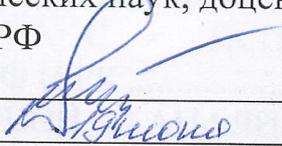


МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ИНСТИТУТ ГОСУДАРСТВА И ПРАВА
Кафедра уголовно-правовых дисциплин

РЕКОМЕНДОВАНО К ЗАЩИТЕ В ГЭК
Заведующий кафедрой, кандидат
юридических наук, доцент, заслуженный
юрист РФ


В.И. Морозов

2023 г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
магистерская диссертация

**ХИЩЕНИЯ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА
(БАНКОВСКИХ КАРТ): ПРОБЛЕМЫ ЗАКОНОДАТЕЛЬНОЙ
РЕГЛАМЕНТАЦИИ И КВАЛИФИКАЦИИ (ПО МАТЕРИАЛАМ РФ И РК)**

40.04.01 Юриспруденция

Магистерская программа «Магистр права»

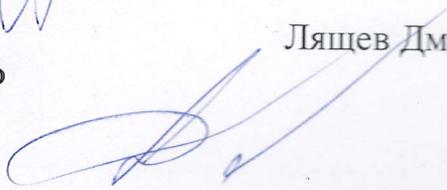
Выполнила работу
студентка 2 курса
очной формы обучения


Мишина Ксения Михайловна

Научный руководитель
кандидат юридических наук


Вассалатий Жанна Васильевна

Рецензент
начальник СЧ СУ УМВД РФ
по Тюменской области
кандидат юридических наук


Лящев Дмитрий Владимирович

Тюмень
2023

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	3
ГЛАВА 1. СРАВНЕНИЕ ПОНЯТИЙ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА, А ТАКЖЕ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ИХ ИСПОЛЬЗОВАНИЕМ В РФ И РК	12
1.1. ПОНЯТИЕ И ОБЩАЯ ХАРАКТЕРИСТИКА ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА В РФ И РК	12
1.2. СРАВНЕНИЕ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА В РФ И РК ...	16
1.3. РАЗВИТИЕ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА ПРЕСТУПЛЕНИЯ, СОВЕРШАЕМЫЕ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА В РФ И РК	22
ГЛАВА 2. УГОЛОВНО-ПРАВОВОЙ АНАЛИЗ ХИЩЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА	29
2.1. ОБЪЕКТИВНЫЕ ПРИЗНАКИ ХИЩЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА	29
2.2. СУБЪЕКТИВНЫЕ ПРИЗНАКИ ХИЩЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА	34
2.3. ХАРАКТЕРИСТИКА ЛИЧНОСТИ ПРЕСТУПНИКА, СОВЕРШАЮЩЕГО ХИЩЕНИЯ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА	38
ГЛАВА 3. ПРОБЛЕМАТИКА В СФЕРЕ ПРЕСТУПНЫХ ДЕЯНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА, ПУТИ СОВЕРШЕНСТВОВАНИЯ ПРАВОВЫХ СРЕДСТВ	43
3.1. ПРОБЛЕМА КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА НА ПРИМЕРЕ КОНКРЕТНОГО УГОЛОВНОГО ДЕЛА	43
3.2. ПУТИ СОВЕРШЕНСТВОВАНИЯ ПРАВОВЫХ СРЕДСТВ В БОРЬБЕ С ПРЕСТУПЛЕНИЯМИ В БАНКОВСКОЙ СФЕРЕ	51
ЗАКЛЮЧЕНИЕ	54
БИБЛИОГРАФИЧЕСКИЙ СПИСОК	58

ВВЕДЕНИЕ

Актуальность темы исследования обусловлена тем, что популярность и удобство безналичных расчетов привлекают внимание не только обычных граждан, но и мошенников. Инновационные технологии, в том числе и в банковской сфере – это мост, соединяющий разные города и страны. Они облегчают коммуникации в области финансовой деятельности, позволяя людям взаимодействовать друг с другом такими способами, которые ранее были немыслимы и невозможны.

Электронные средства платежа, а другими словами – электронные способы осуществления финансовых переводов, на настоящий момент являются одними из самых удобных и распространенных инструментов в жизни человека. Это суждение применимо как к гражданам России и Казахстана, так и к гражданам всех развитых и развивающихся стран.

С помощью электронных средств платежа можно максимально быстро провести онлайн-операции, дистанционно оплатить доставку продуктов или же оформить эксклюзивный заказ из другой страны, перевести безналичные денежные средства близкому человеку или сделать пожертвование иностранным гражданам, попавшим в тяжелые жизненные обстоятельства.

Помимо этого, электронные финансовые инструменты способствуют и заработку. Так, согласно аналитической информации, приведенной специалистами российского банка Русский Стандарт, один из главных трендов валютнообмена 2022 года – растущий интерес россиян к безналичным конвертациям долларов и евро [Информация пресс-центра Банка Русский стандарт].

По сумме же конвертаций перевес в уходящем году на стороне онлайн — его доля составила 71%. Она также выросла по сравнению с 2021 годом, когда составляла 54%.

Кроме того, согласно данным компании, которая занимается разработкой и обслуживанием электронных сайтов и приложений, связанных с онлайн-

переводами денежных средств, в декабре 2022 года в малом бизнесе был зарегистрирован рекордный уровень безналичных операций, составивший 68%. Кроме того, прошедший год характеризовался тенденцией активного развития оплаты при помощи QR-кодов. В частности, общее количество транзакций, осуществленных через QR-коды, за 2022 год возросло в 4,6 раз по сравнению с аналогичным периодом 2021 года [Данные IT-компании Эватор].

В течение последних нескольких лет наблюдался устойчивый рост данного показателя, за исключением периода в марте прошлого года, который был связан с уходом международных операторов. В указанный период доля безналичных платежей сократилась с 64% до 62%, однако уже в апреле ее показатель восстановился до уровня, зарегистрированного в феврале. Стабильное значение показателя на уровне 66% к этому виду платежей было зафиксировано в период с июня по октябрь, однако, в ноябре-декабре произошел повторный рост доли безналичных платежей.

Быстрое и стремительное развитие российского, так называемого электронного рынка, в том числе за счет появления новых векторов развития, вывело Российскую Федерацию на лидирующее место в мире по скорости увеличения безналичных операций и позволило попасть в пятерку мировых лидеров по их количеству за последние несколько лет.

В этом есть заслуга как банковских организаций, так и всех остальных участников рынка: активно и стремительно развивается дистанционное банковское обслуживание, а возможность приема безналичных платежей предусматривается почти в каждом магазине и в каждом электронном приложении. Кроме того, различные стимулирующие поощрения в виде так называемых кешбэков мотивируют людей на еще более частое использование безналичных платежей.

Если говорить о Республике Казахстан, то за 2022 год доля безналичных операций в Казахстане увеличилась с 77,7% до 82,5%. Среди способов безналичных операций наибольшей популярностью пользуются транзакции в

интернете (82,4% от объема всех безналичных операций) [Обзор статистики по безналичным карточным операциям за 2022 год Аналитического центра].

Кроме того, в декабре 2012 года Глава государства в своем Послании представил жителям страны Стратегию развития Республики Казахстан до 2050 года. Главной ее целью стало создание общества на основе сильного государства и развитой экономики, предоставление возможности труда для каждого. Все это в совокупности, по мнению представителей власти, позволит войти Казахстану в тридцатку самых развитых стран мира [Официальный сайт Президента Республики Казахстан].

В рамках указанной Стратегии была разработана и принята Программа «Цифровой Казахстан», которая утверждена Постановлением Правительства Республики Казахстан от 12 декабря 2017 года № 827.

Цель указанной Программы – шаги к опережающему темпу развития экономики республики и улучшение за счет этого качества жизни жителей государства. Этому, по мнению представителей власти, будет способствовать использование новейших технологий, а также создание условий, которые помогут Республике выйти на новый путь развития и обеспечат стабильную долгосрочную перспективу развития цифровой экономики. Способствовать этому будет, в том числе, развитие финансовых и цифровых технологий, а также безналичных платежей.

На фоне такого стремительного роста популярности электронных средств платежа и безналичных расчетов, растет и серьезность проблемы, обусловленной слабой защитой существующих инноваций перед преступными посягательствами и преступными схемами.

Таким образом, можно прийти к выводу, что актуальность исследования тематики, связанной с хищениями, совершаемыми с использованием электронных средств платежа, а также необходимость изучения проблем, возникающих в этой сфере и путей их решения – не вызывает сомнений.

На сегодняшний день большая часть денежных операций совершается с использованием банковских карт – так называемых электронных средств

платежа. Во многом это объясняется удобством по сравнению с классической формой расчета. Оплата благодаря электронным средствам платежа значительно экономит время, позволяет контролировать свои финансы «здесь и сейчас», открывает доступ к сбережениям из любой точки мира. Ровно по этим же причинам растет и частота преступлений, совершаемых с использованием данных технологий.

Такие хищения признаны особым негативным явлением, несмотря на очевидную негативность явления преступлений в целом. Связано это опять же с параллельно развивающимися информационными технологиями, которые активно оказывают влияние на многие сферы государства, в особенности на социально-экономическую.

Названная проблематика отличительна тем, что лица, совершившие преступления и получившие так называемый заработок, инвестируют его в другие преступные сферы, которые зачастую не подконтрольны государству. Такие ситуации наносят вред даже мировым интересам: глобальным финансовым системам и мировой экономике.

Необходимость повышения внимания со стороны законодательных и правоприменительных органов является насущной в свете остроты проблем данной сферы. Это суждение касается как внутригосударственной политики, так и политики мирового сообщества. Официальный сайт Международного валютного фонда содержит релевантную статистическую информацию и предлагает пути решения ключевых проблем, связанных с подобным видом мошенничеств [Маркова, с. 115]. Часть из них будет рассмотрена в данном исследовании.

С целью решения проблем преступных посягательств на денежные средства, хранящиеся в электронном формате, в 2012 году Государственной Думой Российской Федерации был принят Федеральный закон № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации», послуживший началом изменений законодательства страны об уголовной ответственности за новые

виды преступлений, совершенные в форме мошенничества. В результате нововведений 2012 года был предусмотрен новый квалифицирующий признак статьи 158 Уголовного кодекса Российской Федерации. Так, появился пункт «г» в части 3 статьи 158, который предусмотрел ответственность за кражу, совершенную с банковского счета, а равно в отношении электронных денежных средств. Позднее были введены другие, уже отдельные составы преступлений, предусматривающие ответственность за махинации с банковскими картами.

