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

Кафедра уголовного права

Выпускная квалификационная работа
(магистерская диссертация)

на тему: «Мошенничества, совершенные с использованием информационных технологий: юридический анализ и проблемы квалификации»

Выполнил:
Павловская Наталья Александровна
40.04.01- «Юриспруденция»,
год набора – 2023, учебная группа № М31

Научный руководитель:
кандидат юридических наук, доцент, начальник кафедры уголовного права КЮИ МВД России
Амирова Диляра Кафилевна

Рецензент:
заместитель начальника СО ОМВД России по Зеленодольскому району,
подполковник юстиции
Шайхуллина Олеся Владимировна

Дата защиты: «__» _____ 20___ г.

Оценка _____

Казань 2026

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования. Информационная глобализация и цифровизация оказывают существенное влияние на все сферы общественной жизни, способствуя трансформации преступности и преступного поведения лиц, посягающих на охраняемые уголовным законом общественные отношения.

Охрана общественных отношений от преступлений, совершаемых с использованием информационно-коммуникационными технологиями (системами), осуществляется на международном уровне, поскольку информационно-коммуникационные технологии, обладая огромным потенциалом, способным содействовать развитию общества, открывают новые возможности для преступников, могут способствовать увеличению масштабов и разнообразия преступной деятельности и иметь негативные последствия для государств, предприятий и благополучия людей и общества в целом. В связи с этим, в качестве целей в Конвенции ООН против киберпреступности, в качестве целей заявлено содействие принятию и укрепление мер, направленных на повышение эффективности и результативности предупреждения киберпреступности и борьбы с ней; поощрение, облегчение и укрепление международного сотрудничества в предупреждении киберпреступности и борьбе с ней; поощрение, облегчение и поддержка технической помощи и создания потенциала в целях предупреждения киберпреступности и борьбы с ней, особенно в интересах развивающихся стран[1].

В Стратегии национальной безопасности Российской Федерации, утвержденной указом Президента Российской Федерации от 2 июля 2021 г.

[1] Конвенция Организации Объединенных Наций против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям (Принята резолюцией 79/243 Генеральной Ассамблеей от 24 декабря 2024 года) // СПС «Консультант плюс». – URL: https://www.un.org/ru/documents/treaty/A-RES-79-243 (Дата обращения 01.10.2025).

№ 400[1], отмечено, что быстрое развитие информационно-коммуникационных технологий сопровождается повышением вероятности возникновения угроз безопасности граждан, общества и государства. Согласно официальному заявлению Министра внутренних дел Российской Федерации В.А. Колокольцеву, в 2025 году «впервые за последние годы в России сократилось количество преступлений в сфере информационно-коммуникационных технологий». За 12 месяцев 2025 года было зарегистрировано на 11,8 % меньше преступлений, совершенных с использованием информационно-телекоммуникационных технологий, чем в 2024 году. Количество дистанционных краж снизилось на 23,6 %, дистанционных мошенничеств – на 9 %, а преступлений в сфере компьютерной информации – на 42,2 %[2]. Несмотря на снижение количества таких преступлений, их доля в общем количестве преступлений остается высокой. Согласно данным ГИАЦ МВД России, в настоящее время каждое третье преступление совершается с использованием информационно-телекоммуникационных технологий (Таблица № 1).

	ст. 159 УК РФ	ст. 159^3 УК РФ	ст. 159^6 УК РФ
2020	210493	25820	761
2021	238560	10258	431
2022	249984	7288	334
2023	353201	2461	417
2024	379762	273	309
2025	345561	99	319

Таблица 1. Количество зарегистрированных преступлений, совершенных с использованием информационно телекоммуникационных технологий или в сфере компьютерной информации, квалифицированных по ст.ст. 159, 159^3, 159^6 УК РФ.

[1] О Стратегии национальной безопасности Российской Федерации: Указ Президента РФ от 02.07.2021 № 400 // Собр. законодательства Рос. Федерации. – 2021. – № 27 (часть II). – Ст. 5351.

[2] Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2025 года. Министерство внутренних дел Российской Федерации. Официальный сайт. – URL: https://мвд.рф/reports/item/77848182/ (дата обращения: 10.01.2026).

Согласно официальным статистическим данным, за 2025 г. зарегистрировано 675 273 преступлений, совершённых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. При этом более половины указанного массива составляют деяния, связанные с незаконным оборотом безналичных и электронных денежных средств, что свидетельствует о криминализации цифрового имущественного оборота и системном характере соответствующих угроз.

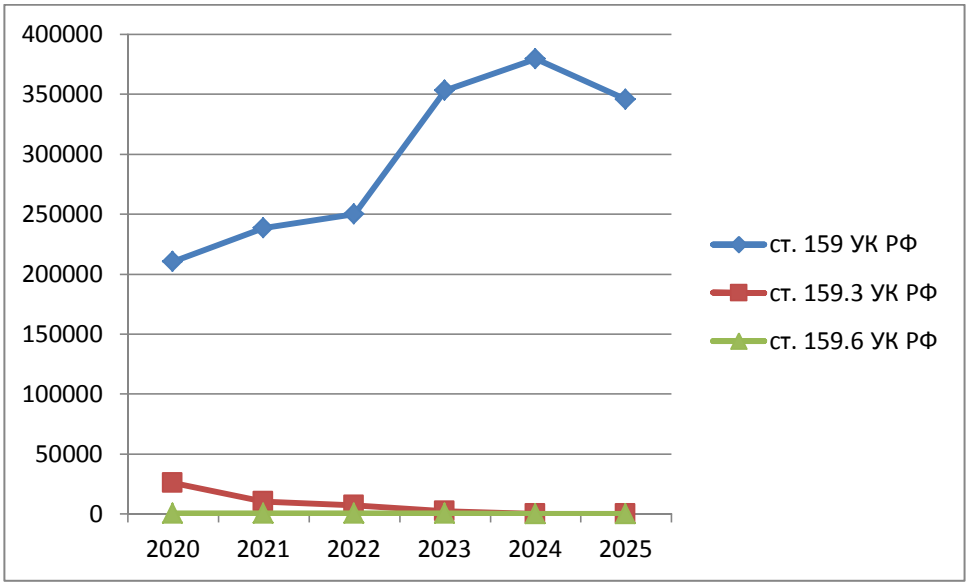

Рисунок 1. Уровень и динамика отдельных видов хищений, совершенных в 2020-2025 г.г. с использованием информационно телекоммуникационных технологий или в сфере компьютерной информации, квалифицированных по ст. ст. 159, 159^3, 159^6 УК РФ.

Следует отметить тенденцию к снижению количества преступлений, квалифицируемых по статьям 159, 159^3 и 159^6 УК РФ. Более того, на 348 035 мошенничеств, квалифицированных по ст. 159 – 159^6 УК РФ, зарегистрированных в 2025 году, 345 461 приходятся на мошенничество с использованием информационно-телекоммуникационных технологий. При этом мошенничество с использованием электронных средств платежа (ст. 159^3 УК РФ) и мошенничество в сфере компьютерной информации (ст. 159^6 УК РФ) количественно несопоставимы с общим массивом цифровых

мошенничеств, что указывает на фрагментарность законодательной конструкции и неравномерность её применения. Существенное расхождение между масштабом цифровых хищений и количеством выявленных составов по специальным нормам подтверждает наличие проблем квалификации и выбора надлежащей уголовно-правовой оценки.

Дополнительным аргументом актуальности является выраженная сложность выявления и расследования цифровых мошенничеств. Из общего числа зарегистрированных преступлений значительная часть относится к категории тяжких и особо тяжких (369 267 фактов), при этом выявление таких деяний осуществляется преимущественно органами внутренних дел, на которые приходится основная нагрузка по противодействию цифровым посягательствам. Массовость преступлений при одновременной технологической сложности способов их совершения обуславливает высокую латентность и затрудняет формирование единообразной правоприменительной практики.

Цифровизация имущественного оборота изменила сам механизм преступного посягательства. Хищения всё чаще совершаются без непосредственного контакта между виновным и потерпевшим, посредством дистанционного доступа к платёжным сервисам, использования средств аутентификации, манипулирования доверием третьих лиц либо сочетания обмана с программно-техническими действиями. В таких условиях традиционные уголовно-правовые конструкции мошенничества, ориентированные на классическую модель межличностного обмана, оказываются недостаточно приспособленными для адекватной оценки современных форм преступного поведения.

Наконец, актуальность исследования обусловлена потребностью в совершенствовании уголовного законодательства. Дискуссионный характер статьи 159^{6} УК РФ, дублирование её диспозиции с нормами главы 28 УК РФ и наличие конкуренции со статьёй 159^{3} УК РФ свидетельствуют о необходимости научного осмысления целесообразности сохранения действующей модели

дифференциации ответственности. Выработка теоретически обоснованных и практически применимых предложений по оптимизации уголовно-правового регулирования мошенничеств в цифровой среде представляет значимый интерес как для науки уголовного права, так и для деятельности следственных и судебных органов.

Степень разработанности темы исследования. Проблематика мошенничества как преступления против собственности получила разностороннее освещение в отечественной уголовно-правовой науке. В трудах А. В. Архипова, М. В. Бажанова, А. Г. Безверхова, А. И. Бойцова, Г. Н. Борзенкова, Б. В. Волженкина, Л. Д. Гаухмана и других исследователей сформированы устойчивые подходы к понятию мошенничества, его составу и отграничению от смежных форм хищений.

В последние годы научный интерес сместился в сторону мошенничеств, совершаемых с использованием электронных средств платежа и цифровых технологий. Указанная проблематика рассматривается в работах И. Р. Бегичева, И. И. Бикеева, О. В. Ершаковой, Л. В. Боровых, М. А. Ефремовой, Н. А. Карповой, Т. И. Саблиной, а также в диссертационных исследованиях С. Я. Бойко, С. В. Васюкова, А. С. Камко и других авторов, где анализируются особенности объективной стороны цифровых посягательств, отдельные вопросы квалификации и доказывания.

Одновременно анализ научных публикаций выявляет отсутствие согласованного подхода к разграничению мошенничества с использованием электронных средств платежа, мошенничества в сфере компьютерной информации и кражи с банковского счёта, а также к их соотношению с преступлениями главы 28 УК РФ. Во многих исследованиях вне поля внимания остаются современные комбинированные схемы цифровых посягательств и противоречивая судебная практика последних лет, что обусловливает необходимость дальнейшей разработки заявленной темы.

Цель и задачи исследования. Целью магистерской диссертации является получение новых знаний о составах мошенничества, совершаемых с

использованием информационных технологий, о проблемах их квалификации, возникающих в правоприменительной практике, выработки уголовно-правовой модели квалификации мошенничеств, совершаемых с использованием информационных технологий, а также формулировании на основе полученных знаний предложений по совершенствованию действующего уголовного законодательства в этой сфере и практики его применения.

Задачи исследования:

1. выявить и систематизировать социальные и правовые предпосылки криминализации мошенничеств, совершаемых с использованием информационных технологий, а также определить их место в системе преступлений против собственности;
2. обобщить зарубежные модели уголовно-правовой ответственности за мошенничества, совершаемые с использованием информационных технологий. Выявить наиболее эффективные модели с точки зрения заимствования опыта;
3. раскрыть содержание объективных признаков мошенничеств, совершаемых с использованием информационных технологий;
4. определить особенности субъективных признаков указанных преступлений;
5. дать уголовно-правовую оценку квалифицированным и особо квалифицированным признакам мошенничеств, совершаемых с использованием информационных технологий;
6. выявить признаки отграничения мошенничеств, совершаемых с использованием информационных технологий, от смежных составов преступлений;
7. выявить и проанализировать проблемы, возникающие в правоприменительной практике квалификации таких мошенничеств, а также, на основе полученных выводов, выработать уголовно-правовую модель квалификации;
8. сформулировать предложения по совершенствованию уголовно-

правовых норм, регламентирующих ответственность за совершение мошенничеств, совершаемым с использованием информационных технологи и практики их применения.

Объект и предмет исследования. Объектом исследования являются общественные отношения, возникающие в связи с уголовно-правовой охраной собственности при совершении мошенничеств с использованием электронных средств платежа и информационных технологий.

Предмет исследования образуют нормы уголовного законодательства Российской Федерации, предусматривающие ответственность за мошенничества, совершаемые с использованием информационных технологий, практика их применения, а также доктринальные подходы к квалификации указанных деяний и их отграничению от смежных составов преступлений.

Методологическую основу исследования образует совокупность общенаучных и специальных юридических методов познания. В работе применяются диалектический метод, формально-юридический и системно-структурный анализ, сравнительно-правовой, а также иные методы.

Нормативно-правовую основу исследования составляют Конституция Российской Федерации, Уголовный кодекс Российской Федерации, федеральные законы, регулирующие использование электронных средств платежа и информационных технологий, иные нормативно-правовые акты.

Теоретическую основу исследования образуют положения отечественной и зарубежной уголовно-правовой доктрины о понятии и признаках мошенничества, механизме хищения и критериях его разграничения со смежными составами преступлений. В работе использованы труды российских и иностранных ученых-юристов, научные статьи и монографии, материалы научно-практических конференций, диссертационные исследования.

Эмпирическую основу исследования составляют материалы судебной практики по уголовным делам о мошенничествах, совершённых с использованием и информационных технологий, отчеты о состоянии преступности МВД РФ.

Научная новизна и основные положения, выносимые на защиту. Научная новизна исследования заключается в формировании комплексного уголовно-правового подхода к квалификации мошенничеств, совершаемых с использованием информационных технологий, основанного на анализе реальных механизмов цифровых посягательств и современной судебной практики, а также выработки модели квалификации таких преступлений для эффективной работы правоприменительных органов.

В работе обоснована избыточность выделения мошенничества в сфере компьютерной информации в качестве самостоятельного состава преступления, предложена концепция концентрации цифровых форм мошенничества в рамках одной специальной нормы, а также уточнены критерии разграничения мошенничества, кражи с банковского счёта и преступлений против компьютерной информации.

На защиту выносятся следующие положения:

1) закрепить расширенное понимание предмета хищения, дополнив примечание к статье 158 УК РФ следующим положением: «1.1. Предметом хищения в статьях настоящей главы признаются движимые и недвижимые вещи, включая наличные деньги и документарные ценные бумаги, а равно иное имущество, в том числе безналичные и электронные денежные средства, бездокументарные ценные бумаги, цифровые финансовые активы, цифровые валюты и иные имущественные права». Это позволит обеспечить единообразие правоприменения и повысить правовую определённость.

2) Необходимо пересмотреть возрастной порог уголовной ответственности за мошенничество с использованием электронных средств платежа. В условиях широкого распространения безналичных расчётов и фактической доступности цифровых платёжных сервисов для несовершеннолетних обманное изъятие электронных денежных средств по своему социально-правовому содержанию не отличается от тайного хищения таких же имущественных ценностей. Сохранение различного возрастного подхода к оценке кражи и мошенничества при безналичном обороте приводит к

формальному разграничению составов и неоднородности правоприменения. В этой связи предлагается установить уголовную ответственность по статье 159^3 УК РФ с четырнадцатилетнего возраста, что соответствует уровню осознания противоправности деяния, характеру причиняемого вреда и современному состоянию цифровых имущественных отношений.

3) Сохранение статьи 159^6 УК РФ в системе преступлений против собственности УК РФ не обеспечивает ясности квалификации цифровых хищений и порождает конкуренцию норм. Предлагается исключить данный состав, сосредоточив уголовно-правовую оценку мошенничеств с применением электронных средств платежа и компьютерных технологий в обновлённой редакции статьи 159^3 УК РФ.

4) Изложить ст. 159^3 УК РФ в следующей редакции.

Статья 159^3 Мошенничество с использованием электронных средств платежа или в сфере компьютерной информации

1. Мошенничество, то есть хищение чужого имущества либо приобретение права на чужое имущество путём обмана или злоупотребления доверием, совершённое с использованием электронных средств платежа или в сфере компьютерной информации, –

наказывается штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на срок до трех лет.

2. То же деяние, совершенное группой лиц по предварительному сговору, а равно с причинением значительного ущерба гражданину, -

наказывается штрафом в размере до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до двух лет, либо обязательными работами на срок до четырехсот восьмидесяти часов, либо исправительными работами на срок до двух лет, либо принудительными

работами на срок до пяти лет с ограничением свободы на срок до одного года или без такового, либо лишением свободы на срок до пяти лет с ограничением свободы на срок до одного года или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные лицом с использованием своего служебного положения, а равно в крупном размере, -

наказываются штрафом в размере от ста тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до двух лет или без такового, либо лишением свободы на срок до шести лет со штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев либо без такового и с ограничением свободы на срок до полутора лет либо без такового.

4. Мошенничество в сфере компьютерной информации, совершенное с банковского счета, а равно в отношении электронных денежных средств,

наказываются штрафом в размере от ста тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до двух лет или без такового, либо лишением свободы на срок до шести лет со штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев либо без такового и с ограничением свободы на срок до полутора лет либо без такового.

5. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, совершенные организованной группой либо в особо крупном размере, -

наказываются лишением свободы на срок до десяти лет со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного

дохода осужденного за период до трех лет либо без такового и с ограничением свободы на срок до двух лет либо без такового.

Примечание. Под мошенничеством в сфере компьютерной информации понимается хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

5) Предлагается модель квалификации цифровых хищений, основанная на механизме доступа к денежным средствам. На первом этапе фиксируются имущественный результат (списание, перевод, оформление кредита/займа) и юридически значимый потерпевший (владелец счёта, банк/МФО), что определяет адресата обмана. Далее устанавливается способ получения возможности распоряжения средствами: при тайной оплате/списании без введения кого-либо в заблуждение деяние квалифицируется как кража с банковского счёта (п. «г» ч. 3 ст. 158 УК РФ); при введении в заблуждение либо злоупотреблении доверием – как мошенничество по ст. 159 УК РФ, а при использовании электронного средства платежа – по ст. 159^3 УК РФ. Если хищение достигнуто вмешательством в обработку компьютерной информации (ввод, блокирование, модификация и т. п.), применяется ст. 159^6 УК РФ. Комбинированные схемы оцениваются по фактам, включая совокупность. Отдельно проверяется наличие самостоятельных посягательств на информационную безопасность (ст. 272–274^1 УК РФ) и роль соучастников («дропы», курьеры, организаторы) по их умыслу и функции.

Теоретическая и практическая значимость исследования. Теоретическая значимость исследования состоит в уточнении уголовно-правовых подходов к квалификации мошенничеств, совершаемых с использованием электронных средств платежа и компьютерных технологий, а также в развитии представлений о соотношении норм о преступлениях против собственности и преступлениях против компьютерной информации. Сформулированные

выводы могут быть использованы при дальнейшем научном анализе цифровых форм хищений и при совершенствовании уголовного законодательства.

Практическая значимость работы заключается в возможности применения полученных результатов в деятельности следственных и судебных органов при квалификации преступлений, связанных с хищением безналичных денежных средств, а также при подготовке разъяснений, методических рекомендаций и учебных материалов по уголовному праву. Положения диссертации могут быть использованы в учебном процессе юридических вузов и при разработке предложений по корректировке уголовно-правовых норм.

Апробация результатов исследования. Основные положения и выводы, сформулированные в магистерской диссертации, докладывались на международной научно-практической конференции «Борьба с преступностью: теория и практика» (КЮИ МВД России, 20 марта 2025 г.) и Всероссийском круглом столе «Дистанционные хищения и кибербезопасность» (КЮИ МВД России, 13 марта 2025 г.), а также были использованы при подготовке эссе и доклада на конкурс, посвященный Дню российской науки (КЮИ МВД России, 1–6.02.2026 г.). Основные положения были отражены в опубликованных статьях:

1. Павловская Н.А. Проблемы уголовной ответственности курьеров при совершении мошенничества с использованием информационных технологий / Н.А. Павловская, Г.И. Шарафиева // Научный аспект. – 2024. – Т. 37, № 5. – С. 5078-5083.

2. Павловская Н.А. Особенности квалификации хищений, совершенных с использованием информационных технологий / Н.А. Павловская // Инновационная экономика и современный менеджмент. – 2026. – № 1. – С. 3-8.

3. Павловская Н.А. Проблемы правоприменительной практики в судах при квалификации преступлений и назначении наказаний / Н. А. Павловская // Н.А. Павловская // Инновационная экономика и современный менеджмент. – 2026. – № 2. – С. 20-25.

Структура магистерской диссертации определяется ее целями и задачами

и включает в себя введение, три главы, состоящих из семи параграфов, заключение, список использованной литературы, приложения.

ГЛАВА 1. ОБЩАЯ ХАРАКТЕРИСТИКА МОШЕННИЧЕСТВ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

§ 1. Социальные предпосылки криминализации мошенничеств, совершенных с использованием информационных технологий и их общая характеристика

Современное общество развивается в условиях интенсивного внедрения цифровых технологий, определяющих новые формы социального и экономического взаимодействия. Электронные способы передачи данных и дистанционные коммуникации превращаются в обычную практику функционирования государственных структур, бизнеса и частных лиц. Формирование цифровой среды приводит к постепенному вытеснению традиционных механизмов управления и обслуживания населения более гибкими и технологичными системами[1].

Создание разветвленной телекоммуникационной инфраструктуры и единых цифровых платформ обеспечивает возможность проведения образовательных, финансовых и административных операций независимо от территориального расположения участников взаимодействия. Однако масштабное использование электронных сервисов влечет рост угроз, связанных с неправомерным доступом к информации и вмешательством в автоматизированные системы. Поэтому вопросы защиты данных приобретают характер правового и организационного приоритета, требующего постоянного развития средств предотвращения киберпреступлений[2].

---

[1] Косенков А.Ю. Цифровизация в ракурсе философских исследований: новые угрозы и способы их преодоления // Наука и инновации. – 2020. – № 11. – С. 37.

[2] Громыко А.А., Солтанов В.Р. Цифровая трансформация общества, цели и стратегии // Современные тенденции развития науки и мирового сообщества в эпоху цифровизации:

Расширение цифровой среды невозможно без повышения уровня подготовленности пользователей, способных профессионально и ответственно обращаться с цифровыми ресурсами. Необходимое условие успешного функционирования цифровой экономики и развития дистанционных форм занятости – система обучения и популяризации навыков работы с технологиями.

Экономические процессы также претерпевают существенные изменения: электронная торговля, автоматизация операций, использование больших массивов данных становятся основой формирования новой модели хозяйственной деятельности. Результатом является появление дополнительных рынков занятости, развитие предпринимательских инициатив и внедрение инновационных технологических решений.

Развитие вычислительной техники и телекоммуникационных сетей привело к тому, что информационные процессы приобрели устойчивый трансграничный характер. Интернет и иные цифровые платформы обеспечивают постоянный и практически неограниченный обмен данными между государствами, организациями и частными лицами. В результате информационная сфера перестает быть вспомогательным элементом и превращается в одну из основных основ функционирования государственного аппарата, финансовой системы и сферы услуг.

Такая переориентация на цифровые решения потребовала формулирования целостной государственной позиции относительно обеспечения информационной безопасности. Для этих целей был принят доктринальный акт – Доктрина информационной безопасности Российской Федерации [1], в котором обобщены теоретические подходы и обозначены базовые ориентиры государственной политики в обозначенной области.

сборник материалов XIX Международной научно-практической конференции, Москва, 30 ноября 2023 года. – Москва: Алеф, 2023. – С. 351.

[1] Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 05.12.2016 № 646 // Собр. законодательства Рос. Федерации. – 2016. – № 50. – Ст. 7074.

Доктрина задала направление дальнейшего нормативного развития, обозначив круг угроз, подлежащих нейтрализации, а также общие принципы реагирования на них.

Исходя из доктринальных установок, в национальной правовой системе постепенно сформирован комплекс мер, ориентированных на регулирование обращения цифровой информации[1]. Этот комплекс включает:

– установление требований к функционированию информационных систем и сетей связи;

– регламентацию порядка передачи, хранения и обработки данных;

– определение условий доступа к информационным ресурсам;

– закрепление специальных процедур осуществления оперативно-розыскных и следственных действий, проводимых в цифровой среде.

Иными словами, речь идет не только о регламентации правомерного использования цифровых технологий, но и о создании правовых механизмов выявления и пресечения противоправных деяний, совершаемых с их применением.

Несмотря на наличие такой нормативной основы, в практической плоскости наблюдается устойчивая тенденция к росту преступлений, совершаемых с использованием технических средств. Наиболее типичными инструментами являются сеть Интернет, распределенные системы передачи информации, специализированное программное обеспечение, а также вредоносные программы, направленные на нарушение функционирования компьютерных систем или несанкционированный доступ к данным. Подобные посягательства затрагивают как частные, так и публичные интересы, а в отдельных случаях могут оказывать воздействие на геополитическую

[1] Лобач Д.В. Развитие российского уголовного законодательства в сфере противодействия преступлениям, совершаемым в сети Интернет // Уголовное право: стратегия развития в XXI веке. – 2023. – № 3. – С. 23.

устойчивость и международную безопасность [1] . Таким образом, технологический прогресс одновременно создает условия для модернизации управления и открывает новые возможности для криминальной деятельности.

Широкое внедрение цифровых объектов в сферу управления, финансовый оборот и хозяйственную деятельность в целом приводит к тому, что появляются новые модели преступного поведения, не всегда вписывающиеся в традиционные уголовно-правовые конструкции. Даже при наличии сложившейся системы норм, регулирующих общественные отношения в сфере цифровой информации, происходит расширение перечня составов преступлений, связанных с использованием современных технологий [2] . Законодатель вынужден учитывать эволюцию способов совершения противоправных деяний и адаптировать к ним применяемые меры уголовно-правового воздействия.

В рассматриваемой ситуации особую нагрузку несет государство как субъект, обязанность которого состоит в обеспечении защиты информационной сферы и национальных интересов в данной области. В публичных заявлениях Президент Российской Федерации В. В. Путин не раз обращал внимание на необходимость выстраивания такой системы регулирования, при которой обработка персонализированных цифровых данных граждан не превращается в инструмент произвольного вмешательства в их частную и экономическую жизнь. В частности, подчеркивалось, что банковские и иные коммерческие структуры не должны обладать неограниченным доступом к полному объёму сведений о гражданах. Подобное ограничение направлено на снижение рисков злоупотреблений со стороны участников экономического оборота.

Вместе с тем статистика преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, за 2023 и 2024 годы

---

[1] Захарцев С.И., Сальников В.П., Алексанин А.С. Оперативно-розыскная деятельность и информационная безопасность как часть военной безопасности России // Известия Российской академии ракетных и артиллерийских наук. – 2018. – № 2(102). – С. 103.

[2] Ровина Е.Е., Гурьянова З.З. Компьютерные преступления вчера и сегодня // Научный дайджест Восточно-Сибирского института МВД России. – 2022. – № 3(17). – С. 83.

показывала рост, а в 2025 г. их количество пошло на спад[1]. Вместе с тем уровень таких преступлений остается критично высоким: почти половина таких преступлений (48,2%) относится к категориям тяжких и особо тяжких (369,3 тыс.; +7,8%), четыре преступления из пяти (84,8%) совершаются с использованием сети «Интернет» (649,1 тыс.; +23,2%), почти половина (45,2%) – средств мобильной связи (346,0 тыс.; +14,3%). Почти две трети таких преступлений (63,5%) совершается путем кражи или мошенничества: 486,3 тыс. (+2,3%), почти каждое восьмое (12,4%) – с целью незаконного производства, сбыта или пересылки наркотических средств: 94,6 тыс. (+16,1%).

Это свидетельствует о том, что наличие доктринальных актов и развитой нормативной базы само по себе не обеспечивает нейтрализацию криминогенного потенциала цифровой среды. Государство вынуждено не только совершенствовать правовое регулирование, но и развивать специализированные механизмы уголовно-правового противодействия, включая криминализацию новых форм деяний, совершаемых с использованием информационных технологий, а также усиливать профилактические меры, ориентированные на снижение уязвимости информационной инфраструктуры и защиту прав граждан.

В криминологическом анализе цифровой преступности наибольший интерес представляют не только абсолютные показатели, но и структурные изменения. Начиная с марта 2022 г. фиксируется снижение числа зарегистрированных эпизодов несанкционированного списания денежных средств с банковских карт. Это падение коррелирует с серьёзными трансформациями платёжного ландшафта: ограничением работы на территории Российской Федерации международных платёжных систем Visa и Mastercard, прекращением функционирования ряда сервисов бесконтактной оплаты (Google Pay, Samsung Pay и др.), а также отзывом лицензий у отдельных кредитных

[1] Министерство внутренних дел Российской Федерации. Сводный обзор 2024 года. Доклад о состоянии преступности и результатах работы органов внутренних дел Российской Федерации [Электронный ресурс]. – URL: https://мвд.рф/reports/item/60248328/ (дата обращения: 16.11.2025).

организаций Центральным банком России[8]. В результате сузился массив операций, проводимых с использованием инфраструктуры, традиционно эксплуатируемой преступниками, что повлекло перераспределение криминальной активности.

Однако рассматривать официальную статистику как исчерпывающий источник при оценке преступности в сфере цифровой информации было бы методологически неверно. Такие данные выполняют преимущественно ориентирующую функцию: позволяют обнаружить общие тенденции, оценить распространённость отдельных видов посягательств, выделить территории концентрации преступной активности и наметить направления профилактики. Вместе с тем высокая латентность цифровых преступлений, сложность их выявления и фиксации, трансграничный характер каналов совершения неизбежно приводят к неполному отражению реального объёма противоправного поведения.

