МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Кафедра уголовного права и криминологии

ДИПЛОМНАЯ РАБОТА

на тему **«УГОЛОВНО-ПРАВОВЫЕ СРЕДСТВА ПРОТИВОДЕЙСТВИЯ ХИЩЕНИЯМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ (ПО МАТЕРИАЛАМ СУДЕБНОЙ ПРАКТИКИ)»**

Выполнил
Назаров Александр Вячеславович,
обучающийся по специальности
40.05.02 Правоохранительная деятельность,
2021 года набора, 123 учебного взвода

Руководитель
доцент кафедры
кандидат юридических наук, доцент
Гарифуллина Разиля Файзуллиловна

К защите _рекомендуется_
рекомендуется / не рекомендуется
Начальник кафедры _____ И.Р. Диваева
подпись
Дата защиты «___» _____ 2026 г. Оценка _____

ПЛАН

Введение……...3
Глава 1. Уголовная ответственность за хищения путем использования информационных технологий……7
§ 1. Социальная обусловленность уголовной ответственности за хищения путем использования информационных технологий……...7
§ 2. История развития законодательства Российской Федерации о хищениях с использованием информационных технологий……..…..11
Глава 2. Уголовно-правовая характеристика хищений, совершаемых с использованием информационных технологий……..…..16
§ 1. Объективные признаки хищений путем использования информационных технологий……..16
§ 2. Субъективные признаки хищений путем использования информационных технологий……..22
§ 3. Квалифицирующие и особо квалифицирующие признаки хищений путем использования информационных технологий……26
Глава 3. Совершенствование уголовного законодательства, предусматривающего ответственность за хищения путем использования информационных технологий, и практика его применения……..……...35
§ 1. Проблемы квалификации хищений, совершаемых с использованием информационных технологий, в уголовном праве Российской Федерации…...35
§ 2. Перспективы совершенствования уголовного законодательства в сфере хищений с использованием информационных технологий……..40
Заключение……46
Список использованной литературы……...49
Приложение 1……56

ВВЕДЕНИЕ

Актуальность темы исследования. Стремительная цифровизация всех сфер общественной жизни и экономики, наряду с несомненными преимуществами, породила новые, высокотехнологичные формы преступной деятельности. Хищения, совершаемые с использованием информационных технологий (ИТ), превратились в одну из наиболее серьезных угроз экономической безопасности Российской Федерации. Их масштабы исчисляются миллиардами рублей, а уровень латентности остается крайне высоким в силу транснационального характера, анонимности и сложности механизма данных преступлений.

Так, за январь-октябрь 2025 г. 297 преступлений по ст. 159.6 УК РФ, что демонстрирует незначительный рост на 3,1 % по сравнению с аналогичным периодом прошлого года. Несмотря на этот небольшой прирост, данная статья составляет лишь малую долю (около 0,05%) в общем массиве зарегистрированных мошенничеств и менее 0,1 % среди всех преступлений, совершённых с использованием информационных технологий. Это указывает на то, что классические формы кибермошенничества (по ст. 159 УК РФ) остаются доминирующими, в то время как, непосредственно компьютерное мошенничество, как самостоятельный состав регистрируется относительно редко[1].

Преступники постоянно совершенствуют свои методы, используя фишинг, вредоносное программное обеспечение, взлом баз данных, несанкционированный доступ к банковским счетам и системам дистанционного банковского обслуживания. Это ставит перед законодателем и правоприменителем сложнейшую задачу по адекватному и своевременному противодействию. Действующее уголовное законодательство, в частности, нормы главы 21 Уголовного кодекса РФ «Преступления против

[1] Министерство внутренних дел Российской Федерации. Краткая характеристика состояния преступности за январь-октябрь 2025 г. [Электронный ресурс]. URL: https://xn--b1aew.xn-- p1ai/reports/item/47055751/ (датаобращения: 25.11.2025).

собственности»(далее – УК РФ), вынуждено адаптироваться к реалиям цифровой эпохи, что порождает множество дискуссионных вопросов квалификации. В этой связи анализ и обобщение судебной практики становится ключевым инструментом для выявления пробелов в правовом регулировании и сложностей, возникающих у судов при применении уголовно-правовых норм.

Степень научной разработанности проблемы преступлений с использованием информационных технологий в отечественной юридической науке является значительной, но фрагментарной и развивающейся. Так, классические труды по уголовному праву (Таганцев Н.С., Пионтковский А.А.) и собственности (Кочои С.М., Елисеев С.А., Лопашенко Н.А.) служат основой для анализа заявленной проблемы. Выработаны базовые дефиниции и классификации киберпреступности (Чекунов И.Г., Тропина Т.Л., Суслопаров А.В.). Детально исследован ключевой состав – мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ). Учёные проанализировали его объективные и субъективные признаки (Хилюта В.В., Дворецкий М.Ю.), проблемы квалификации и отграничения от смежных составов (Яни П.С., Безверхов А.Г.), специфику соучастия (Дмитренко А.П., Русскевич Е.А.) и законодательную конструкцию норм (Хисамова З.И.). Эти исследования тесно связаны с правоприменительной практикой и основываются на постановлениях Пленума Верховного Суда Российской Федерации, и работах по теории квалификации (Рарог А.И., Кудрявцев В.Н., Гаухман Л.Д.).

Объектом исследования являются общественные отношения, возникающие в связи с совершением хищений с использованием информационных технологий и применением уголовно-правовых средств для противодействия им.

Предмет исследования составляют нормы уголовного законодательства Российской Федерации, предусматривающие ответственность за хищения, материалы опубликованной судебной практики, а также доктринальные источники по исследуемой проблематике.

Целью выпускной квалификационной работы является комплексный анализ уголовно-правовых средств противодействия хищениям, совершаемым с использованием информационных технологий, и на этой основе разработка предложений по совершенствованию законодательства и правоприменительной практики.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Проследить историческую эволюцию и социальную обусловленность уголовно-правового регулирования ответственности за хищения с использованием информационных технологий в российском законодательстве.

2. Раскрыть уголовно-правовую характеристику хищений, совершаемых с использованием информационных технологий (далее – ИТ): определить объект, предмет, объективную и субъективную стороны данного преступления.

3. Проанализировать состав мошенничества в сфере компьютерной информации (ст. 159.6 УК РФ) как основного средства противодействия, включая квалифицирующие и особо квалифицирующие признаки.

4. Исследовать и обобщить материалы судебной практики по делам о хищениях с использованием ИТ для выявления типичных проблем квалификации, отграничения от смежных составов (кражи, мошенничества) и оценки доказательств.

5. Выявить системные проблемы и противоречия в действующем уголовном законодательстве, регулирующем ответственность за IT-хищения.

6. Разработать конкретные предложения и рекомендации по совершенствованию уголовного законодательства и практики его применения.

Методологическая основа исследования включает в себя совокупность общенаучных и частно-научных методов познания: диалектический, формально-логический, сравнительно-правовой, системно-структурный, статистический методы, а также метод анализа судебной практики.

Нормативную и эмпирическую базу исследования составили Конституция РФ, Уголовный кодекс РФ, иные федеральные законы, постановления Пленума

Верховного Суда Российской Федерации. Эмпирическую основу работы образуют опубликованные материалы судебной практики, включая решения Верховного Суда Российской Федерации, обзоры судебной практики, а также приговоры и постановления федеральных судов общей юрисдикции по конкретным уголовным делам о хищениях с использованием информационных технологий.

Структура работы обусловлена целью и задачами исследования и включает в себя введение, три главы, шесть параграфов, заключение, список использованной литературы.

ГЛАВА 1. УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ ЗА ХИЩЕНИЯ ПУТЕМ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

§1. Социальная обусловленность уголовной ответственности за хищения путем использования информационных технологий

Социальная обусловленность уголовно-правового запрета является фундаментальным принципом криминализации деяний, означающим, что законодатель вводит уголовную ответственность не произвольно, а в ответ на реальные общественные потребности, вызванные ростом общественной опасности тех или иных форм поведения. Хищения, совершаемые с использованием информационных технологий, представляют собой яркий пример такого социально обусловленного правового явления, необходимость уголовно-правового противодействия которому диктуется всей логикой развития современного информационного общества.

Как справедливо отмечается в Стратегии развития информационного общества Российской Федерации на 2017-2030 гг., формирование цифровой экономики и информационного пространства является ключевым направлением национального развития[1]. Однако параллельно с предоставлением безграничных технологических возможностей произошла трансформация криминальной среды, которая активно использует новые инструменты для посягательств на охраняемые законом ценности. Информация, превратившись в ключевой экономический актив, одновременно стала и главным объектом, и инструментом преступных посягательств. Социальная обусловленность криминализации хищений в сфере информационных технологий проистекает из совокупности следующих взаимосвязанных факторов.

Во-первых, решающим фактором выступает исключительно высокая и постоянно растущая общественная опасность данных деяний. Практика

[1] О стратегии развития информационного общества в Российской Федерации на 2017-2030 годы: указ Президента Российской Федерации от 9 мая 2017 г. № 203 // Собр. законодательства Рос. Федерации. – 2017. – № 20, ст. 2901.

свидетельствует о лавинообразном росте количества таких преступлений и колоссальном размере причиняемого ущерба, который многократно превышает ущерб от традиционных форм хищения. По данным МВД России, за 2024 г. по «Мошенничеству» (ст. 159, 159.1-159.6 УК РФ) было осуждено 37 457 человек, при этом зафиксирован значительный рост киберпреступлений (до 40% всех преступлений в ИКТ-сфере) и ущерба от них[1]. Глобальный масштаб проблемы подчеркивается и тем, что, по оценкам компании «Symantec», ежегодный мировой доход от преступлений в сфере информационных технологий достигает 114 млрд долларов[2]. Подобные деяния наносят удар не только по имущественным интересам конкретных лиц и организаций, но и подрывают основы национальной экономической безопасности, доверие к цифровым финансовым институтам и, как следствие, тормозят развитие цифровой экономики в целом, что подтверждается инициативами на высшем государственном уровне, такими как создание системы обмена информацией о киберугрозах. Так, глава Сбербанка Герман Греф выступил с предложением о формировании специального органа, обеспечивающего безопасность от киберпреступлений – Министерство по чрезвычайным ситуациям в информационной сфере[3]. А в 2018 г. В.В. Путин анонсировал создание ИТ-системы обмена информацией о киберугрозах.

Во-вторых, социальную значимость проблемы усугубляет транснациональный и латентный характер киберхищений. Преступники, действуя анонимно в глобальной сети, зачастую не знакомы друг с другом в реальной жизни, а их взаимодействие осуществляется посредством

---

[1] Министерство внутренних дел Российской Федерации. Краткая характеристика состояния преступности за январь-декабрь 2024 г. [Электронный ресурс]. URL: https://xn--b1aew.xn-- p1ai/reports/item/47055751/ (датаобращения: 25.11.2025).

[2]Чекунов И.Г. Киберпреступность: понятие и классификация // Российский следователь. 2022. № 2. С. 38.

[3] Хисамова З.И. О конструкции норм уголовного законодательства, предусматривающих ответственность за преступления, совершаемые с использованием информационно-телекоммуникационных технологий // В сборнике: уголовная политика и культура противодействия преступности. Материалы Международной научнопрактической конференции. Краснодарский университет МВД России. 2016. С. 346.

виртуальных средств идентификации[1]. Это создает серьезные препятствия для правоохранительных органов, чье реагирование, по признанию аналитиков, не успевает за скоростью технологического развития, а раскрываемость таких преступлений не превышает 5%[2]. Способность совершать хищения дистанционно, без непосредственного контакта с потерпевшим, и мгновенно выводить средства с использованием криптовалют и иных цифровых инструментов, формирует новую, более изощренную и опасную криминальную среду.

