности реализации имущественных посягательств в условиях цифровой среды. Они могут быть систематизированы по формам (дистанционные кражи и дистанционные мошенничества) и соответствующим им способам совершения преступления, представленным применительно к дистанционным кражам персонализированными и техническими способами, а применительно к дистанционным мошенничествам – способами, основанными на активном обмане либо технически опосредованном воздействии на цифровую среду.

Глава 2. Уголовно-правовые средства противодействия хищениям, совершаемым дистанционно

2.1. Система уголовно-правовых средств противодействия хищениям, совершенным дистанционно

В предыдущем параграфе обосновано, что применительно к предлагаемому пониманию дистанционного хищения основное значение имеют кража и мошенничество. В связи с этим систему уголовно-правовых запретов, применяемых при совершении таких преступлений, целесообразно рассмотреть по уровням в зависимости от непосредственной связи соответствующей нормы с механизмом завладения чужим имуществом.

Первый, основной уровень составляют нормы, непосредственно предусматривающие ответственность за хищение имущества при использовании дистанционного способа его совершения. К ним относятся п. «г» ч. 3 ст. 158 УК РФ, предусматривающий ответственность за кражу с банковского счёта, а равно в отношении электронных денежных средств, ст. 159^3 УК РФ – мошенничество с использованием электронных средств платежа, и ст. 159^6 УК РФ – мошенничество в сфере компьютерной информации.

Особое место на данном уровне занимает п. «г» ч. 3 ст. 158 УК РФ. Появление в норме указания на банковский счёт и электронные денежные средства связано с изменением способов обращения имущества и расширением возможностей его дистанционного перемещения. Однако само использование банковских приложений, электронных средств платежа или иных технических инструментов ещё не определяет уголовно-правовую квалификацию. Для разграничения кражи и мошенничества необходимо установить прежде всего способ завладения денежными средствами, характер воздействия на потерпевшего и фактическую роль использованного технического средства в механизме преступления. Так, например, длительное

время в правоприменительной практике существовала проблема разграничения п. «г» ч. 3 ст. 158 УК РФ и ст. 159^3 УК РФ. Несмотря на то, что в самом законе (а именно в п. «г» ч. 3 ст. 158 УК РФ) указано, что по данной статье надлежит квалифицировать деяния только в том случае, если отсутствуют признаки состава преступления, предусмотренного ст. 159^3 УК РФ, на практике некоторые трудности всё же возникают. До издания Верховным судом РФ Определения № 12-УДП20-5-К6 от 29.09.2020[76] и Определения Конституционного суда РФ от 09.07.2021 № 1374-О[77], существовала проблема с квалификацией хищений денежных средств посредством осуществления бесконтактной оплаты товаров и услуг банковской картой, принадлежащей другому лицу, без права распоряжения данными средствами. В одних случаях указанные деяния квалифицировали по ст. 159^3 УК РФ[78], а в других – по п. «г» ч. 3 ст. 158 УК РФ[79]. Однако после издания соответствующих уточнений определено, что работники торговых организаций, осуществляющие платёжные операции с банковскими картами, в соответствии со своими трудовыми обязанностями не должны идентифицировать личность покупателя с личностью собственника банковской карты по документам, ввиду чего такие преступные деяния нужно квалифицировать именно по п. «г» ч. 3 ст. 158 УК РФ. При этом, несмотря на то, что указанная проблема была решена, ряд сложностей квалификации данных преступных деяний всё же существует и сегодня.

---

[76] Определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 29.09.2020 № 12-УДП20-5-К6 [Электронный документ]. – URL: https://legalacts.ru/sud/opredelenie-sudebnoi-kollegii-po-ugolovnym-delam-verkhovnogo-suda-rossiiskoi-federatsii-ot-29092020-n-12-udp20-5-k6/ (дата обращения: 08.03.2026).

[77] Определение Конституционного Суда РФ от 09.07.2021 № 1374-О «О прекращении производства по делу о проверке конституционности пункта “г” части третьей статьи 158 и статьи 159^3 Уголовного кодекса Российской Федерации в связи с запросом Железнодорожного районного суда города Рязани» [Электронный документ]. – URL: https://www.consultant.ru/document/cons_doc_LAW_391466/ (дата обращения: 09.03.2026).

[78] См., например: Приговор № 1-209/2020 от 28 мая 2020 г. по делу № 1-209/2020 [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/eu9NH0NOnvbh/ (дата обращения: 10.03.2026); Приговор № 1-212/2020 от 26 мая 2020 г. по делу № 1-212/2020 [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/Dxt1HJcYfi6v/ (дата обращения: 11.03.2026).

[79] См., например: Приговор № 1-1-2/2020 1-37/2019 от 5 февраля 2020 г. по делу № 1-1-2/2020, Р. районный суд (Ульяновская область) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/QpzWyBiSwe64/ (дата обращения: 12.03.2026); Приговор № 1-159/2019 1-16/2020 от 4 февраля 2020 г. по делу № 1-159/2019, К. районный суд (Красноярский край) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/Zy0Ny2UbqxVJ/ (дата обращения: 13.03.2026).

Так, например, ввиду активного развития новых информационных технологий в настоящее время существуют сложности при квалификации хищений безналичных денежных средств при оплате различных товаров и услуг при помощи специальных мобильных приложений, смарт-часов, других устройств, поддерживающих технологии MST, NFC и т.д. Указанный вопрос не получил должной законодательной регламентации, поскольку он не рассматривается в разъяснениях Верховного суда РФ, хотя научные дискуссии, основанные на правоприменительном опыте, по этому поводу в юридическом сообществе активно ведутся[80]. Чаще всего такие деяния оцениваются как мошенничество[81], однако опираясь на выработанную правоприменительную практику относительно квалификации хищений безналичных денежных средств с применением бесконтактной системы оплаты товаров и услуг, считаем необходимым распространить действие п. «г» ч. 3 ст. 158 УК РФ и на рассматриваемый вид хищений при оплате различных товаров и услуг при помощи специальных мобильных приложений, смарт-часов, других устройств, поддерживающих технологии MST, NFC и т.д., поскольку в данном случае злоумышленники, используя тот или иной гаджет, оснащённый соответствующей технологией, расплачиваются им так же, как и банковской картой с функцией бесконтактной оплаты, только применяя чуть более сложный путь получения доступа к безналичным денежным средствам, которые как и в случае с банковской картой можно получить в результате выполнения нехитрых манипуляций с тем или иным гаджетом. Вследствие этого считаем необходимым с целью уточнения правоприменительной практики внести соответствующее изменение в Постановление Пленума Верховного суда РФ от 27.12.2002 № 29 «О судебной практике по делам о краже, грабеже и разбое» (с изм. и доп.).

[80] Байбарин А.А., Садчикова Д.Н. Кража безналичных и электронных денег: об актуальных проблемах правоприменения // Вестник Сургутского государственного университета. 2022. № 1 (35). С. 60-68.
[81] Приговор № 1-38/2020 от 12 ноября 2020 г. по делу № 1-38/2020, А. районный суд (Республика Татарстан) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/mckKk0siqExx/ (дата обращения: 14.03.2026).

Также не менее дискуссионным является отграничение рассматриваемого состава от мошенничества в сфере компьютерной информации, предусмотренного ст. 159[6] УК РФ. Указанная проблема носит устойчивый характер и неоднократно отмечается в научной литературе[82]. Сегодня наблюдается значительная неоднозначность судебной практики в отношении действий, которые могут быть квалифицированы как кража с банковского счёта (п. «г» ч. 3 ст. 158 УК РФ) или как мошенничество в сфере компьютерной информации (п. «в» ч. 3 ст. 159[6] УК РФ). Сложность заключается в том, что оба вида хищений совершаются дистанционно с использованием электронных средств и направлены на незаконное завладение чужими денежными средствами. Однако, как верно отмечают А.И. Ситникова и Г.В. Назаренко, критерием разграничения является объективная сторона непосредственного воздействия. Так, при краже субъект использует уже функционирующий механизм распоряжения денежными средствами, не вмешиваясь в компьютерную информацию или работу программного обеспечения, тогда как при мошенничестве в сфере компьютерной информации имеет место целенаправленное вмешательство в функционирование средств хранения, обработки или передачи информации, что создаёт условия для завладения чужими средствами[83]. При этом на практике данный критерий часто игнорируется, что приводит к ошибочной квалификации и неоднозначным судебным решениям. Так, любое использование онлайн-банкинга, мобильных приложений или дистанционного доступа к счёту нередко квалифицируется по статье 159[6] УК РФ, даже при отсутствии вмешательства в работу программного обеспечения или средств защиты информации. В то же время, как справедливо отмечают

[82] Лукьянова Ю.В., Амирова Д.К. Кража с банковского счета, а равно в отношении электронных денежных средств: проблемы квалификации и отграничения от смежных составов преступлений // Ученые записки Казанского юридического института МВД России. 2024. № 2 (18). С. 23-28; Юсупова А.Ф. Хищение денежных средств с банковского счета, а равно в отношении электронных денежных средств: проблемы квалификации и уголовной ответственности // Вопросы российской юстиции. 2024. № 34. С. 427-437.

[83] Ситникова А.И., Назаренко Г.В. Проблемы толкования и квалификации альтернативных видов хищений, совершаемых с банковского счета или в отношении электронных денежных средств // Научный вестник Омской академии МВД России. 2025. Т. 31, № 3(98). С. 246-252.

Ю.В. Лукьянова и Д.К. Амирова, при краже с банковского счёта виновное лицо использует уже существующий и корректно функционирующий механизм распоряжения денежными средствами, не изменяя алгоритмов его работы и не воздействуя на компьютерную информацию в техническом смысле, и в таких случаях имеет место тайное хищение чужого имущества, а не мошенничество в сфере компьютерной информации[84]. Кроме того, в условиях цифровизации финансово-экономических отношений способы совершения дистанционных хищений всё чаще носят комплексный характер, сочетающий элементы вмешательства в информационные системы и последующее незаконное списание денежных средств с банковских счетов потерпевших. В подобных ситуациях, по справедливому замечанию отдельных исследователей, действия виновного формально могут содержать признаки как мошенничества в сфере компьютерной информации, так и кражи с банковского счёта, что порождает конкуренцию уголовно-правовых норм и затрудняет выбор подлежащей применению статьи Особенной части УК РФ[85].

В результате отсутствие в уголовном законе чётко сформулированных критериев разграничения данных составов приводит к тому, что правоприменительная практика по аналогичным фактическим обстоятельствам формируется неоднородно, а правовая оценка содеянного во многом зависит от усмотрения конкретного суда. И хотя в доктрине уголовного права уже разрабатываются критерии разграничения указанных составов преступлений, по верному утверждению А.С. Мирончик и А.В. Суслопарова, исчерпывающего ответа на все возникающие в

[84] Лукьянова Ю.В., Амирова Д.К. Кража с банковского счета, а равно в отношении электронных денежных средств: проблемы квалификации и отграничения от смежных составов преступлений // Ученые записки Казанского юридического института МВД России. 2024. № 2 (18). С. 23-28.

[85] Иванов М.Г., Николаев А.Ю. Проблемы разграничения составов имущественных преступлений, связанных с информационными технологиями (ст. 159^3, 159^6 и п. «г» ч. 3 ст. 158 УК РФ) // Вестник РУК. 2020. № 3 (41). С. 123-126; Барчуков В.К. К вопросу о квалификации мошенничества в сфере компьютерной информации // Пробелы в российском законодательстве. 2017. № 2. С. 128-130; Крумина Д.И. Использование идентификационных данных в преступных целях: вопросы разграничения составов преступлений (ст. 158, 159, 159^3, 159^6 УК РФ) // Вестник ВолГУ. Серия 9: Исследования молодых ученых. 2022. № 20. С. 126-127 и др.

правоприменительной практике вопросы они не содержат[86]. Всё это в совокупности позволяет сделать вывод о наличии устойчивых проблем квалификации кражи, совершённой с банковского счёта либо в отношении электронных денежных средств. В результате превентивный потенциал п. «г» ч. 3 ст. 158 УК РФ реализуется не в полной мере, что свидетельствует о необходимости дальнейшего теоретического осмысления данного состава преступления, уточнения его уголовно-правовых признаков и выработки единообразных подходов к квалификации краж, совершаемых в дистанционной форме.

Для совершенствования действия п. «г» ч. 3 ст. 158 УК РФ и обеспечения единообразия правоприменительной практики представляется целесообразным принять следующие меры. Во-первых, следует внести изменение в Постановление Пленума Верховного суда РФ от 27.12.2002 № 29 «О судебной практике по делам о краже, грабеже и разбое» (с изм. и доп.), указав, что кража с банковского счёта охватывает также случаи незаконного распоряжения безналичными денежными средствами с использованием современных цифровых платёжных инструментов (мобильных приложений, электронных кошельков, смарт-устройств и иных средств бесконтактной оплаты), функционально заменяющих банковскую карту. Во-вторых, необходимо выработать чёткие критерии разграничения п. «г» ч. 3 ст. 158 УК РФ и ст. 159[6] УК РФ, исходя из приоритетного объекта посягательства и степени вмешательства в функционирование информационных систем, используемых при совершении хищения, и закрепить их в разъяснениях Пленума Верховного Суда РФ, а именно определить, что действия, направленные исключительно на тайное завладение чужими денежными средствами без модификации, блокировки или удаления компьютерной информации, квалифицируются по п. «г» ч. 3 ст. 158 УК РФ, а действия, сопровождаемые вмешательством в работу

[86] Мирончик А.С., Суслопаров А.В. Хищения в электронной среде как разновидность информационных преступлений: проблемы разграничения и квалификации // Юридические исследования. 2019. № 9. С. 17-30.

программного обеспечения или средствами хранения информации, следует квалифицировать по ст. 159^6 УК РФ как мошенничество в сфере компьютерной информации. Такой подход позволит суду ориентироваться на объективный признак – характер воздействия на объект преступления, а не на внешние формы использования технических средств. Считаем, что реализация указанных мер позволит устранить конкуренцию уголовно-правовых норм, повысить предсказуемость правоприменения и тем самым обеспечить более эффективную защиту имущественных интересов граждан в условиях цифровизации финансово-экономических отношений.

Переходя к анализу следующей нормы, устанавливающей ответственность за дистанционные хищения в рамках «основного уровня», укажем, что ст. 159^3 УК РФ предусматривает ответственность за мошенничество с использованием электронных средств платежа. Определим, что после издания Верховным судом РФ Определения № 12-УДП20-5-К6 от 29.09.2020[87] и Определения Конституционного суда РФ от 09.07.2021 № 1374-О[88], правоприменительная практика по этой норме была унифицирована, и она фактически пополнила список «мёртвых норм», которые исключены из области реального применения[89]. Об этом свидетельствует официальная судебная статистика. Так, например, если в 2019 г. по данной статье в России было зарегистрировано 16 119 преступлений, то в 2023 г. – всего 2 461 преступление, а в 2024 г. – 273. Более наглядно динамика движения указанной разновидности преступной деятельности представлена в Диаграмме (см. рис. 2).

[87] Определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 29.09.2020 № 12-УДП20-5-К6 [Электронный документ]. – URL: https://legalacts.ru/sud/opredelenie-sudebnoi-kollegii-po-ugolovnym-delam-verkhovnogo-suda-rossiiskoi-federatsii-ot-29092020-n-12-udp20-5-k6/ (дата обращения: 15.03.2026).

[88] Определение Конституционного Суда РФ от 09.07.2021 № 1374-О «О прекращении производства по делу о проверке конституционности пункта “г” части третьей статьи 158 и статьи 159^3 Уголовного кодекса Российской Федерации в связи с запросом Железнодорожного районного суда города Рязани» [Электронный документ]. – URL: https://www.consultant.ru/document/cons_doc_LAW_391466/ (дата обращения: 16.03.2026).

[89] Русскевич Е.А., Чернова К.Б. Актуальные проблемы квалификации хищений, совершаемых с использованием электронных средств платежа // Вестник экономической безопасности. 2021. № 1. С. 128-130.

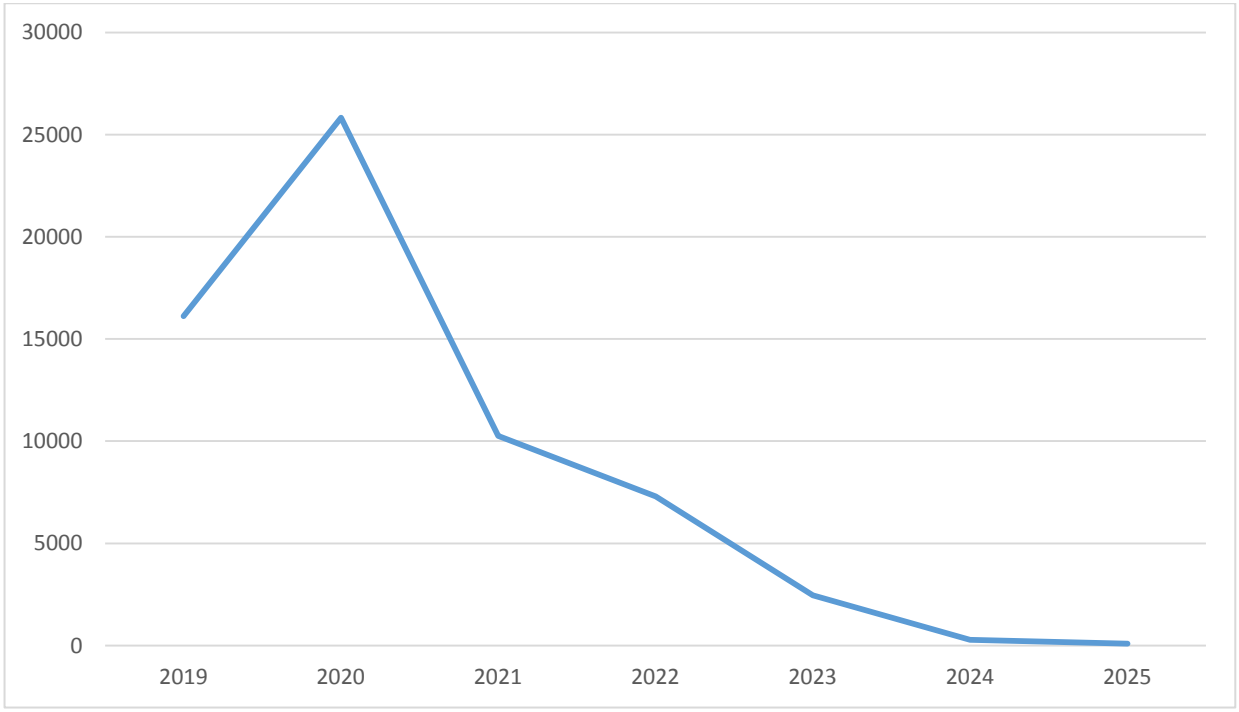


Рисунок 2. Мошенничества с использованием электронных средств платежа в Российской Федерации в 2019–2025 гг. [90]

Как видно, после принятия соответствующих Определений Верховного суда РФ и Конституционного суда РФ число зарегистрированных преступлений по данной статье значительно снизилось, вследствие чего возникли вопросы относительно эффективности действия указанной нормы права в принципе, что является, по нашему усмотрению, основной проблемой квалификации преступных деяний по данной норме. Для решения указанной проблемы полагаем, Верховному Суду РФ также представляется необходимым уточнить подходы к применению ст. 159^3 УК РФ с учётом современных механизмов дистанционного мошенничества. Необходимость такого уточнения обусловлена существенным сокращением практики применения данной нормы, что свидетельствует не об отсутствии соответствующих мошеннических посягательств, а о наличии проблемы их разграничения с иными составами. В связи с этим в судебных разъяснениях целесообразно конкретизировать признаки ситуации, при которой

[90] Состояние преступности [Электронный ресурс]. – URL: https://xn--b1aew.xn--p1ai/reports/6/ (дата обращения: 17.03.2026).

использование электронного средства платежа образует предусмотренный ст. 159^3 УК РФ способ совершения мошенничества, в том числе определить его непосредственную связь с механизмом передачи денежных средств потерпевшим под воздействием обмана или злоупотребления доверием. При этом такое уточнение не должно сводиться к формированию исчерпывающего перечня способов совершения преступления или расширению сферы действия уголовно-правовой нормы, а должно быть направлено на обеспечение её единообразного и предсказуемого применения.

Ранее ещё одной значимой проблемой квалификации ст. 159^3 УК РФ была недостаточная конкретизация понятия «электронные средства платежа». Уточним, что в редакции Федерального закона от 23 апреля 2018 г. № 111-ФЗ, в статье было введено рассматриваемое понятие как новое средство совершения мошенничества. Однако его формулировка не охватывала все современные способы безналичных расчётов, ограничиваясь, по сути, традиционными банковскими картами и электронными кошельками, что порождало неоднозначность правоприменения. В частности, ранее диспозиция ст. 159^3 УК РФ не включала такие современные инструменты, как мобильные приложения с токенизацией, QR-платежи или смарт-кошельки, вследствие чего одни и те же действия – завладение средствами через мобильное приложение, цифровую карту или предоплаченную карту – могли квалифицироваться либо по ст. 159^3 УК РФ, либо по общей норме о мошенничестве (ст. 159 УК РФ), что создавало ситуацию правовой неопределённости. Однако с принятием Федерального закона от 13 февраля 2025 г. № 9-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» данная проблема была частично решена. Теперь электронное средство платежа определяется как совокупность средств и способов, позволяющих клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения для осуществления перевода денежных средств с использованием информационно-коммуникационных технологий, электронных носителей информации и

технических устройств, включая платежные карты, их токенизированные версии, мобильные приложения, QR-платежи и другие цифровые инструменты[91]. Тем не менее, ст. 159[3] УК РФ в целом сохраняет малоинформативную диспозицию, полностью совпадающую с заголовком статьи, что выражается в недостаточной детализации квалифицирующих признаков, таких как конкретные способы завладения средствами, технические средства реализации хищения. Эта недостаточность продолжает создавать трудности при единообразной правовой оценке действий лиц, использующих различные электронные инструменты, и повышает риск неоднозначного толкования статьи в судебной практике.

Учитывая недостаточную распространённость применения ст. 159[3] УК РФ в судебной практике, представляется необходимым дополнить соответствующее постановление Пленума Верховного Суда Российской Федерации разъяснениями, направленными на формирование единообразного подхода к квалификации рассматриваемых деяний. В частности, целесообразно раскрыть содержание признака использования электронного средства платежа как способа совершения мошенничества, определить обстоятельства, позволяющие признать такое использование юридически значимым для квалификации, и обозначить критерии разграничения ст. 159[3] УК РФ с иными составами хищений. Это позволило бы обеспечить более последовательное применение специальной уголовно-правовой нормы в тех случаях, когда электронное средство платежа непосредственно используется в механизме завладения чужим имуществом. Далее перейдём к анализу ст. 159[6] УК РФ.

Характеризуя мошенничество в сфере компьютерной информации, укажем, что ст. 159[6] УК РФ направлена на охрану общественных отношений, связанных с обеспечением безопасности компьютерной информации и

[91] Федеральный закон от 13.02.2025 № 9-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» [Электронный документ]. – URL: https://www.consultant.ru/document/cons_doc_LAW_498604/5bdc78bf7e3015a0ea0c0ea5bef708a6c79e2f0a/ (дата обращения: 18.03.2026).

функционированием информационных систем. Однако правоприменители на практике встречаются с рядом сложностей при квалификации деяний по данном составу преступлений, и даже сам факт существования в уголовном законе данной нормы с момента её введения в УК РФ многими учёными отрицается ввиду неудачности самой формулировки диспозиции данной разновидности мошенничества[92].

В первую очередь, проанализируем структурное расположение и общее содержание данной нормы. Как замечают отдельные исследователи, казуистичный подход к выделению отдельных статей для разных видов мошенничества является не совсем уместным, поскольку выделение некоторых видов таких преступлений (как в случае с мошенничеством в сфере компьютерной информации) в содержательном компоненте не совсем логично относить именно к мошенничествам. После введения в УК РФ данного специального состава преступления вызывает сомнение «выполнение» при совершении таких преступных деяний основного признака мошенничества – злоупотребления доверием или обмана, поскольку в случае с использованием специального программного обеспечения, необходимого для завладения чужим имуществом или правом на чужое имущество имеет место быть обман, скорее не конкретного лица (волевой компонент), а техники и соответствующей программы. Хотя именно конкретный способ совершения преступления в виде обмана или злоупотребления доверием, по справедливому замечанию некоторых исследователей, является обязательным признаком объективной стороны любого вида мошенничества[93]. В связи с этим отдельные авторы даже предлагают исключить данную норму из УК РФ и ввести её в действие внутри ст. 158 УК РФ, мотивируя это тем, что при совершении подобных

[92] Шевелева С.В. Мошенничество в сфере компьютерной информации: особенности квалификации и конкуренции со смежными составами преступлений // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2017. № 4 (40). С. 230.

[93] Барокко Л.А. К вопросу об особенностях мошенничества, совершенного с использованием информационно-телекоммуникационных технологий по уголовному законодательству Российской Федерации // Вестник экономической безопасности. 2024. № 1. С. 15-19.

деяний присутствует главный признак кражи – тайность[94]. Другие – указывают на некорректное расположение ст. 159[6] УК РФ, в целом, в структуре Особенной части УК РФ[95]. А иные – предлагают переименовать ст. 159[6] УК РФ в «хищение в сфере компьютерной информации», подчёркивая тем самым лишь условную связь рассматриваемого состава преступления с мошенническими действиями[96]. Однако при всей противоречивости данной нормы, справедливости ради, стоит отметить, что законодатель, вводя в действие указанный состав преступления, справедливо руководствовался, скорее всего, исключительно прикладными целями. Кроме того, стоит отметить, как уже упоминалось ранее (более подробно см. п. 1 Главы 1 данной работы), обман конкретного лица в этом случае всё-таки присутствует, хотя и как бы – «по умолчанию».

Также укажем на одну из важнейших проблем применения данной нормы, а именно – фактическое поглощение статьёй 159[6] УК РФ ст. 272 (неправомерный доступ к компьютерной информации) и ст. 274 (нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей) УК РФ. Это обнаруживается посредством сравнения объективной стороны указанных деяний, где неправомерный доступ к компьютерной информации, а также нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей практически являются частью преступления, предусмотренного ст. 159[6] УК РФ, при условии, если эти действия приводят к завладению чужим имуществом или правом на чужое имущество. Однако санкции указанных норм, по справедливому замечанию исследователя

[94] Скоморохова М.С. Проблемы квалификации мошенничества в сфере компьютерной информации // Вопросы российской юстиции. 2024. № 30. С. 387-393; Корнеева А.В. Смежные и конкурирующие нормы: вопросы квалификации // Вестник Университета имени О. Е. Кутафина. 2024. № 4 (117). С. 56-65.

[95] Гладких В.И. Компьютерное мошенничество: а были ли основания его криминализации? // Российский следователь. 2014. № 22. С. 25-31.

[96] Простосердов М.А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им: дис. ... канд. юрид. наук. М., 2016. С. 83; Мусьял И.А. Дифференцированные виды мошенничества: теоретические и практические проблемы: дис. ... канд. юрид. наук. Курск, 2018. С. 13.

Н.А. Лопашенко, рассогласованны, поскольку за основной состав преступлений, предусмотренных ст. 272 и 274 УК РФ назначается более суровое наказание (до 2-х лет лишения свободы), нежели за совершение мошеннических действий, предусмоpенных ч. 1 ст. 159[6] УК РФ (до 4-х месяцев ареста), хотя эти составы преступлений по логике должны соотноситься как часть и целое. Помимо прочего, в ст. 159[6] УК РФ и ст. 272, ст. 274 УК РФ наблюдается полное пересечение состава компьютерного мошенничества по признакам «модификация, блокирование компьютерной информации»[97], в то время как такой признак состава преступления, предусмотренного ст. 159[6] УК РФ – удаление компьютерной информации» фактически тождественен «уничтожению компьютерной информации» из ст. 272 и ст. 274 УК РФ, вследствие чего также возникают противоречия в процессе правоприменения[98].

Кроме того, обратим внимание на п. 20 Постановления Пленума Верховного Суда РФ от 30.11.2017 № 48 (с изм. и доп.) «О судебной практике по делам о мошенничестве, присвоении и растрате», согласно которому, в том случае, если мошеннические действия, предусмотренные ст. 159[6] УК РФ, совершаются посредством распространения, использования и создания соответствующих вредоносных компьютерных программ, получения доступа к компьютерной информации, данные деяния необходимо дополнительно квалифицировать по ст. 272, 273, либо 274 УК РФ[99]. Указанное положение также противоречит законодательной логике, поскольку дополнительная квалификация преступления необходима согласно общим принципам уголовного права только в том случае, если данные деяния не охватываются общим составом, но в ситуации со ст. 272 и ст. 159[6] УК РФ, как раз это и наблюдается (здесь отмечается совпадение элементов

[97] Лопашенко Н.А. Компьютерное мошенничество – новое слово в понимании хищения или ошибка законодателя? // Пермский юридический альманах. Ежегодный научный журнал. 2019. № 2 (1). С. 598-609.
[98] Болсуновская Л.М. Анализ способов совершения мошенничества в сфере компьютерной информации // Проблемы экономики и юридической практики. 2015. № 6. С. 108-111.
[99] Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 (ред. от 15.12.2022) «О судебной практике по делам о мошенничестве, присвоении и растрате» [Электронный документ]. – URL: https://www.consultant.ru/document/cons_doc_LAW_283918/ (дата обращения: 19.03.2026).

объективной стороны), вследствие чего возникает некая противоречивость[100], что подтверждают данные современной правоприменительной практики[101].

Как видим, сам факт существования ст. 159^6 УК РФ в действующей редакции встречает множество противоречий не просто в процессе применения нормы на практике, но и в части соответствия данной нормы общему пониманию содержания понятия мошенничество и принятым уголовно-правовой наукой «стандартам» построения норм закона, вследствие чего обнаруживаемые сложности требуют дополнительной законодательной регламентации.

Для совершенствования данной нормы предлагаем следующее. Считаем целесообразным уточнить также посредством разъяснений Верховного Суда РФ диспозицию нормы, конкретизировав признаки мошенничества в сфере компьютерной информации. Это позволит устранить правовую неопределённость, связанную с отсутствием прямого упоминания обмана или злоупотребления доверием, и укрепит соответствие статьи «классическим» признакам мошенничества. Также рекомендуется разграничить пересечение ст. 159^6 с нормами ст. 272–274 УК РФ. Это позволит устранить эффект «двойной превенции», устранить противоречия в санкциях и обеспечить согласованность уголовно-правовой квалификации. Можно предусмотреть, что действия, включающие неправомерный доступ или модификацию компьютерной информации с целью завладения чужим имуществом, квалифицируются исключительно по ст. 159^6 УК РФ, без обязательного дополнительного квалифицирования по ст. 272–274 УК РФ. В итоге данные меры позволят обеспечить логичность, согласованность и

[100] Фролов М.Д. Уголовно-правовое и криминологическое противодействие мошенничеству в сфере компьютерной информации: дис. ... канд. юрид. наук: 12.00.08. М., 2018. С. 170.

[101] См., например: Приговор № 1-36/2023 1-463/2022 от 26 октября 2023 г. по делу № 1-36/2023, К. городской суд (Владимирская область) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/yKACyWLbR9Zb/ (дата обращения: 20.03.2026); Приговор № 1-374/2020 от 23 октября 2020 г. по делу № 1-374/2020, К. районный суд г. Ростова-на-Дону (Ростовская область) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/mncw7jMm2Zmn/ (дата обращения: 21.03.2026); Приговор № 1-243/2020 от 29 июля 2020 г. по делу № 1-243/2020, О. городской суд (Республика Башкортостан) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/eLKpELsMEF5w/ (дата обращения: 22.03.2026) и др.

практическую применимость ст. 159^6 УК РФ, а также повысить её эффективность в защите общественных отношений в сфере информационных технологий.

Безусловно, выявленные недостатки в наименовании, содержании норм, обеспечивающих противодействие уголовно-правовыми мерами хищениям, совершаемым дистанционно, не являются единственными, и современные исследователи, специализирующиеся на изучении данной сферы правоприменения и законодательного регулирования, высказывают и другие критические замечания, вследствие чего указанный перечень проблем является открытым. Однако, в целом, именно обнаруженные проблемы дифференциации уголовной ответственности за такие специализированные виды дистанционных хищений, по нашему усмотрению, особо нуждаются в решении для обеспечения при квалификации преступных деяний из данной сферы правильной уголовно-правовой оценки.

В целом нормы основного уровня (п. «г» ч. 3 ст. 158, ст. 159^3 и ст. 159^6 УК РФ) непосредственно закрепляют ответственность за различные способы противоправного завладения имуществом в условиях цифровизации общественных отношений (а при необходимости – общие составы ст. 158 и 159 УК РФ). Вместе с тем анализ указанных составов показывает, что дистанционные хищения не исчерпываются лишь непосредственным завладением чужими денежными средствами и иными подобными «операциями». Их совершение нередко становится возможным благодаря использованию специальных технических средств, вмешательству в информационные системы либо созданию условий для последующего неправомерного распоряжения похищенным имуществом. В связи с этим система уголовно-правового противодействия дистанционным хищениям включает не только нормы, непосредственно предусматривающие ответственность за хищение, но и иные составы, обеспечивающие защиту цифровой инфраструктуры и препятствующие реализации преступного

механизма[102]. Представляется необходимым обратиться к рассмотрению вспомогательного (технологического) уровня уголовно-правовых запретов, включающего нормы об ответственности за неправомерное воздействие на компьютерную информацию и информационные системы. Данные положения выполняют обеспечительную функцию, поскольку направлены на пресечение действий, которые могут выступать способом подготовки, совершения либо сокрытия дистанционных хищений, а также позволяют дать уголовно-правовую оценку тем элементам преступной деятельности, которые выходят за пределы непосредственного завладения имуществом.

Так, второй уровень системы уголовно-правовых запретов дистанционных хищений образуют нормы, предусматривающие ответственность за преступления в сфере компьютерной информации (ст. 272–274 УК РФ). Их особенность заключается в том, что они не направлены непосредственно на охрану имущественных отношений, поскольку предметом посягательства в данных составах выступает не имущество как таковое, а установленный порядок обращения, хранения, обработки и защиты компьютерной информации, а также функционирования информационных систем. Вместе с тем в условиях цифровизации именно данные нормы приобретают особое значение для противодействия дистанционным хищениям, поскольку компьютерная информация и информационные системы всё чаще выступают не только средством совершения преступления, но и самостоятельным элементом механизма преступного воздействия.

Как указывалось ранее, применительно к дистанционным хищениям положения ст. 272–274 УК РФ выполняют обеспечительную функцию, поскольку криминальное воздействие на информационную среду нередко предшествует непосредственному завладению имуществом либо обеспечивает возможность его совершения. Так, неправомерный доступ

[102] Соловьев В.С. Проблемы квалификации преступлений, совершаемых с использованием торрент-технологий // Уголовное право: стратегия развития в XXI веке. 2023. № 3. С. 109–118.

к компьютерной информации (ст. 272 УК РФ) может выражаться в получении доступа к данным, позволяющим распоряжаться чужими денежными средствами (сведениям банковских карт, данным для входа в личные кабинеты, электронным ключам доступа и иной конфиденциальной информации). При этом сам по себе факт получения такой информации ещё не всегда означает окончание хищения, однако создаёт необходимые условия для последующего противоправного обращения имущества в пользу виновного.

Особую сложность в рамках рассматриваемого исследования, как отмечалось, представляет разграничение неправомерного доступа к компьютерной информации и дистанционных хищений, совершаемых с использованием цифровых технологий. Вместе с тем самостоятельная квалификация по ст. 272 УК РФ возможна в тех случаях, когда неправомерный доступ имеет самостоятельное значение, выражается в незаконном проникновении в информационную систему и причиняет вред отношениям по обеспечению безопасности компьютерной информации, выходя за пределы непосредственного механизма хищения. В свою очередь, ст. 273 УК РФ, устанавливающая ответственность за создание, использование и распространение вредоносных компьютерных программ, имеет значение для рассматриваемой категории преступлений в связи с развитием автоматизированных способов совершения дистанционных хищений. Использование вредоносного программного обеспечения позволяет преступникам получать удалённый доступ к устройствам потерпевших, перехватывать данные авторизации, изменять параметры электронных операций либо обходить защитные механизмы информационных систем. При этом вредоносная программа выступает не самостоятельной целью преступного посягательства, а инструментом реализации имущественного умысла, что требует установления её роли в общей структуре совершённого деяния. Ст. 274 УК РФ, предусматривающая ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи

компьютерной информации, также может иметь значение при оценке отдельных случаев дистанционных посягательств, однако применяется преимущественно в ситуациях, когда вред возникает вследствие нарушения установленных правил обращения с информационными системами, а не в результате корыстного умышленного воздействия на чужое имущество. Поэтому её значение для системы дистанционных хищений является менее выраженным по сравнению со ст. 272 и 273 УК РФ.

Как видим, нормы ст. 272–274 УК РФ не являются альтернативой составам хищений, предусмотренным п. «г» ч. 3 ст. 158, ст. 159^3 и ст. 159^6 УК РФ, а формируют технологический уровень уголовно-правовой охраны, обеспечивая защиту той цифровой среды, в которой реализуется преступный механизм. Их применение требует учёта характера вмешательства в информационные системы, самостоятельности причинённого вреда и направленности умысла виновного (о проблемах разграничения указанных норм было сказано ранее). Именно такой подход позволяет избежать расширительного толкования «компьютерных составов» и обеспечить разграничение между непосредственным хищением имущества и использованием цифровых технологий как способа его совершения.

И, наконец, самостоятельное значение в системе уголовно-правовых запретов дистанционных хищений приобретает инфраструктурный (обеспечительный) уровень, представленный нормами, направленными на пресечение действий, обеспечивающих последующее распоряжение, перемещение и легализацию похищенных денежных средств. В данном контексте особое значение приобретает ст. 187 УК РФ, устанавливающая ответственность за неправомерный оборот средств платежей. Значение этой нормы для рассматриваемой сферы обусловлено тем, что современные дистанционные хищения всё чаще представляют собой не единичное действие конкретного преступника, а сложный механизм, включающий несколько взаимосвязанных этапов (получение доступа к имуществу потерпевшего, совершение операции по его изъятию, последующее

перемещение денежных средств и сокрытие их происхождения). В связи с этим уголовно-правовая охрана имущественных отношений в цифровой среде не может ограничиваться только установлением ответственности непосредственного исполнителя хищения, поскольку эффективность преступных схем во многом обеспечивается наличием лиц и инструментов, позволяющих завершить преступный умысел.

Особое значение, как было отмечено ранее, приобрели изменения, внесённые в ст. 187 УК РФ Федеральным законом от 24 июня 2025 г. № 176-ФЗ, вступившие в силу 5 июля 2025 г., которыми была усилена уголовно-правовая охрана платёжной сферы посредством установления самостоятельной ответственности за неправомерные действия с электронными средствами платежа. Указанные изменения имеют непосредственное значение для противодействия дистанционным хищениям, поскольку позволили учесть повышенную общественную опасность действий лиц, которые непосредственно не завладевают имуществом потерпевшего, однако создают условия для реализации преступного механизма путём предоставления, передачи или использования платёжных инструментов в противоправных целях[103].

В научной литературе справедливо отмечается, что развитие цифровых форм хищений обусловило усложнение структуры преступного поведения. Преступление может включать не только действия по непосредственному завладению имуществом, но и совокупность обеспечивающих операций, связанных с использованием цифровой инфраструктуры и финансовых инструментов. В связи с этим отдельного уголовно-правового внимания требуют лица, обеспечивающие движение денежных средств внутри преступной схемы, поскольку именно они позволяют сохранить анонимность участников и затруднить установление конечного выгодоприобретателя[104].

[103] Федеральный закон от 24.06.2025 № 176-ФЗ «О внесении изменений в статью 187 Уголовного кодекса Российской Федерации» [Электронный документ]. – URL: https://www.consultant.ru/document/cons_doc_LAW_508353/ (дата обращения: 12.05.2026).
[104] Васильева А.В. Дропперы в системе киберпреступности: уголовно-правовые проблемы квалификации и перспективы законодательного регулирования // Вопросы российской юстиции. 2025. № 37. С. 279-287.

Одним из наиболее распространённых проявлений такой инфраструктурной поддержки является деятельность так называемых дропперов – лиц, предоставляющих свои банковские счета, карты или иные электронные средства платежа для получения, перемещения либо обналичивания денежных средств, полученных в результате дистанционных хищений. При этом общественная опасность подобных действий заключается не только в самом факте передачи платёжного инструмента, но и в создании устойчивого механизма функционирования преступных схем, позволяющего отделить непосредственного исполнителя хищения от лица, получающего фактическую имущественную выгоду[105].

Масштаб распространения подобных практик также подтверждает необходимость самостоятельного уголовно-правового воздействия на данный элемент преступной инфраструктуры. Согласно данным Службы финансового мониторинга России, к 2025 г. в информационных массивах регулятора содержались сведения примерно о 1,2 млн лиц, связанных с использованием банковских счетов в противоправных схемах (дропперах), при этом ежемесячно выявляется около 100 тыс. счетов, используемых в подобных целях[106]. Указанные показатели свидетельствуют о том, что деятельность дропперов приобрела системный характер и фактически сформировалась как самостоятельный инфраструктурный элемент дистанционной преступности.

В совокупности эти данные позволяют сделать вывод о том, что деятельность дропперов представляет собой не случайное содействие отдельным преступлениям, а самостоятельный элемент механизма современной дистанционной преступности. Использование посредников для получения и вывода похищенных денежных средств повышает эффективность преступных схем, затрудняет раскрытие преступлений и

[105] Желудков М.А. Дропперство как новый вид соучастия в хищении денежных средств // Право: история и современность. 2025. № 3. С. 378–388; Антонов Ю.И., Костиков А.Д. Об уголовной ответственности за дропперство (чч. 3-6 ст. 187 УК РФ) // Образование и право. 2026. № 1. С. 760–766.

[106] База дроппов насчитывает 1,2 млн человек [Электронный ресурс]. – URL: https://tass.ru/ekonomika/25171949 (дата обращения 30.06.2026).

способствует сохранению анонимности участников противоправной деятельности. В свою очередь, включение положений ст. 187 УК РФ в систему противодействия дистанционным хищениям имеет самостоятельное уголовно-правовое значение, поскольку позволяет воздействовать не только на непосредственных исполнителей хищения, но и на лиц, обеспечивающих инфраструктурную поддержку преступной деятельности. Тем самым законодатель учитывает современную структуру цифровой преступности, в которой противоправное завладение имуществом всё чаще является результатом взаимодействия нескольких участников, выполняющих различные функции в рамках единого механизма.

Далее с учётом проведённого ранее исследования системы уголовно-правовых запретов в сфере дистанционных хищений, выявленных проблем их применения и предложенных направлений совершенствования представляется необходимым перейти к определению критериев разграничения п. «г» ч. 3 ст. 158 УК РФ, ст. 159^3 УК РФ и ст. 159^6 УК РФ. В связи с этим представляется целесообразным последовательно рассмотреть каждую из указанных уголовно-правовых норм с позиции выявления их специфических признаков и установления соответствующих критериев разграничения.

Ключевым критерием разграничения будет являться предмет преступного посягательства. Так, как уже отмечалось ранее, в соответствии с п. «г» ч. 3 ст. 158 УК РФ предметом преступления признаются денежные средства, находящиеся на банковском счёте, а равно электронные денежные средства. Соглашаясь с мнением отдельных исследователей, укажем, что предмет дистанционных хищений в современных условиях цифровизации и быстрых изменений имущественных отношений отличается от традиционного понимания предмета преступления как материальной вещи, на которую воздействует преступник[107].

[107] Беляков А.В., Адылин Д.М. К вопросу об объективных признаках состава преступлений, предусмотренных статьей 159^3 УК РФ // Вестник Самарского юридического института. 2023. № 1 (52). С. 29-35.

Под безналичными денежными средствами следует понимать денежные средства, существующие в форме записей на банковских счетах и используемые для осуществления расчётов посредством перевода соответствующих сумм между субъектами гражданского оборота. В соответствии со ст. 128 и 140 ГК РФ безналичные денежные средства признаются имуществом и относятся к объектам гражданских прав, несмотря на отсутствие у них вещной формы. Их специфика заключается в том, что они не обладают материальной осязаемостью, а закрепляются в информационно-учётных системах кредитных организаций, что, однако, не исключает возможности их противоправного изъятия и обращения в пользу виновного.