На искажение статистической картины воздействует совокупность причин. Потерпевшие не всегда обращаются в правоохранительные органы. Иногда речь идёт о небольшом размере ущерба, иногда – о недоверии к возможности установить виновных и добиться возмещения. К этому добавляется позиция организаций, владеющих информационными системами. Новые маркетплейсы, службы доставки и другие сервисы, стремясь быстро выйти на рынок, не всегда выстраивают полноценную систему защиты данных. Утечки персональной информации могут происходить как в результате внешнего вмешательства, так и вследствие нарушения режимов обработки со стороны сотрудников. При этом сведения о таких инцидентах нередко остаются внутри компании: руководство опасается репутационных потерь и ограничивается внутренними мерами. Граждане, в свою очередь, нередко предпочитают не вовлекаться в длительные процедуры, связанные с уголовным преследованием, если последствия происшествия воспринимаются как несущественные. В научных работах вполне обоснованно говорится о том, что значительная часть преступлений, совершаемых в сети Интернет, так и не

переходит в плоскость официального учёта, «теряясь» в массиве электронных коммуникаций.

При таких условиях статистические сведения логично воспринимать как сигнальную систему. Они указывают на появление новых моделей преступного поведения, позволяют зафиксировать изменения в структуре посягательств, но не могут служить единственным основанием для выводов о реальных масштабах цифровой преступности. Вместе с тем эта информация востребована при разработке документов в сфере национальной и информационной безопасности, при формировании стратегий предупреждения и пресечения соответствующих деяний.

Особенно наглядно уязвимость цифровой среды проявилась в период пандемии COVID-19. Введение ограничений на передвижение населения и быстрый переход на дистанционные формы работы привели к ускоренной цифровизации ключевых сфер жизни. Образовательные организации, медицинские учреждения, органы социальной защиты, торговые и финансовые структуры в краткие сроки перевели значительную часть процессов в онлайн-форматы. Это означало резкое увеличение объёма обрабатываемых и хранимых данных, концентрацию чувствительной информации в информационных системах различного уровня.

Преступная среда отреагировала на эти изменения оперативно. Цифровые ресурсы стали рассматриваться как удобная цель: доступ к базам данных, каналам электронной связи, платёжным сервисам обеспечивал возможности для хищений, шантажа, нарушения функционирования отдельных элементов инфраструктуры. С 2019 г. в разных странах зафиксирован ряд показательных инцидентов. В Аргентине при атаке на государственный банк данных злоумышленники получили полный массив сведений, связанных с удостоверениями личности граждан. В Греции в результате воздействия на информационные системы в городе Салоники была серьёзно нарушена работа налоговых органов, что отразилось и на транспортной сфере. Российская

практика демонстрирует использование интернет-торговых площадок для неправомерного доступа к персональным данным с применением ботнетов.

Эти примеры подчёркивают ещё одну важную особенность – преступления в цифровой сфере редко укладываются в рамки одной юрисдикции. Трассировка вредоносного трафика, установление лиц, управляющих ботнетами или распространяющих вредоносное программное обеспечение, как правило, требует международного сотрудничества. Показательно дело, в рамках которого взаимодействие правоохранительных органов России и США позволило получить информацию о деятельности хакерской группы и в итоге пресечь её деятельность на территории Российской Федерации[1]. Это демонстрирует, что без комплексного, межгосударственного подхода борьба с цифровой преступностью неизбежно сталкивается с серьёзными ограничениями.

Существенные изменения происходят и в самой структуре преступных посягательств. Те схемы, которые ещё недавно доминировали в экономической преступности – финансовые пирамиды, рейдерские захваты, – постепенно уступают место более сложным конструкциям, основанным на использовании современных IT-технологий [2] . Применяются вредоносные программные продукты, эксплуатируются уязвимости в программном обеспечении, создаются распределённые сети, предназначенные для анонимизации действий. Преступник всё чаще опирается не на прямое физическое воздействие, а на дистанционное манипулирование информацией и техническими системами.

В эту картину органично вписывается стремительное развитие технологий искусственного интеллекта. Ряд исследователей отмечает, что распространение ИИ по масштабу последствий сопоставимо с крупными

---

[1] Серебренникова А.В. Цифровая криминалистика и ее значение для расследования преступлений // International Law Journal. – 2019. – Т. 2. – № 4. – С. 127.

[2] Суворова В.В., Суворова Л.А. Совершение преступлений с использованием социальной инженерии: постановка проблемы // Теория и практика приоритетных научных исследований: сборник научных трудов по материалам VIII Международной научнопрактической конференции, Смоленск, 13 августа 2019 года. – Смоленск: МНИЦ «Наукосфера», 2019. – С. 72.

технологическими сдвигами прошлого, затрагивая способы организации производства, управления и коммуникации[1]. Тот же механизм работает и в криминальной сфере. Алгоритмы, способные анализировать большие массивы данных, имитировать поведение пользователей, генерировать контент, пригодный для мошеннических схем, создают дополнительные возможности для злоумышленников. Право и институты обеспечения безопасности не всегда успевают адаптироваться к новым формам угроз[2].

Результат уже очевиден на уровне повседневной практики. Увеличивается количество преступлений, связанных с несанкционированным доступом к информационным системам, фишинговыми рассылками, распространением вредоносного программного обеспечения. На отдельном месте – операции с криптовалютами. Псевдоанонимный или анонимизированный характер многих транзакций в этой сфере создаёт благоприятную среду для сокрытия доходов, полученных преступным путём, и существенно осложняет работу правоохранительных органов по их обнаружению и блокированию.

Современная практика противодействия преступлениям в цифровой сфере убедительно демонстрирует, что усиление технических средств защиты не устраняет главную уязвимость – человеческий фактор. Чем более сложными становятся программные и аппаратные барьеры, тем настойчивее преступники обращаются к методам психологического воздействия. Социальная инженерия (СИ) в этом смысле выступает особой формой компьютерной преступности, при которой объектом воздействия становится не программный код, а поведение человека.

В основе СИ лежит эксплуатация доверия, неосведомлённости или невнимательности лица. Злоумышленник создаёт ситуацию, в которой адресат сам передаёт конфиденциальные данные, вводит реквизиты банковской карты,

---

[1] Серебренникова А.В. Указ. соч. – С. 126.

[2] Колин К.К. Цифровая революция и искусственный интеллект: новые горизонты и опасности // Партнерство цивилизаций. – 2020. – № 1-2. – С. 103.

сообщает коды подтверждения или совершает действия с носителями информации. При этом внешняя оболочка коммуникации – логотипы банков, имена сотрудников, оформление письма – воспроизводит привычные для пользователя формы делового общения. Исследователи, несмотря на различия в формулировках, сходятся в том, что социальную инженерию следует рассматривать как деятельность, направленную на несанкционированное получение информации за счёт использования уязвимостей человеческой психики, а не программной среды[1].

Широкое распространение получили фишинговые атаки, при которых сообщения направляются от имени известных организаций и содержат ссылки на поддельные сайты или вложения с вредоносным программным обеспечением. Используются и более сложные сценарии: телефонные звонки с подменой номера, легендирование под сотрудников служб безопасности, попытки физического доступа в офисные помещения под предлогом выполнения технических работ. Эффект «разбросанных носителей», когда USB-устройства с вредоносным программным обеспечением сознательно оставляются в местах общего пользования, по-прежнему срабатывает: подключая такой носитель к рабочему компьютеру, сотрудник фактически открывает злоумышленнику доступ к внутренней сети. Последствия подобных действий выражаются не только в утечке отдельных файлов, но и в компрометации массивов данных, блокировании работы информационных систем, прямых финансовых потерях и нарушении деловой репутации организации.

На этом фоне технологическое развитие усиливает противоправный потенциал цифровой среды. Как справедливо отмечают Е. В. Виноградова и С. И. Захарцев, современные технологические достижения, включая информационные и медицинские, одновременно создают для человека новые возможности и порождают проблемы, требующие выхода права на

[1] Янгаева М.О. Социальная инженерия как способ совершения киберпреступлений // Вестник Сибирского юридического института МВД России. –2021. –№ 1 (42). –С. 135.

междисциплинарный уровень, где юридические конструкции взаимодействуют с философскими, этическими и нравственными основаниями [1]. Без такого расширения горизонта правового мышления, по мнению авторов, затруднительно выработать адекватные ответы на глобальные угрозы, формируемые в техносфере.

Особую роль в этих процессах играет искусственный интеллект. Развитие ИИ позволяет за считанные секунды выполнять операции, которые для человека требуют значительных интеллектуальных и временных затрат [2]. Нейросетевые генеративные модели создают изображения, тексты, аудио- и видеозаписи, которые трудно отличить от реальных. На этой основе сформировалось явление deepfake – синтетических материалов, визуально воспроизводящих конкретных лиц. Такие материалы могут использоваться для дискредитации отдельных личностей, давления в политических и корпоративных конфликтах, распространения дезинформации. Тем самым технологии, изначально создававшиеся как инструмент упрощения коммуникации и творчества, становятся ресурсом для криминальных практик.

Не менее проблемным оказывается и развитие систем цифровой идентификации. Биометрические методы аутентификации – по отпечаткам пальцев, изображению лица, голосу – воспринимались как более «надёжная» альтернатива паролям. Однако практический опыт показывает, что злоумышленники адаптируются и к этим механизмам: используются поддельные биометрические шаблоны, программы, имитирующие голос, технологии подмены изображения. В результате сами по себе биометрические системы без дополнительных организационных и правовых гарантий не обеспечивают необходимого уровня защиты.

---

[1] Виноградова Е.В., Захарцев С.И. Актуальные мысли о праве. – М.: Юрлит, 2023. – С. 221.

[2] Осипова И.Н. Искусственный интеллект − угроза или помощник человека? // Экономика. Общество. Человек: материалы Всероссийской научно-практической конференции с международным участием / ред. Е.Н. Чижова. Т. 1. Вып. XXXVII. – Белгород: Белгородский государственный технологический университет им. В. Г. Шухова, 2019. – С. 180.

Стремительное расширение Интернета вещей создаёт ещё один пласт уязвимостей. Подключённые к сети датчики, камеры, элементы «умного дома», производственное оборудование и транспортные средства, при недостаточном уровне защиты, превращаются в точки доступа к сетям организаций и частных лиц. Киберпреступные группировки формируют сложные цепочки проникновения: через мало защищённые устройства они выходят к более ценным ресурсам, используя распределённые сети и скрытые каналы связи. Коммуникация между участниками таких групп происходит преимущественно в закрытых мессенджерах, что затрудняет их идентификацию и документирование.

На этом фоне становится очевидным, что правоприменительная практика в сфере борьбы с IT-преступностью не всегда успевает за скоростью технологических изменений. Методы расследования, алгоритмы реагирования, а также нормативное регулирование зачастую основываются на модельных ситуациях, которые уже устарели. Это побуждает пересматривать подходы как на уровне теории, так и в оперативно-следственной работе.

Противодействие социально-инженерным и иным цифровым атакам требует сочетания технических, организационных и правовых средств. Важнейшее направление – формирование у пользователей устойчивых навыков безопасного поведения в сети: умения критически оценивать поступающую информацию, распознавать типичные схемы обмана, соблюдать правила обращения с персональными и финансовыми данными. Необходимы систематические обучающие мероприятия, тестирование персонала, выработка в организациях понятных и жёстких регламентов работы с информацией, внедрение многофакторной аутентификации и механизмов оперативного уведомления о подозрительных действиях. Показательной в этом плане является деятельность Центрального банка Российской Федерации, который отслеживает новые мошеннические схемы, анализирует их и проводит широкую информационную кампанию, разъясняя населению характер угроз и способы защиты.

Тем не менее наблюдаемое в обществе отношение к цифровой безопасности остаётся противоречивым. Значительная часть пользователей по-прежнему использует простые пароли, безразлично относится к запросам о передаче персональных данных, переходит по ссылкам из писем, не проверяя их подлинность [1]. Это создаёт благоприятные условия для расширения цифровой преступности. В итоге ущерб, причиняемый такими деяниями, выходит за рамки частных случаев: подрывается доверие к цифровым сервисам, возникают риски для устойчивости финансовой системы и отдельных элементов управления. Наличие статистически подтверждаемого роста преступлений, связанных с цифровой информацией, а также их проникновение в новые сферы общественной жизни свидетельствуют о необходимости дальнейшего развития правовых средств реагирования и системной профилактической работы.

В российской уголовно-правовой науке и правоприменительной практике достаточно устойчивым стало разграничение понятий IT-преступлений и ИТТ-преступлений, поскольку речь идёт о различных по своей природе формах противоправного поведения, требующих неодинаковых подходов к квалификации и доказыванию.

Под IT-преступлениями обычно понимают деяния, при которых объектом посягательства выступают компьютерная информация, программные средства, технические устройства или сам процесс функционирования информационных систем. Суть таких посягательств заключается во вмешательстве в обработку, хранение либо передачу данных, нарушении режима работы сетевых или аппаратных комплексов, создании и распространении вредоносных программных продуктов. Уголовный кодекс Российской Федерации выделяет подобные деяния в специальной главе 28 «Преступления в сфере компьютерной информации» (ст. 272, 273, 274 УК РФ), что отражает их самостоятельный характер и структуру предмета доказывания.

[1] Осипова И.Н. Указ. соч. – С. 179.

ИТТ-преступления (совершаемые с использованием информационно-телекоммуникационных технологий) имеют иную природу: цифровая среда здесь выступает не объектом воздействия, а средством и способом достижения преступного результата, направленного на совершенно другие объекты охраны – собственность, общественную безопасность, порядок управления, конституционные права граждан и т. д. Типичным примером служит мошенничество, предусмотренное ст. 159^6 УК РФ. Компьютерная система, сеть или цифровой сервис в таких случаях только обеспечивают выполнение обманных действий, тогда как реальный вред причиняется имущественным отношениям и субъектам гражданского оборота.

Смысл различия сводится к тому, что:

- в IT-преступлениях воздействие направлено на информацию либо систему её обработки;

- в ИТТ-преступлениях информационно-телекоммуникационные технологии используются как инструмент совершения преступления в иной сфере правоотношений.

Такое разграничение имеет не только теоретическое, но и практическое значение: оно определяет состав преступления, предмет доказывания, квалификационные признаки и пределы уголовной ответственности. Для IT-преступлений требуется установить факт вмешательства в информационную инфраструктуру и последствия такого воздействия; в делах же об ИТТ-преступлениях первостепенным является доказательство фактов хищения, обмана или получения доступа к ценностям – материальным либо нематериальным.

Стремительное технологическое развитие не только облегчает повседневную жизнь, но и объективно расширяет арсенал средств, которыми располагают лица, совершающие мошенничества. По мере совершенствования цифровых инструментов меняются способы совершения хищений, появляются новые комбинации традиционных и инновационных приёмов обмана, усложняется структура преступной деятельности. Мошенничество в этих

условиях выступает не статичной конструкцией, а постоянно изменяющимся феноменом, приспосабливающимся к экономическим, социальным и технологическим условиям[1].

Криминологический и уголовно-правовой анализ позволяет выделять множество оснований для классификации мошенничества: по сфере совершения (банковская, страховая, потребительская, цифровая и др.), по месту (в физическом пространстве, в сети Интернет, в смешанной форме), по механизму преступного воздействия (злоупотребление доверием, использование подложных документов, манипуляция информацией, эксплуатация уязвимостей цифровой инфраструктуры), по объекту посягательства (имущество граждан, денежные средства организаций, права требования и т. п.). Неудивительно, что перечень разновидностей мошенничества постоянно расширяется: каждая новая технологическая платформа, платёжный сервис или коммуникационный канал становится потенциальной основой для формирования новой схемы обмана.

С переходом к индустриальному обществу и последующим этапом цифровой трансформации мошенничество фактически вышло на иной уровень. Массовое распространение персональных компьютеров, подключение всё большего числа пользователей к глобальной сети, развитие электронной коммерции привели к тому, что интернет и иные цифровые каналы коммуникации из вспомогательного инструмента превратились в среду, в которой разворачивается значительная часть мошеннических схем. Интернет как глобальная коммуникационная инфраструктура объединяет сети разных государств, регионов и организаций, что делает возможным совершение посягательств в отношении потерпевших, территориально находящихся в иных государствах, при минимальных затратах для самого преступника. По мере

[1] Баубекова Ж., Носова Е.С., Кабанова Н.А. Мошенничество: социальное влияние и роль цифровых технологий в его распространении // Вестник евразийской науки. – 2024. – Т. 16, № S1.

роста числа пользователей и объема онлайн-операций мошенники закономерно переносят свою активность в цифровое пространство[1].

Вместе с распространением сети и развитием электронных платёжных и торговых систем на первый план выдвинулась проблема киберпреступности. Кибермошенничество из эпизодического явления превратилось в массовую форму преступности, создающую серьёзные угрозы как для отдельных граждан, так и для финансового сектора, систем государственного управления и корпоративной среды. Лица, осуществляющие такие деяния, постоянно адаптируют свои методы: комбинируют технические и психологические приёмы, используют анонимизацию трафика, применяют специализированные программные средства, эксплуатируют пробелы в цифровой грамотности населения.

К числу распространённых механизмов кибермошенничества относятся фишинг, неправомерные операции с банковскими картами, кража персональных данных, а также различные формы злоупотребления электронными платёжными средствами. Объединяет их общая направленность: завладение финансовыми ресурсами или конфиденциальной информацией пользователей, которая впоследствии может монетизироваться либо использоваться для иных преступных целей[2].

Фишинг представляет собой один из наиболее типичных примеров. При данных схемах злоумышленник имитирует надёжный источник – банк, государственный орган, известную коммерческую организацию, социальную сеть – и формирует у адресата ложное чувство доверия. Сообщение может поступать по электронной почте, через мессенджер, в социальной сети и сопровождаться ссылкой на поддельный сайт либо вложением с вредоносным программным обеспечением. Адресата побуждают перейти по ссылке, ввести

---

[1] Шалагин А.Е., Идиятуллов А.Д. Трансформация преступности в XXI веке: особенности предупреждения и противодействия // Вестник Казанского юридического института МВД России. – 2021. – Т. 12, № 2(44). – С. 227.

[2] Намысов Е.Д. Мошенничество в цифровую эпоху в связи с общественными изменениями // Криминологический журнал. – 2023. – № 3. – С. 150.

реквизиты банковской карты, логин и пароль от «личного кабинета», подтвердить якобы срочную операцию. В ряде случаев вредоносное приложение устанавливается на устройство автоматически при открытии файла, после чего конфиденциальная информация становится доступна преступнику. В современных условиях такие рассылки всё чаще формируются с использованием нейросетевых моделей: тексты и интерфейсы сайтов становятся более убедительными, стилистически приближенными к официальным ресурсам, что затрудняет их распознавание рядовым пользователем.

Отдельного внимания заслуживает блок преступлений, связанных с банковскими картами. По мере распространения безналичных платежей и самообслуживающих устройств (банкоматов, терминалов) сформировался устойчивый массив мошеннических схем, базирующихся на копировании реквизитов карты и использовании их для дальнейших незаконных операций. Одним из устойчивых технических приёмов является скимминг. Под ним понимают установку на банкомат (или терминал) специального устройства, считывающего информацию с магнитной полосы карты при её вводе в приёмник. Такие устройства могут быть изготовлены кустарным способом и визуально почти не отличаться от штатных элементов банкомата. Полученные данные позволяют создавать дубликаты карт или осуществлять удалённые транзакции без физического предъявления оригинала. Дальнейший оборот этих сведений включает их продажу на теневых площадках, передачу иным участникам преступных групп, использование в транснациональных схемах хищения денежных средств.

Часто скимминг сочетается с применением скрытых видеокамер или иных средств фиксации, позволяющих записать вводимый клиентом ПИН-код. Камеры маскируются в корпусе банкомата, в нависающих конструкциях, в дополнительных панелях. При наличии и реквизитов карты, и ПИН-кода злоумышленник получает фактически полный доступ к находящимся на счёте денежным средствам. Масштаб последствий подобных схем подтверждается

многими статистическими обзорами: ежегодно миллионы пользователей по всему миру сталкиваются с неправомерным списанием средств или иным использованием их платёжных данных[1].

Несмотря на развитие технических методов, сохраняют актуальность и более «традиционные» формы обмана, адаптированные к современным условиям. Одной из таких схем остаются телефонные звонки от лиц, представляющихся «сотрудниками службы безопасности банка». Типичный сценарий строится на создании у адресата ощущения немедленной угрозы: ему сообщают о якобы совершаемой крупной операции, предлагается «срочно» предотвратить списание, для чего необходимо назвать реквизиты карты, коды из поступающих SMS-сообщений, CVV-код и другие сведения. В действительности именно предоставление этой информации и даёт преступнику возможность выполнить операции с картой в интересах себя или третьих лиц. Несмотря на широкую информационную кампанию и многократное разъяснение населению опасности такого общения, значительное количество граждан продолжает поддаваться подобным воздействиям, что свидетельствует о сохраняющемся разрыве между техническими средствами защиты и реальным поведением пользователей[2].

Все указанные схемы демонстрируют общий тренд: мошенничество активно использует преимущества цифровой среды, а также психологические и организационные слабости её участников. Технологии, призванные ускорить и упростить экономический оборот, при отсутствии надлежащих навыков безопасного поведения и эффективного институционального контроля превращаются в удобную площадку для преступной деятельности. На этом фоне задача уголовного закона и правоприменения состоит не только в квалификации уже совершённых деяний, но и в выработке адекватных

[1] Струков А.Е. Понятие и способы мошенничества // Вестник магистратуры. – 2022. – № 1-2(124). – С. 10.
[2] Струков А.Е. Указ. соч. – С. 11.

подходов к оценке новых моделей мошенничества, которые возникают на стыке технических инноваций и классических схем обмана.

Мошенничество, будучи формально отнесённым к преступлениям против собственности, по своим последствиям выходит далеко за рамки имущественных отношений. Масштабная распространённость таких деяний, их способность быстро «подстраиваться» под экономические и технологические изменения делают мошенничество фактором, влияющим на состояние социального доверия и устойчивость общественных институтов.

Прежде всего затрагивается восприятие гражданами деятельности органов публичной власти. Сообщения о коррупционных схемах, злоупотреблениях при распределении бюджетных средств, участии должностных лиц в сомнительных финансовых операциях воспринимаются как доказательство того, что сама государственная система подвержена мошенничеству. При отсутствии убедительной реакции со стороны компетентных органов формируется убеждение в избирательности применения закона, что подрывает веру в государство как гаранта прав и свобод.

Наряду с этим мошенничества отражаются на оценке работы судебной системы. Если решения по отдельным делам о хищениях и злоупотреблениях воспринимаются как несправедливые, недостаточно мотивированные или заведомо «формальные», граждане делают вывод о неспособности судов обеспечить надлежащую защиту интересов потерпевших. В таких условиях снижается готовность использовать судебные механизмы, усиливается склонность к поиску обходных, в том числе неформальных способов разрешения конфликтов.

Финансовый сектор испытывает на себе непосредственное давление мошеннических схем. Хищения со счетов, неправомерные транзакции по банковским картам, использование поддельных платёжных инструментов, утечка персональных и платёжных данных – всё это подрывает уверенность клиентов и инвесторов в устойчивости и надёжности кредитных организаций. Граждане начинают ограничивать своё взаимодействие с банками,

отказываются от использования ряда цифровых сервисов, предпочитают хранить средства в наличной форме или в минимально «цифровизированных» инструментах. Для финансовой системы такие процессы оборачиваются сжатием ресурсной базы, сокращением инвестиционной активности и ростом издержек на обеспечение безопасности.

Аналогичные тенденции прослеживаются и в сфере цифровой экономики. Распространённость мошенничества в онлайн-торговле, при дистанционной оплате товаров и услуг, в работе электронных платформ приводит к тому, что часть пользователей переходит к осторожной модели поведения: они либо снижают объём операций, либо вовсе отказываются от участия в электронных сделках. Тем самым тормозится развитие цифровых сервисов, ослабляются эффекты от внедрения электронных платёжных и торговых систем.

Правоохранительные органы оказываются в сложном положении: с одной стороны, именно на них возлагается задача выявления и расследования мошенничеств, с другой – высокая латентность таких преступлений и объективные трудности их раскрытия создают в общественном сознании впечатление неэффективности принимаемых мер. Если значительная часть обращений граждан не приводит к быстрому и ощутимому результату, формируется установка о «бесполезности» обращения в полицию. Это подрывает авторитет правоохранительных органов и ослабляет взаимодействие граждан с системой уголовной юстиции.

Особый пласт последствий связан с внутригрупповым и межличностным доверием. В тех случаях, когда жертвами мошенничества становятся представители определённых национальных, религиозных или иных групп, либо когда сами преступники маскируются под «своих» по отношению к потерпевшим, возникают дополнительные зоны напряжённости. Люди начинают более настороженно относиться к предложениям о совместных проектах, коллективных финансовых вложениях, благотворительных инициативах, даже если они исходят изнутри общности. Это снижает уровень

солидарности, усложняет поддержание традиционных форм взаимопомощи, ослабляет способность группы к самоорганизации.

В совокупности мошенничество формирует фон недоверия, в котором исходная презумпция добросовестности участника взаимодействия постепенно вытесняется ожиданием обмана. Последствия проявляются на различных уровнях:

– в межличностной сфере – в виде роста подозрительности и замкнутости;

– в институциональной плоскости – в виде снижения доверия к государственным органам, судам, финансовым и иным организациям;

– в экономике – в виде осторожности инвесторов и потребителей, уменьшения готовности пользоваться цифровыми сервисами;

– в социокультурной сфере – в виде ослабления внутригрупповых связей и изменения системы ценностных ориентиров.

В этих условиях противодействие мошенничеству должно рассматриваться не только как задача уголовного преследования, но и как направление государственной социальной политики. Требуется сочетание нескольких блоков мер: совершенствование уголовно-правовых составов и санкций; повышение качества расследования и судебного разбирательства по делам о мошенничестве; развитие механизмов финансового и цифрового просвещения населения; формирование прозрачных стандартов деятельности органов власти и бизнеса. Только при условии системного подхода возможно не только снижать уровень мошенничества, но и восстанавливать подорванное доверие, без которого устойчивое развитие общества и экономики оказывается затруднительным.

Эффективность уголовно-правовых мер в сфере противодействия мошенничеству остаётся предметом серьёзных дискуссий. Нормы, сформированные в период доминирования традиционных форм экономических отношений, изначально ориентировались на ситуации непосредственного контакта между преступником и потерпевшим, использование подложных

документов, инсценировок либо злоупотребление личным доверием. Однако развитие цифровых технологий радикально изменило модель преступного поведения: хищения всё чаще совершаются дистанционно, в распределённых информационных системах, где средства и способы обмана существенно отличаются от классических. В результате уголовный закон, детально регламентирующий «офлайновые» варианты обманных действий, нередко оказывается недостаточным для адекватного реагирования на современные угрозы.

Серьёзное затруднение вызывает изменение объекта преступного посягательства. Помимо традиционного имущества и денежных средств, в сферу преступного интереса включены персональные данные, идентификаторы доступа, цифровые профили, криптоактивы. Хищение в ряде случаев осуществляется без контакта с материальным носителем имущества и даже без участия потерпевшего, посредством автоматизированных процессов. При такой модели действия нормы о мошенничестве, ориентированные на классическое злоупотребление доверием, оказываются формально неприменимыми либо позволяют использовать неоднозначные конструкции квалификации.

Не менее проблемным является вопрос доказывания. Использование анонимизирующих инструментов, зарубежных серверов, виртуальных телефонных номеров и специальных программ существенно осложняет установление исполнителя и маршрутов движения похищенных средств. Многие цифровые следы исчезают в короткие сроки, а их фиксация требует специальной технической подготовки и оборудования. Следственные подразделения, действующие в рамках классических процессуальных процедур, не всегда обладают необходимыми ресурсами для работы с подобного рода доказательствами.

Ситуацию усугубляет высокая латентность цифровых мошенничеств. Потерпевшие, особенно в сфере бизнеса, предпочитают не обращаться в правоохранительные органы из боязни репутационных потерь или из-за малого размера ущерба. Это приводит к искажению официальной статистики и

снижению информированности о масштабах проблемы, что, в свою очередь, влияет на государственную политику в данной сфере.

Значительную роль играет и трансграничность таких деяний. Множество схем основывается на использовании инфраструктуры, расположенной за пределами Российской Федерации. Уголовная юрисдикция в этих условиях сталкивается с объективными ограничениями: запросы правовой помощи требуют длительного времени, а сотрудничество не всегда возможно из-за различий правовых режимов и интересов государств.

Отставание законодательства от темпов технологического развития выявляется особенно отчётливо. Создание и принятие нормативных актов требует длительных процедур согласования, тогда как новые преступные схемы возникают и исчезают за считанные месяцы. В результате правоприменение вынуждено опираться на расширительное толкование отдельных норм о мошенничестве либо на квалификацию по смежным составам, что порождает правовую неопределённость.

Нельзя не учитывать и кадровый фактор. Уровень цифровой подготовки работников следственных органов, судов и экспертов далеко не всегда соответствует сложности современных преступных схем. Население, в свою очередь, часто не обладает навыками безопасного поведения в сети, что облегчает реализацию преступных намерений. Разрыв в уровне компетенций между преступниками и лицами, призванными противодействовать их деятельности, объективно снижает результативность уголовно-правовых механизмов.

Одновременно с указанными изменениями с 2022 г. обозначился ещё один фактор, повлиявший на рост рисков в цифровой среде: проведение специальной военной операции и связанное с этим увеличение числа добровольческих инициатив, онлайн-сборов и обращений за помощью. Повестка поддержки военнослужащих, гуманитарных поставок, лечения раненых и помощи семьям приобрела высокую эмоциональную значимость, что сделало её удобной для злоупотребления доверием в интернете. На практике

это привело к распространению мошеннических «историй» и обращений, внешне похожих на благотворительные кампании, но фактически направленных на хищение денег и (или) получение доступа к банковским реквизитам и учётным записям пользователей.