Кроме того, а Российской Федерации для достижения обозначенной цели был принят ряд национальных программных документов: Концепция о долгосрочном социально-экономическом и разработанная на основании поручения Президента Российской Федерации В. В. Путина Стратегия развития информационного общества до 2030 года. Указанные акты ясно отражают необходимость повышения безопасности информационной сферы [Скопин, с. 14].

Перечисленные шаги, предпринятые Российской Федерацией и Республикой Казахстан, свидетельствуют об актуальности основной целевой задачи, стоящей перед государствами – усиление цифровой экономической политики и защита общественных отношений, связанных с использованием электронных расчетов.

Изложенные выше обстоятельства обусловили выбор и актуальность исследуемой темы диссертации.

Цель работы – полный и всесторонний правовой анализ преступлений (хищений), совершаемых с использованием электронных средств платежа, выявление и предложение решений проблем законодательной регламентации и квалификации данного вида преступлений с учетом материалов Российской Федерации и Республики Казахстан.

Исходя из обозначенной цели, можно выделить ряд задач, выполнение которых обеспечит всестороннее освещение темы:

1. Анализ понятия и описание характеристик электронных средств платежа (средств электронного платежа) в Российской Федерации и Республики Казахстан соответственно.
2. Сравнение преступлений, совершаемых с использованием электронных средств платежа (средств электронного платежа) в Российской Федерации и Республики Казахстан.
3. Исследование развития уголовной ответственности за преступления, совершаемые с использованием электронных средств платежа (средств электронного платежа) в Российской Федерации и Республики Казахстан.
4. Исследование объективных и субъективных признаков хищений, совершаемых с использованием электронных средств платежа (средств электронного платежа) в Российской Федерации и Республики Казахстан.
5. Изучение криминологической характеристики личности преступника, совершающего хищение с использованием электронных средств платежа (средств электронного платежа).
7. Выявление проблемы квалификации хищений, совершаемых с использованием электронных средств платежа, на примере конкретного кейса.
8. Поиск путей совершенствования уголовно-правовых средств в борьбе с преступлениями в банковской сфере.

Объектом исследования выступают общественные отношения, так или иначе связанные с реализацией уголовно-правовых норм двух государств, направленных на защиту права собственности в сфере расчета безналичными денежными средствами.

Предметом исследования являются нормы уголовного законодательства Российской Федерации и Республики Казахстан, защищающие право собственности граждан и организаций, сложившаяся практика, а также проблемы их применения.

Методологическую основу работы составили как общие, так и частные методы, применяемые в юридических науках. Благодаря системному методу

было проведено изучение сложных конструкций и явлений, составляющих единую правовую систему.

На основе индукции, дедукции и сравнительного метода удалось найти общее, а также провести различия в законодательствах двух стран – России и Казахстана.

Был использован и историко-правовой метод, который помог в исследовании становления норм, связанных с хищениями, совершаемыми с использованием электронных средств платежа, а также изменений, прошедших в новейшей правовой истории смежного законодательства.

Кроме того, использовался и статистический метод, который способствовал изучению различных статистических данных при формировании криминологического портрета лиц, совершающих преступные деяния с использованием электронных средств платежа.

Формально-юридический или иначе догматический метод также нашел свое применение в данной работе, с его помощью проведено исследование правовых фактов и явлений через уяснение смысла и значимости норм права, исходя из ее собственного содержания.

Уголовные преступления, предусмотренные пунктом «г» части 3 статьи 158 и статьи 159.3 Уголовного кодекса Российской Федерации, а также пунктом 4 части 2 статьи 188 и пунктом 4 части 2 статьи 190 Уголовного кодекса Республики Казахстан, анализировались с различных позиций, выявлялись общие и особенные части, что позволило получить ряд выводов о составляющих частях составов преступлений.

Теоретической основой исследования послужили труды различных ученых, среди которых: Е.А. Маркова, А. Ю. Скопин, А.В. Архипов, А.В. Креховец, М.А. Степанова, Е.В. Царев, Е.А. Русскевич, С.А. Иванчина, З.И. Хисамов, М.Ю. Хмелев, А.В. Шульга, А.А. Южин, П.С. Яни, И.А. Тамазов, С.А. Петров, Б.В. Волженкин, Н.В. Вишнякова, А.В. Савенков, А.В. Бондарь, А.Ю. Филаненко и другие.

Нормативной и эмпирической основами исследования послужили действующее законодательство Республики Казахстан и Российской Федерации, Постановления Пленума Верховного суда Российской Федерации, Нормативные постановления Верховного суда Республики Казахстан, а также судебная практика различных судов.

Теоретическое значение работы состоит в том, что проведенное исследование и сделанные в результате этого выводы могут быть использованы при качественном совершенствовании действующего законодательства и практики его применения как в Российской Федерации, так в и Республике Казахстан. Помимо введения новелл в законодательство, предлагается и ряд других мероприятий, которые действительно могли бы снизить процент ошибочной квалификации совершенных преступлений в рассматриваемой сфере, а также систематизировать судебную практику по аналогичным делам во всей стране.

Апробация результатов исследования.

Отдельные положения выпускной квалификационной работы были апробированы на XVIII Международной научной конференции «GYLYM JÁNE BILIM — 2023», приуроченной ко Дню работников науки, проводимая Евразийским национальным университетом им. Л.Н. Гумилева на лучшую научно-исследовательскую работу студентов и молодых ученых, по итогам которой доклад Мишиной К.М. занял I место в секции «Современные вызовы и поиск эффективных решений в уголовной политике».

Статья Мишиной К.М. представлена в соответствующем сборнике Международной научной конференции «GYLYM JÁNE BILIM — 2023».

Кроме того, принята к публикации в Международном научно-исследовательском журнале «Современный ученый» № 6, 2023 год, статья Мишиной К.М. на тему «Уголовная ответственность за хищения безналичных денежных средств по уголовному законодательству Республики Казахстан и Российской Федерации: сравнительно-правовой анализ».

Структура работы. Выпускная квалификационная работа магистра состоит из введения, трех глав, включающих в себя 8 параграфов, заключения и библиографического списка.

ГЛАВА 1. СРАВНЕНИЕ ПОНЯТИЙ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА, А ТАКЖЕ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ИХ ИСПОЛЬЗОВАНИЕМ В РФ И РК

1.1. ПОНЯТИЕ И ОБЩАЯ ХАРАКТЕРИСТИКА ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА В РФ И РК

Толкование термина «Электронные средства платежа» содержится в Федеральном законе Российской Федерации от 27.06.2011 № 161-ФЗ «О национальной платежной системе». Так, согласно статье 3 названного Федерального закона, под электронными средствами платежа следует понимать средство и (или) способ, позволяющие клиенту оператора по переводу 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.

Исходя из толкования можно понять, что данный термин неразрывно связано с термином «Оператор по переводу денежных средств». Исследование этих понятий в совокупности необходимо для понимания сущности и природы электронных средств платежа.

Так, под оператором по переводу электронных денежных средств понимается организация, которая в соответствии с законодательством Российской Федерации вправе осуществлять перевод денежных средств (в соответствии со статьей 3 Федерального закона Российской Федерации от 27.06.2011 № 161-ФЗ "О национальной платежной системе").

Операторами по переводу денежных средств могут являться следующие организации: Банк России; кредитные организации, имеющие право на осуществление перевода денежных средств и государственная корпорация развития «ВЭБ.РФ» (государственная корпорация развития). Данный перечень является исчерпывающим.

Указанием Банка России от 14.09.2011 № 2694-У «О порядке уведомления Банка России оператором электронных денежных средств» был образован перечень операторов электронных денежных средств, который постоянно меняет свой состав. Актуальный список кредитных организаций, зарегистрированных на территории Российской Федерации, содержится на сайте Центрального Банка РФ, а их количество постоянно меняется. Связано это с регулярной выдачей и отзывом лицензий, необходимых для осуществления банковской деятельности (на 03.04.2023 число кредитных организаций составляет 64 штуки).

Если же говорить о термине «Электронные средства платежа» в рамках законодательства Республики Казахстан, то стоит проанализировать Закон Республики Казахстан «О платежах и платежных системах» от 26.07.2016 года № 11-VI ЗРК.

Так, можно заметить, что данного понятия в дословной его формулировке в законодательстве Республики Казахстан не содержится, но можно встретить схожие формулировки, которые, на первый взгляд, могут показаться нетождественными.

К примеру, в статье 1 названного закона можно встретить понятие «Средство электронного платежа», которое подразумевает под собой платежную карточку или иной электронный носитель, содержащих информацию, которая позволяет отправителю денег, имеющему полномочие совершать платеж и (или) перевод денег, инициировать осуществление платежа и (или) перевода денег, а также осуществлять иные операции, предусмотренные договором между ним и эмитентом средства электронного платежа.

В свою очередь, под эмитентом средства электронного платежа понимается юридическое лицо, осуществляющее выпуск средства электронного платежа.

Таким образом, можно прийти к выводу, что термины российского законодательства «Электронные средства платежа» и «Оператор по переводу денежных средств» являются синонимами казахстанским терминам «Средство

электронного платежа» и «Эмитент средства электронного платежа» соответственно.

Стоит отметить, что законодатель Республики Казахстан также определил конкретных субъектов в качестве эмитентов: Национальный Банк РК, банки второго уровня и Национальный оператор почты. Данный перечень также является закрытым, а это значит, что никакие другие лица и организации не имеют права выпускать электронные деньги.

Наряду с данными терминами можно проанализировать и понятия, касающиеся самих электронных денежных средств. Так, согласно статье 3 Федерального закона от 27.06.2011 № 161-ФЗ "О национальной платежной системе", под электронными денежными средствами понимаются денежные средства, которые предварительно предоставлены одним лицом (лицом, предоставившим денежные средства) другому лицу, учитывающему информацию о размере предоставленных денежных средств без открытия банковского счета (обязанному лицу), для исполнения денежных обязательств лица, предоставившего денежные средства, перед третьими лицами и в отношении которых лицо, предоставившее денежные средства, имеет право передавать распоряжения исключительно с использованием электронных средств платежа. При этом не являются электронными денежными средствами денежные средства, полученные организациями, осуществляющими профессиональную деятельность на рынке ценных бумаг, клиринговую деятельность, деятельность оператора финансовой платформы, деятельность по организации привлечения инвестиций, деятельность по управлению инвестиционными фондами, паевыми инвестиционными фондами и негосударственными пенсионными фондами, деятельность операторов информационных систем, в которых осуществляется выпуск цифровых финансовых активов, и (или) деятельность операторов обмена цифровых финансовых активов и осуществляющими учет информации о размере предоставленных денежных средств без открытия банковского счета в

соответствии с законодательством, регулирующим деятельность указанных организаций.