Электронные денежные средства, в свою очередь, имеют самостоятельную правовую регламентацию. Согласно ст. 3 ФЗ от 27.06.2011 № 161-ФЗ «О национальной платёжной системе» (с изм. и доп.) электронные денежные средства представляют собой «денежные средства, которые предварительно предоставлены одним лицом (лицом, предоставившим денежные средства) другому лицу, учитывающему информацию о размере предоставленных денежных средств без открытия банковского счета (обязанному лицу), для исполнения денежных обязательств лица, предоставившего денежные средства, перед третьими лицами и в отношении которых лицо, предоставившее денежные средства, имеет право передавать распоряжения исключительно с использованием электронных средств платежа»[108]. Приведённое законодательное определение позволяет выделить признаки электронных денежных средств, имеющие значение для уголовно-правовой оценки посягательств на них.

В первую очередь, электронные денежные средства существуют вне банковского счёта и учитываются в специализированных платёжных системах, что принципиально отличает их от безналичных денежных средств

[108] Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платёжной системе» [Электронный документ]. – URL: https://www.consultant.ru/document/cons_doc_LAW_115625/ (дата обращения: 23.03.2026).

в классическом понимании. Также их оборот осуществляется исключительно посредством электронных средств платежа, что предопределяет дистанционный характер операций с ними и повышенную уязвимость к преступным посягательствам в цифровой среде. И, наконец, правовая природа электронных денежных средств носит обязательственный характер, поскольку они выражают право требования владельца к обязанному лицу на исполнение соответствующих денежных обязательств. Указанные особенности обусловливают их самостоятельное выделение в уголовном законе в качестве предмета преступления и подчеркивают специфику дистанционных хищений, совершаемых с использованием современных платёжных технологий.

В результате электронные денежные средства представляют собой денежные ресурсы, предоставленные для использования без открытия банковского счета с применением электронных средств платежа. В отличие от них, безналичные расчеты могут осуществляться как через банковские счета, так и без них. Основное различие заключается в том, что безналичные денежные средства предполагают участие кредитной организации, тогда как электронные деньги могут «циркулировать» автономно, без обязательного участия банка. Как следствие электронное средство платежа выступает инструментом, посредством которого клиент получает возможность распоряжаться денежными средствами и инициировать переводы с использованием информационно-телекоммуникационных технологий. При этом в целом несмотря на различия в механизмах хранения и учёта, безналичные и электронные денежные средства обладают общими признаками имущественных ценностей и способны выступать предметом кражи, поскольку их незаконное списание либо иное тайное изъятие влечёт причинение реального имущественного ущерба потерпевшему. Именно этим обстоятельством обусловлено их прямое указание законодателем в диспозиции п. «г» ч. 3 ст. 158 УК РФ как самостоятельного предмета преступного посягательства.

Проводя дальнейший анализ предмета дистанционных хищений, укажем, что согласно п. 5 Постановления Пленума Верховного Суда РФ от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» (с изм. и доп.), предметом мошенничества с использованием электронных средств (ст. 159^3 УК РФ) также являются безналичные денежные средства, в том числе электронные денежные средства[109]. При этом предмет преступления, предусмотренного ст. 159^6 УК РФ, имеет более расширительное содержание.

В ст. 159^6 УК РФ предмет преступления сформулирован наиболее широко и включает чужое имущество либо право на чужое имущество[110], что подтверждается положениями п. 20 Постановления Пленума Верховного Суда РФ от 30.11.2017 № 48[111]. Вместе с тем в научной литературе указывается, что фактически дополнительным предметом данного преступления является компьютерная информация, посредством воздействия на которую осуществляется завладение имуществом[112]. Между тем указанное обстоятельство не находит отражение в разъяснениях Верховного Суда РФ, согласно которым при использовании вредоносных программ, неправомерном доступе к компьютерной информации либо ином незаконном воздействии на информационные системы действия виновного подлежат дополнительной квалификации по ст. 272–274 УК РФ при наличии соответствующих признаков[113]. Вследствие этого, соглашаясь с мнением Н.А. Лопашенко укажем, что единственным предметом преступления, предусмотренного ст. 159^6 УК РФ является чужое имущество либо право на

[109] Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 (ред. от 15.12.2022) «О судебной практике по делам о мошенничестве, присвоении и растрате» [Электронный документ]. – URL: https://www.consultant.ru/document/cons_doc_LAW_283918/ (дата обращения: 24.03.2026).
[110] Самиулина Я.В. Мошенничество в сфере компьютерной информации: проблемы законодательной регламентации // Вестник Самарского юридического института. 2023. № 3 (54). С. 62-65.
[111] Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 (ред. от 15.12.2022) «О судебной практике по делам о мошенничестве, присвоении и растрате» [Электронный документ]. – URL: https://www.consultant.ru/document/cons_doc_LAW_283918/ (дата обращения: 25.03.2026).
[112] Новикова Е.П. Отграничение мошенничества с использованием электронных средств платежа от смежных составов преступлений // Вестник ВИ МВД России. 2024. № 4. С. 204-209.
[113] Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 (ред. от 15.12.2022) «О судебной практике по делам о мошенничестве, присвоении и растрате» [Электронный документ]. – URL: https://www.consultant.ru/document/cons_doc_LAW_283918/ (дата обращения: 26.03.2026).

чужое имущество, а компьютерная информация является средством совершения данного преступления[114].

Так, предмет преступления выступает одним из ключевых дифференцирующих признаков дистанционных хищений. Для п. «г» ч. 3 ст. 158 УК РФ характерно посягательство непосредственно на денежные средства в безналичной или электронной форме, для ст. 159^3 УК РФ – на электронные денежные средства, для ст. 159^6 УК РФ – на чужое имущество и право на чужое имущество со средством в виде компьютерной информации. Однако помимо общепринятого подхода к квалификации дистанционных хищений по указанным составам при определении предмета преступлений также выделяются и проблемные вопросы.

В первую очередь, выделим проблемы с определением предмета преступления при квалификации деяний, связанных с хищением не «традиционных» безналичных и электронных денежных средств, а цифровой валюты особо распространённой в настоящее время. Следует учитывать, что термин «цифровая валюта» закреплён в российском законодательстве и используется в качестве правовой категории, определяющей соответствующий объект гражданского оборота. В свою очередь, криптовалюта представляет собой технологическую разновидность цифрового актива, основанную на применении криптографических методов и распределённых реестров. При этом категории «виртуальная валюта» и «виртуальные активы» обладают более широким содержанием, поскольку могут охватывать не только криптовалюту, но и иные цифровые объекты, имеющие экономическую ценность, в связи с чем их использование в уголовно-правовом контексте требует терминологической осторожности и дополнительной конкретизации.

Соглашаясь с мнением отдельных исследователей, отметим, что цифровой валютой (в том числе криптовалютой) можно пользоваться для

[114] Лопашенко Н.А. Компьютерное мошенничество – новое слово в понимании хищения или ошибка законодателя? // Пермский юридический альманах. 2019. № 2. С. 598-609.

осуществления реальных покупок и оплаты реальных услуг, вследствие чего она может стать объектом преступного посягательства «цифровых воров»[115]. Указанная позиция находит постепенное подтверждение у законодателя. Так, цифровая валюта, не имеющая материального (физического) выражения, определяется законодательством (ч. 3 ст. 1 Федерального закона «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» от 31.07.2020 № 259-ФЗ (с изм. и доп.)) как объект оборота в рамках гражданских правоотношений[116]. При этом она тоже признаётся современной правоприменительной практикой как объект, подлежащий уголовно-правовой защите. Конституционный Суд РФ в Постановлении от 20.01.2026 № 2-П подтвердил, что имущественные права на цифровую валюту подлежат судебной защите, и отказ в защите по формальным основаниям (например, отсутствию уведомления налоговых органов) нарушает право на судебную защиту, гарантированное Конституцией РФ[117]. Такое толкование также укрепляет идею о том, что право собственности на цифровые финансовые активы не может быть «выброшено» за рамки уголовно-правовой охраны от хищений только из-за отсутствия материальной формы. Кроме того, согласно материалам судебной практики, это «нелегальное» платёжное средство активно используется участниками организованных преступных группировок при осуществлении сбыта наркотических средств[118], а выборочные данные социологического опроса, проведённого к.ю.н.

[115] Юсупова А.Ф. Криптовалюта как предмет преступления, предусмотренного п. «г» ч. 3 ст. 158 УК РФ // Вопросы российской юстиции. 2023. № 26. С. 444-450.

[116] Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» (с изм. и доп.) [Электронный документ]. URL: https://www.consultant.ru/document/cons_doc_LAW_358753/ (дата обращения: 27.03.2026).

[117] Постановление Конституционного Суда РФ от 20.01.2026 № 2-П «По делу о проверке конституционности части 6 статьи 14 Федерального закона "О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации" в связи с жалобой гражданина Тимченко Дмитрия Игоревича» [Электронный документ]. – URL: https://www.consultant.ru/document/cons_doc_LAW_524655/ (дата обращения: 28.03.2026).

[118] См., например: Приговор № 1-164/2023 1-4/2024 от 30 января 2024 г. по делу № 1-164/2023, О. районный суд г. Барнаула (Алтайский край) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/pyNbXiWS6dYR/ (дата обращения: 29.03.2026); Приговор № 1-363/2022 1-37/2023 1-5/2024 от 30 января 2024 г. по делу № 1-363/2022, О. районный суд г. Рязани (Рязанская область) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/d9uYFORTGB6c/ (дата обращения: 30.03.2026).

Г.Р. Григоряном, свидетельствуют, что 58% опрошенных исследователей признают криптовалюту в современности предметом дистанционных хищений[119]. В свою очередь, отдельные учёные прямо отмечают, что цифровая валюта, наряду с вещами, имеющими материальную форму объектами, а также безналичными денежными средствами в современности может выступать предметом преступлений против собственности, в том числе хищений, совершаемых дистанционно[120].

Так, соглашаясь с данным утверждением, считаем, что цифровая валюта (в том числе криптовалюта) может выступать предметом дистанционных хищений, поскольку обладает имущественной ценностью, возможностью экономического оборота и фактической способностью выступать объектом противоправного завладения. Специфика цифровых активов при этом заключается в отсутствии традиционной материальной формы, а также в особенностях их хранения, передачи и контроля посредством информационных систем, что обусловливает необходимость учёта особенностей цифровой среды при уголовно-правовой оценке соответствующих деяний.

Данный подход получил нормативное подтверждение в обновлённых разъяснениях Верховного Суда Российской Федерации (Постановлением Пленума Верховного Суда РФ от 16.06.2026 № 19 были внесены изменения в Постановление Пленума ВС РФ от 27.12.2002 № 29 «О судебной практике по делам о краже, грабеже и разбое»[121]), в соответствии с которыми к предмету хищения отнесены не только традиционные объекты имущественных отношений, но и цифровая валюта, цифровые права и иные цифровые активы. Указанное разъяснение имеет принципиальное значение для

---

[119] Григорян Г.Р. Мошенничество в сфере компьютерной информации: проблемы криминализации, законодательной регламентации и квалификации: автореф. дис. ... канд. юрид. наук: 12.00.08. – Самара, 2021. С. 17.

[120] Телеш Н.С. Цифровая валюта (криптовалюта) как предмет хищения // Вестник науки. 2024. № 6 (75). С. 714-717.

[121] Постановление Пленума Верховного Суда РФ от 27.12.2002 № 29 (ред. от 15.12.2022) «О судебной практике по делам о краже, грабеже и разбое» [Электронный документ]. – URL: https://www.consultant.ru/document/cons_doc_LAW_40412/ (дата обращения: 31.03.2026).

развития практики квалификации дистанционных хищений, поскольку устраняет существовавшую ранее неопределённость относительно возможности признания цифровых активов предметом преступного посягательства. Вместе с тем, само признание цифровой валюты предметом хищения не устраняет всех проблем её уголовно-правовой оценки. В отличие от традиционных объектов имущественных отношений, цифровые активы существуют в рамках информационной среды, а возможность распоряжения ими определяется наличием доступа к соответствующим цифровым ключам, аккаунтам либо иным средствам идентификации владельца. В связи с этим остаются актуальными вопросы разграничения способов завладения цифровыми активами, а также установления критериев квалификации действий виновного в зависимости от характера воздействия на цифровую инфраструктуру. И отдельную сложность представляет определение размера ущерба, обусловленное высокой волатильностью курса подобных цифровых активов и отсутствием их официального курса, устанавливаемого Банком России. В этой связи представляется обоснованным ориентироваться на рыночные котировки соответствующих цифровых активов, формируемые на ведущих криптовалютных биржах и агрегаторах цен, отражающих средневзвешенную стоимость на момент совершения преступления либо фактического выбытия такой цифровой валюты из владения потерпевшего, с учётом конкретных обстоятельств дела и сложившейся правоприменительной практики. В связи с этим представляется необходимым дальнейшее уточнение положений Постановления Пленума Верховного Суда РФ от 27.12.2002 № 29 «О судебной практике по делам о краже, грабеже и разбое» с учётом особенностей цифровой валюты как предмета дистанционных хищений. Реализация указанного подхода позволит обеспечить единообразие судебной практики и сформировать более устойчивые критерии уголовно-правовой оценки дистанционных хищений в условиях цифровизации имущественного оборота.

При этом предмет дистанционного хищения не ограничивается денежными средствами и иными цифровыми активами. В частности, применительно к мошенничеству в сфере компьютерной информации, предусмотренному ст. 159[6] УК РФ, предметом может выступать любое чужое имущество либо право на чужое имущество, завладение которым стало возможным вследствие предусмотренного законом неправомерного воздействия на компьютерную информацию или функционирование соответствующих средств и сетей. Поэтому использование компьютерных технологий при совершении хищения само по себе не превращает похищаемое имущество в «цифровой» предмет, и цифровой характер может относиться к способу совершения преступления, тогда как предметом остаётся соответствующее имущество или право на него.

Другим возможным предметом дистанционных хищений в настоящее время можно признать современные виртуальные валюты, которые представляют собой своеобразные электронные денежные средства, используемые, например, для продажи и приобретения виртуальных товаров на разных интернет-платформах[122] или для получения бонусов торговой организации, хотя их юридический статус на законодательном уровне и не определён. При этом отдельно стоит заметить, что такая валюта приобретается за реальные денежные средства, являющиеся легальной денежной единицей в РФ, и конвертируется в неё (если речь идёт об обратном процессе), а значит, в результате неправомерного завладения такой виртуальной валютой лицу будет нанесён реальный материальный ущерб. В качестве примера приведём дело гражданки А., которая, работая в качестве оператора на АЗС и зная о проведении акции «Топливо за бонусы», путем обмана регистрировала карты лояльности на вымышленных лиц и начисляла при оплате клиентами на них бонусы. В результате гражданка А. применяла данные бонусы при расчете за топливо и таким образом извлекала

[122] Киктенко А.А. Предмет преступления, предусмотренного п. «г» ч. 3 ст. 158 Уголовного кодекса Российской федерации // Вестник РУК. 2022. № 3 (49). С. 103-107.

материальную выгоду. Однако судом в качестве предмета такого дистанционного хищения было признано топливо[123]. Вследствие этого считаем, что и подобную виртуальную, и цифровую (в том числе, криптовалюту) можно признать предметом дистанционного хищения, и активное развитие информационной сферы и проникновение в эту сферу всё новых и новых суррогатов денежных средств требует оперативного обновления отечественного законодательства в соответствии с запросами времени[124].

Таким образом, предмет дистанционных хищений выступает не только формально-юридическим элементом состава преступления, но и важнейшим признаком, позволяющим разграничивать кражу с банковского счёта (п. «г» ч. 3 ст. 158 УК РФ), мошенничество с использованием электронных средств платежа (ст. 159^3 УК РФ) и мошенничество в сфере компьютерной информации (ст. 159^6 УК РФ). При этом цифровая форма существования имущества не должна отождествляться с цифровым способом совершения хищения.

Объективная сторона дистанционных хищений также выступает одним из ключевых критериев, позволяющих разграничить кражу и различные формы мошенничества в условиях цифровой среды. Специфика данных преступлений обусловлена тем, что противоправное завладение имуществом осуществляется не посредством прямого физического воздействия на объект посягательства, а через использование информационно-телекоммуникационных технологий.

Так, для преступления, предусмотренного п. «г» ч. 3 ст. 158 УК РФ, характерен тайный способ хищения денежных средств, находящихся на банковском счёте либо в форме электронных денежных средств. Существенным признаком объективной стороны рассматриваемого состава

[123] Ермакова О.В. Вопросы обоснованности законодательной регламентации преступлений против собственности, совершаемых в сфере IT-технологий // Вестник Сибирского юридического института МВД России. 2023. № 2 (51). С. 23-29.
[124] Лещенко В.П. Предмет мошенничества с использованием электронных средств платежа // Гуманитарные, социально-экономические и общественные науки. 2019. № 2. С. 92-95.

является тайный характер изъятия денежных средств с банковского счёта либо в отношении электронных денежных средств без непосредственного взаимодействия с потерпевшим.

В свою очередь, объективная сторона преступления, предусмотренного ст. 159^3 УК РФ, выражается в хищении чужих денежных средств посредством использования электронных средств платежа. Как отмечалось ранее, в соответствии с п. 19 ст. 3 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платёжной системе» электронное средство платежа (заменившее собой в 2018 г. понятие «платежные карты» и охватывающее более широкий спектр инструментов, включая электронные кошельки, платежные приложения, банковские карты и устройства для дистанционных переводов) представляет собой средство или способ, позволяющий составлять, удостоверять и передавать распоряжения о переводе денежных средств с применением информационно-телекоммуникационных технологий и электронных носителей информации. К таким средствам относятся не только банковские карты, но и электронные кошельки, мобильные платёжные приложения и иные технические устройства[125]. Электронное средство платежа обладает следующими признаками: участие клиента и оператора перевода денежных средств; предоставление клиенту возможности отдавать распоряжения о переводе денежных средств; использование форм безналичных расчетов; применение информационно-телекоммуникационных технологий; использование электронных носителей информации, включая платежные карты и иные технические устройства. Следует отметить, что электронное средство платежа рассматривается законодательством как исключительное средство управления электронными денежными средствами. Банкомат, в свою очередь, выступает лишь как вспомогательный инструмент, обеспечивающий возможность снятия наличных с использованием электронных средств платежа. Так, уголовно-правовая квалификация деяния

[125] Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платёжной системе» [Электронный документ]. – URL: https://www.consultant.ru/document/cons_doc_LAW_115625/ (дата обращения: 01.04.2026).

строится на воздействии именно на электронное средство платежа, а не на денежные средства в их материальной форме[126]. При этом особо стоит подчеркнуть, что в отличие от кражи, при мошенничестве по ст. 159^3 УК РФ завладение денежными средствами осуществляется путём введения в заблуждение владельца либо иного лица, участвующего в платёжной операции, что придаёт деянию характер активного обмана, реализуемого в дистанционной форме.

Наиболее сложной по конструкции является объективная сторона преступления, предусмотренного ст. 159^6 УК РФ. Она включает действия по завладению чужим имуществом либо приобретению права на него посредством обмана или злоупотребления доверием, совершённые путём ввода, удаления, блокирования или модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. Понятие компьютерной информации и информационно-телекоммуникационной сети раскрывается в Федеральном законе от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изм. и доп.)[127]. При этом отдельно подчеркнём, что указанные способы воздействия охватывают широкий спектр неправомерных действий – от внедрения вредоносного кода до манипулирования данными в автоматизированных системах, что придаёт данному составу преступления выраженный технологический характер. Особенностью объективной стороны ст. 159^6 УК РФ является то, что обман реализуется опосредованно – через воздействие на информационные системы, в результате чего вводится в заблуждение не столько конкретное лицо, сколько автоматизированный механизм обработки

[126] Матюхина Т.И., Ивлев К.А. Электронные средства платежа как средство совершения преступления, предусмотренного ст. 159^3 Уголовного кодекса РФ // Universum: экономика и юриспруденция. 2025. № 1 (123). С. 54-56.

[127] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный документ]. – URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 02.04.2026).

информации, что справедливому замечанию отдельных исследователей несколько «размывает» «классическое» понимание хищения, создавая некоторую правовую неопределённость[128].

Как видим, принципиальное различие между рассматриваемыми составами определяется не самим фактом использования информационно-телекоммуникационных технологий, а тем, каким образом они включены в механизм завладения имуществом. При квалификации по п. «г» ч. 3 ст. 158 УК РФ потерпевший не участвует в передаче денежных средств и не совершает действий, направленных на их отчуждение (денежные средства изымаются виновным тайно и помимо воли их владельца). При мошенничестве, предусмотренном ст. 159^3 УК РФ, напротив, потерпевший либо иное лицо, участвующее в платёжной операции, совершает юридически значимое действие по распоряжению денежными средствами, однако делает это вследствие обмана или злоупотребления доверием, а обязательным специальным признаком является использование электронного средства платежа. В ст. 159^6 УК РФ завладение имуществом достигается уже иным способом, виновный воздействует на компьютерную информацию либо на функционирование соответствующей информационной системы, вследствие чего имущественный результат достигается без формирования у потерпевшего ошибочного представления о фактических обстоятельствах передачи имущества.

Для разграничения указанных составов необходимо устанавливать прежде всего непосредственный механизм перехода имущества в распоряжение виновного: при краже – изъятие имущества помимо воли потерпевшего; при мошенничестве с использованием электронного средства платежа – передача имущества самим потерпевшим либо иным участвующим в операции лицом под воздействием обмана или злоупотребления доверием; при мошенничестве в сфере компьютерной информации – завладение

[128] Недиков В.Б. Проблемные вопросы уголовной ответственности за интернет-мошенничество: опыт России и Германии // Вопросы российской юстиции. 2024. № 33. С. 394-410.

имуществом, обусловленное неправомерным воздействием на компьютерную информацию или функционирование информационной системы. Следовательно, использование банковского приложения, сети Интернет, мобильного устройства или иного цифрового инструмента само по себе не предопределяет квалификацию, определяющим является его функциональное значение в механизме совершения хищения. Именно данный критерий позволяет разграничить дистанционные хищения в случаях, когда внешне сходные способы используются для достижения различного уголовно-правового результата.

Самостоятельное значение для разграничения данных составов основного уровня имеет характеристика субъекта и субъективной стороны соответствующих составов преступлений. Для п. «г» ч. 3 ст. 158 УК РФ субъект преступления является общим. Им признаётся вменяемое физическое лицо, достигшее возраста уголовной ответственности, то есть 14 лет, что вытекает из общего правила, установленного ч. 2 ст. 20 УК РФ для кражи. Субъективная сторона кражи с банковского счёта либо электронных денежных средств выражается исключительно в форме прямого умысла и корыстной цели. При этом специфика дистанционного способа совершения кражи не изменяет психического отношения виновного к содеянному, однако осложняет доказывание осознания именно тайного характера хищения в условиях опосредованного доступа к имуществу.

Субъект мошенничества с использованием электронных средств платежа, предусмотренного ст. 159^3 УК РФ, также является общим и представлен вменяемым физическим лицом, достигшим 16-летнего возраста. Соответствующий возрастной «порог» обусловлен отнесением данного состава к мошенничеству, ответственность за которое наступает по общему правилу. Субъективная сторона данного преступления также характеризуется прямым умыслом и корыстным мотивом. Лицо осознаёт, что путём использования электронного средства платежа, не принадлежащего ему либо используемого без законных оснований, вводит в заблуждение участников

платёжных отношений и незаконно завладевает денежными средствами, и желает их противоправного обращения в свою пользу либо в пользу третьих лиц. Существенным является то, что психическое отношение виновного направлено не только на изъятие имущества, но и на использование обманного механизма, встроенного в процедуру электронных расчётов.

И, наконец, субъект преступления, предусмотренного ст. 159^6 УК РФ, тоже является общим. Это вменяемое физическое лицо, достигшее 16-летнего возраста. Специальных признаков субъект не имеет, несмотря на то что фактическое совершение данного преступления зачастую требует специальных технических навыков. Субъективная сторона мошенничества в сфере компьютерной информации тоже выражается в прямом умысле и корыстном мотиве. Виновный осознаёт, что посредством неправомерного воздействия на компьютерную информацию или функционирование информационных систем осуществляет обман и незаконно завладевает чужим имуществом либо приобретает право на него, и желает наступления соответствующих последствий. При этом особенностью данного состава является опосредованный характер обмана, реализуемого через воздействие на информационные технологии, что нередко вызывает сложности в разграничении его с иными формами хищений[129].

Так, субъект и субъективная сторона дистанционных хищений (по п. «г» ч. 3 ст. 158, ст. 159^3 и ст. 159^6 УК РФ) во многом совпадают по своим формально-юридическим признакам, однако различаются по возрасту привлечения к уголовной ответственности и направленности умысла, что в совокупности с иными элементами состава приобретает значение дифференцирующего критерия. При этом установление законодателем различного возраста уголовной ответственности (14 лет – для кражи, предусмотренной п. «г» ч. 3 ст. 158, и 16 лет – для мошенничества, включая его специальные составы) носит не формальный, а содержательный характер

[129] Ханнанова Д.Р., Штефан А.В. Противодействие хищения в сфере компьютерной информации уголовно-правовыми средствами // Вестник магистратуры. 2025. № 5-1 (164). С. 89–93.

и обусловлено различной степенью социальной и интеллектуальной сложности соответствующих способов преступного поведения. Так, дистанционные кражи в их «персонализированной» форме предполагают более раннюю криминальную доступность, тогда как дистанционные мошенничества требуют более высокого уровня когнитивной оценки ситуации, умения формировать и поддерживать обманную коммуникацию либо управлять цифровой средой с целью введения потерпевшего в заблуждение.

Квалифицирующие признаки дистанционных хищений также выступают важным инструментом дифференциации уголовной ответственности и позволяют учесть повышенную общественную опасность соответствующих посягательств, обусловленную как способом совершения преступления, так и особенностями предмета хищения. Для преступлений, предусмотренных п. «г» ч. 3 ст. 158, ст. 159^3 и ст. 159^6 УК РФ, система квалифицирующих обстоятельств в целом носит сходный характер, однако имеет и принципиальные отличия, отражающие специфику каждой уголовно-правовой конструкции.

Для кражи, совершённой с банковского счёта либо в отношении электронных денежных средств (п. «г» ч. 3 ст. 158 УК РФ), квалифицирующий признак закреплён уже на уровне части третьей указанной статьи. Сам факт посягательства на безналичные или электронные денежные средства законодатель рассматривает как обстоятельство, существенно повышающее общественную опасность деяния. Это обусловлено, с одной стороны, высокой латентностью таких преступлений, а с другой – значительным ущербом, который может быть причинён потерпевшему в краткий промежуток времени вследствие дистанционного способа изъятия имущества. Дополнительное усиление ответственности предусмотрено в ч. 4 ст. 158 УК РФ, где в качестве особо квалифицирующих признаков названы совершение кражи организованной группой либо в особо крупном размере. В ст. 159^3 УК РФ (мошенничество с использованием

электронных средств платежа) квалифицирующие признаки выстроены по «классической» для мошенничества модели. Уже в ч. 2 данной статьи предусмотрена ответственность за совершение деяния группой лиц по предварительному сговору либо с причинением значительного ущерба гражданину. Эти обстоятельства отражают повышенную степень координации преступных действий и усиление негативных последствий для потерпевшего. В ч. 3 ст. 159^3 УК РФ законодатель дополнительно выделяет такие квалифицирующие признаки, как использование виновным своего служебного положения и совершение преступления в крупном размере, что указывает на злоупотребление профессиональным или должностным статусом и значительный масштаб имущественного ущерба. Наивысшая степень общественной опасности закреплена в ч. 4 ст. 159^3 УК РФ, предусматривающей ответственность за совершение преступления организованной группой либо в особо крупном размере. Применительно к дистанционным хищениям данные признаки нередко сочетаются, что свидетельствует о системном и организованном характере преступной деятельности. Квалифицирующие признаки мошенничества в сфере компьютерной информации (ст. 159^6 УК РФ) во многом дублируют конструкцию ст. 159^3 УК РФ, однако обладают дополнительной спецификой. Так, помимо группового характера преступления, значительного ущерба, использования служебного положения, крупного и особо крупного размера, в ч. 3 ст. 159^6 УК РФ прямо выделено совершение деяния с банковского счёта либо в отношении электронных денежных средств. Тем самым законодатель подчёркивает повышенную опасность тех случаев, когда неправомерное вмешательство в компьютерную информацию непосредственно направлено на завладение денежными средствами в цифровой форме. Особо квалифицированный состав, как и в иных статьях о мошенничестве, образуют деяния, совершённые организованной группой либо в особо крупном размере.

Так, квалифицирующие признаки дистанционных хищений выполняют двойственную функцию. С одной стороны, они усиливают уголовно-правовую реакцию на наиболее опасные формы преступного поведения в цифровой среде, а с другой – служат дополнительным критерием при разграничении кражи с банковского счёта и различных видов мошенничества.

Момент окончания дистанционных хищений определяется в зависимости от способа их совершения и конструктивных признаков конкретного состава преступления. При краже с банковского счёта (п. «г» ч. 3 ст. 158 УК РФ) преступление считается оконченным с момента неправомерного списания (изъятия) денежных средств со счёта потерпевшего, то есть с момента завершения банковской операции, в результате которой денежные средства утрачивают контроль со стороны законного владельца и поступают в распоряжение иного лица либо становятся доступными для такого распоряжения, при этом с учётом изменений, действующих с 16.06.2026, окончание преступления связывается с фактом необратимого исполнения платёжного распоряжения в информационной системе банка, независимо от последующего фактического обналичивания или получения денежных средств виновным. При мошенничестве (ст. 159^3 УК РФ) момент окончания связывается с совершением потерпевшим под влиянием обмана либо злоупотребления доверием юридически значимых действий по переводу денежных средств или иному их отчуждению, при условии фактического списания денежных средств с его счёта и их зачисления на счёт, указанный виновным, при этом с 16.06.2026 ключевое значение приобретает момент завершения платёжной транзакции в банковской системе, а не последующее фактическое распоряжение полученными средствами виновным. В случае мошенничества в сфере компьютерной информации (ст. 159^6 УК РФ) преступление признаётся оконченным с момента неправомерного вмешательства в работу компьютерной информации или информационных систем, повлёкшего

безвозмездное изъятие имущества либо приобретение права на него, независимо от последующего фактического получения денежных средств виновным, при этом уточняется, что таким моментом следует считать завершение несанкционированной модификации (блокирования, копирования либо уничтожения) данных, повлекшей изменение режима доступа к имуществу или цифровым активам потерпевшего.

В результате анализ представленных элементов рассматриваемых составов преступлений основного уровня уголовно-правовых средств противодействия дистанционным хищениям позволяет установить алгоритм разграничения указанных преступных деяний. Определяющим критерием выступает предмет преступного посягательства. Так, при посягательстве непосредственно на денежные средства, находящиеся на банковском счёте либо в форме электронных денежных средств, при отсутствии признаков обмана или вмешательства в информационные системы, содеянное подлежит квалификации по п. «г» ч. 3 ст. 158 УК РФ; при использовании электронных средств платежа как инструмента обмана – по ст. 159^3 УК РФ; при посягательстве на имущество или право на него, реализуемом посредством воздействия на компьютерную информацию, – по ст. 159^6 УК РФ. Следующим критерием является характер объективной стороны (тайное изъятие денежных средств без вовлечения потерпевшего в процесс принятия решения свидетельствует о краже; использование обмана, реализуемого через процедуры электронных расчётов, – о мошенничестве с использованием электронных средств платежа; целенаправленное вмешательство в функционирование информационных систем, включая модификацию, блокирование или иное воздействие на компьютерную информацию, – о мошенничестве в сфере компьютерной информации. При этом предлагается исходить не из формального использования технических средств, а из сущности воздействия на объект посягательства. Субъект и субъективная сторона рассматриваемых составов основного уровня дистанционных хищений в целом обладают единообразием базовых

признаков (общий субъект и прямой умысел с корыстной целью), различаясь главным образом по возрасту уголовной ответственности и специфике интеллектуально-волевого отношения виновного к способу совершения преступления. Момент окончания преступления, предусмотренного соответствующими статьями, определяется следующим образом. Так, при краже с банковского счёта – с момента неправомерного списания денежных средств, при мошенничестве – с момента совершения потерпевшим под влиянием обмана либо злоупотребления доверием действий по их переводу или иному отчуждению, при мошенничестве в сфере компьютерной информации – с момента неправомерного воздействия на информационные системы, повлёкшего изъятие имущества либо приобретение права на него. В свою очередь, квалифицирующие признаки конкретизируют степень общественной опасности деяния, однако их частичное совпадение требует системного толкования и недопущения конкуренции норм.

Отдельного внимания требует разграничение указанных составов с преступлениями, предусмотренными ст. 272–274 и ст. 187 УК РФ (преступлениями технологического и инфраструктурного уровней соответственно). В отличие от дистанционных хищений, где компьютерная информация, электронные средства платежа и цифровые сервисы выступают либо предметом посягательства, либо способом изъятия имущества, составы гл. 28 УК РФ (ст. 272–274) направлены на охрану общественных отношений в сфере безопасного функционирования компьютерной информации и информационных систем и характеризуются отсутствием обязательного корыстного результата в виде безвозмездного обращения чужого имущества. В свою очередь, ст. 187 УК РФ охватывает деяния «дропперского» характера и иные операции с электронными средствами платежа, которые сами по себе не всегда образуют хищение, однако могут выступать последующим этапом его реализации либо обеспечивать легализацию и обналичивание похищенных средств. Как видим, при конкуренции указанных норм решающее значение имеет направленность умысла. Квалификация по

ст. 272–274 либо ст. 187 УК РФ исключается в случаях, когда неправомерное воздействие на компьютерную информацию либо оборот электронных средств платежа функционально включены в механизм изъятия имущества и образуют способ совершения хищения. В таких ситуациях указанные действия не обладают самостоятельным уголовно-правовым значением и поглощаются составами дистанционных хищений (п. «г» ч. 3 ст. 158, ст. 159^3, ст. 159^6 УК РФ). Напротив, самостоятельная квалификация по ст. 272–274 либо ст. 187 УК РФ возможна лишь при отсутствии направленности на безвозмездное обращение чужого имущества и при наличии автономного посягательства на информационную безопасность, либо порядок оборота электронных средств платежа.

Таким образом, система уголовно-правовых запретов в сфере дистанционных хищений не образует самостоятельной главы УК РФ и представляет собой структурно-уровневую совокупность взаимосвязанных норм, интегрированных в классические уголовно-правовые институты, при этом её внутреннее строение может быть охарактеризовано как многоуровневая модель уголовно-правовой охраны, обусловленная различной функциональной ролью соответствующих норм в механизме противодействия дистанционным хищениям. Основной уровень образуют составы, непосредственно предусматривающие ответственность за хищение (п. «г» ч. 3 ст. 158, ст. 159^3, ст. 159^6 УК РФ). Вспомогательный (технологический) уровень включают нормы, обеспечивающие уголовно-правовую охрану цифровой среды и противодействие неправомерному воздействию на компьютерную информацию (ст. 272–274 УК РФ). И наконец, инфраструктурный уровень составляют нормы, регламентирующие ответственность за незаконный оборот электронных средств платежа и операции с похищенными активами (ст. 187 УК РФ). Данная конструкция позволяет рассматривать уголовно-правовое противодействие дистанционным хищениям не как совокупность разрозненных норм, а как системно организованный механизм, в котором каждый уровень выполняет

самостоятельную функцию в обеспечении охраны имущественных отношений в цифровой среде. При этом правоприменитель, в первую очередь, опирается на специальные составы дистанционных хищений (п. «г» ч. 3 ст. 158, ст. 159^3, ст. 159^6 УК РФ), тогда как нормы общего характера применяются субсидиарно либо при отсутствии признаков хищения. Вместе с тем практическая реализация данной системы осложняется динамичным развитием цифровых технологий и необходимостью более оперативной адаптации уголовного закона к новым способам противоправного воздействия, что обусловливает актуальность дальнейшего совершенствования указанных уголовно-правовых механизмов с учётом их многоуровневой структуры.

2.2. Наказуемость хищений, совершённых дистанционно

Наказуемость как признак преступления выражает установленную законом возможность применения мер уголовной ответственности, содержание и пределы которых предопределяются оценкой степени общественной опасности деяния с учётом его объекта, способа совершения, характера причинённого ущерба и иных юридически значимых обстоятельств. Вместе с тем, в условиях цифровизации общественных отношений и стремительного развития информационно-телекоммуникационных технологий, как уже указывалось неоднократно, проблема наказуемости дистанционных хищений приобретает особую остроту. Усложнение механизмов совершения преступлений, их многоэтапный и технологически опосредованный характер, рост латентности и устойчивое увеличение масштабов подобных посягательств свидетельствуют о качественной трансформации криминальных угроз в сфере собственности[130]. Одновременно это выявляет ряд существенных проблем в действующей системе уголовно-правовых наказаний, в связи

[130] Соколов Н.А., Георгиевская В.Х. Дистанционные мошенничества с использованием средств массовой информации // Журнал прикладных исследований. 2025. № 10. С. 207-211.

с этим находим необходимым перейти к детальному рассмотрению действующей санкционной политики с целью выявления направлений её дальнейшего совершенствования.

Особый интерес в этой связи представляет сопоставление объёма и характера наказаний, установленных за кражу с банковского счёта или электронных денежных средств (п. «г» ч. 3 ст. 158 УК РФ), мошенничество с использованием электронных средств платежа (ст. 159^3 УК РФ) и мошенничество в сфере компьютерной информации (ст. 159^6 УК РФ) – преступлений «основного уровня». Исследование структуры санкций, их пределов и соотношения с квалифицирующими признаками позволит оценить степень адекватности уголовно-правовой реакции на дистанционные формы хищений, выявить существующие диспропорции в системе наказаний и определить направления её дальнейшего совершенствования.

Обратимся к характеристике санкции, предусмотренной п. «г» ч. 3 ст. 158 УК РФ, как к элементу, отражающему уголовно-правовую оценку повышенной общественной опасности посягательств на безналичные и электронные денежные средства. Санкция указанной нормы носит альтернативный характер и включает в себя несколько видов уголовных наказаний, различающихся по степени строгости и репрессивного воздействия: штраф, принудительные работы и лишение свободы. Каждое из наказаний может дополняться ограничением свободы либо штрафом в качестве дополнительного наказания. Такая конструкция санкции соответствует общим началам назначения наказания, закреплённым в ст. 60 УК РФ, и ориентирует суд на индивидуализацию уголовной ответственности с учётом характера и степени общественной опасности совершённого деяния, личности виновного и обстоятельств дела.

Назначение штрафа в значительном размере (от ста тысяч до пятисот тысяч рублей либо в размере дохода осуждённого за период от одного года до трёх лет) свидетельствует о признании имущественного характера причинённого вреда и направлено, прежде всего, на компенсационное и

превентивное воздействие. Вместе с тем включение в санкцию принудительных работ и лишения свободы подчёркивает, что кража с банковского счёта либо электронных денежных средств рассматривается законодателем не как формальное имущественное правонарушение, а как тяжкое преступление против собственности, способное причинить существенный ущерб как конкретному лицу, так и стабильности экономических отношений в целом. Максимальный предел лишения свободы, установленный на уровне шести лет, относит данный состав к категории тяжких преступлений, что влечёт соответствующие уголовно-правовые последствия, в том числе в части сроков давности, возможности применения условного осуждения и иных институтов. Дополнительное наказание в виде ограничения свободы усиливает контроль за поведением осуждённого после отбытия основного наказания и направлено на предупреждение повторных преступлений, в том числе совершаемых с использованием цифровых технологий.

Наиболее значимой проблемой для указанной нормы является отсутствие минимального стоимостного порога причинённого ущерба, при котором хищение с банковского счёта либо электронных денежных средств признаётся уголовно наказуемым деянием.

Как известно, в рамках общего состава кражи (ч. 1 ст. 158 УК РФ) законодатель, во взаимосвязи с положениями КоАП РФ, фактически исключил уголовную ответственность за хищение имущества на сумму до 2 500 рублей, отнеся такие деяния к административным правонарушениям. Тайные хищения чужого имущества на сумму менее 2 500 рублей влекут наступление уголовной ответственности только в том случае, если данное лицо ранее было подвергнуто административному наказанию за мелкое хищение, предусмотренное ч. 2 ст. 7.27 КоАП РФ на сумму от 1 000 до 2 500

рублей[131]. В этом случае лицо согласно ст. 158.1 УК РФ может быть приговорено к наказанию в виде лишения свободы на срок до 1 года. Так, к примеру, гражданин Н., подвергшийся ранее административному наказанию по ч. 2 ст. 7.27 КоАП РФ, был осуждён Приговором С. городского суда (Томская область) № 1-410/2023 1-78/2024 от 27 февраля 2024 г. по делу № 1-410/2023 за совершение кражи в торговом зале магазина на сумму 873 рубля 75 копеек и приговорён к лишению свободы на срок 4 месяца[132]. В то же время кража с найденной гражданином Р. чужой банковской карты безналичных денежных средств путём бесконтактной оплаты в магазине продуктов на практически в два раза меньшую денежную сумму (около 400 рублей) в соответствии с Приговором № 1-460/2023 1-71/2024 от 28 февраля 2024 г. по делу № 1-460/2023 З. районного суда г. Смоленска в соответствии с устоявшейся уголовно-правовой доктриной была квалифицирована по п. «г» ч. 3 ст. 158 УК РФ. В результате этого осуждённый, не применявший никаких специальных знаний, умений и навыков в сфере информационных технологий был приговорён к 1,5 годам лишения свободы[133]. Как видим, значительного усовершенствования в способе совершения кражи в данном случае не произошло (ввиду общей тенденции перехода к цифровым отношениям во всех сферах общественной жизни), однако наказание за совершение такого тайного хищения, по верному утверждению отдельных исследователей, существенно ужесточилось[134], при том что использование банковских карт и бесконтактных платежей стало повсеместным и фактически обыденным способом расчётов, не предполагающим ни технической сложности, ни

[131] Постановление Пленума Верховного Суда РФ от 27.12.2002 № 29 (ред. от 15.12.2022) «О судебной практике по делам о краже, грабеже и разбое» [Электронный документ]. – URL: https://www.consultant.ru/document/cons_doc_LAW_40412/ (дата обращения: 03.04.2026).

[132] Приговор № 1-410/2023 1-78/2024 от 27 февраля 2024 г. по делу № 1-410/2023, С. городской суд (Томская область) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/0UaLOHMJJD57/ (дата обращения: 02.02.2026).

[133] Приговор № 1-460/2023 1-71/2024 от 28 февраля 2024 г. по делу № 1-460/2023, З. районный суд г. Смоленска (Смоленская область) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/21yaWYl3f4da/ (дата обращения: 03.02.2026).

[134] Назаренко Г.В. Курьёзы толкования уголовно-правовых норм, предусматривающих ответственность за кражу // Вестник ЮГУ. 2023. № 2 (69). С. 81-86.

повышенного уровня общественной опасности по сравнению с традиционными формами тайного хищения.

В связи с этим считаем, что существующее нормативное решение вступает в очевидное противоречие с дифференциацией уголовной ответственности по имущественным преступлениям, выстроенной законодателем в иных составах. Фактически решающим критерием уголовной наказуемости в данном случае становится не размер причинённого вреда, а исключительно способ его причинения – дистанционный, связанный с использованием банковского счёта или электронных денежных средств, но не всегда имеющий, действительно, высоко технологический характер (как, например, в случае с оплатой покупок на незначительные денежные суммы бесконтактным способом чужой банковской картой без подтверждения пароля)[135]. Вследствие этого считаем важным пересмотреть отношение к кражам, осуществляемым бесконтактным способом с банковских карт на незначительную денежную сумму и квалифицируемым по п. «г» ч. 3 ст. 158 УК РФ, определив идентичные «традиционным» тайным хищениям чужого имущества основания для квалификации совершаемых деяний согласно устоявшейся правовой доктрине. Для этого находим необходимым нормативное закрепление стоимостного порога применительно к указанной норме, который предлагается установить в размере до 2 500 рублей, с отнесением таких деяний при отсутствии квалифицирующих признаков к категории малозначительных либо административно наказуемых.

Отдельно укажем, что обращение к стоимостному критерию в данном случае обусловлено прежде всего необходимостью оценки соразмерности уголовно-правового воздействия характеру и степени общественной опасности рассматриваемых деяний. Бесспорно, предлагаемое установление такого критерия затрагивает вопросы криминализации, однако в этой ситуации рассматривается преимущественно с позиций дифференциации

[135] Федоренко К.Ю. Проблемы разграничения кражи с банковского счета и мошенничества // Вопросы российской юстиции. 2025. № 37. С. 330-338.

наказуемости и обеспечения соразмерности уголовной ответственности. Поэтому размер причинённого ущерба исследуется далее не только как характеристика содеянного, но и как основание для совершенствования подходов к его уголовно-правовой оценке и назначению наказания.