В-третьих, особую озабоченность вызывает криминализация молодежной среды. Статистика указывает на устойчивую тенденцию роста числа хищений, совершаемых несовершеннолетними с использованием информационных технологий. Высокий уровень компьютерной грамотности в сочетании с недостаточной социальной зрелостью создает опасный симбиоз, при котором несовершеннолетние легко вовлекаются в совершение IT-преступлений, ошибочно считая их «несерьезными» или «бесконтактными». Данное обстоятельство ставит перед законодателем вопрос о необходимости пересмотра возрастного порога уголовной ответственности за мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ) и его снижении с 16 до 14 лет[3]. Эта мера, поддержанная большинством опрошенных практикующих юристов, была бы социально оправдана, поскольку соответствует реальной степени общественной опасности, исходящей от деяний данной категории.

В-четвертых, ключевым аспектом социальной обусловленности является проблема дифференциации уголовной ответственности. В российском законодательстве хищение путем использования информационных технологий

---

[1] Дмитренко А.П., Русскевич Е.А. О нетипичных аспектах соучастия в преступлениях, совершаемых с использованием информационно-коммуникационных технологий // Вестник Академии Генеральной прокуратуры Российской Федерации 2021. №5 (61). С. 18.

[2] Аналитический обзор «Комплексный анализ состояния преступности в Российской Федерации и расчетные варианты ее развития». – Москва, 2018. [Электронныйресурс].URL:https:mvd/uplpad site 163 document_ text/Kompleksnyy_analiz_maket. 24.04.pdf. (дата обращения: 10.12.2025).

[3] Гриб Д.В. Уголовная ответственность за хищение, совершаемое путем использования информаиоцнных технологий по законодательстве Республики Беларусь и Российской Федерации: дис. … канд. юрид. наук, Москва. 2021. С. 31.

криминализировано как разновидность мошенничества (ст. 159.6 УК РФ). Однако санкции за «традиционное» мошенничество (ст. 159 УК РФ) и за мошенничество в сфере компьютерной информации практически идентичны, что вступает в противоречие с принципом справедливости и не отражает повышенной общественной опасности последнего. Использование информационных технологий предоставляет преступнику беспрецедентный по масштабам доступ к потенциальным жертвам и информационным ресурсам, что качественно меняет характер и потенциал вреда. В этой связи более социально обусловленной представляется позиция, согласно которой хищение путем использования компьютерной техники – есть самостоятельная форма хищения с предусмотренной повышенной санкцией, что адекватно отражает специфику и опасность данного деяния.

Таким образом, социальная обусловленность установления и ужесточения уголовной ответственности за хищения с использованием информационных технологий в России является объективной и многогранной. Она детерминирована резким ростом общественной опасности этих деяний, их транснациональным характером, низкой латентностью, вовлечением в них несовершеннолетних и текущим несоответствием системы наказаний принципам дифференциации ответственности. Дальнейшее совершенствование уголовного законодательства в этой сфере, включая возможное выделение данного деяния в самостоятельный состав и ужесточение санкций, продиктовано насущной социальной потребностью в обеспечении безопасности личности, общества и государства в условиях стремительной цифровой трансформации.

§ 2. История развития законодательства Российской Федерации о хищениях с использованием информационных технологий

История развития уголовного законодательства свидетельствует о том, что каждое преступное деяние непосредственно связано с нормотворческим процессом совершенствования определенных правовых норм, которые предусматривают ответственность за совершение такого деяния. В этой связи известный русский ученый Н. С. Таганцев указал, что «если мы желаем изучить какой-нибудь юридический институт, существующий в данное время, то для правильного его уяснения мы должны проследить его историческую судьбу»[1]. Указанное утверждение не потеряло актуальности и в настоящее время, поскольку исследование развития правового института, явления или нормы, не только способствует совершенствованию законодательства, но и помогает решить существующие проблемы уголовного права, выработать кардинально новый подход их решения.

В связи с этим следует указать, что историческое развитие уголовно-правовых норм, направленных против хищений, совершаемых с использованием информационных технологий, в Российской Федерации прошло несколько этапов, отражающих эволюцию как технологий, так и понимания их криминального потенциала.

1. Советский период (до 1991 г.). В уголовном законодательстве СССР полностью отсутствовали специальные составы преступлений, связанные с использованием компьютерной техники. Понятия «компьютерное преступление» не существовало, а хищения квалифицировались по традиционным нормам о краже, мошенничестве или присвоении. Однако именно в этот период были зафиксированы первые случаи использования вычислительной техники для противоправного завладения имуществом. Так, в 1979 г. в Вильнюсе было совершено хищение 78 584 рублей с помощью ЭВМ, а

[1] Таганцев Н.С. Курс русского уголовного права. Часть Общая. Книга 1-я. Учение о преступлении. СПб., 1874. С. 21.

в 1983 г. в Тольятти путём модификации программы был причинён ущерб на 1 миллион рублей[1]. Эти эпизоды, однако, не привели к криминализации новых способов – они расследовались и квалифицировались в рамках действовавших общих норм, что создавало значительные трудности для правоприменения.

2. 1990-е г.: распад СССР и бурное развитие компьютерных технологий в России обусловили необходимость правового реагирования. Первой значимой вехой стало принятие Уголовного кодекса РФ 1996 г., в который была включена глава 28 «Преступления в сфере компьютерной информации» (ст. 272–274). То есть с начала 60-х гг. по конец 80-х гг., в СССР не существовало специального законодательства об ответственности за преступления, совершаемые путем использования компьютерной техники. В 1991 г. был разработан проект Закона РСФСР «Об ответственности за правонарушения при работе с информацией». Как указывает Д. А. Ястребов, проект Закона предполагал дополнить Уголовный кодекс правовыми нормами, устанавливающими ответственность за преступные деяния в сфере компьютерной информации, однако, данный проект не был реализован в законодательстве СССР[2]. Однако следует согласиться с мнением Козаева Н.Ш., который справедливо указал, что в соответствии с указанными изменениями, не всегда возможно четко определить границы новых составов[3].

Впервые на законодательном уровне были криминализированы: неправомерный доступ к компьютерной информации, создание и распространение вредоносных программ, нарушение правил эксплуатации ЭВМ. Однако эти нормы были ориентированы прежде всего на защиту информации и функционирования компьютерных систем, а не на хищение

---

[1] Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дисс… канд.юрид. наук. Владивосток, 2005. С. 27.

[2]Ястребов Д.А. Информационная безопасность в Российской Федерации: (уголовно-правовая борьба с неправомерным доступом к компьютерной информации) / Д.А. Ястребов, Н.В. Брянцева. Москва: Полтекс, 2006. С. 86.

[3]Козаев Н.Ш. «Электронные» и «Пластиковые деньги» деньги и преступность / Материалы международнойнаучно-практической конференции. ФГАОУ ВПО «Северо-Кавказский федеральный университет»; ФГКУ«Всероссийский научно-исследовательский институт МВД России» (филиал по Северо-Кавказскомуфедеральному округу); НОУ ВПО «Северо-Кавказский гуманитарно-технический институт». 2020. С. 111.

имущества. Квалификация хищений, совершаемых с помощью информационных технологий, по-прежнему осуществлялась по статьям о краже или мошенничестве (ст. 158, 159 УК РФ), что не учитывало специфики «бесконтактного» цифрового способа.

3. 2010-е г.: стремительный рост числа хищений, совершаемых путём вмешательства в компьютерные системы и сети (например, путём взлома онлайн-банкинга, краж данных платежных карт, манипуляций с электронными платежами), выявил пробелы в законодательстве. Проблема усугублялась сложностью квалификации таких деяний по статьям о традиционном мошенничестве, где необходим обман или злоупотребление доверием человека, а не воздействие на информационную систему.

Законодательным ответом стал Федеральный закон от 29.11.2012 № 207-ФЗ, который ввёл в УК РФ ряд специальных составов мошенничества. Ключевой для рассматриваемой сферы стала статья 159.6 УК РФ «Мошенничество в сфере компьютерной информации»[1]. В её диспозиции указан специфический способ: хищение чужого имущества или приобретение права на него путём:ввода, удаления, блокирования, модификации компьютерной информации;иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации либо информационно-телекоммуникационных сетей.

Это позволило чётко отделить киберхищения от традиционного мошенничества и кражи, устранив необходимость доказывания обмана человека. Одновременно была введена ст. 159.3 УК РФ «Мошенничество с использованием платёжных карт», которая охватывает смежную, но иную группу деяний, где преступник, как правило, взаимодействует с финансовыми институтами через персонал или физические носители.

---

[1] О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации: федер. закон Рос. Федерации от 29 ноября 2012 г. № 207-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 23 ноябр. 2012 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 28 ноябр 2012 г. // Рос. газ. – 2012. – 3 декабря.

4. После 2012 г.: несмотря на значительный шаг вперёд, введение ст. 159.6 УК РФ породило в юридическом сообществе серьёзные дискуссии о её природе и месте в системе составов против собственности. Сложились три основных подхода.Так, одни учёные считали, что выделение отдельных составов было избыточным, а проблемы можно было решить путём дополнения квалифицирующих признаков в общую норму о мошенничестве[1]; другие поддерживают выделение специальной нормы как адекватный ответ потребностям практики, облегчающий квалификацию[2]; третьи указывают, что ст. 159.6 УК РФ фактически описывает не мошенничество, а новую, самостоятельную форму хищения[3]. Её специфика – в программно-информационном воздействии на компьютерную систему без тактильного контакта и без обязательного обмана человека.

Критика действующей конструкции ст. 159.6 УК РФ также связана с терминологической неопределённостью. Законодательное определение «компьютерной информации» (примечание к ст. 272 УК РФ) как сведений, представленных в форме электрических сигналов, считается рядом учёных,устаревшим и не охватывающим современные технологии (например, оптоволоконные сети)[4]. В науке предлагаются более широкие понятия, такие как «электронная» или «цифровая» информация.

История российского законодательства в этой области демонстрирует путь от полного игнорирования специфики ИТ-преступлений через защиту информации к целенаправленной криминализации хищений, совершаемых путём вмешательства в компьютерные данные и системы. Ключевым достижением стало введение ст. 159.6 УК РФ в 2012 г. Однако эволюция продолжается: сохраняются споры о юридической природе этого деяния,

---

[1]Догузов С.А. История развития правового регулирования преступлений, связанных с использованием компьютерной информации // Проблемы развития научного потенциала и направления его повышения. 2024. С. 120.

[2] Яни П.С. Специальные виды мошенничества // Законность. 2015. № 8. С. 35–36.

[3] Чупрова А.Ю. Проблемы классификации мошенничества с использованием информационных технологий // Уголовное право. 2020. № 5. С. 134.

[4] Суслопаров А.В. Компьютерные преступления как разновидность преступлений информационного характера: автореф. дисс… канд. юрид. наук. Владивосток, 2010. С. 29.

недостатках терминологии и необходимости дальнейшего совершенствования нормы, возможно, в сторону её трансформации в отдельный состав хищения, а не специальный вид мошенничества. Это отражает постоянный поиск баланса между традиционными правовыми конструкциями и необходимостью адекватного противодействия новым, технологически сложным угрозам.

ГЛАВА 2. УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА ХИЩЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

§1. Объективные признаки хищения путем использования информационных технологий

В теории уголовного права устоялось положение, согласно которому объектом преступления являются охраняемые уголовным законом общественные отношения, которым преступным деянием причиняется вред либо создается реальная угроза его причинения[1]. Верная и исчерпывающая интерпретация содержания объекта преступления выступает фундаментальным условием как для конструирования составов преступлений, так и для адекватной оценки степени их общественной опасности. В свою очередь, иерархия ценностей охраняемых общественных отношений, образующих родовой и непосредственный объект посягательства, детерминирована уголовной политикой государства и получает легальное выражение в нормах, закрепляющих задачи уголовного законодательства (ч. 1 ст. 2 УК РФ).