В Республике Казахстан имеется аналогичный термин «Электронные деньги», содержание которого в разы лаконичнее. Под электронными деньгами понимаются безусловные и безотзывные денежные обязательства эмитента электронных денег, хранящиеся в электронной форме и принимаемые в качестве средства платежа в системе электронных денег другими участниками системы.

Российскому законодателю стоит обратить внимание на такую емкую и лаконичную формулировку в целях устранения недопонимания ее восприятия как со стороны представителей власти, так и со стороны обычных граждан. Этот процесс может привести к эффективному внедрению новых правовых норм, что, в свою очередь, будет способствовать справедливому подходу при решении вопроса квалификации тех или иных преступлений. Кроме того, следует также отметить, что такой подход обеспечит более эффективное выполнение требований законов и нормативных актов, что положительно скажется на доверии граждан к правительству и укреплении общественной безопасности.

1.2. СРАВНЕНИЕ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА В РФ И РК

В Российской Федерации преступные действия, направленные на незаконное завладение безналичными и электронными денежными средствами предусмотрены в виде двух форм хищения (кражи и мошенничества), но регламентируются они при этом тремя статьями уголовного закона – пунктом «г» части 3 статьи 158 Уголовного кодекса Российской Федерации (кража с банковского счета, а равно в отношении электронных денежных средств), статьей 159.3 Уголовного кодекса Российской Федерации (мошенничество с использованием электронных средств платежа), а также пункта «в» части 3 статьи 159.6 Уголовного кодекса Российской Федерации (Мошенничество в сфере компьютерной информации, совершенное с банковского счета). Все три статьи включены в одну главу под названием «Преступления против собственности» с учетом тождества их видового объекта [Архипов, с. 45]. В настоящем исследовании подробно будут проанализированы первые две статьи.

Можно заметить, что в каждом из трех упомянутых составов так или иначе фигурирует понятие «Электронные средства платежа».

Теперь же стоит поговорить о законодательстве Республики Казахстан. Здесь также предусмотрена уголовная ответственность за хищение безналичных денежных средств в виде двух форм хищений, выраженных несколькими составами – пунктом 4 части 2 статьи 188 Уголовного кодекса Республики Казахстан (кража, совершенная путем незаконного доступа в информационную систему либо изменения информации, передаваемой по сетям телекоммуникаций), пунктом 4 части 2 статьи 190 Уголовного кодекса Республики Казахстан (мошенничество, совершенное путем обмана или злоупотребления доверием пользователя информационной системы).

Стоит отметить, что в Республике Казахстан нет такого квалифицирующего признака хищения, как с банковского счета, а равно в отношении электронных

денежных средств, да и вообще отсутствует понятие «Электронные средства платежа» (в рамках рассматриваемых статей). Однако существуют составы преступления хищения имущества путем вмешательства в информационную систему. Такой термин гораздо шире, чем отечественный «аналог» в виде электронных средств платежа.

Согласно статье 1 Закона Республики Казахстан «Об информатизации» от 24.11.2015 № 418-V, информационная система – это организационно упорядоченная совокупность информационно-коммуникационных технологий, обслуживающего персонала и технической документации, реализующих определенные технологические действия посредством информационного взаимодействия и предназначенных для решения конкретных функциональных задач.

Под информационно-коммуникационными технологиями здесь понимается совокупность методов работы с электронными информационными ресурсами и методов информационного взаимодействия, осуществляемых с применением аппаратно-программного комплекса и сети телекоммуникаций.

Электронные информационные ресурсы, в свою очередь, это информация в электронно-цифровой форме, содержащаяся на электронном носителе и в объектах информатизации.

На первый взгляд, исходя из толкования терминов, можно прийти к выводу, что законодатель в данном случае не ограничивается лишь «банковскими» преступлениями, а, напротив, расширяет круг деяний, за которые может предусматриваться ответственность ранее названными нормами Уголовного кодекса Республики Казахстан.

Это суждение особенно играет роль на сегодняшний день, так как под информационными ресурсами (именно до этого понятия можно дойти по так называемой «цепочке» терминов, упомянутой ранее) понимаются и, например, в том числе, не менее актуальные на сегодняшний день различные бонусные баллы, с хищением которых в Российской Федерации, а точнее, с квалификацией их хищения, возникают некоторые проблемы.

Вместе с тем, в своих разъяснениях, Верховный Суд Республики Казахстан сужает толкование мошенничества, совершенного в отношении пользователей информационных систем. Такой вывод вытекает из комментария, содержащегося в пункте 8 Нормативного постановления Верховного Суда Республики Казахстан от 29.06.2017 года № 6.

Так, в указанном пункте содержится положение о том, когда мошенничество, совершенное в отношении пользователей информационных систем, признается оконченным – с момента перевода потерпевшим денежных средств и (или) личных данных виновному или по его указанию другим лицам.

Местом же совершения мошенничества с использованием информационных систем, согласно названному Постановлению, следует считать место нахождения потерпевшего, который переводит денежные средства.

Таким образом, мы видим, что под мошенничеством в информационной системе Верховный Суд Республики Казахстан понимает исключительно мошенничества, связанные с переводом денежных средств, и толкует рассматриваемые нормы ограничительно.

Теперь мы точно видим, как аналогичные по своей сути составы преступлений — хищения электронных денежных средств, имеют кардинальные различия в понятийном аппарате и в формулировках в целом.

При этом нельзя не отметить и сходства в рассматриваемых составах преступлений, рассмотрим некоторые из них.

Так, объективные стороны исследуемых составов преступлений двух стран выражаются исключительно в активных действиях, которые в свою очередь так или иначе направлены на различные воздействия в информационных системах, а также на личную информацию потерпевшего и его денежные средства.

Также стоит отметить и факультативные признаки. Например, для мошенничества факультативным признаком является способ совершения преступления – путем обмана или злоупотребления доверием пользователя информационной системы.

Кроме того, стоит отметить сходства материальной конструкции объективной стороны. И в Российской Федерации, и в Республике Казахстан, такие преступления могут быть признаны оконченными только тогда, когда виновный получил реальную возможность свободно распоряжаться украденными деньгами.

Анализируя особенности субъекта и субъективной стороны исследуемых в данной работе преступлений, можно прийти к выводу, что данные аспекты почти идентичны: субъектом рассматриваемых преступлений как в Республике Казахстан, так и в Российской Федерации — является физическое вменяемое лицо, достигшее шестнадцати лет (для мошенничеств) и четырнадцати лет (для краж), а совершаются преступления лишь с прямым умыслом и корыстной целью.

Если говорить о тяжести рассматриваемых составов преступлений и наказаний за них, то тут мы можем встретить столкнуться с различиями. Если же казахстанский законодатель относит рассматриваемые составы к преступлениям средней тяжести, то российский законодатель разграничивает тяжесть в зависимости от того, каким способом было совершено хищение электронных денежных средств, что представляется более правильным. В случае, если это мошенничество, то тяжесть также будет зависеть от размера похищенного имущества.

Рассмотрим детальнее: например, кража с банковского счета, а равно в отношении электронных денежных средств (пункт «г» части 3 статьи 158 Уголовного кодекса Российской Федерации) относится к ряду тяжких преступлений, так как наказание за него может достигать 6 лет лишения свободы. В случае мошенничества с использованием электронных средств платежа тяжесть содеянного будет зависеть от суммы хищения: небольшая тяжесть (если говорить о части 1 статьи 159.3 Уголовного кодекса Российской Федерации, так как за нее предусмотрено лишение свободы до 3 лет), средняя тяжесть (в случае причинения значительного ущерба гражданину — лишение свободы до 5 лет), тяжкое преступление (при крупном ущербе — лишение свободы до 6 лет), а при

особо крупном размере — часть 4 статьи 159.3 Уголовного кодекса Российской Федерации наказание достигает до 10 лет лишения свободы).

Российский подход в части такой градации наказаний видится более правильным, так как при выборе размера наказания стоит отталкиваться от причинённого ущерба потерпевшему, нежели от способа совершения преступления. Такой подход основан на том, что размер наказания должен быть пропорционален ущербу, который был причинен потерпевшему. В этом случае, нарушители будут наказаны по справедливости, а не по шкале, которая основана на формальных признаках. Такой подход представляется более честным и правильным. В его основе лежит идея о том, что любое преступление должно преследоваться с учетом общественного мнения и последствий для всех участников общественных отношений. Это предполагает правильный выбор тех мер и размеров наказания, которые будут уместными и пропорциональными в каждом конкретном случае. Данный подход является залогом общественной безопасности и справедливости, а данное суждение актуально для большинства стран нашего мира.

Отсюда вытекает и следующий вопрос исследования — сравнение сумм штрафов за аналогичные действия в Республике Казахстан и Российской Федерации. С 1 января 2023 года ставка месячного расчетного показателя в Республике Казахстан увеличена до 3 450 казахстанских тенге, следовательно, при назначении штрафа за кражу, совершенную путем незаконного доступа в информационную систему, его размер будет не более трех тысяч месячных расчетных показателей, то есть 10 350 000 казахстанских тенге, что равнозначно 1 792 368 российским рублям (по состоянию на 03.03.2023). Для мошенничества, которое совершается путем обмана или злоупотребления доверием пользователя информационной системы, сумма штрафа будет составлять не более 13 800 000 казахстанских тенге, что равнозначно 2 389 824 российским рублям (по состоянию на 03.03.2023). В России в это же время кража, совершенная в отношении электронных денежных средств может наказываться штрафом в размере до пятисот тысяч рублей, а мошенничество с использованием

электронных средств платежа — штрафом в размере до ста двадцати тысяч рублей, трехсот и пятисот тысяч рублей за первую, вторую и третью части статьи 159.3 Уголовного кодекса Российской Федерации соответственно).