Наиболее типичные варианты выглядят следующим образом: (1) создание фишинговых страниц «фондов» и «волонтёрских штабов» со сбором пожертвований, где реквизиты незаметно подменяются либо у потерпевшего выманиваются платёжные данные; (2) рассылка сообщений о якобы обязательном «взносе на поддержку СВО» с предложением «отменить списание» через ссылку на поддельный банковский ресурс; (3) запуск сайтов-двойников, предлагающих участникам СВО и членам их семей «выплаты», «компенсации» или «финансовую помощь» при условии регистрации и ввода персональных данных (иногда – под видом «инвестпрограммы»); (4) адресные звонки и сообщения родственникам военнослужащих от имени «военкомата», «командира» или «уполномоченного органа» с просьбой сообщить код из SMS – под предлогом оформления «выплаты», «награды» или «записи», после чего злоумышленники получают доступ к аккаунтам и совершают хищения.

Эти примеры показывают, что динамика ITT-мошенничеств зависит не только от уровня цифровизации и технических уязвимостей, но и от социального контекста. Резонансные события порождают массовый поток сборов, объявлений и просьб о помощи, и тем самым расширяют пространство доверия, которое преступники используют в дистанционных коммуникациях.

§ 2. Ответственность за мошенничество, совершенное с использованием информационных технологий, в зарубежных странах

В зарубежных правопорядках ответственность за мошенничества, совершаемые посредством информационных технологий, формировалась постепенно и не является однородной. Различия связаны как с историческими особенностями отдельных систем, так и с темпами цифровой трансформации экономики и финансовых рынков. Однако практически во всех развитых государствах наблюдается общая тенденция: использование информационно-телекоммуникационных технологий при совершении хищений рассматривается как обстоятельство, существенно повышающее степень общественной опасности, и влечёт ужесточение уголовно-правового воздействия.

В Соединённых Штатах регулирование компьютерного мошенничества и преступлений, связанных с цифровыми технологиями, базируется на федеральном законодательстве. Одним из центральных нормативных актов является Computer Fraud and Abuse Act[1] (CFAA, 18 U.S.C. §1030), который устанавливает ответственность за неправомерный доступ к компьютерным системам, за хищение данных и использование технологий в целях получения имущественной выгоды. Применение CFAA не ограничивается территорией США: закон допускает экстерриториальную юрисдикцию, если преступные действия затрагивают компьютерные системы, функционирующие на территории страны. При квалификации хищений используются также нормы о мошенничестве, совершённом посредством средств связи (wire fraud), что позволяет рассматривать цифровые схемы как разновидность традиционного мошенничества. Применяемые санкции достаточно суровы: в зависимости от

[1] United States. Computer Fraud and Abuse Act (CFAA). 18 U.S.C. § 1030. Закон США от 16 октября 1986 г. № 99-474. – URL: https://www.law.cornell.edu/uscode/text/18/1030 (дата обращения: 16.11.2025).

размера ущерба и организации действий преступника возможны сроки лишения свободы до десяти лет и крупные штрафы.

Для американской модели показательны две вещи: акцент на дистанционные формы мошенничества и ориентация на трансграничные схемы. Для России это напрямую связано с практическими инструментами: быстрым реагированием на движение похищенных средств (включая оперативное приостановление операций), налаженным обменом информацией с банками и цифровыми платформами, а также устойчивыми каналами получения данных по цифровым следам – доменам, аккаунтам, журналам событий, криптокошелькам – когда элементы схемы находятся в разных юрисдикциях.

В германском уголовном законодательстве компьютерное мошенничество выделено в самостоятельный состав. § 263a Strafgesetzbuch (StGB) [1] предусматривает ответственность за действия, направленные на получение имущественной выгоды путём манипулирования процессами обработки данных. Немецкий подход демонстрирует важную особенность: законодатель учитывает, что обман может быть направлен не на человека, а на электронную систему, и признаёт такие действия полноценным мошенничеством. Санкции варьируются от штрафа до лишения свободы на срок до пяти лет, а при отягчающих обстоятельствах – до десяти лет. Кроме того, § 202b и § 202c StGB устанавливают ответственность за перехват данных и подготовку к компьютерным преступлениям, что позволяет реагировать на деятельность, предшествующую самому хищению.

При заимствовании данного опыта в российских условиях это предполагает более чёткое разграничение двух типовых групп случаев: (а) социальная инженерия и введение человека в заблуждение; (б) манипуляции цифровыми процедурами – подмена реквизитов, изменение параметров платежа, имитация страниц авторизации, перехват сессий и иные способы

[1] Germany. Strafgesetzbuch (StGB). Уголовный кодекс ФРГ. § 263a «Computerbetrug». – URL: https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html (дата обращения: 16.11.2025).

влияния на ход обработки информации. Такое разделение уменьшает «перекрытие» норм и делает предмет доказывания более определённым: устанавливается либо факт обмана потерпевшего, либо факт воздействия на цифровой механизм совершения операции.

В Великобритании регулирование распределено между двумя основными законодательными актами: Fraud Act 2006[1] и Computer Misuse Act 1990 (CMA[2]). Первый рассматривает мошенничество как получение имущественной выгоды путём обмана или злоупотребления доверием, включая действия, совершаемые при помощи цифровых технологий. Второй посвящён противоправному вмешательству в работу компьютерных систем и предусматривает санкции за несанкционированный доступ и модификацию данных. Такое разделение позволяет сочетать традиционные и технологически ориентированные подходы: в зависимости от обстоятельств преступление может квалифицироваться одновременно по обоим актам. Судебная практика демонстрирует тенденцию к ужесточению наказаний, особенно в случаях, когда причинён значительный вред финансовой системе или использованы сложные схемы анонимизации.

Для российской практики это означало бы необходимость последовательно отрабатывать вопросы совокупности и разграничения между ст. 159[6] и ст. 272–274 УК РФ, чтобы при наличии реального вмешательства в систему оно получало самостоятельную уголовно-правовую оценку.

Анализ зарубежных подходов показывает ряд общих черт. Во-первых, использование информационных технологий рассматривается как квалифицирующий фактор. Во-вторых, большинство государств стремится создать правовые механизмы, позволяющие преследовать действия, совершённые из-за рубежа, что отражает трансграничный характер цифровых

[1] United Kingdom. Fraud Act 2006. Act of Parliament (c 35). Принят 8 ноября 2006 г., вступил в силу 15 января 2007 г. – URL: https://www.legislation.gov.uk/ukpga/2006/35/contents (дата обращения: 16.11.2025).

[2] United Kingdom. Computer Misuse Act 1990 (CMA). Act of Parliament (c 18). Закон Великобритании об ответственности за несанкционированный доступ к компьютерам. – URL: https://www.legislation.gov.uk/ukpga/1990/18/contents (дата обращения: 16.11.2025).

преступлений. В-третьих, уголовная ответственность нередко дополняется гражданско-правовыми и административными механизмами, включая конфискацию активов, блокировку доменных имён, ограничение доступа к сетевым ресурсам и расширение обязанностей финансовых организаций по мониторингу операций.

Таким образом, зарубежный опыт демонстрирует, что эффективная борьба с мошенничествами, совершаемыми при помощи информационных технологий, требует сочетания специальных уголовных составов, гибких процессуальных механизмов и развитых средств международного сотрудничества. В отличие от традиционных форм мошенничества, где центральным элементом является межличностный обман, современные цифровые схемы основаны на сложных технологических и организационных конструкциях, что требует переосмысления подходов к уголовно-правовой квалификации и расследованию. Сравнительный анализ зарубежных правовых систем подтверждает необходимость постоянного обновления законодательства и расширения компетенций органов правопорядка, поскольку преступники используют технологические решения значительно быстрее, чем государственные системы успевают адаптироваться к новым угрозам.

В итоге можно перенять следующий зарубежный опыт: (1) более точная настройка состава цифрового мошенничества с выделением ситуаций, где ключевым является вмешательство в обработку данных и цифровые процедуры; (2) выверенная практика совокупности и разграничения мошенничества и компьютерных посягательств при наличии технического вмешательства; (3) усиление процессуальных и организационных механизмов, без которых уголовно-правовые запреты работают слабо, – оперативное приостановление и блокировка транзакций, конфискационные инструменты, стандарты взаимодействия с банками и платформами, а также механизмы получения цифровых доказательств по трансграничным каналам. Такое сочетание мер даёт наибольший эффект и может быть реализовано без пересмотра базовой структуры УК РФ.

ГЛАВА 2. УГОЛОВНО-ПРАВОВОЙ АНАЛИЗ МОШЕННИЧЕСТВ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

§ 1. Объективные признаки мошенничеств, совершенных с использованием информационных технологий

Традиция начинать уголовно-правовой анализ с характеристики объекта преступления сформировалась не случайно. Именно установление объекта позволяет определить направленность посягательства, выявить его общественно опасную природу и провести разграничение между преступлением и иными формами противоправного поведения, включая гражданско-правовые деликты. Корректное определение объекта лежит в основе квалификации деяния, поскольку оно задаёт рамки уголовно-правовой оценки и позволяет соотнести фактические обстоятельства с конкретной нормой уголовного закона.

В научной литературе, однако, неоднократно высказывалось мнение о том, что практическая роль объекта преступления чрезмерно акцентирована. Сторонники данного подхода указывают, что формальное несоответствие места уголовно-правовой нормы в системе Особенной части УК РФ не препятствует её применению, а потому значение объекта как системообразующего элемента состава преступления якобы не столь велико[1]. Тем не менее подобная позиция представляется недостаточно убедительной. Отказ от анализа объекта фактически обедняет уголовно-правовую характеристику деяния и снижает

[1] См.: Карабанова Е.Н. Понятие объекта преступления в современном уголовном праве // Журнал российского права. – 2018. – № 6(258). – С. 69.

качество правовой оценки, особенно в условиях усложнения преступных форм, связанных с использованием информационных технологий[1].

Исторически учение об объекте преступления формировалось в русле развития теории состава преступления. Уже во второй половине XIX века в отечественной доктрине предпринимались попытки осмыслить, на что именно направлено преступное посягательство. Так, Н. С. Таганцев связывал объект преступления с уголовно-правовой нормой, полагая, что именно она и подвергается нарушению. По его мнению, при совершении, например, хищения воздействие осуществляется на конкретную вещь, принадлежащую определённому лицу, однако в абстрактном плане посягательство затрагивает установленный правопорядок имущественных отношений и гарантии неприкосновенности собственности[2].

Данная концепция вызвала обоснованную критику как в дореволюционной (С. В. Познышев), так и в советской (А. Н. Трайнин) уголовно-правовой науке. Поскольку уголовный закон не претерпевает фактического ущерба в результате совершения противоправного деяния, он не может быть объектом преступления. Именно С. В. Познышев качестве объекта предлагал рассматривать охраняемые правом блага – реальные состояния лиц или вещей, а также общественные отношения, находящиеся под защитой уголовного закона. В современной науке данная идея получила заслуженное развитие.

В дальнейшем в советской доктрине утвердилось понимание объекта преступления как общественных отношений. Существенный вклад в формирование данного подхода внесли А. А. Пионтковский, В. Н. Кудрявцев, Н. И. Загородников, В. Я. Таций, Б. С. Никифоров, Н. И. Коржанский, В. К. Глистин и другие исследователи. Признание общественных отношений

---

[1] Шаяхметова Ж.Б. Роль и значение объекта преступления в составе преступления // Современные проблемы уголовной политики: Международная коллективная монография. – Екатеринбург: Федеральное государственное бюджетное образовательное учреждение высшего образования «Уральский государственный юридический университет», 2019. – С. 180.

[2] Карабанова Е.Н. Указ. соч. – С. 70.

объектом уголовно-правовой охраны позволило выстроить логичную систему Особенной части уголовного закона, в которой составы преступлений сгруппированы по родовым и видовым объектам.

Развивая данную концепцию, Б. С. Никифоров подчёркивал, что уголовная ответственность возможна лишь при установлении фактического нарушения общественных отношений, находящихся под охраной уголовного закона[1]. Он связывал наступление ответственности с наличием общественно опасного результата, причинно-следственной связи между деянием и этим результатом, а также с виной лица. При этом само по себе совершение определённого действия ещё не образует основание для уголовной ответственности, если не доказано, что оно затронуло охраняемые отношения и причинило им вред. Такой подход позволял чётко отделять уголовно наказуемые деяния от иных форм противоправного поведения.

Наряду с этим в доктрине сохранялись и альтернативные взгляды. Идеи Н. С. Таганцева о посягательстве на правоохраняемые интересы получили развитие в трудах современных авторов. В рамках этого подхода объект преступления рассматривается как совокупность благ и интересов личности и общества: имущественные права, телесная неприкосновенность, свобода, честь, возможность распоряжаться результатами своей деятельности. Эти положения были восприняты авторами фундаментальных курсов уголовного права и легли в основу более гибкого понимания объекта преступления как социально значимых ценностей, которым причинён или мог быть причинён вред[2].

А.В. Наумов, анализируя данную проблему, указывал, что трактовка объекта как общественных отношений вполне оправданна применительно к преступлениям против собственности, где предмет посягательства лишь опосредует нарушение отношений владения, пользования и распоряжения.

---

[1] Никифоров Б.С. Избранное / Составитель канд. юрид. наук А.А. Гравина. – М: Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации, 2010. – С. 22.

[2] Граматкина С.А. Объект преступления и проблемные вопросы его определения // Вестник Юридического института МИИТ. – 2020. – № 1(29). – С. 69.

Однако в преступлениях против личности такая конструкция оказывается недостаточной. В этих случаях объектом следует признавать непосредственно охраняемые уголовным законом блага, затрагиваемые преступным посягательством[1].

Современное состояние уголовно-правовой науки характеризуется признанием объекта преступления в качестве охраняемых уголовным законом общественных отношений либо благ, на которые направлено деяние виновного и которым причинён или может быть причинён вред[2]. Данная концепция сохраняет методологическую ценность и в условиях цифровизации преступности. При мошенничестве с использованием информационных технологий посягательство направлено не только на имущественные интересы потерпевших, но и на устойчивость доверительных отношений в сфере электронного оборота, безопасность цифровых сервисов и надёжность информационных каналов. Это обстоятельство придаёт анализу объекта преступления особое значение и требует его учёта при квалификации современных форм мошенничества.

Размещение норм, устанавливающих уголовную ответственность за мошенничество с использованием информационно-телекоммуникационных технологий в статьях 159, 159^3 и 159^6 главы 21 «Преступления против собственности» раздела VIII «Преступления в сфере экономики» Уголовного кодекса Российской Федерации позволяет определить общую направленность соответствующего посягательства. Такое законодательное решение свидетельствует о том, что родовым объектом данного преступления выступают общественные отношения в сфере экономики, понимаемые как совокупность связей, возникающих в процессе производства, распределения, обмена и потребления материальных и нематериальных благ, включая их оборот в цифровой форме.

---

[1] Наумов А.В. Российское уголовное право. Общая часть: курс лекций. – 7-е изд. – М.: Проспект, 2024. – С. 343.

[2] Квасникова Т.В., Костюк С.А., Лубягин О.И. Понимание объекта преступления в доктрине уголовного права // Закон и власть. – 2025. – № 1. – С. 90.

В рамках указанной группы общественных отношений центральное место занимают отношения собственности, которые образуют видовой объект мошенничества. Именно на эти отношения направлено противоправное воздействие при совершении обмана либо злоупотребления доверием, в том числе с применением информационных технологий и электронных платежных инструментов. Использование цифровых способов распоряжения денежными средствами не изменяет существа посягательства, но трансформирует форму его реализации, что требует уточнения содержания охраняемых отношений.

В научной литературе отсутствует единый подход к пониманию права собственности. Одни авторы рассматривают его преимущественно как экономическую категорию, отражающую отношения присвоения и распределения благ, другие – как юридическую конструкцию, закрепляющую определённый объём правомочий. Более взвешенным представляется подход, согласно которому право собственности имеет двойственную природу, объединяя экономическое содержание и юридическую форму. В экономическом аспекте оно выражает систему объективно складывающихся отношений между субъектами по поводу присвоения средств производства и результатов труда, а в юридическом – получает нормативное оформление и государственную защиту.

Юридическое содержание права собственности раскрывается через нормы гражданского законодательства. В соответствии со статьёй 209 Гражданского кодекса Российской Федерации [1] собственнику принадлежат правомочия владения, пользования и распоряжения имуществом, реализуемые в отношениях с иными лицами. Именно эти правомочия формируют структуру вещного права и определяют пределы допустимого поведения участников гражданского оборота. Посягательство на данные правомочия посредством обмана означает нарушение установленного законом режима собственности.

---

[1] Гражданский кодекс Российской Федерации, часть первая: федеральный закон от 30 ноября 1994 г. № 51-ФЗ (ред. от 31.07.2025) // Собр. законодательства Рос. Федерации. – 1994. – № 32. – Ст. 3301.

Отсутствие у лица прав на соответствующее имущество является необходимым условием признания деяния мошенничеством. Если лицо действует в пределах принадлежащих ему правомочий, исключается сам факт противоправного изъятия чужого имущества либо приобретения права на него. Следовательно, предметом мошеннического посягательства могут выступать только имущество, принадлежащее другим лицам, а также их имущественные права, поскольку воздействие на имущество неизбежно сопряжено с нарушением прав собственника.

В доктрине остаётся дискуссионным вопрос о включении права пользования в содержание объекта мошенничества. Получение права пользования чужим имуществом путём обмана действительно не всегда влечёт переход права собственности или возможности распоряжения. Вместе с тем извлечение полезных свойств из имущества без законных оснований нарушает установленный собственником порядок его использования и потому затрагивает охраняемые законом интересы. В этом смысле неправомерное приобретение права пользования также способно образовывать элемент посягательства на отношения собственности.

Следует учитывать, что объём правомочий собственника не исчерпывается классической триадой. Часть 2 статьи 209 ГК РФ закрепляет возможность собственника совершать любые действия в отношении имущества, не противоречащие закону, включая передачу отдельных правомочий другим лицам при сохранении за собой титула собственника. Тем самым право собственности представляет собой максимально широкий и устойчивый комплекс возможностей, не сопоставимый по своему объёму с иными гражданскими правами.

Исходя из этого, видовой объект мошенничества с использованием информационных технологий охватывает общественные отношения, обеспечивающие гарантированную законом возможность собственника в полном объёме владеть, пользоваться и иным образом распоряжаться принадлежащим ему имуществом, в том числе в цифровой среде. Однако

специфика данного состава преступления обусловлена тем, что посягательство направлено преимущественно на безналичные и электронные денежные средства.

В этой связи обоснованной представляется позиция, согласно которой видовой объект рассматриваемого мошенничества включает не только отношения собственности в их вещно-правовом выражении, но и обязательственные отношения. Современная правоприменительная практика исходит из того, что безналичные и электронные денежные средства существуют в форме записей на счетах и выражают право требования клиента к кредитной или иной финансовой организации. Такой подход отражён, в частности, в правовых позициях Конституционного Суда Российской Федерации[1].

Следовательно, при совершении мошенничества, например, с использованием электронных средств платежа, причиняется вред не только отношениям, связанным с абсолютным правом собственности, но и относительным обязательственным отношениям, опосредующим оборот денежных средств в информационных системах. Потерпевший утрачивает не вещь в материальном выражении, а закреплённое за ним право требования, реализация которого зависит от действий третьего лица – соответствующей организации.

С учётом изложенного видовой объект мошенничества с использованием информационных технологий следует определять как совокупность общественных отношений, обеспечивающих охраняемую законом возможность лица владеть, пользоваться и распоряжаться своим имуществом, а также реализовывать принадлежащее ему обязательственное право требования к кредитной или иной организации. Такая трактовка в наибольшей степени

[1] По делу о проверке конституционности частей шестой и седьмой статьи 115 Уголовно-процессуального кодекса Российской Федерации в связи с жалобой закрытого акционерного общества «Глория»: постановление Конституционного Суда РФ от 10 декабря 2014 г. № 31-П (абз. 2 п. 3) // КонсультантПлюс: справ.-правов. сист. – URL: www.consultant.ru (дата обращ.: 10.01.2026).

отражает специфику преступных посягательств, совершаемых с применением информационных технологий, и позволяет адекватно учитывать их правовую природу при квалификации.

Непосредственный объект мошенничества, предусмотренного статьёй 159 УК РФ, традиционно связывается с общественными отношениями собственности, выражающимися в закреплённой законом возможности собственника владеть, пользоваться и распоряжаться принадлежащим ему имуществом. Посягательство в данном случае направлено не на вещь как таковую, а на имущественную сферу потерпевшего, которая нарушается посредством обмана или злоупотребления доверием. Уголовно-правовая охрана распространяется на сами отношения по распоряжению имуществом, независимо от формы собственности и характера имущественного объекта.

При анализе мошенничества с использованием электронных средств платежа, ответственность за которое установлена статьёй 159^3 УК РФ, непосредственный объект сохраняет ту же природу – это общественные отношения собственности и имущественных прав. Вместе с тем специфика данного состава обусловлена особенностями механизма посягательства. Е.А. Соловьева отмечает, что в таких преступлениях фактически взаимодействуют как минимум три субъекта: владелец безналичных или электронных денежных средств, оператор по переводу денежных средств и лицо, совершающее посягательство[1]. В связи с этим высказывается позиция о том, что в рамках статьи 159^3 УК РФ речь нередко идёт не о классическом изъятии имущества, а о незаконном приобретении права на него. Однако подобная дискуссия относится преимущественно к характеристике предмета преступления и не изменяет содержания непосредственного объекта, которым остаются охраняемые уголовным законом имущественные отношения.

Особенностью статьи 159^3 УК РФ является наличие дополнительного объекта. Посягательство в рамках данной нормы неизбежно затрагивает общественные отношения, обеспечивающие функционирование системы

[1] Соловьева Е.А. Указ. соч. – С. 49.

перевода и оборота безналичных и электронных денежных средств [1]. Мошеннические действия, как правило, сопровождаются подменой личности клиента оператора, искажением данных либо иным вмешательством в установленный порядок совершения транзакций, что нарушает устойчивость и надёжность соответствующих сервисов. При отсутствии вреда таким отношениям квалификация содеянного по статье 159^3 УК РФ утрачивает основание, поскольку именно совмещение посягательства на имущественную сферу и нарушение порядка оказания платёжных услуг отличает данную норму от общего состава мошенничества.

Так, в суд поступило дело об обвинении Лукиной А.В. по ч.2 ст. 159^3 УК РФ. Подсудимая выставила в социальной сети «Инстаграмм» со своего аккаунта «Kartina_showToom_2» объявление о продаже картин по номерам и алмазных мозаик. Затем между ней и Потерпевшей состоялась переписка, в ходе которой Потерпевший №1 сообщила Лукиной А.В. о своем желании у нее купить 70 картин по номерам и 160 алмазных мозаик. В результате действий Лукиной А.В. потерпевшей причинен ущерб на общую сумму 58 250 рублей. При рассмотрении дела суд указал, что при совершении мошенничества как обмана, Лукина А.В. не использовала электронные средства платежа поскольку потерпевшая была обманута во время переписки с подсудимой. Фактически материалы уголовного дела содержат лишь сведения о том, что имело место перечисление денежных средств со счета. Сведения о том, какое программное обеспечение, устройство использовались при совершении преступления материалы дела не содержат. И действия подсудимой были переквалифицированы по ч. 1 ст. 159 УК РФ[2].

В другом деле подсудимая получила доступ к денежным средствам потерпевшего следующим образом: похитила банковскую карту, а затем

---

[1] Сафонова Д.В. Особенности объекта и предмета преступления, предусматривающего ответственность за мошенничество с использованием электронных средств платежа (ст. 159^3 УК РФ) // Правопорядок: история, теория, практика. – 2025. – №4 (47). – С. 85.

[2] Приговор Приволжского районного суда г. Казани Республики Татарстан от 14 апреля 2023 г. № 1-272/2023 [Электронный ресурс] // ГАС «Правосудие». – URL: https://privolzhsky--tat.sudrf.ru (дата обращения: 05.03.2026).

оплачивала покупки путем обмана бармена. Действия были квалифицированы по ч. 1 ст. 159^3 УК РФ[1].

Непосредственный объект мошенничества в сфере компьютерной информации, предусмотренного статьёй 159^6 УК РФ, также формируется вокруг имущественных отношений, однако здесь они реализуются через иные юридические конструкции. Посягательство осуществляется посредством вмешательства в функционирование информационных систем, обработки данных или использования программных средств, в результате чего у потерпевшего утрачивается возможность реализовать принадлежащее ему имущественное право. Вред причиняется не только отношениям собственности, но и обязательственным отношениям, опосредующим оборот безналичных денежных средств и иных имущественных прав в цифровой форме. Потерпевший в таких случаях лишается не материального объекта, а закреплённого за ним права требования, реализация которого зависит от корректной работы информационной инфраструктуры и действий третьих лиц[2].

Таким образом, при всех различиях в способах совершения преступления непосредственный объект мошенничества по статьям 159, 159^3 и 159^6 УК РФ сохраняет единую имущественную природу. Вместе с тем использование информационных технологий приводит к усложнению структуры охраняемых общественных отношений, вовлекая в сферу уголовно-правовой защиты не только классические отношения собственности, но и отношения, обеспечивающие оборот имущественных прав в информационных и платёжных системах. Именно это обстоятельство определяет специфику мошенничества, совершаемого с применением информационных технологий, и должно учитываться при его уголовно-правовой характеристике и квалификации.

---

[1] Приговор Авиастроительного районного суда г. Казани Республики Татарстан от 5 сентября 2019 г. № 1-213/2019 [Электронный ресурс] // Судебные и нормативные акты РФ. – URL: https://sudact.ru/regular/doc/SK3KlfXTdf6R (дата обращения: 05.03.2026).

[2] Барчуков В.К. Непосредственный объект мошенничества в сфере компьютерной информации // Пробелы в российском законодательстве. Юридический журнал. – 2018. – № 7. – С. 156.Ю

В рамках общей нормы о мошенничестве предмет посягательства по ст. 159 УК РФ обычно связывают с чужой вещью, а также с правом на чужое имущество. Такая конструкция во многом опирается на гражданско-правовые представления об объектах оборота. В гражданском праве исходной категорией выступает вещь как объект материального мира, тогда как термин «имущество» употребляется неодинаково: им обозначают и совокупность вещей, и имущественные права, а иногда – имущественную массу в целом. Поэтому в уголовно-правовой доктрине не исчезает вопрос о пределах предмета мошенничества: следует ли ограничивать его материальными вещами или допустимо включать случаи, когда посягательство направлено на приобретение имущественного права (в том числе в бездокументарных формах) и последующее распоряжение им. Именно этим объясняется, что при мошенничестве преступный результат нередко выражается не в изъятии вещи, а в получении юридически оформленной возможности распоряжаться имущественными ценностями[1].

Мошенничество сохраняет родовые признаки хищения, однако отличается усложнённой конструкцией предмета. Имущество в этом случае выступает не только как физически осязаемая вещь, но и как экономическая ценность, опосредованная гражданско-правовыми отношениями. Обращение к положениям гражданского законодательства показывает, что категория «имущество» включает в себя вещи, деньги, ценные бумаги, а также имущественные права и иные объекты гражданских прав. В результате предмет мошенничества по статье 159 УК РФ выходит за рамки классического вещного подхода и охватывает как материальные, так и нематериальные формы имущественного оборота[2].

---

[1] Шабашов А.Д. Юридическая характеристика признаки предмета хищения при совершении мошенничества // Научный форум: сборник статей XIII Международной научно-практической конференции, Пенза, 23 мая 2025 года. – Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2025. – С. 170.

[2] Розенко С.В., Мурзина К.А. Особенности квалификации мошенничества по уголовному законодательству Российской Федерации // Вестник Югорского государственного университета. – 2017. – № 1-2(44). – С. 114.

Именно такая конструкция позволяет квалифицировать в качестве мошенничества посягательства, направленные не на непосредственное изъятие вещи, а на установление контроля над имущественными возможностями потерпевшего. В условиях цифровизации экономики это приобретает особое практическое значение, поскольку обман нередко используется для получения доступа к имущественным правам, реализуемым в электронной среде[1].

Специальный состав мошенничества с использованием электронных средств платежа конкретизирует предмет посягательства применительно к современным формам имущественного оборота. В данном случае преступное поведение ориентировано преимущественно на безналичные денежные средства и электронные денежные средства, обращающиеся в рамках платёжных систем и банковской инфраструктуры. Эти объекты не обладают физической формой, однако имеют самостоятельную экономическую ценность и обеспечивают участие лица в имущественном обороте[2].

С гражданско-правовой точки зрения безналичные денежные средства и электронные деньги в настоящее время квалифицируются как имущественные права, входящие в состав иного имущества. Это обстоятельство принципиально влияет на уголовно-правовую оценку содеянного. Посягательство осуществляется не на вещь как таковую, а на зафиксированную в информационных системах совокупность правомочий, позволяющих требовать от кредитной или иной уполномоченной организации совершения определённых операций в пользу владельца счёта.

Вместе с тем уголовно-правовой смысл предмета по статье 159^3 УК РФ не сводится к абстрактному праву требования. Фактическая направленность преступления заключается в изъятии экономической ценности, выраженной в денежном эквиваленте, и обращении её в пользу виновного или третьих лиц.

---

[1] Крючков М.А. Уголовно-правовая характеристика мошенничества, совершаемого с использованием информационно-коммуникационных технологий // Научный аспект. – 2023. – Т. 1, № 5. – С. 9.