В доктрине уголовного права отсутствует единая позиция относительно определения родового (типового) объекта преступлений, объединенных в разделе VIII Особенной части УК РФ («Преступления в сфере экономики»). Анализ научных воззрений позволяет выявить ряд теоретических подходов. Так, одна группа ученых (Л.Д. Гаухман, С.В. Максимов, Л.М. Колодкин) определяет данный объект через категорию общественных отношений, обеспечивающих законные права различных субъектов в экономической сфере[2].

---

[1] Пионтковский А. А. Учение о преступлении по советскому уголовному праву. Курс советского уголовного права: Общая часть. М., 1961. С. 137.

[2] Уголовное право. Часть Общая. Часть Особенная. Учебник / Под общей ред. Л.Д. Гаухмана, Л.М. Колодкина и С.В. Максимова. М., 1999. С 384.

Иной подход демонстрирует С.М. Кочои, который в качестве непосредственного содержания типового объекта выделяет конкретные социальные блага: собственность, порядок осуществления экономической деятельности, интересы службы в коммерческих и иных организациях[1].

Особого внимания заслуживает критическая позиция С.А. Елисеева, указывающего, что преступления против собственности не ограничиваются экономической сферой в узком смысле, а могут совершаться и в частно-гражданской сфере, что ставит под вопрос универсальность предлагаемых дефиниций[2].

Мы же придерживаемся позиции Н.А. Лопашенко, в соответствии с которой одним из ключевых системообразующих критериев для объединения рассматриваемых преступлений в единый раздел выступает факт их совершения в экономической сфере и причинения ей имущественного ущерба[3]. Данный подход представляется наиболее последовательным и методологически верным.

Видовым объектом данного преступления являются отношения собственности, что непосредственно вытекает из наименования Главы 21 УК РФ «Преступления против собственности».

Непосредственный объект хищений путем использования информационных технологий – это конкретная форма собственности (государственная, частная, муниципальная), к которой относится похищаемое имущество. В доктрине дискутируется вопрос о сложной структуре непосредственного объекта. Так, В.М. Елин в качестве такового признает чужое имущество или право на него, что представляется спорным, поскольку ведет к овеществлению объекта уголовно-правовой охраны[4]. Более обоснованной

---

[1] Кочои С.М. Ответственность за корыстные преступления против собственности: Учебно-практическое пособие. М., 2010. С. 81.

[2]Елисеев С.А. Преступления против собственности: курс лекций. Томск: Издательский Дом Томского государственного университета, 2023. С. 81–86.

[3] Лопашенко Н. А. Посягательства на собственность: монография. М., 2022. С. 11–13.

[4] Елин В. М. Мошенничество в сфере компьютерной информации как новый состав преступления // Бизнесинформатика. № 2 (24). 2020. С. 71.

является позиция, разделяемая большинством ученых, согласно которой анализируемое преступление является двухобъектным[1]. Его основным непосредственным объектом выступают отношения собственности, а дополнительным (факультативным) – отношения в сфере безопасности компьютерной информации, охраняемые главой 28 УК РФ. С данной позицией следует согласиться, поскольку сам способ хищения неразрывно связан с противоправным воздействием на информационные системы и сети.

Особого внимания заслуживает вопрос о предмете хищения. Традиционно в качестве такового признается чужое имущество, обладающее физическим, экономическим и юридическим свойствами. Однако развитие цифровой экономики и системы безналичных расчетов обусловило необходимость признания предметом хищения безналичных и электронных денежных средств, которые, не обладая вещественной формой, имеют явную экономическую ценность. Диспозиция ст. 159.6 УК РФ прямо указывает, что предметом мошенничества в сфере компьютерной информации может быть как чужое имущество, так и право на чужое имущество. Под «правом на имущество» в уголовно-правовом контексте следует понимать имущественные права, удостоверяющие возможность владения, пользования и распоряжения определенными благами, а не право собственности в полном объеме.

Современные реалии выводят на первый план в качестве предмета хищения цифровые финансовые активы, в частности, криптовалюту (цифровые знаки, токены). Несмотря на отсутствие на текущий момент их прямой легализации в Российской Федерации, криптовалюты обладают экономической ценностью, могут быть объектом гражданского оборота (в качестве «цифровых прав» по ст. 128 ГК РФ)[2] и, следовательно, не должны исключаться из сферы уголовно-правовой охраны. Обладая реальной экономической ценностью и

---

[1] Сафонов О.М. Уголовно-правовая оценка использования компьютерных технологий при совершении преступлений: состояние законодательства и правоприменительной практики, перспективы совершенствования: дис. … канд. юрид. наук. М., 2015. С. 115–116.

[2] Гражданский кодекс Российской Федерации: федер. закон Рос. Федерации от 30ноября1994 г. № 51-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 21окт. 1994 г.// Рос. газ. – 1994. – 8декабря.

способностью к обмену на фиатные деньги, биткоины и иные аналогичные активы не должны быть исключены из сферы гражданского оборота. Это же свойство – имущественная ценность – делает их потенциальным предметом хищения, что обуславливает необходимость их уголовно-правовой защиты.

Курс на легализацию цифровых денег подтверждается и наднациональными инициативами. Так, Евразийская экономическая комиссия еще в 2018 г. рассматривала возможность создания общей евразийской криптовалюты. Планировалось, что ее использование в совместных инвестиционных проектах поможет устранить барьеры между национальными финансовыми системами и повысить их эффективность. Развитие цифровых инвестиционных инструментов открывает значительные перспективы для финансирования инноваций в странах ЕАЭС, а интеграцию финансовых рынков целесообразно начинать именно с их инновационного сегмента, чтобы предотвратить появление новых, цифровых барьеров[1].

Социально-экономический потенциал этой технологии огромен. Даже если текущие лидеры, такие как Биткоин, уступят место более совершенным системам, базовые принципы блокчейна продолжат трансформировать платежную среду. Пытаться сдержать этот процесс ограничительным законодательством – значит рисковать проиграть в глобальной конкурентной борьбе на технологическом рынке. История показывает, что рестриктивные нормы недолговечны в противостоянии с динамично развивающимися информационными технологиями.

Неотложность правового регулирования криптовалют и квалификации киберпреступлений подчеркивается растущим числом злоупотреблений в этой сфере. Сегодня цифровыми активами интересуются не только добросовестные инвесторы, но и преступники.

Таким образом, назрела объективная потребность в четком определении правового статуса цифровых финансовых активов и их защите. Предметом

---

[1] Международный семинар: «Блокчейн и криптовалюты: каналы влияния на макроэкономическую политику в евразийском регионе». [Электронный ресурс]. URL: http://www.eurasiancommission.org/ru. (дата обращения: 25.11.2025).

хищения путем использования компьютерной информации, наравне с безналичными и электронными денежными средствами, должны признаваться криптовалюта и криптотокены. Это не только защитит права владельцев, но и создаст правовые условия для развития цифровой экономики.

Объективная сторона преступления представляет собой совокупность признаков, предусмотренных уголовным законом, обуславливающих внешнее проявление общественно опасного деяния, его последствия и причинно-следственную связь между ними. Для хищений, совершаемых с использованием информационных, признаки объективной стороны признаются основными критериями отграничения деяния от другого противоправного поведения традиционных форм хищения.

Так, согласно диспозиции ч. 1 ст. 159.6 УК РФ, объективная сторона характеризуется активными действиями, направленными на изъятие чужого имущества или приобретение права на него специфическим способом – путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Ключевая особенность – это отсутствие характерных для традиционного мошенничества (ст. 159 УК РФ) признаков – обман и злоупотребление доверием. При этом вместо них законодательный акцент сделан на активные неправомерные действия с компьютерной информацией или воздействие на программно-аппаратную среду. Это позволяет сделать вывод, что ст. 159.6 УК РФ устанавливает ответственность за самостоятельную форму хищения, где способом изъятия имущества признается не введение в заблуждение человека, а несанкционированное манипулирование информацией в цифровом пространстве. При этом следует указать: под вводом компьютерной информации понимается внесение в систему ранее отсутствовавших сведений, в том числе ложных, которые инициируют перевод денежных средств или изменение имущественных прав;удаление – это прекращение существования информации;блокирование – это ограничение или

прекращение доступа к компьютерной информации без ее уничтожения; под модификацией понимается любое изменение информации, не связанное с ее удалением или блокированием (например, изменение реквизитов получателя платежа). Что касается иного вмешательства в функционирование средств хранения, обработки или передачи, то здесь важно отметь, что оно представлет оценочное понятие, охватывающее любые действия, нарушающие нормальную работу компьютерных систем и сетей (например, DDoS-атаки, подмена сетевого адреса).

Российский законодательпредусмотрел более широкий и технологически ориентированный перечень способов, что, с одной стороны, позволяет охватить разнообразные схемы противоправной деятельности, а с другой – порождает проблемы правоприменения ввиду отсутствия законодательных дефиниций таких понятий, как «ввод», «удаление», «иное вмешательство».

Момент окончания данного преступления является материальным и, согласно сложившейся судебной практике, связывается с зачислением безналичных или электронных денежных средств на счет виновного либо на счета третьих лиц[1]. Именно с этого момента собственнику причиняется реальный имущественный ущерб, и виновный получает реальную возможность распоряжаться похищенным. Такой подход является верным, поскольку изъятие имущества в цифровой форме происходит практически мгновенно в момент проведения транзакции.

Проведенное исследование объективных признаков хищений, совершаемых с использованием информационных технологий, позволяет констатировать наличие системных проблем в их уголовно-правовой регламентации. В работе установлено, что существующая законодательная конструкция не в полной мере соответствует реалиям цифровой экономики, что создает коллизии в правоприменительной практике.

---

[1] О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 (ред. от 15.12.2022) // Российская газета. – 2017. – № 280.

В качестве ключевого противоречия выделяется несоответствие между фактическим содержанием ст. 159.6 УК РФ, не предусматривающей обман или злоупотребление доверием в качестве конструктивного признака, и ее наименованием, использующим термин «мошенничество». Это приводит к терминологической путанице и нарушает принципы законности и равенства граждан перед законом, поскольку квалификация начинает зависеть не от сути преступных действий, а от формы похищаемых активов (наличные, безналичные или электронные денежные средства).

Сложившаяся ситуация свидетельствует о том, что существующая система составов преступлений против собственности в гл. 21 УК РФ нуждается в дальнейшем совершенствовании. Наиболее целесообразным и логичным шагом по ее оптимизации представляется выделение хищения, совершаемого путем использования информационных технологий, в самостоятельный состав преступления. Это позволит унифицировать квалификацию, устранить имеющиеся правовые пробелы и создать адекватный механизм защиты всего спектра имущественных отношений, включая новые цифровые финансовые активы, в условиях стремительного развития информационного общества.

§ 2. Субъективные признаки хищения путем использования информационных технологий

Субъективная составляющая преступления, будучи неотъемлемым элементом состава, характеризует внутреннее, психическое отношение лица к совершаемому общественно опасному деянию и его последствиям. Применительно к хищениям с использованием информационных технологий анализ субъективных признаков приобретает особую актуальность в связи со спецификой механизма совершения преступления и личностью виновного[1].

[1]Дайшутов М.М., Динека В.И. Признаки субъекта преступления и его правовые критерии // Вестник Московского университета МВД России. 2018. № 6. С. 130.

В соответствии с диспозицией ст. 159.6 УК РФ, субъектом хищения путем использования информационных технологий является физическое, вменяемое лицо, достигшее шестнадцатилетнего возраста. Указанный возрастной порог, установленный российским законодателем, дифференцирован от общего возраста привлечения к уголовной ответственности и обусловлен сложностью и интеллектуальной составляющей данного деяния, требующей, по мнению законодателя, более высокого уровня осознания. Вменяемость как обязательный признак субъекта предполагает, что лицо во время совершения преступления было способно осознавать фактический характер и общественную опасность своих действий и руководить ими. Следует особо подчеркнуть, что субъект преступления, предусмотренного ч. 3 ст. 159.6 УК РФ (квалифицированный состав), является специальным, поскольку предполагает совершение деяния лицом с использованием своего служебного положения.