Можно заметить, что размеры денежных взысканий за аналогичные деяния в Казахстане превышают российские штрафы более, чем в пять-двадцать раз (в зависимости от того, кража это или мошенничество) при условии того, что минимальный размер оплаты труда (минимальная заработная плата) в Республике Казахстан на порядок ниже, чем в Российской Федерации. Это подтверждает тот факт, что штрафы в стране несопоставимы с уровнем жизни казахстанцев и являются одними из самых высоких в СНГ.

Большинство казахстанцев считают, что уровень штрафов не соответствует уровню жизни в стране. Граждане страны понимают, что размер санкций не всегда соответствует характеру нарушения, а готовность граждан выплачивать завышенные суммы остается под вопросом, ведь даже штрафы не всегда являются средством убеждения граждан.

При этом индекс преступности Казахстана составил превышает аналогичный индекс в России [Об индексе преступности в разных странах]. Это свидетельствует о том, что даже крупный размер денежного взыскания не способствует снижению преступности в сфере информационных систем Казахстана. Отсюда вытекает вывод, что в Республике Казахстан имеет место быть увеличение размеров наказания в виде лишения свободы за рассматриваемые виды преступлений. Такой вывод обоснован, так как на практике встречаются ситуации, когда лицам, совершившим преступление, удается оплатить назначенный штраф похищенной в ходе преступления суммой (если осужденный не признал вину, а похищенные денежные средства удалось скрыть от органов следствия и суда). В таких случаях при нарушении закона преступник, простыми словами, ничем не рискует.

1.3. РАЗВИТИЕ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА ПРЕСТУПЛЕНИЯ, СОВЕРШАЕМЫЕ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА В РФ И РК

Совокупность событий и обстоятельств, связанных с существованием нормы, содержащейся в Уголовном кодексе Российской Федерации и предусматривающей ответственность за мошенничество с помощью электронных средств платежа, служит примером негативных последствий чрезмерного внимания определенным проблемам. Рассмотрим детально аспекты принятия этого закона, его последующей доработки и интерпретации судами.

В ноябре 2012 года статья 159.3 Уголовного кодекса Российской Федерации была введена в уголовное законодательство Российской Федерации. Появление ее сопровождалась осуществлением глобального проекта, предложенного Верховным Судом Российской Федерации, который был направлен на разграничение, дифференциацию разных видов мошенничества. В пояснительной записке, актуальной на тот момент, были даны некоторые разъяснения относительно того, в каких случаях имеет место быть данный вид мошенничества – когда при использовании чужой банковской карты при оплате товаров или услуг, лицо ставит подпись в чеке на его имя.

На тот период сложившаяся практика и жизненный опыт свидетельствовали о том, что нет необходимости выделения нового вида хищения, ведь почти 100% расчетов осуществлялись без обязательной подписи клиента банка на кассовом чеке, а представители торговых организаций, в свою очередь, даже не имели полномочий проверки принадлежности карты тому или иному лицу. К тому же, такая проверка вызвала бы ряд негативных эмоций со стороны законных владельцев банковских карт.

В 2017 году Верховный суд представил разъяснения, которые касались и мошенничеств в целом, и конкретно рассматриваемого состава. Так, в пункте 17 Постановления Пленума Верховного суда от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» сказано, что

действия лица следует квалифицировать по статье 159.3 Уголовного кодекса Российской Федерации в случаях, когда хищение имущества осуществлялось с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты путем сообщения уполномоченному работнику кредитной, торговой или иной организации заведомо ложных сведений о принадлежности указанному лицу такой карты на законных основаниях либо путем умолчания о незаконном владении им платежной картой.

Позднее положения Федерального закона от 23.04.2018 № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» внесли коррективы в название статьи 159.3 Уголовного кодекса Российской Федерации. Так, стал использоваться более универсальный термин – «Электронное средство платежа». Это было особенно актуально в связи с повсеместным использованием технологии PayPass.

Кроме того, часть 1 статьи 159.3 Уголовного кодекса Российской Федерации была изменена в части о необходимости обмана уполномоченного работника кредитной, торговой или иной организации. Такая обновленная диспозиция нормы почти дословно воспроизвела свое наименование, что вызвало обоснованную критику со стороны ученых [Креховец, Степанова, с. 158].

Такая ситуация произошла, потому что данное изменение не предполагалось заранее. Первоначальные изменения должны были ограничить использование «платежных карт» в рамках рассматриваемого состава, но со временем, в ходе обсуждения Правовое управление Аппарата Государственной Думы Федерального Собрания Российской Федерации в своих заключениях небезосновательно отметило, что проект статьи 159.3 Уголовного кодекса Российской Федерации необходимо связать с той терминологией, которая используется с 2011 года в Федеральном законе «О национальной платежной системе», а именно в части определения электронных денежных средств от 27.06.2011 года № 161-ФЗ.

С учетом этого было указано, что в «абзац первый части первой статьи 159.3 Уголовного кодекса Российской Федерации не требуется включение повторного

разъяснения рассматриваемого понятия». Архипов А.В. не безосновательно отмечает: «принятая во втором и окончательном чтениях редакция ст. 159.3 УК РФ стала результатом не вполне удачной правки первоначального текста законопроекта, целью которой было всего лишь упрощение формулировки основного состава рассматриваемого преступления, придание ему более компактной формы» [Архипов, с. 4].

До момента принятия Федерального закона от 23.04.2018 года № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» практика правоохранительных органов по делам о мошенничестве, с использованием электронных средств платежа имела спорный характер.

К уголовной ответственности, предусмотренной статьей 159.3 Уголовного кодекса Российской Федерации привлекались те лица, которые, приобретали товары или оплачивали услуги чужой банковской картой, но на такую сумму, при которой не требовалось знание и ввод пин-кода собственника. В то же время, когда лицо незаконно овладевает той же банковской картой, но использует ее для снятия наличных денежных средств посредством банкомата, содеянное квалифицировалась как кража.

Более того, встречались случаи, когда правоохранительные органы вменяли лицам совокупность двух преступлений (кражи и мошенничества) в тех случаях, когда виновные и совершали покупку, и снимали денежные средства в непосредственной близости от кассы посредством банкомата. Стоит отметить избыточную квалификацию содеянного в данном случае. Вопрос о чрезмерности наказания при таких ситуациях стал насущной повесткой обсуждения в научном сообществе.

Уже по истечении времени представители следственных и судебных органов показали свое положительное отношение к тому, чтобы сохранить устоявшееся на время в практике понимание специального вида мошенничества, предусмотренного статьей 159.3 Уголовного кодекса Российской Федерации. Это было достаточно предсказуемым явлением в связи с тем, что новые

разъяснения Пленума Верховного Суда Российской Федерации по данному вопросу не оглашалось.

Но, спустя время, а именно в сентябре 2020 года, было провозглашено новое решение Верховного Суда РФ по делу Ю. Ю. Кактана, которое вновь изменило только определившееся понимание о разграничении кражи и мошенничества в отношении электронных средств платежа. Суд указал, что совершенную с использованием похищенной или поддельной банковской карты оплату товара в магазине, в том числе и в присутствии продавца, необходимо квалифицировать именно как кражу. Правоприменительная практика вновь изменила свой вектор развития. Некоторые авторы подвергли Постановление Пленума Верховного Суда Российской Федерации обоснованной критике, а другие поддержали обновленные разъяснения [Русскевич, с. 16].

Неоднозначность выводов Верховного Суда послужила поводом и для нового специального разбирательства в Конституционном Суде Российской Федерации. В свежем решении от 09.07.2021 Конституционный Суд указал, что идентификация лица как законного владельца платежной карты не является необходимым элементом такой оплаты. Соответственно, это не позволяет расценивать такие деяния как мошенничество, подпадающее под действие части 1 статьи 159.3 Уголовного кодекса Российской Федерации.

Отныне утвержденный двумя судами подход в разграничении двух смежных составов преступлений утвердился и в современной правоприменительной практике. Суды стали обращать внимание на то, что, во-первых, представители торговых организаций не принимали участия в осуществлении операций по списанию денежных средств, во-вторых, имел место актуальный бесконтактный способ оплаты товаров и услуг, а, в-третьих, не было признаков обмана или злоупотребления доверием.

Но, вместе с тем, такие усилия со стороны судебных органов по толкованию статьи 159.3 Уголовного кодекса Российской Федерации завершились появлением новой проблематики, ведь интерпретационная деятельность высших судебных инстанций отменила практику, которая составляла большую часть

уголовных дел в исследуемой сфере. В связи с этим возникло представление, что проблематика аналогичных смежных составов была разрешена, однако, это мнение можно назвать ошибочным, ведь названная проблема остается актуальной и на сегодняшний день.

Довольно сомнительной представляется сама идея о том, что легальное определение использования электронного средства платежа должно быть в неизменном виде воспринято при толковании исследуемого вида мошенничества. Законодатель формулировал его для целей регулирования правомерного поведения субъектов. Это определение обращено к кредитным организациям и их клиентам, в то время как использование электронного средства платежа по смыслу статьи 159.3 Уголовного кодекса Российской Федерации – это действия лица, совершающего хищение.

Таким образом, специфика объективной стороны мошенничества, предусмотренного статьей 159.3 Уголовного кодекса Российской Федерации, выражается в содержании (направленности) обмана — виновный вводит потерпевшего в заблуждение относительно обстоятельств, связанных с электронным средством платежа: действительного держателя платежной карты (например, когда злоумышленник делает рассылку с просьбой одолжить денежные средства от имени третьего лица и прикрепляет измененное в графическом редакторе изображение платежной карты), конечного получателя (подмена реквизитов на официальных сайтах организаций; подмена QR-кодов для оплаты или доступа к приложениям).

Если же анализировать развитие казахстанских уголовных норм, регулирующих интересующие нас отношения, то здесь дела обстоят иначе. Новый уголовный кодекс Республики Казахстан от 03.07.2014 года № 226-V ЗРК заведомо содержал в себе новые положения о так называемых "информационных" кражах и мошенничествах.

Уже на тот момент уголовное законодательство Республики Казахстан предусматривало ответственность за хищение безналичных и электронных денежных средств несколькими способами, как уже отмечалось, путем кражи и

мошенничества (пункт 4 части 2 статьи 188 и пункт 4 части 2 статьи 190 Уголовного кодекса Республики Казахстан соответственно).