[2] Петрякова Л.А. Мошенничество с использованием электронных средств платежа // Вектор науки Тольяттинского государственного университета. Серия: Юридические науки. – 2020. – № 1(40). – С. 35.

Именно поэтому судебная практика последовательно исходит из признания безналичных и электронных денежных средств предметом хищения, несмотря на их нематериальную природу [1] . Такой подход обеспечивает защиту имущественных интересов участников цифрового финансового оборота и устраняет возможность ухода от уголовной ответственности за счёт формальных конструкций гражданского права[2].

Предмет мошенничества в сфере компьютерной информации имеет наиболее сложную и многоуровневую структуру, поскольку связан с использованием информационных технологий и автоматизированных систем обработки данных. В отличие от классических форм мошенничества, здесь объектом воздействия выступают не только имущественные ценности, но и информационные ресурсы, посредством которых осуществляется доступ к ним[3].

Непосредственным предметом по статье 159^{6} УК РФ являются имущественные ценности, получаемые в результате неправомерного вмешательства в функционирование компьютерных систем: безналичные денежные средства, электронные деньги, цифровые финансовые активы и иные экономические ресурсы, учёт которых осуществляется в электронной форме. Компьютерная информация в данном случае выполняет служебную роль, являясь средством достижения имущественного результата, однако именно через манипулирование данными реализуется преступный умысел.

---

[1] О судебной практике по делам о мошенничестве, присвоении и растрате: Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 (ред. от 15.12.2022) // Бюллетень Верховного Суда РФ. – 2018. – № 2; Кассационное определение Седьмого кассационного суда общей юрисдикции от 13.11.2025 № 77-3303/2025 // Справ.-правов. сист. «КонсультантПлюс» [Электронный ресурс]. – Режим доступа: www.consultant.ru (дата обращения: 10.12.2025); Постановление Восьмого кассационного суда общей юрисдикции от 10.03.2022 № 77-1148/2022 // Справ.-правов. сист. «КонсультантПлюс» [Электронный ресурс]. – Режим доступа: www.consultant.ru (дата обращения: 10.12.2025).

[2] Лопашенко Н.А. Преступления против собственности. Книга II. Общая теория хищений. Виды хищения: Авторский курс в 4 книгах. – Москва: Юрлитинформ, 2019. – С. 21.

[3] Крючков М.А. Уголовно-правовая характеристика мошенничества, совершаемого с использованием информационно-коммуникационных технологий // Научный аспект. – 2023. – Т. 1, № 5. – С. 9.

Специфика этого состава заключается в том, что посягательство опосредуется технологической средой. Виновный не вступает в непосредственное взаимодействие с потерпевшим, а воздействует на информационные потоки, алгоритмы и базы данных, что приводит к несанкционированному перераспределению имущественных благ. Такая модель преступного поведения наглядно демонстрирует, что современное мошенничество окончательно вышло за пределы традиционного представления о хищении как о физическом изъятии вещи.

В целом анализ предмета мошенничества по статьям 159, 159^3 и 159^6 УК РФ показывает устойчивую тенденцию к расширению уголовно-правовой охраны имущественных интересов в условиях цифровой экономики. Имущество в его современном понимании всё чаще существует в форме записей, прав и электронных эквивалентов, однако это не снижает необходимости его эффективной защиты средствами уголовного права.

Нельзя не сказать о проблемах, которые сохраняются как на уровне доктрины, так и в правоприменении. Прежде всего обращает на себя внимание отсутствие в уголовном законе легального определения предмета хищения и мошенничества, что вынуждает правоприменителя обращаться к гражданско-правовым категориям и судебным разъяснениям. Такой подход неизбежно приводит к неоднородности квалификации, особенно в ситуациях, когда посягательство направлено на нематериальные объекты, существующие в цифровой форме.

Наиболее дискуссионным остаётся вопрос о соотношении имущества и имущественных прав в структуре предмета мошенничества. С одной стороны, действующая редакция статьи 128 ГК РФ включает имущественные права в состав имущества, что формально позволяет рассматривать их в качестве предмета хищения. С другой стороны, в уголовно-правовой доктрине продолжает воспроизводиться аргумент о вещной природе хищения и невозможности «завладения» правом как таковым. Эти расхождения особенно остро проявляются при квалификации посягательств на безналичные и

электронные денежные средства, цифровые активы и иные результаты функционирования информационных систем. На практике это приводит к колебаниям между признанием содеянного мошенничеством, кражей либо отказом в уголовно-правовой оценке по мотиву отсутствия предмета преступления в традиционном понимании.

Дополнительные сложности связаны с эволюцией гражданского законодательства. Последовательное изменение правового режима безналичных денежных средств – от отнесения к «иному имуществу» к квалификации в качестве имущественного права – объективно усилило неопределённость при применении норм главы 21 УК РФ. Возникает ситуация, при которой один и тот же объект гражданских прав в зависимости от используемой доктринальной конструкции может рассматриваться либо как имущество, либо как право требования, что непосредственно влияет на вывод о наличии или отсутствии состава хищения. В условиях цифровизации имущественного оборота данная проблема приобретает системный характер и выходит за рамки отдельных составов мошенничества.

Существенным представляется и то обстоятельство, что действующая редакция уголовного закона не учитывает в полной мере появление новых объектов имущественного оборота, связанных с использованием информационных технологий. Цифровые финансовые активы, цифровые валюты, электронные записи, обеспечивающие реализацию имущественных требований, фактически уже становятся объектами преступных посягательств, однако их уголовно-правовой статус выводится преимущественно из судебных разъяснений. Такая ситуация снижает уровень правовой определённости и затрудняет формирование единообразной практики.

В целях устранения выявленных проблем и обеспечения устойчивости квалификации представляется целесообразным нормативно закрепить расширенное понимание предмета хищения, включая мошенничество. Оптимальным решением является дополнение примечания к статье 158 УК РФ специальным положением: «1.1. Предметом хищения в статьях настоящей

главы признаются движимые и недвижимые вещи, включая наличные деньги и документарные ценные бумаги, а равно иное имущество, в том числе безналичные и электронные денежные средства, бездокументарные ценные бумаги, цифровые финансовые активы, цифровые валюты и иные имущественные права».

Кроме того, мы считаем возможным поддержать предложение о переименовании главы 21 УК РФ «Преступления против собственности» в «Имущественные преступления»[1]. Данный шаг, по нашему мнению, устранит дискуссии о предмете мошенничеств.

Развитие цифровых форм имущественного оборота ставит под сомнение традиционное представление о физической, материальной природе предмета хищения, которое длительное время рассматривалось в уголовно-правовой доктрине как обязательный признак преступлений против собственности. Современные имущественные отношения все в большей степени реализуются в электронной среде, где экономическую ценность приобретают объекты, не обладающие вещественной формой. Это находит отражение как в законодательстве, так и в правоприменительной практике, связанной с хищением безналичных денежных средств, электронных денег, цифровых валют и иных нематериальных активов.

Действующее гражданское законодательство закрепляет расширительное понимание имущества. В соответствии со статьёй 128 Гражданского кодекса Российской Федерации к имуществу относятся не только вещи, включая наличные деньги и документарные ценные бумаги, но и иное имущество, в том числе имущественные права, безналичные денежные средства, бездокументарные ценные бумаги и цифровые права. Такое нормативное решение свидетельствует об отходе законодателя от исключительно вещного понимания имущественных ценностей и создает основу для признания нематериальных объектов предметом преступлений против собственности.

[1] Соловьева Е.А. Указ. соч. – С. 50.

С учётом этого более оправданным представляется подход, при котором определяющими признаками предмета хищения являются, во-первых, его принадлежность иному лицу, а во-вторых, наличие действительной либо потенциальной экономической ценности, позволяющей объекту участвовать в имущественном обороте. Материальная форма существования объекта не может рассматриваться как решающий критерий уголовно-правовой охраны[1].

Указанные выводы в полной мере применимы к электронным денежным средствам, правовой режим которых установлен Федеральным законом от 27 июня 2011 г. № 161-ФЗ «О национальной платёжной системе»[2]. Согласно пункту 18 статьи 3 данного закона электронные денежные средства используются для осуществления расчётов без открытия банковского счёта и подлежат учёту оператором по переводу денежных средств. Несмотря на отсутствие вещественной формы, такие средства выполняют экономическую функцию денег, подлежат конвертации и потому могут выступать предметом хищения, включая мошенничество, совершаемое с применением информационных технологий.

Аналогичным образом следует оценивать и цифровую валюту, правовой статус которой определён Федеральным законом от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»[3]. Хотя цифровая валюта прямо не признаётся денежной единицей Российской Федерации либо иностранного государства, законодатель относит её к имуществу. Это позволяет рассматривать её в качестве возможного предмета преступлений против собственности при условии соблюдения требований закона, связанных с легальностью оборота и раскрытием информации.

---

[1] Соловьева Е.А. Указ. соч. – С. 51.

[2] О национальной платежной системе: федеральный закон от 27 июня 2011 г. № 161-ФЗ (ред. от 25.05.2025 // Собр. законодательства Рос. Федерации. – 2011. – № 27. – Ст. 3872.

[3] О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон № 259-ФЗ от 31 июля 2020 г. (ред. от 27.10.2025) // Собр. законодательства Рос. Федерации. – 2020.- № 31 (часть 1).- Ст. 5018.

Отдельное место занимают цифровые финансовые активы, которые в силу положений Федерального закона № 259-ФЗ признаются цифровыми правами и, в соответствии со статьёй 128 ГК РФ, относятся к имущественным правам. Их экономическая ценность выражается через денежные требования, корпоративные и иные имущественные притязания, что делает возможным признание таких активов предметом мошенничества и иных форм хищения, несмотря на их нематериальный характер.

В совокупности приведённые положения свидетельствуют о том, что сохранение ориентации уголовного закона исключительно на материальные объекты не соответствует современному состоянию имущественного оборота. Цифровизация экономических отношений объективно требует переосмысления подходов к определению предмета преступлений против собственности, прежде всего мошенничества, совершаемого с использованием информационных технологий, и подтверждает необходимость нормативного закрепления расширенного понимания охраняемых имущественных объектов.

Проведённый анализ показывает, что, несмотря на отсутствие в Уголовном кодексе Российской Федерации самостоятельного состава мошенничества с использованием информационных технологий, данные официальной статистики свидетельствуют о системном и массовом характере таких посягательств. Значительная доля преступлений, совершаемых с применением цифровых каналов, указывает на устойчивую трансформацию мошенничества в технологически опосредованную форму имущественного посягательства. В этих условиях традиционные уголовно-правовые конструкции, ориентированные на материальные объекты, не в полной мере отражают специфику современного имущественного оборота. Анализ объекта и предмета преступления подтверждает необходимость учитывать не только отношения собственности, но и обязательственные связи, реализуемые в цифровой среде. Это требует уточнения нормативных подходов к квалификации мошенничества, совершаемого с использованием

информационных технологий, и адаптации уголовно-правовой охраны к современным формам имущественных отношений.

В действующем уголовном законодательстве Российской Федерации отсутствует нормативное определение объективной стороны преступления. Вместе с тем в уголовно-правовой доктрине она устойчиво рассматривается как совокупность внешне проявленных признаков противоправного поведения, поддающихся установлению и доказыванию в рамках уголовного судопроизводства[1]. Подобный подход соответствует общей логике построения уголовно-правовых норм, в рамках которой привлечение лица к уголовной ответственности возможно лишь при наличии установленного общественно опасного деяния.

Однако для преступлений с материальным составом, к числу которых относится мошенничество, фиксации одного лишь факта деяния недостаточно. В этих случаях требуется также доказать наступление вредных последствий и наличие причинной связи между действиями виновного и причинённым ущербом. В результате объективная сторона мошенничества включает три взаимосвязанных элемента: активное деяние, имущественный вред и причинно-следственную зависимость между ними. Именно через их совокупность воспроизводится фактический механизм преступного посягательства, что позволяет провести разграничение мошенничества и иных преступлений против собственности.

В системе элементов состава преступления объективная сторона занимает самостоятельное и обязательное место[2]. Применительно к мошенничеству она служит основанием для вывода о том, произошло ли выбытие чужого имущества из владения потерпевшего либо приобретение права на него. Данное обстоятельство позволяет отличить мошенничество от смежных составов, в

---

[1] Ибатуллина Д.М. Объективные признаки цифрового мошенничества и их значение для квалификации деяния // Вестник Казанского юридического института МВД России. – 2025. – Т. 16, № 1(59). – С. 69.

[2] Маршева К.С. Объективные признаки мошенничества с использованием электронных средств платежа // Молодой ученый. – 2021. – № 50 (392). – С. 265.

частности от причинения имущественного вреда без признаков хищения, предусмотренного ст. 165 УК РФ[1]. При отсутствии хотя бы одного элемента объективной стороны – например, при недоказанности факта изъятия имущества – квалификация содеянного как мошенничества исключается, что последовательно подтверждается судебной практикой[2].

Отдельного внимания заслуживает вопрос о способе совершения мошенничества. В уголовном законе он неизменно связывается с обманом либо злоупотреблением доверием, что признаётся обязательным признаком всех форм данного преступления[3]. На практике именно способ хищения нередко предопределяет выбор применимой уголовно-правовой нормы. Так, в общем составе мошенничества, предусмотренном ст. 159 УК РФ, законодатель ограничивается указанием на обман или злоупотребление доверием без конкретизации используемых средств. Напротив, выделение специальных составов – ст. 159^3 и 159^6 УК РФ – обусловлено необходимостью учёта специфических форм посягательства, связанных соответственно с использованием электронных средств платежа и с воздействием на компьютерную информацию[4].

Общественно опасное деяние при мошенничестве выражается исключительно в форме активных действий[5]. Данный вид преступления не может быть реализован путём бездействия, поскольку предполагает целенаправленное воздействие либо на сознание потерпевшего, либо на

---

[1] Обзор судебной практики Кемеровского областного суда от 23 июня 2005 г. № 01-19/320 по делам о преступлениях, предусмотренных ст.ст.159, 160, 165, 242, 327 УК РФ [Электронный ресурс] // Справ.-правов. сист. «Гарант». – Режим доступа: https://base.garant.ru/7541393/ (дата обращения: 10.12.2025).

[2] Кассационное определение Второго кассационного суда общей юрисдикции от 17.04.2025 № 77-963/2025 [Электронный ресурс] // КонсультантПлюс: справ.-правов. сист. – URL: www.consultant.ru (дата обращ.: 10.12.2025).

[3] Ибатуллина Д.М. Указ. соч. С. 69.

[4] Деменков В.А., Алехин В.П. Мошенничество в сфере компьютерной информации: к вопросу квалификации и применения ст. 159^6 УК РФ // Тенденции развития науки и образования. – 2023. – № 104-8. – С. 131.

[5] Ибатуллина Д.М. Указ. соч. – С. 70.

функционирование информационных и платёжных механизмов с целью противоправного обращения чужого имущества в пользу виновного.

Активный характер деяния проявляется в совершении конкретных поступков: сообщении определённых сведений, вводе данных, имитации сделок, формировании у потерпевшего искажённых представлений о фактических обстоятельствах. Эти действия носят умышленный характер и направлены на достижение заранее предполагаемого имущественного результата. В этом состоит отличие мошенничества от преступлений, допускающих реализацию противоправного поведения посредством пассивного невыполнения обязанностей.

Как указывается в ст. 159 УК РФ и постановления Пленума Верховного Суда РФ от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», способы реализации деяния при мошенничестве прямо обозначены в уголовном законе и сводятся к обману либо злоупотреблению доверием. Обман, согласно п. 2 постановления Пленума Верховного Суда РФ от 30.11.2017 № 48, заключается в сознательном введении потерпевшего в заблуждение путём сообщения ложных сведений либо умолчания о фактах, имеющих значение для принятия имущественного решения. Такие сведения могут касаться личности виновного, его полномочий, свойств имущества, условий сделки, наличия прав либо предполагаемых событий. При этом обман может выражаться не только в словесной форме, но и посредством активных действий, включая использование поддельных документов, демонстрацию фиктивных предметов сделки или имитацию расчётов.

Злоупотребление доверием согласно п. 3 постановления Пленума Верховного Суда РФ от 30.11.2017 № 48, выражается в использовании сложившихся доверительных отношений с потерпевшим либо с лицом, наделённым полномочиями распоряжаться имуществом, в корыстных целях. К типичным ситуациям относятся случаи, когда виновный, опираясь на личные либо служебные связи, убеждает передать имущество или принимает на себя обязательства, не намереваясь их исполнять. Наличие одного из указанных

способов позволяет отграничить мошенничество от иных форм хищения; при их отсутствии содеянное образует иной состав преступления, например кражу или грабёж.

Цифровая среда существенно расширяет способы распространения заведомо ложной информации. Обман при мошенничестве может реализовываться посредством интернета, мобильной связи и иных информационно-телекоммуникационных сетей. На практике это выражается в рассылке электронных писем от имени известных организаций, размещении фиктивных объявлений о продаже товаров, направлении SMS-сообщений о мнимых выигрышах с требованием уплаты «комиссии» и иных аналогичных действиях. Судебная практика исходит из того, что подобные способы введения в заблуждение полностью охватываются признаками мошенничества. Пленум Верховного Суда РФ от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» разъяснил, что хищение, совершённое путём распространения ложных сведений в сети Интернет, подлежит квалификации по ст. 159 УК РФ, а не по ст. 159^{6} УК РФ. Тем самым подчёркивается, что используемый канал передачи информации не имеет самостоятельного уголовно-правового значения; определяющим остаётся направленность действий на введение потерпевшего в заблуждение.

Наряду с активным сообщением ложных сведений обман в цифровой среде может выражаться и в умолчании о существенных обстоятельствах. Преступник сознательно скрывает факты, знание которых исключило бы передачу имущества. Типичными являются ситуации создания фиктивных интернет-магазинов либо инвестиционных платформ, где умалчивается отсутствие товара, лицензии или реальных гарантий. Пленум Верховного Суда РФ от 30.11.2017 № 48 прямо указал, что обман при мошенничестве может состоять и в сокрытии истинных фактов. Специфика интернет-среды заключается в том, что подобное умолчание часто сочетается с созданием внешней видимости легитимности ресурса, что усиливает вводящее в заблуждение воздействие на пользователя.

Широкое распространение получила и такая форма обмана, как использование поддельных электронных интерфейсов, аккаунтов и сообщений. Преступники создают сайты-двойники банков, платёжных сервисов и интернет-магазинов, визуально неотличимые от официальных ресурсов. Аналогичным образом используются фейковые аккаунты в социальных сетях и мессенджерах, с помощью которых рассылаются ложные сообщения от имени знакомых или представителей организаций. Подобные действия направлены на формирование у потерпевшего ошибочного представления о субъекте либо условиях совершаемой операции и в правоприменительной практике квалифицируются как мошенничество.

Особую группу способов образуют приёмы социальной инженерии, основанные на психологическом воздействии на потерпевшего. В цифровой сфере наибольшее распространение получили фишинг, вишинг и смишинг. Фишинг предполагает выманивание конфиденциальных данных посредством электронных сообщений, имитирующих официальные уведомления известных сервисов. Вишинг реализуется через телефонные звонки, в ходе которых преступник, представляясь сотрудником банка или иной организации, побуждает сообщить реквизиты либо коды подтверждения. Смишинг использует аналогичные приёмы посредством SMS-сообщений. Все указанные способы основаны на обмане и злоупотреблении доверием и укладываются в классическую конструкцию мошенничества. Судебная практика квалифицирует такие деяния как мошенничество, в том числе с использованием электронных средств платежа, если их результатом становится списание денежных средств со счёта потерпевшего.

Мошенничество, будучи формой хищения, предполагает причинение потерпевшему имущественного вреда как обязательный результат. Уголовно-правовое значение имеет не само по себе нарушение охраняемых интересов, а фактическое уменьшение имущественной сферы, выраженное либо в выбытии имущества, либо в утрате юридически обеспеченной возможности распоряжаться им. До наступления такого результата объективная сторона

преступления считается нереализованной, независимо от того, насколько подробно установлены и доказаны обманные действия виновного.

В судебной практике устойчиво проводится разграничение между обманом как способом и имущественным вредом как последствием. Введение лица в заблуждение, даже при его очевидности, не образует оконченного состава, если не подтверждено выбытие имущественного эквивалента из владения либо распоряжения потерпевшего или утрата им соответствующего имущественного права. При отсутствии этих признаков содеянное оценивается либо как покушение, либо – при соответствующей фактической картине – как причинение имущественного ущерба без признаков хищения[1].

Использование информационных технологий не меняет данного подхода, а лишь влияет на форму проявления вреда. Потерпевший может не совершать активных действий по передаче имущества и не осознавать момент его утраты, однако правовая оценка последствий от этого не трансформируется: имущество выходит из сферы его фактического контроля. В делах данной категории суды, как правило, исходят из того, что безналичные денежные средства и электронные деньги охватываются понятием имущества, а их списание в результате обмана приравнивается к хищению[2].

На практике наиболее распространённой формой вреда является уменьшение остатка на счёте потерпевшего (вплоть до полного списания средств) вследствие операций, совершённых под влиянием обмана либо с использованием данных, полученных таким путём. Для квалификации не имеет решающего значения, каким именно способом технически оформлена транзакция – через мобильное приложение, интернет-банк или иной сервис. Существенным является факт выбытия денежных средств и утраты владельцем контроля над ними. Именно с этого момента, как правило, связывается окончание преступления.

---

[1] Маршева К.С. Указ. соч. – С. 264.

[2] Приговор Кировского районного суда г. Казани Республики Татарстан от 26 мая 2020 г. № 1-225/2020 [Электронный ресурс] // Судебные и нормативные акты РФ. – URL: https://sudact.ru/regular/doc/jBH1YaRetCoj (дата обращения: 05.03.2026).

В иных ситуациях вред выражается не в лишении денежных средств как таковых, а в утрате юридически закреплённой возможности распоряжаться имущественным благом. Это характерно для случаев, когда обманом оформляется переход права собственности, уступка требования либо распоряжение активом в реестре. Преступный результат здесь проявляется в возникновении у виновного законодательно обеспеченной возможности владеть или распоряжаться чужим имуществом как своим[1]. Для объектов, подлежащих обязательной регистрации, окончание преступления обычно совпадает с внесением соответствующей записи. Аналогичный подход применяется и к цифровым активам, права на которые фиксируются электронными средствами.

Отдельного внимания заслуживают ситуации, при которых виновный получает доступ к инструментам распоряжения имуществом – интернет-банку, сим-карте, учётной записи либо средствам аутентификации. Если на этом этапе выбытие имущества ещё не произошло, содеянное, как правило, квалифицируется как покушение. Однако последующее отчуждение активов переводит деяние в стадию оконченного преступления, поскольку потерпевший фактически утрачивает возможность распоряжаться принадлежащими ему ценностями.

При квалификации учитываются установленные законом пороговые значения ущерба, применяемые как к традиционным, так и к цифровым формам мошенничества. Технический способ совершения преступления на порядок оценки не влияет: значение имеет реальный объём имущественной утраты либо стоимость имущественного права, которым завладел виновный.

В безналичном обороте окончание мошенничества определяется не физической передачей имущества, а необратимым его выбытием из-под контроля потерпевшего и переходом возможности распоряжения к виновному или подконтрольным ему лицам. При мошенничестве в форме приобретения права решающим является момент возникновения у виновного юридически

[1] Деменков В.А., Алехин В.П. Указ. соч. – С. 132.

оформленного основания распоряжаться чужим имуществом. Если же действия ограничились созданием условий для изъятия, но фактического выбытия не произошло, содеянное образует покушение.

Для привлечения к уголовной ответственности необходимо установить, что имущественный вред стал прямым следствием обманных действий либо злоупотребления доверием. В цифровых схемах между действием и результатом нередко располагаются технические этапы, однако это не изменяет существа причинной связи. Существенным является то, что без совершённых виновным манипуляций ущерб не возник бы.

Так, при фишинговых атаках именно рассылка ложных сообщений формирует у потерпевшего ошибочное представление и побуждает его раскрыть данные, что в дальнейшем приводит к списанию средств [1]. Аналогичным образом при телефонных схемах перевод денег совершается самим потерпевшим, но под воздействием ложной информации [2]. Такие действия не разрывают причинную связь, а выступают предусмотренным элементом механизма хищения.

В большинстве случаев о мошенничестве с использованием информационно-телекоммуникационных технологий операции осуществляются с участием банков, операторов связи и платёжных сервисов. Их действия носят служебный характер и не влияют на уголовно-правовую оценку причинности, поскольку они реализуют операции на основании распоряжений, полученных вследствие обмана. Даже при перечислении средств на счета третьих лиц имущественный вред для потерпевшего наступает в момент их выбытия, а выбор канала перевода является частью преступного замысла.

---

[1] Фот Ю.Д., Туманов Н.И. Фишинг и как с ним бороться // Электронное информационное пространство для науки, образования, культуры: Материалы XI Международной научно-практической конференции. В 3-х частях, Орёл, 19 декабря 2024 года. – Орёл: Орловский государственный институт культуры, 2024. – С. 134.

[2] Тютюнник М.С., Печалов А.К. Противодействия телефонным мошенничествам // Инновационные идеи молодежи в развитии современной науки и образования: Материалы Международной студенческой научно-практической конференции, Ставрополь, 20 февраля 2025 года. – Краснодар: Российское энергетическое агентство, 2025. – С. 80.

Многоэтапный характер современных мошеннических схем и распределение ролей между участниками не препятствуют установлению причинной связи. При наличии единого умысла она прослеживается через вклад каждого звена в общий результат: если без конкретного действия хищение не состоялось бы, такое действие включается в механизм причинения вреда. Соответственно, при доказанности фактического уменьшения имущественной сферы потерпевшего либо юридического закрепления права за виновным объективная сторона мошенничества считается реализованной полностью.

Объективная сторона мошенничества в его общем виде сконструирована законодателем как предельно широкая и абстрактная. В статье 159 УК РФ закреплена модель хищения, при которой решающее значение придаётся не форме или техническому способу обмана, а самому факту введения потерпевшего в заблуждение либо злоупотребления доверием, повлекшему противоправное обращение чужого имущества или права на него. Отказ от детализации конкретных приёмов обмана не случаен: он позволяет охватывать самые различные жизненные ситуации, в которых имущественное поведение потерпевшего формируется под воздействием искажённого представления о действительности.

Именно поэтому общий состав применяется во всех случаях, когда фактические обстоятельства не содержат признаков специальных разновидностей мошенничества [1] . В правоприменении это означает, что подавляющее большинство дистанционных схем, реализуемых с использованием современных средств связи, подпадают под действие статьи 159 УК РФ. Продажа несуществующих товаров через интернет-ресурсы,

[1] Гуц Е. Отграничение общего состава мошенничества от специальных в российском уголовном праве // Государство, право и правоприменительная практика: современные вызовы: Сборник научных трудов IX Всероссийской научно-практической конференции студентов и аспирантов Юридического института Балтийского федерального университета им. Иммануила Канта, Калининград, 23 января 2021 года / Под общей редакцией О.А. Заячковского. – Калининград: Балтийский федеральный университет имени Иммануила Канта, 2022. – С. 168.

размещение фиктивных объявлений, телефонные обращения под видом сотрудников банков или иных организаций объединяет общий механизм: потерпевший, полагая, что действует в своих интересах, добровольно распоряжается имуществом, которое в действительности переходит к виновному. В таких ситуациях объективная сторона реализуется в полном объёме – от обманного воздействия до фактического поступления имущественных ценностей.

Дистанционный формат взаимодействия сам по себе не влияет на уголовно-правовую оценку содеянного[1]. Отсутствие личного контакта между участниками, использование сайтов, мессенджеров или электронной почты не изменяют существа объективной стороны. Определяющим остаётся вопрос о том, привёл ли обман к имущественному поведению потерпевшего и последующему ущербу, а не техническая форма коммуникации[2].

Так, Х., К., Ш. использовали приобретенное вредоносное программное обеспечение для заражения вирусами мобильных устройств, тем самым обеспечивали доступ к ним на правах администратора с правом доступа к расчетным счетам, после чего удаленно отправляли сгенерированные команды посредством SMS-сообщений на перевод денежных средств на подконтрольные им банковские счета. В результате действия вредоносных программ SMS-уведомления о произведенных операциях потерпевшим не приходили, при этом многие из них узнавали о произошедших у них хищениях спустя продолжительное время после обращений к ним следователей или во время разбирательств о недостаче денежных средств при попытке оплатить кредиты и ипотеку, снять наличные денежные средства в банкоматах. Действия Х., К., Ш. квалифицировались по ч. 2 ст. 159^6 УК РФ[3].

---

[1] Харина Е.А. К вопросу о проблемных аспектах квалификации и криминализации мошенничества в сфере компьютерной информации // Российский следователь. – 2023. – № 3. – С. 31.

[2] Гуц Е. Указ. соч. – С. 168.

[3] Приговор Центрального районного суда г. Тюмени от 3 сентября 2018 г. № 1-18/2018 1-528/2017 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа:.https://sudact.ru/regular/doc/ruiCsHOBEBUQ /(дата обращения: 10.12.2025).

Использование информационных технологий в рамках общего состава рассматривается как способ реализации обмана, а не как конструктивный элемент преступления. Подобный подход позволяет сохранить внутреннюю согласованность уголовного закона и избежать неоправданного расширения специальных норм. Общий состав мошенничества выполняет функцию базовой конструкции, к которой обращаются всякий раз, когда цифровые технологии лишь облегчают контакт с потерпевшим, но не формируют самостоятельный механизм хищения. В итоге статья 159 УК РФ сохраняет роль универсальной нормы, способной адаптироваться к изменяющимся формам мошеннического поведения. Она применяется во всех случаях, когда отсутствуют специальные признаки, прямо выделенные законодателем в иных статьях, и тем самым обеспечивает устойчивость уголовно-правовой оценки как традиционных, так и дистанционных форм обманного посягательства[1].