Таким образом, анализ санкции, предусмотренной п. «г» ч. 3 ст. 158 УК РФ, свидетельствует о наличии некоторых диспропорций в системе уголовно-правового реагирования на дистанционные формы хищений. При отсутствии учёта размера причинённого ущерба уголовная ответственность за кражу с банковского счёта либо электронных денежных средств приобретает чрезмерно репрессивный характер и не во всех случаях коррелирует с действительной степенью общественной опасности деяния. Это обусловливает необходимость дальнейшего теоретического осмысления и законодательного уточнения подходов к дифференциации наказуемости дистанционных хищений, в том числе путём сближения критериев уголовной ответственности за бесконтактные формы кражи с общими положениями о тайном хищении чужого имущества. Реализация указанного подхода возможна посредством дополнения п. «г» ч. 3 ст. 158 УК РФ примечанием, устанавливающим, что уголовная ответственность за кражу с банковского счёта либо электронных денежных средств наступает при условии причинения ущерба в размере, превышающем установленный минимальный порог, либо посредством включения в соответствующее Постановление Пленума Верховного Суда РФ разъяснения о необходимости квалификации бесконтактных хищений с банковских карт и электронных средств платежа с учётом стоимостного критерия, предусматривающего отнесение деяний с меньшим размером ущерба к административно наказуемым.

Санкции в статье 159^3 УК РФ законодатель выстраивает по «классической» модели нарастающей репрессивности, увязывая объём и вид уголовно-правового воздействия с формами соучастия, размером причинённого ущерба и использованием служебного положения. При этом санкционная конструкция данной нормы в целом отражает специфику

мошенничества как преступления, основанного на обмане и злоупотреблении доверием, в том числе реализуемых посредством электронных средств платежа. В целом санкция ч. 1 ст. 159^3 УК РФ носит ярко выраженный альтернативный характер и включает широкий спектр наказаний (от штрафа и обязательных либо исправительных работ до принудительных работ и лишения свободы на срок до трёх лет). Такой перечень мер уголовно-правового воздействия свидетельствует о стремлении законодателя обеспечить максимальную гибкость при индивидуализации наказания и учитывать, с одной стороны, имущественный характер вреда, а с другой – степень вовлечённости виновного в противоправную деятельность. В свою очередь, отсутствие минимального порога лишения свободы позволяет судам ориентироваться на преимущественное применение наказаний, не связанных с изоляцией от общества, что в целом соответствует принципу экономии уголовной репрессии. При этом наиболее суровая санкция по основному составу указанного преступного деяния более суровая даже нежели основной состав мошенничества (ст. 159 УК РФ) и мошенничество в сфере компьютерной информации (ст. 159^6 УК РФ), что, по справедливому утверждению отдельных исследователей, также вызывает некоторые вопросы[136].

В ч. 2 ст. 159^3 УК РФ усиление санкции обусловлено либо совершением преступления группой лиц по предварительному сговору, либо причинением значительного ущерба гражданину. Расширение пределов наказаний, включая лишение свободы на срок до пяти лет, отражает более высокую степень криминогенности данных форм поведения и соответствует общей логике дифференциации ответственности за мошенничество в УК РФ.

Далее отметим, что санкция ч. 3 ст. 159^3 УК РФ, в свою очередь, ориентирована на пресечение наиболее опасных форм преступного посягательства, связанных с использованием служебного положения либо

[136] Мирончик А.С., Суслопаров А.В. Хищения в электронной среде как разновидность информационных преступлений: проблемы разграничения и квалификации // Юридические исследования. 2019. № 9. С. 17-30.

совершением деяния в крупном размере. Максимальный предел лишения свободы в шесть лет, а также возможность назначения дополнительного наказания в виде штрафа или ограничения свободы, сближают данный состав по степени строгости с тяжкими преступлениями против собственности.

Наиболее жёсткую санкцию закрепляет ч. 4 ст. 159^3 УК РФ, где уголовная ответственность дифференцируется по признакам организованной преступной деятельности либо особо крупного размера. Лишение свободы на срок до десяти лет с возможным назначением крупного штрафа свидетельствует о признании таких деяний одной из наиболее опасных форм дистанционных хищений, сопряжённых с высокой степенью организованности, устойчивости преступных связей и значительным ущербом имущественным интересам граждан и организаций.

Так, санкции ст. 159^3 УК РФ в целом демонстрируют последовательную и традиционную для мошенничества логику дифференциации уголовной ответственности, в которой решающую роль играют размер причинённого ущерба, форма соучастия и наличие специальных квалифицирующих признаков. Далее перейдём к анализу санкций, предусмотренных ст. 159^6 УК РФ, и затем проанализируем проблемы и пути решения наказуемости по данным схожим составам преступлений.

Первоначально отметим, что ч. 1 ст. 159^6 УК РФ также предусматривает широкий диапазон наказаний (от штрафа и обязательных или исправительных работ до ограничения свободы и ареста, что тоже ориентирует суд на индивидуализацию уголовной ответственности с учётом характера и степени общественной опасности деяния, а также личности виновного). Ч. 2 ст. 159^6 УК РФ усиливает уголовную ответственность при совершении деяния группой лиц по предварительному сговору либо с причинением значительного ущерба. В свою очередь, ч. 3 данной статьи устанавливает ответственность за деяния, совершённые с использованием служебного положения, в крупном размере или с банковского

счёта/электронных денежных средств, что закрепляет квалифицирующие признаки и увеличивает максимальные пределы наказаний (до шести лет лишения свободы и значительного штрафа). Такой подход призван учитывать злоупотребление профессиональным или должностным статусом и причинённый имущественный вред. И, наконец, ч. 4 ст. 159^6 УК РФ закрепляет особо квалифицированные составы преступления – совершение деяния организованной группой или в особо крупном размере, с максимальным сроком лишения свободы до десяти лет и штрафом до одного миллиона рублей. Эта конструкция санкций подчеркивает высокую социальную опасность наиболее тяжких форм дистанционного мошенничества в сфере компьютерной информации. В результате санкции ст. 159^6 УК РФ обеспечивают многоуровневую дифференциацию наказаний, соразмерных характеру, способу совершения и последствиям деяния, сочетая репрессивные и превентивные элементы. Теперь считаем необходимым перейти к выявлению проблемных аспектов и диспропорций, связанных с применением санкций по ст. 159^3 и 159^6 УК РФ.

Прежде всего обращает на себя внимание отсутствие в основных составах преступлений, предусмотренных ст. 159^3 и ст. 159^6 УК РФ, каких-либо стоимостных ориентиров причинённого ущерба, при том что именно имущественный вред является ключевым последствием мошенничества. Данная конструкция означает, что законодатель не связывает момент окончания указанных преступлений с достижением определённого размера ущерба. Преступление признаётся оконченным с момента совершения соответствующих действий (использования электронных средств платежа, неправомерного воздействия на компьютерную информацию либо информационные системы), независимо от фактически причинённого имущественного ущерба. Иными словами, стоимостной критерий не выступает обязательным признаком объективной стороны состава и не выступает конструктивным признаком, влияющим на квалификацию деяния. Так, за совершение преступлений, предусмотренных ч. 1 ст. 159^6, ч. 2 ст. 272,

ч. 3 ст. 30-п. «б» ч. 3 ст. 156^6, ч. 2 ст. 272 УК РФ, и хищение денежных средств в размере 1 725 000 рублей, в соответствии с законом гражданин Н. получил 2 года лишения свободы[137], в то время как гражданин В. нанёс ущерб на сумму 561 000 рублей и был приговорён по ч. 3 ст. 30, п. «б» ч. 3 ст. 159^6 УК РФ практически к идентичному наказанию – 1 году 6 месяцам лишения свободы[138]. Безусловно, приведённые примеры не являются полностью тождественными по фактическим обстоятельствам, объёму обвинения и совокупности инкриминируемых деяний, вследствие чего не позволяют проводить прямое сопоставление назначенных наказаний исключительно через призму размера ущерба. Вместе с тем они демонстрируют общую тенденцию. Действующая конструкция преступлений, предусмотренных ч. 1 ст. 159^3 и ст. 159^6 УК РФ не содержит дифференцирующего механизма, прямо связывающего размер причинённого ущерба с моментом криминализации либо с минимальными порогами уголовной ответственности, что отличает её, например, от общих подходов к мелким хищениям в системе имущественных преступлений. В результате уголовно наказуемым признаётся дистанционное мошенничество вне зависимости от размера причинённого ущерба, тогда как этот критерий учитывается лишь на стадии индивидуализации наказания и квалифицирующих признаков. И одна из проблем заключается не в отсутствии уголовной ответственности за такие деяния, а в том, что размер ущерба не встроен в конструкцию основного состава как элемент, позволяющий формировать более чёткую градацию общественной опасности. Это в отдельных случаях приводит к недостаточной дифференциации уголовной ответственности и формированию диспропорции

[137] См. Приговор № 1-26/2025 от 13 апреля 2025 г. по делу № 1-26/2025, Н. районный суд (Республика Дагестан) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/DMQMgKcBJQml/ (дата обращения: 04.02.2026).

[138] См. Приговор № 1-277/2020 от 29 июля 2020 г. по делу № 1-277/2020, С. районный суд г. Владивостока (Приморский край) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/4AyuDmz7J9oX/ (дата обращения: 05.02.2026).

между характером общественной опасности деяния и строгостью применяемых уголовно-правовых мер.

В этой связи рассмотрим вопрос о нормативном уточнении конструкции ст. 159^3 и ст. 159^6 УК РФ посредством введения дифференцирующих стоимостных критериев (либо в виде квалифицирующих порогов ущерба, либо через унифицированные разъяснения Пленума Верховного Суда РФ о пределах учёта размера ущерба при разграничении и индивидуализации ответственности), что позволит обеспечить более предсказуемую и системную уголовно-правовую оценку дистанционных форм хищений, устранить возникающие диспропорции между фактическим размером причинённого имущественного вреда и строгостью уголовно-правового реагирования, а также повысить единообразие судебной практики при квалификации однородных по своей природе деяний, совершаемых с использованием электронных средств платежа и компьютерной информации.

Не менее дискуссионным является чрезмерно широкий диапазон альтернативных наказаний, предусмотренных ч. 1 ст. 159^3 УК РФ и ч. 1 ст. 159^6 УК РФ соответственно. С одной стороны, по верному замечанию В.В. Радова, такая конструкция расширяет возможности индивидуализации ответственности[139], однако, с другой стороны, в условиях отсутствия чётких критериев оценки степени общественной опасности конкретных видов дистанционного мошенничества это может приводить к нарушению принципа равенства граждан перед законом и судом, и одно и то же деяние может повлечь как ограничение свободы, так и длительное лишение свободы, что снижает предсказуемость уголовно-правовой реакции. В результате суду приходится самостоятельно определять значимость способа совершения преступления, характера вмешательства в информационные системы и

[139] Радов В.В. Наказуемость преступлений в сфере информационных технологий // Вестник Университета имени О. Е. Кутафина. 2025. № 5 (129). С. 128-136.

объёма причинённого вреда, что неизбежно расширяет пределы судебного усмотрения.

Анализ судебной практики по делам о преступлениях, предусмотренных ст. 159^6 УК РФ, в совокупности с сопряжёнными составами ст. 272-274 УК РФ, свидетельствует о значительной вариативности назначаемых наказаний и неоднородности подходов к их индивидуализации. Так, приговором Ш. районного суда Ставропольского края от 10 декабря 2025 г. по делу № 1-313/2025 лицо признано виновным в совершении преступлений, предусмотренных ч. 3 ст. 272 и п.п. «а, в» ч. 3 ст. 159^6 УК РФ, с назначением наказания в виде лишения свободы сроком на 3 года 6 месяцев с отбыванием в исправительной колонии общего режима, с дополнительным наказанием в виде штрафа (акцент суда был сделан на совокупности неправомерного компьютерного вмешательства и последующего хищения денежных средств)[140]. Аналогичный подход прослеживается в приговоре М. городского суда Магаданской области от 3 октября 2025 г. по делу № 1-500/2025, где действия подсудимого квалифицированы по ч. 2 ст. 272, ч. 3 ст. 30, ч. 1 и п. «б» ч. 3 ст. 159^6 УК РФ, где суд учёл стадию неоконченного преступления и назначил наказание в виде 2 лет лишения свободы условно с испытательным сроком, что отразило существенное смягчение санкционного воздействия по сравнению с оконченными формами хищения[141]. Далее укажем, что приговором Ц. районного суда г. Тольятти Самарской области от 14 мая 2020 г. по делу № 1-262/2020 действия подсудимого квалифицированы по ч. 3 ст. 159^6 и ч. 3 ст. 272 УК РФ, и обвиняемому было назначено наказание в виде 2 лет лишения свободы условно с испытательным сроком, что так же, как и в предыдущем примере отражает сравнительно мягкую оценку общественной опасности и отсутствие

[140] Приговор № 1-313/2025 от 9 декабря 2025 г. по делу № 1-313/2025, Ш. районный суд (Ставропольский край) [Электронный документ]. – URL: https://sudact.ru/regular/doc/74r3cDRZ69dj/ (дата обращения: 30.06.2026).
[141] Приговор № 1-500/2025 от 2 октября 2025 г. по делу № 1-500/2025, М. городской суд (Магаданская область) [Электронный документ]. – URL: https://sudact.ru/regular/doc/bQFG9GHw14g8/ (дата обращения: 30.06.2026).

дополнительных квалифицирующих признаков, усиливающих санкционную нагрузку[142]. Ещё более «мягкий уровень» уголовно-правовой оценки прослеживается в приговоре О. городского суда Республики Башкортостан от 29 июля 2020 г. по делу № 1-243/2020, где содеянное также охватывало признаки ст. 159^6 и ст. 272 УК РФ, однако назначенное наказание составило 1 год 6 месяцев лишения свободы условно с испытательным сроком, что демонстрирует минимальный уровень репрессивного воздействия при сохранении формальной квалификации по специальной норме[143].

Безусловно, сопоставление приведённых судебных актов не позволяет говорить о полной тождественности рассматриваемых ситуаций, поскольку каждое дело отличается совокупностью фактических обстоятельств, стадией совершения преступления, наличием либо отсутствием квалифицирующих признаков, а также характером и объёмом установленного судом вмешательства в информационные системы. Вместе с тем даже при учёте указанных различий прослеживается устойчивая тенденция к существенной вариативности санкционной оценки сходных по своей правовой природе деяний, выражающаяся в широком диапазоне назначаемых наказаний при квалификации по ст. 159^6 УК РФ и сопряжённым составам ст. 272–274 УК РФ. Такая неоднородность свидетельствует не о произвольности судебных решений, а о сохраняющейся дискуссионности критериев оценки общественной опасности дистанционных хищений и необходимости их дальнейшей систематизации для обеспечения большей предсказуемости уголовно-правовой реакции.

В этой связи считаем важным на уровне разъяснений Верховного Суда РФ закрепить единые ориентиры индивидуализации наказания по ст. 159^3 и ст. 159^6 УК РФ, предусматривающих необходимость комплексной оценки

[142] Приговор № 1-262/2020 от 13 мая 2020 г. по делу № 1-262/2020, Ц. районный суд г. Тольятти (Самарская область) [Электронный документ]. – URL: https://sudact.ru/regular/doc/7A5Kp6LDx6gQ/ (дата обращения: 30.06.2026).

[143] Приговор № 1-243/2020 от 28 июля 2020 г. по делу № 1-243/2020, О. городской суд (Республика Башкортостан) [Электронный документ]. – URL: https://sudact.ru/regular/doc/eLKpELsMEF5w/ (дата обращения: 30.06.2026).

способа совершения преступления, размера причинённого ущерба и степени вовлечённости организованной группы как взаимосвязанных критериев определения общественной опасности деяния. При этом заслуживает внимания подход, согласно которому отклонение от «сопоставимых санкционных диапазонов» должно носить исключительный характер и подлежать обязательной дополнительной мотивировке со стороны суда, что позволит повысить единообразие судебной практики и предсказуемость уголовно-правовой оценки.

Далее укажем, что санкции рассматриваемых норм также не всегда в должной мере учитывают степень технологической сложности и характер используемых способов совершения дистанционных хищений. На практике одинаковые либо сходные по строгости виды наказаний могут назначаться как за деяния, совершённые с применением сложных информационно-телекоммуникационных технологий, вредоносного программного обеспечения, средств обхода систем защиты, подмены идентификационных данных, автоматизированных алгоритмов удалённого доступа, неправомерного вмешательства в функционирование информационных систем и т.п., так и за преступления, реализуемые посредством относительно простых способов дистанционного обмана либо использования ранее полученных платёжных данных без существенного технического воздействия на цифровую инфраструктуру. Например, приговором К. районного суда г. Томска от 2 декабря 2019 г. по делу № 1-3/2019 установлено, что преступная деятельность гражданина Л. носила выраженный технологически сложный характер и включала не только хищение денежных средств, но и использование специализированных схем неправомерного доступа к защищённым банковским сервисам. Из материалов дела следует, что доступ к счетам потерпевших осуществлялся посредством применения полученных ранее учётных данных и технических средств их обхода, включая использование перехваченной либо заранее собранной информации о банковских операциях, а также координацию действий участников через

цифровые каналы связи. Окончательное наказание было определено в виде 10 лет лишения свободы с отбыванием в исправительной колонии строгого режима[144]. Далее укажем, что приговором С. районного суда г. Томска от 9 декабря 2019 г. по делу № 1-25/2019 установлена ещё более сложная структура преступной деятельности, характеризующаяся системным неправомерным доступом к банковской информации значительного числа потерпевших. Преступная схема включала использование специализированных программно-технических средств для дистанционного доступа к банковским операциям, применение методов обхода защитных механизмов дистанционного банковского обслуживания, а также массовую обработку данных потерпевших с последующим распределением функций между участниками группы. Отдельные элементы деятельности предполагали автоматизацию действий по списанию денежных средств и использование различных каналов их последующего вывода, что свидетельствует о наличии устойчивой цифровой инфраструктуры совершения преступления. Тем не менее назначенные наказания (от 3 лет 6 месяцев до 5 лет 6 месяцев лишения свободы, а по совокупности – до 7 лет лишения свободы) демонстрируют отсутствие выраженной корреляции между уровнем технологической сложности преступной схемы и интенсивностью санкционного реагирования[145].

Это демонстрирует, что даже при наличии существенных различий в технологической организации преступлений (от относительно простого использования ранее полученных данных до многоуровневых схем с элементами автоматизации, распределения ролей и обхода систем защиты) судебная практика не формирует устойчивого подхода к учёту данного обстоятельства при назначении наказания. В результате степень

[144] Приговор № 1-3/2019 1-50/2018 1-580/2017 от 1 декабря 2019 г. по делу № 1-3/2019, К. районный суд г. Томска (Томская область) [Электронный документ]. – URL: https://sudact.ru/regular/doc/xbU4lTLIinWd/ (дата обращения: 30.06.2026).

[145] Приговор № 1-25/2019 1-377/2018 от 8 декабря 2019 г. по делу № 1-275/2018, С. районный суд г.Томска (Томская область) [Электронный документ]. – URL: https://sudact.ru/regular/doc/hktokOrwZgbO/ (дата обращения: 30.06.2026).

общественной опасности фактически определяется преимущественно юридической квалификацией и совокупностью преступлений, тогда как технологическая сложность способа совершения остаётся вторичным и не формализованным критерием, что снижает предсказуемость санкционной оценки. При этом особо стоит подчеркнуть, что общественная опасность дистанционных хищений, как указывалось в п. 1.1 данной работы, определяется не только самим фактом использования информационно-телекоммуникационных технологий, но и характером такого использования, степенью профессиональной подготовки виновного лица, а также объёмом создаваемых рисков для устойчивости цифрового финансового оборота.

В результате находим важным в разъяснениях Верховного Суда РФ ориентировать суды наряду с прочим на необходимость учёта при назначении наказания характера и степени технологической сложности способа совершения дистанционного хищения, уровня вмешательства в информационные системы, использования специализированных программно-технических средств, автоматизированных алгоритмов, вредоносного программного обеспечения, а также степени профессиональной подготовки виновного лица. Дополнительно возможно закрепление подхода, согласно которому применение сложных технологических способов совершения дистанционных хищений должно рассматриваться как обстоятельство, свидетельствующее о повышенной общественной опасности деяния и требующее более строгой уголовно-правовой оценки по сравнению с преступлениями, совершаемыми без существенного технического вмешательства. Такой подход позволит обеспечить более последовательную дифференциацию уголовной ответственности, повысить предсказуемость судебной практики и обеспечить соответствие назначаемого наказания фактическому характеру и степени общественной опасности совершённого деяния.

Также, проводя анализ наказаний по рассматриваемым нормам, соглашаясь с мнением исследователя Н.А. Лопашенко, укажем, что санкции

ст. 159^6 УК РФ и некоторых других норм уголовного закона, устанавливающих ответственность за «цифровые» преступления, в определённой степени рассогласованы, поскольку за основной состав преступлений, предусмотренных ст. 272 и 274 УК РФ назначается более суровое наказание (до 2-х лет лишения свободы), нежели за совершение мошеннических действий, предусмотренных ч. 1 ст. 159^6 УК РФ (до 4-х месяцев ареста), хотя эти составы преступлений по логике должны соотноситься как часть и целое[146]. При этом подобная рассогласованность прослеживается и в более широком контексте регулирования дистанционных хищений. Так, уголовно-правовые последствия дистанционной кражи, предусмотренной п. «г» ч. 3 ст. 158 УК РФ, оказываются существенно строже по сравнению с санкциями, установленными за отдельные формы дистанционного мошенничества, предусмотренные ст. 159^3 и ст. 159^6 УК РФ, несмотря на сходный уровень общественной опасности соответствующих деяний. Между тем как дистанционные кражи, так и дистанционные мошенничества посягают на единый объект уголовно-правовой охраны – имущественные отношения в цифровой сфере, совершаются с использованием информационно-телекоммуникационных технологий, характеризуются высокой латентностью, возможностью быстрого трансграничного перемещения денежных средств, сложностью выявления виновных лиц и значительным масштабом потенциального имущественного ущерба.

Более того, в современных условиях цифровизации различия между дистанционной кражей и отдельными формами дистанционного мошенничества во многом носят юридико-технический характер и обусловлены прежде всего способом воздействия на механизм распоряжения денежными средствами, тогда как фактические последствия для потерпевшего, степень нарушения имущественных интересов и

[146] Лопашенко Н.А. Компьютерное мошенничество – новое слово в понимании хищения или ошибка законодателя? // Пермский юридический альманах. Ежегодный научный журнал. 2019. № 2 (1). С. 598-609.

криминологические характеристики соответствующих деяний зачастую являются сопоставимыми. Вследствие этого существующая дифференциация санкций не всегда отражает реальный уровень общественной опасности дистанционных мошенничеств, особенно совершаемых с использованием сложных цифровых технологий, неправомерного вмешательства в информационные системы либо современных электронных средств платежа.

Так, складывается ситуация, при которой тайное дистанционное изъятие денежных средств с банковского счёта изначально рассматривается законодателем как более опасное деяние по сравнению с мошенническими действиями, совершаемыми посредством воздействия на компьютерную информацию или использования электронных средств платежа, хотя последние нередко характеризуются большей технологической сложностью, более высокой степенью организованности и значительным потенциалом причинения имущественного вреда неопределённому кругу лиц. Подобное соотношение санкций нарушает внутреннюю согласованность системы уголовно-правовых запретов в сфере дистанционных хищений.

Для решения данной проблемы предлагаем унифицировать подход к определению санкций за основные составы дистанционных хищений, предусмотренных п. «г» ч. 3 ст. 158 УК РФ, ст. 159^3 УК РФ и ст. 159^6 УК РФ, установив сопоставимый уровень уголовно-правовой реакции на данные деяния. В частности, обоснованным представляется повышение санкций за основные составы мошенничества с использованием электронных средств платежа и мошенничества в сфере компьютерной информации до уровня санкции, предусмотренной п. «г» ч. 3 ст. 158 УК РФ. Такой подход позволит обеспечить системность и логичность уголовно-правового регулирования дистанционных хищений, устранить необоснованные различия в оценке сходных по общественной опасности преступных деяний и повысить эффективность противодействия преступности в условиях цифровизации имущественных отношений.

Данные обстоятельства указывают на необходимость дальнейшего совершенствования санкционной политики в отношении дистанционных хищений. В целях повышения согласованности и справедливости уголовно-правового регулирования представляется возможным сформулировать ряд конкретных предложений по совершенствованию данных норм.

Во-первых, необходимо нормативно закрепить стоимостные критерии уголовной ответственности по п. «г» ч. 3 ст. 158 УК РФ, установив минимальный размер причинённого ущерба, при котором деяние признаётся преступным, с одновременным отграничением малозначительных посягательств от сферы уголовно-правового регулирования и их возможным отнесением к административным правонарушениям. В первую очередь, речь идёт о случаях бесконтактной оплаты товаров и услуг на незначительные суммы с использованием чужой банковской карты либо иного электронного средства платежа без ввода пароля или применения сложных технических средств. Подобные деяния, как правило, совершаются без необходимости применения специальных знаний в сфере информационных технологий и без вмешательства в функционирование информационных систем, а их способ характеризуется относительной технической простотой, что снижает степень общественной опасности по сравнению с иными формами дистанционных хищений.

Во-вторых, требуется унификация подходов к санкциям за дистанционные формы хищений. Считаем, что дистанционные кражи и дистанционные мошенничества обладают сопоставимой степенью общественной опасности, поскольку совершаются в условиях цифровой среды, посягают на имущественные отношения, характеризуются высокой латентностью, сложностью выявления виновных лиц и возможностью причинения значительного ущерба в краткие сроки. В этой связи представляем оправданным приведение санкций, предусмотренных ст. 159^3 и ст. 159^6 УК РФ, в соответствие с уровнем уголовно-правовой охраны, установленным п. «г» ч. 3 ст. 158 УК РФ, что обеспечит внутреннюю

согласованность системы уголовно-правовых запретов и устранит необоснованные различия в оценке сходных по общественной опасности деяний.

В-третьих, с учётом выявленной проблематики альтернативности санкций, предложим более чётко структурировать пределы судебного усмотрения при назначении наказания по ст. 159^3 и ст. 159^6 УК РФ, поскольку чрезмерно широкий диапазон альтернативных видов наказаний при отсутствии детализированных критериев оценки степени общественной опасности приводит к существенной вариативности правоприменительной практики. И здесь возможно как нормативное сужение санкционных альтернатив, так и их «привязка» к конкретным квалифицирующим признакам, либо формирование соответствующих разъяснений Верховного Суда РФ, обеспечивающих более предсказуемый алгоритм выбора вида и размера наказания. Такой подход позволил бы снизить уровень неопределённости при индивидуализации ответственности и обеспечить более согласованное применение санкций в рамках единой логики уголовно-правовой охраны имущественных отношений в цифровой среде.

Также укажем на разъяснительное закрепление более чётких критериев дифференциации ответственности внутри самих основных составов ст. 159^3 и 159^6 УК РФ, включая обязательный учёт при назначении наказания не только «традиционных» юридически значимых обстоятельств (например, формы и вида соучастия), но и размера причинённого ущерба, способа совершения преступления, в том числе степени технологической сложности совершаемого деяния, раскрывающейся в характере вмешательства в информационные системы, использовании специализированных программно-технических средств и т.п.

И, наконец, в целях устранения выявленной несогласованности санкционной политики и повышения предсказуемости уголовно-правовой оценки дистанционных хищений предлагаем пересмотреть подход к соотношению основных составов дистанционных хищений и

вспомогательных компьютерных составов, а также норм, связанных с обеспечением оборота электронных средств платежа, исходя из их системного построения по уровням уголовно-правовой охраны (основному, вспомогательному (технологическому) и инфраструктурному), обеспечивающим последовательное распределение функций между нормами, непосредственно устанавливающими ответственность за хищение, нормами, создающими условия его совершения, и нормами, регулирующими последующее обращение и легализацию похищенных активов, что позволит обеспечить их более согласованное взаимодействие как элементов единого механизма противодействия преступлениям в цифровой среде и устранить возникающие на практике коллизии и диспропорции при квалификации и назначении наказания.

Полагаем, что реализация указанных предложений позволила бы обеспечить более последовательную дифференциацию уголовной ответственности, усилить соблюдение принципов справедливости и соразмерности наказания, а также повысить эффективность уголовно-правового противодействия дистанционным хищениям в условиях цифровизации имущественных отношений.

Вместе с тем анализ правоприменительной практики по данной категории дел свидетельствует о том, что в целом судебная практика назначения наказания по рассматриваемым составам характеризуется преобладанием условного осуждения и наказаний, не связанных с реальным лишением свободы, особенно в случаях совершения преступлений лицами без устойчивой криминальной направленности и при отсутствии квалифицирующих признаков. Реальное лишение свободы, как правило, назначается при наличии совокупности преступлений, значительного размера ущерба, группового характера деятельности либо организованной структуры преступной схемы. При этом средние сроки лишения свободы в практике судов, как правило, формируются в пределах нижних и средних границ санкций, однако их точная дифференциация осложнена отсутствием

систематизированных статистических данных в открытом доступе. Альтернативные виды наказания (штраф, обязательные и исправительные работы) применяются преимущественно в отношении второстепенных участников преступных схем, выполняющих транзитные либо вспомогательные функции. В результате существующая модель санкций и их судебного применения свидетельствует о том, что наказуемость дистанционных хищений формируется не только на уровне законодательных конструкций, но и в значительной степени на уровне правоприменительного усмотрения, что также усиливает значение единообразия судебной практики и обусловливает необходимость дальнейшей конкретизации критериев назначения наказания по данной категории преступлений.

В целом действующее уголовное законодательство стремится обеспечить гибкую и дифференцированную уголовно-правовую реакцию, сочетая элементы репрессивного и превентивного воздействия при назначении наказаний за дистанционные хищения[147]. Вместе с тем выявленные проблемные вопросы указывают на необходимость совершенствования санкционной политики. Реализация этих мер позволит укрепить принципы справедливости, соразмерности и дифференциации уголовной ответственности, повысить эффективность уголовно-правового противодействия дистанционным формам хищений и сбалансировать санкционную политику в сфере цифровых имущественных посягательств.

Таким образом, система уголовно-правовых запретов дистанционных хищений в российском уголовном законодательстве не образует самостоятельной главы и представляет собой встроенный в традиционные имущественные преступления комплекс норм, в рамках которого уголовно-правовая оценка деяния формируется через взаимодействие «основных» составов хищений (п. «г» ч. 3 ст. 158, ст. 159^3 и ст. 159^6 УК РФ) и норм, обеспечивающих технологическую (ст. 272-274 УК РФ) и финансовую

[147] Карпов К.Н. Особенности квалификации хищений с банковского счёта либо электронных денежных средств // Вестник ОмГУ. Серия. Право. 2019. № 3. С. 138-145.

(ст. 187 УК РФ) инфраструктуру их совершения, при этом информационно-телекоммуникационные технологии в зависимости от конкретной ситуации выступают либо способом изъятия имущества, либо средством обмана, либо инструментом неправомерного доступа к цифровой среде. В случаях, не охватываемых специальными составами, применяются общие нормы о краже и мошенничестве, что, однако, не всегда обеспечивает надлежащую дифференциацию и индивидуализацию уголовной ответственности. Одновременно анализ правоприменительной практики по указанным составам свидетельствует о неоднородности подходов к оценке сходных по своей природе дистанционных хищений, проявляющейся в вариативности квалификации и назначаемых наказаний при сопоставимых фактических обстоятельствах, а также в недостаточной согласованности критериев учета способа совершения преступления, размера ущерба и степени технологической сложности посягательства. Данные обстоятельства в совокупности позволяют констатировать необходимость дальнейшего развития и систематизации уголовно-правового регулирования дистанционных хищений, направленного на повышение его внутренней согласованности, предсказуемости правоприменения и более точное отражение фактической общественной опасности соответствующих деяний, при этом в рамках настоящего исследования уже предложен ряд направлений совершенствования соответствующих уголовно-правовых конструкций, позволяющих частично устранить выявленные диспропорции и повысить согласованность уголовно-правового регулирования дистанционных хищений.

Глава 3. Криминологические основы предупреждения дистанционных хищений

3.1. Криминологическая характеристика лиц, совершающих дистанционные хищения

Ключевое место в системе криминологического предупреждения занимает личность преступника как носитель социально значимых свойств, установок и моделей поведения, реализуемых в цифровой среде. Изучение совокупности социально-демографических, социально-ролевых и психологических характеристик лиц, совершающих дистанционные хищения, позволяет выявить устойчивые закономерности формирования криминального поведения, определить типичные мотивационные комплексы и оценить степень влияния цифровых компетенций на выбор способа совершения преступления. При этом специфика дистанционного способа хищения обусловливает необходимость расширения традиционного криминологического анализа за счёт учёта уровня технической подготовки, особенностей использования электронных платёжных инструментов и характера вовлечённости в сетевые формы преступной деятельности.

Отдельно подчеркнём, что анализ личности преступника в данном контексте имеет не только теоретическое, но и прикладное значение, поскольку полученные данные могут быть использованы для совершенствования профилактических программ, ориентированных на раннее выявление криминогенных групп риска, а также для разработки адресных мер индивидуального и специального предупреждения. Именно комплексное исследование личности лица, совершающего дистанционные хищения, позволяет перейти от формального реагирования на преступление к системному воздействию на причины и условия его совершения. В связи с изложенным первоначально исследуем основные признаки личности преступника, совершающего дистанционные хищения. В рамках настоящего

исследования были проанализированы 200 уголовных дел, находящихся в производстве подразделений дознания и следствия УМВД России в 2020–2025 гг. и имеющих признаки хищений, совершаемых дистанционно (в дальнейшем анализ характеристик личности такого преступника будет производиться именно по заданным характеристикам, см. Приложение 5). При этом выборка формировалась по материалам различных субъектов Российской Федерации, включая регионы с высоким уровнем цифровизации, развитой финансово-банковской инфраструктурой, а также регионы с менее выраженной цифровой средой и иной социально-экономической спецификой. Это обеспечивает межрегиональный характер эмпирической базы исследования и позволяет учитывать возможные различия в практике выявления, расследования и квалификации дистанционных хищений, снижая влияние регионального фактора на криминологические выводы.

Отдельно укажем, что в структуре лиц, совершающих дистанционные хищения, традиционно выделяется организатор преступной деятельности, осуществляющий разработку преступной схемы, координацию действий соучастников, распределение ролей и контроль за движением похищенных денежных средств либо цифровых активов. Как правило, именно данный субъект обеспечивает устойчивость и функционирование преступной структуры. Следующим криминологическим типом выступает технический исполнитель, обеспечивающий информационно-технологическую реализацию преступления посредством использования специализированного программного обеспечения, цифровых инструментов, вредоносных программ либо эксплуатации уязвимостей информационных систем. Отдельное место занимает социальный инженер («звонарь»), специализирующийся на психологическом воздействии на потерпевших с использованием методов убеждения, манипулирования, введения в заблуждение и иных приёмов социальной инженерии. Основной задачей такого участника является преодоление поведенческих механизмов защиты потерпевшего и получение от него необходимой информации либо побуждение к совершению

определённых действий. Наконец, самостоятельным криминологическим типом является дроппер, курьер либо иной номинальный участник, выполняющий вспомогательные функции, связанные с получением, транзитом, обналичиванием либо сокрытием похищенных денежных средств и цифровых активов. Указанные лица нередко обладают минимальным уровнем вовлечённости в организацию преступной схемы, однако обеспечивают её практическое функционирование и затрудняют выявление конечных выгодоприобретателей. Далее исследование личности преступника, совершающего дистанционные хищения, будет производиться исходя из указанных данных. Для определения криминологических типов таких дистанционных преступников было отобрано по 50 уголовных дел, где субъектом преступления выступает организатор, технический исполнитель, социальный инженер и номинальный участник (дроппер). И среди этих категорий преступников сформированы криминологические портреты.

Первоначально дадим социально-демографическую характеристику, связанную с полом личности преступника, совершающего хищения дистанционно. Анализируя имеющиеся сведения, отметим, что большинство таких преступников – это мужчины (78%)[148]. Среди организаторов преступных схем доля мужчин составляет 93%, что объясняется необходимостью стратегического планирования, координации распределённых преступных групп и управления финансовыми потоками. Также высокая доля мужчин фиксируется среди технических исполнителей (88% – мужчины), что обусловлено их ключевой ролью в реализации информационно-технологической составляющей дистанционных хищений. Данный тип участников требует высокой цифровой компетентности, навыков программирования, работы с вредоносным программным обеспечением и обхода систем защиты, что традиционно связано с большей вовлечённостью мужчин в сферу IT. В группе социальных инженеров («звонарей») доля

[148] Судебная практика по уголовным делам России [Электронный ресурс]. – URL: https://sudact.ru/regular/ (дата обращения: 06.02.2026); Архив уголовных дел Белгородского областного суда [Электронный ресурс]. – URL: https://oblsud--blg.sudrf.ru/modules.php?name=sud_delo (дата обращения: 07.02.2026).

мужчин составляет 59%, при этом наблюдается более сбалансированное гендерное распределение по сравнению с иными категориями. Это связано с тем, что данный тип деятельности основан преимущественно на коммуникативных и психологических приёмах воздействия на потерпевших, что снижает значимость технических навыков и расширяет участие лиц вне зависимости от пола, включая женщин. В категории номинальных участников преступных схем доля мужчин составляет 72%, что обусловлено ситуативным характером вовлечения и относительной доступностью данной роли. Так, соглашаясь с мнением отдельных современных исследователей, укажем, что в целом такой высокий процент доли мужчин среди указанных категорий преступников обусловлен их большей социальной активностью, обладанием теоретических и практических знаний и навыков в сфере информационных технологий[149].

Изучая личность преступника, совершающего хищения дистанционно, также особое внимание следует уделить такой социально-демографической характеристике как возраст. В соответствии с данными нашего исследования, для современного преступника, совершающего дистанционные хищения, возраст от 18 до 40 лет является наиболее характерным – 75%. Наименьшую долю среди таких преступников составляют лица моложе 18 и старше 40 лет[150]. Относительно молодой «криминальный возраст», характерный для данной категории преступников, подтверждают данные иных современных криминологических исследований, что обеспечивает репрезентативность выборки[151].

Среди организаторов преступной деятельности преобладают лица в возрасте 30–40 лет (около 55%), при этом значительную долю составляют

[149] Назмеева Л.Р., Богомолов С.Ю. Личность преступника, совершающего мошеннические действия с использованием электронных средств платежа: криминологическая оценка // Вестник Казанского юридического института МВД России. 2021. Т. 12, № 4 (46). С. 535-541.

[150] Судебная практика по уголовным делам России [Электронный ресурс]. – URL: https://sudact.ru/regular/ (дата обращения: 08.02.2026); Архив уголовных дел Белгородского областного суда [Электронный ресурс]. – URL: https://oblsud--blg.sudrf.ru/modules.php?name=sud_delo (дата обращения: 09.02.2026).

[151] Лабутин А.А. Характерные черты личности преступника, совершающего мошенничество с использованием средств мобильной связи (по материалам субъектов Приволжского федерального округа) // Вестник Казанского юридического института МВД России. 2018. № 1 (31). С. 75-78.

также лица 25–30 лет (30%) и старше 40 лет (15%), что обусловлено необходимостью наличия управленческого опыта, устойчивых социальных связей и сформированных навыков координации преступных схем. Технические исполнители характеризуются преимущественным участием лиц в возрасте 20–35 лет (около 65%), при этом 18–20 лет составляют 20%, а старше 35 лет – 15%, что отражает высокую зависимость данного типа от цифровой социализации и актуальных технических компетенций, наиболее выраженных в молодом и раннем зрелом возрасте. Социальные инженеры («звонари») в основном представлены лицами 18–30 лет (около 70%), при этом 30–40 лет составляют 25%, а старше 40 лет – около 5%, что связано с высокой коммуникативной активностью, психологической гибкостью и эффективностью манипулятивного воздействия именно в молодом возрасте. Номинальные участники преступных схем отличаются наиболее равномерной возрастной структурой: 18–25 лет – около 40%, 25–35 лет – 35%, старше 35 лет – 25%, что обусловлено ситуативным характером вовлечения, низким порогом входа в преступную роль и отсутствием требований к специализированной подготовке.

Анализ материалов уголовных дел показывает, что семейно-брачный статус преступников, совершающих дистанционные хищения, имеет выраженную специфику. В отличие от традиционных корыстных преступлений, где доля семейных лиц выше, рассматриваемая категория характеризуется более молодым возрастным составом и, как следствие, меньшей распространённостью устойчивых семейных связей. По данным исследования среди установленных лиц, причастных к дистанционным хищениям: не состоят в браке – 61%, состоят в зарегистрированном браке – 39%. Из них имеют несовершеннолетних детей – 28%.

Среди организаторов преступных схем преобладают лица, не состоящие в браке (около 55%). При этом наличие семейных связей в данной категории нередко носит формальный характер и не препятствует участию в преступной деятельности. Технические исполнители также в большей

степени представлены не состоящими в браке лицами (около 63%), в то время как 37% состоят в браке. Данная тенденция объясняется преимущественно молодым возрастом данной категории и высокой вовлечённостью в профессионально-цифровую среду, часто сопровождающуюся сниженной социальной и семейной устойчивостью. Среди социальных инженеров («звонарей») доля не состоящих в браке составляет около 68%, тогда как 32% находятся в зарегистрированном браке. Преобладание несемейных лиц связано с их большей мобильностью, гибкостью поведения и включённостью в коммуникационно-цифровые формы преступной деятельности, требующие высокой доступности и оперативности взаимодействия. В группе номинальных участников наблюдается наиболее равномерное распределение. Около 58% не состоят в браке, 42% состоят в браке. Данная особенность объясняется ситуативным характером вовлечения, при котором семейное положение не является значимым фактором участия и не препятствует выполнению транзитных функций в преступной схеме.

Так, семейное положение лиц, совершающих дистанционные хищения, характеризуется доминированием лиц, не состоящих в устойчивых семейных отношениях, что отражает как их возрастную структуру, так и особенности криминальной среды, в которой формируется данный тип преступника (см. рис. 3).

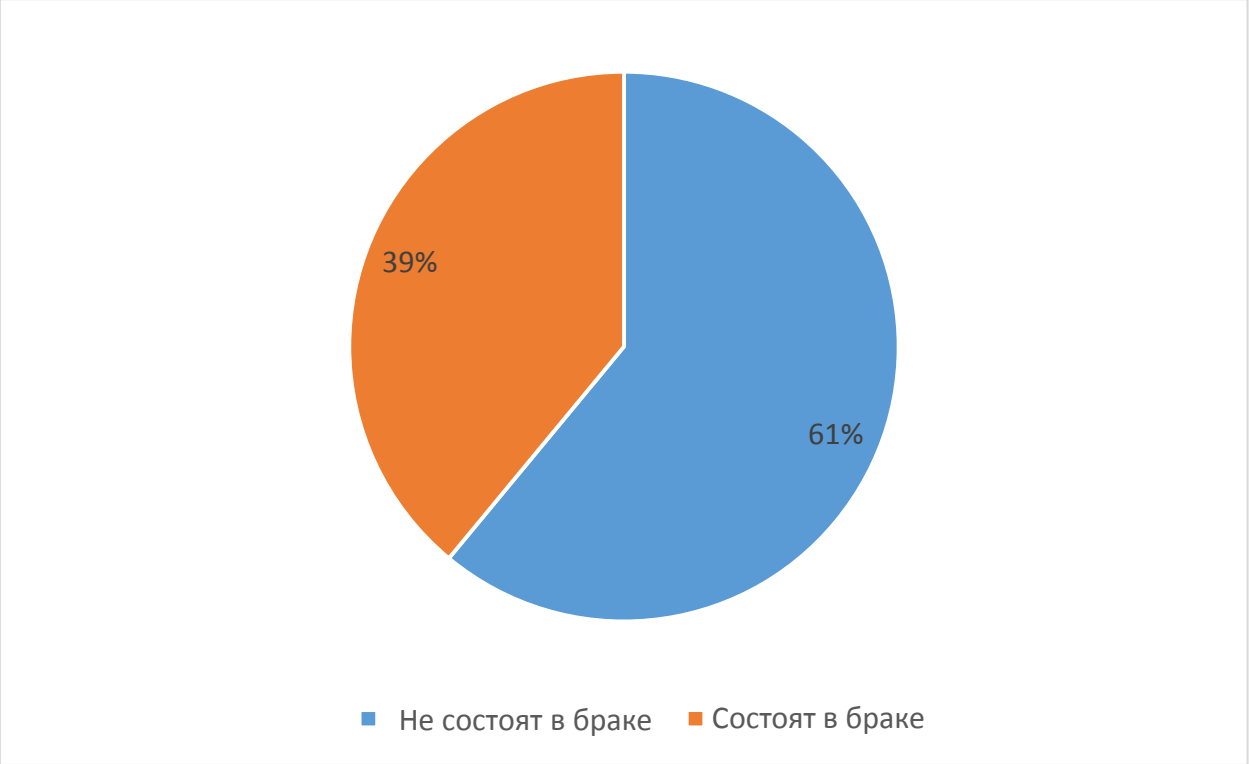


Рисунок 3. Социально-демографическая характеристика, связанная с семейным положением преступника, совершающего дистанционные хищения
(по данным анализа 200 уголовных дел, находящихся в производстве подразделений дознания и следствия УМВД России в 2020–2025 гг.)[152]

Также анализ материалов уголовных дел позволяет определить структуру образовательного уровня лиц, совершающих дистанционные хищения. Общеизвестно, что данные преступления нередко требуют базовой цифровой грамотности и способности работать с электронными коммуникациями, что отражается в образовательном «профиле» таких преступников. По обобщённым статистическим оценкам среднее специальное образование имеют 41% преступников, незаконченное высшее – 17%, высшее образование – 18% (причём около половины из них получили техническую или экономическую подготовку), только среднее общее

[152] Судебная практика по уголовным делам России [Электронный ресурс]. – URL: https://sudact.ru/regular/ (дата обращения: 10.02.2026); Архив уголовных дел Белгородского областного суда [Электронный ресурс]. – URL: https://oblsud--blg.sudrf.ru/modules.php?name=sud_delo (дата обращения: 11.02.2026).