Помимо субъекта преступного деяния важно также рассмотреть сущность субъективной стороны, поскольку она признается выражением психического отношения лица к совершенному преступлению, а также наступившими последствиями, виной, мотивом и целью.

Субъективная сторона рассматриваемого преступления характеризуется виной в форме умысла. Вместе с тем в доктрине уголовного права отсутствует консенсус относительно конкретной разновидности умысла, присущего данному деянию. Преобладающей является точка зрения, согласно которой подобные преступные посягательства могут быть совершены исключительно с прямым умыслом. Однако высказываются и иные научные позиции, в частности, представленная М.Ю. Дворецким, который полагает, что, относясь к категории умышленных преступлений, хищение, предусмотренное ст. 159.6 УК РФ, может быть осуществлено как с прямым, так и с косвенным умыслом[1].

[1]Замалеева С.В. О некоторых проблемах квалификации мошенничества в сфере компьютерной информации // Право и государство: теория и практика. 2022. №7 (211). С. 133.

В свете обозначенной дискуссии представляется методологически верным сослаться на позицию А.И. Рарога, критически оценивающего расширительный подход к виду умысла. Ученый обоснованно указывает, что допущение возможности совершения преступления с косвенным умыслом зачастую является следствием механического, некритического применения законодательной конструкции умысла, разработанной для преступлений с материальным составом, без учета специфики конкретного деяния[1].

Также следует отметить, что прямой вид умысла характеризуется обязательными структурными элементами: интеллектуальным и волевым моментом, относящимся к психической деятельности субъекта преступления.

Интеллектуальный момент прямого умысла включает осознание:

1. Общественной опасности своих действий, направленных на нарушение конфиденциальности, целостности или доступности компьютерной информации;

2. Того, что эти действия являются способом завладения чужим имуществом или правом на него;

3. Фактического содержания и социального значения совершаемых операций с информационными системами[2].

Волевой момент выражается в целенаправленных действиях виновного, направленных на достижение преступного результата – незаконного извлечения имущественной выгоды.

Таким образом, виновное лицо осознает, что путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи информации обращает чужое имущество в свою пользу или пользу третьих лиц, предвидит неизбежность наступления общественно опасных последствий в

---

[1]Бавсун М.В. Квалификация преступлений по признакам субъективной стороны: учебник для вузов. 2-е изд., испр. и доп. М.,Юрайт, 2025. С. 77.

[2]Медведев Е.В. Уголовное право России. Общая часть : учебник для вузов. 2-е изд., перераб. и доп. М., Юрайт, 2025. С. 79.

виде причинения имущественного ущерба собственнику и желает их наступления.

Обязательным признаком субъективной стороны также является корыстная цель. Содержательно она представляет собой стремление виновного обратить чужое имущество в свою пользу или в пользу других лиц. В научной и судебной практике корыстная цель трактуется широко: она присутствует не только тогда, когда преступник обогащается лично, но и когда он действует в интересах иных лиц (близких, знакомых или даже незнакомых, в благополучии которых он заинтересован по любым мотивам – симпатии, состраданию и т.д.). Как верно отмечено в п. 26 Постановления Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48, корыстная цель заключается в стремлении распорядиться похищенным имуществом как своим собственным[1]. Следовательно, даже если мотивация виновного включала элементы «альтруизма» (например, хищение средств для помощи больным детям), это не исключает наличия корыстной цели, поскольку изъятие и обращение чужого имущества осуществляется вопреки воле собственника. На что обращает свое внимание и С.А. Петров, утверждающий, что корыстная цель не исключается даже в тех случаях, когда лицо стремиться к улучшению благосостояния третьего лица[2].

Таким образом, субъективные признаки хищения путем использования информационных технологий, будучи в целом традиционными для хищений (прямой умысел, корыстная цель, общие и специальные признаки субъекта), наполняются специфическим содержанием, обусловленным цифровой средой совершения преступления и современным портретом личности киберпреступника, что должно учитываться как при квалификации деяний, так и в правоприменительной практике.

---

[1]О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 (ред. от 15.12.2022) // Российская газета. – 2017. – № 280.

[2] Петров С.А. Хищение чужого имущества или приобретение права на него путем обмана: уголовно-правовая оценка и совершенствование правовой регламентации: автореф. дис. … канд. юрид. наук. М., 2015. С. 26

§ 3. Квалифицирующие и особо квалифицирующие признаки хищения путем использования информационных технологий

Квалифицированные виды хищения, совершаемые с использованием информационных технологий, по уголовному законодательству Российской Федерации – это признаки, существующие помимо признаков основного состава. Главным критерием выделения квалифицирующих и особо квалифицирующих признаков является повышенная степень общественной опасности.

Так, в соответствии с ч. 2 ст. 159.6 УК РФ законодатель предусмотрел следующие квалифицирующие признаки:

1. Совершение преступления группой лиц по предварительному сговору;
2. Причинение значительного ущерба гражданину.

Понятие «группа лиц по предварительному сговору», как и признак «причинение значительного ущерба гражданину», закреплено в УК РФ. Согласно ч. 2 ст. 35 УК РФ, преступление признается совершенным группой лиц по предварительному сговору, если в нем участвовали лица, заранее договорившиеся о совместном совершении преступления. Общепризнанным является толкование, согласно которому для наличия этого признака необходимо установить двух или более исполнителей.

Изучение 52 материалов уголовных дел по данным видам хищений показало, что существенных проблем при установлении квалифицирующего признака, предусмотренного ч. 2 ст. 159.6 УК РФ, не возникает. В мотивировочной части решений суды раскрывают содержание этого признака, указывая, что действия виновных лиц согласованы, взаимосвязаны и направлены на достижение общего результата – завладения имуществом, при этом каждый выполняет отведенную ему роль.

Пример из практики: так, в 2023 году гражданин М.Р.Р., используя мессенджер Telegram, приобрел у неустановленного лица взломанную учетную запись гражданина В.А.Н. на портале «Госуслуги». Получив доступ к

персональным данным, М.Р.Р. подал от имени В.А.Н. заявку на потребительский займ в МФК «Триумвират» на сумму 5 000 рублей. Для этого он модифицировал компьютерную информацию в личном кабинете, указав реквизиты подконтрольной банковской карты. После одобрения займа деньги были перечислены на карту сообщника, который перевел большую часть средств М.Р.Р.

Действия М.Р.Р. были квалифицированы по ч. 1 ст. 159.6 УК РФ как мошенничество в сфере компьютерной информации, то есть хищение чужого имущества путем ввода и модификации компьютерной информации. Дополнительно его действия подпадали под ст. 272 УК РФ (неправомерный доступ к компьютерной информации)[1].

На основании изложенного можно выделить следующие критерии установления квалифицирующего признака «группа лиц по предварительному сговору»:

1. Участие не менее двух лиц, подлежащих уголовной ответственности. Согласно ч. 1 ст. 35 УК РФ, для признания преступления совершенным группой лиц требуется участие в нем не менее двух исполнителей. Участие в хищении лиц, не подлежащих уголовной ответственности (в силу возраста или невменяемости), исключает квалификацию деяния по признаку совершения группой лиц по предварительному сговору, хотя эти лица могут непосредственно причинять преступный вред.

В науке существует иная точка зрения. Так, некоторые авторы полагают, что состав участников группы могут образовывать и лица, не являющиеся субъектами преступления, но фактически выполняющие часть объективной стороны[2]. Суть этой позиции заключается в том, что совместно с субъектом преступления может действовать иное лицо, непосредственно участвующее в посягательстве. Это требует законодательной инициативы по признанию такого

---

[1]Приговор Новолакского районного суда Республики Дагестан от 13 апреля 2023 г. по делу № 1-26/2023: [электронный ресурс] // Судебные и нормативные акты РФ (СудАкт). – URL: https://sudact.ru/ (дата обращения: 08.12.2025).

[2]Кузнецова М.Д. Мошенничество в уголовно-правовом исследовании // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2024. №2 (66). С. 162.

лица соучастником, что позволило бы применить к нему уголовное наказание, а в отношении субъекта преступления установить отягчающие признаки.

Ю.Е. Пудовочкин предложил рассматривать субъекта как в статусе исполнителя, так и посредственного причинителя, несущего ответственность и за действия, совершенные лицом не являющимся субъектом, что может быть основанием для признания соучастия[1].

По мнению автора, такое понимание группового способа совершения преступления является спорным, поскольку в российской уголовно-правовой теории соучастники должны обладать всеми признаками субъекта преступления. Более обоснованным представляется законодательное решение данной проблемы путем самостоятельного определения в институте соучастия совершения преступления совместно с субъектом в качестве квалифицирующего признака.

2. Наличие предварительного сговора, достигнутого до начала выполнения объективной стороны преступления, включая стадию приготовления. Если договоренность возникла в момент совершения деяния, сговор не считается предварительным.

Групповой характер будет присутствовать, когда один из соисполнителей выполняет часть действий, описанных в диспозиции ст. 159.6 УК РФ (например, блокирование информации), а другой выполняет иные действия, без которых совершение преступления невозможно (например, модификацию или удаление информации), поскольку все они входят в объективную сторону преступления.

Сложным является вопрос о наличии данного признака, когда один соучастник совершает неправомерные действия с компьютерной информацией, а другой осуществляет манипуляции по перечислению средств и их обналичиванию, причем его действия формально не входят в объективную сторону ст. 159.6 УК РФ.

---

[1]Пудовочкин Ю.Е. Судебная практика квалификации преступлений, совершенных в соучастии //Криминологический журнал БГУЭП. 2021. №2 (16). С. 7.

Во-первых, изъятие безналичных средств со счета потерпевшего является оконченным хищением. Последующий вывод средств представляет собой форму распоряжения похищенным. Поэтому действия лица, намеревавшегося лишь участвовать в обналичивании, следует квалифицировать как пособничество, что исключает вменение признака «группа лиц по предварительному сговору» (как квалифицирующего признака соисполнительства).

Во-вторых, согласно п. 10 ПостановленияПленума Верховного Суда Российской Федерации от 27 декабря 2002 г. № 29 «О судебной практике по делам о краже, грабеже и разбое», если другие участники в соответствии с распределением ролей совершили согласованные действия, направленные на оказание непосредственного содействия исполнителю, содеянное ими является соисполнительством и не требует дополнительной квалификации по ст. 33 УК РФ[1].

Таким образом, правоприменительная практика исходит из того, что лица, совершившие действия, составляющие объективную сторону компьютерного мошенничества, являются соисполнителями независимо от участия в непосредственном изъятии средств со счета.

3. Действия каждого участника содержат признаки объективной и субъективной стороны данного преступления.Объективная сторона хищения при совершении группой лиц по предварительному сговору имеет особенность, когда сговор достигается дистанционно, через интернет. Присоединение одного лица к начатому другим лицу преступному посягательству, входящему в объективную сторону ст. 159.6 УК РФ, следует квалифицировать как совершение преступления группой лиц по предварительному сговору. Например, если преступник, не сумев получить доступ к сети, приостанавливает свои действия и находит соисполнителя для доведения замысла до конца.

---

[1]О судебной практике по делам о краже, грабеже и разбое: постановление Пленума Верховного Суда Российской Федерации от 27 декабря 2002 г. № 29 (ред. от 15.12.2022) // Российская газета. – 2002. – № 280.

Рассмотрим также квалифицирующий признак «причинение значительного ущерба гражданину».Значительный ущерб определяется с учетом имущественного положения потерпевшего и не может составлять менее пяти тысяч рублей (примечание к ст. 158 УК РФ). В теории выделяют объективный критерий (стоимость похищенного, финансовое положение потерпевшего) и субъективный критерий (осознание виновным значительности ущерба)[1].