Выделение мошенничества с использованием электронных средств платежа в самостоятельный состав связано не столько с появлением новых форм обмана, сколько с изменением самого механизма изъятия денежных средств. В условиях безналичных расчётов хищение все чаще осуществляется не через непосредственную передачу имущества потерпевшим, а посредством платёжной инфраструктуры, обеспечивающей дистанционный доступ к счетам[2]. В рамках статьи 159^3 УК РФ именно эта особенность – использование электронных инструментов управления денежными средствами – приобретает определяющее значение для оценки объективной стороны.

По своей правовой природе данное деяние сохраняет признаки мошенничества в его классическом понимании. Хищение совершается путём обмана либо злоупотребления доверием и приводит к имущественному ущербу. Однако в отличие от общего состава, здесь обман не ограничивается

[1] Гуц Е. Указ. соч. – С. 172.

[2] Матюхина Т.И., Ивлев К.А. Электронное средство платежа как средство совершения преступления предусмотренного ст. 159^3 Уголовного кодекса РФ [Электронный ресурс] // Universum: экономика и юриспруденция: электрон. научн. журн. – 2024. – № 1(123). – Режим доступа: https://7universum.com/ru/economy/archive/item/18992 (дата обращения: 10.12.2025).

формированием ошибочного представления у потерпевшего, а направлен на запуск платёжной операции в электронной системе. Итогом становится списание денежных средств со счёта, осуществлённое через платёжный механизм, а не передача имущества «вручную»[1].

Законодательное расширение понятия электронного средства платежа позволило охватить широкий круг технических решений, используемых для распоряжения денежными средствами. Речь идёт не только о банковских картах, но и о системах интернет- и мобильного банкинга, электронных кошельках, терминалах самообслуживания и иных программно-технических средствах[2]. Поэтому для квалификации не имеет принципиального значения, использовался ли физический носитель или программное приложение. Существенным является сам факт совершения операции в рамках платёжной системы, обеспечивающей безналичный оборот.

При этом электронное средство платежа не образует предмет хищения. Оно не изымается и не обращается в пользу виновного, а выполняет вспомогательную роль – служит способом доступа к денежным средствам. Объектом посягательства остаются имущественные отношения, связанные с владением и распоряжением деньгами. Затрагивание интересов устойчивости безналичных расчётов носит производный характер и не формирует самостоятельного элемента объективной стороны.

Практическое значение такого подхода проявляется при разграничении статьи 159^3 УК РФ и общего состава мошенничества. Если обман реализуется в личном общении и приводит к передаче наличных денежных средств, применение специальной нормы исключается. Иная ситуация складывается, когда потерпевший под влиянием ложных сведений переводит деньги на карту, подтверждает операцию в мобильном приложении либо осуществляет оплату через терминал. В этих случаях хищение совершается именно через электронное средство платежа и подлежит квалификации по статье 159^3 УК РФ.

---

[1] Матюхина Т.И., Ивлев К.А. Указ. соч.
[2] Маршева К. С. Указ. соч. – С. 264.

В правоприменении сформировались устойчивые модели таких посягательств. К ним относятся расчёты чужими банковскими картами, в том числе бесконтактные; получение реквизитов и одноразовых кодов под видом служебной необходимости с последующим списанием средств; оплата товаров и услуг за счёт чужих безналичных средств; операции через мобильный банк после получения контроля над номером телефона, привязанным к счёту. В подобных ситуациях обман может быть направлен как на конкретное лицо, так и на платёжную систему, функционирование которой предполагает добросовестное использование средств аутентификации.

Так, в мае 2021 года супружеская пара, действуя в сговоре с неустановленными лицами, организовала фиктивную схему хищения денежных средств интернет-магазина. Мужчина зарегистрировал фирму своей супруги в системе «Портал поставщиков» и разместил предложения о продаже несуществующих услуг для маркетплейса. Неустановленные лица «приобрели» эти товары на общую сумму более 23 млн рублей, указав в качестве способа оплаты реквизиты неплатёжеспособных банковских карт. Из-за недостатков системы проверки поступления средств интернет-магазин перечислил деньги на счёт организации, получившей фиктивную оплату. Часть похищенных средств (примерно 7 млн рублей) была легализована через аффилированные юридические лица[1].

Итак, в обобщённом виде объективная сторона мошенничества с использованием электронных средств платежа выражается в том, что виновный либо самостоятельно инициирует безналичную операцию с применением чужого платёжного инструмента, либо побуждает потерпевшего совершить такую операцию в свою пользу. Обман или злоупотребление доверием направлены на функционирование платёжного механизма, а преступный результат проявляется в списании денежных средств со счёта потерпевшего и

[1] Приговор Вахитовского районного суда города Казани № 1-198/2023 от «18» июля 2023 года [Электронный ресурс] // ГАС «Правосудие». – Режим доступа: https://vahitovsky--tat.sudrf.ru/ (дата обращения: 10.12.2025).

их фактическом получении виновным. Специфика статьи 159^3 УК РФ сводится к необходимости доказать использование электронного средства платежа; иные элементы объективной стороны сохраняют характер, присущий мошенничеству в целом.

Появление статьи 159^6 УК РФ связано с необходимостью уголовно-правовой оценки ситуаций, при которых хищение осуществляется не через прямое воздействие на потерпевшего, а посредством вмешательства в функционирование информационных систем. В подобных делах внимание смещается с межличностного взаимодействия на процессы хранения, обработки и передачи компьютерной информации, поскольку именно через них реализуется механизм изъятия имущества.

Объективная сторона данного состава включает действия, прямо названные в законе: ввод, удаление, блокирование и модификацию компьютерной информации, а равно иные формы вмешательства в работу технических средств и сетей. На практике это выражается в программно-техническом воздействии, нарушающем установленный режим функционирования информационной системы и создающем условия для неправомерного распоряжения имуществом. При расследовании таких дел обычно возникает необходимость установить, какие именно изменения были внесены в систему и каким образом они повлияли на принятие ею управленческих решений, повлекших имущественные потери.

В отличие от иных форм мошенничества, при применении статьи 159^6 обман нередко адресован не конкретному лицу, а автоматизированной системе. Потерпевший может узнать о произошедшем лишь спустя время – при сверке остатков, анализе операций или получении уведомлений от обслуживающей организации. Однако отсутствие непосредственного контакта не устраняет обман как таковой: он проявляется в искажении информационной среды, вследствие чего система воспринимает ложные данные как правомерные и осуществляет операции, ведущие к ущербу.

Манипулирование компьютерной информацией принимает различные формы, что хорошо видно из материалов уголовных дел. В одних случаях речь идёт о корректировке записей в банковских базах данных, в других – об использовании уязвимостей программного обеспечения для инициирования несанкционированных транзакций, в третьих – о вмешательстве в каналы связи между клиентом и кредитной организацией с подменой реквизитов платежей. Общим для этих ситуаций остаётся одно: виновный сознательно формирует такую конфигурацию данных, при которой автоматизированная система осуществляет перечисление денежных средств или иное распоряжение имуществом без законных оснований.

Специфика объективной стороны статьи 159^{6} заключается в сочетании корыстного умысла и компьютерного вмешательства. Данное преступление нельзя отождествлять ни с посягательствами, направленными исключительно на нарушение работы системы, ни с классическими случаями введения потерпевшего в заблуждение путём общения. Техническое воздействие здесь служит инструментом реализации обманного механизма и подчинено цели извлечения имущественной выгоды.

В результате мошенничество в сфере компьютерной информации предстает как особая форма хищения, при которой противоправное обращение имущества осуществляется через искажение цифровых процессов. Объективная сторона выражается в активных действиях по изменению или нарушению работы информационных систем, наступившем имущественном вреде и причинной связи между вмешательством и полученным результатом. Несмотря на технологическую сложность способа, сущность посягательства остаётся неизменной и подлежит оценке в рамках общей логики мошеннических преступлений[1].

В подавляющем количестве случаев преступление совершается путем ввода и модификации информации в корпоративные базы данных компаний. Как правило преступники, являются работниками данных компаний и

[1] Харина Е. А. Указ. соч. – С. 33.

используют свое служебное положение с целью неправомерного завладения денежными средствами клиентов. Так, «умышленно из корыстной заинтересованности, используя свое служебное положение, с целью неправомерного доступа к охраняемой законом компьютерной информации, содержащей персональные данные клиентов ПАО «Вымпелком» и персональные данные их лицевых счетов, с целью ее модификации, под своими индивидуальными и учетными данными осуществила доступ в компьютерную программу «1С»»[1].

Второй типичный способ совершения преступления стоит характеризировать по смыслу п. 20 Постановления Пленума Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», как вмешательство, а именно целенаправленное воздействие программных и программно-аппаратных средства на серверы, средства вычислительной техники и информационно-телекоммуникационные сети. Злоумышленники, используя вредоносное программное обеспечение, взламывают считывающие устройства банкоматов, электронные базы данных и систему защиты аккаунтов. К примеру, «Осуществил ввод компьютерной информации, а именно привнесение новых последовательных электронных сигналов в систему хранения информации с помощью средств ввода, а именно: клавиатуры и соответствующей программы считывания графической информации» [2]. Также распространённым способом совершения анализируемого преступления выступает создание так называемых «фишингсайтов», то есть электронных ресурсов внешне схожих с официальными электронными ресурсами платежных систем и популярных социальных сетей, которые содержат вредоносное программное обеспечение. К примеру, «посредством рассылки на используемые ими абонентские номера

[1] Приговор Октябрьского городского суда РБ 29 июля 2020 года. № 1-243/2020 [Электронный ресурс] // ГАС «Правосудие». – Режим доступа: https://bsr.sudrf.ru/bigs/portal.htm (дата обращения: 10.12.2025).

[2] Приговор Центрального районного суда города Кемерово № 1-573/2020 от «08» сентября 2020 года [Электронный ресурс] // ГАС «Правосудие». – Режим доступа: https://bsr.sudrf.ru/bigs/portal.htm дата обращения: 10.12.2025).

sms-сообщений определенного вида, содержащих ссылку для перехода на сайт «Интернет» – ресурса специального вредоносного компьютерного программного обеспечения».

Так, ФИО19, работая продавцом-консультантом в салоне связи, действовавшем в системе дилерских и субдилерских соглашений с ПАО «Мегафон», имел служебный доступ к информационно-биллинговой системе «Greenfield». Доступ был предоставлен ему в связи с исполнением трудовых обязанностей, после прохождения обучения и под обязательство соблюдения требований информационной безопасности. Использование системы допускалось исключительно для обслуживания абонентов при наличии их волеизъявления и соответствующих заявлений.

Находясь на рабочем месте, ФИО19 использовал предоставленные ему логин и пароль вне служебных целей. Без обращения клиента и при отсутствии каких-либо законных оснований он осуществил вход в биллинговую систему и произвёл действия, не предусмотренные его полномочиями. В частности, им была оформлена сим-карта на абонентский номер, находившийся в салоне связи, при этом в базу данных оператора были внесены заведомо недостоверные сведения об абоненте. Сим-карта была зарегистрирована на третье лицо, не осведомлённое о совершаемых действиях, и привязана к конкретному лицевому счёту. Эти операции повлекли модификацию компьютерной информации и создали возможность распоряжения денежными средствами, учитываемыми в системе оператора.

В дальнейшем ФИО19 реализовал преступный умысел, направленный на завладение денежными средствами. Используя функционал «Greenfield», он выявил сведения об ошибочном платеже, поступившем от абонента ФИО4, скопировал электронные документы, подтверждающие платёж, и на их основе изготовил фиктивное заявление об ошибочном перечислении средств. Данное заявление было зарегистрировано в системе от имени третьего лица, после чего оператор связи, действуя в автоматическом режиме и полагаясь на изменённые

данные, произвёл перевод денежных средств в сумме 8 798 рублей 05 копеек с лицевого счёта ФИО4 на лицевой счёт, подконтрольный ФИО19.

После зачисления денежных средств ФИО19 проверил баланс лицевого счёта через оформленную им сим-карту, а затем посредством мобильного приложения оператора перевёл указанные средства на виртуальную карту платёжной организации. Завершающим этапом стало перечисление денежных средств с виртуальной карты на личный банковский счёт ФИО19, открытый в кредитной организации.

Таким образом, по делу установлено, что ФИО19, используя своё служебное положение и предоставленный ему доступ к охраняемой законом компьютерной информации, осуществил её неправомерную модификацию, что повлекло автоматическое перераспределение денежных средств и их последующее изъятие в свою пользу. Хищение было совершено не путём непосредственного обмана потерпевшего, а через вмешательство в функционирование информационной системы оператора связи, что определило квалификацию содеянного как мошенничество в сфере компьютерной информации[1].

Вывод по параграфу. Мошенничество, совершаемое с применением информационных технологий, сохраняет имущественную природу, но реализуется через иные механизмы причинения вреда. Объективная сторона таких посягательств характеризуется активными действиями, направленными либо на формирование у потерпевшего искажённого представления, либо на вмешательство в функционирование платёжных и информационных систем. Обязательным элементом остаётся наступление реального имущественного вреда и установление причинной связи между действиями виновного и его последствиями. Использование цифровых средств не трансформирует сущность

[1] Приговор Кировского районного суда города Самары № 1-226/2024 от «08» апреля 2024 года [Электронный ресурс] // ГАС «Правосудие». – Режим дорступа: https://kirovsky--sam.sudrf.ru/ (дата обращения: 10.12.2025).

мошенничества, но усложняет структуру охраняемых отношений и требует более точного разграничения общего и специальных составов.

§ 2. Субъективные признаки мошенничеств, совершенных с использованием информационных технологий

Субъективная сторона преступления в уголовно-правовой доктрине рассматривается как обязательный элемент состава, без установления которого исключается возможность привлечения лица к уголовной ответственности. По определению А.И. Рарога, она отражает внутреннюю сторону противоправного поведения и выражается в психическом отношении лица к совершаемому деянию и его последствиям [1]. В научной литературе подчёркивается, что именно через субъективную сторону раскрываются особенности сознательной и волевой деятельности человека, поскольку носителем таких свойств может выступать лишь конкретная личность. В этом смысле субъективная сторона неразрывно связана с субъектом преступления и опосредует его способность осознавать характер совершаемых действий и направлять их в соответствии с избранной линией поведения.

В традиционном понимании содержание субъективной стороны охватывается совокупностью признаков вины, мотива и цели. Эти элементы образуют внутреннее единство и не существуют изолированно друг от друга: вина определяет форму психического отношения к деянию, мотив отражает побудительные причины поведения, а цель фиксирует представление лица о желаемом результате. Их установление требует анализа фактических

[1] Рарог А.И. Вина, ответственность и наказание // Избранное: сборник статей. – Москва: Проспект, 2022. – С. 161.

обстоятельств дела и поведения лица до, во время и после совершения преступления.

Применительно к мошенничеству субъективная сторона характеризуется виной в форме прямого умысла и корыстной направленностью поведения. Лицо осознаёт противоправный характер своих действий, предвидит наступление имущественного вреда и желает его причинения ради извлечения имущественной выгоды. Именно данная совокупность признаков позволяет отграничить мошенничество от гражданско-правовых споров и иных форм неправомерного поведения [1]. Вместе с тем правоприменительная практика показывает, что установление субъективных признаков мошенничества сопряжено с существенными трудностями. Следственные органы нередко сталкиваются с ситуациями, когда виновные выдвигают версии о намерении исполнить принятые на себя обязательства либо о временном характере изъятия денежных средств, что осложняет доказывание умысла и корыстной направленности[2].

Введение специальных составов мошенничества было направлено на повышение определённости квалификации и снижение числа ошибок при расследовании имущественных посягательств. Однако статистические данные свидетельствуют о том, что значительная часть уголовных дел прекращается ещё на стадии предварительного расследования, и одной из причин этого, по мнению А.П. Перетолчина, выступает невозможность надёжного установления субъективной стороны [3]. В результате обостряются проблемы разграничения составов, оценки доказательств и обеспечения баланса между публичными интересами и правами участников уголовного процесса.

---

[1] Залескина А.Н. Особенности установления субъективной стороны мошенничества // Научный дайджест Восточно-Сибирского института МВД России. – 2020. – № 6(9). – С. 91.

[2] Новикова А.И. К вопросу о субъективных признаках мошенничества // Молодой ученый. – 2021. – № 53 (395). – С. 103.

[3] Перетолчин А.П. Уголовная ответственность за мошенничество с использованием электронных средств платежа: дисс. ... канд. юрид. наук: 12.00.08 / Перетолчин Артем Павлович; [Место защиты: ФГАОУ ВО «Дальневосточный федеральный университет»]. – Иркутск, 2021. – С. 142.

В доктрине обращается внимание на то, что для большинства специальных видов мошенничества сохраняются общие признаки хищения, включая форму вины и направленность умысла. Исключение составляет мошенничество в сфере компьютерной информации, где специфика способа совершения деяния влияет на механизм реализации умысла, но не устраняет необходимости доказывания его прямого характера. Следовательно, мотив, цель и вина должны подтверждаться не предположениями, а совокупностью объективных данных, вытекающих из обстоятельств конкретного дела.

Таким образом, установление субъективной стороны мошенничества имеет определяющее значение для правильной уголовно-правовой оценки содеянного. Смещение акцента исключительно на технические способы и средства совершения хищения неизбежно снижает качество квалификации. Без надлежащего выявления внутренней стороны деяния, прежде всего формы вины, применение уголовного наказания противоречит основополагающим принципам уголовного права.

Вина в уголовном праве выступает основным субъективным основанием ответственности и непосредственно выражает принцип субъективного вменения, закреплённый в статье 5 УК РФ. Привлечение лица к уголовной ответственности допустимо лишь при условии установления его виновного отношения к совершенному деянию и наступившим последствиям. Само по себе причинение вреда либо формальное несоответствие поведения требованиям закона не образуют основания уголовной ответственности без доказанного психического отношения лица к содеянному.

В структуре субъективной стороны вина занимает центральное место, тогда как мотив и цель носят факультативный характер и приобретают уголовно-правовое значение лишь в тех случаях, когда прямо предусмотрены законодателем в конструкции состава преступления. Вина представляет собой внутреннее отношение лица к деянию, проявляющееся в форме умысла или неосторожности и находящее внешнее выражение в конкретных действиях. Мотив и цель, в свою очередь, предшествуют формированию преступного

намерения и отражают побудительные причины поведения и представление лица о желаемом результате.

Для мошенничества как интеллектуально сложной формы посягательства характерны специфические трудности доказывания субъективных признаков. На стадии предварительного расследования обвиняемые нередко отрицают корыстную направленность своих действий, представляя произошедшее как неудавшуюся хозяйственную операцию либо добросовестную сделку. Возмещение причинённого ущерба сопровождается ссылками на неблагоприятные обстоятельства, якобы воспрепятствовавшие исполнению обязательств, что используется для отрицания умышленного характера поведения. Подобные версии усложняют установление подлинных побуждений и целей, лежащих в основе совершённого деяния, и остаются одной из наиболее проблемных сторон расследования мошеннических посягательств.

Применительно к мошенничеству, включая его формы, реализуемые с использованием информационных технологий, вина возможна исключительно в форме прямого умысла. Сам характер обмана и злоупотребления доверием предполагает осознанное и целенаправленное поведение, направленное на достижение определённого имущественного результата[1]. В ряде случаев обман адресуется не самому потерпевшему, а третьим лицам или автоматизированным системам, однако это не устраняет необходимости установления преднамеренности действий и их ориентации на причинение имущественного вреда.

Н.А. Лопашенко подчёркивает, что умысел на обман и корыстная цель должны возникнуть до начала реализации соответствующих способов мошенничества[2]. Если намерение сформировалось уже после заключения сделки либо передачи имущества, отсутствует необходимая субъективная

[1] Упоров И.В., Бондарь А.В. Признаки субъективной стороны мошенничества и их значение при отграничении данного вида хищения от иных преступлений // Актуальные вопросы экономики и управления: сб. материалов III Междунар. науч.-практ. конф. – Новосибирск, 2018. – С. 175-180.

[2] Лопашенко Н.А. Преступления против собственности. Книга II. Общая теория хищений. Виды хищения: Авторский курс в 4 книгах. – Москва: Юрлитинформ, 2019. – С. 103.

основа преступления, и содеянное не может квалифицироваться как мошенничество. Данный подход последовательно отражается и в разъяснениях Верховного Суда РФ, ориентирующих правоприменителя на анализ момента возникновения умысла.

Отсутствие прямого умысла исключает уголовную ответственность и переводит спор в плоскость гражданско-правовых отношений. В этой связи принципиальным является разграничение обмана как объективного признака и корыстной цели как элемента субъективной стороны. Наличие факта введения в заблуждение не всегда свидетельствует о стремлении извлечь имущественную выгоду. Лицо может действовать, руководствуясь иными побуждениями – заблуждаясь относительно своих прав, стремясь предотвратить иное неблагоприятное последствие либо действуя по мотивам личной неприязни. В подобных ситуациях обман не сопровождается тем внутренним содержанием, которое требуется для признания деяния мошенничеством.

Пленум Верховного Суда РФ от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» (п. 26) определяет корыстную цель как стремление изъять или обратить чужое имущество в свою пользу либо распорядиться им как собственным. Вместе с тем расширительное толкование данного признака, допускающее неопределённый круг лиц, в пользу которых может быть совершено хищение, вызывает обоснованные возражения среди ученых[1]. Подобный подход размывает границы корыстной цели и ослабляет её разграничительную функцию. Представляется оправданным более сдержанное понимание данного признака, при котором корыстная цель сохраняет чёткую связь с личной имущественной заинтересованностью виновного и поддаётся надёжному доказыванию в рамках конкретного уголовного дела.

При анализе субъективной стороны мошенничества особое внимание должно уделяться мотиву противоправного поведения, поскольку именно он предшествует формированию преступного намерения и опосредует

[1] Яни П.С. Корысть как признак хищения // Законность. – 2019. –№ 3. – С. 23-24

возникновение вины. Умысел не существует автономно от совершаемого деяния: он реализуется и получает уголовно-правовое значение исключительно в процессе совершения преступления. В этой связи корректное установление направленности умысла имеет принципиальное значение для решения вопросов квалификации и разграничения стадий преступной деятельности[1].

В уголовно-правовой теории традиционно различают конкретизированный и неконкретизированный умысел, что приобретает практическое значение при оценке оконченности преступления и квалификации покушения. Так, в ситуациях незаконного завладения электронным средством платежа возможны различные модели дальнейшего поведения виновного. Если лицо намеревается непосредственно изъять денежные средства, например, путём снятия наличных через банкомат, при отсутствии завершения деяния по независящим причинам содеянное подлежит оценке как покушение на кражу. Иная правовая оценка требуется в случаях, когда виновный использует электронное средство платежа, умалчивая о его принадлежности другому лицу, либо привлекая посредников, – здесь незавершённость деяния образует покушение на мошенничество. Аналогичный подход применяется и при квалификации приготовления к преступлению, учитывая, что уголовная ответственность за данную стадию предусмотрена лишь в отношении тяжких и особо тяжких посягательств[2].

В рамках статьи 159 УК РФ, как и в отношении иных форм мошенничества, категория тяжести преступления определяется совокупностью объективных и субъективных факторов, включая размер причинённого ущерба, способ совершения деяния, участие группы лиц либо использование служебного положения. При этом действующее уголовное законодательство последовательно исходит из того, что вина, мотив и цель образуют

[1] Упоров И.В., Бондарь А.В. Признаки субъективной стороны мошенничества и их значение при отграничении данного вида хищения от иных преступлений // Актуальные вопросы экономики и управления: сборник материалов III Международной научно-практической конференции, Новосибирск, 16 января – 13 2018 года. – Новосибирск: Общество с ограниченной ответственностью «Центр развития научного сотрудничества», 2018. – С. 178.
[2] Залескина А.Н. Указ. соч. – С. 94.

взаимосвязанную систему элементов субъективной стороны, каждый из которых подлежит самостоятельному установлению и не может подменять собой другие признаки[1].

Для признания деяния мошенничеством необходимо доказать, что лицо осознавало противоправный характер своего поведения, предвидело возможность наступления общественно опасных последствий и внутренне ориентировалось на их достижение. Данная психическая направленность поведения имеет определяющее значение для уголовно-правовой оценки содеянного. В отношении мошенничества с использованием электронных средств платежа умышленный характер вины фактически вытекает из самой природы деяния: использование заведомо чужого платёжного инструмента объективно исключает возможность добросовестного заблуждения и не допускает причинения имущественного вреда по неосторожности.

В соответствии с действующим уголовным законодательством субъектом мошенничества признаётся вменяемое физическое лицо, достигшее шестнадцатилетнего возраста. Вместе с тем А.П. Перетолчин пишет о заметном смещении возрастной структуры лиц, совершающих такие деяния [2]. Существенную долю осуждённых составляют лица моложе тридцати лет, причём значительная часть из них имеет среднее специальное либо высшее образование. Отмечается устойчивая тенденция к снижению среднего возраста виновных, что объективно связано с ранним и массовым вовлечением молодёжи в использование цифровых технологий и электронных финансовых инструментов.

Указанная динамика закономерна, поскольку именно представители младших возрастных групп наиболее активно осваивают современные информационные и платёжные технологии, обладают практическими навыками работы с мобильными приложениями, интернет-банкингом и дистанционными сервисами. Одновременно это обстоятельство усложняет выявление и

[1] Новикова А.И. Указ. соч. – С. 105.
[2] Перетолчин А.П. Указ. соч. – С. 146.

расследование соответствующих преступлений, требуя привлечения специалистов и использования специальных методов доказывания. В научной литературе справедливо подчёркивается, что лица, совершающие мошенничество в данной сфере, нередко располагают не только теоретическими знаниями, но и устойчивыми прикладными умениями, что напрямую отражается на характере и способе противоправного поведения[1].

При всём разнообразии используемых технических приёмов основой мошенничества неизменно остаётся обман либо злоупотребление доверием, направленные на противоправное обращение чужого имущества. В рассматриваемой сфере таким имуществом выступают безналичные и электронные денежные средства, доступ к которым обеспечивается как посредством материальных носителей, так и через дистанционные каналы связи. Именно сочетание обманного воздействия и имущественного результата позволяет отграничить данные деяния от иных форм неправомерного использования платёжных инструментов.

Распространённость подобных посягательств среди молодых лиц актуализирует вопрос о возрастных границах уголовной ответственности. В доктрине высказываются различные подходы к определению минимального возраста привлечения к ответственности: одни исследователи акцентируют внимание на уровне общественной опасности и распространённости деяния в подростковой среде, другие – на способности лица осознавать противоправный характер своего поведения. Представляется, что при решении данного вопроса необходим комплексный учёт всех указанных факторов, включая социальные и технологические реалии.

Следует учитывать, что гражданское законодательство признаёт частичную дееспособность лица с четырнадцатилетнего возраста. На практике это означает возможность открытия банковского счёта и оформления

---

[1] Уголовно-юрисдикционная деятельность в условиях цифровизации: монография / Н.А. Голованова, А.А. Гравина, О.А. Зайцев и др. – М.: Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации; ООО «Юридическая фирма Контракт», 2019 – С. 108.

платёжной карты при наличии паспорта. Тем самым законодатель исходит из того, что лицо уже в этом возрасте понимает назначение электронных средств платежа, порядок их использования и последствия совершаемых операций. Более того, современные банковские практики демонстрируют ещё более раннее вовлечение несовершеннолетних в безналичный оборот, включая выпуск карт для детей младшего школьного возраста под контролем родителей.

В условиях, когда электронные деньги фактически приравнены по удобству и обороту к наличным, подростки нередко ориентируются в функционале цифровых платёжных сервисов не хуже взрослых. Если уголовный закон допускает привлечение к ответственности с четырнадцати лет за тайное хищение безналичных средств, то логично поставить вопрос о сопоставимости такого подхода с оценкой обманного изъятия тех же имущественных ценностей. Разграничение между кражей и мошенничеством в подобных ситуациях нередко носит формальный характер и порождает неоднозначные правовые последствия.

Иллюстративным является следующий пример судебной практики.

О.П. получила от ФИО1 банковскую карту ПАО «Сбербанк» для приобретения спиртных напитков. Понимая, что передача карты не означала согласия на свободное распоряжение денежными средствами, находящимися на банковском счёте, она использовала предоставленный доступ вопреки воле владельца.

В течение 14 и 15 июля 2018 года карта применялась ею при оплате товаров в ряде торговых точек города Оренбурга. При совершении безналичных расчётов О.П. действовала как лицо, уполномоченное распоряжаться денежными средствами, хотя такого права не имела. Работники магазинов исходили из внешней правомерности операций, что обусловило списание денежных средств со счёта ФИО1. Общая сумма расходов составила 3917 рублей 76 копеек.

На этом противоправные действия не были прекращены. 15 июля 2018 года О.П. прибыла в дополнительный офис ПАО «Сбербанк», располагая

банковской картой и известным ей пин-кодом. Через банкомат она произвела снятие наличных денежных средств со счёта ФИО1 в размере 1500 рублей. Операция была выполнена без уведомления владельца счёта и без его согласия. Полученными денежными средствами О.П. распорядилась самостоятельно[1].

Фактические обстоятельства дела свидетельствуют о последовательном использовании разных способов изъятия денежных средств с одного банковского счёта: сначала посредством безналичных расчётов с применением электронного средства платежа, затем путём снятия наличных через банкомат. Оба способа были реализованы при осознании отсутствия законных оснований для распоряжения чужими денежными средствами и повлекли причинение потерпевшему имущественного вреда.