Указанные составы преступлений в интересующей нас части не изменялись с момента их введения (2014 год). Связано это с тем, что термин «информационная система» заведомо охватывал наибольшее количество возможных общественно опасных деяний и не содержал в себе спорных формулировок.

В 2017 году вышли лишь дополнительные разъяснения Верховного суда Республики Казахстан. Так, в положениях Нормативного постановления Верховного Суда Республики Казахстан от 29.06.2017 № 6 «О судебной практике по делам о мошенничестве» содержались следующие комментарии касательно «информационных» мошенничеств.

Мошенничество, совершенное в отношении пользователей информационных систем, признается оконченным с момента перевода потерпевшим денежных средств и (или) личных данных виновному или по его указанию другим лицам.

Местом совершения мошенничества с использованием информационных систем следует считать место нахождения потерпевшего, который переводит денежные средства.

Под мошенничеством, совершенным путем обмана или злоупотребления доверием пользователя информационной системы следует признавать действия виновного, направленные на завладение имуществом или правом на имущество пользователя информационной системы, совершенные посредством информационных технологий (компьютера, компьютерных программ, интернета, сотового телефона и т. п.), путем размещения в информационной системе заведомо недостоверных сведений или программ, с целью реализации его преступного умысла на обман пользователя посредством Qiwi-кошелька, интернет-банкинга и т. д.

Названные разъяснения можно назвать вполне уместным. Более того, в отличие от российской практики, они не исказили первоначальное восприятие

состава преступления, предусмотренного пунктом 4 части 2 статьи 190 Уголовного кодекса Республики Казахстан и не поменяли ход судебной практики в сфере «информационных мошенничеств».

ГЛАВА 2. УГОЛОВНО-ПРАВОВОЙ АНАЛИЗ ХИЩЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА

2.1. ОБЪЕКТИВНЫЕ ПРИЗНАКИ ХИЩЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА

Известно, что в науке уголовного права объектом преступления называются такие общественные отношения, которые охраняются уголовным законом и которым причиняется вред (создается реальная угроза причинения такого вреда) в результате совершения преступления [Мельникова, с. 512].

Так, объективная сторона рассматриваемых в исследовании видов краж и мошенничеств характеризуется активными действиями, воздействующими либо на информационную систему (актуально для законодательства Республики Казахстан), либо на банковский счет пользователя посредством использования электронных средств платежа (актуально для законодательства Российской Федерации) и факультативными признаками, которые де-юре разнятся в России и Казахстане в связи с разным понятийным аппаратом, но де-факто представляют собой одни и те же действия лиц, направленные на хищение денежных средств с чужих банковских карт.

Если говорить о конструкции объективной стороны рассматриваемых составов преступлений как в России, так и в Казахстане — преступления, предусмотренные пунктом «г» части 3 статьи 158 Уголовного кодекса Российской Федерации, статьей 159.3 Уголовного кодекса Российской Федерации, а также пунктом 4 части 2 статьи 188 Уголовного кодекса Республики Казахстан, пунктом 4 части 2 статьи 190 Уголовного кодекса Республики Казахстан, являются материальными, то есть признаются оконченными с момента наступления реальных последствий [Иванчина, с. 25].

Стоит детальнее разобрать объективную сторону рассматриваемых преступлений на конкретном примере.

Так, для полного понимания состава преступления, закрепленного в статье 159.3 Уголовного кодекса Российской Федерации, необходимо рассмотреть три

вида объектов – непосредственный, видовой и родовой. Определение последних двух объектов не вызывает сложностей. Благодаря чёткому закреплению названия разделов Уголовного кодекса Российской Федерации, в том числе и раздела, в котором расположена анализируемая статья, нетрудно выяснить, что родовым объектом рассматриваемого преступления признаются общественные отношения в сфере экономики. Если углубиться детальнее, то под экономикой понимается совокупность производства, перераспределения и потребления материальных и нематериальных благ. Далее проанализируем название главы Уголовного кодекса, в которой расположена статья: «Преступления против собственности». Так можно понять, что видовым объектом являются общественные отношения, направленные на защиту собственности. Стоит отметить, что защита прав собственности закреплена и на конституционном уровне, являясь значимым звеном в борьбе с мошенничеством.

Так, положениями статьи 8 Конституции Российской Федерации, принятой всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020, установлена неприкосновенность и равная защита всех форм собственности. Изучение категории собственности в данном случае должно сопровождаться анализом следующих элементов: экономического (с акцентом на материальный ущерб) и правового (с акцентом на нарушение нематериальных прав и интересов лиц, организаций). Непосредственным объектом преступления, предусмотренного статьей 159.3 Уголовного кодекса Российской Федерации, являются общественные отношения, связанные с охраной имущества собственников, против которого совершается конкретное запрещенное уголовным законом посягательство.

Верно отмечает в одной из своих работ Анисимов В. Ф.: «непосредственным объектом хищения является та форма собственности, в которой находится похищаемое имущество» [Анисимов, с. 381]. Именно поэтому четкое понимание природы непосредственного объекта исследуемого преступного посягательства необходимо начинать с анализа понятийного аппарата и термина, содержащихся в диспозиции нормы, а именно – «Электронное средство платежа».

Подробнее о значении этого термина говорилось ранее, поэтому сейчас можно делать вывод о том, что под формой собственности в данном случае понимаются именно денежные средства.

Собственнику денежных средств причиняется реальный ущерб в случае, когда деньги выходят из его правообладания в результате преступных посягательств. Человек не может ни пользоваться, ни распоряжаться принадлежащим ему на праве закона имуществом. Это значит, что непосредственным объектом преступления, совершенного с использованием электронных средств платежа, являются отношения собственности граждан и организаций по отношению к денежным средствам. Преступные действия могут выражаться в фальсификации данных, использовании похищенных или поддельных карт, в виде взлома систем безопасности и так далее. Все это по отдельности и в совокупности может привести к серьезным финансовым потерям для граждан и организаций, а также к нарушению баланса национальной платежной системы. Поэтому борьба с такими видами преступлений является одной из главных задач правоохранительных органов каждого государства.

Не следует забывать и о том, что в современном мире, где все больше операций проводится безналичным путем через электронные средства платежа, возникает необходимость особого внимания информационной безопасности. Стоит отметить, что современные технологии и электронные средства платежа действительно существенно упрощают жизнь человека. Они обеспечивают возможность проведения операций в любом месте и в любое время суток, что является несомненным преимуществом. Однако, вместе с этим, возникает и риск кражи или утечки конфиденциальной информации.

Преступления, связанные с использованием платежных карт, зачастую направлены на взлом систем безопасности, а также связаны с электронными коммуникациями. Все это объясняет и оправдывает необходимость добавления дополнительного объекта преступного посягательства – информационной безопасности, которой наряду с общественными отношениями причиняется немалый ущерб. Такие преступления порой приводят к масштабным

финансовым потерям для граждан и организаций, а также к нарушению стабильности национальной платежной системы в целом. В связи с этим особое внимание стоит уделить защите персональных данных и конфиденциальности информации.

Перед внесением изменений в абзацы 1 и 2 пункта 17 Постановления Пленума Верховного Суда РФ от 30.11.2017 № 48, закон определял хищение денег через электронный платеж как преступление, которое включает в себя общественно опасное деяние, общественно опасные последствия и причинно-следственную связь между ними. Состав преступления был связан с использованием обмана или злоупотребления доверием владельца или иного лица, с оплатой товаров или услуг бесконтактным путем, не задействовавшим работников торговых организаций при списании денег с банковского счета.

Определением Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 29.09.2020 № 12-УДП20–5-К6 установлено, что обман или злоупотребление доверием является спецификой этого преступления.

Однако, Постановлением Пленума Верховного Суда РФ от 29.06.2021 № 22 «О внесении изменений в отдельные постановления Пленума Верховного Суда Российской Федерации по уголовным делам» были внесены изменения, которые не раскрывали объективную сторону рассматриваемого преступления. Это спровоцировало затруднения в определении данного состава преступления.

Хотя абзацы, объясняющие объективную сторону уголовного правонарушения, были исключены из закона, сам состав преступления и уголовное законодательство сохранили свою силу.

Можно было предположить, что позднее Пленум Верховного Суда по-новому интерпретирует объективную сторону преступления, но по истечению двух лет надежды на новые разъяснения Верховного Суда снижаются.

Необходимо обратить внимание на способы совершения преступления, так как они являются основой для разграничения смежных составов. Законодатель предусматривает два способа: обман и злоупотребление доверием. Однако, часть 1 статьи 159.3 Уголовного кодекса Российской Федерации не указывает на

конкретные способы мошенничества, что приводит к разной квалификации действий виновных лиц.

Законодательные изменения 2018 года внесли изменения в статью 159.3 Уголовного кодекса Российской Федерации, которые исключили обязательный признак состава преступления – обман уполномоченного работника кредитной, торговой или иной организации. Тем не менее, следует отметить, что статья 159.3 Уголовного кодекса Российской Федерации предусматривает специальный вид мошенничества, относительно статьи 159 Уголовного кодекса Российской Федерации, независимо от того, на кого был направлен обман – на самого потерпевшего или на работника организации.

Однако, чтобы исключить квалифицирующий признак «совершение мошенничества группой лиц», преступное лицо и уполномоченный работник кредитной, торговой или иной организации не должны находиться в доверительных отношениях. В противном случае, если уполномоченный работник позволяет преступнику совершать задуманные действия, это будет расцениваться как преступление, совершенное группой лиц.

Подводя итог, следует отметить, что на данный момент отсутствует точное законодательное закрепление объективной стороны состава преступления, предусмотренного статьей 159.3 Уголовного кодекса Российской Федерации, что вызывает сомнения в применении данной нормы на практике.

2.2. СУБЪЕКТИВНЫЕ ПРИЗНАКИ ХИЩЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА

В данном случае, раскрывая вопрос субъективных признаков хищений, совершенных с использованием электронных средств платежа, можно рассмотреть субъективную сторону и мошенничества, и краж в совокупности.

Общие требования к субъекту преступления закреплены в статье 19 Уголовного кодекса Российской Федерации и статье 15 Уголовного кодекса Республики Казахстан, согласно положениям которых, уголовной ответственности подлежит вменяемое физическое лицо, достигшее возраста уголовной ответственности.