образование – 22%; образование ниже среднего – 2%. Так, совокупно 76% преступников имеют образование не ниже среднего специального, что отражает требуемый уровень цифровой компетентности (см. рис. 4).

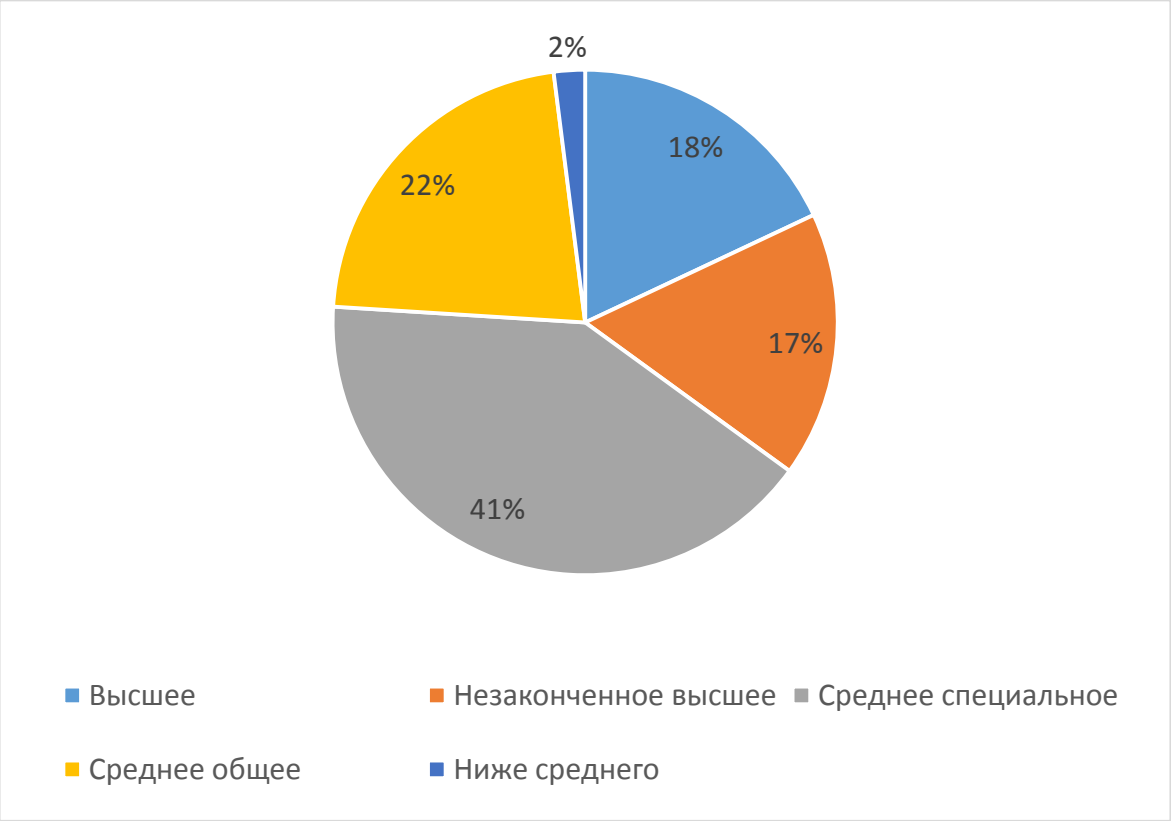


Рисунок 4. Социально-демографическая характеристика, связанная с образованием преступника, совершающего дистанционные хищения

(по данным анализа 200 уголовных дел, находящихся в производстве подразделений дознания и следствия УМВД России в 2020–2025 гг.)[153]

Организаторы преступных схем характеризуются относительно более высоким образовательным уровнем, где преобладают лица со средним специальным (35%) и высшим образованием (25%), а также незаконченным высшим (25%), при незначительной доле лиц со средним общим образованием (10%) и единичных случаев более низкого уровня образования

[153]Судебная практика по уголовным делам России [Электронный ресурс]. – URL: https://sudact.ru/regular/ (дата обращения: 12.02.2026); Архив уголовных дел Белгородского областного суда [Электронный ресурс]. – URL: https://oblsud--blg.sudrf.ru/modules.php?name=sud_delo (дата обращения: 13.02.2026).

(5%), что обусловлено необходимостью аналитических и управленческих компетенций. Технические исполнители преимущественно имеют среднее специальное образование (50%), а также незаконченное высшее (20%) и высшее (20%), при минимальной доле лиц со средним общим образованием (10%), что отражает их ориентацию на прикладные цифровые навыки и техническую подготовку. Социальные инженеры («звонари») характеризуются доминированием среднего специального (40%) и среднего общего образования (30%), при наличии незаконченного высшего (15%) и высшего образования (10%), что свидетельствует о преобладании коммуникативных и поведенческих компетенций над формализованной образовательной подготовкой. Номинальные участники преступных схем отличаются наибольшей долей лиц со средним общим (38%) и средним специальным образованием (39%), при наличии незаконченного высшего (8%) и высшего образования (17%), что подтверждает ситуативный характер вовлечения и низкий порог входа в криминальную деятельность.

Профессиональный статус преступников, совершающих дистанционные хищения, в свою очередь, отличается неустойчивостью и отсутствием стабильной занятости. Выборочный анализ судебных данных показывает следующее распределение преступников: не имели постоянной занятости –48% установленных лиц; работали в сфере торговли, услуг или логистики – 22%; имели опыт работы в ИТ-сфере – 12%; были студентами – 10%; занимались фрилансом и нерегулярными подработками – 8% (см. рис. 5).

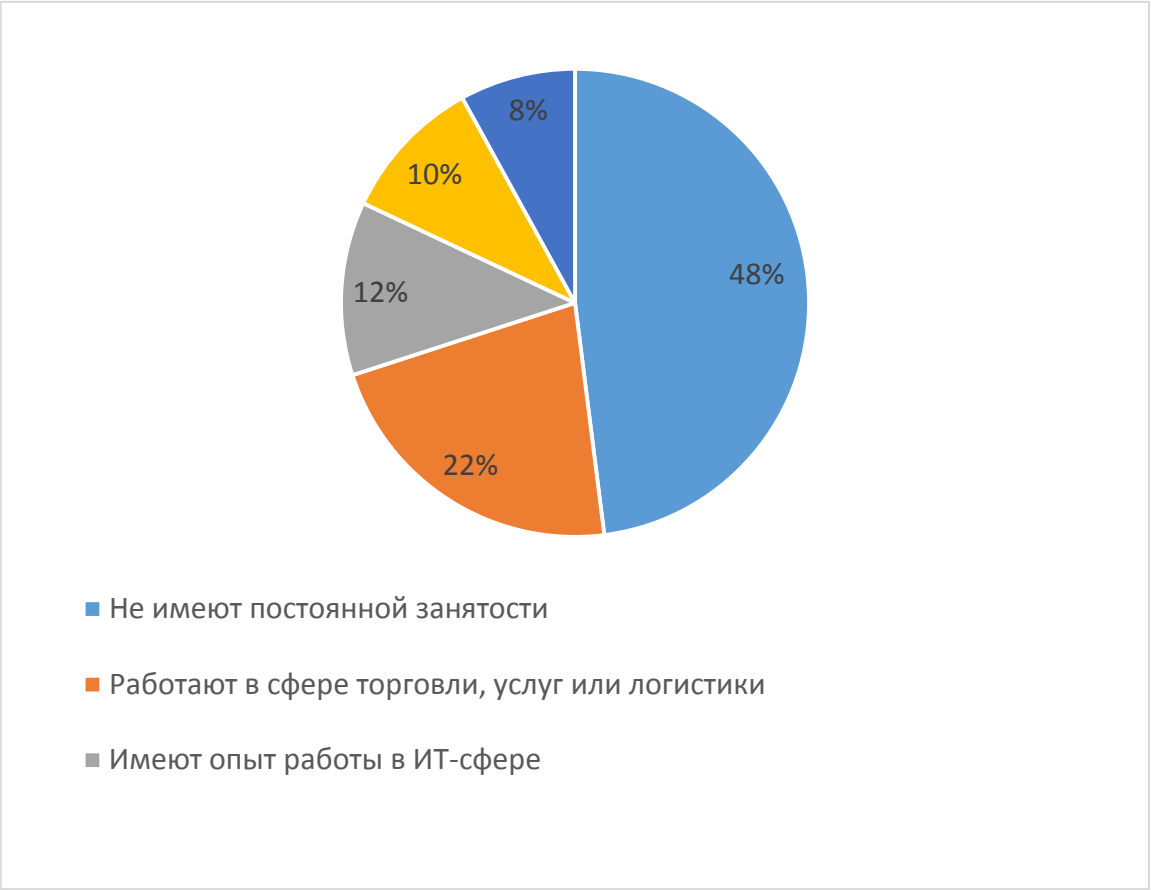


Рисунок 5. Социально-демографическая характеристика, связанная с профессиональной занятостью преступника, совершающего дистанционные хищения
(по данным анализа 200 уголовных дел, находящихся в производстве подразделений дознания и следствия УМВД России в 2020–2025 гг.)[154]

Так, организаторы преступных схем в значительной степени представлены лицами, не имеющими постоянной занятости (40%), а также ранее работавшими в сферах торговли, услуг и логистики (30%). Кроме того, часть организаторов имела опыт фриланса и нерегулярных подработок (15%), тогда как доля лиц с ИТ-опытом (10%) и студентов (5%) является ограниченной, что связано с преимущественно управленческо-координационной природой их деятельности. Технические исполнители

[154] Судебная практика по уголовным делам России [Электронный ресурс]. – URL: https://sudact.ru/regular/ (дата обращения: 14.02.2026); Архив уголовных дел Белгородского областного суда [Электронный ресурс]. – URL: https://oblsud--blg.sudrf.ru/modules.php?name=sud_delo (дата обращения: 15.02.2026).

характеризуются доминированием ИТ-сферы (35%), а также значительной долей лиц без постоянной занятости (30%). Дополнительно они представлены лицами, занятыми в торговле и услугах (15%), студентами (10%) и фрилансерами (10%), что отражает их профессионально-цифровую специализацию. Социальные инженеры («звонари») преимущественно не имеют постоянной занятости (55%), при этом значительная часть ранее работала в сфере торговли и услуг (25%). Студенты составляют 15%, а лица, занятые фрилансом, – 5%, что свидетельствует о высокой гибкости данной категории и ориентации на коммуникативные формы деятельности. Номинальные участники преступных схем в наибольшей степени представлены лицами без постоянной занятости (67%), а также работниками сферы торговли и услуг (18%). Студенты составляют 10%, а лица с опытом фриланса – 2%, что подтверждает их наиболее низкий порог входа в преступную деятельность и ситуативный характер вовлечения. Вследствие этого отметим, что высокая доля лиц без официальной работы указывает на значимую роль экономической мотивации быстрого незаконного заработка. При этом отсутствие постоянной занятости в данной категории лиц не всегда связано с материальной нуждой или невозможностью трудоустройства, а в ряде случаев отражает сознательный отказ от официальной занятости в пользу получения более высокого и быстрого дохода посредством противоправной деятельности. Представители ИТ-сферы чаще выполняют технические функции, а лица с опытом работы в продажах – функции коммуникативного воздействия на жертв преступных посягательств.

Анализ уголовно-правового статуса лиц, совершающих дистанционные хищения, показывает, что данная категория преступников сочетает в себе как особенности «новой» цифровой преступности, так и «классические» черты имущественных правонарушителей. При этом значительная часть таких лиц впервые вступает в криминальную деятельность именно в цифровой среде, что отличает их от «традиционных» мошенников и воров, для которых характерен накопленный криминальный опыт. Так, по данным исследования

уголовных дел, среди таких лиц ранее не привлекались к уголовной ответственности – 54% преступников. Это отражает латентный характер дистанционных хищений и отсутствие необходимости у преступника обладать криминальным опытом, поскольку участие в «удалённых» преступных «схемах» требует прежде всего цифровых навыков, а не криминального прошлого. Кроме того, как указывалось ранее, многие вовлекаются в преступную деятельность в молодом возрасте под влиянием корыстных мотивов или социальных контактов, не имея устойчивого криминального опыта. Между тем, 27% таких преступников имели одну предыдущую судимость, 19% – две и более (см. рис. 6).

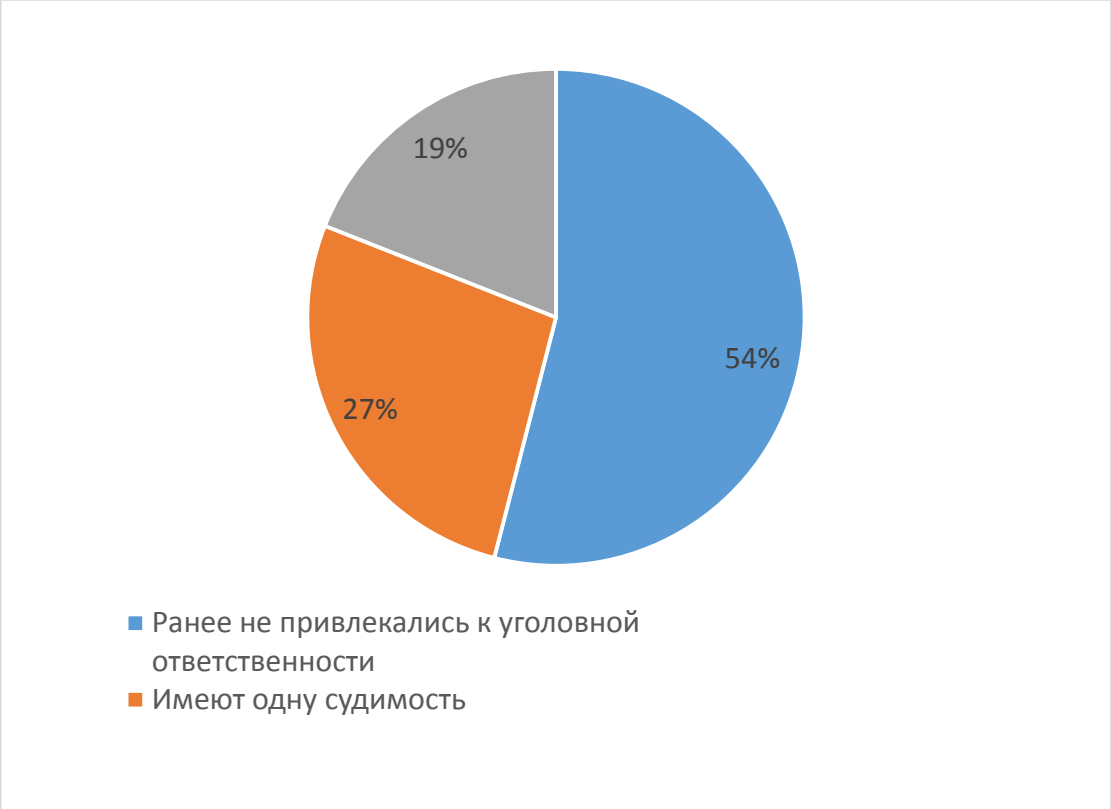


Рисунок 6. Уголовно-правовая характеристика лиц, совершающих дистанционные хищения, по признаку наличия судимости (по данным анализа 200 уголовных дел, находящихся в производстве подразделений дознания и следствия УМВД России в 2020–2025 гг.)[155]

[155] Судебная практика по уголовным делам России [Электронный ресурс]. – URL: https://sudact.ru/regular/ (дата обращения: 16.02.2026); Архив уголовных дел Белгородского областного суда [Электронный ресурс]. – URL: https://oblsud--blg.sudrf.ru/modules.php?name=sud_delo (дата обращения: 17.02.2026).

В разрезе характеристики криминологических типов установлено, что среди организаторов преступных схем доля ранее не привлекавшихся к уголовной ответственности составляет около 35%, что указывает на наличие у части из них первичной криминализации именно в цифровой среде. Среди технических исполнителей данный показатель составляет около 40%, что связано с вовлечением в преступную деятельность лиц, обладающих специализированными цифровыми навыками, но не имеющих устойчивого криминального прошлого. Среди социальных инженеров («звонарей») доля ранее не привлекавшихся к уголовной ответственности достигает около 65%, что объясняется большим ситуативным характером вовлечения, ориентацией на коммуникативные и психологические навыки и относительно низким уровнем осознания преступной специфики на начальных этапах участия. В группе номинальных участников преступных схем данный показатель является наиболее высоким и составляет около 78%, что обусловлено их вспомогательной ролью, минимальным уровнем вовлечённости в организацию преступной схемы и часто случайным либо оппортунистическим характером участия.

По статьям о мошенничестве с использованием информационно-коммуникационных технологий (ст. 159^3 и 159^6 УК РФ) привлекается 71% лиц, что в основном характерно для социальных инженеров («звонарей») и организаторов преступных схем, поскольку именно данные категории обеспечивают реализацию механизмов обмана, введения потерпевших в заблуждение и применения методов социальной инженерии. По статьям о кражах (в первую очередь п. «г» ч. 3 ст. 158 УК РФ), привлекается 21% лиц, что преимущественно характерно для технических исполнителей и части дропперов, участвующих в прямом доступе к электронным денежным средствам либо обеспечивающих их неправомерное списание и последующее движение по транзитным схемам. По иным составам преступлений (8%),

включая ст. 187, 272–274 УК РФ, привлекаются преимущественно технические исполнители, номинальные участники[156].

Показатель рецидива по дистанционным хищениям выглядит следующим образом: повторное совершение тождественных и (или) однородных преступлений – 35%; переход на другие имущественные преступления – 11%; отсутствие повторных преступлений – 54% (см. рис. 7).

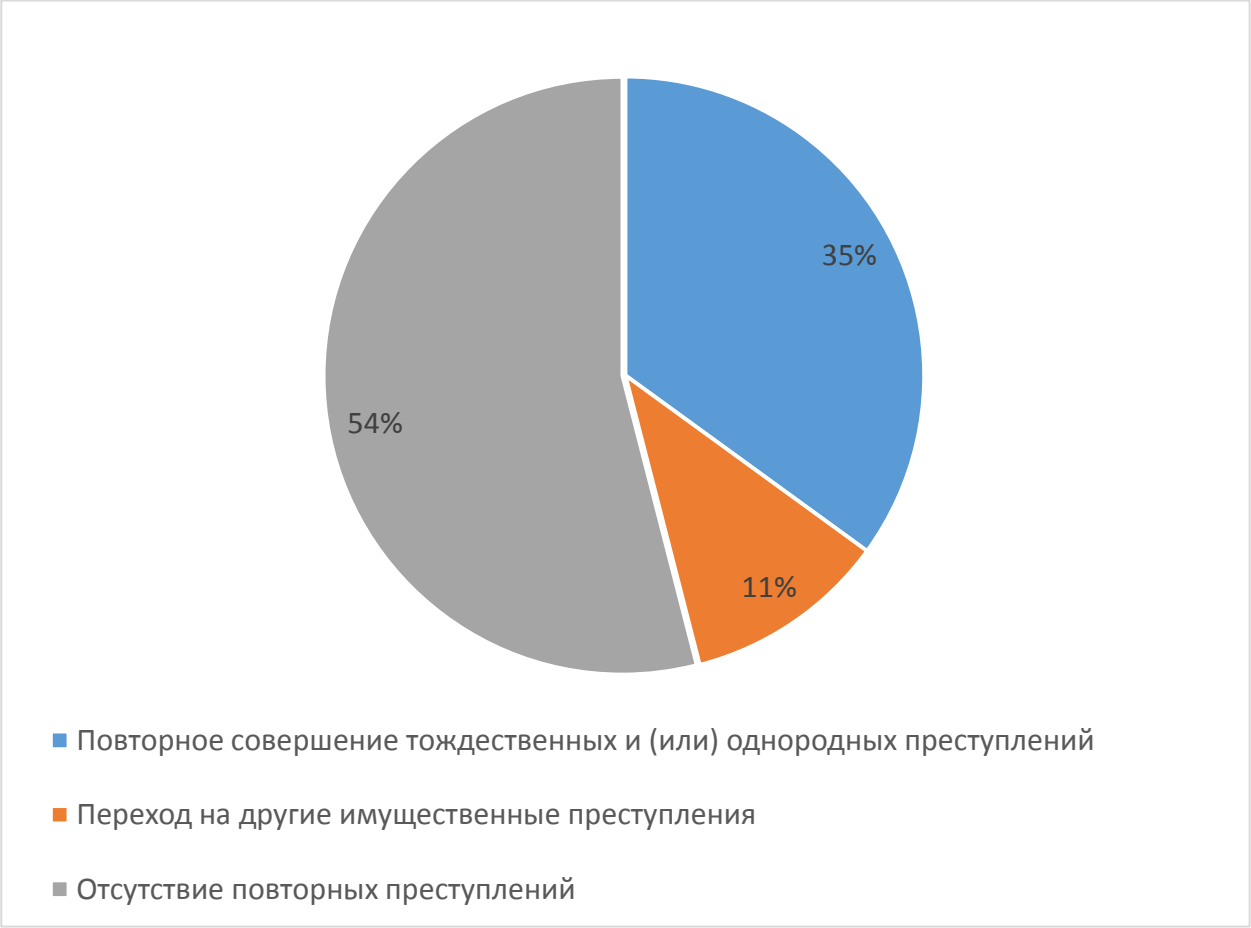


Рисунок 7. Уголовно-правовая характеристика лиц, совершающих дистанционные хищения, по признаку повторности преступной деятельности (по данным анализа 200 уголовных дел, находящихся в производстве подразделений дознания и следствия УМВД России в 2020–2025 гг.)[157]

[156] Судебная практика по уголовным делам России [Электронный ресурс]. – URL: https://sudact.ru/regular/ (дата обращения: 18.02.2026); Архив уголовных дел Белгородского областного суда [Электронный ресурс]. – URL: https://oblsud--blg.sudrf.ru/modules.php?name=sud_delo (дата обращения: 19.02.2026).
[157] Судебная практика по уголовным делам России [Электронный ресурс]. – URL: https://sudact.ru/regular/ (дата обращения: 22.02.2026); Архив уголовных дел Белгородского областного суда [Электронный ресурс]. – URL: https://oblsud--blg.sudrf.ru/modules.php?name=sud_delo (дата обращения: 23.02.2026).

Анализ рецидива в разрезе криминологических типов лиц, совершающих дистанционные хищения, позволяет выявить существенные различия в устойчивости преступного поведения. Среди организаторов преступных схем повторное совершение тождественных либо однородных преступлений составляет 55%, переход к иным имущественным преступлениям – 15%, отсутствие повторной преступной активности – 30%, что обусловлено формированием устойчивой криминальной установки и профессионализацией управленческой деятельности в цифровой преступной среде. Среди технических исполнителей повторная преступная активность фиксируется на уровне 45%, переход к иным имущественным либо смежным компьютерным преступлениям – 20%, отсутствие рецидива – 35%, что связано с накоплением специализированных цифровых навыков и их возможной последующей криминальной конвертацией. Среди социальных инженеров («звонарей») повторное совершение преступлений составляет 25%, переход к иным составам – 10%, отсутствие повторной преступной активности – 65%, что отражает преимущественно ситуативный характер вовлечения и отсутствие устойчивой криминальной специализации. В группе номинальных участников повторная преступная активность составляет 15%, переход к иным преступлениям – 5%, отсутствие рецидива – 80%, что объясняется разовым характером вовлечения и низким уровнем интеграции в структуру организованной преступной деятельности.

Это подтверждает, что большая часть лиц совершает дистанционные хищения не на профессиональной основе, а под воздействием временных материальных или социальных факторов. Однако значительный процент лиц, совершающих тождественные и (или) однородные преступные деяния также указывает на криминальную профессионализацию данной категории преступников. В целом лица, осуждённые за дистанционные хищения, отличаются относительно низким уровнем агрессивности и конфликтности, что влияет как на выбор наказания, так и на характер их поведения в местах лишения свободы. Для них характерны высокий уровень адаптивности,

умение соблюдать правила и сравнительно невысокий риск повторного участия в криминальных схемах при наличии альтернатив трудоустройства[158].

Психологический портрет лиц, совершающих дистанционные хищения, формируется под влиянием специфики их деятельности, не предполагающей непосредственного физического контакта с жертвой, но требующей высокой степени когнитивной, коммуникативной и организационной активности. В целом, по справедливым оценкам исследователей, для данной категории характерны рациональность, ориентация на оценку рисков и выгод, способность к планированию и адаптации поведения в изменяющихся цифровых условиях[159]. Вместе с тем указанные характеристики проявляются неодинаково в зависимости от выполняемой криминальной роли.

Как верно заключают некоторые современные учёные, организаторы преступных схем отличаются выраженной стратегической рациональностью, системностью мышления и высоким уровнем самоконтроля. Их психологический профиль характеризуется доминированием планирующего типа поведения, склонностью к долгосрочному моделированию преступных действий и распределению ролей между участниками. Для них характерна эмоциональная дистанцированность от последствий преступления, что сочетается с выраженными управленческими и манипулятивными качествами, позволяющими координировать деятельность других участников дистанционных хищений[160].

Технические исполнители характеризуются преобладанием когнитивно-аналитического типа мышления, высокой концентрацией внимания и устойчивыми навыками работы с информационно-телекоммуникационными системами. Их психологический профиль

[158] Сидорова Е.З. Современные криминологические характеристики цифровой преступности (цифровой преступник и его жертва) // Сибирский юридический вестник. 2023. № 3 (102). С. 70-78.
[159] Талан М.В., Шавалеев Б.Э. Криминологический анализ личности мошенника в сфере неправомерного использования электронных средств платежа // Вестник СПбГУ. Серия 14. Право. 2023. № 1. С. 108-122.
[160] Рязанова Е.Н. Криминологическая характеристика личности преступника, совершающего преступные деяния в сфере экономики с использованием информационно-коммуникационных технологий // Социология и право. 2022. № 3. С. 375-282.

ориентирован на решение прикладных задач, связанных с обходом технических защитных механизмов, использованием цифровых инструментов и обеспечением функционирования преступной инфраструктуры. Эмоциональная составляющая, как правило, выражена слабо, что способствует восприятию преступной деятельности как технической задачи, а не как социально значимого противоправного деяния.

Социальные инженеры («звонари») обладают выраженными коммуникативными и эмпатийно-манипулятивными способностями, позволяющими эффективно воздействовать на психологическое состояние потерпевших. Их поведение характеризуется гибкостью, адаптивностью и умением выстраивать доверительные отношения в краткосрочной перспективе. При этом эмоциональная холодность проявляется ситуативно и направлена преимущественно на подавление критического восприятия у жертвы, что обеспечивает успешную реализацию сценариев обмана[161].

Номинальные участники преступных схем представляют собой наименее устойчивую в психологическом отношении категорию, для которой характерны сниженный уровень критического анализа ситуации, ситуативная мотивация и высокая внушаемость. Их вовлечение в преступную деятельность нередко носит оппортунистический характер и связано с восприятием участия как разовой возможности получения материальной выгоды. При этом уровень эмоциональной включённости в преступный процесс минимален, что способствует восприятию своих действий как технического или формального посредничества[162].

В целом психологическая структура лиц, совершающих дистанционные хищения, демонстрирует сочетание рационально-интеллектуальных и манипулятивных характеристик, однако степень их выраженности существенно варьируется в зависимости от функциональной роли в

[161] Шашкина Е.В. Криминалистические данные об участниках организованных преступных групп, совершающих мошенничество с использованием средств мобильной связи // Право и государство: теория и практика. 2024. № 1 (229). С. 309-311.
[162] Сидорова Е.З. Современные криминологические характеристики цифровой преступности (цифровой преступник и его жертва) // Сибирский юридический вестник. 2023. № 3 (102). С. 70-78.

преступной схеме, что обусловливает необходимость дифференцированного подхода к их криминологической оценке. Также указанные типологические характеристики целесообразно дополнять поведенческими признаками.

Согласно данным исследования материалов уголовных дел[163], организатор дистанционных хищений, помимо указанных характеристик, как правило, проявляет себя через наличие устойчивых цифровых и организационных моделей поведения. Для него характерно создание и поддержание преступной инфраструктуры: подбор участников, распределение ролей, контроль денежных потоков, организация каналов связи и выбор способов сокрытия следов. В цифровой среде он может использовать несколько аккаунтов, различные мессенджеры, закрытые интернет-площадки, сервисы анонимизации, виртуальные номера и иные инструменты сокрытия личности. Его активность носит системный характер. Он чаще не совершает единичные действия, а формирует повторяемую схему, анализирует эффективность способов обмана, контролирует действия исполнителей и адаптирует преступный механизм под изменения условий.

Социальный инженер («звонарь») отличается прежде всего особенностями коммуникационного поведения. Его ключевым инструментом является не техническое воздействие на информационную систему, а психологическое влияние на потерпевшего. Для него характерны способность быстро адаптировать сценарий разговора, использование заранее подготовленных легенд, владение речевыми моделями убеждения и давления, имитация деятельности сотрудников банков, государственных органов либо иных организаций. В цифровой среде такие лица могут использовать различные номера телефонов, аккаунты, голосовые сервисы и заранее подготовленные материалы для повышения доверия. Основной маркер такого участника – высокая интенсивность коммуникаций и работа по

[163] Судебная практика по уголовным делам России [Электронный ресурс]. – URL: https://sudact.ru/regular/ (дата обращения: 18.02.2026); Архив уголовных дел Белгородского областного суда [Электронный ресурс]. – URL: https://oblsud--blg.sudrf.ru/modules.php?name=sud_delo (дата обращения: 19.02.2026).

шаблонным сценариям с последующей адаптацией под конкретного потерпевшего.

Технический исполнитель дистанционных хищений представляет собой лицо, обеспечивающее непосредственную техническую реализацию преступной схемы и обладающее более высоким уровнем цифровой компетентности по сравнению с иными участниками. В отличие от организатора, такой субъект, как правило, не определяет общую стратегию преступления, однако отвечает за конкретные технологические процессы: создание и настройку программных инструментов, поиск и обработку цифровой информации, использование вредоносного программного обеспечения, организацию удалённого доступа к информационным системам, подмену цифровых идентификаторов, создание фиктивных интернет-ресурсов либо применение способов обхода механизмов защиты. Для данной категории характерны устойчивый интерес к цифровым технологиям, использование специализированных технических ресурсов и каналов коммуникации, знание профессиональной терминологии, применение программного обеспечения для автоматизации действий и сокрытия цифровых следов. В поведенческом отношении такие лица могут отличаться повышенной рациональностью, ориентацией на решение технических задач, сниженной эмоциональной вовлечённостью в последствия преступления и восприятием противоправной деятельности как выполнения определённого набора операций. При этом технологическая компетентность не всегда сопровождается самостоятельным принятием решений. Технический исполнитель чаще реализует указания организаторов, оставаясь элементом общей преступной инфраструктуры.

Номинальный участник дистанционных хищений (в том числе дроппер) представляет собой лицо, которое обеспечивает преступной группе доступ к необходимым финансовым и цифровым инструментам, однако обычно не принимает участия в разработке технической стороны преступления. Его роль заключается в предоставлении банковских карт,

счетов, электронных кошельков, сим-карт, аккаунтов либо иных реквизитов, используемых для получения, перемещения и последующего вывода денежных средств. В отдельных случаях дропперы самостоятельно осуществляют перевод или обналичивание полученных денежных средств либо передают третьим лицам доступ к используемым банковским и иным платёжным инструментам. На возможную вовлечённость в такую деятельность могут указывать поиск в социальных сетях и мессенджерах предложений о быстром заработке, участие в закрытых группах, где предлагаются посреднические услуги, использование нескольких банковских карт и счетов, регулярная смена аккаунтов и номеров связи. В отличие от технического исполнителя, дроппер, как правило, не выполняет специализированных действий, связанных с воздействием на информационные системы, а обеспечивает отдельный этап перемещения, хранения или последующего вывода похищенных денежных средств. При этом степень его осведомлённости о преступном характере совершаемых действий может быть различной и должна оцениваться с учётом конкретных обстоятельств вовлечения и выполняемой функции. Использование дропперов позволяет другим участникам преступной схемы дистанцировать себя от операций с похищенными средствами, затрудняя установление их конечного получателя и фактической структуры преступной деятельности.

Выделение поведенческих признаков имеет практическое значение прежде всего для раннего выявления лиц, которые могут быть вовлечены в соответствующие схемы. Их совокупность может использоваться при анализе цифровой активности и выборе направлений профилактической и оперативной работы, однако сама по себе ни один из перечисленных признаков не свидетельствует о причастности лица к преступлению. Значение имеет именно сочетание нескольких обстоятельств.

Представленные результаты помогают сформировать «портрет» типичного преступника, совершающего дистанционные хищения. Типичный преступник, совершающий дистанционные хищения, – это мужчина (78%) в

возрасте от 18 до 40 лет (75%), не состоящий в браке (61%), с образованием не ниже среднего специального (76%), официально не имеющий постоянной занятости (48%) либо занятый в сфере услуг и торговли (22%), реже – в ИТ-сфере (12%) или являющийся студентом (10%). Основную долю преступлений составляют мошенничества с использованием ИКТ (71%). Более половины таких лиц ранее не судимы (54%), при этом повторное совершение тождественных преступлений характерно для 35%. Психологически данный тип личности преступников отличается рациональностью, манипулятивностью, эмоциональной дистанцированностью, низким уровнем агрессивности и преимущественно корыстной мотивацией. Далее дадим характеристику конкретным типам личности преступника, совершающего хищения дистанционно.

Согласно результатам статистического исследования материалов уголовных дел, организатор дистанционных хищений – это мужчина в возрасте 30–40 лет, не состоящий в браке, обладающий средним специальным, высшим либо незаконченным высшим образованием, не имеющий постоянной занятости либо занятый в сфере торговли и услуг, действующий в рамках групповой преступной деятельности, ранее судимый, характеризующийся выраженной рациональностью, системностью мышления, эмоциональной дистанцированностью и устойчивой корыстной направленностью мотивации с высокой степенью криминальной профессионализации. Поведенческим маркером организатора выступает его цифровая активность, выражающаяся в управлении несколькими коммуникационными каналами, координации участников через мессенджеры и закрытые группы, а также в систематическом контроле финансовых потоков и распределении ролей внутри преступной схемы.

Технический исполнитель дистанционных хищений – это мужчина в возрасте 20–35 лет, не состоящий в браке, обладающий средним специальным, высшим либо незаконченным высшим образованием, чаще связанный с ИТ-сферой либо не имеющий постоянной занятости,

выполняющий функции технического обеспечения преступных схем, ранее судимый, характеризующийся преобладанием аналитико-когнитивного типа мышления, высокой концентрацией внимания, сниженной эмоциональной вовлечённостью и восприятием преступной деятельности как совокупности технологических операций. Поведенческим маркером технического исполнителя является регулярное использование специализированного программного обеспечения, инструментов обхода защиты информационных систем и участие в технических форумах, закрытых чатах и иных цифровых площадках, связанных с IT-деятельностью.

Социальный инженер («звонарь») в дистанционных хищениях – это мужчина в возрасте 18–30 лет, не состоящий в браке, со средним специальным либо средним общим образованием, не имеющий постоянной занятости либо занятый в сфере услуг, ранее не судимый, характеризующийся высокой коммуникативной компетентностью, выраженными манипулятивными способностями, психологической гибкостью и способностью к ситуативному эмоциональному подавлению критического восприятия у потерпевших. Поведенческим маркером «звонаря» является высокая интенсивность исходящих коммуникаций, использование заранее заготовленных сценариев разговоров, а также быстрая адаптация речевых моделей под поведение конкретного потерпевшего в процессе взаимодействия.

Номинальный участник дистанционных хищений – это мужчина в возрасте 18–25 лет, не состоящий в браке, имеющий среднее специальное либо среднее общее образование, не имеющий постоянной занятости, ранее не судимый, характеризующийся ситуативностью мотивации, сниженным уровнем критического анализа, высокой внушаемостью и отсутствием устойчивой криминальной установки. Поведенческим маркером номинального участника является поиск предложений о «лёгком заработке» в мессенджерах и социальных сетях, участие в закрытых группах с

финансовыми предложениями и частая смена банковских и цифровых идентификаторов (карт, аккаунтов, номеров).

3.2. Мотивация и вербовка лиц, совершающих хищения дистанционно

Система мотивов, определяющих преступное поведение лиц, совершающих дистанционные хищения, представляет собой сложное и многоуровневое образование. Формирование и реализация этих мотивов обусловлены совокупностью детерминантов преступного поведения, которые создают соответствующую криминогенную основу и определяют условия, в которых возникает и реализуется преступная мотивация. В отношении дистанционных хищений к числу таких детерминантов относятся социально-экономические обстоятельства, особенности социального окружения и психологического восприятия преступной деятельности, доступность цифровых технологий и каналов коммуникации, а также субъективное восприятие преступником степени риска и вероятности привлечения к ответственности. При этом указанные детерминанты не определяют содержание мотивации механически, а создают условия для формирования конкретных мотивов и влияют на их реализацию. Поэтому их рассмотрение необходимо прежде всего для понимания того, под воздействием каких обстоятельств формируется мотивационная основа дистанционных хищений.

Основу мотивационной структуры дистанционного преступника составляет корысть, традиционно рассматриваемая криминологией как ключевая цель имущественных преступлений. Так, согласно отдельным экспертным оценкам, четыре пятых криминологических детерминантов имеют именно экономический характер[164]. Отдельно подчеркнём, что любые разновидности хищений (в том числе и совершаемые в дистанционной форме) сами по себе предполагают получение реальной материальной выгоды от совершения преступления, в связи с чем логично предположить,

[164] Алексеев А.И. Криминологическая профилактика: теория, опыт, проблемы / А.И. Алексеев, С.И. Герасимов, А.Я. Сухарев. – М., 2001. С. 61.

что особо важную роль в процессе формирования и развития исследуемого вида преступности имеют именно детерминанты в социально-экономической сфере. В подтверждение также укажем, что согласно исследованиям зарубежных учёных M. Faloutsos, D. Barman, A. Banerjee, побуждающим фактором IT-хищений в 90% случаев выступает именно нехватка денежных средств, соединённая с увлечённостью азартными интернет-играми[165], что также подтверждает тезис о ведущей роли корысти в системе детерминант дистанционных хищений. Однако специфика дистанционных хищений придаёт этому мотиву особые характеристики.

Во-первых, наблюдается ориентация не только на получение непосредственной имущественной выгоды, но и на стремление к её максимально быстрому, технологически оптимизированному и зачастую автоматизированному извлечению. Дистанционное хищение позволяет реализовывать корыстные цели без необходимости физического контакта с потерпевшим, что формирует представление о «рационализированном» способе получения прибыли, где человеческий фактор минимизирован. В связи с эти отметим, что преступники, осуществляющие дистанционные хищения, как правило, имеют достаточный уровень криминальной подготовки, хорошее техническое обеспечение, необходимое им для совершения преступлений такого рода. Кроме того, такие преступники часто образуют преступные группы, которые осуществляют преступную деятельность, в том числе на межрегиональном или даже на международном уровне[166]. Так, для совершения дистанционных хищений обычного желания получить прибыль противозаконным способом лицу бывает недостаточно, для этого преступнику требуется специальная подготовка, начиная от получения необходимых криминальных знаний о функционировании тех или иных инструментов работы в виртуальной среде до наличия специального оборудования, а нередко и широких связей в преступном мире. Исходя из

[165] Banerjee A. et al. Cyber-fraud is one typo away // IEEE INFOCOM 2008-The 27th Conference on Computer Communications. IEEE, 2008. P. 1939–1947.
[166] Лустин В.И. Дистанционные мошенничества // Закон и власть. 2023. № 5. С. 64-76.

этого считаем, что затрачивать различные собственные ресурсы для извлечения материальной выгоды можно только в том случае, если эта выгода значительная, и, как следствие, преступный заработок должен быть соответствующим затратам, но никак не единственным в жизни преступника. Это даёт основание заключить, что такие «типичные» детерминанты совершения преступлений корыстной и (или) корыстно-насильственной направленности в социально-экономической сфере в данной «системе координат» работают специфическим образом.

В качестве примера можно привести дело гражданина Б., обвиняемого в совершении преступлений, предусмотренных ч. 2 ст. 272, ч. 1 ст. 163 УК РФ (Приговор № 1-1204/2023 от 19 сентября 2023 г. по делу № 1-1204/2023 П. районного суда г. Краснодара (Краснодарский край)), за осуществление неправомерного доступа к охраняемой законом компьютерной информации, совершенное из корыстной заинтересованности, а также хищение (в 7 эпизодах). Судом признано, что гражданин Б. значительных материальных трудностей не испытывал, обучался на 4 курсе в Краснодарском ККИ (филиал) АНОО ВО ЦС РФ «Российский университет кооперации», но имел желание значительно финансово обогатиться[167]. Так, основным мотивом совершения преступлений было не тяжёлое материальное положение и финансовые проблемы, а желание получить прибыль противозаконным способом, причём не просто прибыль, а значительную прибыль.

Другой пример – дело гражданина Л., признанного виновным в совершении преступлений, предусмотренных ч. 3 ст. 159^6, ч. 2 ст. 272, ч. 2 ст. 273, ч. 1 ст. 30, ч. 3 ст. 159^6 УК РФ (Приговор № 1-95/2019 от 4 июня 2019 г. по делу № 1-95/2019 О. районного суда г. Владимира (Владимирская область)). Согласно материалам следствия, гражданин Л. совершил мошеннические действия в сфере компьютерной информации в крупном размере, а также из корыстных побуждений осуществил неправомерный

[167] Приговор № 1-1204/2023 от 19 сентября 2023 г. по делу № 1-1204/2023, П. районный суд г. Краснодара (Краснодарский край) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/XQpfF23Iq75J/ (дата обращения: 24.02.2026).

доступ к охраняемой законом компьютерной информации, что повлекло модификацию компьютерной информации и причинение крупного ущерба, а также ряд других общественно опасных посягательств. Примечательно, что несмотря на то, что в судебном заседании гражданин Л. пояснял, что на момент совершения преступления находился в затруднительном материальном положении, что и подтолкнуло его к противозаконной деятельности, преступник был официально трудоустроен, и, согласно показаниям свидетелей, ни осуждённый, ни его семья не испытывали финансовых трудностей, ни в чём не нуждались и «ни в чем себе не отказывали»[168].

Гражданка Л., виновная в совершении тайного хищения содержащихся на кредитных картах денежных средств умерших клиентов банка с использованием служебного положения, также не испытывала серьёзных материальных трудностей и похищенные денежные средства потратила на строительные материалы для своего дома, оплату различных услуг и покупку золотых украшений. В результате потерпевшим был причинён ущерб в крупном размере на сумму более 250 тыс. рублей (Приговор № 1-474/2018 1-53/2019 от 4 февраля 2019 г. по делу № 1-474/2018 К. районного суда г. Омска (Омская область))[169].

Как видим, представленные материалы уголовных дел подтверждают вывод о том, что дистанционные хищения чаще всего совершаются не для удовлетворения «первичных» материальных потребностей (например, для пропитания, оплаты коммунальных услуг, проезда и т.п.), а для существенного собственного финансового обогащения (причём нередко на значительные денежные суммы). Так, корыстная мотивация усиливается эффектом низкой субъективной затратности. Преступнику не требуется

[168] Приговор № 1-95/2019 от 4 июня 2019 г. по делу № 1-95/2019 О. районного суда г. Владимира (Владимирская область) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/v59eyhN7lzJq/ (дата обращения: 25.02.2026).
[169] Приговор № 1-474/2018 1-53/2019 от 4 февраля 2019 г. по делу № 1-474/2018 К. районный суд г. Омска (Омская область) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/95KLby0BvwJY/ (дата обращения: 26.02.2026).