Правоприменительная практика показывает, что установление данного признака осуществляется путем сложения сумм при совершении ряда тождественных преступлений. Признак является оценочным, но верхний предел, как правило, не превышает 250 000 рублей.

М.И. Третьяк отмечает, что при определении признака следует исходить из принципа субъективного вменения: даже если потерпевшему причинен значительный ущерб, но виновный не мог этого осознавать, хищение не может быть квалифицировано по этому признаку[2]. Это предложение заслуживает внимания, однако его применение на практике проблематично, так как преступник часто не обладает информацией об имущественном положении потерпевшего, а его умысел может быть неопределенным. Требовать обязательного осознания точного размера ущерба спорно.

В целях унификации и независимости от инфляции автор считает целесообразнымзакрепить в примечании к ст. 158 УК РФ фиксированную базовую величину, что в свою очередь сделает независимым данный критерий исчисления от социально-экономических и политических преобразований, а также не будет необходимости вносить корректировки размеров ущерба в федеральные законы.

Согласно п. 31 Постановления Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 «О судебной практике по делам о

---

[1]Гаухман Л.Д. Квалификация преступлений: закон, теория, практика. 8-е изд., перераб. и дополн. М., 2021.С. 378.

[2] Третьяк М.И. Мошенничество как преступление против собственности в современном уголовном праве:курс лекций. М., Юрлитинформ, 2023. С. 101.

мошенничестве, присвоении и растрате», при решении вопроса о значительном ущербе суды должны учитывать имущественное положение потерпевшего. Мнение потерпевшего оценивается в совокупности с другими материалами дела[1].

Далее рассмотрим особо квалифицирующие признаки, предусмотренные ч. 3 и ч. 4 ст. 159.6 УК РФ.

1. Крупный размер (ч. 3 ст. 159.6 УК РФ).Согласно примечанию к ст. 158 УК РФ, крупным размером признается стоимость имущества, превышающая 250 000 рублей. Это традиционный и хорошо изученный признак. Дифференциация ответственности в зависимости от размера причиненного ущерба для преступлений против собственности общепризнанна. Однако при хищении безналичных средств сумма, полученная преступником, может быть меньше из-за комиссий банка. Этот факт не должен влиять на квалификацию, так как размер ущерба определяется суммой, списанной со счета потерпевшего.

Федеральным законом от 23.04.2018 № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» в ч. 3 ст. 159.6 УК РФ был введен особо квалифицирующий признак «с банковского счета, а равно в отношении электронных денежных средств»[2]. По мнению автора, при введении этой нормы не в полной мере были учтены критерии дифференциации ответственности. Поскольку большинство компьютерных мошенничеств по своей цифровой природе направлено на безналичные или электронные средства, данный признак фактически становится основным, а предшествующие квалифицирующие признаки используются редко. Е.А. Русскевич справедливо отмечает, что это привело к тому, что ч. 3 ст. 159.6 УК РФ стала основным

---

[1]О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 (ред. от 15.12.2022) // Российская газета. – 2017. – № 280.

[2] О внесении изменений в Уголовный кодекс Российской Федерации: федер. закон Рос. Федерации от 23 апреля 2018 г. № 111-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 10 апр. 2018 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 18 апр. 2018 г. // Рос. газ. – 2018. – 25 апреля.

составом, нивелировав части 1 и 2. Автор полагает, что данный признак целесообразно исключить из ч. 3 ст. 159.6 УК РФ[1].

2. Совершение организованной группой или в особо крупном размере (ч. 4 ст. 159.6 УК РФ).

Организованная группа – наиболее опасная форма соучастия. Согласно ч. 3 ст. 35 УК РФ, это устойчивая группа лиц, заранее объединившихся для совершения одного или нескольких преступлений. И. Сироткин указывает, что каждый участник организованной группы должен признаваться соисполнителем независимо от роли[2]. Общественная опасность таких хищений состоит в долгосрочной мотивации участников.Согласно п. 15 Постановления Пленума Верховного Суда Российской Федерации от 27.12.2002 № 29 «О судебной практике по делам о краже, грабеже и разбое», об устойчивости могут свидетельствовать наличие организатора, предварительный план, стабильность состава, распределение ролей, длительность подготовки, техническая оснащенность[3]. Эти признаки являются конститутивными для квалификации по ч. 4 ст. 159.6 УК РФ. На практике наибольшую сложность вызывает установление именно признака устойчивости.

Особо крупный размер. В соответствии с примечанием к ст. 158 УК РФ, особо крупным размером признается стоимость имущества, превышающая 1 миллион рублей. Введение этого признака соответствует доктрине дифференциации ответственности.

Немаловажным остается аспект, касающийся определения размера ущерба. Согласно п.п. 31, 33 Постановления Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», для исчисления значительного

---

[1]Русскевич Е.А. Новые нормы УК об «электронном» мошенничестве и коррупционных преступлениях // Уголовный процесс. 2018. № 7. С. 32.

[2] Сироткин И. Ответственность участников организованных групп и преступных организаций // Законность. 2019. № 10. С. 38.

[3]О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 (ред. от 15.12.2022) // Российская газета. – 2017. – № 280.

ущерба следует обращаться к примечанию 2 к ст. 158 УК РФ (не менее 5 000 руб.), а для исчисления крупного и особо крупного размера – к примечанию к ст. 159.1 УК РФ (свыше 1 500 000 руб. и 6 000 000 руб. соответственно). Эта позиция неудачна из-за отсутствия в ст. 159.6 УК РФ единых стоимостных критериев. Обращение к разным статьям является вынужденным применением закона по аналогии, что прямо запрещено ч. 2 ст. 3 УК РФ. Устранение этого пробела – прерогатива законодателя.

По мнению автора, для единообразия в примечании к ст. 158 УК РФ необходимо установить единые стоимостные пороги для всех форм хищения, включая мошенничество в сфере компьютерной информации. Также в диспозиции ст. 159.6 УК РФ следует использовать единый термин – «размер» ущерба. В сложных случаях для определения размера ущерба требуется назначение экономической экспертизы[1].

Проведенный анализ квалифицирующих и особо квалифицирующих признаков мошенничества в сфере компьютерной информации (ст. 159.6 УК РФ) позволяет сформулировать следующие выводы.

Квалифицирующие признаки данного состава (совершение группой лиц по предварительному сговору и причинение значительного ущерба гражданину) соответствуют традиционной системе дифференциации ответственности за имущественные преступления и направлены на учет повышенной общественной опасности деяния. Их установление в правоприменительной практике в целом не вызывает непреодолимых сложностей, однако требует тщательной оценки характера совместных действий виновных и индивидуальной имущественной ситуации потерпевшего.

Признак «группа лиц по предварительному сговору» формируется на основе устоявшихся в теории и практике критериев: участие не менее двух исполнителей, наличие сговора до начала исполнения объективной стороны и выполнение каждым соисполнителем действий, входящих в эту объективную

[1]Майстренко Г.А. К вопросу о необходимости пересмотра понятий «крупный ущерб», «особо крупный ущерб» в уголовном законодательстве России // Образование и право. 2022. № 3. С. 280.

сторону. Современные технологии дистанционного взаимодействия не меняют сущности данного признака, но актуализируют вопросы доказывания факта предварительной договоренности и согласованности ролей.

Признак «причинение значительного ущерба гражданину», будучи оценочным, вызывает дискуссии относительно необходимости учета субъективного восприятия размера ущерба виновным. Представляется, что для обеспечения единообразия судебной практики и независимости от инфляции целесообразно законодательно закрепить фиксированную базовую величину значительного ущерба в примечании к ст. 158 УК РФ.

Особо квалифицирующие признаки (крупный и особо крупный размер, совершение организованной группой) отражают высшую степень общественной опасности компьютерного мошенничества. Вместе с тем действующая законодательная конструкция содержит системные недостатки: введение специального признака «с банковского счета, а равно в отношении электронных денежных средств» (ч. 3 ст. 159.6 УК РФ) нивелирует значение основного и квалифицированного составов, а отсутствие единых стоимостных критериев для определения размера ущерба в рамках одной статьи (ст. 159.6 УК РФ) создает правовую неопределенность и вынуждает правоприменителя к недопустимой аналогии закона.

Таким образом, квалифицированные виды хищения, совершаемые с использованием информационных технологий, сохраняют классическую для имущественных преступлений структуру отягчающих признаков, но требуют адаптации подходов к их установлению в цифровой среде и неотложного законодательного устранения внутренних противоречий в системе стоимостных критериев для обеспечения принципа правовой определенности и эффективной дифференциации уголовной ответственности.

ГЛАВА 3. СОВЕРШЕНСТВОВАНИЕ УГОЛОВНОГО ЗАКОНОДАТЕЛЬСТВА, ПРЕДУСМАТРИВАЮЩЕГО ОТВЕТСТВЕННОСТЬ ЗА ХИЩЕНИЯ ПУТЕМ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, И ПРАКТИКА ЕГО ПРИМЕНЕНИЯ

§ 1. Проблемы квалификации хищений, совершаемых с использованием информационных технологий, в уголовном праве Российской Федерации

В современную эпоху, когда цифровизация пронизывает все сферы жизни общества и государства, мы сталкиваемся с парадоксальным явлением: технологический прогресс, наряду с колоссальными преимуществами, порождает новые, изощренные формы противоправной деятельности. Криминальный мир стремительно мигрирует в цифровое пространство, активно используя информационно-телекоммуникационные сети для совершения преступлений. В ответ на этот вызов одной из ключевых задач государства становится эффективное противодействие так называемым «киберпреступлениям». Однако сам этот термин, несмотря на его широкое употребление, не имеет законодательного закрепления в Российской Федерации, что уже создает концептуальные трудности. В научном сообществе можно наблюдать спектр мнений: от узкого понимания киберпреступления как акта, непосредственно направленного против компьютерных систем или данных[1], до максимально широкой трактовки, включающей любую противоправную деятельность, где ИТ-технологии выступают инструментом или средой. На практике чаще сталкиваемся со вторым подходом: киберпреступление – это любое противоправное деяние, совершаемое с

[1]Долотова Н.П. Киберпреступность в банковской сфере в Российской Федерации // Гуманитарные, социально-экономические и общественные науки. 2024. №12. С. 216.

использованием компьютеров или сети Интернет, от сравнительно малозначительных правонарушений до тяжких преступлений[1].

К наиболее распространенным видам таких преступлений сегодня относятся: хищение личных данных (взлом аккаунтов, фишинг, кража финансовой информации); финансовые махинации (мошенничество с банковскими картами, кибервымогательство, отмывание денег); создание и распространение вредоносного программного обеспечения; атаки на критическую инфраструктуру (кибертерроризм); нарушение авторских прав в цифровой форме; использование интернета для торговли людьми[2]. Эти деяния обладают рядом специфических признаков. Во-первых, их средством или орудием всегда выступают компьютеры, сети, специальное ПО. Во-вторых, они посягают на двойной объект: непосредственно на безопасность компьютерной информации и на смежное право, например, собственность. В-третьих, для их совершения необходимы специальные познания в ИТ-сфере. В-четвертых, они всегда носят умышленный и целенаправленный характер.

Статистика красноречиво свидетельствует о масштабе проблемы. Так, в 2021 году было зарегистрировано 517 722 преступления с использованием ИТ, в 2022 – 510 143, а в 2023 году этот показатель резко вырос до 676 951, в 2024 г. показатель достиг 765 365 преступлений. Особенно тревожен рост хищений: если в 2021 году против собственности было совершено 156 792 таких преступления, то в 2023 – уже 356 079, а в 2024 – 445 690. Эта тревожная динамика делает критически важным точное и единообразное применение уголовного закона, в частности, правильную квалификацию хищений, совершаемых в цифровой среде[3].

---

[1]Головинов, О.Н., Погорелов, А.В. Киберпреступность в современной экономике: состояние и тенденции развития // Вопросы инновационной экономики. 2020. №6(1). С. 74.