Так, субъектом преступления может признаваться только физическое лицо. Это суждение актуально не только для рассматриваемых составов преступлений, но и для всех в целом. К уголовной ответственности, в отличие от иных видов ответственности (административной, налоговой, гражданско-правовой), не может быть привлечено юридическое лицо, и, даже если транзакции и финансовые операции с электронными денежными средствами незаконно осуществлялись от лица организации. В данном случае подлежит установлению конкретное физическое лицо, действовавшее на тот момент от лица фирмы. Именно данное физическое лицо будет привлечено к уголовной ответственности в случае установления в его действиях признаков состава преступления [Филиппов, с. 30].

Кроме того, общим является и правило о вменяемости лица. Вменяемость означает, что лицо в момент совершения преступления способно осознавать общественную опасность своего деяния, а также руководить им. Стоит отметить, что не подлежит уголовной ответственности лицо, которое и, например, похитило деньги, но находилось в этот момент в состоянии невменяемости, то есть не могло и не осознавало общественную опасность своего деяния в силу какого-либо расстройства психики или заболевания.

Если же говорить о возрасте уголовной ответственности, то тут имеются различия. В случае мошенничества с использованием электронных средств платежа и мошенничества в информационных системах, уголовная ответственность наступает по общему правилу – с 16 лет. Если рассматривать кражу в отношении электронных денежных средств, а также кражу путем незаконного доступа в информационную систему, то в данном случае к ответственности может быть привлечено лицо, достигшее не общего установленного шестнадцатилетнего возраста, а пониженного – 14 лет (на момент совершения преступления).

С чем связана такая дифференциация, за казалось бы, смежные деяния, пытается объяснить А.И. Бойцов: «Снижение возраста уголовной ответственности за кражу, грабеж и разбой, объясняется не только более высокой общественной опасностью данных имущественных посягательств, обусловленной более опасным способом их совершения, но и более широкой их распространенностью среди совершаемых подростками преступлений, обусловленной уровнем их социализации, предопределяющим как интеллектуальную, так и исполнительскую доступность данных способов хищения для 14-летних» [Бойцов, с. 773] .

Кроме того, Л.Д. Ермакова считает, что в части 2 статьи 20 Уголовного кодекса Российской Федерации закон перечисляет лишь те деяния, общественную опасность которых в полной мере может осознать лицо, достигшее 14 лет. Опасность и значение этих посягательств доступны, по мнению специалистов, пониманию подростков» [Здравомыслов, с. 217]. Мнение Л.Д. Ермаковой видится более грамотным исходя из целей уголовного законодательства, ведь все-таки главным критерием определения возраста уголовной ответственности является возможность понимания, осознания лицом общественной опасности совершаемого им деяния.

С учетом данного утверждения, законодательство обоснованно устанавливает, что ответственность за совершение мошенничества возникает

только после достижения лицом общего возраста уголовной ответственности – 16 лет.

Каких-либо конкретных разъяснений о характеристиках субъекта преступления, предусмотренного статьей 159.3 Уголовного кодекса Российской Федерации – Верховный суд не дает, в то время, как, например, по статьям 159.2 и 159.5 можно найти встретить более подробные комментарии данной инстанции. Так, субъектом преступления, предусмотренного статьей 159.2 Уголовного кодекса Российской Федерации, может быть лицо, как не имеющее соответствующего права на получение социальных выплат, так и обладающее таким правом (например, в случае введения в заблуждение относительно фактов, влияющих на размер выплат). Или же, к примеру, субъектом преступления, предусмотренного статьей 159.5 УК РФ, может быть признано лицо, выполнившее объективную сторону данного преступления (например, страхователь, застрахованное лицо, иной выгодоприобретатель, вступившие в сговор с выгодоприобретателем представитель страховщика, эксперт). Единственное разъяснение, которое можно встретить в Постановлении Пленума Верховного Суда РФ от 30.11.2017 N 48 (ред. от 15.12.2022) "О судебной практике по делам о мошенничестве, присвоении и растрате", касающееся субъекта преступления – это то, что под лицами, использующими свое служебное положение при совершении мошенничества, присвоения или растраты (в том числе по части 3 статьи 159.3 Уголовного кодекса Российской Федерации), следует понимать должностных лиц, обладающих признаками, предусмотренными пунктом 1 примечаний к статье 285 УК РФ, государственных или муниципальных служащих, не являющихся должностными лицами, а также иных лиц, отвечающих требованиям, предусмотренным пунктом 1 примечаний к статье 201 УК РФ (например, лицо, которое использует для совершения хищения чужого имущества свои служебные полномочия, включающие организационно-распорядительные или административно-хозяйственные обязанности в коммерческой организации).

Мошенничество – это преступление, требующее определенных интеллектуальных способностей и жизненного опыта. Оно характеризуется использованием психологических механизмов, быстроты мышления и реакции. Следовательно, мошенничество среди несовершеннолетних встречается значительно реже.

Субъективная сторона рассматриваемых составов преступлений представляет собой совокупность предусмотренных законом признаков, которые характеризуют состояние лица на момент совершения общественно опасного деяния. Здесь стоит исследовать три компонента: вину, мотив и цель.

Вина отражает внутреннее, психическое отношение лица к совершенному им преступлению и наступившим в результате последствиям. Исходя из теории уголовного права, вина делится на два вида – умышленную и неосторожную. Преступления, предусмотренные пунктом «г» части 3 статьи 158 и статьи 159.3 Уголовного кодекса Российской Федерации с субъективной стороны характеризуется исключительно прямым умыслом.

Если же мы говорим, про мошенничество с использованием электронных средств платежа, то здесь Лицо должно осознавать, что использует поддельное или принадлежащее другому лицу электронное средство платежа, а также должно предвидеть возможность наступления последствий в виде причинения ущерба и желать их наступления.

Элемент, побуждающий на совершение рассматриваемых преступлений – мотив, при рассмотрении данного вида преступления является факультативным и не влияет на размер наказания. Здесь стоит четко разграничивать корыстные мотивы и корыстные цели. Для правоприменителя в данном случае важна именно цель, которая подтверждает или опровергает умышленный характер преступления.

Свидетельством наличия злонамеренных намерений лица при получении выплат является явное отсутствие юридических прав на получение соответствующих выплат, а также использование фальшивых документов для их получения и сокрытие информации о причинах прекращения выплат.

2.3. ХАРАКТЕРИСТИКА ЛИЧНОСТИ ПРЕСТУПНИКА, СОВЕРШАЮЩЕГО ХИЩЕНИЯ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА

Показатель результативной раскрываемости хищений с использованием электронных средств платежа не велик. Это суждение актуально как для Российской Федерации, так и для Республики Казахстан.

Рассматриваемые преступления отличаются высоким уровнем латентности в связи с повышенной степенью скрытности незаконных банковских операций, что свидетельствует о необходимости проведения профилактических и предупредительных методов на индивидуальном уровне [36]. Это подразумевает под собой детальное, подробное изучение личности преступника.

Криминология фокусируется на личности преступника как на основном объекте исследования. Важность данного вопроса заключается в том, что совершение преступления является выражением индивидуальной воли, которая определяется личностными характеристиками и особенностями субъекта, являющегося активным участником психологических и социальных взаимодействий.

Криминальный признак социализации предполагает, что лицо, совершающее преступление, действует как участник общественного сообщества, который выражает коллективную психологию и культурные ценности определенного времени и места, а также свои индивидуальные особенности, включая правовые, моральные, этические и другие убеждения и ценности.

По мнению Ю. А. Ковалевой, личность преступника может быть рассмотрена в качестве модели, социально-психологической конструкции, которая обладает определенными специфическими чертами. Данный термин обозначает накопленные научные понимания о характеристиках людей, совершающих преступления [Ковалева, с. 115]. Немаловажными признаками этой личности являются радикальные воззрения, негативное отношение к

моральным ценностям и использование опасных инструментов для удовлетворения своих потребностей.

Обычно изучение личности преступника начинается с анализа его социально-демографических характеристик, которые включают в себя такие факторы, как пол, возраст, семейное положение, образование и другие факторы. Анализ названных факторов позволяет выявить уровень преступной активности у различных групп населения.

Так, статистические сведения о хищениях денежных средств с банковских карт свидетельствует о том, что подобные преступления совершает значительно больше мужчин (67,42 %), чем женщин (32,58 %).

В исследовании социально-демографических характеристик личности преступника следует обратить особое внимание на возрастной показатель, так как оно существенно влияет на потребности, жизненные планы, интересы и образ жизни человека. Например, совершаемые преступления с использованием электронных средств платежа можно условно классифицировать по возрастным группам.

- старше 50 лет — 6 %;
- 30-49 лет — 60 %;
- 25-29 лет — 17 %;
- 18-24 года — 16 %;
- до 18 лет — 1 %.

Большинство преступников данной категории относятся к возрастной группе от 30 до 49 лет. Как отмечает Л. М. Прокументов, с возрастом происходят изменения в личности людей - меняются их социальные роли и функции, опыт, взгляды и поведение в конфликтных ситуациях [Прокументов, с. 54]

Преступное поведение взрослых является более общественно опасным, чем у молодых преступников, так как они имеют больший жизненный опыт, сформировавший их характер и потребности. В этом возрасте формируется модель криминальной активности, начатая в более юном возрасте.

Внимательно стоит рассмотреть уровень образования преступников этой сферы. В криминологии часто возникает предположение о том, что уровень образования выделяет именно мошенников среди общей массы преступников. Хотя уровень образования не может являться исчерпывающим фактором в определении наличия криминогенных факторов, он непосредственно влияет на формирование общих представлений о морали и ценностных ориентациях личности.

Преступников в сфере неправомерного использования электронных средств платежа можно разбить по уровню образования на следующие группы:

- высшее профессиональное — 4,07 %;
- среднее профессиональное — 41,15 %;
- среднее общее — 35,41 %;
- основное общее, начальное или без образования — 19,37 % [Сводные статистические сведения о состоянии судимости в России за 2022 год].

Представленная информация указывает на то, что большинство преступников, занимающихся незаконным использованием электронных средств платежа, имеют средний уровень образования. Это подтверждается при анализе социально-ролевых характеристик данной группы преступников.