затрачивать физические усилия, рисковать обнаружением в реальной среде или вступать в прямое противоборство. Такая рационализация преступного поведения повышает привлекательность дистанционных хищений для лиц, стремящихся к минимизации издержек при максимизации финансового результата.

Кроме того, цифровая среда порождает особую категорию мотивов, связанных с использованием технологических возможностей как средства самоутверждения. У лиц, обладающих высоким уровнем компьютерной грамотности, дистанционное хищение нередко сопряжено с мотивом демонстрации собственной компетентности. Преодоление технических барьеров, обход цифровой защиты, манипулирование программными процессами выступают своеобразным способом подтверждения профессиональной состоятельности и своеобразного интеллектуального превосходства. Подобный мотив особенно ярко выражен у преступников-«технократического» типа, для которых материальная выгода сочетается с интеллектуальным удовлетворением от успешного применения накопленных знаний. В связи с этим укажем, что многие лица, имея необходимые знания, умения и навыки в сфере дистанционных технологий, в дальнейшем целенаправленно, осознавая противозаконность своих намерений, их совершенствуют и приобретают криминальные «профессии», которые позволяют на постоянной основе извлекать доход. Исследователи верно отмечают, что современные цифровые преступники часто занимаются самообразованием в соответствующей сфере и обладают высоким интеллектом[170]. Так, характеризуя криминологический портрет киберпреступника, учёные справедливо указывают, что такие лица нередко имеют специальное техническое образование, активно осваивают в сети Интернет разнообразные видеоматериалы и инструкции по использованию

[170] Прыткова А.А. Криминологический портрет киберпреступника // Международный журнал гуманитарных и естественных наук. 2022. № 4-3. С. 152-157.

цифровых технологий, в том числе в преступных целях[171], что подтверждается данными представленного ранее криминологического исследования. При этом соответствующие преступные знания, умения и навыки эти лица чаще всего получают самостоятельно, целенаправленно повышая свои криминальные «компетенции»[172].

В подтверждении данного тезиса приведём дело гражданина Ф., осуждённого по ч. 2 ст. 159^6 УК РФ и ч. 1 ст. 222 УК РФ приговором С. районного суда г. Иваново (Ивановская область) № 1-2/2020 1-2/2021 1-5/2019 1-97/2018 от 21 июня 2021 г. Следствием установлено, что одной из причин совершения дистанционного хищения стало увлечение обвиняемого информационными технологиями, которое в дальнейшем переросло в совершение уже противозаконных действий в сети Интернет. Известно, что осуждённый первоначально скачал программу «Софт» и попытался разобраться в ней, а в дальнейшем, когда его уровень пользования программой достиг продвинутого, начал использовать данное программное обеспечение в противозаконных целях, извлекая реальную материальную выгоду от совершения преступных действий[173].

Как видим, престижность «криминального образования» в настоящее время, действительно, повышается, и многие лица делают это не просто из собственного интереса, а для «прокачки» преступных умений и навыков, позволяющих не только получать прибыль посредством совершения преступлений, но и удовлетворять свои «профессиональные» (пусть и противозаконным способом) амбиции.

Дополнительным элементом мотивационной структуры выступает эффект «цифровой безличности», когда виртуальная коммуникация создаёт

---

[171] Белевитина Ю.В. Криминологический портрет личности киберпреступника в современной России // Инновационная наука. 2022. № 12-2. С. 61-64.

[172] См., например: Приговор № 1-573/2020 от 8 сентября 2020 г. по делу № 1-573/2020 Ц. районного суда г. Кемерово (Кемеровская область) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/x4yF5QuhexHV/ (дата обращения: 27.02.2026).

[173] Приговор № 1-2/2020 1-2/2021 1-5/2019 1-97/2018 от 21 июня 2021 г. С. районного суда г. Иваново (Ивановская область) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/IifZELYWnygP/ (дата обращения: 28.02.2026).

иллюзию отсутствия реального вреда. Я.И. Гилинский справедливо отмечает, что в эпоху постмодерна молодёжь проводит много времени в интернет-сетях и в онлайн-играх, и, с одной стороны, подобная психологическая разгрузка – это хорошо. Однако, с другой стороны, по справедливому замечанию учёного, очень часто подобные увлечения оканчиваются не просто через чур значительным увлечением информационной средой, но и совершением в ней реальных преступлений, например, кибермошенничества[174]. Доктор философии, преподаватель Университета Райдера Соединённых Штатов Америки Джон Сулер также справедливо отмечает, что в киберпространстве человек действует более свободно, чем в реальности, вследствие чего ввиду воздействия различных психологических факторов (от ощущения полной анонимности в сети Интернет до асинхронности действий преступника и потенциальной жертвы) возникает, так называемый, «эффект растормаживания», что, в свою очередь, повышает риски формирования в виртуальной среде преступного поведения[175]. Так, совершая дистанционные хищения, преступник психологически дистанцируется от фактического имущественного ущерба, воспринимая его как «часть системы», а не как ущерб конкретному лицу. Это снижает внутренние барьеры и способствует формированию установки на допустимость противоправного поведения.

Отдельно укажем, что цифровая среда предлагает виновному широкие возможности для сокрытия следов, «маскировки» личности и совершения преступлений из-за границы национальных юрисдикций. Исследователи справедливо отмечают, что сама сущность киберпреступности определяет её экономическую и социальную опасность, поскольку для рассматриваемой разновидности преступности транснациональность является естественной вещью, поскольку взаимодействие между субъектами преступления

[174] Гилинский Я.И. Криминология и девиантология постмодерна. – СПб.: Алетейя, 2024. С. 99.
[175] Федосеева О.И. Психологические особенности формирования личности несовершеннолетнего киберпреступника // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2022. № 4 (60). С. 174-178.

осуществляется, как правило, именно заочно[176]. Кроме того, такой же виртуальный контакт происходит и между преступником и жертвой преступления, ввиду чего границы между регионами, странами и даже континентами для киберпреступников не важны. Субъективное восприятие низкой вероятности привлечения к ответственности становится существенным мотивационным фактором. Стремление минимизировать риск наказания побуждает преступника выбирать дистанционные формы хищения как альтернативу традиционным видам имущественных посягательств. Общеизвестно, что в настоящее время в свободном доступе находятся средства анонимизации данных в виртуальном пространстве, к которым может получить доступ любой желающий, что позволяет пользоваться данными услугами не только законопослушных граждан, но и преступников, позволяя им оставаться незамеченными – не оставлять никаких «цифровых следов» при совершении дистанционных хищений, позволяющих их идентифицировать. Так, сегодня выделяют несколько наиболее распространённых методов анонимизации в цифровом пространстве, одним из которых является использование прокси-сервисов, позволяющих скрывать свои персональные данные, маскировать и подменять IP-адреса. Нередко преступниками используются непосредственно анонимные сети, которые не просто скрывают идентифицирующие сведения, но и размещают на собственных ресурсах веб-сайты (пример, известная сеть Даркнет)[177]. Эти и другие средства анонимизации используются либо по отдельности, либо совместно, в результате чего наиболее «продвинутые» преступники получают практически «стопроцентную защиту» от уголовного преследования[178]. Это формирует особую установку на «безнаказанность»,

[176] Шумилин В.П., Лысенко Е.С., Острякова А.Ф. Проблемы законодательства о киберпреступности // Аграрное и земельное право. 2022. № 5 (209). С. 137-140.
[177] Заурби Л.Ш. О некоторых факторах, препятствующих эффективному раскрытию и расследованию преступлений, совершаемых в киберпространстве // Вестник экономической безопасности. 2021. № 2. С. 258-263.
[178] Алейников Д.П., Зык А.В. Современные технологии анонимизации в сети Интернет // Образование и право. 2021. № 7. С. 223-224.

которая укрепляет решение о совершении преступления даже у лиц, ранее не склонных к криминальному поведению.

Кроме того, важным мотиватором при совершении дистанционных хищений выступает и ситуативное воздействие. Появление у субъекта возможности использовать случайно обнаруженные уязвимости, доступ к чужим данным или техническим ресурсам. Спонтанные решения, принимаемые в ситуации «низкого риска и высокой выгоды», нередко становятся отправной точкой для формирования устойчивых преступных установок. В качестве примера укажем на распространённость в настоящее время хищений денежных средств с чужих банковских карт при случайном получении доступа к ним, в том числе посредством оплаты товаров и услуг бесконтактным способом. Укажем, что в таких случаях чаще всего преступник, получив доступ к чужим электронным денежным средствам, первоначально не имеет мотива хищения этих средств, но под воздействием ситуативных условий редко отказывается от «соблазна». В итоге подобные деяния квалифицируются как кража, совершённая с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного статьей 159^3 настоящего Кодекса) по п. «г» ч. 3 ст. 158 УК РФ[179].

Анализ мотивационной структуры лиц, совершающих дистанционные хищения, позволяет констатировать её многофакторный и системный характер. Несмотря на то что корысть традиционно выступает базовым мотивом имущественных преступлений, в условиях цифровой среды она приобретает специфическое содержание и дополняется рядом иных мотивационных компонентов.

Корыстная составляющая выражается в стремлении получить имущественную выгоду, причём в рассматриваемой группе преступлений она нередко связана с ожиданием быстрого и повторяемого дохода. Для

[179] См., например: Приговор № 1-163/2025 от 21 апреля 2025 г. по делу № 1-163/2025, Т. городской суд (Челябинская область) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/TUE1h7MpWCNR/ (дата обращения: 01.03.2026).

отдельных лиц совершение дистанционных хищений может восприниматься как источник систематического заработка, что отличает их поведение от ситуационного завладения чужим имуществом.

Другую сторону мотивации образует стремление сократить собственные затраты и вероятность разоблачения. Дистанционный способ совершения преступления позволяет действовать без непосредственного контакта с потерпевшим, использовать готовые цифровые инструменты, распределять отдельные операции между участниками и в ряде случаев автоматизировать их выполнение. Поэтому выбор такого способа может быть связан не только с размером предполагаемой выгоды, но и с оценкой его как более удобного и менее рискованного.

У лиц, выполняющих технические функции, дополнительное значение иногда приобретает стремление применить имеющиеся знания и навыки. Использование специальных программных средств, поиск уязвимостей и обход технических ограничений могут восприниматься ими как профессиональный вызов или способ самоутверждения. Однако данный мотив нельзя считать обязательным для всех технических исполнителей, поскольку в конкретных случаях специальные навыки используются исключительно как средство достижения корыстной цели.

Дистанционный характер взаимодействия способен влиять и на восприятие последствий преступления. Отсутствие непосредственного контакта с потерпевшим, распределение действий между несколькими лицами и использование обезличенных каналов связи создают психологическую дистанцию между виновным и причинённым вредом. В определённых случаях это может облегчать совершение преступления и снижать субъективное восприятие его последствий.

При принятии решения о совершении дистанционного хищения существенное значение имеет и оценка вероятности разоблачения. Анонимизация отдельных операций, использование подставных лиц, последовательное перемещение денежных средств между различными

счетами и иные способы сокрытия могут создавать у виновного представление о невысокой вероятности установления его личности. Такая оценка риска способна влиять на выбор дистанционного способа совершения преступления.

Наконец, встречаются ситуации, когда преступный умысел возникает из конкретной возможности получить доступ к чужим денежным средствам или данным. Первоначально такое поведение может носить ситуативный характер, однако при повторении преступлений и закреплении соответствующей модели поведения оно способно перерасти в более устойчивую форму преступной деятельности.

Так, каждый из этих компонентов обладает относительной автономией, но в реальной мотивационной сфере они образуют интегрированную совокупность, определяющую направленность преступного поведения. Вместе с тем указанные мотивационные компоненты проявляются неодинаково в зависимости от криминологического типа лица, участвующего в совершении дистанционного хищения. Так, для организатора преступной деятельности ведущими являются корыстный, рационально-технологический и профессионально-статусный компоненты. Его мотивация связана не только с получением прибыли, но и с построением устойчивой преступной модели, распределением ролей и повышением эффективности функционирования группы. Технический исполнитель, напротив, чаще ориентирован на реализацию конкретных технологических задач, поэтому в его мотивационной структуре преобладают рационально-технологический и профессионально-статусный компоненты, выражающиеся в стремлении применить специальные знания и навыки для решения поставленных задач, при этом эмоциональная связь с последствиями преступления может быть снижена. Социальный инженер («звонарь») преимущественно действует под влиянием корыстного и психологически-коммуникативного компонентов. Его мотивация связана с возможностью получения вознаграждения за успешное воздействие на потерпевших, использованием навыков убеждения

и манипуляции. В отличие от указанных категорий, мотивация номинального участника (дроппера) чаще имеет ситуативно-оппортунистический характер и выражается в стремлении получить быстрый доход при минимальном вовлечении в основную преступную деятельность, что нередко сопровождается недооценкой общественной опасности собственных действий. Как видим, различия мотивационных структур позволяют рассматривать дистанционные хищения не как однородное преступное поведение, а как сложную систему, в которой каждый участник выполняет определённую функцию и руководствуется специфическим набором мотивов.

В результате специфика дистанционных хищений заключается в том, что технологическая среда не только предоставляет инструменты совершения преступления, но и активно влияет на мотивационную систему субъекта, стимулируя, усиливая или трансформируя его внутренние установки. Такая трансформация мотивационной сферы напрямую отражается и на том, каким образом организаторы дистанционных хищений формируют круг исполнителей, вследствие чего возникает необходимость анализа практикуемых способов их вербовки.

Первоначально определим, что процесс вербовки исполнителей дистанционных хищений представляет собой самостоятельный криминологический феномен, тесно связанный с организованными формами преступности в цифровой среде. В механизме вербовки исполнителей дистанционных хищений существенное значение приобретает дифференциация ролей завербованных лиц, позволяющая одновременно раскрыть структуру преступной деятельности и определить направления её предупреждения. В этой связи выделяются типовые категории участников: дропперы, предоставляющие свои банковские счета либо платёжные инструменты за вознаграждение, нередко под влиянием введения в заблуждение относительно легальности таких действий; обнальщики, осуществляющие последующее обналичивание и перераспределение

похищенных денежных средств, как правило, уже с осознанием противоправного характера совершаемых операций; а также IT-специалисты, обеспечивающие техническую реализацию преступного умысла посредством создания фишинговых ресурсов, вредоносного программного обеспечения и иных цифровых инструментов, при этом их вовлечение носит преимущественно адресный и целевой характер.

Рассматривая основные механизмы вовлечения в преступную деятельность такого рода, укажем, что одним из ключевых «каналов» привлечения исполнителей являются интернет-ресурсы. «Криминальные биржи» могут находиться в Даркнете, но нередко доступны также через обычный интернет под видом анонимных платформ для фриланса, технических консультаций или обмена данными, а также в мессенджерах, социальных сетях. На таких ресурсах вербовка осуществляется посредством размещения объявлений о вакансии, требующей минимальной квалификации: «оператор колл-центра», «финансовый посредник», «партнёр по приёму платежей», «менеджер по клиентским коммуникациям» и т.п. Содержательная часть объявлений формулируется нейтрально, с акцентом на высоком заработке и возможностях удалённой работы, тогда как преступный характер деятельности раскрывается только после установления доверительных контактов. Организаторы дистанционных хищений часто применяют элементы социального инжиниринга, создавая иллюзию легитимности предлагаемых задач. Вербовщики целенаправленно используют алгоритмы рекомендаций и тематические сообщества для поиска лиц, потенциально склонных к участию в преступлениях: молодых людей с интересом к заработку в интернете, пользователей, демонстрирующих финансовые трудности, и лиц, проявляющих активность в группах, связанных с криптовалютами и онлайн-заработком.

Способы вербовки в интернет-ресурсах включают: персонализированную коммуникацию, когда кандидат получает прямое сообщение с предложением работы с «гибким графиком» и «мгновенными

выплатами»; массовые рекламные рассылки, маскирующиеся под объявления о временной подработке; создание псевдолегальных сообществ, посвящённых инвестициям, финансовой аналитике или электронной коммерции, где потенциальные исполнители постепенно приобщаются к теневым схемам и т.д. Особым инструментом становятся закрытые чаты в мессенджерах, формирующие эффект «сообщества избранных». Претенденту могут сообщать, что он участвует в работе иностранного финансового стартапа, исследовательского центра или криптовалютной платформы. Лишь после первичного вовлечения преступники постепенно раскрывают истинный характер поручаемых действий, которые, однако, уже воспринимаются исполнителем в контексте ранее созданной атмосферы доверия.

В качестве примера приведём дело о совершении организованной группой дистанционных хищений денежных средств в виде криптоактивов (Приговор № 1-379/2024 1-51/2025 от 20 апреля 2025 г. по делу № 1-379/2024 А. районный суд г. Сочи). Согласно материалам следствия, при совершении мошеннических операций при купле-продаже криптовалюты организаторы преступной группы предлагали лицам работу «оператором», в обязанности которого входила пересылка фото банковских карт, логинов и паролей, а также создание в личном кабинете клиентов банка реквизитов для оплаты и некоторые другие функции. В результате у, так называемых, «операторов» создавалась иллюзия легальности трудовой деятельности, хотя, на самом деле, они являлись исполнителями в составе преступной группы, осуществляющей дистанционно мошенничества. Вербовка исполнителей происходила в закрытой группе в мессенджере «Телеграмм»[180].

Особо также выделяются финансовые схемы, маскирующиеся под инвестиционные проекты. Они предполагают участие исполняющего лица в трансфере денежных средств, обналичивании криптовалюты или создании

[180] Приговор № 1-379/2024 1-51/2025 от 20 апреля 2025 г. по делу № 1-379/2024 А. районный суд г. Сочи (Краснодарский край) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/XW0LNH7qH8Yg/ (дата обращения: 02.03.2026).

цепочек транзакций. Вербовщики позиционируют такие действия как помощь иностранным клиентам, участие в международных расчётах, посредничество в операциях с цифровыми активами, выполнение технических процедур по обмену валют и т.д. Кандидату обещают высокое вознаграждение за минимальные усилия, что особенно привлекательно для социально уязвимых категорий населения. Преступный характер деятельности маскируется терминологией, характерной для финансовой сферы: «верификация», «арбитраж», «маржинальная операция», «ликвидность», «USDT-трафик». Таким образом, вербовка также маскируется под законный процесс финансового взаимодействия. Так, например, гражданка Н., осуждённая Приговором № 1-28/2025 от 15 апреля 2025 г. по делу № 1-28/2025 К. районным судом (Пермский край) в совершении преступления, предусмотренного п. «г» ч. 3 ст. 158 УК РФ, регулярно в мессенджере «Телеграмм» предлагала различным лицам инвестировать денежные средства для получения дополнительного дохода, а затем дистанционно, путем ввода цифровых кодов, которые заменяют и считываются банковской системой, как электронная цифровая подпись клиента, вовлекала потерпевших в противозаконные денежные транзакции. При этом гражданка Н. выдавала неосведомлённым лицам свои манипуляции за процесс инвестиций, которые не требовали никаких сверх усилий[181].

Изучение материалов уголовных дел и правоприменительной практики позволяет также выделить устойчивые способы привлечения исполнителей дистанционных хищений, при которых вовлекаемые лица изначально осознают противоправный характер предполагаемой деятельности. В таких случаях речь идёт не о заблуждении либо ошибочном восприятии ситуации, а о целенаправленной вербовке соучастников в рамках реализации организованных преступных схем. Наиболее типичным механизмом подбора исполнителей выступает адресное либо массовое распространение

[181] Приговор № 1-28/2025 от 15 апреля 2025 г. по делу № 1-28/2025 К. районный суд (Пермский край) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/FYhBzi0JL7C/ (дата обращения: 03.03.2026).

предложений о незаконном заработке через цифровые коммуникационные каналы, например, социальные сети и мессенджеры. Подобные предложения ориентированы на поиск лиц, готовых сознательно участвовать в противоправной деятельности за материальное вознаграждение. После установления контакта потенциальному исполнителю уже прямо указывается на незаконный характер предстоящих действий, что формирует осознанное согласие на участие в преступлении. Особую форму вербовки представляет вовлечение лиц, ранее пострадавших от аналогичных дистанционных мошенничеств. Используя сведения о виктимном опыте таких субъектов, организаторы преступных схем прибегают к элементам психологического воздействия, включая шантаж и угрозы, вынуждая их принять участие в преступной деятельности. Несмотря на наличие принуждающих факторов, данные лица понимают противоправную сущность поручаемых им действий, что отличает данную модель вовлечения от ситуаций неосознанного соучастия.

Также важным элементом вербовочного механизма в данном случае является создание системы подконтрольности исполнителя. Перед началом участия в преступной схеме от него нередко требуют предоставления видеозаписи с фиксацией персональных данных и выражением согласия на выполнение преступных поручений. Подобные материалы используются организаторами как средство давления, направленное на предотвращение выхода соучастника из преступной деятельности и на поддержание его лояльности под угрозой возможных негативных последствий. Вовлекаемые таким образом лица нередко выполняют функции, так называемых, дропперов, осознанно принимая на себя роль посредников при получении, перемещении и передаче похищенных денежных средств. Их действия осуществляются в рамках чётко выстроенной структуры, предусматривающей распределение ролей, финансовый контроль и вознаграждение за оказанные «услуги». Управление деятельностью таких исполнителей, как правило, осуществляется через специально выделенные

звенья преступной группы, координирующие движение денежных потоков и обеспечивающие их последующий вывод[182]. При этом отдельно стоит подчеркнуть, что достаточно часто в таких преступных схемах, по верному утверждению отдельных исследователей, участвуют несовершеннолетние[183].

Кроме того, вербовка исполнителей дистанционных хищений подлежит оценке через призму института соучастия в преступлении, закреплённого в ст. 33 УК РФ, поскольку именно распределение ролей позволяет определить уголовно-правовую природу действий каждого участника. В зависимости от фактического содержания поведения вовлекаемых лиц их роль может квалифицироваться как исполнитель, пособник, подстрекатель либо организатор. Согласно ч. 2 ст. 33 УК РФ в условиях дистанционных хищений к числу исполнителей могут относиться лица, осуществляющие непосредственное взаимодействие с цифровыми системами: ввод данных, осуществление переводов, манипулирование учётными записями, использование банковских и криптовалютных инструментов в рамках единой преступной схемы и т.д. В свою очередь, организатор (ч. 3 ст. 33 УК РФ) в таких схемах выполняет функции создания преступной структуры, распределения ролей, определения способов совершения хищений и координации действий участников. Подстрекательство (ч. 4 ст. 33 УК РФ) выражается в склонении лица к совершению дистанционного хищения путём обещаний дохода, обмана, убеждения или иных форм психического воздействия, что наиболее характерно для этапа первичной вербовки через цифровые каналы. Пособничество (ч. 5 ст. 33 УК РФ) проявляется в содействии совершению преступления, например, путём предоставления технических средств доступа, а также устранения препятствий для вывода похищенных денежных средств и цифровых активов. При этом

[182] Головчанский А.В. Анагенез механизма совершения дистанционных мошенничеств в условиях противодействия подменной коммуникации // Вестник ВИ МВД России. 2024. № 4. С. 261-269.

[183] Ахмедов У.О. Способы вовлечения несовершеннолетнего в совершение преступления с использованием информационно-телекоммуникационных технологий как предмет доказывания по уголовным делам // Вестник ВИ МВД России. 2024. № 4. С. 164-171; Соловьев В.С. Криминологические исследования преступности несовершеннолетних в условиях цифровизации общества: ожидания и реальность // Алтайский юридический вестник. 2024. № 1(45). С. 92-99.

разграничение форм соучастия требует установления степени вовлечённости лица в преступную деятельность, характера его осведомлённости о преступном замысле и наличия согласованности действий с иными участниками.

В свою очередь, при наличии устойчивого объединения лиц, заранее договорившихся о совершении дистанционных хищений с распределением функций между участниками, такие действия могут квалифицироваться как совершённые организованной группой. В таких случаях вербовка выступает системообразующим элементом преступной деятельности, обеспечивающим её воспроизводство через постоянное привлечение. В результате при более высокой степени структурированности, наличии иерархии, централизованного управления, финансового контроля и устойчивой конспирации, а также при направленности на совершение тяжких или особо тяжких преступлений, в исключительных случаях возможно определение признаков преступного сообщества (ст. 210 УК РФ). Однако применение данной нормы требует установления качественно более высокого уровня организованности по сравнению с организованной группой.

Как видим, вербовка в системе дистанционных хищений выступает не только способом вовлечения новых участников, но и юридически значимым элементом структуры соучастия, определяющим квалификацию действий в рамках ст. 33 УК РФ (от исполнителя до организатора), а также влияющим на установление формы преступного объединения. Однако в свете последних изменений отечественного уголовного законодательства определим, что особое значение в данном контексте приобретают изменения, внесённые в ст. 187 УК РФ Федеральным законом от 24 июня 2025 г. № 176-ФЗ, вступившие в силу с 5 июля 2025 года, которыми была усилена уголовно-правовая охрана платёжной сферы, в том числе путём криминализации действий, связанных с незаконным оборотом и передачей электронных средств платежа, используемых в преступных целях. Данные изменения фактически закрепили на уровне уголовного закона наиболее

распространённую форму вовлечения дропперов в преступные схемы дистанционных хищений и создали дополнительные правовые механизмы для пресечения соответствующих каналов вербовки и блокировки оборота платёжных инструментов, используемых в преступной деятельности[184]. Указанные изменения свидетельствуют о стремлении законодателя учитывать современные механизмы функционирования организованной киберпреступности и смещать акцент уголовно-правового противодействия не только на непосредственных исполнителей дистанционных хищений, но и на инфраструктуру их совершения, включая систему подбора, вовлечения и использования лиц, обеспечивающих движение и обналичивание похищенных денежных средств. В этой связи исследование способов вербовки приобретает особое криминологическое значение, поскольку позволяет выявить устойчивые модели формирования преступных связей и механизмы воспроизводства участников дистанционной преступной деятельности, в том числе для их адекватной уголовно-правовой оценки.

В целом вербовка исполнителей дистанционных хищений представляет собой самостоятельный и структурированный элемент механизма организованной киберпреступности. Её содержание и формы напрямую обусловлены распределённым характером преступных групп, цифровой средой функционирования и необходимостью постоянного восполнения человеческих ресурсов. С учётом изложенного способы вербовки исполнителей дистанционных хищений целесообразно разделить на две основные группы: латентное вовлечение и осознанное вовлечение.

Первая группа характеризуется введением лица в заблуждение относительно истинной сущности выполняемых действий. Вербовка осуществляется под видом легальной либо около легальной деятельности и основывается на маскировке преступных задач под социально приемлемые формы занятости. Такое вовлечение нередко осуществляется через

[184] Федеральный закон от 24.06.2025 № 176-ФЗ «О внесении изменений в статью 187 Уголовного кодекса Российской Федерации» [Электронный документ]. – URL: https://www.consultant.ru/document/cons_doc_LAW_508353/ (дата обращения: 12.05.2026).

предложения «удалённой работы» с нейтральными наименованиями должностей (например, оператор, менеджер, посредник, партнёр по платежам), отмечается использование профессиональной финансово-технической терминологии, создающей иллюзию законности операций и поэтапное раскрытие содержания поручаемых действий, при котором противоправный характер деятельности становится очевидным лишь после первичного вовлечения и формирования доверия.

Для осознанного вовлечения характерно прямое информирование потенциального исполнителя о незаконности предполагаемой деятельности и ориентация на лиц, готовых сознательно участвовать в преступлении за вознаграждение. В рамках действия данной модели преступного взаимодействия отмечается рассылка предложений криминального заработка через социальные сети и мессенджеры, адресный подбор лиц, ранее проявлявших интерес к теневым цифровым практикам либо обладающих соответствующими навыками, вовлечение лиц, ранее ставших жертвами аналогичных мошенничеств, с использованием элементов давления, шантажа или угроз, формирование механизмов подконтрольности (фиксация персональных данных, видео подтверждение согласия), направленных на удержание исполнителя в преступной деятельности.

Таким образом, мотивация дистанционных хищений носит системный характер и формируется под воздействием цифровой среды. Её основу составляет корыстный компонент, ориентированный преимущественно не на удовлетворение базовых потребностей, а на получение значительной и устойчивой материальной выгоды. Ему сопутствует рационально-технологический компонент, выражающийся в стремлении минимизировать издержки и риски за счёт удалённого, автоматизированного характера преступных действий. Существенную роль играет профессионально-статусный компонент, связанный с самоутверждением через демонстрацию технической компетентности. Психологический компонент цифровой безличности снижает эмпатию и внутренние запреты за счёт анонимности и

дистанцирования от последствий, а риско-ориентированный – основан на восприятии низкой вероятности привлечения к уголовной ответственности ввиду особенностей функционирования цифровой среды. Дополняет систему ситуативно-оппортунистический компонент, возникающий при случайном доступе к чужим ресурсам в условиях высокой выгоды и низкого субъективного риска. Вместе с тем данные мотивационные компоненты проявляются различно в зависимости от роли лица в преступной структуре. У организатора преобладают мотивы получения систематической выгоды и управления преступным процессом, у технического исполнителя – реализация профессиональных навыков и решение технологических задач, у социального инженера – достижение результата через коммуникативное воздействие, а у номинального участника (дроппера) – получение быстрого вознаграждения при минимальном вовлечении в содержание преступной схемы. Из указанной мотивационной базы логично вытекают способы вербовки, которые опираются на те же психологические механизмы. Вербовка исполнителей дистанционных хищений реализуется по двум принципиально различным криминологическим моделям – латентной и осознанной, каждая из которых использует собственный набор инструментов воздействия. Их объединяет активное использование возможностей цифровой среды, психотехнических методов влияния и организационной иерархии преступных групп, что в совокупности обеспечивает устойчивость и воспроизводимость дистанционных хищений как формы организованной преступной деятельности. При этом в целом проведённый анализ мотивации и механизмов вербовки лиц, совершающих дистанционные хищения, позволяет определить условия, способствующие формированию преступной мотивации и вовлечению новых участников в соответствующую деятельность. К числу таких условий относятся, в частности, корыстная заинтересованность, стремление к получению дохода при минимизации личных рисков, восприятие цифровой среды как пространства относительной анонимности, а также доступность каналов поиска и вовлечения

потенциальных участников. Выявление указанных обстоятельств имеет значение для определения направлений предупреждения дистанционных хищений, которые рассматриваются в следующем параграфе.

3.3. Система предупреждения дистанционных хищений

Переходя к анализу сложившейся в настоящее время системы мер предупреждения дистанционных хищений, отметим, что её основу составляют не только непосредственно меры предупреждения указанной разновидности преступности, определяемые особенностями совершения дистанционных хищений, но и совокупность субъектов, объектов предупреждения. Всё это образует систему предупреждения рассматриваемой преступной деятельности, вследствие чего считаем необходимым поэтапно проанализировать все её основные элементы.

Под объектом предупреждения дистанционных хищений следует понимать совокупность причин, условий, факторов, детерминирующих развитие указанной разновидности преступности, саму преступность, общественные отношения, охраняемые уголовным законом, которым может быть причинён вред в случае совершения дистанционного хищения, а также лиц, которые могут быть подвержены таким преступным посягательствам, и лиц, склонных к совершению дистанционных хищений[185]. Другими словами, под объектом предупреждения в данном случае необходимо понимать всё то, на что направлена деятельность по предупреждению совершения таких преступлений. Поскольку детерминантам рассматриваемой разновидности преступности и самой преступности в предыдущем параграфе посвящено достаточно много внимания, считаем необходимым определить группы лиц, которые потенциально могут совершить дистанционные хищения и чаще всего совершают такие преступления при воздействии на них неблагоприятных внешних факторов. Кроме того, особо выделим саму

[185] Факторный комплекс преступности в современном мире: материалы Международной научной конференции, Москва, 18 ноября 2021 г. / под ред. В.Ю. Голубовского. – М.: Дашков и К°, 2022. С. 80.

личность профилактируемого, потенциально подверженную преступным посягательствам.

Итак, в первую очередь, обозначим, что потенциальными жертвами дистанционных хищений в настоящее время являются практически все лица, имеющие какие-либо денежные средства, имущество или права на имущество. Однако в зоне риска находятся граждане, которые активно пользуются цифровыми технологиями и безналичным расчётом, поскольку чаще всего дистанционные преступники похищают именно «виртуальные» деньги, списывая их разными способами с расчётных счетов граждан. При этом стоит подчеркнуть, что злоумышленники, как правило, «добираются» до денежных средств физических лиц через мобильное устройство, имеющее доступ в сеть Интернет, и на которое установлено приложение «Мобильный банк» или другая программа, позволяющая получить доступ к банковской карте и совершать безналичные переводы. В связи с этим считаем, что активное пользование современными гаджетами и соответствующим программным обеспечением в несколько раз повышает шансы стать жертвой преступника, совершающего в дистанционной форме хищения[186].

Кроме того, считаем необходимым указать, что в «красной» зоне риска находятся социально незащищённые лица, а именно – пожилые люди, которые в силу возраста и своего социального положения, как правило, имеют некоторые сбережения, хранят их в банке, но ввиду низкого уровня цифровой грамотности и высокой степени доверчивости чаще других становятся жертвами уловок злоумышленников. Так, согласно данным социологического исследования, по мнению респондентов – сотрудников правоохранительных органов, 52% потерпевших при совершении дистанционных хищений в настоящее время составляют именно пожилые лица (см. Приложение 1-2). Исследователь А.В. Сычёва справедливо замечает, что пожилые люди редко хорошо владеют навыками работы за

[186] Рогова Е.В. Уголовно-правовое противодействие преступлениям против собственности в современных условиях // Уголовная юстиция. 2025. № 26. С. 43–47.

компьютером, пользования мобильным устройством на «продвинутом» уровне, в результате чего преступникам нередко удаётся без значительных трудностей с помощью нехитрых мошеннических действий завладеть денежными средствами пенсионеров. Это обусловливает необходимость проведения в отношении пожилых людей особенно активной профилактической работы, позволяющей обезопасить данную социальную группу от дистанционных хищений. Однако, справедливости ради, отметим, что специфика развития указанной разновидности преступности, выражающаяся в чрезвычайно стремительном изменении форм и способов совершения таких преступлений на фоне постоянной трансформации цифрового пространства и появления новых информационных технологий, также обязывает субъектов предупреждения повышать уровень цифровой грамотности всего населения, обеспечивая тем самым заблаговременное противодействие совершению дистанционных хищений.

Также, как было отмечено ранее, к объектам предупреждения необходимо относить лиц, склонных к совершению того или иного вида преступлений. Считаем, что в случае с дистанционными хищениями такими лицами будут, в первую очередь, граждане, имеющие, как минимум, базовые навыки работы с различными электронными гаджетами. Особо выделяются криминально заинтересованные лица, обладающие знаниями, умениями и навыками в сфере компьютерной информации на «продвинутом» уровне. Именно их «руками», как правило, совершаются наиболее опасные преступные посягательства. Так, например, лица, действующие в составе организованной группы, обвинённые приговором К. городского суда Владимировской области в июне 2023 г. в совершении преступлений, предусмотренных ч. 5 ст. 33, ч. 3 ст. 272, ч. 5 ст. 33, ч. 2 ст. 273 и ч. 4 ст. 159[6] УК РФ, обладали специальными знаниями, умениями и навыками работы в сфере компьютерной информации, функционирования различных банковских и международных платежных систем, а также регулярно повышали свой криминальный профессиональный уровень, справедливо

полагая, что без соответствующих знаний, умений и навыков совершить указанное преступное посягательство было мало возможно[187]. В подтверждение также укажем, что согласно данным выборочного статистического исследования, среди преступников, совершающих дистанционные хищения, высшее образование имеют 18%, причём около половины технической или экономической направленности, а совокупно 76% преступников имеют образование не ниже среднего специального, что отражает требуемый уровень цифровой компетентности (см. п. 3.1)[188].

Также отдельно выделим «традиционные» группы лиц, склонных к совершению преступлений вообще и дистанционных хищений в частности. К таким группам, прежде всего, относятся лица с устойчивыми криминогенными установками, ранее судимые за корыстные и корыстно-насильственные преступления, а также лица, находящиеся в неблагоприятной социально-экономической ситуации. Для указанной категории характерно использование дистанционных хищений как относительно «безопасного» с точки зрения разоблачения способа преступного обогащения, не требующего непосредственного контакта с потерпевшим. Нередко такие лица вовлекаются в преступную деятельность в качестве исполнителей дистанционных хищений в составе организованной преступной группировки, выполняя вспомогательные функции (так называемые «дроппы», курьеры, лица, предоставляющие свои банковские счета и средства связи и т.д.). При этом внешняя простота выполняемых ими действий зачастую нивелирует осознание высокой общественной опасности совершаемого, что требует адресного профилактического воздействия, направленного на формирование позитивной правовой культуры и высокого

[187] Приговор № 1-12/2023 1-390/2022 от 16 июня 2023 г. К. городского суда [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/2dMsxJbKfhLR/ (дата обращения: 04.03.2026).
[188] Судебная практика по уголовным делам России [Электронный ресурс]. – URL: https://sudact.ru/regular/ (дата обращения: 05.03.2026); Архив уголовных дел Белгородского областного суда [Электронный ресурс]. – URL: https://oblsud--blg.sudrf.ru/modules.php?name=sud_delo (дата обращения: 06.03.2026).

уровня правосознания и предупреждение вовлечения в преступную деятельность на ранних стадиях[189].

Так, объект предупреждения дистанционных хищений представляет собой многоуровневую и сложную систему, включающую как потенциальных потерпевших, так и лиц, склонных к совершению указанных преступлений, а также причины, факторы и условия, способствующие их совершению. Многообразие и неоднородность данных объектов предопределяют необходимость комплексного и дифференцированного профилактического воздействия, эффективность которого во многом зависит от согласованной деятельности различных субъектов предупреждения. В этой связи представляется целесообразным перейти к рассмотрению данного вопроса.

Условно современные криминологи разделяют субъектов предупреждения на такие группы как специализированные и факультативные субъекты, а также субъекты-участники.

К специализированным субъектам предупреждения относят различные государственные и негосударственные организации, а также органы власти разных уровней, целенаправленно осуществляющие специальные полномочия по борьбе с той или иной разновидностью преступной деятельности. В отношении противодействия дистанционным хищениям можно выделить такие специализированные субъекты предупреждения, как органы МВД России, ФСИН РФ, Прокуратура РФ, Следственный комитет РФ и т.д. В разрезе борьбы с дистанционными хищениями особо выделим специальное Управление по организации противодействия противоправным использованиям информационно-коммуникационных технологий МВД РФ (далее – Управление), созданное в структуре Министерства внутренних дел России в сентябре 2022 г. По утверждению официального представителя МВД РФ И.В. Волк, данное структурное подразделение было создано в связи

[189] Антонян Ю.М., Эминов В.Е. Личность преступника. Криминолого-психологическое исследование [Электронный ресурс]. – URL: https://fb2.top/lichnosty-prestupnika-kriminologo-psihologicheskoe-issledovanie-522609/read (дата обращения: 07.03.2026).

с возросшим количеством кибератак, дистанционных хищений и общим активным развитием противозаконной деятельности в цифровой индустрии[190]. Согласно положению, к основным задачам деятельности Управления относится организация выявления, предупреждения, пресечения, раскрытия преступлений, которые совершаются с использованием информационно-коммуникационных технологий, анализ криминалистически значимой для предупреждения таких преступлений информации, обеспечение взаимодействия Управления с другими органами власти России и некоторые другие направления работы[191]. При этом в положениях отдельных территориальных подразделений Управления (например, в УБК ГУ МВД России по Санкт-Петербургу и Ленинградской области) дополнительно уточняется, что одной из главных задач деятельности таких подразделений является предупреждение, выявление, пресечение, раскрытие именно имущественных преступлений, которые совершаются с использованием информационно-коммуникационных технологий[192].

Факультативные субъекты предупреждения – это различные органы и организации, для которых предупреждение, выявление, пресечение, раскрытие различных видов преступлений не является основным направлением деятельности. В качестве примера в данном случаем можно привести органы исполнительной власти Российской Федерации различных уровней, отвечающие за реализацию государственной политики в сфере печати и массовой информации, СМИ. Общеизвестно, что наиболее распространённым способом повышения цифровой грамотности населения вне образовательных организаций является как раз проведение различного рода информационных кампаний, в ходе которых до граждан доводятся актуальные сведения о наиболее популярных в криминальной среде способах

[190] В МВД создано управление по борьбе с киберпреступностью [Электронный ресурс]. – URL: https://www.kommersant.ru/doc/5592758 (дата обращения: 08.03.2026).
[191] Положение об Управлении по организации борьбы с противоправным использованием информационно-коммуникационных технологий Министерства внутренних дел Российской Федерации [Электронный ресурс]. – URL: https://xn--b1aew.xn--p1ai/mvd/structure1/Upravlenija/ (дата обращения: 09.03.2026).
[192] Управление по борьбе с противоправным использованием информационно-коммуникационных технологий [Электронный ресурс]. – URL: https://otdel-k.spb.ru/ (дата обращения: 10.03.2026).

совершения преступлений, в том числе и дистанционных хищений. Например, в настоящее время на известных новостных порталах в сети Интернет регулярно размещается информация о схемах противостояния, так называемым, «телефонным» мошенникам. Так, «Лента.ру» поясняет, что к типичным схемам таких мошенничеств сегодня можно отнести следующие сценарии: «попавшие в беду родственники», «звонок из службы безопасности банка», «ошибочный перевод», «вымышленный выигрыш в лотерею», «просьба перезвонить от знакомого», «обман по СМС-рассылке» и многое другое[193]. Издательство «Коммерсантъ» также указывает, что необходимо делать, если Вам звонит телефонный мошенник, и как определить, что это именно он[194]. На официальных сайтах органов власти различного уровня тоже периодически размещается вся необходимая информация по противодействию дистанционным хищениям[195]. Полагаем, что проведение такого рода информационных кампаний в настоящее время достаточно эффективно, поскольку такие инструменты имеют большие возможности для воздействия на широкую аудиторию, вследствие этого считаем необоснованным недооценивание роли факультативных субъектов в сфере предупреждения исследуемой разновидности преступности, хотя и их работа требует совершенствования, согласно данным опроса сотрудников правоохранительных органов, которые были приведены раннее.

Третьим элементом системы субъектов предупреждения преступлений являются субъекты-участники – это лица и различные организации, которые косвенно принимают участие в правоохранительной деятельности профилактического характера на служебной или добровольной основе. К субъектам-участникам предупреждения дистанционных хищений можно, к примеру, отнести частные предприятия, технически обеспечивающие

[193] По телефону и через Госуслуги. Главные схемы, которыми пользуются мошенники в 2023 году, чтобы красть деньги россиян [Электронный ресурс]. – URL: https://lenta.ru/articles/2023/08/07/moshenniki/ (дата обращения: 13.03.2026).

[194] Что делать, если звонит телефонный мошенник [Электронный ресурс]. – URL: https://www.kommersant.ru/doc/4977233 (дата обращения: 14.03.2026).

[195] Профилактика мошенничеств с использованием средств сотовой связи и Интернет-ресурсов [Электронный ресурс]. – URL: https://adm.gov86.org/399/688/795/3110/ (дата обращения: 15.03.2026).

информационную защиту сервисов различных кампаний, в том числе поддерживая нормальную работу виртуальных сетей и проведение в них финансовых операций. Так, ПАО «Сбербанк» предлагает своим клиентам различные сервисы кибербезопасности в приложении СберБанк Онлайн с целью защиты безналичных денежных средств, хранящихся на расчётных счетах граждан: «Определитель номера», «Антивирус», «Близкие рядом», «Закрыть доступ к картам, счетам и вкладам» и другое. Эти сервисы являются продуктами работы внутренней службы безопасности банка, и с их помощью также косвенно осуществляется борьба с дистанционными хищениями[196]. С подобными предложениями защиты сегодня также выступают операторы сотовой связи, хотя и они требуют дальнейшего совершенствования в связи с усложнением механизмов преступного поведения.

И, наконец, самым важным элементом системы предупреждения преступности является совокупность мер борьбы с тем или иным криминальным явлением, направленных на противодействие разным процессам детерминации конкретных видов преступлений. По классификации наиболее распространённой в криминологической науке, все меры предупреждения преступности делятся по их направленности действия, а именно на общесоциальные, правовые, организационно-управленческие, технические, культурно-воспитательные и некоторые другие меры. Считая представленную классификацию наиболее исчерпывающей, в представленном исследовании будем придерживается именно этой «схемы» для определения специфики предупреждения дистанционных хищений.

Меры общесоциального характера, безусловно, перед собой не ставят непосредственной цели борьбы с преступностью в самых разных её проявлениях и предупреждения преступной деятельности. Однако, учитывая тот факт, что хищения (пусть и дистанционные) преследуют основную

[196] Сервисы кибербезопасности в приложении СберБанк Онлайн [Электронный ресурс]. – URL: http://www.sberbank.ru/ru/person/cybersecurity/sberbank_online/ (дата обращения: 16.03.2026).