В этой связи можно задаться вопросом: если обвиняемый не достиг 16 лет, то при сходных обстоятельствах он будет нести ответственность за кражу (ст. 158 УК РФ), но не будет отвечать за мошенничество (ст. 159^3 УК РФ).

С учётом изложенного представляется обоснованным вывод о целесообразности установления уголовной ответственности за мошенничество с использованием электронных средств платежа с четырнадцатилетнего возраста. Такой подход согласуется с уровнем фактической осведомлённости несовершеннолетних о механизмах безналичного оборота, характером причиняемого вреда и тенденциями развития цифровой экономики.

Подводя итог, можно сформулировать следующие положения. Во-первых, субъективная сторона мошенничества с использованием электронных средств платежа по своей структуре не отличается от общего состава мошенничества и выражается в умышленной вине и корыстной направленности поведения. Во-вторых, корыстная цель должна устанавливаться самостоятельно и не подменяться фактом обмана, который относится к объективной стороне преступления. В-третьих, уровень осознания противоправности обманного

[1] Приговор Ленинского районного суда г. Оренбурга (Оренбургская область) № 1-601/2018 от 22 ноября 2018 г. [Электронный ресурс] // Актофакт: архив судебных дел и решений. – Режим доступа: https://actofact.ru/case-56RS0018-1-601-2018-2018-09-28-2-0/ (дата обращения: 10.12.2025).

изъятия безналичных и электронных денежных средств позволяет признать допустимым снижение возраста уголовной ответственности до четырнадцати лет. В этой связи целесообразно рассмотреть внесение соответствующих изменений в часть вторую статьи 20 Уголовного кодекса Российской Федерации, что отвечало бы современным условиям цифрового имущественного оборота и задачам уголовно-правовой охраны.

§ 3. Квалифицированные и особо-квалифицированные признаки мошенничеств, совершенных с использованием информационных технологий

В действующем уголовном законодательстве Российской Федерации квалифицирующие и особо квалифицирующие признаки мошенничества закреплены в статьях 159, 159^3 и 159^6 УК РФ и отражают стремление законодателя дифференцировать уголовную ответственность с учётом характера причинённого вреда, способа совершения преступления и степени общественной опасности деяния.

Общий состав мошенничества, предусмотренный статьёй 159 УК РФ, содержит развернутую систему квалифицирующих обстоятельств. К ним относятся совершение преступления группой лиц по предварительному сговору, причинение значительного ущерба гражданину, использование служебного положения, а также хищение в крупном и особо крупном размере. Эти признаки традиционны для преступлений против собственности и ориентированы прежде всего на оценку последствий деяния и формы соучастия. Значительный, крупный и особо крупный размеры ущерба служат основным критерием усиления ответственности и позволяют учитывать масштаб имущественного вреда независимо от конкретного способа обмана. Использование служебного положения выступает самостоятельным

квалифицирующим обстоятельством, поскольку предполагает злоупотребление доверием, основанным на профессиональном или должностном статусе виновного, и облегчает реализацию преступного умысла.

Статья 159^3 УК РФ, устанавливающая ответственность за мошенничество с использованием электронных средств платежа, по своей структуре во многом воспроизводит модель общего состава, однако адаптирована к особенностям безналичного оборота. В качестве квалифицирующих признаков здесь также закреплены совершение преступления группой лиц по предварительному сговору, использование служебного положения, а равно причинение крупного и особо крупного ущерба. Специфика данной нормы заключается в том, что использование электронного средства платежа изначально включено в объективную сторону основного состава и не рассматривается как отягчающее обстоятельство. Усиление ответственности связано не с техническим способом хищения, а с масштабом причинённого вреда и повышенной опасностью организованных либо должностных форм преступного поведения. Таким образом, законодатель исходит из того, что социальная опасность мошенничества в сфере безналичных расчётов возрастает прежде всего при концентрации имущественного ущерба либо при вовлечении лиц, обладающих специальными полномочиями или доступом к платёжной инфраструктуре.

Особое место занимает статья 159^6 УК РФ, посвящённая мошенничеству в сфере компьютерной информации. В данной норме квалифицирующие признаки связаны не только с размером причинённого ущерба и формами соучастия, но и с характером вмешательства в функционирование информационных систем. Наряду с традиционными обстоятельствами – совершением преступления группой лиц, использованием служебного положения, причинением крупного и особо крупного ущерба – законодатель акцентирует внимание на повышенной опасности посягательств, затрагивающих устойчивость автоматизированных процессов обработки данных. Хотя способы вмешательства (ввод, удаление, модификация информации, иное воздействие на системы) формируют объективную сторону

основного состава, именно сочетание таких действий с крупным имущественным результатом либо организованной формой совершения преступления переводит деяние в разряд квалифицированных и особо квалифицированных.

Можно вывод о единой логике законодательного регулирования. Во всех трёх статьях квалифицирующие признаки направлены на учёт двух основных факторов: масштаба имущественного вреда и степени организованности преступного поведения. Использование информационных технологий и цифровых инструментов само по себе не рассматривается как достаточное основание для ужесточения ответственности, поскольку включено в конструкцию основного состава соответствующих преступлений. Усиление уголовно-правовой реакции обусловлено тем, что цифровая среда облегчает причинение значительного вреда, позволяет действовать группами и использовать служебный доступ, что в совокупности существенно повышает опасность мошенничества для имущественного оборота и доверия к информационным и платёжным системам.

1. Совершение мошенничества группой лиц по предварительному сговору (ч. 2 ст. 159; ч. 2 ст. 159^3; ч. 2 ст. 159^6 УК РФ) и организованными группами (ч. 4 ст. 159; ч. 4 ст. 159^3; ч. 4 ст. 159^6 УК РФ)

Мошенничество будет совершено группой лиц по предварительному сговору в случае, если будет установлено, что: 1. в нем принимали участие не менее чем два лица; 2. данные лица должна заранее договориться о содеянном.

Рассматривая подобного рода преступления, суд обязан установить, что конкретный из участников деяния совершал, какие именно действия были им реализованы, и изложить в приговоре подробно доказательства по каждому преступному лицу.

Мошенничество, совершенное организованной группой лиц либо в особо крупном размере, или повлекшее лишение права гражданина на жилое помещение регламентируется ч. 4 ст. 159 УК РФ. Такое преступление является тяжким и наказывается максимально лишением свободы до 10 лет.

Признаками организованной группы являются: численность, устойчивость, цель объединения и распределение ролей.

Организатор отвечает за все совершенное членами группы, о чем он знал, а участники – лишь за те действия, в которых они участвовали лично.

Для мошенничеств, совершаемых с использованием информационных технологий, характерна особая форма организованности, отличающаяся от традиционных моделей преступных групп. Устойчивость таких объединений нередко обеспечивается не личными связями между участниками, а функциональным распределением ролей и использованием цифровых каналов взаимодействия. В структуре группы могут выделяться лица, отвечающие за техническое вмешательство в информационные системы, участники, обеспечивающие перевод и обналичивание денежных средств, а также так называемые «дропы», формально участвующие в финансовых операциях, но не осведомлённые в полном объёме о механизме преступления.

Особенностью цифровых организованных групп является их территориальная рассредоточенность. Участники могут находиться в разных субъектах Российской Федерации или за её пределами, что не препятствует координации действий за счёт мессенджеров, анонимных сетей и специализированных программных средств. При этом отсутствие личного знакомства между участниками не исключает признания группы организованной, если установлены устойчивость взаимодействия, согласованность действий и подчинённость единому замыслу.

Судебная практика при оценке таких преступлений всё чаще исходит из того, что доказательствами устойчивости и организованности могут служить цифровые следы: история переписки, повторяемость операций, использование единых технических решений и финансовых маршрутов. Тем самым классические признаки организованной группы получают новое содержание, адаптированное к условиям цифровой преступности, где решающее значение имеет не форма контакта между участниками, а функциональная взаимозависимость их действий в рамках единого преступного механизма.

2. Использование служебного положения (ч. 3 ст. 159; ч. 3 ст. 159^3; п. «а» ч. 3 ст. 159^6 УК РФ)

Под использованием служебного положения следует понимать умышленное использование лицом своих служебных полномочий, а также связанных с осуществлением таких полномочий возможностей оказывать влияние, которое определяется значимостью занимаемой им должности, на других лиц в целях совершения им незаконных действий. Использование служебного положения следовало бы определить как дополнительный способ хищения[1].

Пункт 29 Постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» к лицам, использующим свое служебное положение при совершении мошенничества», относит: 1. государственных или муниципальных служащих, которые не являются должностными лицами; 2. должностных лиц, соответствующих признакам, указанным в пункте 1 примечаний к статье 285 УК РФ; 3. иных лиц в соответствии с требованиями пункта 1 примечаний к статье 201 УК РФ (например, лицо, в служебные полномочия которого включены организационно-распорядительные или административно- хозяйственные полномочия в коммерческой организации).

Если говорить об использовании виновным лицом своего служебного положения, необходимо в обязательном порядке представить доказательства того, что совершение мошенничества стало возможным только за счет использования своего должностного положения. Это говорит о том, что должностное лицо, а также служащий муниципальный или государственный, который не считается должностным лицом, лицо, которое исполняет управленческие полномочия в организации, несмотря на интересы своей

[1] Балашова Н.А. Особенности квалификации мошенничества с использованием служебного положения // Вестник Уральского института экономики, управления и права. – 2018. – №1. – С. 23.

службы, использует возможности, которые предоставлены ему исходя из служебных полномочий для осуществления незаконного завладения имуществом, для приобретения права на него[1].

Так, примером привлечения к уголовной ответственности по ч. 3 ст. 159 УК РФ на практике служит приговор Автозаводского районного суда г. Тольятти Самарской области от 20 ноября 2018 года. Согласно приговору Катаев А.В. был признан виновным в совершении преступления, предусмотренного ч.3 ст. 159 УК РФ, т.к. деяние было совершено при выполнении им организационно – распорядительными и административно – хозяйственными функциями в организации, в которой он являлся директором[2].

В условиях цифровизации особое содержание приобретает признак использования служебного положения при совершении мошенничества. В ИТ-среде служебные полномочия нередко выражаются не во властных или управленческих функциях в классическом понимании, а в наличии легитимного доступа к информационным ресурсам, программным интерфейсам и массивам данных. Такое положение характерно для сотрудников операторов связи, банков, платёжных сервисов, аутсорсинговых ИТ-компаний, администраторов информационных систем и иных лиц, чья трудовая функция предполагает работу с цифровой инфраструктурой.

Использование служебного положения в подобных случаях проявляется в выходе за пределы предоставленных полномочий либо в формально правомерном доступе, применённом вопреки целям службы. Преступное поведение может выражаться в изменении записей в базах данных, создании фиктивных учётных записей, неправомерном использовании служебных логинов и паролей, манипулировании алгоритмами обработки информации. Существенно, что такие действия становятся возможными именно благодаря

---

[1] Гончаров Д.Ю., Гончарова С.Г. Квалификация мошенничества, совершенного с использованием служебного положения. // Вестник ВГУ. Сер.: Право. – 2021. – № 3. – С. 283.
[2] Приговор Автозаводского районного суда г. Тольятти Самарской области №1- 749/2018 [Электронный ресурс] // ГАС «Правосудие». – Режим доступа: https://avtozavodsky--sam.sudrf.ru/modules.php?name=sud_delo&srv_num=1/ (дата обращения: 10.12.2025).

профессиональному статусу лица и доверенному ему уровню доступа, недоступному обычным пользователям.

Судебная практика при квалификации подобных деяний исходит из необходимости установить причинную связь между служебным доступом и возможностью совершения мошенничества. Сам факт трудоустройства в организации либо владение техническими навыками не образует данного признака. Определяющим является то, что без использования служебных прав и связанных с ними цифровых возможностей преступление не могло бы быть реализовано либо было бы существенно затруднено. В этом проявляется специфика «служебного положения» в ИТ-сфере, где злоупотребление доверием приобретает технологическую форму и опосредуется механизмами функционирования информационных систем.

3. Причинение значительного (ч. 2 ст. 159; ч. 2 ст. 159^3; ч. 2 ст. 159^6 УК РФ), крупного (ч. 3 ст. 159; ч. 3 ст. 159^3; п. «б» ч. 3 ст. 159^6 УК РФ) и особо крупного ущерба (ч. 4 ст. 159; ч. 4 ст. 159^3; ч. 4 ст. 159^6 УК РФ) как квалифицирующий признак

Значительный ущерб является нефиксированной суммой, определяется из того, какое имущественное положение занимает потерпевшее лицо. Важно отметить, что данная сумма не должна быть менее пяти тысяч рублей.

Следует иметь в виду, что размер мошенничества определяется исходя из стоимости похищенного имущества на день совершения преступления, а при определении ущерба, подлежащего возмещению, необходимо учитывать стоимость имущества на день принятия решения о возмещении вреда с последующей индексацией на момент исполнения приговора.

Такой ущерб оценивается исходя из имущественного положения потерпевшего, но не может составлять менее пяти тысяч рублей.

То есть данная сумма не считается единственным критерием, который бы говорил о значительности причиненного ущерба потерпевшему лицу. В каждом случае нужно в обязательном порядке учитывать имущественное положение потерпевшего, а именно установить его доход, с какой периодичностью он его

получает, есть ли на его иждивении лица, требующие определенных затрат, установить совокупный доход всех членов семьи, с которым он имеет совместное хозяйство. Мнение потерпевшего лица о значительности причиненного ему ущерба должно рассматриваться судом совместно с материалами дела, которые подтверждают стоимость похищенного имущества, а также само имущественное положение потерпевшего[1].

Таким образом, значительность ущерба, который причинен, например, безработному лицу, имеющему на иждивении трех малолетних детей, и директору магазина, имеющему постоянный, стабильный доход, будет различна.

Следовательно, понятие значительного ущерба является оценочным, он исходит не только из вышеперечисленных пунктов, но и из таких факторов, как наличие автомобиля, недвижимости и т.д.

Размер причиненного ущерба путем мошеннических действий определяется исходя из стоимости похищенного имущества на день совершения противоправного, уголовно-наказуемого деяния, а при определении ущерба, который подлежит возмещению потерпевшему лицу стоит учитывать стоимость имущества на день принятия решения овозмещении вреда с соответствующей последующей индексацией на момент исполнения приговора суда.

Крупным размером признается стоимость имущества, превышающая двести пятьдесят тысяч рублей, а особо крупным – один миллион рублей.

4. Мошенничество в сфере компьютерной информации, совершенное с банковского счета, а равно в отношении электронных денежных средств (п. «в» ч. 3 ст. 159^6 УК РФ).

Понятие электронного средства платежа дано в п. 19 ст. 3 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе». Это средство и (или) способ, позволяющие клиенту оператора по переводу

[1] Корниенкова М.Р., Русскевич Л.А. Особенности и проблемы квалификации мошенничества // Вестник экономической безопасности. – 2024. – № 1. – С. 117.

денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств.

Хищение денежных средств с банковского счета, а равно в отношении электронных денежных средств возможно и путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, что является специальным видом мошенничества и влечет уголовную ответственность по п. «в» ч. 3 ст. 159^6 УК РФ.

По смыслу ст. 159^6 УК РФ вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей признается целенаправленное воздействие программных и (или) программно-аппаратных средств на серверы, средства вычислительной техники (компьютеры), в том числе переносные (портативные) – ноутбуки, планшетные компьютеры, смартфоны, снабженные соответствующим программным обеспечением, или на информационно-телекоммуникационные сети, которое нарушает установленный процесс обработки, хранения, передачи компьютерной информации, что позволяет виновному или иному лицу незаконно завладеть чужим имуществом или приобрести право на него (п. 20 Постановления Пленума Верховного Суда РФ от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате»).

ГЛАВА 3. ПРОБЛЕМЫ КВАЛИФИКАЦИИ И ОТГРАНИЧЕНИЯ МОШЕННИЧЕСТВ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

§ 1. Отграничение мошенничеств, совершенных с использованием информационных технологий от смежных составов преступлений

Вопросы разграничения составов, предусмотренных статьями 159, 159^3 и 159^6 УК РФ, а также их разграничения с иными формами хищения, длительное время остаются предметом устойчивых споров в следственной и судебной практике. Причина этих затруднений заключается не только в внешнем сходстве соответствующих деяний, но и в трансформации самого механизма хищения в условиях безналичного оборота и автоматизированных платёжных систем. Использование электронных платёжных инструментов и программно-технической инфраструктуры приводит к тому, что традиционные признаки изъятия имущества утрачивают наглядность, а момент выбытия денежных средств становится опосредованным и распределённым во времени.

После введения специальных норм о мошенничестве с использованием электронных средств платежа и мошенничестве в сфере компьютерной информации правоприменение столкнулось с отсутствием единых ориентиров квалификации.

Федеральный закон «О национальной платежной системе» объясняет различие между электронными деньгами и традиционными безналичными расчётами. Электронные деньги существуют в цифровом виде, не привязаны к конкретному счёту и могут использоваться только через специальные платежные инструменты, такие как электронные кошельки и мобильные приложения. Безналичные деньги, напротив, связаны с банковским счётом и могут переводиться без использования электронных средств платежа.

Примечателен случай, связанный с использованием системной ошибки в бонусной программе лояльности одной российской авиакомпании. Осуждённый воспользовался сбоем, позволявшим оплачивать авиабилеты бонусными милями с заблокированного счёта, при этом фактически мили с баланса не списывались. Суд первой инстанции квалифицировал эти действия как мошенничество с использованием электронных средств платежа (ч. 4 ст. 159^3 УК РФ). Однако апелляционная инстанция сочла такую квалификацию неправомерной, указав, что бонусные мили не являются электронными средствами платежа в понимании закона, а деяние не содержало признаков хищения, поскольку имущество авиакомпании не выбыло из её владения. В действиях осуждённого был усмотрен обман, направленный на извлечение материальной выгоды за счёт неполученных доходов авиакомпании. В результате преступление было переквалифицировано по п. «б» ч. 2 ст. 165 УК РФ как причинение имущественного ущерба путём обмана без признаков хищения[1].

Одни и те же по существу действия – списание денежных средств со счёта через дистанционные сервисы – в зависимости от подхода следователя или суда получали оценку либо как общее мошенничество, либо как специальный состав по статье 159^3 УК РФ, либо как кража. Нередко решающим аргументом становилось то обстоятельство, что владелец счёта не участвовал в передаче имущества и узнавал о произошедшем уже после совершения операций, что воспринималось как признак тайного изъятия.

Эти противоречия нашли отражение и в доктрине. Так, П. С. Яни последовательно обосновывает квалификацию использования чужой банковской карты при оплате товаров в торговой организации как мошенничества с применением электронных средств платежа, указывая на

[1] Приговор № 22-2816/2023 22-8/2024 от 17 января 2024 г. (Суд Ханты-Мансийского автономного округа (Ханты-Мансийский автономный округ-Югра)) // Судебные и нормативные акты РФ [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/8PZTV2464SmQ (дата обращения: 10.12.2025).

наличие обманного механизма в платёжном обороте [1]. М. А. Филатова, напротив, исходит из того, что при отсутствии взаимодействия с потерпевшим и при незнании им о совершаемых операциях подобные действия образуют состав кражи [2]. Данная дискуссия во многом отражала реальное состояние практики, в которой единообразие оценок отсутствовало.

Характерным примером стала ситуация, рассмотренная по делу Кактана Ю. Ю. Установлено, что он обнаружил банковскую карту потерпевшего с функцией бесконтактной оплаты и в течение двух дней использовал её для оплаты покупок в магазинах и кафе. Со счёта было списано 3 026,54 рубля; дальнейшее распоряжение средствами оказалось невозможным вследствие блокировки карты владельцем. Суд первой инстанции квалифицировал содеянное как покушение на кражу с банковского счёта (ч. 3 ст. 30, п. «г» ч. 3 ст. 158 УК РФ), апелляционная инстанция лишь исключила признак причинения значительного ущерба.

Шестой кассационный суд общей юрисдикции, напротив, переквалифицировал действия осуждённого на покушение на мошенничество с использованием электронных средств платежа (ч. 3 ст. 30, ч. 1 ст. 159^3 УК РФ), сославшись на умолчание о незаконном владении картой. Однако заместитель Генерального прокурора Российской Федерации обоснованно указал, что при бесконтактной оплате сотрудники торговых организаций не участвуют в распоряжении денежными средствами и не вводятся в заблуждение, а после изменений 2018 года законодатель специально выделил кражу с банковского счёта в п. «г» ч. 3 ст. 158 УК РФ. Верховный Суд Российской Федерации поддержал эту позицию, отметив, что исключение из диспозиции статьи 159^3

---

[1] Яни П.С. Хищение с использованием чужой банковской карты в магазине следует квалифицировать как мошенничество // Законность. – 2020. – № 12. – С. 42.

[2] Филатова М.А. Хищение с использованием чужой банковской карты в магазине образует состав кражи // Законность. – 2020. – № 12. – С. 37.

УК РФ указания на обман уполномоченного работника изменило границы применения данной нормы[1].

Несмотря на разъяснения, данные Верховным Судом Российской Федерации, в правоприменительной практике сохраняются сложности при разграничении мошенничества с использованием электронных средств платежа, предусмотренного статьёй 159^3 УК РФ, и мошенничества в сфере компьютерной информации, ответственность за которое установлена статьёй 159^6 УК РФ. Наиболее проблемными являются ситуации, когда в рамках одного эпизода противоправное изъятие денежных средств осуществляется с применением нескольких технологических приёмов, сочетающих использование платёжных сервисов и воздействие на программно-техническую инфраструктуру.

Позиция Пленума Верховного Суда ориентирует правоприменителя на анализ способа совершения посягательства. Если имущественный результат достигнут путём неправомерного доступа к компьютерной информации, модификации данных, использования вредоносного программного обеспечения либо иного вмешательства в установленный порядок обработки, хранения или передачи информации, содеянное подлежит квалификации по статье 159^6 УК РФ.

Якутский городской суд вынес приговор в отношении двух участников организованной группы, признав их виновными в совершении мошенничества в сфере компьютерной информации (ст. 159^6 УК РФ). Преступная схема была организована следующим образом. Участники группы получили незаконный доступ к локальной сети банка, серверам и компьютерам сотрудников с помощью вредоносных программ, которые позволяли обходить системы защиты информации. Используя данные программы, злоумышленники модифицировали компьютерную информацию и вмешивались в работу

[1] Определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 29.09.2020 № 12-УДП20-5-К6 [Электронный ресурс] // КонсультантПлюс: справ.-правов. сист. – URL: www.consultant.ru (дата обращ.: 10.12.2025).

автоматизированных систем, в частности – управляли программным обеспечением банкоматов. В ходе реализации преступного плана неустановленные участники группы устанавливали на серверы и ПК банка программные модули, обеспечивавшие скрытое управление банкоматами. После этого с помощью специального программного обеспечения банкоматам передавались команды на цикличную выдачу денежных средств. Таким образом, происходила фактическая модификация данных о состоянии кассет банкоматов и формирование несанкционированных команд на выдачу наличных. Осужденные в этой схеме исполняли роль так называемых «обналичников». Они по указаниям организатора выезжали к заранее определённым банкоматам и извлекали выданные денежные средства. В данном случае хищение денежных средств было совершено путём модификации компьютерной информации и иным вмешательством в функционирование средств хранения, обработки и передачи компьютерной информации[1].

Если деньги списываются с чужой карты через банкомат без ведома владельца, такие деяния квалифицируются как кража. Если карта предъявляется сотруднику банка или магазина с целью завладения средствами, это мошенничество с использованием электронных средств платежа (статья 159^3 УК РФ). Так, гражданка, используя найденную банковскую карту, совершила серию покупок в торговых точках города Торжка Тверской области на сумму более 12 тыс. рублей. Суд квалифицировал ее действия по статье 159^3 УК РФ[2]. В аналогичных обстоятельствах гражданин платил найденной картой

[1] Приговор № 1-681/2019 от 26 августа 2019 г. по делу № 1-1462/2018 (Якутский городской суд (Республика Саха (Якутия))) // Судебные и нормативные акты РФ [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/8jIATe7oVfNK (дата обращения: 10.12.2025).

[2] Приговор № 1-60/2020 от 16 июля 2020 г. по делу № 1-60/2020 (Торжокский городской суд (Тверская область)) // Судебные и нормативные акты РФ [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/3aVp8BqhtdQ1 (дата обращения: 10.12.2025).

путем бесконтактной оплаты, действия квалифицированы по п. «г» ч. 3 ст. 158 УК РФ[1].

Верховный Суд указал, что хищение денежных средств путем оплаты товаров с использованием чужой банковской карты подлежит квалификации как кража, совершенная с банковского счета (п. «г» ч. 3 ст. 158 УК РФ) (п. 49 Обзора судебной практики Верховного Суда Российской Федерации № 3 (2021), утв. Президиумом Верховного Суда РФ 10.11.2021)[2].

На практике суды квалифицируют по статье 159^6 УК РФ деяния, которые следовало бы квалифицировать по ст. 158 или 160 УК РФ[3]. Например, бухгалтер, совершающий фиктивные платежи через интернет-банк, может быть осужден за мошенничество в сфере компьютерной информации, хотя фактически его действия ближе к мошенничеству. Такая правоприменительная практика остается спорной и требует уточнения.

Хищение также может происходить путем доступа к учетным данным владельца карты. Верховный Суд рекомендует квалифицировать такие действия как кражу[4], но на практике возникают разночтения, особенно при удаленном переводе средств. Так, Т.Н.Д. тайно завладел мобильным телефоном Л.С.В., на котором было установлено приложение «Сбербанк Онлайн» с учётной записью потерпевшего. Воспользовавшись телефоном и привязанной к нему банковской картой, Т.Н.Д. дистанционно оформил от имени Л.С.В. кредит в ПАО «Сбербанк России» на сумму 7 000 рублей, а также получил микрозаймы в размере 9 000, 4 000 и 12 700 рублей в нескольких

---

[1] Приговор № 1-1139/2023 от 27 декабря 2023 г. по делу № 1-1139/2023 (Подольский городской суд (Московская область)) // Судебные и нормативные акты РФ [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/I2zXxHzWLTbv (дата обращения: 10.12.2025).

[2] Обзор судебной практики Верховного Суда Российской Федерации № 3 (2021), утв. Президиумом Верховного Суда РФ 10.11.2021) // КонсультантПлюс: справ.-правов. сист. – URL: www.consultant.ru (дата обращ.: 10.12.2025).

[3] Кассационное определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 01.06.2021 № 5-УДП21-44-К2 // КонсультантПлюс: справ.-правов. сист. – URL: www.consultant.ru (дата обращ.: 10.12.2025).

[4] О судебной практике по делам о мошенничестве, присвоении и растрате: Постановление Пленума Верховного Суда РФ от 30.11.2017 г. № 48 // Бюллетень Верховного Суда РФ. – 2018. – № 2.

микрофинансовых организациях. Полученные средства были зачислены на банковский счёт Л.С.В. Представитель ПАО «Сбербанк России», признанного потерпевшим, указал, что действия Т.Н.Д. следовало квалифицировать как кражу с банковского счёта (п. «г» ч. 3 ст. 158 УК РФ), поскольку доступ к денежным средствам был получен путём использования персональных данных владельца, а не путём обмана банка. При этом фактическое возмещение ущерба было осуществлено самим Л.С.В., который погасил кредит за свой счёт. Суд кассационной инстанции признал, что действия Т.Н.Д. ошибочно квалифицированы по ч. 1 ст. 159 УК РФ. Суд указал, что, по существу, имело место тайное хищение денежных средств с банковского счёта, что подпадает под признаки кражи по п. «г» ч. 3 ст. 158 УК РФ[1].

При наличии самостоятельных признаков посягательства на информационную безопасность возможна дополнительная квалификация по статьям 272, 273 или 274^1 УК РФ. В тех случаях, когда виновное лицо использует электронное средство платежа – банковскую карту, мобильное приложение, интернет-банк – в пределах предусмотренного системой функционала, не нарушая алгоритмов её работы, правовая оценка осуществляется по статье 159^3 УК РФ либо, при отсутствии признаков специального состава, по статье 159 УК РФ.

Фактические механизмы преступлений, однако, нередко выходят за рамки таких упрощённых конструкций. Распространены схемы, при которых обман применяется на первоначальном этапе – для получения логинов, паролей, одноразовых кодов подтверждения, – тогда как последующее распоряжение денежными средствами осуществляется через вход в учётную запись и проведение операций, формально допустимых для системы, но не санкционированных владельцем. В подобных случаях обман и технические действия образуют единую причинную цепочку, но сохраняют относительную

[1] Приговор № 1-479/2023 1-63/2024 от 10 января 2024 г. по делу № 1-479/2023 (Советский районный суд г. Брянска (Брянская область)) // Судебные и нормативные акты РФ [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/CqaUmhM7Lvq (дата обращения: 10.12.2025).

самостоятельность. Это исключает автоматическую квалификацию по одной статье и требует либо оценки по совокупности преступлений, либо учёта стадийности противоправного поведения.

На практике именно такие комбинированные ситуации чаще всего приводят к квалификационным ошибкам. Формальное отнесение всего комплекса действий либо к статье 159^3 УК РФ, либо к статье 159^6 УК РФ без анализа их последовательности и функционального назначения искажает уголовно-правовую оценку. В одних случаях из поля зрения выпадает вмешательство в компьютерную информацию, в других – необоснованно криминализируется обычное использование платёжного инструмента, не выходящее за пределы штатной работы системы. Это подтверждает, что при оценке технологически сложных посягательств решающим является восстановление фактического механизма хищения и установление тех действий, которые непосредственно обеспечили выбытие имущества.