Исходя из мнения Ю. С. Караваевой, необходимо понимать, что наличие определенного социального статуса и роли не гарантирует преступное поведение со стороны личности [Караваева, с. 177]. Тем не менее, анализ социально-ролевой позиции личности в обществе помогает выявить наиболее подверженные группы лиц и определить специфические меры для предотвращения потенциально негативных последствий. В криминологии социально-ролевые характеристики рассматриваются как важный фактор, способствующий возникновению преступного поведения, и их взаимодействие может определять его проявление.

Преступления в сфере неправомерного использования электронных средств платежа актуальны среди следующих категорий лиц:

- трудоспособные лица без постоянного источника дохода (59,78 %);

- лица рабочих специальностей (19,02 %);
- нетрудоспособные (2,64 %);
- учащиеся и студенты (1,64 %);
- безработные трудоспособные (1,08 %).

Отсутствие постоянного законного дохода является экономической причиной, объясняющей представленные данные. Неоспоримо, что отсутствие стабильного источника доходов способствует увеличению преступности.

Почти половина осужденных имела предыдущие судимости, а треть преступлений была совершена рецидивистами. Это свидетельствует о слабой эффективности мер по борьбе с корыстными преступлениями. Лишение свободы не всегда оказывает воспитательное воздействие на осужденных, особенно если они уже имеют криминальную мотивацию и асоциальные установки. Лишение свободы не всегда оказывает воспитательное воздействие на осужденных, особенно если они уже имеют криминальную мотивацию и асоциальные установки. Высокий уровень рецидива преступлений является дестабилизирующим фактором для общественного развития.

Для того, чтобы осознать причины преступлений в полной мере, стоит проанализировать и нравственную подструктуру личности, ее отношение к социальным ценностям, гражданским обязанностям, моральным установкам, интересам, ориентирам и взглядам, а также к нормам морали и права, и выбранным стратегиям удовлетворения своих потребностей.

Так, по мнению В. Е. Эминова, материальные потребности вызывают корыстную мотивацию поступков. Слабая материальная обеспеченность, характерная для преступников, часто выступает причиной совершения корыстного преступления [Эминов, с. 56].

Как уже отмечалось ранее, при квалификации содеянного по одному из составов преступлений, совершаемых с использованием электронных средств платежа, корыстная цель является обязательным элементом субъективной стороны, в рамках которой виновное лицо и осуществляет свои действия. Это может происходить из соображений личной выгоды, лицом может

преследоваться целью наживы или же обогащения третьих лиц (в судьбе которых виновное лицо так или иначе может быть заинтересовано). Данные суждения актуальны и касательно многих других преступлений, направленных на подрыв общественных отношений в сфере собственности.

Если углубляться детальнее, то в основе преступной мотивации лежат противоречия между имеющимся образом жизни и желаемыми достижениями, что оказывает на мошенника негативное влияние.

Таким образом, анализ личности преступника показал, что преступления, связанные с использованием электронных средств платежа, чаще совершают мужчины (67,42 %), чем женщины (32,58 %). Большинство преступников данной категории относятся к возрастной группе от 30 до 49 лет. Преступное поведение взрослых является более общественно опасным, чем у молодых преступников, так как они имеют больший жизненный опыт, сформировавший их характер и потребности. В этом возрасте формируется модель криминальной активности, начатая в более юном возрасте. Большинство преступников, занимающихся незаконным использованием электронных средств платежа, имеют средний уровень образования. Отсутствие постоянного законного дохода является экономической причиной, объясняющей представленные данные. Неоспорим и тот факт, что отсутствие стабильного источника доходов способствует увеличению преступности.

Приведенные результаты исследования личности преступника, совершившего мошенничество с использованием электронных средств платежа, могут эффективно использоваться при создании стратегий по борьбе с преступностью и улучшении социально-правового регулирования в области сокращения преступности, девиантного поведения и других форм общественной нестабильности.

ГЛАВА 3. ПРОБЛЕМАТИКА В СФЕРЕ ПРСТУПНЫХ ДЕЯНИЙ,
СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ЭЛКТРОННЫХ СРЕДСТВ
ПЛАТЕЖА, ПУТИ СОВЕРШЕНСТВОВАНИЯ ПРАВОВЫХ СРЕДСТВ
3.1. ПРОБЛЕМА КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С
ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА НА ПРИМЕРЕ
УГОЛОВНОГО ДЕЛА

В связи с озвученными в работе проблемами, особенно в части меняющихся разъяснений и формулировок, касающихся хищений с использованием электронных средств платежа и различных подходов к пониманию объективной стороны, логичным становится вывод об отсутствии единого подхода в разъяснении проблемных вопросов, а также вывод о том, что правоприменительная практика не сложилась до конца должным образом.

С подобными проблемами сталкивается большая часть представителей правоохранительных органов: это и следователи на стадии предварительного расследования, и прокуроры при надзоре за законностью и обоснованностью принятых решений, и судьи при вынесении итоговых решений.

Данный факт подтверждается анализом судебной практики. Так, на примере дела № 1-266/2021 Сургутского городского суда Ханты-Мансийского автономного округа – Югры от 05.04.2021 можно заметить, с какими трудностями сталкиваются должностные лица при квалификации преступных посягательств.

Так, в данном случае, в 2019 году из-за сбоя в программе лояльности одной из авиакомпаний пользователь получил возможность перманентно приобретать авиабилеты со скидкой до 90% (в его личном кабинете накопились бонусные баллы — «Мили», за счет которых происходило применение скидки, но сами «Мили» с бонусного счета не списывались). Со временем пользователь понял, что на этом можно зарабатывать и стал предлагать авиабилеты со скидкой для третьих лиц. У него появились постоянные «покупатели», которые в

большинстве случаев летали одними и теми же рейсами на протяжении длительного периода времени. Спустя время Авиакомпания благодаря аналитическим инструментам отследила, что определенные рейсы не приносят должной прибыли, а большинство пассажиров на этих рейсах зарегистрированы через один личный кабинет.

При этом, органы следствия и суд первой инстанции признали мужчину виновным в совершении преступления, предусмотренного статьей 159.3 Уголовного кодекса Российской Федерации — за мошенничество с использованием электронных средств платежа. Под электронными средствами платежа в данном случае признали эти самые бонусы — «Мили», что, исходя из приведенных ранее исследований, является грубым нарушением.

Стоит повторить, что согласно законодательству Российской Федерации, «Мили» — не могут являться электронными средствами платежа, а авиакомпания, в свою очередь, не может являться оператором по переводу денежных средств, так как она не может признаваться кредитной организацией.

Так, согласно Правилам бонусной программы, «Мили» — это условные расчетные единицы, которые не могут быть конвертированы в какую-либо валюту. При этом суд счел правомерным признание бонусных миль как денежной единицы, произвольно установив курс бонусов по отношению к рублю. Суд в данном случае приравнял один рубль и одну бонусную милю, несмотря на то, что фактически «Мили» представляют собой набор компьютерных кодов и не имеют обеспечения. Также стоит отметить, что в ходе проведенной в рамках дела судебно-бухгалтерской экспертизы не ставился и не разрешался вопрос о стоимости одной бонусной мили, что также, является грубым нарушением.

Действительно, зачастую для упрощения внутренних расчетов организации признают, что 1 бонус равен 1 рублю. Однако даже наличие такого внутреннего курса не позволяет заявлять о стоимости 1 бонуса в размере 1 рубля, поскольку ликвидность бонуса гораздо ниже, поэтому его стоимость должна

быть ниже стоимости 1 рубля. Только рубль может быть использован при любых расчетах на территории страны, чего нельзя сказать о «Милях».

Кроме того, было установлено, что участникам бонусной программы необязательно знакомиться с ее правилами. При регистрации правила программы не появляются на экране, подтверждать ознакомление с правилами не требуется. Поэтому можно сделать логичный вывод, что пользователь совершал те действия, которые позволяет ему делать программное обеспечение и заданные алгоритмы. Различные сведения, полученные в рамках служебного расследования, прямо указывали на то, что причина случившегося — системная ошибка программного обеспечения.

По словам пользователя, неполадки в работе сайта периодически случались, но об этом на главном экране появлялось предупреждение (использовать в это время сайт было технически невозможно). Как только неполадки устранялись, сообщение о неполадках исчезало и сайт становился активным.

Тут стоит вспомнить мнения ученых, которые ссылаются на необходимость «активного» обмана каким-либо действием при совершении мошенничеств.

При этом, исходя из показаний представителя потерпевшей стороны следовало, что причины данной системной ошибки не выявлены, а вопрос о том, какие алгоритмы могли привести или привели к системному сбою — не исследовался. Равным образом не исследовался вопрос и о разработчике программного обеспечения, который также может нести ответственность за произошедшее. Можно предположить, что обвинение конкретного пользователя — это самый легкий и простой способ компенсировать убытки от некачественного программного обеспечения.

Кроме того, стоит отметить, что банковские карты, с помощью которых оплачивалась денежная часть авиабилетов, принадлежали именно пользователю, то есть не являлись поддельными или похищенными. Это свидетельствует о том, что пользователь не использовал для оплаты чужие или поддельные банковские

карты, а данный факт, как способ совершения преступления, обязателен для квалификации деяний по статье 159.3 Уголовного кодекса Российской Федерации. Указанный довод подтверждался актуальными на тот момент положениями пункта 17 Постановления Пленума Верховного суда от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», действия лица следует квалифицировать по статье 159.3 Уголовного кодекса Российской Федерации в случаях, когда хищение имущества осуществлялось с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты путем сообщения уполномоченному работнику кредитной, торговой или иной организации заведомо ложных сведений о принадлежности указанному лицу такой карты на законных основаниях либо путем умолчания о незаконном владении им платежной картой.

Возникшая системная ошибка предоставила «расширенные» возможности для участников программы, которые проявлялись в возможности многократного применения скидки. Само утверждение, что пользователь воспользовался системной ошибкой программы, при которой не производилось списание и начисление миль, исключает наличие обмана, как способа совершения преступления, а также говорит о том, что пользователь никаких активных действий для незаконного получения бонусных «миль» не выполнял. Признаки какого-либо несанкционированного вмешательства пользователем в программное обеспечение авиакомпании в материалах дела отсутствовали.