задачу – материального обогащения, данные меры приобретают важное криминологическое значение[197]. Согласно официальным сведениям МВД России, удельный вес лиц без постоянного источника дохода, совершивших преступления, в 2022-2025 гг. составил более 60%[198]. При этом, например, по ст. 159^3 УК РФ (мошенничество с использованием электронных средств платежа – «классической» разновидности дистанционного хищения) в среднем более 70% осуждённых составляют трудоспособные лица, которые не имеют постоянного источника дохода[199]. Это даёт основание полагать, что нестабильное материальное положение является одним из главных факторов, детерминирующих рост дистанционных хищений, а значит, общесоциальные меры предупреждения преступности экономического характера, направленные на укрепление материальной защищённости граждан, действительно, эффективны в деле противодействия рассматриваемой разновидности преступной деятельности.

Также подчеркнём важность общесоциальных мер предупреждения преступности, имеющих политический характер. Безусловно, политические мотивы при совершении киберпреступлений корыстной направленности имеют далеко не доминирующую роль. Они чаще всего имеют место быть только при совершении кибератак на IT-системы других государств, имеющие цель вывести из строя работу информационных баз, обеспечивающих хранение важной для национальной безопасности государства информации, по «платному заказу» правительств «недружественных» стран[200]. Однако функционирование самой политической системы также оказывает самое непосредственное влияние на рост преступности. По справедливому замечанию Д.О. Тепловой,

[197] Бражников Д.А. Противодействие тайному хищению чужого имущества: монография. М.: ЮНИТИ-ДАНА, 2017. С. 151.
[198] Краткая характеристика состояния преступности в Российской Федерации [Электронный ресурс]. – URL: https://xn--b1aew.xn--p1ai/reports/item/47055751/ (дата обращения: 17.03.2026).
[199] Основные социально-демографические и уголовно-правовые признаки осужденных по ст. 159^3 и 159^6 УК РФ [Электронный ресурс]. – URL: https://www.advgazeta.ru/mneniya/osnovnye-sotsialno-demograficheskie-i-ugolovno-pravovye-priznaki-osuzhdennykh-po-st-159-3-i-159-6-uk/ (дата обращения: 18.03.2026).
[200] Рогова Е.В. Уголовно-правовое противодействие киберпреступности в России и Китае: сравнительно-правовой аспект // Вестник Университета прокуратуры Российской Федерации. 2024. № 1(99). С. 84–90.

политическая воля к предупреждению и противодействию той или иной разновидности преступности не может быть в реальности претворена в жизнь без наведения порядка в организации деятельности самих структур органов власти и управления[201]. Так, коррупция, протекционизм, разобщённость и рассогласованность региональной и федеральной властей, а также иные негативные явления, «паразитирующие» в политической системе, только вредят нормальному развитию общественных отношений, укреплению институтов гражданского общества и правового государства. Вследствие этого считаем, что избавление общества и государства от этих негативных политических явлений необходимо не только для общего укрепления развития политических отношений в стране, но и для предупреждения разного рода преступлений, в том числе и дистанционных хищений, поскольку стабильность политической сферы жизни государства обеспечивает также и стабильность работы властных структур, в задачи которых входит, в том числе противодействие преступной деятельности разных видов и форм.

На основании изложенного можно сделать вывод о том, что общесоциальные меры предупреждения как общеуголовной преступности в целом, так и отдельных её видов, включая дистанционные хищения, в долгосрочной перспективе способны продемонстрировать высокую эффективность. Именно общесоциальные меры предупреждения преступности могут стать надёжной основой для проведения специально-криминологической профилактики, противодействуя развитию криминогенных факторов, поэтому нивелировать их значимость вопреки сложившимся в криминологической науке стереотипам не вполне оправданно.

Далее выделим правовые меры предупреждения дистанционных хищений, направленные на совершенствование отечественного

[201] Теплова Д.О. Криминологические основы противодействия организованному мошенничеству: монография. М.: РГУП, 2017. С. 175.

законодательства, обеспечивающего защиту личности, общества и государства от указанной разновидности преступной деятельности. Анализируя данный вопрос, считаем необходимым подчеркнуть, что современный уголовный закон ввиду стремительного развития научно-технического прогресса в сфере цифровых технологий имеет значительное количество недостатков в сфере борьбы с дистанционными хищениями. Как уже многократно указывалось ранее, такого рода деяния чаще всего квалифицируют по п. «г» ч. 3 ст. 158 УК РФ УК РФ (кража с банковского счета), ст. 159^3 (мошенничество с использование электронных средств платежа), ст. 159^6 (мошенничество в сфере компьютерной информации), ст. 272 (неправомерный доступ к компьютерной информации), ст. 273 (создание, использование и распространение вредоносных компьютерных программ) УК РФ и некоторым другим статьям[202]. Однако правоприменители, занимающиеся предупреждением дистанционных хищений, справедливо отмечают определённые трудности при проведении правовой оценки совершаемых противоправных деяний в рамках действующей уголовно-правовой системы[203], что указывает на существенные недостатки отечественного законодательства в сфере борьбы с этим видом преступности. Так, согласно данным проведённого социологического опроса, большинство сотрудников оценивают правовые механизмы как недостаточные или требующие доработки. Только 9% опрошенных считают их полностью достаточными, тогда как 57% оценивают их как скорее недостаточные или недостаточные (см. Приложение 1-2). Это свидетельствует о необходимости совершенствования нормативно-правовой базы, в том числе в части ответственности за дистанционные хищения, а также расширения полномочий и возможностей правоохранительных органов в условиях цифровой среды (более подробно меры

[202] Рябинина Т.К., Ряполова Я.П., Чистилина Д.О. актуальные проблемы выявления и расследования дистанционных хищений с банковского счета // Вестник БелЮИ МВД России. 2023. № 4. С. 31-38.

[203] Казанские уголовно-процессуальные и криминалистические чтения: материалы Междунар. науч-практ. конф. (Казань, 28 апр. 2022 г.): в 2 ч. / редкол.: Ю.Н. Кулешов (отв. ред.) и др.; Казан. ин-т (фил.) ВГУЮ. Казань: ЮрЭксПрактик, 2022. С. 80.

совершенствования отечественного уголовного законодательства в данной сфере приведены в Главе 2 настоящего исследования). Вместе с тем укажем, что правовые меры предупреждения должны учитывать дифференциацию лиц, участвующих в совершении дистанционных хищений, поскольку организаторы преступных схем, технические исполнители, номинальные участники («дропперы») и лица, осуществляющие «социально-инженерическое» воздействие, обладают различной степенью общественной опасности и выполняют неодинаковые функции в механизме преступной деятельности. В связи с этим совершенствование уголовно-правового регулирования должно быть направлено не только на устранение пробелов квалификации, но и на формирование дифференцированного подхода к уголовно-правовой оценке действий различных участников дистанционных преступных схем с учётом их фактической роли, уровня вовлечённости и характера выполняемых функций.

Организационно-управленческие меры предполагают разработку программно-целевого планирования деятельности субъектов предупреждения и координацию их активностей в сфере борьбы с конкретными видами преступности, в том числе и хищениям, совершаемым в дистанционной форме. К числу таких мер, к примеру, можно отнести усовершенствование работы сотрудников правоохранительных органов, в чьи должностные обязанности непосредственно входит противодействие дистанционным хищениям. С этой целью считаем необходимым обеспечить надлежащее кадровое обеспечение субъектов предупредительной деятельности, и, прежде всего, сотрудников органов внутренних дел. А.Я. Минин справедливо указывает, что в связи со стремительным развитием цифровых технологий сотрудникам компетентных органов приходится сегодня быстро осваивать специальные профессиональные компетенции[204]. Несмотря на значительную сеть образовательных учреждений в России, осуществляющих подготовку будущих сотрудников правоохранительных

[204] Минин А.Я. Актуальные проблемы цифрового права. М.: МГПУ, 2021. С. 73.

органов, вопросы противодействия киберугрозам современности не всегда находят должное отражение в учебных планах, а количество вузов, обучающих студентов именно в соответствии с новыми цифровыми запросами времени, ограничено. В связи с этим согласимся с учёными, указывающими на необходимость системной подготовки специалистов по направлению «Информационная безопасность» в вузах высших МВД России с целью обеспечения правоохранительных органов компетентными сотрудниками, способными противостоять новым криминальным угрозам[205]. Кроме того, укажем на необходимость открытия соответствующих образовательных программ высшего образования в системе вневедомственных высших учебных заведений[206].

Не менее актуально и должное методическое обеспечение работы соответствующих подразделений органов внутренних дел, позволяющее достойно противостоять «цифровым» преступникам и выстраивать всю предупредительную деятельность подразделения с учётом особенностей совершения конкретных видов дистанционных хищений, специфики оперативной обстановки в том или ином регионе, других криминологически значимых критериев. Считаем, что разработка соответствующих методических рекомендаций по вопросам раскрытия и расследования дистанционных хищений должна происходить посредством обобщения и анализа юридической практики при совместных усилиях научного сообщества юристов, занимающихся проблемами противодействия дистанционным хищениям, и сотрудников правоохранительных органов, специализирующихся на расследовании и раскрытии такого рода преступлений (например, сотрудников подразделений Управления по организации борьбы с противоправным использованием информационно-коммуникационных технологий МВД РФ). Подчеркнём, что в настоящее

[205] Пархоменко С.В., Евдокимов К.Н. Предупреждение компьютерной преступности в Российской Федерации: интегративный и комплексный подходы // Всероссийский криминологический журнал. 2015. № 2. С. 265-276.

[206] Рогова Е.В., Перетолчин А.П. Преступления против собственности в условиях цифровой трансформации // Академический юридический журнал. 2022. Т. 23, № 3(89). С. 256–264.

время в систематизированном виде представлены только отдельные авторские рекомендации по предупреждению подобного рода хищений[207], однако комплексные тактико-криминалистические рекомендации, направленные на повышение эффективности раскрытия, расследования и предупреждения дистанционных хищений сегодня по-прежнему отсутствуют.

Кроме того, укажем на необходимость обеспечения эффективного внутриведомственного и межведомственного взаимодействия структур, осуществляющих противодействие дистанционным хищениям. Примером такого эффективного взаимодействия является выстраивание «деловых» отношений между созданными в 2022 г. в России подразделениями по борьбе с противоправным использованием информационно-коммуникационных технологий и основными операторами сотовой связи и банками России с тщательной проработкой вопроса механизмов сотрудничества между ведомствами по части оперативного исполнения запросов правоохранительных органов банками и операторами сотовой связи с целью повышения раскрываемости дистанционных хищений[208]. Однако в настоящее время существуют примеры и не совсем удачного выстраивания такого межведомственного взаимодействия указанных структур. Например, как справедливо отмечают исследователи, сегодня отсутствуют механизмы оперативной блокировки так называемых фишинговых сайтов (в настоящее время этот вид деятельности осуществляется исключительно через посредничество Роскомнадзора России)[209], вследствие чего до вынесения соответствующего решения о блокировке проходит слишком много времени, и злоумышленникам удаётся совершить ещё множество преступных деяний, что значительно ухудшает криминогенную обстановку и способствует

[207] См., например: Мазуров И.Е. Методика расследования хищений, совершенных с использованием интернет-технологий: дис. ... канд. юрид. наук. – Ростов, 2017. – 188 с.
[208] Шпетная А.В. Взаимодействие правоохранительных органов с банками и операторами сотовой связи в предупреждении дистанционных мошенничеств // Юридическая наука. 2023. № 5. С. 209-211.
[209] Евтушенко И.И. Актуальные направления виктимологической профилактики дистанционных хищений // Виктимология. 2022. № 1. С. 90-98.

развитию у преступников криминальных умений и навыков, повышая их уровень криминального профессионализма.

Отдельный вопрос связан с международным сотрудничеством в сфере противодействия дистанционным хищениям, поскольку значительная часть таких преступлений, как справедливо отмечает А.В. Чернякова, носит трансграничный характер и совершается с использованием зарубежной цифровой инфраструктуры, иностранных платёжных сервисов, хостинг-провайдеров и сетей связи[210]. В этих условиях эффективное предупреждение и раскрытие дистанционных хищений невозможно без налаженного взаимодействия российских правоохранительных органов с иностранными. При этом отдельно следует подчеркнуть, что Интерпол (The International Criminal Police Organization – Международная организация уголовной полиции) выступает ключевой структурой, объединяющей усилия силовых органов государств-членов для обмена информацией и координации действий по выявлению и пресечению трансграничной преступной деятельности, включая преступления в цифровой сфере[211].

В продолжение укажем, что важнейшую роль в указанном направлении играет сотрудничество Министерства внутренних дел Российской Федерации с Интерполом. Несмотря на попытки некоторых государств ограничить международное взаимодействие, Российская Федерация продолжает поддерживать активные связи с Интерполом и участвует в международном обмене оперативной информацией о преступниках и их действиях, в том числе совершающих дистанционные хищения. Как отметил глава МВД России В.А. Колокольцев, сотрудничество с Интерполом в настоящее время продолжается и включает передачу данных о лицах, причастных к тяжким преступлениям, из зарубежных юрисдикций в Россию, в том числе если речь

[210] Чернякова А.В. Международный и зарубежный опыт уголовно-правового противодействия хищениям, совершаемым с использованием компьютерной информации // Юридическая наука и правоохранительная практика. 2018. № 4 (46). С. 168-179.
[211] Interpol [Электронный ресурс]. – URL: https://www.interpol.int/ (дата обращения: 19.03.2026).

идёт о дистанционных хищениях[212]. Так, например, Интерпол предоставляет Национальному центральному бюро Интерпола МВД России и другим участникам международного сотрудничества инструменты для обмена криминальной информацией, в том числе базами данных, международными уведомлениями и каналами связи, ускоряющими процесс получения и передачи данных о подозреваемых, украденных средствах и цифровых следах преступной деятельности[213].

При этом взаимодействие через Интерпол включает не только правоохранительные запросы или розыск подозреваемых, но также участие в международных операциях по борьбе с транснациональными группами, осуществляющими дистанционные хищения и иные киберпреступления. Международные операции, координируемые Интерполом совместно с национальными органами, демонстрируют эффективность коллективного обмена данными и ресурсами для пресечения преступной инфраструктуры, используемой для дистанционных хищений, фишинга, внедрения вредоносного ПО и незаконного вывода денежных средств. Кроме того, международное сотрудничество способствует унификации подходов и выработке общих стандартов реагирования на киберугрозы, обмену передовыми практиками и тактико-оперативными методиками[214]. И такие механизмы важны для адаптации национальной практики расследования дистанционных хищений к современным вызовам цифровой преступности, а также ускорения раскрытия транснациональных преступных схем и обмену информацией между странами-участницами.

Однако при всех положительных эффектах следует отметить, что потенциал международного сотрудничества между правоохранительными органами разных стран реализован не в полной мере. Существуют

[212] Сотрудничество с Интерполом продолжается [Электронный ресурс]. – URL: https://ria.ru/20240402/ (дата обращения: 20.03.2026).
[213] Что такое Интерпол и чем он занимается [Электронный ресурс]. – URL: https://www.rbc.ru/base/21/02/2025/ (дата обращения: 21.03.2026).
[214] Международное сотрудничество [Электронный ресурс]. – URL: https://rapsinews.ru/digital_law_news/20251028/ (дата обращения: 22.03.2026).

объективные препятствия, связанные с различиями в национальном законодательстве, сложностью процедур международной правовой помощи, а также неполным исполнением ответов на информационные запросы между государствами. В этой связи представляется целесообразным дальнейшее совершенствование правовых механизмов обмена информацией, использование электронных каналов взаимодействия и разработку и дальнейшее совершенствование совместных образовательных и методических программ для повышения качества международной координации в сфере борьбы с дистанционными хищениями. Между тем, в целом международное сотрудничество, реализуемое при участии МВД России и Интерпола, выступает важным организационно-управленческим «инструментом» повышения эффективности предупреждения дистанционных хищений, особенно в условиях трансграничности цифровой преступности, и требует дальнейшего развития и институционального укрепления.

Далее укажем, что особое значение в системе организационно-управленческих мер предупреждения дистанционных хищений также имеют единые информационные базы с криминологически значимой информацией, создаваемые не только на международном уровне (например, в рамках взаимодействия с Интерполом), но на национальном – в специализированных подразделениях органов внутренних дел, осуществляющих борьбу с противоправным использованием информационно-коммуникационных технологий. Речь, прежде всего, идёт о подразделениях по борьбе с киберпреступностью (в том числе о подразделениях Управления по организации борьбы с противоправным использованием информационно-коммуникационных технологий МВД России), в рамках деятельности которых формируются и постоянно актуализируются специализированные ведомственные базы данных. Указанные информационные ресурсы аккумулируют сведения о фишинговых интернет-ресурсах, мошеннических сайтах и страницах в социальных сетях, номерах телефонов, банковских

картах, электронных кошельках и иных платёжных инструментах, используемых в преступных целях, а также о типовых «сценариях» и алгоритмах совершения дистанционных хищений и другом[215]. Анализ данных массивов позволяет не только выявлять конкретных лиц, причастных к совершению преступлений, но и прогнозировать развитие криминальных схем, своевременно фиксировать появление новых способов хищений и формировать адресные профилактические меры. Кроме того, использование таких информационных ресурсов способствует выявлению серийности преступной деятельности и установлению устойчивых межрегиональных и трансграничных преступных связей.

Так, организационно-управленческие меры предупреждения дистанционных хищений играют системообразующую роль в обеспечении координации деятельности субъектов профилактики, формировании кадрового потенциала, развитии методического обеспечения и налаживании межведомственного и международного взаимодействия. Для повышения результативности организационно-управленческих мер представляется целесообразным реализовать комплекс усовершенствований, ориентированных на выявление и пресечение деятельности различных категорий участников дистанционных хищений. В частности, необходимы создание специализированных образовательных программ и курсов повышения квалификации сотрудников правоохранительных органов в сфере цифровой криминалистики и противодействия дистанционным хищениям, что позволит более эффективно выявлять организаторов преступных схем, технических исполнителей и лиц, осуществляющих «социально-инженерическое» воздействие. Одновременно требуется разработка комплексных методических рекомендаций по раскрытию и предупреждению дистанционных хищений с учётом распределения ролей между участниками преступной деятельности, а также расширение и актуализация ведомственных и международных информационных баз, содержащих

[215] МВД России [Электронный ресурс]. – URL: https://мвд.рф (дата обращения: 23.03.2026).

сведения о типичных способах совершения преступлений, используемых цифровых инструментах и механизмах вовлечения номинальных участников («дропперов»). Кроме того, особое значение приобретает оптимизация межведомственного и международного взаимодействия, включая ускорение обмена оперативной информацией и внедрение защищённых электронных каналов связи, обеспечивающих своевременное выявление организованных преступных групп и координацию мер по пресечению дистанционных хищений. Далее перейдём к анализу действующих технических мер предупреждения хищений, совершаемых дистанционно.

В настоящее время для защиты от дистанционных хищений применяют технические меры, обеспечивающие защиту финансовых отношений. Они включают в себя несколько уровней: меры по защите устройств клиента, каналов связи и инфраструктуры банка. Разберём эти меры более подробно. В первую очередь укажем, что для защиты устройств клиента в настоящее время применяется комплекс технологий. Самым распространённым способом защиты является многофакторная аутентификация, которая требует обязательного использования второго фактора при входе с нового устройства или изменении настроек. Это может быть одноразовый код из СМС, push-уведомление в зарегистрированном приложении или аппаратный ключ. Данные технологии защищают от фишинга и кражи паролей, делая такой «украденный» пароль бесполезным без доступа к устройству подтверждения. Технология 3D Secure версии 2.0, используемая при онлайн-оплате, в свою очередь, анализирует сотни параметров, включая историю покупок, устройство и геолокацию. Если не обнаружено подозрительных манипуляций, то платеж проходит без дополнительных действий. В сомнительных случаях система запрашивает подтверждение в приложении по биометрии или SMS-кодом. Это защищает от мошеннических списаний,

осуществляемых в виртуальной среде[216]. Следующим важным способом защиты клиента в современности является биометрическая верификация с помощью сканирования лица, отпечатка пальцев или радужной оболочки глаза. Биометрический шаблон хранится в защищенной области устройства, что предотвращает удаленный доступ к счету в случае кражи логина и пароля, а также защищает от подмены лица по фото или видео[217]. Также одним из способов защиты клиента остается сканирование устройства на угрозы мобильным приложением банка в фоновом режиме. При этом проверяется наличие root-прав, эмуляторов, программ удаленного доступа и т.п. При обнаружении критических рисков доступ к операциям блокируется. Это защищает от атак с использованием вредоносного программного обеспечения и ситуаций, когда мошенник убедил жертву установить программу удаленного доступа.

Следующий уровень технических мер – это защита каналов связи. Укажем, что в современности для защиты каналов связи и передачи данных используется комплекс мероприятий, направленных на создание технических барьеров для перехвата данных или подмены получателя. HTTPS или TLS шифрование обеспечивает защищенный канал передачи всех данных между клиентом и банком. Это предотвращает перехват трафика и атаки типа Man-in-the-Middle («Человек посередине») в публичных Wi-Fi сетях[218]. Антифрод-мониторинг интернет-эквайринга анализирует интернет-платежи по сотням условий в реальном времени. Система сопоставляет IP-адрес покупателя с адресом магазина, проверяет BIN-коды карт и частоту попыток. Подозрительные операции блокируются, что защищает от тестовых транзакций мошенников и использования похищенных данных карт в сомнительных магазинах. Система «Антифрод» уже со стороны банка

[216] 3-D Secure 2.0 [Электронный ресурс]. – URL: https://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:3-D_Secure_2.0_(3D-Secure_3DS) (дата обращения: 24.03.2026).

[217] Винокуров А.В. Биометрические системы идентификации в кредитных организациях как инструмент противодействия мошенничеству // Финансы и кредит. 2016. № 21 (693). С. 15-23.

[218] Русаков А.О., Чалый Р.А. Методы защиты от атаки «Человек посередине» в Wi-Fi сетях // Актуальные проблемы авиации и космонавтики. 2016. № 12. С. 767-769.

анализирует все операции в дистанционном банковском обслуживании. ML-модели ищут аномалии, в том числе посредством ИИ-анализа мошеннических операций, такие как резкое изменение поведения клиента, наличие нехарактерных операций, большое количество запросов и т.п. Это защищает от любых сомнительных транзакций, включая случаи, когда клиент действует под влиянием мошенников. Проверка получателя через сверку счетов происходит при создании нового шаблона перевода или вводе реквизитов. Система проверяет их по базам данных и показывает клиенту подтверждение принадлежности счета[219]. Это, в том числе, предотвращает перевод денег на счета «дропов», если клиента убедили перевести средства на, так называемый, безопасный счет. В качестве примера приведём разработку ПАО «Сбербанк России» для пользователей приложения «СберБанк Онлайн» сервиса «Проверка операций близкого», позволяющий технически с помощью ряда автоматических операций, онлайн-помощнику определить законность проводимых безналичных переводов денежных средств того или иного человека, не способного самостоятельно противостоять мошенникам. Приложение «СберБанк Онлайн» пришлёт автоматическое уведомление, в том случае, если пользователь захочет перевести кому-либо денежные средства, с помощью которого можно либо подтвердить перевод, либо отклонить (в случае бездействия в течение 12-ти часов приложение самостоятельно отклонит перевод)[220].

Отдельно укажем, что в том случае, если мошеннику всё же удалось инициировать операцию, используется уровень защиты внутри банковской инфраструктуры (заключительный уровень реализации технических мер предупреждения дистанционных хищений в современности). При использовании данного механизма подозрительные операции, получившие при запросе одобрение от клиента, не проводится мгновенно, а

[219] Антифрод-системы (Anti-fraud) [Электронный ресурс]. – URL: https://encyclopedia.kaspersky.ru/glossary/antifraud/ (дата обращения: 25.03.2026).
[220] Проверка переводов близкого [Электронный ресурс]. – URL: http://www.sberbank.ru/ru/person/dist_services/blizkie-ryadom (дата обращения: 26.03.2026).

запрашивается дополнительное подтверждение через звонок робота или push-уведомление. Это защищает от импульсивных переводов, давая клиенту время проанализировать операцию на предмет возможного преступного воздействия со стороны мошенников. Автоматический обмен данными об угрозах обеспечивает синхронизацию в реальном времени информации о мошеннических счетах, IP-адресах и номерах телефонов между банками и регулятором. Это предотвращает повторное использование одной и той же мошеннической инфраструктуры против разных банков и защищает от много эпизодных дистанционных хищений с использованием различных подставных лиц и счетов. При этом ключевым элементом данной системы является сбор информации о том, какие операции оказались мошенническими, а какие – ложными срабатываниями. При этом для дальнейшего самообучения системы полученные данные постоянно возвращаются в ML-модели, обрабатываются и используются в процессе адаптации к новым преступным угрозам.

Для объективной оценки эффективности представленных технических мер используется система ключевых показателей, разделенных на operational-метрики (работа в реальном времени) и бизнес-метрики (финансовый результат). Главным интегральным показателем является процент отраженных попыток хищений. При этом в настоящее время операторы связи посредством предоставления услуг мобильного скоринга в качестве дополнений к антифрод-решениям банков демонстрируют способность блокировать до 90-95% мошеннических атак до того, как деньги будут списаны со счета. Это означает, что из ста попыток украсть деньги система пропускает лишь 5-10, что является достаточно высоким результатом[221].

Однако, несмотря на относительно высокую эффективность современных средств защиты, имеются ряд факторов, которые позволяют

[221] Билайн признан самым безопасным оператором в 2025 году по комплексу механизмов защиты абонентов сотовой связи [Электронный ресурс]. – URL: https://www.comnews.ru/content/241963/2025-10-28/2025-w44/1180/bilayn-priznan-samym-bezopasnym-operatorom-2025-godu-kompleksu-mekhanizmov-zaschity-abonentov-sotovoy-svyazi (дата обращения: 27.03.2026).

преступникам находить слабые места в системах защиты и осуществлять дистанционные хищения. При этом главным фактором риска объективно являются постоянно развивающиеся технологии социальной инженерии. Человек может «под диктовку» установить программу удаленного доступа, назвать код из СМС или перевести деньги на, так называемый, безопасный счет. Биометрия и MFA в такой ситуации мало эффективны, потому что легитимный пользователь подтверждает операцию сознательно. Также к факторам риска следует отнести слепые зоны в данных, задержки в обновлении баз угроз, уязвимость каналов связи, разрозненность систем защиты разных банков, регуляторные ограничения, конфликт между удобством и безопасностью и т.д. Кроме того, все большее распространение получают сложные многоэтапные схемы с использованием машинного обучения. В таких случаях используется атака, включающая в себя комбинацию телефонного звонка, фишингового письма, подмены сайта и социальной инженерии, которую сложно «отразить».

В связи с этим для повышения эффективности систем защиты от дистанционных хищений необходимо использовать проактивную, адаптивную и многослойную архитектуру, которая учитывает не только технические, но и психологические, организационные аспекты такого рода противоправной деятельности. Для решения данной задачи предлагается внедрение комплексной системы защиты от дистанционных хищений с использованием электронных средств платежа (Свидетельство о государственной регистрации программы для ЭВМ № 2026667563 «Программа для определения рисков дистанционных хищений с использованием электронных средств платежа» от 09.06.2026 г.; см. Приложение 3-4). При разработке данной программы учитывались следующие данные, полученные в результате настоящего исследования: типичные способы совершения дистанционных хищений с использованием электронных средств платежа; характерные этапы реализации мошеннических «сценариев» (установление контакта с потерпевшим,

введение его в заблуждение, получение доступа к средствам и их последующее выведение); признаки использования социальной инженерии при совершении преступлений; типичные каналы коммуникации, используемые преступниками (телефонная связь, мессенджеры, фишинговые сайты и электронные письма); особенности использования программ удалённого доступа и иных технических средств, применяемых злоумышленниками; а также выявленные в ходе исследования организационные и технические уязвимости в системах дистанционного банковского обслуживания, способствующие совершению указанных преступлений. Программа построена на принципе машинного обучения и анализирует в реальном времени новые данные об атаках – как успешных, так и предотвращённых, – которые затем возвращаются в модели и используются для формирования новых правил за счёт создания петли обратной связи (feedback loop). Представленная программа использует комплексную защиту, основанную на сочетании проактивного анализа угроз и интеллектуальных моделей на графах и последовательностях. Кроме того, она включает модуль противодействия социальной инженерии, основанный на анализе особенностей поведения клиентов и преступника. Завершающим элементом является непрерывное обучение и разработка новых правил на основе анализа выявленных правонарушений.

В результате использования разработанной программы на синтетических выборках удалось на 23% увеличить полноту обнаружения (Recall) мошеннических действий и на 32% уменьшить количество ложных срабатываний. Указанное программное обеспечение показало свою практическую применимость и эффективность при выявлении подозрительных операций, что подтверждает возможность внедрения разработанного решения в деятельность правоохранительных органов и иных субъектов профилактики дистанционных хищений. Полученные результаты свидетельствуют о том, что применение комплексного подхода, основанного на учёте криминологических, организационных и поведенческих факторов

дистанционных хищений, позволяет существенно повысить эффективность выявления противоправных операций с использованием электронных средств платежа. Указанные показатели подтверждают выводы, полученные в ходе теоретического исследования, согласно которым дистанционные хищения характеризуются многоэтапным механизмом реализации, активным использованием методов социальной инженерии, а также сочетанием технических и психологических способов воздействия на потерпевшего. Учёт данных особенностей при построении алгоритмов анализа транзакционной активности и поведенческих моделей пользователей позволяет более точно выявлять признаки мошеннических действий и минимизировать вероятность ошибочной идентификации легитимных операций.

Так, проведённый анализ современных технических средств защиты показывает, что противодействие дистанционным хищениям требует применения комплексного подхода, основанного на сочетании различных уровней защиты: безопасности устройств клиента, защищенности каналов связи и совершенствования внутренней инфраструктуры банковских организаций. Вместе с тем эффективность указанных мер во многом зависит от способности систем защиты учитывать особенности механизма совершения дистанционных хищений, включая использование социальной инженерии, многоэтапных мошеннических сценариев и распределение ролей между организаторами, техническими исполнителями, номинальными участниками и иными субъектами преступных схем. В этой связи особое значение приобретает внедрение интеллектуальных программных решений, основанных на анализе больших массивов данных, выявлении аномалий финансовой активности, поведенческих паттернов преступников и потенциальных потерпевших, а также постоянном обновлении алгоритмов противодействия противоправным действиям с учётом трансформации способов дистанционных хищений и используемых цифровых технологий.

Отдельную группу составляют культурно-воспитательные меры предупреждения, позволяющие сформировать у граждан ценностные ориентации на законопослушное поведение, а также предупредить о возможностях совершения преступлений такого рода. Эти меры, с одной стороны, имеют прямую взаимосвязь с общесоциальными мерами предупреждения, являясь их составной частью, а, с другой стороны, образуют самостоятельную группу, поскольку направленны непосредственно на формирование у граждан высокого уровня правосознания и правовой культуры. Отдельно укажем, что согласно данным социологического опроса в части профилактики сотрудники считают наиболее эффективными меры, направленные именно на информирование населения и повышение цифровой грамотности, а также оперативную блокировку подозрительных счетов и номеров. Эти меры были выбраны 74%, 69% и 63% респондентов соответственно, что говорит о доминирующем мнении о необходимости просвещения граждан и быстрого реагирования на признаки мошенничества. При этом 41% сотрудников считают, что граждане плохо осведомлены о методах дистанционных хищений, что напрямую влияет на их уязвимость. В связи с этим существующие профилактические мероприятия, по оценке сотрудников, имеют преимущественно среднюю эффективность (53%), а 36% оценивают их как низкие, что свидетельствует о необходимости пересмотра подходов к предупреждению преступлений, в том числе расширения охвата профилактической работы и повышения её системности (см. Приложение 1-2).

В качестве примера культурно-воспитательных мер предупреждения преступности можно привести проведение разными организациями и органами власти мероприятий по повышению уровня правовой культуры, правосознания, а также в общем морально-нравственных устоев в обществе. Так, например, в соответствии с примерной рабочей программой воспитания в образовательной организации высшего образования, утверждённой Министерством науки и высшего образования РФ в 2021 г., основной целью воспитательной работы является создание для обучающихся специальных

условий для удовлетворения их потребностей в социально-культурном, нравственном, профессиональном и интеллектуальном развитии. Кроме того, в программе отмечается важность достижения задачи приобщения студентов к нормам морали, а также воспитание у обучающихся уважения к закону и к правопорядку[222]. Схожие вопросы решают, осуществляя свою деятельность, и различные органы исполнительной власти. Например, одним из направлений работы Министерства внутренних дел России является регулярное правовое информирование граждан об ответственности за противоправное поведение, в числе которых разработка памяток с последующим доведением информации до граждан: «О правах граждан, ставших жертвами правонарушений», «Управление “К” предупреждает», «Владельцам пластиковых банковских карт», «Не дай себя обмануть», «Моя экономическая безопасность» и других[223]. Это и многое другое отвечает целям реализации культурно-воспитательных мер предупреждения не только преступности в целом, но и отдельным её разновидностям, в частности, в том числе дистанционным хищениям, посредством воздействия как на потенциальных преступников, так и на потенциальных жертв преступления.

Кроме того, характеризуя данный аспект реализации предупредительной деятельности, считаем отдельно выделить такое направление борьбы с дистанционными хищениями как виктимологическая работа с населением, особенно с социально незащищёнными категориями лиц, которые ввиду различных психологических особенностей, не способны противостоять дистанционным хищениям. Ещё раз подчеркнём, что среди опрошенных сотрудников правоохранительных органов, имеющих многолетний стаж в системе органов внутренних дел, наиболее эффективными мерами профилактики 74% респондентов считают меры, направленные на информирование населения, и 69% – на повышение

[222] Примерная рабочая программа воспитания в образовательной организации высшего образования [Электронный ресурс]. – URL: https://minobrnauki.gov.ru/upload/2021/04/ (дата обращения: 28.03.2026).
[223] Памятки для граждан [Электронный ресурс]. – URL: https://xn--b1aew.xn--p1ai/booklets (дата обращения: 29.03.2026).

цифровой грамотности (см. Приложение 1-2). Например, в настоящее время достаточно распространена на основе анализа типичных схем совершения дистанционных хищений подготовка виктимологических рекомендаций в виде специального контента в форме визуальных, аудио-, аудиовизуальных материалов, который размещается в СМИ, социальных сетях, в сети Интернет, демонстрируется на тематических мероприятиях перед разными социальными группами населения и целевыми аудиториями[224]. Так, сотрудники УМВД России по Курской области ежегодно проводят беседы о типичных схемах совершения дистанционных мошенничеств с обучающимися общеобразовательных организаций[225], а региональное Отделение Социального фонда России по Курской области регулярно на официальном сайте размещает информацию о мерах предосторожности, которые могут помочь избежать незащищённым слоям населения простых уловок дистанционных мошенников[226]. Как видим, виктимологическое предупреждение дистанционных хищений предусматривает работу с различными категориями населения, которые могут стать жертвами таких преступлений.

Для повышения эффективности культурно-воспитательных мер представляется целесообразным расширение охвата профилактических мероприятий посредством активного использования современных цифровых платформ, социальных сетей и иных каналов массовой коммуникации для распространения виктимологического контента, ориентированного на наиболее уязвимые категории потенциальных потерпевших с учётом типичных механизмов воздействия, используемых социальными инженерами. Особое значение имеет разработка интерактивных образовательных модулей и цифровых симуляторов мошеннических

[224] Старостенко О.А. Алгоритм осуществления виктимологической профилактики дистанционных хищений // Гуманитарные, социально-экономические и общественные науки. 2023. № 4. С. 190-193.
[225] В Курске сотрудники полиции рассказали учащимся образовательных учреждений о мошеннических схемах [Электронный ресурс]. – URL: https://46.xn--b1aew.xn--p1ai/news/item/49544300 (дата обращения: 30.03.2026).
[226] Региональное Отделение СФР призывает курян не поддаваться на уловки мошенников! [Электронный ресурс]. – URL: https://sfr.gov.ru/branches/kursk/news/~2024/04/15/262732 (дата обращения: 31.03.2026).

ситуаций, позволяющих гражданам формировать практические навыки безопасного поведения в цифровой среде, своевременного распознавания методов психологического воздействия, а также способов вовлечения в деятельность в качестве номинальных участников. Наряду с этим необходимы систематизация и унификация профилактических рекомендаций с учётом различий в уровне цифровой грамотности, возрасте, социальном положении и степени виктимности отдельных групп населения. Дополнительно представляется оправданной организация регулярного мониторинга эффективности просветительских мероприятий с последующей корректировкой их содержания в зависимости от трансформации преступных схем, изменения механизмов вовлечения, а также появления новых цифровых угроз и способов совершения дистанционных хищений.

Так, под системой предупреждения дистанционных хищений необходимо понимать совокупность отношений, выстраиваемых между субъектами предупредительной деятельности и объектами предупреждения, направленных на достижение цели борьбы с дистанционными хищениями в условиях угроз и вызовов современности. Под объектом предупреждения в данном случае необходимо понимать всё то, на что направлена деятельность по предупреждению совершения таких преступлений (причины, условия и факторы, детерминирующие развитие рассматриваемой разновидности преступной деятельности, саму преступность, группы лиц, которые потенциально могут совершить дистанционные хищения, а равно и потенциальных жертв таких посягательств). К субъектам предупреждения следует отнести специализированные субъекты, чья деятельность непосредственно направлена на борьбу с дистанционными хищениями (например, органы МВД России, ФСИН РФ, Прокуратуры РФ, Следственный комитет РФ и т.д.), факультативные субъекты – различные органы и организации, для которых предупреждение, выявление, пресечение, раскрытие дистанционных хищений, не является основной функцией деятельности (например, Федеральное собрание Российской Федерации,

которое разрабатывает и принимает нормативные правовые акты, обеспечивающие правовую основу для противодействия дистанционным хищениям), а также субъекты-участники – это лица и различные организации, которые косвенно принимают участие в правоохранительной деятельности профилактического характера на служебной или добровольной основе (например, частные предприятия, обеспечивающие технологически информационную защиту сервисов различных кампаний, в том числе поддерживая нормальную работу информационно-телекоммуникационных сетей и проведение в них финансовых операций). Также важным элементом системы предупреждения данной разновидности преступности является совокупность мер борьбы с дистанционными хищениями. Условно эти меры предупреждения можно разделить по направленности действия на общесоциальные, правовые, организационно-управленческие, технические, культурно-воспитательные и некоторые другие меры, где общесоциальные меры выполняют задачу минимизации влияния на общество негативных антисоциальных явлений, правовые решают проблему обеспечения эффективно функционирующей нормативно-правовой системы защиты общества и государства от таких преступных посягательств, организационно-управленческие предполагают разработку программно-целевого планирования деятельности субъектов предупреждения и координацию их активностей в сфере борьбы с дистанционными хищениями, технические – позволяют разработать более совершенные с технической точки зрения механизмы защиты информационного пространства и усложнить процесс совершения таких преступлений, а культурно-воспитательные меры предупреждения решают проблему повышения у населения цифровой грамотности.

Таким образом, проведённое исследование позволяет заключить, что лица, совершающие дистанционные хищения, формируют относительно устойчивый криминологический тип, характеризующийся значительной цифровой адаптивностью и вовлечённостью в распределённые преступные

схемы, включающие организаторов, технических исполнителей, социальных инженеров и номинальных участников. Указанные характеристики свидетельствуют о трансформации традиционного образа имущественного преступника под влиянием цифровой среды и росте роли технологического компонента в структуре противоправного поведения. Мотивационная основа данных деяний преимущественно выражена в корыстной направленности и стремлении к быстрому извлечению материальной выгоды при минимизации личных рисков, что обусловливает активное использование дистанционных и анонимизированных форм преступной деятельности. При этом вербовка новых участников носит системный и технологически опосредованный характер, реализуясь через цифровые каналы коммуникации и механизмы психологического воздействия, что обеспечивает устойчивое воспроизводство преступных схем и вовлечение социально уязвимых лиц в такого рода деятельность. В этих условиях система предупреждения дистанционных хищений представляет собой многоуровневый и взаимосвязанный комплекс мер, эффективность которого определяется согласованностью правовых, организационно-управленческих, технических, общесоциальных и культурно-воспитательных мер. При этом результативное противодействие возможно лишь при одновременном воздействии на личность правонарушителя, процессы его мотивации и вербовки, а также на причины и условия, способствующие совершению таких преступлений. В этой связи в работе предложены основные направления совершенствования системы предупреждения дистанционных хищений. Их реализация позволит повысить эффективность профилактического воздействия, обеспечить снижение уровня рассматриваемой преступности и укрепить защищённость имущественных отношений в условиях цифровой трансформации.

Заключение

Современный этап развития общества характеризуется масштабной цифровизацией социально-экономических процессов, активным внедрением информационно-телекоммуникационных технологий в сферу финансовых отношений, расширением дистанционных форм взаимодействия и увеличением объёма операций, совершаемых в электронном формате. Наряду с очевидными положительными последствиями цифровой трансформации общественных отношений указанные процессы обусловили возникновение новых угроз имущественной безопасности личности, общества и государства, одной из наиболее опасных форм проявления которых стали дистанционные хищения. Использование электронных средств платежа, цифровых платформ, телекоммуникационных сетей, вредоносного программного обеспечения, технологий социальной инженерии и иных информационных инструментов изменило характер взаимодействия между преступником и потерпевшим, усложнило процессы выявления и расследования преступлений, а также поставило перед правоприменительной практикой новые задачи, связанные с квалификацией и предупреждением преступных деяний в цифровой среде. В этих условиях особую актуальность приобретает необходимость выработки единых подходов к пониманию сущности дистанционных хищений, определению их уголовно-правовой природы и формированию эффективной системы предупреждения указанных преступлений.

Проведённое исследование позволило комплексно рассмотреть уголовно-правовые и криминологические аспекты дистанционных хищений, выявить особенности их механизма, определить проблемы квалификации и предупреждения, а также сформулировать предложения, направленные на совершенствование отечественного уголовного законодательства и практики противодействия таким преступлениям.

Дистанционные хищения следует рассматривать не как самостоятельный институт уголовного права, а как современную форму

реализации классического института хищения в условиях цифровизации общественных отношений. Их специфика обусловлена не изменением юридической природы хищения, а трансформацией способа совершения преступления, реализуемого посредством цифровой инфраструктуры, электронных платёжных инструментов и иных средств удалённого воздействия. Предложенное в исследовании определение дистанционного хищения позволяет сформировать теоретическую основу для дальнейшего совершенствования уголовно-правового регулирования, единообразия квалификации и развития системы предупреждения соответствующих преступлений в условиях цифровой трансформации имущественных отношений.

Основными формами дистанционных хищений выступают дистанционные кражи и дистанционные мошенничества, каждая из которых характеризуется собственными механизмами преступного воздействия и системой способов совершения преступления. Для дистанционных краж преимущественно характерны способы, связанные с неправомерным доступом к цифровой инфраструктуре, учётным записям и электронным средствам платежа, а для дистанционных мошенничеств – способы, основанные на персонализированном обмане потерпевшего либо технически опосредованном формировании ложной информационной ситуации. Это свидетельствует о комплексной технической и социально-психологической природе дистанционных хищений и необходимости их уголовно-правовой оценки с учётом особенностей используемых цифровых технологий, характера воздействия на потерпевшего и механизма совершения преступления.

Установлено, что действующая система уголовно-правового регулирования дистанционных хищений не образует самостоятельного института либо отдельной главы уголовного закона, а представляет собой многоуровневую совокупность взаимосвязанных норм, объединённых общей целью охраны имущественных отношений в цифровой среде. Первый –

основной – уровень образуют нормы, непосредственно предусматривающие ответственность за дистанционные формы хищения: п. «г» ч. 3 ст. 158, ст. 159^3 и ст. 159^6 УК РФ, а при отсутствии специальных признаков соответствующих составов применяются общие нормы о краже и мошенничестве (ст. 158 и 159 УК РФ). Второй – технологический – уровень составляют нормы, обеспечивающие уголовно-правовую охрану информационной среды и предусматривающие ответственность за неправомерное воздействие на компьютерную информацию и информационные системы (ст. 272–274 УК РФ), которые могут выступать дополнительным элементом уголовно-правовой оценки при использовании технических способов совершения хищения. Третий – инфраструктурный – уровень включает нормы, направленные на защиту электронных платёжных инструментов, финансовой инфраструктуры и оборота цифровых средств платежа, в том числе ст. 187 УК РФ. Такая многоуровневая модель позволяет рассматривать противодействие дистанционным хищениям как системный механизм, объединяющий защиту имущества, цифровой среды и обеспечивающей её финансовой инфраструктуры. Вместе с тем эффективность данной модели осложняется высокой скоростью развития цифровых технологий, появлением новых способов совершения противоправных действий и необходимостью постоянной адаптации уголовно-правовых средств к изменяющимся формам цифровой преступности.