Отсутствие прямого контакта между виновным и владельцем денежных средств само по себе не определяет квалификацию. В безналичном обороте изъятие осуществляется не путём физической передачи, а посредством исполнения распоряжений оператором перевода денежных средств. Поэтому для разграничения кражи, предусмотренной статьёй 158 УК РФ, и мошенничества по статьям 159, 159^3 или 159^6 УК РФ существенным является не факт личного общения с собственником, а способ возникновения у виновного возможности распоряжаться чужими средствами. Если списание произошло без формирования заблуждения у какого-либо лица и без использования доверительных отношений – например, при тайном использовании найденной банковской карты без обмана и без технического вмешательства, – квалификация по статье 158 УК РФ может быть обоснованной. Напротив, когда имущественный результат обусловлен тем, что потерпевший либо иное лицо, обеспечивающее сохранность доступа к счёту, действовало под влиянием ложных сведений или умолчания, сохраняются основания для квалификации как мошенничества.

Пограничные ситуации наглядно проявляются при использовании одноразовых кодов подтверждения. Формально распоряжение о переводе формирует злоумышленник, а операцию исполняет банк; однако предварительное введение потерпевшего в заблуждение – под видом «защиты счёта», «проверки операции» или «отмены списания» – выступает необходимым условием доступа к денежным средствам. В таких случаях обман сохраняет уголовно-правовое значение, несмотря на то что потерпевший сам не инициировал перевод, что позволяет квалифицировать содеянное по статьям 159 или 159^{3} УК РФ.

Особую категорию образуют схемы, при которых обман адресован не владельцу денежных средств, а третьим лицам, от действий которых зависит режим доступа к платёжным сервисам. К ним относятся эпизоды неправомерного восстановления контроля над номером телефона либо переоформления SIM-карты, когда работник оператора связи вводится в заблуждение относительно законности совершаемых действий. В результате злоумышленник получает доступ к мобильному банку и инициирует списание средств. Потерпевший при этом исключён из коммуникации не по собственной воле, а вследствие созданной преступником конфигурации доступа; имущественный ущерб наступает через опосредованное, но причинно обусловленное обманом поведение третьего лица. Такие действия подлежат квалификации как мошенничество, а при наличии вмешательства в информационные системы – по статье 159^{6} УК РФ с возможной совокупностью.

Современная позиция Верховного Суда Российской Федерации исходит из того, что заблуждение не обязательно должно формироваться у собственника имущества. Достаточно, чтобы обман был адресован лицу, чьи действия обеспечили выбытие имущества либо возникновение у виновного возможности распоряжаться им. Следовательно, отсутствие прямого контакта с владельцем средств не исключает мошенничества; исключающим фактором является отсутствие обманного или доверительного механизма, послужившего причиной имущественного результата.

Вопрос квалификации преступлений, связанных с хищением безналичных и электронных денежных средств остается актуальным. Существующая редакция уголовного законодательства содержит ряд норм, предусматривающих ответственность за такие преступления, но их разграничение на практике вызывает сложности. Это особенно заметно в случае кражи с банковского счета, мошенничества с использованием электронных средств платежа и мошенничества в сфере компьютерной информации, так как все эти преступления схожи по предмету посягательства и способу их совершения.

Анализ правоприменительной практики и доктринальных подходов к квалификации мошенничеств, совершаемых в цифровой среде, позволяет говорить о системной избыточности статьи 159^6 УК РФ и обоснованности её исключения из Уголовного кодекса Российской Федерации. Выделение мошенничества в сфере компьютерной информации в самостоятельный состав не устранило квалификационные коллизии, а, напротив, усложнило разграничение смежных норм и привело к устойчивой неопределённости при оценке механизма хищения.

По своей юридической природе деяния, охватываемые статьёй 159^6 УК РФ, не формируют самостоятельного вида посягательства на собственность. Применение компьютерных технологий, программных средств и информационных систем не трансформирует сущность мошенничества как хищения, основанного на обмане либо злоупотреблении доверием, а лишь отражает конкретную форму реализации преступного умысла. При этом неправомерное воздействие на компьютерную информацию уже охватывается нормами главы 28 УК РФ и не требует дублирования в специальной имущественной норме.

Сохранение статьи 159^6 УК РФ фактически стирает границы между преступлениями против собственности и преступлениями против информационной безопасности. Это порождает конкуренцию уголовно-правовых норм и затрудняет выбор надлежащей квалификации. На практике

сходные по механизму деяния получают различную правовую оценку в зависимости от формального описания способа, что не соответствует требованиям правовой определённости и единообразия применения уголовного закона.

В целях устранения указанных противоречий целесообразно отказаться от конструкции «мошенничества в сфере компьютерной информации» как самостоятельного состава и сосредоточить регулирование цифровых форм мошенничества в рамках одной специальной нормы – статьи 159^3 УК РФ. При этом диспозиция указанной статьи должна охватывать как использование электронных средств платежа, так и иные компьютерные технологии, применяемые для обманного изъятия имущества.

Неправомерное воздействие на компьютерную информацию, выражающееся в несанкционированном доступе, модификации данных либо использовании вредоносных программ, при таком подходе подлежит самостоятельной уголовно-правовой оценке по статьям 272, 273 и 274^1 УК РФ по правилам совокупности преступлений. Искусственное «поглощение» подобных действий специальным составом мошенничества не требуется и не отвечает логике системного построения уголовного закона.

Предлагаем исключить из УК РФ ст. 159^6, а ст. 159^3 и изложить в следующей редакции.

Статья 159^3. Мошенничество с использованием электронных средств платежа или в сфере компьютерной информации

1. Мошенничество, то есть хищение чужого имущества либо приобретение права на чужое имущество путём обмана или злоупотребления доверием, совершённое с использованием электронных средств платежа или в сфере компьютерной информации, –

наказывается штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо ограничением

свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на срок до трех лет.

2. То же деяние, совершенное группой лиц по предварительному сговору, а равно с причинением значительного ущерба гражданину, -

наказывается штрафом в размере до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до двух лет, либо обязательными работами на срок до четырехсот восьмидесяти часов, либо исправительными работами на срок до двух лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до одного года или без такового, либо лишением свободы на срок до пяти лет с ограничением свободы на срок до одного года или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные лицом с использованием своего служебного положения, а равно в крупном размере, -

наказываются штрафом в размере от ста тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до двух лет или без такового, либо лишением свободы на срок до шести лет со штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев либо без такового и с ограничением свободы на срок до полутора лет либо без такового.

4. Мошенничество в сфере компьютерной информации, совершенное с банковского счета, а равно в отношении электронных денежных средств,

наказываются штрафом в размере от ста тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до двух лет или без такового, либо лишением свободы на срок до шести лет со штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за

период до шести месяцев либо без такового и с ограничением свободы на срок до полутора лет либо без такового.

5. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, совершенные организованной группой либо в особо крупном размере, -

наказываются лишением свободы на срок до десяти лет со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового и с ограничением свободы на срок до двух лет либо без такового.

Примечание. Под мошенничеством в сфере компьютерной информации понимается хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Таким образом, квалификация по статьям 158, 159, 159^3 и 159^6 УК РФ требует не формальной фиксации используемых технологий, а детального анализа объективной стороны: каким образом был получен доступ к денежным средствам, за счёт каких действий сформировано распоряжение и имело ли место вмешательство в установленный порядок обработки компьютерной информации. Именно этот анализ позволяет избежать подмены мошенничества кражей, необоснованного применения статьи 159^6 УК РФ либо игнорирования совокупности преступлений.

Мы считаем, что действующее законодательство нуждается в пересмотре, поскольку существующая система квалификации преступлений, связанных с хищением безналичных и электронных денежных средств, порождает правоприменительные сложности. Если закон будет четко определять, какие преступления подпадают под новый состав, это позволит сократить ошибки в квалификации и повысит эффективность расследования.

§ 2. Квалификация мошенничеств, совершенных с использованием информационных технологий и проблемы, возникающие в практике следственных и судебных органов

Обман потерпевших, как правило, осуществляется одними лицами, тогда как получение, перемещение и обналичивание денежных средств возлагается на иных участников, выполняющих вспомогательные функции. В результате уголовному преследованию преимущественно подвергаются курьеры и лица, предоставляющие банковские счета для движения похищенных средств («дропы»), тогда как организаторы преступных схем во многих делах остаются вне пределов процессуальной досягаемости.

Подобная схема соучастия существенно осложняет уголовно-правовую оценку содеянного. Отсутствие у курьеров и дропов прямого контакта с потерпевшими неизбежно ставит вопрос о пределах их ответственности, форме соучастия и реальном содержании умысла. Анализ приговоров свидетельствует, что суды нередко признают указанных лиц соисполнителями мошенничества, исходя из их включённости в общий механизм преступления и осознания противоправного характера совершаемых действий. Вместе с тем доказательственная база по таким делам часто ограничивается перепиской в мессенджерах и совокупностью косвенных данных, что приводит к различиям в правовой оценке и назначаемых наказаниях при сходных фактических обстоятельствах.

Анализ судебных решений по делам данной категории выявляет различия в подходах к квалификации и оценке роли участников преступной схемы, что свидетельствует об отсутствии устойчивого единообразия при применении норм уголовного закона о соучастии. Для конкретизации обозначенных проблем в настоящей работе рассмотрены четыре приговора по делам о дистанционных мошенничествах, при этом три из них вынесены в отношении лиц, выполнявших функции курьеров и непосредственно участвовавших в

получении денежных средств у потерпевших, – Сидорова С.И. [1], Зареева Д.Р. [2] и Кузнецова Н.С. [3], а один приговор – в отношении лица, использовавшего банковские реквизиты для приёма и перераспределения похищенных денежных средств, – Салихова Р.М. [4] Сопоставление указанных судебных актов позволяет проследить, каким образом суды соотносят фактическое содержание действий подсудимых с признаками мошенничества, разграничивают формы соучастия, устанавливают умысел и индивидуализируют наказание при различной роли лица в общем механизме преступления.

Исследование судебных приговоров по делам о дистанционных мошенничествах позволяет констатировать, что курьеры и дропы включаются в преступный механизм на различных этапах и выполняют неодинаковые по содержанию функции. Вместе с тем при уголовно-правовой оценке содеянного это различие нередко сглаживается, что приводит к формальному уравниванию их правового статуса.

Так, курьеры, привлекавшиеся к ответственности (дела Сидорова С.И., Зареева Д.Р. и Кузнецова Н.С.), действовали по инструкциям, получаемым через мессенджеры, и выполняли функции по получению денежных средств у потерпевших с их последующей передачей либо переводом третьим лицам. При этом они не участвовали в переговорах с потерпевшими и не формировали ложные представления, лежащие в основе обмана. Несмотря на это, суды исходят из того, что именно действия курьеров обеспечивают завершённость мошеннической схемы, и квалифицируют их поведение как соисполнительство

---

[1] Приговор Зеленодольского городского суда Республики Татарстан № 1-42/2024 от 31 мая 2024 года (УИД: 16RS0040-01-2023-003885-04) // Зеленодольский городской суд Республики Татарстан. – URL https://zelenodolsky--tat.sudrf.ru (дата обращения 01.12.2025).

[2] Приговор Чистопольского городского суда Республики Татарстан № 1-136/2024 от 09 апреля 2024 года (УИД: 16RS0040-01-2024-000756-95) // Чистопольский городской суд Республики Татарстан. – URL https:// https://chistopolsky.tat.sudrf.ru/ (дата обращения 01.12.2025).

[3] Приговор Зеленодольского городского суда Республики Татарстан № 1-140/2024 от 11 июня 2024 года (УИД: 16RS0040-01-2024-000256-43) // Зеленодольский городской суд Республики Татарстан. – URL https://zelenodolsky--tat.sudrf.ru (дата обращения 01.12.2025).

[4] Приговор Вятскополянского районного суда Кировской области № 1-5/2025 от 14 января 2025 года (УИД: 16RS0040-01-2024-007180-29) // Вятскополянский районный суд Кировской области. – URL: https://vyatskopolyansky--kir.sudrf.ru/ (дата обращения 01.12.2025).

по ч. 2–3 ст. 159 УК РФ, не придавая самостоятельного значения отсутствию личного участия в обмане.

Иная роль прослеживается в деле Салихова Р.М., где подсудимый использовал банковские реквизиты для приёма, перераспределения и обналичивания похищенных денежных средств. Он не взаимодействовал с потерпевшими и подключался к преступной схеме после фактического изъятия денежных средств. Тем не менее суд квалифицировал его действия как мошенничество, что фактически приводит к размыванию границы между хищением и последующими операциями с похищенным.

Можно сделать вывод, что в правоприменительной практике приоритет был отдан формальному включению лица в преступную схему, тогда как реальное содержание его действий и степень влияния на обман потерпевшего остаются на втором плане, что ставит под сомнение обоснованность признания курьеров и дропов соисполнителями без дифференциации их фактической роли.

В судебной практике по делам о дистанционных мошенничествах выработался подход, при котором лица, выполняющие функции курьеров, как правило, рассматриваются судами в качестве соисполнителей преступления. Это наглядно прослеживается в приговорах по делам Сидорова С.И., Зареева Д.Р. и Кузнецова Н.С., где подробно описан согласованный характер действий подсудимых и «неустановленных лиц», подчёркивая их включённость в общий преступный механизм и подчинённость инструкциям, получаемым от неустановленных лиц посредством мессенджеров.

При таком подходе содержание объективной стороны мошенничества зачастую остаётся вне самостоятельной оценки. Курьеры не участвуют в формировании обмана, не ведут переговоров с потерпевшими и не создают ложных представлений, послуживших основанием для передачи денежных средств. Их действия направлены на реализацию уже состоявшегося обмана и фактическое изъятие денежных средств, что по своему характеру сближает их роль с содействием совершению преступления. Тем не менее возможность

квалификации таких действий как пособничества судами, как правило, не анализируется.

Иная по содержанию, но сходная по правовой оценке ситуация имеет место в деле Салихова Р.М.. Подсудимый использовал банковские реквизиты для приёма, перераспределения и обналичивания похищенных денежных средств, не взаимодействуя с потерпевшей и не влияя на формирование её волеизъявления. Несмотря на это, суд квалифицировал его действия как мошенничество, фактически приравняв по объёму уголовной ответственности к лицам, непосредственно участвовавшим в обмане.

Подобный подход приводит к смешению различных стадий преступной деятельности, при котором хищение отождествляется с последующим распоряжением похищенными средствами. В результате различия в фактической роли участников нивелируются, а объём уголовной ответственности определяется преимущественно степенью формальной включённости в преступную схему.

Показательной является и позиция суда по делу Салихова Р.М. в части квалифицирующих признаков, где признак «значительного ущерба» был исключён как поглощённый признаком «крупного размера». В то же время в иных судебных актах оба признака применяются одновременно без специального обоснования, что указывает на отсутствие устойчивых ориентиров в оценке последствий преступления.

Аналогичная неоднородность прослеживается и при установлении субъективной стороны. Доводы подсудимых о неосознании преступного характера выполняемых действий судами, как правило, отвергаются со ссылкой на элементы конспирации – маскировку, смену одежды, запрет на обсуждение деталей и использование анонимных каналов связи. При этом в судебных решениях не проводится разграничение между пониманием противоправности выполняемой деятельности в целом и осознанием конкретного способа мошенничества, что придаёт выводам о наличии прямого умысла оценочный

характер и затрудняет формирование единообразной правоприменительной практики.

Доказывание по делам о дистанционных мошенничествах выстраивается вокруг анализа переписки в мессенджере Telegram. Во всех рассмотренных приговорах именно переписка с пользователями, использующими никнеймы «Технический отдел», «Валентин», «Харитон», «Kirill», положена в основу выводов о согласованности действий подсудимых и наличии предварительного сговора. Такая модель доказывания прослеживается в делах Сидорова С.И., Зареева Д.Р. и Кузнецова Н.С., где переписка рассматривалась в качестве основного источника сведений о роли подсудимого в преступной схеме.

В материалах дел отсутствуют сведения о проведении компьютерно-технических экспертиз, анализе IP-адресов, используемых устройств и иных цифровых следов, что не позволяет установить организаторов преступных схем. В результате в приговорах переписка приобретает универсальный характер, одновременно служа доказательством умысла, сговора и распределения ролей, без дополнительной проверки её происхождения и достоверности.

В ситуациях, когда позиция подсудимого в судебном заседании отличается от показаний, данных на стадии предварительного расследования, суды нередко прибегают к оглашению последних. Так, по делу Сидорова С.И. противоречия были разрешены посредством приоритета следственных показаний, при том что их оценка в совокупности с иными доказательствами носила формальный характер. Аналогичный подход прослеживается и в деле Кузнецова Н.С., где признательные показания, данные ранее, имели определяющее значение для вывода о наличии умысла.

Показания потерпевших по делам о телефонном мошенничестве, как правило, воспринимаются судами как достоверные и последовательные, что обусловлено возрастом потерпевших и очевидностью причинённого ущерба. Вместе с тем доказательственная база редко дополняется объективными данными: не проводится фонетическая идентификация голосов, не

анализируется биллинг телефонных соединений, не сопоставляются маршруты передвижения курьеров с временными интервалами телефонных звонков.

При таком подходе предмет доказывания фактически сужается до поведения конкретного исполнителя, тогда как анализ всей преступной структуры и выявление иных участников подменяются формальной констатацией включённости подсудимого в переписку, что ограничивает возможности всестороннего и полного исследования обстоятельств дела.

Открытым остается вопрос индивидуализации наказания. Сопоставление приговоров в отношении Сидорова С.И. и Зареева Д.Р. показывает, что при сходных функциях курьеров и сопоставимом характере участия в преступлении суды приходят к различным выводам о мере уголовной ответственности, не всегда последовательно соотнося её с фактическим вкладом подсудимых в реализацию преступной схемы. Так, Сидорову С.И. было назначено 5 лет лишения свободы (условно), а Зарееву Д.Р. 1 год 11 месяцев лишения свободы (условно).

В большинстве рассмотренных приговоров суды подробно фиксируют наличие смягчающих обстоятельств, включая признание вины, сотрудничество со следствием, частичное возмещение ущерба и семейные обстоятельства. Однако их влияние на окончательный размер наказания остаётся ограниченным. Так, в деле Салихова Р.М. , выполнявшего функции дропа, суд учёл активное способствование расследованию и уход за престарелой матерью, но отказался от применения более мягких механизмов, ограничившись снижением наказания в пределах санкции.

Сложившаяся практика назначения наказаний по делам о дистанционных мошенничествах создаёт риск чрезмерной репрессивности в отношении исполнителей низового уровня. При отсутствии установленных организаторов основная тяжесть уголовной ответственности возлагается на курьеров и дропов, что ставит вопрос о соразмерности назначаемых наказаний их фактической роли и о соответствии применяемого подхода задачам предупреждения преступлений данной категории.

Рассмотрение сложностей квалификации совершаемых с использованием информационных технологий, позволило автору разработать модель квалификации таких преступлений в виде алгоритма мыслительной деятельности.

Шаг 1. Зафиксировать имущественный ущерб и потерпевшего.

Сначала следует установить, какое именно имущественное благо выбыло: списание средств со счёта, перевод электронных денег, оформление кредита/микрозайма, перевод на счета третьих лиц и т. п. Далее важно определить, кто является потерпевшим в юридически значимом смысле: владелец счёта (карты), банк или МФО (например, при мошенническом оформлении кредита), иной субъект. От этого зависит выбор нормы и то, кому именно был адресован обман (если он имел место).

Шаг 2. Определить механизм получения доступа к деньгам.

Далее нужно ответить на основной вопрос: за счёт чего у виновного возникла возможность распорядиться денежными средствами? В практике цифровых хищений этот вопрос обычно разграничивает кражу и мошенничество, а также позволяет отличить обман от вмешательства в обработку данных.

2.1. Обмана не было, доверие не использовалось.

Если списание или оплата совершены тайно, без формирования заблуждения у какого-либо лица и без легендирования (типичный пример – бесконтактная оплата найденной картой), то квалификация, как правило, смещается в сторону кражи (п. «г» ч. 3 ст. 158 УК РФ). Такой подход подтверждён позицией Верховного Суда РФ (Обзор № 3 (2021), п. 49).

2.2. Имел место обман или злоупотребление доверием.

Если доступ к средствам обеспечен тем, что потерпевший (либо иное лицо, от действий которого зависит распоряжение средствами) действовал под влиянием ложных сведений или умолчания – например, сообщил коды из SMS, «подтвердил отмену списания», поверил звонку «службы безопасности банка» и т. п., – имеются основания квалификации как мошенничества. В зависимости

от обстоятельств речь идёт о ст. 159 УК РФ либо о ст. 159^3 УК РФ, когда обман реализован с использованием электронного средства платежа.

2.3. Доступ получен через вмешательство в обработку компьютерной информации

Если хищение достигнуто путём ввода, удаления, блокирования, модификации компьютерной информации либо иного воздействия, которое нарушает работу средств хранения, обработки или передачи данных, деяние квалифицируется по ст. 159^6 УК РФ (при действующей конструкции). Пленум ВС РФ № 48 (п. 20) разъясняет, что «вмешательство» – это целенаправленное программное либо программно-аппаратное воздействие, которое нарушает процесс обработки, хранения или передачи информации.

2.4. Комбинированная схема (наиболее типичная для практики)

Нередко обман используется как «вход» в схему: у потерпевшего выманивают логин, пароль, одноразовый код, доступ к аккаунту, после чего перевод выполняется уже через штатный функционал интернет-банка или приложения. В таких случаях важно не упрощать картину: обман и последующие действия образуют единую причинную цепочку, но при этом отдельные эпизоды могут иметь относительную самостоятельность. Поэтому вопрос решается по фактам: возможна квалификация по одной норме, а при наличии самостоятельных действий (например, незаконный доступ, вредоносное ПО) – по совокупности.

Шаг 3. Выбрать «профильную» норму по итогам шага 2.

В прикладном плане удобно исходить из следующей логики выбора:

– ст. 158 УК РФ (п. «г» ч. 3) – когда списание/оплата осуществлены тайно, без обмана и без доказанного вмешательства в обработку данных (например, использование найденной карты для оплаты).

– ст. 159 УК РФ – когда обман установлен, но специальный признак использования электронного средства платежа либо компьютерного вмешательства отсутствует или не доказан.

– ст. 159^3 УК РФ – когда обман/доверие реализованы с использованием электронного средства платежа (карта, мобильное приложение, интернет-банк) в рамках функционала системы и без доказанного вмешательства в обработку данных.

– ст. 159^6 УК РФ – когда доказано вмешательство в обработку компьютерной информации в смысле ст. 159^6 и разъяснений Пленума ВС РФ.

Шаг 4. Проверить необходимость дополнительной квалификации по главе 28 УК РФ

После выбора основной нормы следует отдельно оценить, есть ли самостоятельные действия против информационной безопасности: несанкционированный доступ, создание/использование вредоносного ПО, воздействие на инфраструктуру, обход механизмов защиты и т. п. При наличии таких признаков деяние квалифицируется дополнительно по ст. 272, 273, 274^1 УК РФ по правилам совокупности (если соответствующие составы не «поглощаются» и реально присутствуют).

Шаг 5. Квалифицировать действия соучастников: организаторов, «дропов», курьеров.

Для оценки ролей соучастников следует исходить из двух вопросов: что охватывалось умыслом лица и какую функцию оно выполняло в механизме хищения. По делам о цифровых мошенничествах нередко привлекаются «исполнители инфраструктуры» – курьеры, «дропы», каналы обналичивания. Их ответственность зависит от того, доказана ли осведомлённость об обманном происхождении средств и включённость в общий план действий.

Исходя из вывода об избыточности ст. 159^6 УК РФ, в диссертации предлагается сосредоточить цифровые формы мошенничества в одной специальной норме – обновлённой ст. 159^3 УК РФ, а технические посягательства на информационную безопасность оставить в самостоятельном блоке главы 28 УК РФ и оценивать их по правилам совокупности.

При таком подходе схема квалификации становится проще и логичнее.

Шаг 1. Имеется ли обман или злоупотребление доверием?

1. Нет – квалификация по ст. 158 УК РФ (кража с банковского счёта при тайной оплате или списании).

2. Да – квалификация по ст. 159 УК РФ, если цифровая среда не образует специального признака, либо по обновлённой ст. 159^3 УК РФ, когда хищение совершено с использованием электронных средств платежа и (или) компьютерной среды.

Шаг 2. Было ли самостоятельное незаконное воздействие на компьютерную информацию или инфраструктуру? (ст. 272–274^1 УК РФ)

Да – дополнительно применяется глава 28 УК РФ по правилам совокупности.

Смысл этой модели в том, что цифровые инструменты рассматриваются прежде всего как способ реализации умысла, а не как особая «природа» посягательства. Тогда квалификация строится от фактического механизма изъятия и роли обмана, а технические атаки на системы и данные получают отдельную оценку там, где они действительно присутствуют и доказаны.

Таким образом, изучение судебных решений по делам о дистанционных мошенничествах показывает, что при формально сходной квалификации фактическое содержание уголовной ответственности существенно различается. Курьеры и дропы, выполняющие вспомогательные и нередко зависимые функции, зачастую приравниваются судами к лицам, непосредственно осуществляющим обман потерпевших. Отсутствие чётких критериев оценки роли подсудимого приводит к размыванию границ между формами соучастия, особенно при квалификации действий дропов. Существенные проблемы выявляются и в доказывании, где переписка в мессенджерах фактически подменяет комплексное исследование преступной схемы. Назначение наказаний при этом характеризуется повышенной репрессивностью в отношении исполнителей низового уровня, тогда как организаторы преступлений во многих делах остаются неустановленными.

ЗАКЛЮЧЕНИЕ

Итак, в работе был осуществлен комплексный уголовно-правовой анализ мошенничеств, совершаемых с использованием информационных технологий, и выявлены проблемы их квалификации в современной правоприменительной практике.

В первой главе установлено, что цифровизация экономических и социальных процессов объективно изменила способы совершения мошенничеств, не затронув при этом их правовую природу как преступлений против собственности. Использование электронных средств платежа, дистанционных сервисов и автоматизированных систем выступает формой реализации преступного умысла, а не самостоятельным видом посягательства. Анализ зарубежного законодательства показал, что в большинстве правопорядков цифровые формы мошенничества не выделяются в обособленные составы, а охватываются общими нормами с учётом способа совершения преступления.

Во второй главе раскрыты объективные и субъективные признаки мошенничеств, совершаемых с использованием информационных технологий. Установлено, что решающее значение для квалификации имеет механизм изъятия имущества и характер причинной связи между обманом и имущественным результатом.

Мошенничество, совершаемое с применением информационных технологий, сохраняет имущественную природу, но реализуется через иные механизмы причинения вреда. Объективная сторона таких посягательств характеризуется активными действиями, направленными либо на формирование у потерпевшего искажённого представления, либо на вмешательство в функционирование платёжных и информационных систем. Обязательным элементом остаётся наступление реального имущественного вреда и установление причинной связи между действиями виновного и его

последствиями. Использование цифровых средств не трансформирует сущность мошенничества, но усложняет структуру охраняемых отношений и требует более точного разграничения общего и специальных составов

Субъективная сторона таких преступлений характеризуется прямым умыслом и корыстной целью, при этом применение цифровых инструментов не влияет на содержание вины, а лишь определяет форму её реализации. Анализ квалифицированных и особо квалифицированных составов позволил выявить тенденцию к усложнению конструкции мошенничества за счёт включения в неё технических характеристик, не всегда имеющих самостоятельное уголовно-правовое значение.

Третья глава была посвящена проблемам разграничения мошенничеств, совершаемых с использованием информационных технологий, со смежными составами преступлений. На основе изучения судебной практики показано, что наибольшие затруднения возникают при квалификации хищений безналичных денежных средств и при соотношении статей 159, 159^{3}, 159^{6} УК РФ, а также норм главы 28 УК РФ. Сделан вывод о том, что существование статьи 159^{6} УК РФ не устраняет, а, напротив, усиливает конкуренцию норм и порождает неоднородность правоприменения. Анализ конкретных дел подтвердил, что сходные по механизму деяния получают различную правовую оценку в зависимости от формального описания способа, что противоречит требованиям правовой определённости.

Наиболее существенным результатом исследования является обоснование системной избыточности статьи 159^{6} УК РФ. Показано, что деяния, охватываемые данной нормой, не образуют самостоятельного вида мошенничества, а неправомерное воздействие на компьютерную информацию уже получает адекватную уголовно-правовую оценку в рамках статей 272, 273 и 274^{1} УК РФ. В связи с этим в работе сформулировано предложение об исключении статьи 159^{6} УК РФ и о концентрации цифровых форм мошенничества в рамках обновлённой редакции статьи 159^{3} УК РФ,

охватывающей как использование электронных средств платежа, так и иных компьютерных технологий, применяемых для обманного изъятия имущества.

Практическая ценность полученных выводов заключается в возможности их использования при квалификации преступлений следственными и судебными органами, а также при подготовке методических рекомендаций и разъяснений. Материалы исследования могут быть использованы в учебном процессе и при дальнейшей научной разработке проблем уголовно-правовой оценки цифровых посягательств.