[2]НурмухаметовР.Н. К вопросу о проблемах квалификации хищений, совершенных с применением информационных технологий // Международный журнал гуманитарных и естественных наук. 2024. №12-1 (99). С. 181.

[3]Министерство внутренних дел Российской Федерации. Краткая характеристика состояния преступности за январь-декабрь 2021 г., за январь-декабрь 2022 г., за январь-декабрь 2023 г., за январь-декабрь 2024 г. [Электронный ресурс]. URL: https://xn--b1aew.xn--p1ai/reports/item/47055751/ (датаобращения: 25.11.2025).

Именно здесь возникает основная правовая коллизия. На практике суды демонстрируют диаметрально противоположные подходы к квалификации, по сути, однотипных действий. Анализ судебных решений позволяет выделить несколько характерных сценариев, которые наглядно иллюстрируют проблему.

1. Хищение путем внедрения вредоносной программы. Так, гражданин М., используя вредоносное ПО, несанкционированно подключился к банковскому счету потерпевшего К. в системе «Мобильный банк» и перевел 54 000 рублей на свой электронный кошелек. Суд квалифицировал его действия по п. «в» ч. 2 ст. 158 УК РФ как кражу. Однако, согласно разъяснениям Пленума Верховного Суда РФ (п. 16 Постановления № 37 от 15.12.2022), если мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ) совершено посредством использования вредоносных программ, оно требует дополнительной квалификации по ст. 273 УК РФ[1]. Таким образом, более точной в данном случае была бы квалификация по ч. 2 ст. 159.6 и ч. 1 ст. 273 УК РФ, так как виновный не просто тайно похитил деньги, а совершил это путем вмешательства в работу компьютерной системы с помощью специального инструмента – вредоносной программы[2].

2. Хищение с использованием сохраненных банковских реквизитов. С. совершил хищение 20 153 рублей со счета А., используя реквизиты карты, которые он переписал ранее. Суд Владивостока квалифицировал это как мошенничество в сфере компьютерной информации (п. «в» ч. 3 ст. 159.6 УК РФ). Это классическая ошибка. Пленум ВС РФ (п. 21 Постановления №48 от 30.11.2017) прямо указывает: если хищение совершено путем использования учетных данных (паролей, реквизитов) без оказания воздействия на ПО или сети, то это – кража (ст. 158 УК РФ). Здесь отсутствует признак «обмана»

---

[1]О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» : постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37 // Бюллетень Верховного Суда РФ. – 2023. – № 3.

[2]Приговор Братского городского суда Иркутской области от 19 декабря 2020 г. по делу № 1-558/2020: [электронный ресурс] // Судебные и нормативные акты РФ (СудАкт). – URL: https://sudact.ru/ (дата обращения: 10.12.2025).

системы, имеет место лишь тайное использование чужого цифрового ключа, аналогичного связке физических ключей[1].

3. Хищение с купленного телефона, где остались данные «Мобильного банка».

Р., купив телефон, использовал оставшиеся в нем сохраненные данные для доступа к банковскому счету прежнего владельца и перевел 15 700 рублей. Суд квалифицировал действия по ст. 159.6 УК РФ. Это снова неверно. Использование данных, к которым виновный получил доступ законным способом (покупка устройства), но без права распоряжаться привязанными к ним финансовыми ресурсами, – это типичная кража (ст. 158 УК РФ). Обмана или взлома системы не было[2].

4. Классическое мошенничество в сети. Г. разместил на сайте объявление о продаже несуществующего телефона по низкой цене и, вступив в переписку, убедил потерпевшего перевести ему 18 000 рублей на электронный кошелек. Буденновский суд верно квалифицировал это по ст. 159 УК РФ как мошенничество. Здесь присутствует ключевой элемент – обман человека: злоумышленник распространяет заведомо ложные сведения (о наличии товара) через интернет, что вводит потерпевшего в заблуждение и побуждает его добровольно передать деньги[3].

5. Хищение посредством программы несанкционированного доступа. Добровольский В. приобрел специализированную программу для взлома, с ее помощью получил доступ к компьютеру потерпевшего, скопировал банковские учетные данные и перевел 55 800 рублей. Суд применил только ст. 159.6 УК РФ. Однако, следуя уже упомянутым разъяснениям Пленума ВС РФ, такие действия

---

[1]Приговор Советского районного суда г. Владивостока от 15 мая 2021 г. по делу № 1-718/2021: [электронный ресурс] // Судебные и нормативные акты РФ (СудАкт). – URL: https://sudact.ru/ (дата обращения: 10.12.2025).

[2]Приговор Яшкульского районного суда Республики Калмыкия от 25 марта 2022 г. по делу № 1-1453/2022: [электронный ресурс] // Судебные и нормативные акты РФ (СудАкт). – URL: https://sudact.ru/ (дата обращения: 10.12.2025).

[3]Приговор Буденновского городского суда Ставропольского края от 18 апреля 2020 г. по делу № 1-1358/2020: [электронный ресурс] // Судебные и нормативные акты РФ (СудАкт). – URL: https://sudact.ru/ (дата обращения: 10.12.2025).

требуют совокупной квалификации: ст. 159.6 (как форма хищения) и ст. 273 УК РФ (как использование вредоносной программы). Игнорирование второго состава не отражает всей общественной опасности деяния[1].

Эти примеры ясно показывают, что корень проблемы лежит в несовершенстве конструкции ст. 159.6 УК РФ «Мошенничество в сфере компьютерной информации». По своей объективной стороне это деяние не является мошенничеством в классическом понимании, так как в нем отсутствует главный признак – обман или злоупотребление доверием человека. Фактически эта норма описывает хищение путем вмешательства в автоматизированный процесс обработки информации: когда виновный, не вводя в заблуждение владельца, заставляет компьютерную систему совершить ошибочные действия (перевод средств, списание товара) посредством ввода команд, вредоносного кода или несанкционированного доступа. Это ближе к механизму кражи, но совершенной особым, «цифровым» способом.

Сложившаяся ситуация, когда суды вынуждены «подгонять» цифровые хищения под три разные статьи (158, 159 или 159.6), порождает правовую неопределенность, усложняет работу следствия и способствует ошибкам в квалификации. Для исправления этого положения назрела объективная необходимость законодательной реформы. Наиболее логичным и практичным решением видится исключение из УК РФ статьи 159.6 и введение нового квалифицирующего признака в статье 158 УК РФ «Кража». Формулировка может выглядеть так: «... совершенная с использованием компьютерной информации, информационно-телекоммуникационных сетей, включая сеть «Интернет», либо вредоносных компьютерных программ».Такой подход позволит четко разграничить составы: кража (ст. 158) – тайное хищение, в том числе цифровое, путем вмешательства в автоматическую систему; мошенничество (ст. 159) – хищение путем обмана человека, независимо от того, происходит ли это взаимодействие онлайн или оффлайн; адекватно

[1]Приговор Орловского районного суда Орловской области от 15 сентября 2022 г. по делу № 1-1814/2022: [электронный ресурс] // Судебные и нормативные акты РФ (СудАкт). – URL: https://sudact.ru/ (дата обращения: 10.12.2025).

отразить общественную опасность деяния, так как цифровой способ совершения кражи повышает ее латентность, масштабируемость и сложность раскрытия; сохранить необходимость дополнительной квалификации по статьям 272, 273, 274.1 УК РФ, когда хищение сопряжено с неправомерным доступом или использованием вредоносного ПО, что полностью соответствует разъяснениям Верховного Суда.

Таким образом, совершенствование уголовного закона в направлении четкого разделения «цифровой кражи» и «онлайн-мошенничества» является насущной потребностью, продиктованной реалиями цифровой эпохи и необходимостью обеспечения единообразия, а значит, и справедливости правосудия.

§ 2. Перспективы совершенствования уголовного законодательства в сфере хищений с использованием информационных технологий

Совершенствование уголовно-правовых норм, направленных на противодействие хищениям с использованием информационных технологий, является объективной необходимостью в условиях стремительной цифровизации экономики и общественных отношений. Ключевой нормой в этой сфере выступает ст. 159.6 УК РФ «Мошенничество в сфере компьютерной информации», анализ которой в свете правоприменительной практики и доктринальных исследований выявляет ряд системных проблем, требующих законодательного решения.

Основная коллизия ст. 159.6 УК РФ заключается в её формальном отнесении к мошенничеству при отсутствии в диспозиции главного конститутивного признака этого преступления – обмана или злоупотребления доверием, приводящего к добровольной передаче имущества самим потерпевшим.

Более того, согласно п. 21 постановления Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», акцентируется внимание на хищении, осуществляемом путем распространения заведомо ложных сведений в информационно-телекоммуникационных сетях, включая сеть Интернет, что при данных обстоятельствах следует квалифицировать по ст. 159 УК РФ[1].

Практическим примером, иллюстрирующим типичный механизм мошенничества в сфере компьютерной информации (ст. 159.6 УК РФ), может служить дело подсудимого Д. В целях хищения денежных средств с причинением значительного ущерба он совершил ряд последовательных действий, основанных на обмане и несанкционированном вмешательстве в работу информационных систем. Используя осведомленность о банковских процедурах, Д. отправил потерпевшему М. заведомо ложное SMS-сообщение о блокировке его банковских карт. Когда введенный в заблуждение М. перезвонил на указанный номер, Д., представившись сотрудником банка, незаконно получил конфиденциальные данные: номер карты и кодовое слово. Впоследствии, используя компьютер с доступом в сеть, Д. ввел эти данные на официальном сайте банка, что представляет собой модификацию компьютерной информации и несанкционированный доступ. Получив таким образом контроль над банковским счетом М., Д. с помощью сервиса «Мобильный банк» совершил несколько переводов на общую сумму 2 133 121 рубль на подконтрольный ему счет, чем окончательно завершил хищение. Данный казус наглядно демонстрирует сочетание элементов социальной инженерии (обман для получения реквизитов) и непосредственного вмешательства в компьютерную информацию (несанкционированный доступ

[1]О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 (ред. от 15.12.2022) // Российская газета. – 2017. – № 280.

через интернет-банк), что составляет объективную сторону состава преступления, предусмотренного ст. 159.6 УК РФ[1].

Как показывает судебная практика типичная схема заключается в несанкционированном доступе к компьютерной информации (путем взлома, фишинга, использования вредоносного ПО), последующей модификации данных и тайном завладении средствами со счетов потерпевшего. Потерпевший не совершает каких-либо действий по передаче имущества, более того, он часто не подозревает о хищении в момент его совершения[2]. Это сближает данный способ с кражей, но отличает его особым «инструментарием» – вмешательством в функционирование информационных систем.

Таким образом, ст. 159.6 УК РФ фактически устанавливает ответственность не за разновидность обмана, а за хищение, совершаемое особым способом – путем использования информационных технологий. В этой связи, обоснованным является предложение о переименовании статьи и изменении её диспозиции на «Хищение путем использования информационных технологий», что соответствует терминологии международных актов и документов СНГ (например, Соглашения о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере информационных технологий от 28 сентября 2018 г.).

Следующей назревшей проблемой следует считать проблему определения предмета преступления в цифровой среде. Законодательное определение электронных денежных средств (далее – ЭДС) в Федеральном законе «О национальной платежной системе» носит технико-организационный характер, описывая системы хранения и передачи стоимости, но не даёт им чёткой гражданско-правовой и, как следствие, уголовно-правовой квалификации[3]. По

---

[1]Приговор Ленинского районного суда г. Екатеринбурга от 21 ноября 2022 г. по делу № 1-144/2022: [электронный ресурс] // Судебные и нормативные акты РФ (СудАкт). – URL: https://sudact.ru/ (дата обращения: 08.12.2025).

[2] Зобнина С.А. Уголовная ответственность за хищение, совершаемое путем использования информационных технологий // Молодой ученый. 2024. № 43(542). С. 195.