Вместе с тем определено, что действующее уголовное законодательство и правоприменительная практика сталкиваются с рядом проблем, обусловленных развитием цифровых технологий, конкуренцией уголовно-правовых норм и отсутствием единых подходов к квалификации отдельных форм дистанционных хищений. В этой связи в исследовании предложены направления совершенствования уголовного законодательства и судебного толкования, связанные с расширением понимания предмета хищения за счёт включения цифровой валюты и иных виртуальных активов,

уточнением критериев разграничения дистанционных краж и мошенничеств, а также обеспечением единообразия правоприменительной практики в условиях цифровизации имущественных отношений.

В целом действующая система наказуемости дистанционных хищений ориентирована на обеспечение дифференцированной уголовно-правовой реакции с учётом характера, способа и последствий совершаемых деяний. Вместе с тем проведённый анализ выявил наличие отдельных диспропорций в санкционной политике, связанных с разграничением дистанционных форм хищений, оценкой степени их общественной опасности, учётом технологической сложности способов совершения преступлений и некоторых других проблем. В этой связи в исследовании предложен ряд направлений совершенствования уголовно-правового регулирования в указанной сфере, реализация которых позволит обеспечить большую согласованность системы санкций, укрепить принципы справедливости и соразмерности уголовной ответственности, а также повысить эффективность противодействия дистанционным имущественным посягательствам в условиях цифровизации общественных отношений.

Проведённый анализ материалов уголовных дел позволил сформировать обобщённый криминологический портрет лица, совершающего дистанционные хищения. Это мужчина молодого или среднего возраста, не состоящий в браке, обладающий образованием не ниже среднего специального, не имеющий устойчивой занятости либо занятый в сфере услуг, торговли или информационных технологий. Для данной категории лиц характерны преимущественно корыстная мотивация, рациональность поведения, эмоциональная дистанцированность и невысокий уровень открытой агрессии, при этом значительная часть преступлений совершается в форме дистанционного мошенничества с использованием информационно-коммуникационных технологий.

Одновременно установлено, что современная система дистанционных хищений характеризуется внутренней ролевой дифференциацией участников

преступной деятельности. В её структуре выделяются организаторы, осуществляющие координацию преступных схем и распределение функций; технические исполнители, обеспечивающие реализацию преступлений посредством использования цифровых технологий; социальные инженеры, оказывающие психологическое воздействие на потерпевших; а также номинальные участники (например, дропперы, вовлекаемые в преступную деятельность для транзита и сокрытия похищенных денежных средств). Выявленные особенности личности указанных категорий преступников имеют существенное значение для формирования дифференцированной системы предупреждения дистанционных хищений и определения приоритетных направлений профилактического воздействия.

Мотивационная структура лиц, совершающих дистанционные хищения, носит комплексный и многоуровневый характер, поскольку определяется не только корыстной направленностью, но и совокупностью иных психологических и поведенческих факторов, обусловленных спецификой цифровой среды. Ключевым выступает корыстный компонент, выражающийся в стремлении к получению материальной выгоды, при этом зачастую не связанной с удовлетворением базовых потребностей, а ориентированной на быстрое и систематическое извлечение дохода. Рационально-технологический компонент проявляется в стремлении использовать возможности цифровой среды для повышения эффективности преступной деятельности, минимизации временных затрат и снижения вероятности обнаружения. Риско-ориентированный компонент связан с субъективным восприятием низкой вероятности привлечения к ответственности вследствие анонимности, удалённого характера взаимодействия и сложности выявления участников преступной схемы. Психологический компонент цифровой безличности выражается в снижении эмоционального восприятия последствий преступления, ослаблении эмпатии к потерпевшему и формировании представления о противоправных действиях как об обезличенном процессе взаимодействия с цифровыми

ресурсами. Профессионально-статусный компонент связан со стремлением к самоутверждению через демонстрацию технических, коммуникативных либо организационных навыков и восприятие преступной деятельности как сферы применения собственных компетенций. Дополнительно может проявляться ситуативно-оппортунистический компонент, возникающий при случайном получении доступа к чужим данным или ресурсам в условиях сочетания высокой выгоды и низкого субъективного риска. При этом установлено, что указанные мотивационные компоненты проявляются неодинаково в зависимости от функциональной роли лица в преступной схеме.

В целом проведённый анализ мотивационной сферы лиц, совершающих дистанционные хищения, свидетельствует о том, что реализация преступной мотивации в условиях цифровой среды во многом обусловлена существованием устойчивых механизмов вовлечения новых участников в преступную деятельность. В этой связи особое криминологическое значение приобретает исследование способов вербовки, поскольку именно через них обеспечиваются воспроизводство преступных связей, распределение функциональных ролей и поддержание устойчивости организованных форм дистанционной преступности.

Установлено, что вербовка в системе дистанционных хищений выступает не только средством привлечения новых участников, но и юридически значимым элементом института соучастия, влияющим на квалификацию действий в рамках ст. 33 УК РФ. В зависимости от характера выполняемых функций вовлекаемые лица могут выступать исполнителями, организаторами, пособниками либо подстрекателями, а при наличии устойчивой структуры с распределением ролей деятельность участников может приобретать признаки организованной группы или, в исключительных случаях, преступного сообщества. Дополнительное значение данная проблема получила в связи с изменениями, внесёнными в ст. 187 УК РФ Федеральным законом от 24 июня 2025 г. № 176-ФЗ, усилившими уголовно-правовую охрану платёжной сферы и фактически закрепившими на

законодательном уровне ответственность за наиболее распространённые формы вовлечения номинальных участников (дропперов) в схемы дистанционных хищений. Это свидетельствует о смещении акцента уголовно-правового противодействия с отдельных исполнителей на инфраструктуру организованной киберпреступности, включая механизмы подбора, вовлечения и использования участников преступных схем.

Способы вербовки исполнителей дистанционных хищений, в свою очередь, целесообразно подразделять на две основные группы – латентное и осознанное вовлечение. Латентное вовлечение основывается на сокрытии преступного характера деятельности и маскировке противоправных действий под легальные формы занятости, тогда как осознанное вовлечение предполагает прямое информирование лица о незаконности предполагаемой деятельности и ориентировано на привлечение лиц, готовых участвовать в преступных схемах за материальное вознаграждение. Так, анализ механизмов мотивации и вербовки участников дистанционных хищений свидетельствует о том, что противодействие данной разновидности преступности требует не только уголовно-правового реагирования на уже совершённые деяния, но и формирования комплексной системы предупреждения, ориентированной на выявление причин, условий и факторов, обеспечивающих воспроизводство преступных схем в цифровой среде.

Система предупреждения дистанционных хищений представляет собой совокупность взаимосвязанных субъектов, объектов и мер профилактического воздействия, направленных на минимизацию криминогенных факторов, снижение виктимности населения и пресечение деятельности лиц, вовлечённых в организованные цифровые преступные структуры. Выявлено, что существенными проблемами предупреждения дистанционных хищений являются высокий уровень латентности преступлений, трансграничный характер преступной деятельности, недостаточная оперативность получения информации от банковских организаций и операторов связи, нехватка специализированных кадров,

недостаточный уровень цифровой грамотности населения, а также высокая скорость адаптации преступных схем к изменениям цифровой среды. Отдельной проблемой выступает сложность выявления организаторов дистанционных хищений, использующих анонимные цифровые платформы, «подставных лиц» и распределённые схемы взаимодействия. В связи с этим сформулирован вывод о том, что эффективное предупреждение дистанционных хищений возможно исключительно при реализации комплексного и многоуровневого подхода.

В качестве практических рекомендаций предлагается: совершенствование механизмов межведомственного взаимодействия правоохранительных органов, банковских организаций, операторов связи и иных субъектов противодействия дистанционным хищениям; разработка единых алгоритмов оперативного обмена информацией между ними; расширение возможностей использования современных цифровых средств выявления и анализа мошеннических операций; совершенствование процедур блокировки подозрительных транзакций; повышение уровня профессиональной подготовки сотрудников правоохранительных органов в области расследования дистанционных преступлений и некоторые другие меры. Реализация предложенных мер позволит существенно повысить оперативность выявления и пресечения дистанционных хищений, укрепить координацию между всеми субъектами профилактической системы и обеспечить более высокий уровень защищённости имущественных отношений в цифровой среде. В совокупности это будет способствовать снижению латентности рассматриваемых преступлений, сокращению сроков их раскрытия и повышению общей эффективности противодействия.

Перспективы дальнейших научных исследований по указанной проблематике связаны с изучением преступлений, совершаемых с использованием технологий искусственного интеллекта, криптовалют, анонимных цифровых платформ и автоматизированных систем обработки данных, исследованием новых механизмов социальной инженерии,

развитием виктимологических подходов к предупреждению цифровой преступности, а также разработкой современных моделей адаптивного противодействия преступлениям в условиях дальнейшей цифровизации общественных отношений.

В завершение можно заключить, что дистанционные хищения образуют внутренне согласованную группу имущественных преступлений, характеризующуюся трансформацией «классических» признаков хищения под воздействием цифровой среды, сложной мотивационной структурой личности преступника и специфическими способами совершения преступлений и вербовки исполнителей. Это подтверждает необходимость не только дальнейшей дифференциации уголовно-правовых норм и разработки единых критериев квалификации, но и формирования комплексной превентивной стратегии, включающей согласованное применение уголовно-правовых и криминологических мер. Такая стратегия должна обеспечивать раннее выявление и нейтрализацию потенциальных угроз, адаптивное реагирование на появление новых цифровых технологий, способных использоваться для совершения хищений, и создание условий, при которых защита имущественных интересов граждан и юридических лиц становится системной, многоуровневой и эффективной. В конечном итоге реализация обозначенного подхода позволит сформировать устойчивый и адаптивный механизм противодействия, обладающий прогностической и превентивной направленностью и обеспечивающий опережающее реагирование на трансформацию цифровых криминальных практик, тем самым гарантируя системную и долгосрочную защищённость имущественных отношений в условиях усложняющейся цифровой среды.

Список литературы

Нормативные акты и официальные документы

1. Конвенция ООН о киберпреступности [Электронный документ]. – URL: https://www.un.org/ru/documents/treaty/A-RES-79-243 (дата обращения: 15.02.2026).

2. Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23.11.2001) [Электронный документ]. – URL: https://base.garant.ru/4089723/ (дата обращения: 10.02.2026).

3. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) [Электронный документ]. – URL: http://www.constitution.ru/ (дата обращения: 16.01.2026).

4. Уголовный кодекс РФ (первая редакция от 13 июня 1996 г.) [Электронный документ]. – URL: http://pravo.levonevsky.org/kodeksru/uk.htm (дата обращения: 28.01.2026).

5. Уголовный кодекс РФ от 13.06.1996 № 63-ФЗ (с доп. и изм.) [Электронный документ]. – URL: https://www.consultant.ru/document/cons_doc_LAW (дата обращения: 10.03.2026).

6. Уголовно-исполнительный кодекс РФ от 08.01.1997 № 1-ФЗ (с доп. и изм.) [Электронный документ]. – URL: https://www.consultant.ru/document/cons_doc_LAW (дата обращения: 10.03.2026).

7. Уголовно-процессуальный кодекс РФ от 18.12.2001 № 174-ФЗ (с доп. и изм.) [Электронный документ]. – URL: https://www.consultant.ru/document/cons_doc_LAW (дата обращения: 10.03.2026).

8. Федеральный закон «О внесении изменений в Уголовный кодекс Российской Федерации» от 23.04.2018 № 111-ФЗ [Электронный ресурс]. – URL: https://www.consultant.ru/document/cons_doc_LAW (дата обращения: 24.02.2026).

9. Федеральный закон от 24.06.2025 № 176-ФЗ «О внесении изменений в статью 187 Уголовного кодекса Российской Федерации» [Электронный документ]. – URL: https://www.consultant.ru/document/cons_doc_LAW_508353/ (дата обращения: 12.05.2026).

10. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный документ]. – URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 02.04.2026).

11. Федеральный закон от 27.06.2011 № 161-ФЗ (с изм. и доп.) «О национальной платежной системе» [Электронный документ]. – URL: https://www.consultant.ru/document/cons_doc_LAW_115625/ (дата обращения: 01.03.2026).

12. Федеральный закон от 03.07.2016 № 325-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации» [Электронный документ]. – URL: https://www.consultant.ru/document/cons_doc_LAW_200714/ (дата обращения: 23.02.2026).

13. Федеральный закон от 29.11.2012 № 207-ФЗ (ред. от 03.07.2016) «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» [Электронный документ]. – URL: https://www.consultant.ru/document/cons_doc_LAW_138322/ (дата обращения: 19.02.2026).

14. Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» (с изм. и доп.) [Электронный документ]. – URL: https://www.consultant.ru/document/cons_doc_LAW_358753/ (дата обращения: 27.03.2026).

15. Федеральный закон от 13.02.2025 № 9-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» [Электронный

документ]. – URL: https://www.consultant.ru/document/cons_doc_LAW_498604/ (дата обращения: 18.03.2026).

16. Федеральный закон от 01.04.2025 № 41-ФЗ (ред. от 31.07.2025) «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации» [Электронный документ]. – URL: https://www.consultant.ru/document/cons_doc_LAW_502182/ (дата обращения: 01.07.2026).

17. Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. 2021. № 27. Ст. 5351.

18. Определение Конституционного Суда РФ от 09.07.2021 № 1374-О «О прекращении производства по делу о проверке конституционности пункта “г” части третьей статьи 158 и статьи 159^3 Уголовного кодекса Российской Федерации в связи с запросом Железнодорожного районного суда города Рязани» [Электронный документ]. – URL: https://www.consultant.ru/document/cons_doc_LAW_391466/ (дата обращения: 16.03.2026).

19. Определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 29.09.2020 № 12-УДП20-5-К6 [Электронный документ]. – URL: https://legalacts.ru/sud/opredelenie-sudebnoi-kollegii-po-ugolovnym-delam-verkhovnogo-suda-rossiiskoi-federatsii-ot-29092020-n-12-udp20-5-k6/ (дата обращения: 15.03.2026).

20. Постановление Конституционного Суда РФ от 20.01.2026 № 2-П «По делу о проверке конституционности части 6 статьи 14 Федерального закона «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» в связи с жалобой гражданина Тимченко Дмитрия Игоревича» [Электронный

документ]. – URL: https://www.consultant.ru/document/cons_doc_LAW_524655/ (дата обращения: 28.03.2026).

21. Постановление Пленума Верховного Суда РФ от 27.12.2002 № 29 (ред. от 15.12.2022) «О судебной практике по делам о краже, грабеже и разбое» [Электронный ресурс]. – URL: https://www.consultant.ru/document/cons_doc_LAW_40412/ (дата обращения: 31.03.2026).

22. Постановление Пленума Верховного Суда РФ от 16.06.2026 № 19 «О внесении изменений в постановление Пленума Верховного Суда Российской Федерации от 27 декабря 2002 года № 29 «О судебной практике по делам о краже, грабеже и разбое» [Электронный документ]. – URL: https://www.consultant.ru/document/cons_doc_LAW_537044/ (дата обращения 29.06.2026).

23. Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 (ред. от 15.12.2022) «О судебной практике по делам о мошенничестве, присвоении и растрате» [Электронный документ]. – URL: https://www.consultant.ru/document/cons_doc_LAW_283918/ (дата обращения: 19.03.2026).

Материалы судебной практики

24. Приговор № 1-474/2018 1-53/2019 от 4 февраля 2019 г. по делу № 1-474/2018, К. районный суд г. Омска (Омская область) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/95KLby0BvwJY/ (дата обращения: 26.02.2026).

25. Приговор № 1-95/2019 от 4 июня 2019 г. по делу № 1-95/2019 О. районного суда г. Владимира (Владимирская область) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/v59eyhN7lzJq/ (дата обращения: 25.02.2026).

26. Приговор № 1-159/2019 1-16/2020 от 4 февраля 2020 г. по делу № 1-159/2019, К. районный суд (Красноярский край) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/Zy0Ny2UbqxVJ/ (дата обращения: 13.03.2026).

27. Приговор № 1-1-2/2020 1-37/2019 от 5 февраля 2020 г. по делу № 1-1-2/2020, Р. районный суд (Ульяновская область) [Электронный ресурс]. –

URL: https://sudact.ru/regular/doc/QpzWyBiSwe64/ (дата обращения: 12.03.2026).

28. Приговор № 1-209/2020 от 28 мая 2020 г. по делу № 1-209/2020 [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/eu9NH0NOnvbh/ (дата обращения: 10.03.2026).

29. Приговор № 1-212/2020 от 26 мая 2020 г. по делу № 1-212/2020 [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/Dxt1HJcYfi6v/ (дата обращения: 11.03.2026).

30. Приговор № 1-277/2020 от 29 июля 2020 г. по делу № 1-277/2020, С. районный суд г. Владивостока (Приморский край) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/4AyuDmz7J9oX/ (дата обращения: 05.02.2026).

31. Приговор № 1-243/2020 от 29 июля 2020 г. по делу № 1-243/2020, О. городской суд (Республика Башкортостан) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/eLKpELsMEF5w/ (дата обращения: 22.03.2026) и др.

32. Приговор № 1-573/2020 от 8 сентября 2020 г. по делу № 1-573/2020 Ц. районного суда г. Кемерово (Кемеровская область) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/x4yF5QuhexHV/ (дата обращения: 27.02.2026).

33. Приговор № 1-374/2020 от 23 октября 2020 г. по делу № 1-374/2020, К. районный суд г. Ростова-на-Дону (Ростовская область) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/mncw7jMm2Zmn/ (дата обращения: 21.03.2026).

34. Приговор № 1-38/2020 от 12 ноября 2020 г. по делу № 1-38/2020, А. районный суд (Республика Татарстан) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/mckKk0siqExx/ (дата обращения: 14.03.2026).

35. Приговор № 1-2/2020 1-2/2021 1-5/2019 1-97/2018 от 21 июня 2021 г. С. районного суда г. Иваново (Ивановская область) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/IifZELYWnygP/ (дата обращения: 28.02.2026).

36. Приговор № 1-12/2023 1-390/2022 от 16 июня 2023 г., К. городской суд (Владимирская область) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/2dMsxJbKfhLR/ (дата обращения: 04.03.2026).

37. Приговор № 1-617/2023 от 5 сентября 2023 г. по делу № 1-617/2023, С. городской суд (Республика Коми) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/e82eh3iuUxbK/ (дата обращения: 28.02.2026).

38. Приговор № 1-1204/2023 от 19 сентября 2023 г. по делу № 1-1204/2023, П. районный суд г. Краснодара (Краснодарский край) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/XQpfF23Iq75J/ (дата обращения: 24.02.2026).

39. Приговор № 1-137/2023 от 12 октября 2023 г. по делу № 1-137/2023, О. районный суд г. Иваново (Ивановская область) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/tijN7saagGZ0/ (дата обращения: 27.02.2026).

40. Приговор № 1-36/2023 1-463/2022 от 26 октября 2023 г. по делу № 1-36/2023, К. городской суд (Владимирская область) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/yKACyWLbR9Zb/ (дата обращения: 20.03.2026).

41. Приговор № 1-164/2023 1-4/2024 от 30 января 2024 г. по делу № 1-164/2023, О. районный суд г. Барнаула (Алтайский край) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/pyNbXiWS6dYR/ (дата обращения: 29.03.2026).

42. Приговор № 1-363/2022 1-37/2023 1-5/2024 от 30 января 2024 г. по делу № 1-363/2022, О. районный суд г. Рязани (Рязанская область) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/d9uYFORTGB6c/ (дата обращения: 30.03.2026).

43. Приговор № 1-410/2023 1-78/2024 от 27 февраля 2024 г. по делу № 1-410/2023, С. городской суд (Томская область) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/0UaLOHMJJD57/ (дата обращения: 02.02.2026).

44. Приговор № 1-203/2024 1-661/2023 от 28 февраля 2024 г. по делу № 1-203/2024, А. городской суд (Нижегородская область) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/iSu7Y2LER5lo/ (дата обращения: 25.02.2026).

45. Приговор № 1-460/2023 1-71/2024 от 28 февраля 2024 г. по делу № 1-460/2023, З. районный суд г. Смоленска (Смоленская область) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/21yaWYl3f4da/ (дата обращения: 03.02.2026).

46. Приговор № 1-203/2024 1-661/2023 от 28 февраля 2024 г. по делу № 1-203/2024, А. городской суд (Нижегородская область) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/iSu7Y2LER5lo/ (дата обращения: 26.02.2026).

47. Приговор № 1-26/2025 от 13 апреля 2025 г. по делу № 1-26/2025, Н. районный суд (Республика Дагестан) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/DMQMgKcBJQml/ (дата обращения: 04.02.2026).

48. Приговор № 1-28/2025 от 15 апреля 2025 г. по делу № 1-28/2025 К. районный суд (Пермский край) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/FYhBzi0JL7C/ (дата обращения: 03.03.2026).

49. Приговор № 1-379/2024 1-51/2025 от 20 апреля 2025 г. по делу № 1-379/2024 А. районный суд г. Сочи (Краснодарский край) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/XW0LNH7qH8Yg/ (дата обращения: 02.03.2026).

50. Приговор № 1-163/2025 от 21 апреля 2025 г. по делу № 1-163/2025, Т. городской суд (Челябинская область) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/TUE1h7MpWCNR/ (дата обращения: 01.03.2026).

51. Приговор № 1-25/2019 1-377/2018 от 8 декабря 2019 г. по делу № 1-275/2018, С. районный суд г. Томска (Томская область) [Электронный документ]. – URL: https://sudact.ru/regular/doc/hktokOrwZgbO/ (дата обращения: 29.06.2026).

52. Приговор № 1-583/2025 от 23 ноября 2025 г. по делу № 1-583/2025, М. городской суд (Московская область) [Электронный документ]. – URL: https://sudact.ru/regular/doc/ctffI1JUQVNq/ (дата обращения: 29.06.2026).

53. Приговор № 1-178/2025 от 12 ноября 2025 г. по делу № 1-178/2025, Б. районный суд (Республика Крым) [Электронный документ]. – URL: https://sudact.ru/regular/doc/GSrqVh21SwmJ/ (дата обращения: 29.06.2026).

54. Приговор № 1-313/2025 от 9 декабря 2025 г. по делу № 1-313/2025, Ш. районный суд (Ставропольский край) [Электронный документ]. – URL: https://sudact.ru/regular/doc/74r3cDRZ69dj/ (дата обращения: 30.06.2026).

55. Приговор № 1-500/2025 от 2 октября 2025 г. по делу № 1-500/2025, М. городской суд (Магаданская область) [Электронный документ]. – URL: https://sudact.ru/regular/doc/bQFG9GHw14g8/ (дата обращения: 30.06.2026).

56. Приговор № 1-262/2020 от 13 мая 2020 г. по делу № 1-262/2020, Ц. районный суд г. Тольятти (Самарская область) [Электронный документ]. – URL: https://sudact.ru/regular/doc/7A5Kp6LDx6gQ/ (дата обращения: 30.06.2026).

57. Приговор № 1-243/2020 от 28 июля 2020 г. по делу № 1-243/2020, О. городской суд (Республика Башкортостан) [Электронный документ]. – URL: https://sudact.ru/regular/doc/eLKpELsMEF5w/ (дата обращения: 30.06.2026).

58. Приговор № 1-3/2019 1-50/2018 1-580/2017 от 1 декабря 2019 г. по делу № 1-3/2019, К. районный суд г. Томска (Томская область) [Электронный документ]. – URL: https://sudact.ru/regular/doc/xbU4lTLIinWd/ (дата обращения: 30.06.2026).

59. Приговор № 1-25/2019 1-377/2018 от 8 декабря 2019 г. по делу № 1-275/2018, С. районный суд г. Томска (Томская область) [Электронный документ]. – URL: https://sudact.ru/regular/doc/hktokOrwZgbO/ (дата обращения: 30.06.2026).

Научная, учебная и справочная литература

60. Алексеев, А. И. Криминологическая профилактика: теория, опыт, проблемы / А. И. Алексеев, С. И. Герасимов, А. Я. Сухарев. – М., 2001. – 340 с.

61. Богданчиков, С. В. противодействие преступным посягательствам на абсолютные права собственности (хищения): монография / С. В. Богданчиков. – Москва: ЮНИТИ-ДАНА: Закон и право, 2017. – 160 с.

62. Бражников, Д. А. Противодействие тайному хищению чужого имущества: монография / Д. А. Бражников. – Москва: ЮНИТИ-ДАНА, 2017. – 207 с.

63. Гилинский, Я. И. Криминология и девиантология постмодерна / Я. И. Гилинский. – Санкт-Петербург: Алетейя, 2024. – 242 с.

64. Клепицкий, И. А. Новое экономическое уголовное право / И. А. Клепицкий. – Москва: Проспект, 2021. – 983 с.

65. Кузнецов, М. В. Социальная инженерия и социальные хакеры / М. В. Кузнецов. – Санкт-Петербург: БХВ-Петербург, 2007. – 368 с.

66. Минин, А. Я. Актуальные проблемы цифрового права / А. Я. Минин. – Москва: МГПУ, 2021. – 132 с.

67. Скворцов, Л. И. Большой толковый словарь правильной русской речи: 8000 слов и выражений / Л. И. Скворцов. – Москва: ООО «Издательство Оникс»: ООО «Издательство «Мир и образование», 2009. – 1104 с.

68. Теплова, Д. О. Криминологические основы противодействия организованному мошенничеству: монография / Д. О. Теплова. – Москва: РГУП, 2017. – 220 с.

69. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства / В. Ф. Шаньгин. – Москва: ДМК Пресс, 2010. – 544 с.

Статьи и материалы конференций

70. Алейников Д. П. Современные технологии анонимизации в сети Интернет / Д. П. Алейников, А.В. Зык // Образование и право. 2021. № 7. С. 223–224.

71. Алёхин, А. А. Теоретические аспекты кибермошенничества: понятие, правовая природа и виды / А. А. Алёхин // Государственная служба и кадры. 2024. № 2. С. 17–20.

72. Антонов, Ю. И. Об уголовной ответственности за дропперство (ч. 3-6 ст. 187 УК РФ) / Ю. И. Антонов, А. Д. Костиков // Образование и право. 2026. № 1. С. 760–766.

73. Архипов, А. В. Актуальные вопросы квалификации хищения безналичных денежных средств / А. В. Архипов // Вестн. Том. гос. ун-та. 2017. № 418. С. 195–198.

74. Ахмедов, У. О. Способы вовлечения несовершеннолетнего в совершение преступления с использованием информационно-телекоммуникационных технологий как предмет доказывания по уголовным делам / У. О. Ахмедов // Вестник ВИ МВД России. 2024. № 4. С. 164–171.

75. Байбарин, А. А. Кража безналичных и электронных денег: об актуальных проблемах правоприменения / А. А. Байбарин, Д. Н. Садчикова // Вестник Сургутского государственного университета. 2022. № 1 (35). С. 60–68.

76. Барокко, Л. А. К вопросу об особенностях мошенничества, совершенного с использованием информационно-телекоммуникационных технологий по уголовному законодательству Российской Федерации / Л. А. Барокко // Вестник экономической безопасности. 2024. № 1. С. 15–19.

77. Барчуков, В. К. К вопросу о квалификации мошенничества в сфере компьютерной информации / В. К. Барчуков // Пробелы в российском законодательстве. 2017. № 2. С. 128–130.

78. Барчуков, В. К. Терминология мошенничества в сфере компьютерной информации / В. К. Барчуков // Пробелы в российском законодательстве. 2017. № 4. С. 163–165.

79. Бачигина, Н. А. Проблемы построения юридических конструкций специальных составов преступлений / Н. А. Бачигина // Вестник Ярославского государственного университета им. П. Г. Демидова. Серия Гуманитарные науки. 2025. Т. 19, № 2 (72). С. 280–287.

80. Белевитина, Ю. В. Криминологический портрет личности киберпреступника в современной России / Ю. В. Белевитина // Инновационная наука. 2022. № 12–2. С. 61–64.

81. Беляков, А. В. К вопросу об объективных признаках состава преступлений, предусмотренных статьей 159^3 УК РФ / А. В. Беляков, Д. М. Адылин // Вестник Самарского юридического института. 2023. № 1 (52). С. 29–35.

82. Благов, Е. В. Назначение наказания, не подлежащего исполнению, по Уголовному кодексу Российской Федерации / Е. В. Благов // Азиатско-тихоокеанский регион: экономика, политика, право. 2025. Т. 27, № 3. С. 139–154.

83. Благов, Е. В. О предписаниях уголовного законодательства как аксиомах / Е. В. Благов // Юридический вестник Самарского университета. 2024. Т. 10, № 2. С. 33–41.

84. Благов, Е. В. О стадиях освобождения от уголовной / Е. В. Благов ответственности // Юридический вестник Самарского университета. 2022. Т. 8, № 3. С. 70–76.

85. Благов, Е. В. Проблемы мелкого преступления в уголовном законодательстве / Е. В. Благов // Юридический вестник Самарского университета. 2025. Т. 11, № 3. С. 67–75.

86. Благов, Е. В. Проблемы уголовно-правовых категорий / Е. В. Благов // Труды Института государства и права Российской академии наук. 2026. Т. 21, № 3. С. 253–273.

87. Благов, Е. В. Уголовно-правовая терминология: проблемы нормативного соотношения / Е. В. Благов // Труды Института государства и права Российской академии наук. 2025. Т. 20, № 3. С. 163–181.

88. Болсуновская, Л. М. Анализ способов совершения мошенничества в сфере компьютерной информации / Л. М. Болсуновская // Проблемы экономики и юридической практики. 2015. № 6. С. 108–111.

89. Васильева, А. В. Дропперы в системе киберпреступности: уголовно-правовые проблемы квалификации и перспективы

законодательного регулирования / А. В. Васильева // Вопросы российской юстиции. 2025. № 37. С. 279–287.

90. Винокуров, А. В. Биометрические системы идентификации в кредитных организациях как инструмент противодействия мошенничеству / А. В. Винокуров // Финансы и кредит. 2016. № 21 (693). С. 15–23.

91. Гаврилов, Б. Я. Об эффективности уголовно-правовых санкций в системе наказаний в современной уголовной политике государства / Б. Я. Гаврилов, Е. В. Рогова // Вестник Восточно-Сибирского института МВД России. 2024. № 2 (109). С. 82–96.

92. Гладких, В. И. Компьютерное мошенничество: а были ли основания его криминализации? / В. И. Гладких // Российский следователь. 2014. № 22. С. 25–31.

93. Головин, А. Ю. Социальная инженерия в механизме преступной деятельности в сфере информационно телекоммуникационных технологий / А. Ю. Головин, Е. В. Головина // Известия ТулГУ. Экономические и юридические науки. 2021. № 2. С. 3–13.

94. Головчанский, А. В. Анагенез механизма совершения дистанционных мошенничеств в условиях противодействия подменной коммуникации / А. В. Головчанский // Вестник ВИ МВД России. 2024. № 4. С. 261–269.

95. Давыдов, В. О. Несколько тезисов к вопросу о проблематике практики рассмотрения сообщений и расследования уголовных дел о преступлениях, связанных с дистанционным хищением денежных средств / В. О. Давыдов // Известия ТулГУ. Экономические и юридические науки. 2022. № 1. С. 32–38.

96. Дворянкин, О. А. Интернет мошенничество – это новая интернет технологии или жадность и алчность неистребимы...? / О. А. Дворянкин // НАУ. 2021. № 64–1. С. 14–20.

97. Диваева, И. Р. Дистанционное мошенничество: вопросы профилактики / И. Р. Диваева // Аграрное и земельное право. 2022. № 11 (215). С. 185–187.

98. Думанская, Е. И. Мошенничество с использованием электронных средств платежа: трансформация в законе и практике / Е. И. Думанская, А. Г. Меньшикова // Правопорядок: история, теория, практика. 2022. № 3 (34). С. 50–57.

99. Евтушенко, И. И. Актуальные направления виктимологической профилактики дистанционных хищений / И. И. Евтушенко // Виктимология. 2022. № 1. С. 90–98.

100. Еремин, С. Г. О способах мошенничеств без визуального контакта с потерпевшим и методах их предупреждения / С. Г. Еремин, А. В. Сычева // Baikal Research Journal. 2022. № 1. С. 23–26.

101. Ермакова, О. В. Вопросы обоснованности законодательной регламентации преступлений против собственности, совершаемых в сфере IT-технологий / О. В. Ермакова // Вестник Сибирского юридического института МВД России. 2023. № 2 (51). С. 23–29.

102. Желудков, М. А. Дропперство как новый вид соучастия в хищении денежных средств / М. А. Желудков // Право: история и современность. 2025. № 3. С. 378–388.

103. Журавлева, Г. В. Мошенничество в сфере компьютерной информации: спорные вопросы теории и практики / Г. В. Журавлева, Н. А. Карпова // Вестник Московского университета МВД России. 2017. № 5. С. 153–158.

104. Заурби, Л. Ш. О некоторых факторах, препятствующих эффективному раскрытию и расследованию преступлений, совершаемых в киберпространстве / Л. Ш. Заурби // Вестник экономической безопасности. 2021. № 2. С. 258–263.

105. Иванов, М. Г. Проблемы разграничения составов имущественных преступлений, связанных с информационными технологиями (ст. 159^3, 159^6 и

п. «г» ч. 3 ст. 158 УК РФ) / М. Г. Иванов, А. Ю. Николаев // Вестник РУК. 2020. № 3 (41). С. 123–126.

106. Иванчин, А. В. Реальный круг источников уголовного права России / А. В. Иванчин // Российский следователь. 2024. № 1. С. 27–30.

107. Иванчин, А. В. Квалифицированные составы преступлений против личной свободы в УК РФ: проблемы законодательной техники и пути их решения / А. В. Иванчин, А. С. Ковалькова // Журнал юридических исследований. 2022. Т. 7, № 2. С. 99–105.

108. Иванчин, А. В. Юридико-психологические аспекты определения возраста, с которого наступает уголовная ответственность / А. В. Иванчин, Л. О. Кулева, Ф. Х. Наурбиева // Вестник Ярославского государственного университета им. П. Г. Демидова. Серия Гуманитарные науки. 2022. Т. 16, № 4 (62). С. 612–623.

109. Ивлиев, П. В. Влияние СМИ на распространение преступности и криминальной субкультуры в России / П. В. Ивлиев, А. А. Глухова // Право и государство: теория и практика. 2021. № 11 (203). С. 50–54.

110. Казанские уголовно-процессуальные и криминалистические чтения: материалы Междунар. науч-практ. конф. (Казань, 28 апр. 2022 г.): в 2 ч. / редкол.: Ю. Н. Кулешов (отв. ред.) и др.; Казан. ин-т (фил.) ВГУЮ. – Казань: ЮрЭксПрактик, 2022. Ч. 1. – 306 с.

111. Карпов, К. Н. Особенности квалификации хищений с банковского счёта либо электронных денежных средств / К. Н. Карпов // Вестник ОмГУ. Серия. Право. 2019. № 3. С. 138–145.

112. Киктенко, А. А. Предмет преступления, предусмотренного п. «г» ч. 3 ст. 158 Уголовного кодекса Российской Федерации / А. А. Киктенко // Вестник РУК. 2022. № 3 (49). С. 103–107.

113. Кирилюк, М. А. Характеристика способов дистанционных хищений денежных средств как этап ситуационного анализа / М. А. Кирилюк, А. Н. Литвиненко // Вестник экономической безопасности. 2023. № 1. С. 119–225.

114. Коликов, Н. Л. Профессиональная компьютерная преступность и мошенничество / Н. Л. Коликов // Вестник ЮУрГУ. Серия: Право. 2011. № 40 (257). С. 61–64.

115. Корнеева, А. В. Смежные и конкурирующие нормы: вопросы квалификации / А. В. Корнеева // Вестник Университета имени О. Е. Кутафина. 2024. № 4 (117). С. 56–65.

116. Красовская, Н. Р. К вопросу о кибермошенничестве / Н. Р. Красовская, А. А. Гуляев // Вестник Удмуртского университета. Социология. Политология. Международные отношения. 2022. № 1. С. 133–138.

117. Крумина, Д. И. Использование идентификационных данных в преступных целях: вопросы разграничения составов преступлений (ст. 158, 159, 159^3, 159^6 УК РФ) / Д. И. Крумина // Вестник ВолГУ. Серия 9: Исследования молодых ученых. 2022. № 20. С. 126–127.

118. Крутиков, И. Л. Воспрепятствование правосудию: вопросы законодательной техники и дифференциации уголовной ответственности / И. Л. Крутиков // Право и управление. 2025. № 3. С. 139–144.

119. Крутиков, И. Л. Разглашение данных предварительного расследования: дефекты законодательной техники / И. Л. Крутиков // Адвокатская практика. 2025. № 4. С. 44–49.

120. Крутиков, И. Л. Укрывательство преступлений: исторический и законодательно-технический аспекты / И. Л. Крутиков // Журнал прикладных исследований. 2025. № 8. С. 209–214.

121. Кулев, А. Г. Решения прокурора по уголовному делу, поступившему с итоговым актом предварительного расследования, как самостоятельная стадия уголовного судопроизводства / А. Г. Кулев // Евразийский юридический журнал. 2025. № 2 (201). С. 352–355.

122. Лабутин, А. А. Характерные черты личности преступника, совершающего мошенничество с использованием средств мобильной связи (по материалам субъектов Приволжского федерального округа) / А. А. Лабутин

// Вестник Казанского юридического института МВД России. 2018. № 1 (31). С. 75–78.

123. Левашова, О. В. Понятие мошенничества с использованием мобильных средств связи и сети интернет / О. В. Левашова, Е. Ю. Сурнова // Государственная служба и кадры. 2021. № 2. С. 114–117.

124. Левинова, Т. А. Событие преступления vs состав преступления: парадокс разрешен? / Т. А. Левинова // Ius Publicum et Privatum. 2022. № 3 (18). С. 131–140.

125. Леканова, Е. Е. Неправомерный оборот электронных средств платежа и платежных документов, не являющихся ценными бумагами: уголовно-правовая характеристика / Е. Е. Леканова // Полицейская и следственная деятельность. 2025. № 4. С. 52–72.

126. Лещенко, В. П. Предмет мошенничества с использованием электронных средств платежа / В. П. Лещенко // Гуманитарные, социально–экономические и общественные науки. 2019. № 2. С. 92–95.

127. Лопашенко, Н. А. Компьютерное мошенничество – новое слово в понимании хищения или ошибка законодателя? / Н. А. Лопашенко // Пермский юридический альманах. 2019. № 2. С. 598–609.

128. Лукьянова, Ю. В. Кража с банковского счета, а равно в отношении электронных денежных средств: проблемы квалификации и отграничения от смежных составов преступлений / Ю. В. Лукьянова, Д. К. Амирова // Ученые записки Казанского юридического института МВД России. 2024. № 2 (18). С. 23–28.

129. Лустин, В. И. Дистанционные мошенничества / В. И. Лустин // Закон и власть. 2023. № 5. С. 64–76.

130. Лушникова, М. В. Правовое регулирование денежной системы Российской Федерации в условиях цифровой экономики: финансово-правовые проблемы / М. В. Лушникова // Вестник Ярославского государственного университета им. П. Г. Демидова. Серия Гуманитарные науки. 2024. Т. 18, № 2 (68). С. 256–269.

131. Маилян, А. В. О криминалистической характеристике отдельных видов интернет мошенничества / А. В. Маилян // Право и государство: теория и практика. 2019. № 3 (171). С. 98–100.

132. Максуров, А. А. Некоторые аспекты регламентации передачи прав на информационную технологию / А. А. Максуров // Вестник Российской правовой академии. 2025. № 2. С. 150–165.

133. Максуров, А. А. Общеправовые и отраслевые принципы правового обеспечения информационной безопасности / А. А. Максуров // Транспортное право и безопасность. 2025. № 3 (55). С. 215–222.

134. Максуров, А. А. Основные пути адаптации обеспечительных мер при рассмотрении дел о защите гражданских прав в сети Интернет / А. А. Максуров // Юридический вестник Дагестанского государственного университета. 2025. Т. 53, № 1. С. 152–162.

135. Максуров, А. А. Финансово-экономические преступления: вопросы согласования понятий / А. А. Максуров // Юридический вестник Дагестанского государственного университета. 2023. Т. 45, № 1. С. 60–69.

136. Маркова, Е. А. К вопросу о квалификации хищения с банковского счета, а равно в отношении электронных денежных средств (в генезисе) / Е. А. Маркова // Вестник БелЮИ МВД России. 2021. № 3. С. 83–89.

137. Маслиенко, М. А. Особенности квалификации краж и мошенничеств, совершаемых в информационно телекоммуникационных сетях / М. А. Маслиенко // ППД. 2023. № 4 (54). С. 46–52.

138. Матюхина, Т. И. Электронные средства платежа как средство совершения преступления, предусмотренного ст. 159^3 Уголовного кодекса Российской Федерации / Т. И. Матюхина, К. А. Ивлев // Universum: экономика и юриспруденция. 2025. № 1 (123). С. 54–56.

139. Мирончик, А. С. Хищения в электронной среде как разновидность информационных преступлений: проблемы разграничения и квалификации / А. С. Мирончик, А. В. Суслопаров // Юридические исследования. 2019. № 9. С. 17–30.

140. Назаренко, Г. В. Курьёзы толкования уголовно-правовых норм, предусматривающих ответственность за кражу / Г. В. Назаренко // Вестник ЮГУ. 2023. № 2 (69). С. 81–86.

141. Назмеева, Л. Р. Личность преступника, совершающего мошеннические действия с использованием электронных средств платежа: криминологическая оценка / Л. Р. Назмеева, С. Ю. Богомолов // Вестник Казанского юридического института МВД России. 2021. Т. 12, № 4 (46). С. 535–541.

142. Напсоков, А. Р. Проблемы организации деятельности по раскрытию дистанционных мошенничеств и краж с банковских карт / А. Р. Напсоков // Пробелы в российском законодательстве. 2020. № 4. С. 262–264.

143. Недиков, В. Б. Проблемные вопросы уголовной ответственности за интернет-мошенничество: опыт России и Германии / В. Б. Недиков // Вопросы российской юстиции. 2024. № 33. С. 394–410.

144. Новикова, Е. П. Отграничение мошенничества с использованием электронных средств платежа от смежных составов преступлений / Е. П. Новикова // Вестник ВИ МВД России. 2024. № 4. С. 204–209.

145. Павлова, Л. О. Дефекты судебной практики об изменении категории преступления / Л. О. Павлова // Актуальные проблемы российского права. 2024. Т. 19, № 1 (158). С. 119–131.

146. Павлова Л. О. Проблемы исполнения решения суда об освобождении от уголовной ответственности с назначением судебного штрафа / Л. О. Павлова // Евразийский юридический журнал. 2025. № 8 (207). С. 407–409.

147. Пархоменко С. В. Предупреждение компьютерной преступности в Российской Федерации: интегративный и комплексный подходы / С. В. Пархоменко, К. Н. Евдокимов // Всероссийский криминологический журнал. 2015. № 2. С. 265–276.

148. 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.

149. 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.

150. 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.

151. 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.

152. 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.

153. 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.

154. 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.

155. 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.

156. Пивнева, Л. В. Уголовно-правовое регулирование дистанционных хищений в России / Л. В. Пивнева // Проблемы правоохранительной деятельности. 2026. № 2. С. 58–63.

157. 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.

158. 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.

159. 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. 78-85.

160. Полстовалов, О. В. Организованные формы онлайн-мошенничества: виды, содержание и элементы криминалистической характеристики / О. В. Полстовалов, Р. Р. Галяутдинов // Вестник КГУ. 2023. № 4. С. 205–211.

161. Прудников, И. Д. Уголовно-правовая оценка кибервымогательства / И. Д. Прудников // Вестник Ярославского государственного университета им. П. Г. Демидова. Серия Гуманитарные науки. 2023. Т. 17, № 3 (65). С. 426–433.

162. Прыткова, А. А. Криминологический портрет киберпреступника / А. А. Прыткова // Международный журнал гуманитарных и естественных наук. 2022. № 4–3. С. 152–157.

163. Радов, В. В. Наказуемость преступлений в сфере информационных технологий / В. В. Радов // Вестник Университета имени О. Е. Кутафина. 2025. № 5 (129). С. 128–136.

164. Раненкова, Е. А. Проблемные аспекты уголовно–правовой оценки объективной стороны хищения, совершенного с банковского счета, а равно в отношении электронных денежных средств, либо с использованием электронных средств платежа / Е. А. Раненкова, С. Ю. Шемчук // Криминологический журнал. 2021. № 2. С. 42–48.