Перспективы дальнейших исследований связаны с анализом влияния новых финансовых и технологических инструментов, включая распределённые реестры и автоматизированные платёжные системы, на конструкцию мошенничества и с выработкой устойчивых критериев уголовно-правовой оценки цифровых форм хищений в условиях продолжающейся трансформации экономических отношений.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

I. Нормативные правовые акты

1. Конвенция Организации Объединенных Наций против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям (Принята резолюцией 79/243 Генеральной Ассамблеей от 24 декабря 2024 года) // СПС «Консультант плюс». – URL: https://www.un.org/ru/documents/treaty/A-RES-79-243 (Дата обращения 01.10.2025).
2. Конституция Российской Федерации от 12 декабря 1993 г. (с изм. от 14.03.2020) // Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 04.07.2020.
3. Гражданский кодекс Российской Федерации, часть первая: Федеральный закон от 30 ноября 1994 г. № 51-ФЗ (ред. от 31.07.2025) // Собр. законодательства Рос. Федерации. – 1994. – № 32. – Ст. 3301.
4. Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 № 63-ФЗ (ред. от 20.02.2026) // Собр. законодательства Рос. Федерации. – 1996. – № 25. – Ст. 2954.
5. О национальной платежной системе: Федеральный закон от 27 июня 2011 г. № 161-ФЗ (ред. от 25.05.2025) // Собр. законодательства Рос. Федерации. – 2011. – № 27. – Ст. 3872.
6. О внесении изменений в Уголовный кодекс Российской Федерации: Федеральный закон от 23.04.2018 № 111-ФЗ // Собр. законодательства Рос. Федерации. – 2018. – № 18. – Ст. 2581.
7. О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный

закон № 259-ФЗ от 31 июля 2020 г. (ред. от 27.10.2025) // Собр. законодательства Рос. Федерации. – 2020. – № 31 (часть 1). – Ст. 5018.

8. Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 05.12.2016 № 646 // Собр. законодательства Рос. Федерации. – 2016. – № 50. – Ст. 7074.
9. О Стратегии национальной безопасности Российской Федерации: Указ Президента РФ от 02.07.2021 № 400 // Собр. законодательства Рос. Федерации. – 2021. – № 27 (часть II). – Ст. 5351.
10. United States. Computer Fraud and Abuse Act (CFAA). 18 U.S.C. § 1030. Закон США от 16 октября 1986 г. № 99-474. – URL: https://www.law.cornell.edu/uscode/text/18/1030 (дата обращения: 16.11.2025).
11. Germany. Strafgesetzbuch (StGB). Уголовный кодекс ФРГ. § 263a «Computerbetrug». – URL: https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html (дата обращения: 16.11.2025).
12. United Kingdom. Fraud Act 2006. Act of Parliament (c 35). Принят 8 ноября 2006 г., вступил в силу 15 января 2007 г. – URL: https://www.legislation.gov.uk/ukpga/2006/35/contents (дата обращения: 16.11.2025).
13. United Kingdom. Computer Misuse Act 1990 (CMA). Act of Parliament (c 18). Закон Великобритании об ответственности за несанкционированный доступ к компьютерам. – URL: https://www.legislation.gov.uk/ukpga/1990/18/contents (дата обращения: 16.11.2025).

II. Монографии, учебники, учебные пособия

14. Виноградова Е.В. Актуальные мысли о праве / Е.В. Виноградова, С.И. Захарцев. – М.: Юрлит, 2023. –232 с.
15. Лопашенко Н.А. Преступления против собственности. Книга II. Общая теория хищений. Виды хищения: Авторский курс в 4 книгах / Н.А. Лопашенко. – Москва: Издательство «Юрлитинформ», 2019. – 192 с.

16. Наумов А.В. Российское уголовное право. Общая часть: курс лекций. – 7-е изд. – М.: Проспект, 2024. – 816 с.
17. Никифоров Б.С. Избранное / Составитель канд. юрид. наук А.А. Гравина. – М: Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации, 2010. – 224 с.
18. Перетолчин А.П. Уголовная ответственность за мошенничество с использованием электронных средств платежа: дисс. ... канд. юрид. наук: 12.00.08 / Перетолчин Артем Павлович; [Место защиты: ФГАОУ ВО «Дальневосточный федеральный университет»]. – Иркутск, 2021. – 239 с.
19. Соловьева Е.А. Преступления, совершаемые в платежных системах монография / Е.А. Соловьева; под ред. докт. юрид. наук, проф. Н.А. Лопашенко. – Москва: Юрлитинформ, 2021. – 172, [2] с.
20. Уголовно-юрисдикционная деятельность в условиях цифровизации: монография / Н.А. Голованова, А.А. Гравина, О.А. Зайцев и др. – М.: Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации; ООО «Юридическая фирма Контракт», 2019 – 212 с.
21. Упоров И.В. Признаки субъективной стороны мошенничества и их значение при отграничении данного вида хищения от иных преступлений / И.В. Упоров, А.В. Бондарь // Актуальные вопросы экономики и управления: сборник материалов III Международной научно-практической конференции, Новосибирск, 16 января – 13 2018 года. – Новосибирск: Общество с ограниченной ответственностью «Центр развития научного сотрудничества», 2018. – С. 175-180.
22. Ушаков Р.М. Квалификация хищений, совершаемых с использованием информационных технологий: монография / Р.М. Ушаков. – Москва: Юстицинформ, 2023. – 160 с.

III. Статьи, научные публикации

23. Аванесян Д.Н. Влияние цифровизации на российскую экономику и общество / Д.Н. Аванесян // Виртуозы науки: Сборник тезисов Международной научно-практической конференции студентов и молодых учёных за 2023 г, Краснодар, 06–15 ноября 2023 года. – Краснодар: Кубанский государственный аграрный университет им. И.Т. Трубилина, 2024. – С. 593-594.
24. Балашова Н.А. Особенности квалификации мошенничества с использованием служебного положения / Н.А. Балашова // Вестник Уральского института экономики, управления и права.- 2018.- №1.- С.20 – 27.
25. Барчуков В.К. Непосредственный объект мошенничества в сфере компьютерной информации / В.К. Барчуков // Пробелы в российском законодательстве. Юридический журнал. – 2018. – № 7. – С. 154-157.
26. Баубекова Ж. Мошенничество: социальное влияние и роль цифровых технологий в его распространении / Ж. Баубекова, Е.С. Носова, Н.А. Кабанова // Вестник евразийской науки. – 2024. – Т. 16, № S1.
27. Гончаров Д.Ю., Гончарова С.Г. Квалификация мошенничества, совершенного с использованием служебного положения / Д.Ю. Гончаров, С.Г. Гончарова // Вестник ВГУ. Сер.: Право. – 2016. – № 3. – С. 281 – 291.
28. Граматкина С.А. Объект преступления и проблемные вопросы его определения / С.А. Граматкина // Вестник Юридического института МИИТ. – 2020. – № 1(29). – С. 66-73.
29. Громыко А.А. Цифровая трансформация общества, цели и стратегии / А.А. Громыко, В.Р. Солтанов // Современные тенденции развития науки и мирового сообщества в эпоху цифровизации: сборник материалов XIX Международной научно-практической конференции, Москва, 30 ноября 2023 года. – Москва: Алеф, 2023. – С. 350-352.

30. Гуц Е. Отграничение общего состава мошенничества от специальных в российском уголовном праве / Е. Гуц // Государство, право и правоприменительная практика: современные вызовы: Сборник научных трудов IX Всероссийской научно-практической конференции студентов и аспирантов Юридического института Балтийского федерального университета им. Иммануила Канта, Калининград, 23 января 2021 года / Под общей редакцией О.А. Заячковского. – Калининград: Балтийский федеральный университет имени Иммануила Канта, 2022. – С. 167-172.
31. Деменков В.А. Мошенничество в сфере компьютерной информации: к вопросу квалификации и применения ст. 159^6 УК РФ / В.А. Деменков, В.П. Алехин // Тенденции развития науки и образования. – 2023. – № 104-8. – С. 130-132.
32. Залескина А.Н. Особенности установления субъективной стороны мошенничества / А.Н. Залескина // Научный дайджест Восточно-Сибирского института МВД России. – 2020. – № 6(9). – С. 91-95.
33. Захарцев С.И. Оперативно-розыскная деятельность и информационная безопасность как часть военной безопасности России / С.И. Захарцев, В.П. Сальников, А.С. Алексанин // Известия Российской академии ракетных и артиллерийских наук. – 2018. – № 2(102). – С. 102–106.
34. Ибатуллина Д.М. Объективные признаки цифрового мошенничества и их значение для квалификации деяния / Д.М. Ибатуллина // Вестник Казанского юридического института МВД России. – 2025. – Т. 16, № 1(59). – С. 66-73.
35. Иванова А.А. Проблемы определения понятия «объект преступления» в современном уголовном праве / А.А. Иванова. // Молодой ученый. – 2024. – № 27 (526). – С. 149-151.
36. Ильина М.Д. К вопросу об объекте преступления / М.Д. Ильина // Актуальные вопросы юридической науки глазами молодых исследователей: Сборник статей по итогам Четвертой Всероссийской научной конференции курсантов, студентов, адъюнктов, аспирантов и соискателей, Рязань, 02 февраля 2024 года. – Москва – Нижний Новгород: Постер-М, Российская

академия народного хозяйства и государственной службы при Президенте РФ, 2024. – С. 221-224.

37. Карабанова Е.Н. Понятие объекта преступления в современном уголовном праве / Е.Н. Карабанова // Журнал российского права. – 2018. – № 6(258). – С. 69-77.

38. Квасникова Т.В. Понимание объекта преступления в доктрине уголовного права / Т.В. Квасникова, С.А. Костюк, О.И. Лубягин // Закон и власть. – 2025. – № 1. – С. 89-91.

39. Колин К.К. Цифровая революция и искусственный интеллект: новые горизонты и опасности // Партнерство цивилизаций. – 2020. – № 1-2. – С. 100–106.

40. Корниенкова М. Р. Особенности и проблемы квалификации мошенничества / М.Р. Корниенкова, Л.А. Русскевич // Вестник экономической безопасности. – 2024. – № 1. – С. 115-119.

41. Косенков А.Ю. Цифровизация в ракурсе философских исследований: новые угрозы и способы их преодоления / А.Ю. Косенков // Наука и инновации. – 2020. – № 11. – С. 36–40

42. Крючков М.А. Уголовно-правовая характеристика мошенничества, совершаемого с использованием информационно-коммуникационных технологий / М.А. Крючков // Научный аспект. – 2023. – Т. 1, № 5. – С. 7-14.

43. Лобач Д.В. Развитие российского уголовного законодательства в сфере противодействия преступлениям, совершаемым в сети Интернет / Д.В. Лобач // Уголовное право: стратегия развития в XXI веке. – 2023. – № 3. – С. 21–27.

44. Маршева К.С. Объективные признаки мошенничества с использованием электронных средств платежа / К.С. Маршева // Молодой ученый. – 2021. – № 50 (392). – С. 262-265.

45. Матюхина Т.И., Ивлев К.А. Электронное средство платежа как средство совершения преступления, предусмотренного ст. 159^3 Уголовного кодекса РФ [Электронный ресурс] // Universum: экономика и юриспруденция:

электрон. научн. журн. – 2024. – № 1(123). – Режим доступа: https://7universum.com/ru/economy/archive/item/18992 (дата обращения: 10.12.2025).

46. Намысов Е.Д. Мошенничество в цифровую эпоху в связи с общественными изменениями / Е.Д. Намысов // Криминологический журнал. – 2023. – № 3. – С. 148-154.
47. Новикова А. И. К вопросу о субъективных признаках мошенничества / А.И. Новикова. // Молодой ученый. – 2021. – № 53 (395). – С. 103-107.
48. Осипова И.Н. Искусственный интеллект − угроза или помощник человека? // Экономика. Общество. Человек: материалы Всероссийской научно-практической конференции с международным участием / ред. Е.Н. Чижова. Т. 1. Вып. XXXVII. – Белгород: Белгородский государственный технологический университет им. В. Г. Шухова, 2019. –С. 179–182.
49. Петрякова Л.А. Мошенничество с использованием электронных средств платежа / Л.А. Петрякова // Вектор науки Тольяттинского государственного университета. Серия: Юридические науки. – 2020. – № 1(40). – С. 33-37.
50. Рарог А.И. Вина, ответственность и наказание / А.И. Рарог // Избранное: сборник статей. – Москва: Проспект, 2022. – С. 160-174.
51. Ровина Е. Е. Компьютерные преступления вчера и сегодня / Е.Е. Ровина, З.З. Гурьянова // Научный дайджест Восточно-Сибирского института МВД России. – 2022. – № 3(17). – С. 81–85.
52. Розенко С.В. Особенности квалификации мошенничества по уголовному законодательству Российской Федерации / С.В. Розенко, К.А. Мурзина // Вестник Югорского государственного университета. – 2017. – № 1-2(44). – С. 113-116.
53. Сафонова Д. В. Особенности объекта и предмета преступления, предусматривающего ответственность за мошенничество с использованием электронных средств платежа (ст. 159^3 УК РФ) / Д.В. Сафонова // Правопорядок: история, теория, практика. – 2025. – №4 (47). – С. 83-88.

54. Семенова И.В. Социальная природа преступления в сфере цифровой информации / И.В. Семенова // Вестник Санкт-Петербургского военного института войск национальной гвардии. – 2024. – № 2(27). – С. 63-71.
55. Серебренникова А.В. Цифровая криминалистика и ее значение для расследования преступлений / А.В. Серебренникова // International Law Journal. – 2019. – Т. 2. – № 4. – С. 126–133.
56. Струков А.Е. Понятие и способы мошенничества / А.Е. Струков // Вестник магистратуры. – 2022. – № 1-2(124). – С. 10-12.
57. Суворова В.В. Совершение преступлений с использованием социальной инженерии: постановка проблемы / В.В. Суворова, Л.А. Суворова // Теория и практика приоритетных научных исследований: сборник научных трудов по материалам VIII Международной научнопрактической конференции, Смоленск, 13 августа 2019 года. – Смоленск: МНИЦ «Наукосфера», 2019. – С. 71–74.
58. Тютюнник М.С. Противодействия телефонным мошенничествам / М.С. Тютюнник, А.К. Печалов // Инновационные идеи молодежи в развитии современной науки и образования: Материалы Международной студенческой научно-практической конференции, Ставрополь, 20 февраля 2025 года. – Краснодар: Российское энергетическое агентство, 2025. – С. 79-83.
59. Филатова М.А. Хищение с использованием чужой банковской карты в магазине образует состав кражи / М.А. Филатова // Законность. – 2020. – № 12. – С. 34–38.
60. Фот Ю.Д. Фишинг и как с ним бороться / Ю.Д. Фот, Н.И. Туманов // Электронное информационное пространство для науки, образования, культуры: Материалы XI Международной научно-практической конференции. В 3-х частях, Орёл, 19 декабря 2024 года. – Орёл: Орловский государственный институт культуры, 2024. – С. 134-138.

61. Харина Е.А. К вопросу о проблемных аспектах квалификации и криминализации мошенничества в сфере компьютерной информации / Е.А. Харина // Российский следователь. – 2023. – № 3. – С. 29-33.
62. Шабашов А.Д. Юридическая характеристика признаки предмета хищения при совершении мошенничества / А.Д. Шабашов // Научный форум: сборник статей XIII Международной научно-практической конференции, Пенза, 23 мая 2025 года. – Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2025. – С. 170-172.
63. Шалагин А.Е. Трансформация преступности в XXI веке: особенности предупреждения и противодействия / А.Е. Шалагин, А.Д. Идиятуллов // Вестник Казанского юридического института МВД России. – 2021. – Т. 12, № 2(44). – С. 227-235.
64. Шаяхметова Ж.Б. Роль и значение объекта преступления в составе преступления / Ж.Б. Шаяхметова // Современные проблемы уголовной политики: Международная коллективная монография. – Екатеринбург: Федеральное государственное бюджетное образовательное учреждение высшего образования «Уральский государственный юридический университет», 2019. – С. 179-188.
65. Яковец Ю.В. Функции интеллекта Человека разумного − первоисточники института партнерства цивилизаций // Партнерство цивилизаций. – 2020. – № 1-2. – С. 100–106.
66. Янгаева М.О. Социальная инженерия как способ совершения киберпреступлений // Вестник Сибирского юридического института МВД России. – 2021. – № 1 (42). – С. 133–138
67. Яни П.С. Корысть как признак хищения / П.С. Яни // Законность. – 2019. – № 2(1012). – С. 23-27.
68. Яни П.С. Хищение с использованием чужой банковской карты в магазине следует квалифицировать как мошенничество / П.С. Яни // Законность. – 2020. – № 12. – С. 39–43.

IV. Эмпирические материалы (материалы судебной, следственной и иной правоприменительной практики)

69. По делу о проверке конституционности частей шестой и седьмой статьи 115 Уголовно-процессуального кодекса Российской Федерации в связи с жалобой закрытого акционерного общества «Глория»: постановление Конституционного Суда РФ от 10 декабря 2014 г. № 31-П (абз. 2 п. 3) // КонсультантПлюс: справ.-правов. сист. – URL: www.consultant.ru (дата обращ.: 10.01.2026).
70. О судебной практике по делам о мошенничестве, присвоении и растрате: Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 (ред. от 15.12.2022) // Бюллетень Верховного Суда РФ. – 2018. – № 2.
71. Обзор судебной практики Верховного Суда Российской Федерации № 3 (2021), утв. Президиумом Верховного Суда РФ 10.11.2021) // КонсультантПлюс: справ.-правов. сист. – URL: www.consultant.ru (дата обращ.: 10.12.2025).
72. Кассационное определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 01.06.2021 № 5-УДП21-44-К2 // КонсультантПлюс: справ.-правов. сист. – URL: www.consultant.ru (дата обращ.: 10.12.2025).
73. Постановление Восьмого кассационного суда общей юрисдикции от 10.03.2022 № 77-1148/2022 [Электронный ресурс] // КонсультантПлюс: справ.-правов. сист. – URL: www.consultant.ru (дата обращ.: 10.12.2025).
74. Кассационное определение Седьмого кассационного суда общей юрисдикции от 13.11.2025 № 77-3303/2025 [Электронный ресурс] // КонсультантПлюс: справ.-правов. сист. – URL: www.consultant.ru (дата обращ.: 10.12.2025).

75. Кассационное определение Второго кассационного суда общей юрисдикции от 17.04.2025 № 77-963/2025 [Электронный ресурс] // КонсультантПлюс: справ.-правов. сист. – URL: www.consultant.ru (дата обращ.: 10.12.2025).
76. Определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 29.09.2020 № 12-УДП20-5-К6 [Электронный ресурс] // КонсультантПлюс: справ.-правов. сист. – URL: www.consultant.ru (дата обращ.: 10.12.2025).
77. Обзор судебной практики Кемеровского областного суда от 23 июня 2005 г. № 01-19/320 по делам о преступлениях, предусмотренных ст.ст.159, 160, 165, 242, 327 УК РФ // Справ.-правов. сист. «Гарант» [Электронный ресурс]. – Режим доступа: https://base.garant.ru/7541393/ (дата обращения: 10.12.2025).
78. Приговор Центрального районного суда г. Тюмени от 3 сентября 2018 г. № 1-18/2018, 1-528/2017 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: https://sudact.ru/regular/doc/ruiCsHOBEBUQ/ (дата обращения: 10.12.2025).
79. Приговор Автозаводского районного суда г. Тольятти Самарской области от 2018 г. № 1-749/2018 [Электронный ресурс] // ГАС «Правосудие». – Режим доступа: https://avtozavodsky--sam.sudrf.ru/modules.php?name=sud_delo&srv_num=1/ (дата обращения: 10.12.2025).
80. Приговор Ленинского районного суда г. Оренбурга (Оренбургская область) от 22 ноября 2018 г. № 1-601/2018 [Электронный ресурс] // Актофакт: архив судебных дел и решений. – Режим доступа: https://actofact.ru/case-56RS0018-1-601-2018-2018-09-28-2-0/ (дата обращения: 10.12.2025).
81. Приговор Якутского городского суда (Республика Саха (Якутия)) от 26 августа 2019 г. № 1-681/2019 по делу № 1-1462/2018 [Электронный ресурс] // Судебные и нормативные акты РФ. – URL: https://sudact.ru/regular/doc/8jIATe7oVfNK (дата обращения: 10.12.2025).

82. Приговор Торжокского городского суда (Тверская область) от 16 июля 2020 г. № 1-60/2020 [Электронный ресурс] // Судебные и нормативные акты РФ. – URL: https://sudact.ru/regular/doc/3aVp8BqhtdQ1 (дата обращения: 10.12.2025).
83. Приговор Октябрьского городского суда Республики Башкортостан от 29 июля 2020 г. № 1-243/2020 [Электронный ресурс] // ГАС «Правосудие». – Режим доступа: https://bsr.sudrf.ru/bigs/portal.htm (дата обращения: 10.12.2025).
84. Приговор Центрального районного суда г. Кемерово от 8 сентября 2020 г. № 1-573/2020 [Электронный ресурс] // ГАС «Правосудие». – Режим доступа: https://bsr.sudrf.ru/bigs/portal.htm (дата обращения: 10.12.2025).
85. Приговор Подольского городского суда (Московская область) от 27 декабря 2023 г. № 1-1139/2023 [Электронный ресурс] // Судебные и нормативные акты РФ. – URL: https://sudact.ru/regular/doc/I2zXxHzWLTbv (дата обращения: 10.12.2025).
86. Приговор Советского районного суда г. Брянска (Брянская область) от 10 января 2024 г. № 1-479/2023, 1-63/2024 [Электронный ресурс] // Судебные и нормативные акты РФ. – URL: https://sudact.ru/regular/doc/CqaUmhM7Lvq (дата обращения: 10.12.2025).
87. Приговор суда Ханты-Мансийского автономного округа – Югры от 17 января 2024 г. № 22-2816/2023, 22-8/2024 [Электронный ресурс] // Судебные и нормативные акты РФ. – URL: https://sudact.ru/regular/doc/8PZTV2464SmQ (дата обращения: 10.12.2025).
88. Приговор Кировского районного суда г. Самары от 8 апреля 2024 г. № 1-226/2024 [Электронный ресурс] // ГАС «Правосудие». – Режим доступа: https://kirovsky--sam.sudrf.ru/ (дата обращения: 10.12.2025).
89. Приговор Чистопольского городского суда Республики Татарстан от 9 апреля 2024 г. № 1-136/2024 (УИД: 16RS0040-01-2024-000756-95) [Электронный ресурс]. – URL: https://chistopolsky.tat.sudrf.ru/ (дата обращения: 01.12.2025).

90. Приговор Вахитовского районного суда г. Казани от 18 июля 2023 г. № 1-198/2023 [Электронный ресурс] // ГАС «Правосудие». – Режим доступа: https://vahitovsky--tat.sudrf.ru/ (дата обращения: 10.12.2025).
91. Приговор Приволжского районного суда г. Казани Республики Татарстан от 14 апреля 2023 г. № 1-272/2023 [Электронный ресурс] // ГАС «Правосудие». – URL: https://privolzhsky--tat.sudrf.ru (дата обращения: 05.03.2026).
92. Приговор Авиастроительного районного суда г. Казани Республики Татарстан от 5 сентября 2019 г. № 1-213/2019 [Электронный ресурс] // Судебные и нормативные акты РФ. – URL: https://sudact.ru/regular/doc/SK3KlfXTdf6R (дата обращения: 05.03.2026).
93. Приговор Кировского районного суда г. Казани Республики Татарстан от 26 мая 2020 г. № 1-225/2020 [Электронный ресурс] // Судебные и нормативные акты РФ. – URL: https://sudact.ru/regular/doc/jBH1YaRetCoj (дата обращения: 05.03.2026).
94. Приговор Зеленодольского городского суда Республики Татарстан от 31 мая 2024 г. № 1-42/2024 (УИД: 16RS0040-01-2023-003885-04) [Электронный ресурс]. – URL: https://zelenodolsky--tat.sudrf.ru (дата обращения: 01.12.2025).
95. Приговор Зеленодольского городского суда Республики Татарстан от 11 июня 2024 г. № 1-140/2024 (УИД: 16RS0040-01-2024-000256-43) [Электронный ресурс]. – URL: https://zelenodolsky--tat.sudrf.ru (дата обращения: 01.12.2025).
96. Приговор Вятскополянского районного суда Кировской области от 14 января 2025 г. № 1-5/2025 (УИД: 16RS0040-01-2024-007180-29) [Электронный ресурс]. – URL: https://vyatskopolyansky--kir.sudrf.ru/ (дата обращения: 01.12.2025).

ПРИЛОЖЕНИЯ

Приложение 1. Новая редакция ст. 159^3 УК РФ

Статья 159^3 Мошенничество с использованием электронных средств платежа или в сфере компьютерной информации

1. Мошенничество, то есть хищение чужого имущества либо приобретение права на чужое имущество путём обмана или злоупотребления доверием, совершённое с использованием электронных средств платежа или в сфере компьютерной информации, –

наказывается штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на срок до трех лет.

2. То же деяние, совершенное группой лиц по предварительному сговору, а равно с причинением значительного ущерба гражданину, -

наказывается штрафом в размере до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до двух лет, либо обязательными работами на срок до четырехсот восьмидесяти часов, либо исправительными работами на срок до двух лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до одного года или без такового, либо лишением свободы на срок до пяти лет с ограничением свободы на срок до одного года или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные лицом с использованием своего служебного положения, а равно в крупном размере, -

наказываются штрафом в размере от ста тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от

одного года до трех лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до двух лет или без такового, либо лишением свободы на срок до шести лет со штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев либо без такового и с ограничением свободы на срок до полутора лет либо без такового.

4. Мошенничество в сфере компьютерной информации, совершенное с банковского счета, а равно в отношении электронных денежных средств,

наказываются штрафом в размере от ста тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до двух лет или без такового, либо лишением свободы на срок до шести лет со штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев либо без такового и с ограничением свободы на срок до полутора лет либо без такового.

5. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, совершенные организованной группой либо в особо крупном размере, -

наказываются лишением свободы на срок до десяти лет со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового и с ограничением свободы на срок до двух лет либо без такового.

Примечание. Под мошенничеством в сфере компьютерной информации понимается хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Приложение 2. Модель квалификации преступлений, совершаемых с использованием информационных технологий

Шаг 1 Зафиксировать имущественный ущерб и потерпевшего

Что выбыло?

· Списание средств со счёта
· Перевод электронных денег
· Оформление кредита / микрозайма
· Перевод на счета третьих лиц
· Иное имущественное выбытие

Кто является потерпевшим?

· Владелец счёта / карты
· Банк или МФО (при мошеннически оформленном кредите)
· Иной субъект

От ответа зависит выбор нормы и адресат обмана.

Шаг 2 Определить механизм получения доступа к денежным средствам

2.1 – Без обмана

Списание совершено тайно, без формирования заблуждения и без легендирования.

Пример: бесконтактная оплата найденной картой.

– Кража (п. «г» ч. 3 ст. 158 УК РФ)

2.2 – Обман / злоупотребление доверием

Потерпевший действовал под влиянием ложных сведений: сообщил код, поверил звонку «службы безопасности».

– Мошенничество: ст. 159 или ст. 159^3 УК РФ (при использовании ЭСП)

2.3 – Вмешательство в обработку данных

Ввод, удаление, блокирование, модификация компьютерной информации; воздействие на средства хранения и передачи данных.

– ст. 159^6 УК РФ

2.4 – Комбинированная схема

Обман – «вход» в схему: у потерпевшего выманивают логин, пароль, OTP-код, затем перевод через штатный функционал.

– Единая причинная цепочка; при самостоятельных действиях – квалификация по совокупности норм

Шаг 3 Выбрать «профильную» норму УК РФ

СТАТЬЯ	УСЛОВИЕ ПРИМЕНЕНИЯ
ст. 158 п. «г» ч. 3	Списание / оплата осуществлены тайно, без обмана и без доказанного вмешательства в обработку данных. Типичный пример: использование найденной карты для бесконтактной оплаты.
ст. 159	Обман установлен, однако специальный признак (использование ЭСП или компьютерное вмешательство) отсутствует или не доказан.
ст. 159.3	Обман / злоупотребление доверием реализованы с использованием электронного средства платежа (карта, мобильное приложение, интернет-банк) в рамках штатного функционала системы, без вмешательства в обработку данных.
ст. 159.6	Доказано вмешательство в обработку компьютерной информации в смысле ст. 159^{6} и разъяснений Пленума ВС РФ № 48, п. 20 (целенаправленное программное воздействие, нарушающее процесс обработки, хранения или передачи информации).

Шаг 4 Проверить необходимость дополнительной квалификации по гл. 28 УК РФ

После выбора основной нормы следует оценить, есть ли самостоятельные действия против информационной безопасности:

Несанкционированный доступ к компьютерной информации	**ст. 272 УК РФ**
Создание, использование и распространение вредоносного ПО	**ст. 273 УК РФ**
Неправомерное воздействие на критическую информационную инфраструктуру	**ст. 274^{1} УК РФ**

Шаг 5 Квалифицировать действия соучастников

Два вопроса для оценки ролей соучастников:

Вопрос 1: Что охватывалось умыслом?
Установить осведомлённость лица об обманном происхождении средств и о характере совершаемого деяния.

Вопрос 2: Какую функцию выполняло лицо?
Определить роль в механизме хищения: организатор, пособник, «дроп», курьер, оператор обнала.

Типичные роли в цифровом мошенничестве:

Организатор	«Дроп»	Курьер	Обнальщик
Руководит схемой, распределяет роли и функции	Предоставляет счёт для зачисления похищенных денежных средств	Физически получает или перевозит средства	Канал вывода и конвертации средств

Приложение 3. Модель квалификации преступлений, совершаемых с использованием информационных технологий, в случае обновлённой ст. 159.3 УК РФ

Тайное хищение
Без обмана
→ ст. 158 УК РФ

Обман / доверие
Без специального признака
→ ст. 159 УК РФ

Обман + ЭСП / среда
Специальный признак доказан
→ ст. 159³ УК РФ

+ Совокупность по гл. 28 УК РФ *(при наличии самостоятельного незаконного воздействия)*
ст. 272 · ст. 273 · ст. 274 · ст. 274¹ УК РФ