[3] О национальной платежной системе: федер. закон Рос. Федерации от 27 июня 2011 г. № 161-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 14 июня 2011 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 22 июня 2011 г. // Рос. газ. – 2011. – 30 июня.

этой причине возникает вопрос о том, что следует относить к единицам стоимости, а что – к электронным деньгам. А.И. Лукашов придерживается той позиции, что титульные знаки WebMoney Transfer – это хранящиеся в электронном виде на программно-техническом устройстве единицы стоимости, которые выражают сумму обязательств эмитента перед пользователями, и принимаемые в качестве законного средства платежа только эмитентом[1]. Вместе с тем из такого понимания единиц стоимости следует, что титульные знаки WebMoney Transfer не являются электронными деньгами, что не соответствует действительности. Таким образом, невозможно провести различия между электронными деньгами и единицами стоимости.

Кроме того, в доктрине ведутся споры о том, являются ли электронные денежные средства, криптоактивы и иные цифровые права «имуществом» в смысле ст. 128 ГК РФ и, соответственно, предметом хищения. Пленум Верховного Суда Российской Федерации в постановлении от 30.11.2017 № 48 указал, что безналичные денежные средства, а также бездокументарные ценные бумаги признаются имуществом. Однако для новейших форм цифровых активов такая определённость отсутствует. Это создаёт трудности в квалификации, когда хищению подвергаются, например, токены или средства на электронных кошельках, не связанных напрямую с банковским счетом. Перспективным направлением является законодательное закрепление положения о том, что предметом хищения по ст. 159.6 УК РФ наряду с имуществом являются права на имущество, включая право требования и иные права, удостоверенные в электронной (цифровой) форме. Это позволило бы подвести под действие нормы любые экономически ценные цифровые активы, устранив существующий правовой пробел.

Не менее важной проблемой следует рассматривать вопрос об обоснованности санкций, которые предусмотрены уголовным законодательством за совершение данного вида преступных посягательств. К

---

[1] Лукашов А.И. Операции в системе WebMoney Transfer: легальная деятельность или преступление? //Юридический мир. 2009. № 9. С. 87.

примеру, если сравнить санкции статей 159 и 159.6 УК РФ, то увидим их отличия только в первых частях. В частности, за простое мошенничество (ч. 1 ст. 159) предусмотрено наказание вплоть до лишения свободы на срок до двух лет, тогда как за простое «компьютерное мошенничество» (ч. 1 ст. 159.6) лишение свободы не предусмотрено вовсе. При этом санкции за квалифицированные составы (ч. 2-4) в обеих статьях идентичны[1]. Это противоречит принципу дифференциации ответственности, так как хищения с использованием информационных технологий характеризуются повышенной общественной опасностью в силу ряда признаков: трансграничный характер, латентность, возможность причинения ущерба в особо крупных размерах мгновенно, подрыв доверия к финансовым и платежным системам. В связи с этим предлагается:

— ужесточить санкцию ч. 1 ст. 159.6 УК РФ, введя в качестве максимального наказания лишение свободы на срок до 3-4 лет, что будет соответствовать тяжести деяния;

— ввести специальный квалифицирующий признак – «совершение деяния лицом с использованием своего служебного положения, связанного с доступом к информационным системам, средствам их защиты или администрированию». Это актуально для инсайдерских атак, когда хищение совершается IT-специалистами компаний или сотрудниками банков;

— рассмотреть вопрос о повышении верхних пределов наказания для квалифицированных составов (ч. 3 и ч. 4) с учетом потенциального масштаба ущерба.

Следует также обратить внимание на проблему возраста установления уголовной ответственности за хищение путем использования информационных технологий. Действующая редакция УК РФ устанавливает ответственность по ст. 159.6 с 16 лет. Однако учитывая, что за кражу (ст. 158 УК РФ), в том числе с банковского счета, и грабеж (ст. 161 УК РФ) ответственность наступает с 14

[1] Петров В.Н. Уголовная ответственность за хищение, совершаемое путем использования информационных технологий // Молодой ученый. 2024. № 22(521). С. 410.

лет, а хищения с использованием ИТ по степени и характеру общественной опасности (тайное завладение имуществом) сопоставимы с кражей, логичным представляется снижение возраста уголовной ответственности по ст. 159.6 УК РФ до 14 лет. Это также отвечает реалиям цифрового общества, где несовершеннолетние зачастую обладают высокими техническими навыками, а доступ к соответствующим технологиям широко распространен.

В заключении хотелось бы отметить: перспективы совершенствования уголовного законодательства в исследуемой сфере лежат в плоскости: 1) пересмотра юридической природы деяния и выделения его в самостоятельную форму хищения; 2) расширительного легального определения предмета преступления для охвата всех видов цифровых ценностей; 3) построения гибкой и адекватной системы санкций, отражающей повышенную опасность киберхищений; 4) корректировки возраста ответственности в целях устранения существующего дисбаланса. Комплексная реализация этих мер позволит повысить эффективность противодействия одному из самых динамично развивающихся видов экономической преступности.

ЗАКЛЮЧЕНИЕ

Проведенное комплексное исследование уголовно-правовых средств противодействия хищениям, совершаемым с использованием информационных технологий, позволяет констатировать, что данный вид преступности представляет собой одну из наиболее серьезных и динамично развивающихся угроз экономической безопасности Российской Федерации в условиях глобальной цифровизации. Высокая общественная опасность IT-хищений обусловлена их транснациональным и латентным характером, способностью причинять ущерб в особо крупных размерах мгновенно, а также подрывать доверие граждан и бизнеса к электронным платежным и финансовым системам. Исторический анализ эволюции законодательства показал путь от полного отсутствия специальных норм к созданию в 2012 г. ст. 159.6 УК РФ «Мошенничество в сфере компьютерной информации», что стало ответом на вызовы времени. Однако, как показало исследование, действующая правовая конструкция содержит фундаментальное внутреннее противоречие: будучи формально отнесенной к мошенничеству, диспозиция данной нормы фактически описывает не обман человека, а специфический способ хищения — тайное завладение имуществом путем вмешательства в функционирование автоматизированных информационных систем. Это терминологическое несоответствие является коренной причиной множества проблем в правоприменительной практике.

Анализ материалов судебной практики выявил отсутствие единообразного подхода к квалификации цифровых хищений. Типичными являются случаи, когда схожие действия суды квалифицируют по-разному: как кражу (ст. 158 УК РФ), мошенничество (ст. 159 УК РФ) или мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ). Частые ошибки, связанные с неправильным отграничением простого использования похищенных реквизитов (кража) от непосредственного воздействия на компьютерную информацию с помощью вредоносных программ. Такая

правовая неопределенность нарушает принципы законности, равенства и справедливости, затрудняет работу правоохранительных органов и снижает эффективность противодействия данному виду преступности. Уголовно-правовая характеристика исследуемого деяния позволила выявить и другие системные проблемы. Во-первых, остается дискуссионным вопрос о признании предметом предложения новейших цифровых активов, таких как криптовалюты и токены, в силу нечеткости их правового статуса. Во-вторых, система квалифицирующих признаков ст. 159.6 УК РФ является дисбалансированной: специальный признак «хищение с банковского счета или электронных денежных средств» (ч. 3) фактически поглощает основные составы, так как подавляющее большинство IT-хищений совершается именно в отношении таких ценностей. Кроме того, отсутствие в статье единых стоимостных критериев ущерба вынуждает правоприменителя обращаться к различным примечаниям, что является скрытой аналогией закона. В-третьих, санкции за данное преступление не в полной мере отражают его повышенную общественную опасность: основной состав (ч. 1) не предусматривает лишения свободы, а наказание за квалифицированные виды идентично наказанию за обычное мошенничество, что не учитывает масштабности и особой вредоносности киберпреступлений. В-четвертых, установление возраста уголовной ответственности с 16 лет создает необоснованный разрыв с кражей (ответственность с 14 лет) и не соответствует реалиям вовлечения в данную деятельность технически грамотных несовершеннолетних.

В целях устранения выявленных противоречий и повышения эффективности уголовно-правового противодействия IT-хищениям необходима комплексная законодательная реформа. Наиболее логичным и перспективным направлением представляется коренное изменение подхода к криминализации данного деяния. Целесообразно исключить статью 159.6 УК РФ из числа видов мошенничества и ввести в главу 21 УК РФ новый самостоятельный состав преступления – «Хищение, совершенное с использованием информационных технологий». Альтернативным, но также эффективным решением может стать

введение в ст. 158 УК РФ («Кража») специального квалифицирующего признака, описывающего цифровой способ совершения. Это позволит четко разграничить составы: хищение путем вмешательства в автоматическую систему (цифровая кража) и хищение путем обмана человека (мошенничество, в том числе в сети). Параллельно необходимо: закрепить в примечании к ст. 158 УК РФ единые для всех форм хищения стоимостные критерии ущерба; ужесточить санкции за хищение с использованием ИТ, адекватно отразив его повышенную опасность; рассмотреть вопрос о снижении возраста ответственности до 14 лет; и легально расширить понятие предмета преступления, включив в него все экономически значимые цифровые права и активы. Реализация этих предложений создаст непротиворечивый, технологически нейтральный и эффективный правовой механизм, который будет способен адекватно реагировать на постоянно эволюционирующие угрозы в цифровой сфере, обеспечивая надежную защиту собственности, экономических интересов личности, общества и государства.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

I. Нормативные правовые акты и иные официальные документы

1. Конституция Российской Федерации: принята всенародным голосованием 12 декабря 1993 г. с учетом поправок, внесенных Законом Рос. Федерации о поправках к Конституции Рос. Федерации от 1 июля 2020 г. № 1–ФКЗ // Собр. законодательства Рос. Федерации. – 2020. – № 1.

2. Гражданский кодекс Российской Федерации: федер. закон Рос. Федерации от 30 ноября 1994 г. № 51-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 21 окт. 1994 г. // Рос. газ. – 1994. – 8 декабря.

3. Уголовный кодекс Российской Федерации: федер. закон Рос. Федерации от 13 июня 1996 г. № 63–ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 24 мая 1996 г., одобрен Советом Федер. Рос. Федерации 5 июня 1996 г. // Рос. газ. – 1996. – 18 июня.

4. О национальной платежной системе: федер. закон Рос. Федерации от 27 июня 2011 г. № 161-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 14 июня 2011 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 22 июня 2011 г. // Рос. газ. – 2011. – 30 июня.

5. О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации: федер. закон Рос. Федерации от 29 ноября 2012 г. № 207-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 23 ноябр. 2012 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 28 ноябр 2012 г. // Рос. газ. – 2012. – 3 декабря.

6. О внесении изменений в Уголовный кодекс Российской Федерации: федер. закон Рос. Федерации от 23 апреля 2018 г. № 111-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 10 апр. 2018 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 18 апр. 2018 г. // Рос. газ. – 2018. – 25 апреля.

7. О стратегии развития информационного общества в Российской Федерации на 2017-2030 годы: указ Президента Российской Федерации от 9 мая

2017 г. № 203 // Собр. законодательства Рос. Федерации. – 2017. – № 20, ст. 2901.

II. Учебная, научная литература и иные материалы

1. Бавсун М.В. Квалификация преступлений по признакам субъективной стороны: учебник для вузов / М. В. Бавсун, С. В. Векленко. – 2-е изд., испр. и доп. – Москва: Юрайт, 2025. – 143 с.

2. Гаухман Л.Д. Квалификация преступлений: закон, теория, практика / Л.Д. Гаухман. – 8-е изд., перераб. и доп. – Москва: Юриспруденция, 2021. – 378 с.

3. Головинов О.Н. Киберпреступность в современной экономике: состояние и тенденции развития / О.Н. Головинов, А.В. Погорелов // Вопросы инновационной экономики. – 2020. – Т. 10, № 6 (1). – С. 73–88.

4. Гриб Д.В. Уголовная ответственность за хищение, совершаемое путем использования информационных технологий по законодательству Республики Беларусь и Российской Федерации: дис. ... канд. юрид. наук: 12.00.08 / Д.В. Гриб. – Москва, 2021. – 215 с.