165. Рогова, Е. В. Определения термина «виктимологическая безопасность» в общей структуре криминологического знания / Е. В. Рогова, Е. С. Качурова // Юрислингвистика. 2024. № 32 (43). С. 32–36.

166. Рогова, Е. В. Корыстная преступность в условиях информационной глобализации / Е. В. Рогова // Вестник Казанского юридического института МВД России. 2022. Т. 13, № 2 (48). С. 69–74.

167. Рогова, Е. В. Криминологическая характеристика корыстных преступлений против собственности в условиях цифровизации / Е. В. Рогова // Всероссийский криминологический журнал. 2025. Т. 19, № 4. С. 378–389.

168. Рогова, Е. В. Перспективы законодательного закрепления квалифицирующих признаков в современных условиях цифровизации / Е. В. Рогова // Публичное и частное право. 2025. № 1 (47). С. 108–113.

169. Рогова, Е. В. Уголовное наказание: к вопросу о его сущности / Е. В. Рогова // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2023. № 4 (97). С. 105–110.

170. Рогова, Е. В. Уголовно-правовое противодействие кибер-преступности в России и Китае: сравнительно-правовой аспект / Е. В. Рогова // Вестник Университета прокуратуры Российской Федерации. 2024. № 1 (99). С. 84–90.

171. Рогова, Е. В. Уголовно-правовое противодействие преступлениям против собственности в современных условиях / Е. В. Рогова // Уголовная юстиция. 2025. № 26. С. 43–47.

172. Рогова, Е. В. Дифференциация уголовной ответственности соучастников преступления / Е. В. Рогова, Р. А. Забавко // Известия Юго-Западного государственного университета. Серия: История и право. 2022. Т. 12, № 5. С. 82–93.

173. Рогова, Е. В. Общественная опасность деяния: теоретико-правовые законодательные и правоприменительные аспекты / Е. В. Рогова, Р. А. Забавко // Академический юридический журнал. 2024. Т. 25, № 3 (97). С. 440–449.

174. Рогова, Е. В. Межотраслевая дифференциация ответственности в контексте введения уголовного проступка / Е. В. Рогова, Р. А. Забавко, О. В. Ивушкина // Вестник Восточно-Сибирского института МВД России. 2022. № 2 (101). С. 106–115.

175. Рогова, Е. В. Преступления против собственности в условиях цифровой трансформации / Е. В. Рогова, А. П. Перетолчин // Академический юридический журнал. 2022. Т. 23, № 3 (89). С. 256–264.

176. Родивилин, И. П. Типологизация лиц, совершающих преступления в сфере компьютерной информации, по способу преступного деяния / И. П. Родивилин // Научный вестник Омской академии МВД России. 2017. № 4 (67). С. 25–29.

177. Русаков, А. О. Методы защиты от атаки «Человек посередине» в Wi–Fi сетях / А. О. Русаков, Р. А. Чалый // Актуальные проблемы авиации и космонавтики. 2016. № 12. С. 767–769.

178. Русскевич, Е. А. Актуальные проблемы квалификации хищений, совершаемых с использованием электронных средств платежа / Е. А. Русскевич, К. Б. Чернова // Вестник экономической безопасности. 2021. № 1. С. 128–130.

179. Рябинина, Т. К. Актуальные проблемы выявления и расследования дистанционных хищений с банковского счета / Т. К. Рябинина, Я. П. Ряполова, Д. О. Чистилина // Вестник БелЮИ МВД России. 2023. № 4. С. 31–38.

180. Рязанова, Е. Н. Криминологическая характеристика личности преступника, совершающего преступные деяния в сфере экономики с использованием информационно-коммуникационных технологий / Е. Н. Рязанова // Социология и право. 2022. № 3. С. 375–282.

181. Савченко, М. М. Квалификационные ошибки применения ст. 159^3 и п. «г» ч. 3 ст. 158 Уголовного кодекса РФ / М. М. Савченко // Право и практика. 2022. № 3. С. 138–141.

182. Самиулина, Я. В. Мошенничество в сфере компьютерной информации: проблемы законодательной регламентации / Я. В. Самиулина // Вестник Самарского юридического института. 2023. № 3 (54). С. 62–65.

183. Семенов, А. В. Ст. 159^3 УК РФ «Квалификация мошенничества, совершенного с использованием электронных средств платежа» / А. В. Семенов // Вестник науки. 2025. № 3 (84). С. 198–203.

184. Сидорова, Е. З. Современные криминологические характеристики цифровой преступности (цифровой преступник и его жертва) / Е. З. Сидорова // Сибирский юридический вестник. 2023. № 3 (102). С. 70–78.

185. Силантьев, С. А. Освобождение от уголовной ответственности как средство её дифференциации: общие и частные проблемы и пути их решения / С. А. Силантьев // Российско-азиатский правовой журнал. 2024. № 4. С. 84–89.

186. Симонова, С. В. Обработка данных пользователей цифровых платформ: актуальные вопросы совершенствования законодательства и практик / С. В. Симонова // Вестник Ярославского государственного университета им. П.Г. Демидова. Серия Гуманитарные науки. 2022. Т. 16, № 4 (62). С. 642–649.

187. Ситникова, А. И. Проблемы толкования и квалификации альтернативных видов хищений, совершаемых с банковского счета или в отношении электронных денежных средств / А. И. Ситникова, Г. В. Назаренко // Научный вестник Омской академии МВД России. 2025. Т. 31, № 3(98). С. 246–252.

188. Скоморохова, М. С. Проблемы квалификации мошенничества в сфере компьютерной информации / М. С. Скоморохова // Вопросы российской юстиции. 2024. № 30. С. 387–393.

189. Смагоринский, Б. П. О некоторых актуальных способах совершения мошенничества в отношении физических лиц в современных условиях / Б. П. Смагоринский, А. В. Сычева // Вестник Волгоградской академии МВД России. 2022. № 2 (61). С. 172–178.

190. Смоляков, А. Н. Ответственность за хищение безналичных денежных средств и цифровой валюты в странах англосаксонской и континентальной системы права / А. Н. Смоляков // Вестник Санкт-Петербургского университета МВД России. 2022. № 1 (93). С. 151–156.

191. Смоляков, А. Н. Хищение безналичных денежных средств и цифровой валюты: проблемы конструирования составов преступлений / А. Н. Смоляков // Вестник Ярославского государственного университета имени П. Г. Демидова. Серия Гуманитарные науки. 2022. Т. 16, № 1 (59). С. 110–117.

192. Соколов, Н. А. Дистанционные мошенничества с использованием средств массовой информации / Н. А. Соколов, В. Х. Георгиевская // Журнал прикладных исследований. 2025. № 10. С. 207–211.

193. Соловьев, В. С. Искусственный интеллект в совершении преступлений: новации правоприменительного толкования / В. С. Соловьев // Уголовное право: стратегия развития в XXI веке. 2025. № 4. С. 108–116.

194. Соловьев, В. С. Криминологические исследования преступности несовершеннолетних в условиях цифровизации общества: ожидания и

реальность / В. С. Соловьев // Алтайский юридический вестник. 2024. № 1 (45). С. 92–99.

195. Соловьев, В. С. Криминологическое значение принятия Конвенции ООН против киберпреступности / В. С. Соловьев // Общество и право. 2026. № 2 (96). С. 55–60.

196. Соловьев, В. С. Проблемы квалификации преступлений, совершаемых с использованием торрент-технологий / В. С. Соловьев // Уголовное право: стратегия развития в XXI веке. 2023. № 3. С. 109–118.

197. Соловьев, В. С. Распространение запрещенной информации через файлообменники: что доказывает умысел / В. С. Соловьев // Уголовный процесс. 2025. № 4 (244). С. 60–67.

198. Соловьев, В. С. Информационно-когнитивные технологии в механизме цифровой виктимизации / В. С. Соловьев, А. Н. Игнатов // Вестник Казанского юридического института МВД России. 2023. Т. 14, № 1 (51). С. 59–66.

199. Соловьев, В. С. Криминологический анализ показателей виктимизации российского общества / В. С. Соловьев, А. В. Симоненко // Общество и право. 2023. № 4 (86). С. 8–14.

200. Соловьев, В. С. Мошенничество с использованием электронных средств платежа: per motris non lates / В. С. Соловьев, К. Ю. Шевчук-Горобец // Гуманитарные, социально-экономические и общественные науки. 2022. № 12. С. 231–235.

201. Соловьев, О. Г. Современное состояние отечественного законодательства в сфере оборота цифровых валют и цифровых активов и вопросы правоприменения в уголовно-правовой сфере / О. Г. Соловьев, А. А. Князьков // Вестник Ярославского государственного университета имени П. Г. Демидова. Серия Гуманитарные науки. 2024. Т. 18, № 3 (69). С. 440–447.

202. Старостенко, О. А. Алгоритм осуществления виктимологической профилактики дистанционных хищений / О. А. Старостенко // Гуманитарные, социально-экономические и общественные науки. 2023. № 4. С. 190–193.

203. Старостенко, О. А. Криминологическая характеристика и основные параметры виктимологического предупреждения дистанционных хищений / О. А. Старостенко // Вестник КРУ МВД России. 2022. № 4 (58). С. 22–27.

204. Сычева, А. В. Некоторые способы совершения «дистанционного» мошенничества / А. В. Сычева // Вестник Волгоградской академии МВД России. 2020. № 4 (55). С. 167–172.

205. Талан, М. В. Криминологический анализ личности мошенника в сфере неправомерного использования электронных средств платежа / М. В. Талан, Б. Э. Шавалеев // Вестник СПбГУ. Серия 14. Право. 2023. № 1. С. 108–122.

206. Телеш, Н. С. Цифровая валюта (криптовалюта) как предмет хищения / Н. С. Телеш // Вестник науки. 2024. № 6 (75). С. 714–717.

207. Третьякова, Н. С. Анализ законодательного описания хищений, совершенных различными способами / Н. С. Третьякова // Сибирское юридическое обозрение. 2011. № 14. С. 84–87.

208. Факторный комплекс преступности в современном мире: материалы Международной научной конференции, Москва, 18 ноября 2021 г. / под ред. В.Ю. Голубовского. – Москва: Дашков и К°, 2022. – 270 с.

209. Федоренко, К. Ю. Проблемы разграничения кражи с банковского счета и мошенничества / К. Ю. Федоренко // Вопросы российской юстиции. 2025. № 37. С. 330–338.

210. Федосеева, О. И. Психологические особенности формирования личности несовершеннолетнего киберпреступника / О. И. Федосеева // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2022. № 4 (60). С. 174–178.

211. Халиков, А. Н. Проблема квалификации дистанционных хищений как отдельного состава преступления / А. Н. Халиков // Евразийская адвокатура. 2025. № 4 (75). С. 117–122.

212. Ханнанова, Д. Р. Противодействие хищения в сфере компьютерной информации уголовно-правовыми средствами / Д. Р. Ханнанова, А. В. Штефан // Вестник магистратуры. 2025. № 5–1 (164). С. 89–93.

213. Харламова, Н. А. Дискуссионные вопросы определения субъекта юридической техники / Н. А. Харламова // Вестник Ярославского государственного университета им. П. Г. Демидова. Серия Гуманитарные науки. 2025. Т. 19, № 1 (71). С. 100–107.

214. Харламова, Н. А. К вопросу о понятии специального состава преступления / Н. А. Харламова // Вестник Ярославского государственного университета им. П. Г. Демидова. Серия Гуманитарные науки. 2024. Т. 18, № 3 (69). С. 458–465.

215. Хилюта, В. В. Признаки мошеннического обмана в теории и практике уголовного закона / В. В. Хилюта // Всероссийский криминологический журнал. 2009. № 2. С. 13–21.

216. Чернякова, А. В. Международный и зарубежный опыт уголовно–правового противодействия хищениям, совершаемым с использованием компьютерной информации / А. В. Чернякова // Юридическая наука и правоохранительная практика. 2018. № 4 (46). С. 168–179.

217. Шашкина, Е. В. Криминалистические данные об участниках организованных преступных групп, совершающих мошенничество с использованием средств мобильной связи / Е. В. Шашкина // Право и государство: теория и практика. 2024. № 1 (229). С. 309–311.

218. Шевелева, С. В. Мошенничество в сфере компьютерной информации: особенности квалификации и конкуренции со смежными составами преступлений / С. В. Шевелева // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2017. № 4 (40). С. 230.

219. Шпетная, А. В. Взаимодействие правоохранительных органов с банками и операторами сотовой связи в предупреждении дистанционных мошенничеств / А. В. Шпетная // Юридическая наука. 2023. № 5. С. 209–211.

220. Шумилин, В. П. Проблемы законодательства о киберпреступности / В. П. Шумилин, Е. С. Лысенко, А. Ф. Острякова // Аграрное и земельное право. 2022. № 5 (209). С. 137–140.

221. Шумихин, В. Г. Седьмая форма хищения чужого имущества / В. Г. Шумихин // Вестник Пермского университета. Юридические науки. 2014. № 2 (24). С. 229–233.

222. Энгельгардт, А. А. Вопросы квалификации мошенничества в сфере компьютерной информации / А. А. Энгельгардт // Право. Журнал Высшей школы экономики. 2016. № 4. С. 86–94.

223. Энгельгардт, А. А. О понимании мошенничества в сфере компьютерной информации / А. А. Энгельгардт // Вестник Московского университета МВД России. 2016. № 8. С. 84–90.

224. Юсупова, А. Ф. Криптовалюта как предмет преступления, предусмотренного п. «г» ч. 3 ст. 158 УК РФ / А. Ф. Юсупова // Вопросы российской юстиции. 2023. № 26. С. 444–450.

Диссертации. Авторефераты диссертаций

225. Голятина, С. М. Методика расследования хищений электронных денежных средств: дис. ... канд. юрид. наук: 12.00.12 / Голятина Светлана Михайловна. – Волгоград, 2022. – 196 с.

226. Григорян, Г. Р. Мошенничество в сфере компьютерной информации: проблемы криминализации, законодательной регламентации и квалификации: автореф. дис. ... канд. юрид. наук: 12.00.08 / Григорян Гарик Рафикович. – Самара, 2021. – 23 с.

227. Жданович, В. В. Трансформация регулирования банковской деятельности в условиях развития цифровых технологий: дис. ... канд. экон. наук: 08.00.10 / Жданович Виталий Витальевич. – Москва, 2021. – 208 с.

228. Зотина, Е. В. Мошенничество с использованием информационно-телекоммуникационных технологий и приемов социальной инженерии: криминологическое исследование: дис. ... канд. юрид. наук: 5.1.4 / Зотина Елена Владимировна. – Москва, 2023. – 250 с.

229. Имаева, Ю. Б. Особенности расследования хищений, совершенных с использованием кредитных и расчетных карт: дис. ... канд. юрид. наук: 12.00.12 / Имаева Юлия Борисовна. – Ростов-на-Дону, 2015. – 207 с.

230. Киктенко, А. А. Уголовная ответственность за кражу, совершенную с банковского счета, а равно в отношении электронных денежных средств: дис. ... канд. юрид. наук: 5.1.4 / Киктенко Анна Александровна. – Москва, 2023. – 163 с.

231. Киселева, И. А. Мошенничество на потребительском рынке: теоретико-правовое исследование: дис. ... канд. юрид. наук: 12.00.08 / Киселева Ирина Анатольевна. – Н. Новгород, 2011. – 227 с.

232. Мазуров, И. Е. Методика расследования хищений, совершенных с использованием интернет-технологий: дис. ... канд. юрид. наук: 12.00.12 / Мазуров Игорь Евгеньевич. – Ростов-на-Дону, 2017. – 188 с.

233. Маилян, А. В. Совершенствование методики расследования хищения с использованием электронных средств платежа: дис. ... канд. юрид. наук: 12.00.12 / Маилян Ани Варужановна. – Краснодар, 2021. – 221 с.

234. Мусьял, И. А. Дифференцированные виды мошенничества: теоретические и практические проблемы: дис. ... канд. юрид. наук: 12.00.08 / Мусьял Ирина Александровна. – Курск, 2018. – 259 с.

235. Перетолчин, А. П. Уголовная ответственность за мошенничество с использованием электронных средств платежа: дис. ... канд. юрид. наук: 12.00.08 / Перетолчин Артем Павлович. – Красноярск, 2021. – 233 с.

236. Простосердов, М. А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им: дис. ... канд. юрид. наук: 12.00.08 / Простосердов Михаил Александрович. – Москва, 2016. – 232 с.

237. Старостенко, О. А. Виктимологическое предупреждение хищений, совершаемых дистанционно: дис. ... канд. юрид. наук: 5.1.4 / Старостенко Олег Александрович. – Краснодар, 2023. – 232 с.

238. Старостенко, Н. И. Первоначальный этап расследования хищений, совершенных с применением методов социальной инженерии и информационно-телекоммуникационных технологий: дис. ... канд. юрид. наук: 5.1.4 / Старостенко Нина Игоревна. – Краснодар, 2023. – 238 с.

239. Фролов, М. Д. Уголовно-правовое и криминологическое противодействие мошенничеству в сфере компьютерной информации: дис. ... канд. юрид. наук: 12.00.08 / Фролов Михаил Дмитриевич. – Москва, 2018. – 211 с.

Электронные ресурсы

240. 18 U.S. Code § 1030 – Fraud and related activity in connection with computers [Электронный ресурс]. – URL: https://www.law.cornell.edu/uscode/text/18/1030 (дата обращения: 12.02.2026).

241. Banerjee A. et al. Cyber-fraud is one typo away // IEEE INFOCOM 2008-The 27th Conference on Computer Communications, 2008. P. 1939–1947.

242. Code pénal [Электронный ресурс]. – URL: https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070719/ (дата обращения: 14.02.2026).

243. Fraud Act 2006 [Электронный ресурс]. – URL: https://www.legislation.gov.uk/ukpga/2006/35/ (дата обращения: 11.02.2026).

244. Interpol [Электронный ресурс]. – URL: https://www.interpol.int/ (дата обращения: 19.03.2026).

245. Strafgesetzbuch [Электронный ресурс]. – URL: https://www.gesetze-im-internet.de/stgb/ (дата обращения: 13.02.2026).

246. Theft Act 1968 [Электронный ресурс]. – URL: https://www.legislation.gov.uk/ukpga/1968/ (дата обращения: 10.02.2026).

247. Антифрод-системы (Anti-fraud) [Электронный ресурс]. – URL: https://encyclopedia.kaspersky.ru/glossary/antifraud/ (дата обращения: 25.03.2026).

248. Антонян Ю.М., Эминов В.Е. Личность преступника. Криминолого-психологическое исследование [Электронный ресурс]. – URL: https://fb2.top/lichnosty–prestupnika–kriminologo–psihologicheskoe–issledovanie–522609/read (дата обращения: 07.03.2026).

249. Архив уголовных дел Белгородского областного суда [Электронный ресурс]. – URL: https://oblsud--blg.sudrf.ru/modules.php?name=sud_delo (дата обращения: 07.02.2026).

250. Билайн признан самым безопасным оператором в 2025 году по комплексу механизмов защиты абонентов сотовой связи [Электронный ресурс]. – URL: https://www.comnews.ru/content/241963/2025-10-28/2025-w44/1180/bilayn-priznan-samym-bezopasnym-operatorom-2025-godu-kompleksu-mekhanizmov-zaschity-abonentov-sotovoy-svyazi (дата обращения: 27.03.2026).

251. В Курске сотрудники полиции рассказали учащимся образовательных учреждений о мошеннических схемах [Электронный ресурс]. – URL: https://46.xn--b1aew.xn--p1ai/news/ (дата обращения: 30.03.2026).

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

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

254. В МВД создано управление по борьбе с киберпреступностью [Электронный ресурс]. – URL: https://www.kommersant.ru/doc/5592758 (дата обращения: 08.03.2026).

255. Законопроект № 186266-7 [Электронный ресурс]. – URL: https://sozd.duma.gov.ru/bill/186266-7 (дата обращения: 17.02.2026).

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

257. 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).

258. 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).

259. 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).

260. Краткая характеристика состояния преступности в Российской Федерации [Электронный ресурс]. – URL: https://xn--b1aew.xn--p1ai/reports/item/47055751/ (дата обращения: 17.03.2026).

261. Л. районный суд г. Саранска (Республика Мордовия) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/6e0BO62jtxm5/ (дата обращения: 07.03.2026).

262. Латентность киберпреступности превысила 60% [Электронный ресурс]. – URL: https://rapsinews.ru/digital_law_news/20240424/309839280.html (дата обращения: 29.06.2026).

263. МВД России [Электронный ресурс]. – URL: https://мвд.рф (дата обращения: 23.03.2026).

264. Международное сотрудничество [Электронный ресурс]. – URL: https://rapsinews.ru/digital_law_news/20251028/ (дата обращения: 22.03.2026).

265. О. районный суд г. Новокузнецка (Кемеровская область) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/ULO9JOi7W3oj/ (дата обращения: 05.03.2026).

266. Обзор операций, совершённых без добровольного согласия клиентов финансовых организаций за 2024 год [Электронный ресурс]. – URL: https://cbr.ru/analytics/ib/operations_survey/2024/ (дата обращения: 29.06.2026).

267. Основные социально-демографические и уголовно-правовые признаки осужденных по ст. 159^3 и 159^6 УК РФ [Электронный ресурс]. – URL: https://www.advgazeta.ru/mneniya/osnovnye-sotsialno-demograficheskie-i-ugolovno-pravovye-priznaki-osuzhdennykh-po-st-159-3-i-159-6-uk/ (дата обращения: 18.03.2026).

268. Памятки для граждан [Электронный ресурс]. – URL: https://xn--b1aew.xn--p1ai/booklets (дата обращения: 29.03.2026).

269. По телефону и через Госуслуги. Главные схемы, которыми пользуются мошенники в 2023 году, чтобы красть деньги россиян [Электронный ресурс]. – URL: https://lenta.ru/articles/2023/08/07/moshenniki/ (дата обращения: 13.03.2026).

270. Положение об Управлении по организации борьбы с противоправным использованием информационно-коммуникационных технологий Министерства внутренних дел Российской Федерации [Электронный ресурс]. – URL: https://xn--b1aew.xn--p1ai/mvd/structure1/Upravlenija/ (дата обращения: 09.03.2026).

271. Пояснительная записка к проекту федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации и иные законодательные акты Российской Федерации» [Электронный ресурс]. – URL: https://sozd.duma.gov.ru/bill/53700-6 (дата обращения: 12.03.2026).

272. Примерная рабочая программа воспитания в образовательной организации высшего образования [Электронный ресурс]. – URL: https://minobrnauki.gov.ru/upload/2021/04/ (дата обращения: 28.03.2026).

273. Проверка переводов близкого [Электронный ресурс]. – URL: http://www.sberbank.ru/ru/person/dist_services/blizkie-ryadom (дата обращения: 26.03.2026).

274. Профилактика мошенничеств с использованием средств сотовой связи и Интернет-ресурсов [Электронный ресурс]. – URL: https://adm.gov86.org/399/688/795/3110/ (дата обращения: 15.03.2026).

275. Региональное Отделение СФР призывает курян не поддаваться на уловки мошенников! [Электронный ресурс]. – URL: https://sfr.gov.ru/branches/kursk/news/~2024/04/15/262732 (дата обращения: 31.03.2026).

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

277. Россияне перевели мошенникам 168 млрд руб. за 11 месяцев 2024 года [Электронный ресурс]. – URL: https://www.kommersant.ru/doc/7421098 (дата обращения: 09.02.2026).

278. С. районный суд г. Иваново (Ивановская область) [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/ (дата обращения: 06.03.2026).

279. Сервисы кибербезопасности в приложении СберБанк Онлайн [Электронный ресурс]. – URL: http://www.sberbank.ru/ru/person/cybersecurity/ (дата обращения: 16.03.2026).

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

281. Состояние преступности [Электронный ресурс]. – URL: https://xn--b1aew.xn--p1ai/reports/6/ (дата обращения: 17.03.2026).

282. Сотрудничество с Интерполом продолжается [Электронный ресурс]. – URL: https://ria.ru/20240402/ (дата обращения: 20.03.2026).

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

284. Судебная практика по уголовным делам России [Электронный ресурс]. – URL: https://sudact.ru/regular/ (дата обращения: 06.02.2026);

285. Управление по борьбе с противоправным использованием информационно-коммуникационных технологий [Электронный ресурс]. – URL: https://otdel-k.spb.ru/ (дата обращения: 10.03.2026).

286. Что делать, если звонит телефонный мошенник [Электронный ресурс]. – URL: https://www.kommersant.ru/doc/ (дата обращения: 14.03.2026).

287. Что такое Интерпол и чем он занимается [Электронный ресурс]. – URL: https://www.rbc.ru/base/21/02/2025/ (дата обращения: 21.03.2026).

288. Число IT-преступлений в России в 2025 году сократилось до 675 тыс. [Электронный ресурс]. – URL: https://tass.ru/obschestvo/26385451 (дата обращения: 29.06.2026).

289. Обзор операций, совершенных без добровольного согласия клиентов финансовых организаций [Электронный ресурс]. – URL: https://www.cbr.ru/analytics/ib/operations_survey (дата обращения: 30.06.2026).

290. 3-D Secure 2.0 [Электронный ресурс]. – URL: https://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:3-D_Secure_2.0 (дата обращения: 24.03.2026).

Приложение 1

Анкета для социологического опроса, проведённого среди сотрудников правоохранительных органов Курской и Белгородской областей «Дистанционные хищения и меры их предупреждения»

1. В каком подразделении Вы проходите службу?

☐ Уголовный розыск

☐ Следственное подразделение

☐ Подразделение по борьбе с киберпреступлениями

☐ Дежурная часть

☐ Другое _____

2. Ваш стаж службы в правоохранительных органах:

☐ До 1 года

☐ 1–3 года

☐ 3–5 лет

☐ 5–10 лет

☐ Более 10 лет

3. Сталкиваетесь ли Вы в служебной деятельности с дистанционными хищениями?

☐ Да, регулярно

☐ Да, иногда

☐ Нет

4. Какие виды дистанционных хищений встречаются чаще всего? (несколько вариантов)

☐ Телефонное мошенничество

☐ Хищения с банковских карт

☐ Мошенничество в интернете (фишинг, поддельные сайты и т.д.)

☐ Хищения, совершаемые в социальных сетях и мессенджерах

5. Как Вы оцениваете уровень распространённости дистанционных хищений в настоящее время?

☐ Очень высокий

☐ Высокий

☐ Средний

☐ Низкий

6. Какие категории граждан чаще всего становятся потерпевшими?

☐ Пожилые люди

☐ Лица среднего возраста

☐ Молодёжь

☐ Несовершеннолетние

☐ Все категории в равной степени

7. С какими основными трудностями Вы сталкиваетесь при раскрытии дистанционных хищений?

☐ Установление личности преступника

☐ Использование анонимных средств связи

☐ Трансграничный характер преступлений

☐ Недостаток технических средств

☐ Иное

8. На Ваш взгляд меры уголовно-правового характера являются достаточными для борьбы с дистанционными хищениями?

☐ Да

☐ Скорее да

☐ Скорее нет

☐ Нет

9. Как Вы оцениваете уровень взаимодействия правоохранительных органов с банками и операторами связи?

☐ Высокий

☐ Средний

☐ Низкий

☐ Отсутствует

10. Какие профилактические меры Вы считаете наиболее эффективными?

☐ Информирование населения через СМИ

☐ Повышение цифровой грамотности граждан

☐ Профилактические беседы и лекции

☐ Оперативная блокировка счетов и номеров

☐ Ужесточение уголовной ответственности

11. Насколько, по Вашему мнению, граждане осведомлены о способах дистанционных хищений?

☐ Хорошо осведомлены

☐ Частично осведомлены

☐ Плохо осведомлены

☐ Практически не осведомлены

12. Участвуете ли Вы лично в профилактической работе с населением?

☐ Да, регулярно

☐ Да, периодически

☐ Нет

13. Как Вы оцениваете эффективность профилактики дистанционных хищений в целом?

☐ Высокая

☐ Средняя

☐ Низкая

14. Какие меры предупреждения дистанционных хищений следует усилить в первую очередь?

15. Ваши предложения по повышению эффективности борьбы с дистанционными хищениями.

Приложение 2

Данные социологического опроса, проведённого среди сотрудников правоохранительных органов Курской и Белгородской областей «Дистанционные хищения и меры их предупреждения»

Вопрос / вариант ответа	Процент (%)
1. В каком подразделении Вы проходите службу?	
Уголовный розыск	32
Следственное подразделение	28
Подразделение по киберпреступлениям	18
Дежурная часть	12
Другое	10
2. Ваш стаж службы в правоохранительных органах:	
До 1 года	8
1–3 года	18
3–5 лет	22
5–10 лет	27
Более 10 лет	25
3. Сталкиваетесь ли Вы в служебной деятельности с дистанционными хищениями?	
Да, регулярно	62
Да, иногда	30
Нет	8
4. Какие виды дистанционных хищений встречаются чаще всего? (возможно несколько вариантов)	
Телефонное мошенничество	78
Хищения с банковских карт	71
Интернет-фишинг	64

Хищения, совершаемые в социальных сетях и мессенджерах	59
5. Как Вы оцениваете уровень распространённости дистанционных хищений?	
Очень высокий	48
Высокий	37
Средний	13
Низкий	2
6. Какие категории граждан чаще всего становятся потерпевшими?	
Пожилые люди	52
Лица среднего возраста	26
Молодёжь	12
Несовершеннолетние	4
Все категории в равной степени	6
7. С какими трудностями Вы сталкиваетесь при расследовании дистанционных хищений? (несколько вариантов)	
Установление личности преступника	82
Использование анонимных средств связи	76
Трансграничный характер преступлений	61
Недостаток технических средств	44
Иное	39
8. На Ваш взгляд меры уголовно-правового характера являются достаточными для борьбы с дистанционными хищениями?	
Да	9
Скорее да	34
Скорее нет	38
Нет	19

9. Как Вы оцениваете уровень взаимодействия с банками и операторами связи?	
Высокий	21
Средний	46
Низкий	25
Отсутствует	8
10. Какие профилактические меры Вы считаете наиболее эффективными? (до 3 вариантов)	
Информирование населения через СМИ	74
Повышение цифровой грамотности	69
Оперативная блокировка счетов и номеров	63
Профилактические беседы	41
Ужесточение уголовной ответственности	38
11. Насколько граждане осведомлены о способах дистанционных хищений?	
Хорошо осведомлены	6
Частично осведомлены	38
Плохо осведомлены	41
Практически не осведомлены	15
12. Участвуете ли Вы лично в профилактической работе с населением?	
Да, регулярно	28
Да, периодически	44
Нет	28
13. Как Вы оцениваете общую эффективность профилактики дистанционных хищений?	
Высокая	11
Средняя	53
Низкая	36

14. Какие меры предупреждения дистанционных хищений следует усилить в первую очередь? (обобщённые ответы)	
Информационная работа с населением	42
Усиление взаимодействия с банками и операторами связи	31
Укрепление технического оснащения подразделений	27
15. Ваши предложения по повышению эффективности борьбы с дистанционными хищениями (обобщённые ответы)	
Усиление межведомственного взаимодействия	35
Повышение цифровой грамотности населения	29
Совершенствование законодательства	21
Расширение полномочий правоохранительных органов	15

Приложение 3

Описание программы для ЭВМ для определения рисков дистанционных хищений с использованием электронных средств платежа

Программа предназначена для автоматизированного выявления, предотвращения дистанционных хищений с использованием электронных платёжных средств. В отличие от классических антифрод-систем, которые анализируют только технические параметры транзакций, данная программа интегрирует криминологические знания о личности преступника, его мотивации, способах вовлечения в преступную деятельность и виктимологической уязвимости потенциальных жертв.

Программа решает три основные задачи. Первая – обнаружить аномальные и потенциально мошеннические транзакции в потоке платежей. Вторая – на основе полученных в диссертации результатов анализа 200 уголовных дел и выявленных закономерностей оценить не только саму транзакцию, но и профиль получателя средств на предмет соответствия типичному портрету преступника, а также профиль отправителя на предмет виктимологической уязвимости. Третьей задачей является формирование персонализированных предупреждений для клиентов с учётом конкретного сценария мошенничества и обеспечить обратную связь для дообучения моделей на основе вновь раскрытых преступлений. Программа ориентирована на использование в банках, платёжных системах, правоохранительных органах и исследовательских центрах, занимающихся противодействием киберпреступности.

На входе программа принимает структурированные данные о транзакции, включающие стандартные поля – идентификатор клиента, сумму, время, тип операции, страну и категорию мерчанта, баланс до и после операции, а также расширенные криминологические поля – возраст и пол отправителя и получателя, уровень цифровой грамотности отправителя, сведения о том, был ли клиент ранее жертвой мошенничества, образование и

занятость получателя, признак групповой активности. Если какие-либо криминологические поля отсутствуют, программа заполняет их вероятностными значениями на основе статистических распределений, полученных из анализа уголовных дел.

Далее программа выполняет три независимые оценки. Первая оценка – это виктимологическая уязвимость отправителя. Программа анализирует возраст клиента, его цифровую грамотность и историю предыдущих инцидентов. Если клиент старше 60 лет, имеет низкий уровень цифровой грамотности или уже становился жертвой мошенников, программа повышает его виктимологический множитель. Этот множитель в дальнейшем снижает порог срабатывания системы, то есть для уязвимых клиентов даже небольшое отклонение от нормы может привести к блокировке операции.

Вторая оценка – криминологический риск получателя. Программа сопоставляет профиль счёта или карты получателя с типичным портретом преступника, определяемым на основе исследуемых статистических данных. Кроме того, программа анализирует историю транзакций получателя на наличие дропперских паттернов – быстрый ввод и вывод средств, множество источников поступлений, мелкие тестовые переводы перед крупными, молодой возраст счёта.

Третья оценка – сценарий мошенничества. Программа сопоставляет транзакцию с одним из типичных сценариев, выявленных в ходе криминологического анализа. Сценарий «ошибочного перевода» распознаётся, когда сумма операции равна сумме недавнего входящего перевода от того же отправителя. Сценарий «звонка из службы безопасности банка» распознаётся, если перед операцией клиент получил подозрительный звонок и переводит деньги новому физическому лицу. Сценарий «помощи родственнику» распознаётся, когда сумма значительно превышает средние траты клиента, получатель новый и не является юридическим лицом. Сценарий «перевода на безопасный счёт» распознаётся, по ключевым словам, в назначении платежа или имени получателя и т.д.

Параллельно с криминологическим анализом программа запускает ансамбль моделей машинного обучения. Модель Isolation Forest выступает в роли быстрого фильтра, выявляя статистические аномалии без обучения на размеченных данных. Модель XGBoost, обученная на исторических данных с учётом криминологических признаков, выдаёт калиброванную вероятность мошенничества. Для клиентов с богатой историей транзакций дополнительно применяется LSTM-сеть, которая анализирует временные паттерны поведения. Для выявления организованных схем используется графовая нейронная сеть, которая анализирует связи между счетами. Итоговая вероятность мошенничества вычисляется как взвешенная комбинация выходов всех моделей и криминологических оценок.

На основе итоговой вероятности и виктимологического множителя программа принимает одно из четырёх решений. При низком риске, когда вероятность ниже 0,3, транзакция одобряется без дополнительных проверок. При среднем риске, от 0,3 до 0,6, клиенту направляется push-уведомление с просьбой подтвердить операцию. При высоком риске, от 0,6 до 0,8, транзакция блокируется, и клиенту отправляется детальное предупреждение с описанием выявленного сценария мошенничества. При критическом риске, выше 0,8, транзакция блокируется, клиенту поступает звонок от службы безопасности и, при необходимости, информация передаётся в правоохранительные органы.

Этап обратной связи и дообучения реализует замкнутый цикл, характерный для современных антифрод-систем. Когда мошенничество подтверждается в ходе расследования, а тем более, когда возбуждается уголовное дело, данные по этому инциденту попадают в буфер обратной связи. После накопления ста новых прецедентов программа автоматически дообучает модели XGBoost, учитывая новые схемы и типы преступников. Это позволяет системе адаптироваться к эволюции криминальных методов, не дожидаясь ручного переобучения.

Описывая входные данные, укажем, что программа принимает на вход структурированный набор данных о банковских транзакциях. Основная единица данных – одна платёжная операция. Входные данные могут быть как синтетическими (генерируются самой программой для тестирования и отладки), так и реальными (загружаются из банковских систем в виде CSV, Excel или через прямой запрос к базе данных). Каждая транзакция в исходном наборе должна содержать следующие поля: Customer ID – уникальный идентификатор клиента, совершающего операцию (это может быть номер счёта, номер карты или внутренний идентификатор банковской системы); Timestamp – дата и время совершения транзакции с точностью до секунды или минуты (необходимо для анализа временных паттернов и построения последовательностей); Amount – сумма транзакции в денежном выражении; Transaction type – тип операции.

Merchant country – страна, где зарегистрирован банк-получатель. Для операций внутри страны указывается HOME_COUNTRY. Для трансграничных операций – код страны: US, UK, DE, CN, OTHER или HIGH_RISK_COUNTRY. Merchant category – категория торгово-сервисного предприятия (возможные значения: RETAIL (розничная торговля), FOOD (общепит), TRAVEL (путешествия, авиабилеты, отели), UTILITIES (коммунальные платежи), ENTERTAINMENT (развлечения, игры)).

Balance before – баланс на счёте клиента до совершения транзакции (используется для расчёта доли списанных средств и оценки влияния операции на финансовое состояние клиента). Balance after – баланс на счёте клиента после совершения транзакции.

Is fraud – целевая метка, указывающая, является ли транзакция мошеннической. Принимает значение 1 для мошеннических операций и 0 для легитимных. Это поле требуется только для обучения моделей с учителем (XGBoost, LSTM). Для работы Isolation Forest и для реального инференса оно не требуется.

Возраст отправителя – возраст клиента в годах. Тип данных – целое число от 18 до 100. Пол отправителя – пол клиента. Возможные значения: male, female. Тип данных – категориальная строка. Уровень цифровой грамотности – оценка способности клиента распознавать мошеннические схемы и пользоваться цифровыми сервисами. Тип данных – число с плавающей точкой от 0 до 1, где 0 – полное отсутствие навыков, 1 – эксперт. Рассчитывается на основе истории операций, возраста, образования. Признак предыдущего виктимного опыта – индикатор того, становился ли клиент ранее жертвой дистанционного мошенничества. Тип данных – целое число 0 или 1.

Возраст получателя – возраст владельца счёта или карты получателя. Тип данных – целое число от 18 до 80. Пол получателя – пол. Возможные значения: male, female. Образование получателя – уровень и направление образования. Возможные значения: secondary – среднее общее, specialized_secondary – среднее специальное, higher – высшее, technical – техническое, it – информационные технологии, higher_economic – высшее экономическое. Занятость получателя – текущий трудовой статус. Возможные значения: employed – работает, unemployed – безработный, student – студент, retired – пенсионер, it – занят в ИТ-сфере, trade_services – сфера услуг или торговли. Признак групповой активности – индикатор того, связан ли счёт получателя с другими подозрительными счетами. Тип данных – целое число 0 или 1. История транзакций отправителя – DataFrame или список предыдущих операций клиента за последние 90 дней. Необходим для расчёта скользящих средних, отклонений и поведенческих паттернов. История транзакций получателя – DataFrame или список операций счёта получателя. Необходим для выявления дропперских паттернов – быстрого ввода и вывода средств, множества источников, тестовых переводов, молодого возраста счёта. Признак подозрительного звонка перед операцией – индикатор того, поступал ли на телефон клиента звонок с номера из базы мошенников непосредственно перед транзакцией. Тип данных – целое число 0 или 1.

Целевая метка – используется только для обучения моделей. Указывает, является ли транзакция подтверждённым мошенничеством. Тип данных – целое число 0 или 1. Кроме этих обязательных полей, программа может принимать дополнительные атрибуты транзакции, такие как идентификатор устройства (device ID), IP-адрес, регион, операционную систему мобильного приложения и другие параметры, которые используются для обогащения признакового пространства.

В итоге программа формирует несколько видов выходных данных: результаты классификации отдельных транзакций, метрики качества моделей, визуализации и объяснения решений, а также сигналы о состоянии данных. Для каждой проанализированной транзакции программа возвращает следующий набор полей. Идентификатор транзакции – уникальный номер, позволяющий связать результат с исходной операцией. Предсказанная метка – бинарное значение, указывающее, отнесла ли модель операцию к мошенническим (1) или к легитимным (0). Вероятность мошенничества – дробное число от 0 до 1, показывающее степень уверенности модели в том, что операция является мошеннической. Уровень риска – категориальная оценка, получаемая путём пороговой обработки вероятности. Возможные значения: низкий (вероятность менее 0,3), средний (0,3-0,6), высокий (0,6-0,8), критический (более 0,8).

В результате следует рекомендация – строка с практическим действием («Одобрить», «Отправить пуш-уведомление для подтверждения», «Заблокировать, запросить дополнительную аутентификацию», «Немедленная блокировка и звонок клиенту»). Текст предупреждения для клиента – персонализированное сообщение, формируемое на основе выявленного сценария мошенничества и характеристик клиента. Кроме основного результата, программа возвращает детальные криминологические оценки, которые могут быть полезны для аналитиков службы безопасности.

Виктимологический множитель отправителя – число от 1 до 2, показывающее, во сколько раз снижен порог блокировки для данного

клиента. Значение 1 означает стандартный порог, 2 – порог снижен вдвое. Расчёт учитывает возраст, цифровую грамотность и историю предыдущих инцидентов. Криминологический риск получателя – число от 0 до 1, оценивающее, насколько профиль получателя соответствует типичному портрету преступника. Признак дропперской активности – булево значение, указывающее, идентифицирован ли счёт получателя как дропперский. Тип данных – логический. Дополнительно возвращается уровень уверенности в этом решении – число от 0 до 1. Тип вовлечения получателя – категория, показывающая, каким образом владелец счёта предположительно был вовлечён в преступную деятельность. Возможные значения: LATENT – латентное вовлечение, человек может не осознавать, что участвует в преступлении; CONSCIOUS – осознанное вовлечение с пониманием противоправности; COERCED – принудительное вовлечение под давлением. Для моделей, поддерживающих объяснимость, программа также возвращает SHAP-значения для каждой транзакции. SHAP-значения показывают, насколько каждый признак увеличил или уменьшил вероятность мошенничества по сравнению с базовым средним. Например, SHAP-значение для признака «ночное время» может быть положительным и большим, указывая, что именно этот фактор сильнее всего повлиял на решение модели отнести операцию к мошенническим.

Таким образом, программа представляет собой интеллектуальную криминолого-ориентированную антифрод-систему нового поколения, сочетающую методы машинного обучения, поведенческой аналитики и прикладной криминологии. Благодаря механизму непрерывного дообучения система способна адаптироваться к быстро изменяющимся способам совершения дистанционных хищений и повышать точность выявления новых преступных схем. Использование программы позволяет снизить количество успешных мошеннических операций, минимизировать финансовые потери банков и клиентов, а также повысить эффективность профилактики дистанционных хищений.

Приложение 4

5951 24.06.26

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2026667563

Программа для определения рисков дистанционных хищений с электронных платежных средств

Правообладатель: ***Федеральное государственное бюджетное образовательное учреждение высшего образования «Юго-Западный государственный университет» (RU)***

Автор(ы): ***Пивнева Людмила Валерьевна (RU)***

Заявка № **2026666921**
Дата поступления **22 мая 2026 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***09 июня 2026 г.***

Руководитель Федеральной службы
по интеллектуальной собственности

Ю.С. Зубов

Приложение 5

Формуляр изучения материалов уголовных дел о дистанционных хищениях

№	Блок изучаемых сведений	Фиксируемые показатели
1	Общие сведения об уголовном деле	Год производства, субъект Российской Федерации, количество лиц
2	Характеристика совершённого преступления	Квалификация, форма и способ хищения
3	Социально-демографическая характеристика лица	Пол, возраст, семейное положение, наличие детей, уровень образования, занятость, сфера трудовой деятельности, опыт использования ИТК
4	Уголовно-правовая характеристика личности	Наличие и количество судимостей, рецидив, характер предшествующей преступной деятельности
5	Роль в механизме совершения преступления	Организатор, технический исполнитель, социальный инженер, номинальный участник (дроппер)
6	Поведенческие характеристики	Особенности поведения при подготовке и совершении преступления, характер взаимодействия с соучастниками и потерпевшими, способы использования цифровых средств и каналов коммуникации,

		особенности распределения и выполнения преступных функций, особенности использования аккаунтов, телефонных номеров, платёжных средств и иных цифровых инструментов, применение мер по сокрытию следов преступной деятельности и т.п.
7	Мотивационные и иные криминологически значимые сведения	Мотив совершения преступления, характер вовлечения в преступную деятельность, иные обстоятельства, имеющие криминологическое значение