5. Дайшутов М.М. Признаки субъекта преступления и его правовые критерии / М.М. Дайшутов, В.И. Динека // Вестник Московского университета МВД России. – 2018. – № 6. – С. 127–131.

6. Дмитренко А.П. О нетипичных аспектах соучастия в преступлениях, совершаемых с использованием информационно-коммуникационных технологий / А.П. Дмитренко, Е.А. Русскевич // Вестник Академии Генеральной прокуратуры Российской Федерации. – 2021. – № 5 (61). – С. 16–21.

7. Догузов С.А. История развития правового регулирования преступлений, связанных с использованием компьютерной информации / С.А. Догузов, Л.А. Букалерова // Проблемы развития научного потенциала и направления его повышения: сборник статей Международной научно-

практической конференции (г. Новосибирск, 20 июня 2024 года). – Уфа: Аэтерна, 2024. – С. 119–125.

8. Долотова Н.П. Киберпреступность в банковской сфере в Российской Федерации / Н.П. Долотова // Гуманитарные, социально-экономические и общественные науки. – 2024. – № 12. – С. 215–219.

9. Елин В.М. Мошенничество в сфере компьютерной информации как новый состав преступления / В.М. Елин // Бизнес-информатика. – 2020. – № 2 (24). – С. 69–78.

10. Елисеев С.А. Преступления против собственности: курс лекций / С.А. Елисеев. – Томск: Издательский Дом Томского государственного университета, 2023. – 194 с.

11. Замалеева С.В. О некоторых проблемах квалификации мошенничества в сфере компьютерной информации / С.В. Замалеева // Право и государство: теория и практика. – 2022. – № 7 (211). – С. 132–135.

12. Зобнина С.А. Уголовная ответственность за хищение, совершаемое путем использования информационных технологий / С.А. Зобнина, М.О. Краснова // Молодой ученый. – 2024. – № 43 (542). – С. 194–196.

13. Козаев Н.Ш. «Электронные» и «пластиковые» деньги и преступность / Н.Ш. Козаев // Актуальные проблемы борьбы с преступлениями в сфере экономики : материалы международной научно-практической конференции. – Ставрополь: Северо-Кавказский федеральный университет, 2020. – С. 110–115.

14. Кочои С.М. Ответственность за корыстные преступления против собственности: учебно-практическое пособие / С.М. Кочои. – Москва: Проспект, 2010. – 112 с.

15. Кузнецова М.Д. Мошенничество в уголовно-правовом исследовании / М.Д. Кузнецова // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2024. – № 2 (66). – С. 161–166.

16. Лопашенко Н.А. Посягательства на собственность: монография / Н.А. Лопашенко. – Москва: Проспект, 2022. – 256 с.

17. Лукашов А.И. Операции в системе WebMoney Transfer: легальная деятельность или преступление? / А.И. Лукашов // Юридический мир. – 2009. – № 9. – С. 85–89.

18. Майстренко Г.А. К вопросу о необходимости пересмотра понятий «крупный ущерб», «особо крупный ущерб» в уголовном законодательстве России / Г.А. Майстренко // Образование и право. – 2022. – № 3. – С. 279–283.

19. Медведев Е.В. Уголовное право России. Общая часть: учебник для вузов / Е.В. Медведев. – 2-е изд., перераб. и доп. – Москва: Юрайт, 2025. – 168 с.

20. Нурмухаметов Р.Н. К вопросу о проблемах квалификации хищений, совершенных с применением информационных технологий / Р.Н. Нурмухаметов // Международный журнал гуманитарных и естественных наук. – 2024. – № 12-1 (99). – С. 180–184.

21. Петров С.А. Хищение чужого имущества или приобретение права на него путем обмана: уголовно-правовая оценка и совершенствование правовой регламентации: автореферат дис. ... канд. юрид, наук: 12.00.08 / С.А. Петров. – Москва, 2015. – 28 с.

22. Петров В.Н. Уголовная ответственность за хищение, совершаемое путем использования информационных технологий / В.Н. Петров // Молодой ученый. – 2024. – № 22 (521). – С. 409–412.

23. Пионтковский А.А. Учение о преступлении по советскому уголовному праву / А.А. Пионтковский // Курс советского уголовного права: Общая часть. Т. 2. – Москва: Госюриздат, 1961. – 265 с.

24. Пудовочкин Ю.Е. Судебная практика квалификации преступлений, совершенных в соучастии / Ю.Е. Пудовочкин // Криминологический журнал БГУЭП. – 2021. – № 2 (16). – С. 5–12.

25. Русскевич Е.А. Новые нормы УК об «электронном» мошенничестве и коррупционных преступлениях / Е.А. Русскевич // Уголовный процесс. – 2018. – № 7. – С. 31–35.

26. Сафонов О.М. Уголовно-правовая оценка использования компьютерных технологий при совершении преступлений: состояние законодательства и правоприменительной практики, перспективы совершенствования: дис. ... канд. юрид. наук: 12.00.08 / О.М. Сафонов. – Москва, 2015. – 215 с.

27. Сироткин И. Ответственность участников организованных групп и преступных организаций / И. Сироткин // Законность. – 2019. – № 10. – С. 37–41.

28. Суслопаров А.В. Компьютерные преступления как разновидность преступлений информационного характера: автореферат дис. ... канд. юрид.наук: 12.00.08 / А. В. Суслопаров. – Владивосток, 2010. – 29 с.

29. Таганцев Н.С. Курс русского уголовного права. Часть Общая. Книга 1. Учение о преступлении / Н.С. Таганцев. – Санкт-Петербург: Тип. М.М. Стасюлевича, 1874. – 464 с.

30. Третьяк М.И. Мошенничество как преступление против собственности в современном уголовном праве: курс лекций / М.И. Третьяк. – Москва: Юрлитинформ, 2023. – 152 с.

31. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис.... канд. юрид. наук: 12.00.08 / Т.Л. Тропина. – Владивосток, 2005. – 215 с.

32. Уголовное право России. Часть Общая. Часть Особенная: учебник / под общей ред. Л.Д. Гаухмана, Л.М. Колодкина, С.В. Максимова. – Москва: Юриспруденция, 1999. – 784 с.

33. Хисамова З.И. О конструкции норм уголовного законодательства, предусматривающих ответственность за преступления, совершаемые с использованием информационно-телекоммуникационных технологий / З.И. Хисамова // Уголовная политика и культура противодействия преступности: материалы Международной научно-практической конференции. – Краснодар: Краснодарский университет МВД России, 2016. – С. 344–348.

34. Чекунов И.Г. Киберпреступность: понятие и классификация / И.Г. Чекунов // Российский следователь. – 2022. – № 2. – С. 36–40.

35. Чупрова А.Ю. Проблемы классификации мошенничества с использованием информационных технологий / А.Ю. Чупрова // Уголовное право. – 2020. – № 5. – С. 132–138.

36. Яни П.С. Специальные виды мошенничества / П.С. Яни // Законность. – 2015. – № 8. – С. 34–38.

37. Ястребов Д.А. Информационная безопасность в Российской Федерации: (уголовно-правовая борьба с неправомерным доступом к компьютерной информации) / Д.А. Ястребов, Н.В. Брянцева. – Москва: Полтекс, 2006. – 196 с.

III. Эмпирические материалы

1. О судебной практике по делам о краже, грабеже и разбое : постановление Пленума Верховного Суда Российской Федерации от 27 декабря 2002 г. № 29 (ред. от 15.12.2022) // Бюллетень Верховного Суда РФ. – 2003. – № 2.

2. О судебной практике по делам о мошенничестве, присвоении и растрате : постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 (ред. от 15.12.2022) // Бюллетень Верховного Суда РФ. – 2018. – № 2.

3. О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» : постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37 // Бюллетень Верховного Суда РФ. – 2023. – № 3.

4. Приговор Буденновского городского суда Ставропольского края от 18 апреля 2020 г. по делу № 1-1358/2020: [электронный ресурс] // Судебные и

нормативные акты РФ (СудАкт). – URL: https://sudact.ru/ (дата обращения: 10.12.2025).

5. Приговор Братского городского суда Иркутской области от 19 декабря 2020 г. по делу № 1-558/2020: [электронный ресурс] // Судебные и нормативные акты РФ (СудАкт). – URL: https://sudact.ru/ (дата обращения: 10.12.2025).

6. Приговор Советского районного суда г. Владивостока от 15 мая 2021 г. по делу № 1-718/2021: [электронный ресурс] // Судебные и нормативные акты РФ (СудАкт). – URL: https://sudact.ru/ (дата обращения: 10.12.2025).

7. Приговор Яшкульского районного суда Республики Калмыкия от 25 марта 2022 г. по делу № 1-1453/2022: [электронный ресурс] // Судебные и нормативные акты РФ (СудАкт). – URL: https://sudact.ru/ (дата обращения: 10.12.2025).

8. Приговор Ленинского районного суда г. Екатеринбурга от 21 ноября 2022 г. по делу № 1-144/2022: [электронный ресурс] // Судебные и нормативные акты РФ (СудАкт). – URL: https://sudact.ru/ (дата обращения: 08.12.2025).

9. Приговор Орловского районного суда Орловской области от 15 сентября 2022 г. по делу № 1-1814/2022: [электронный ресурс] // Судебные и нормативные акты РФ (СудАкт). – URL: https://sudact.ru/ (дата обращения: 10.12.2025).

10. Приговор Новолакского районного суда Республики Дагестан от 13 апреля 2023 г. по делу № 1-26/2023: [электронный ресурс] // Судебные и нормативные акты РФ (СудАкт). – URL: https://sudact.ru/ (дата обращения: 08.12.2025).

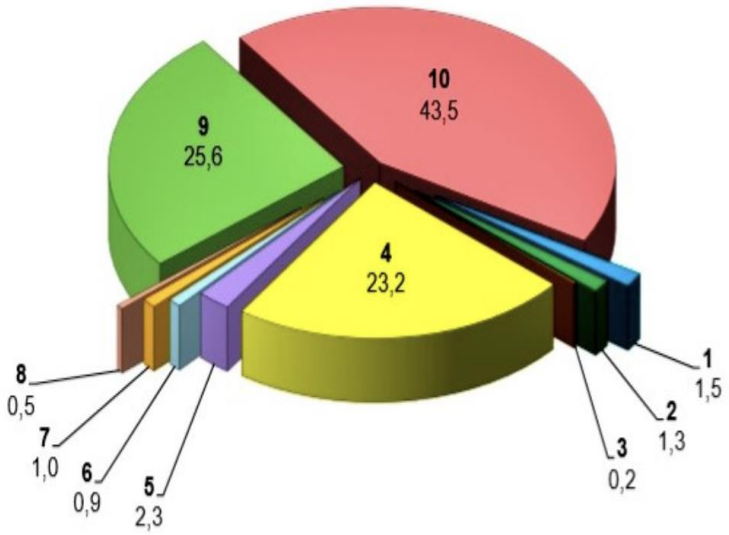
Материал вычитан, цифры, факты, цитаты сверены с первоисточником. Материал не содержит сведений, составляющих государственную и служебную тайну  А.В. Назаров

ПРИЛОЖЕНИЕ 1

СОСТОЯНИЕ ПРЕСТУПНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

СТРУКТУРА ПРЕСТУПНОСТИ (в %)

январь - декабрь



1 - взяточничество

2 - убийство, умышленное причинение тяжкого вреда здоровью, изнасилование

3 - хулиганство

4 - мошенничества ст. 159-159.6 УК РФ

5 - управление транспортным средством в состоянии опьянения лицом, подвергнутым административному наказанию или имеющим судимость

6 - нарушение правил дорожного движения и эксплуатации транспортных средств

7 - грабеж, разбой

8 - присвоение или растрата

9 - кража

10 - прочие