Если углубляться в материалы исследуемого дела детальнее, то стоит напомнить, что возможность применения скидок предоставлялась и продолжает предоставляться Авиакомпанией добровольно. Для гарантии исключения убытков вследствие предоставления акций или скидок, все компании устанавливают допустимый диапазон маржи для своих товаров и услуг. Так, Авиакомпания установила ограничение: использование «Миль» было доступно при условии оплаты банковской картой не менее 1 рубля от стоимости авиабилета или иной услуги. То есть компания просчитала максимальный уровень скидки, которую может предложить клиентам без значительных

убытков — ее предел мог достигать 99%. Данный фактор был проигнорирован как органами следствия, так и судом, вынесшим решение.

Кроме того, в данном деле, суд не высказался по поводу отсутствия в материалах исследования по определению количества пассажиров (заполняемости) аналогичных рейсов в период до того, как лицо осуществляло деятельность по продаже билетов на рейсы со скидкой и в период осуществления им продажи билетов с применением скидки, а также не провел сравнение данных показателей. Вместе с тем, сторона защиты неоднократно ходатайствовала об исследовании данного вопроса, но требования проигнорированы. При этом, многие доказательства по делу в своей совокупности свидетельствовали о том, что, во-первых, пользователь рекламировал и совершал активный поиск реальных клиентов именно для этой авиакомпании, предлагая им более выгодные условия, а этим, в свою очередь, создавал условия для роста продаж. Во-вторых, пользователь увеличивал приток новых пассажиров, тем самым реально повышал доход авиакомпании. Без указанного исследования говорить даже и об упущенной выгоде (в рамках квалификации по статье 165 Уголовного кодекса Российской Федерации – необоснованно). Факт значительного увеличения количества пассажиров, пользующихся услугами авиакомпании, подтверждает то, что реальных убытков авиакомпания в указанный период времени не понесла.

Стоит отметить, что после произошедшего Авиакомпания изменила правила программы: был повышен обязательный порог оплаты авиабилетов банковской картой (теперь необходимо оплатить хотя бы 99 рублей от стоимости авиабилета, а остальную сумму можно покрыть за счет бонусов), что подтверждает доводы об убыточности прежней маркетинговой тактики и необходимости ее коррекции. Вместе с тем, вина за неудачную маркетинговую кампанию перекладывается на обычного пользователя.

Таким образом, можно прийти к четкому и однозначному выводу, что действия пользователя не могут охватываться тем составом преступления,

который предусмотрен статьей 159.3 Уголовного кодекса Российской Федерации.

Более того, стоит оценить, насколько охватываются те же действия пользователя уже статьей 159 Уголовного кодекса Российской Федерации – обычным мошенничеством, ведь на стадии предварительного расследования у должностных лиц возникал вопрос о квалификации содеянного либо по статье 159.3, либо по статье 159 Уголовного кодекса Российской Федерации.

Под любым мошенничеством, в первую очередь, понимается хищение чужого имущества или приобретение права на чужое имущество. Согласно Постановлению Пленума Верховного Суда РФ от 27.12.2002 № 29 «О судебной практике по делам о краже, грабеже и разбое», под хищением понимается изъятие чужого имущества в пользу виновного или других лиц. В данном случае считать «Мили» предметом даже обычного мошенничества — ошибочно, так как они представляют из себя меру скидки, условную расчетную единицу. Это также подтверждается и тем, что приобрести билет или какую-либо услугу у авиакомпании, полностью оплатив товар «Милями» — нельзя. Билет можно приобрести лишь за деньги, а предоставленные в личном кабинете «Мили» использовать как сумму, на которую снижается продажная цена товара, реализуемого покупателю.

Исходя из положений статей 130 и 150 Гражданского кодекса Российской Федерации, «Мили» не могут быть признаны ни недвижимым (к недвижимости относятся земельные участки, участки недр и все, что прочно связано с землей, то есть объекты, перемещение которых без несоразмерного ущерба их назначению невозможно, в том числе здания, сооружения, объекты незавершенного строительства), ни движимым имуществом (в силу правовой природы «Мили»). Также мили нельзя отнести к нематериальным благам (блага неимущественного характера, лишённые экономического содержания и вообще не имеющие стоимостного выражения). Кроме того, «Мили» не имеют обеспечения, так как представляют собой набор компьютерных кодов, децентрализованы и предполагают частично анонимное использование.

Все это свидетельствует о том, что «Мили» по своей природе не могут быть предметом хищения. А какое-либо иное имущество из законного владения Авиакомпании в пользу подсудимого или иных лиц незаконно и безвозмездно не изымалось. Более того, Авиакомпания имела возможность заблокировать или списать накопленные «Мили», которые по мнению органа следствия являлись предметом мошенничества. Это, в свою очередь, противоречит природе хищения, ведь получается, что предмет хищения не выбывал из правообладания Авиакомпании. Пользователь не удерживал у себя какое-либо имущество или денежные средства, которые в соответствии с положениями законодательства или договора должны были поступить в собственность ПАО авиакомпании.

Поэтому в данной ситуации крайне категоричным становятся выводы о том, что действия пользователя охватываются составом мошенничества, а уж тем более – составом мошенничества с использованием электронных средств платежа.

Более верной квалификацией такого деяния предполагается квалификация по статье 165 Уголовного кодекса Российской Федерации – причинение имущественного ущерба путем обмана или злоупотребления доверием. Для объективной стороны названного состава обязательно отсутствие признаков хищения, что в данном случае наиболее соответствует содеянному.

Хотя, стоит повторить, что преступление, предусмотренное пунктом «б» части 2 статьи 165 Уголовного кодекса Российской Федерации, считается оконченным с момента неисполнения лицом своей обязанности по передаче имущества или уплате денежных средств потерпевшему в особо крупном размере. Вместе с тем, у пользователя отсутствовала какая-либо дополнительная обязанность по передаче имущества или уплате денежных средств сверх итоговой стоимости билета, которая автоматически подсчитывалась на официальном сайте авиакомпании при покупке авиабилета и которую он уплачивал в должном размере.

Таким образом, российскому законодателю стоило бы обратить внимание на формулировки аналогичных составов хищений из Уголовного кодекса

Республики Казахстан: здесь ключевым фактором играют уже не электронные средства платежа, а факт неправомерного доступа в информационную систему, факт вмешательства в информационно-коммуникационные технологии.

Заимствование названного терминологического аппарата в российское законодательство позволило бы избежать ошибок в квалификации подобных преступлений и усилило бы позицию правоохранительных органов в цифровой экономической сфере, а также воспрепятствовало бы появлению новых преступных схем, не охваченных законом на сегодняшний день.

3.2. ПУТИ СОВЕРШЕНСТВОВАНИЯ ПРАВОВЫХ СРЕДСТВ В БОРЬБЕ С ПРЕСТУПЛЕНИЯМИ В БАНКОВСКОЙ СФЕРЕ

Как уже стало понятно исходя из данного исследования, глобальной актуальной проблемой в сфере хищений с использованием электронных средств платежа является проблема неверной квалификации содеянного. Связана проблематика с совокупностью следующих факторов: достаточно объемные термины, закрепленные в Федеральном законе «О национальной платежной системе» от 27.06.2011 № 161-ФЗ, к которому отсылает Уголовный кодекс Российской Федерации, частые изменения в диспозициях самих норм, а также в разъяснениях Пленума Верховного Суда Российской Федерации; отсутствие развернутой и законодательно закрепленной иллюстрации объективных сторон совершаемых деяний; а также имеющаяся конкуренция норм Уголовного кодекса Российской Федерации.

Здесь представляется достаточно важным рассмотрение средств улучшения работы правоохранительных органов в борьбе с подобными преступными деяниями. На основании исследования можно сформулировать следующие рекомендации.

В первую очередь требуется принятие нового Постановления Пленума Верховного Суда Российской Федерации или же введение новых положений в имеющееся Постановление с целью разъяснения объема преступных деяний, связанных с хищениями, совершенных с использованием электронных средств платежа. Целью новых разъяснений должно стать разграничение и устранение такой тонкой грани между рассматриваемыми составами преступлений: кража с банковского счета, а равно в отношении электронных денежных средств и мошенничество, совершенное с использованием электронных средств платежа.

Кроме того, необходимы разъяснения, касающиеся посягательств на различные электронные бонусы, которые нельзя признать денежной единицей, но благодаря которым можно частично или полностью производить расчеты в тех или иных организациях.

Также, российскому законодателю стоит обратить внимание на понятийный аппарат, касающийся аналогичных вопросов, Республики Казахстан. Как уже отмечалось ранее, заимствование идеи термина «информационная система» в российское законодательство позволило бы избежать ошибок в квалификации некоторых преступлений и усилило бы позицию правоохранительных органов в цифровой экономической сфере, а также воспрепятствовало бы появлению новых преступных схем, не охваченных на сегодняшний день законом.

Наряду с указанным, необходимо и появление новых разъяснений, касающихся способов совершения мошенничества – обмана и злоупотребления доверием. Спорным остается вопрос о наличии обмана или злоупотребления доверием в случае возникновения «компьютерной», системной программной ошибки. Говорить об обязательных способах совершения преступления (обман или злоупотребление доверием) в таком случае нельзя — компьютерную программу или системные алгоритмы нельзя обмануть в том понимании, которое закладывал в этот термин законодатель, а также нельзя внедриться в доверие системы дистанционного банковского обслуживания. Можно лишь использовать несовершенства системы, ее уязвимости. Также были бы значимыми разъяснения Верховного Суда по вопросу о необходимости исследования участия разработчиков программного обеспечения в совершенных преступных посягательствах.

Все более частое использование альтернативных наличным деньгам вариантов платежных средств людьми навязывает необходимость детального изучения сущности обращения с ними. Здесь видится возможным внесение корректировок в учебные планы по направлениям, связанных с экономической деятельностью и юриспруденцией – с целью уменьшения количества спорных ситуаций на практике. Также в связи с актуальностью использования альтернативных денежным средствам вариантов стоит повышать грамотность не только специалистов, но и обычных граждан, использующих такие методы в своих расчетах.

Не последнее место в вопросе противодействия преступлениям, совершаемым с использованием электронных средств платежа, занимает грамотно организованная система подготовки кадров правоохранительных органов. На сегодняшний день уровень подготовки лиц, непосредственно осуществляющих раскрытие и расследование рассматриваемых деяний, недостаточен, поэтому повышение их квалификации «извне» приходится уместным. В связи с тем, что почти все хищения с банковского счета, а равно в отношении электронных денежных средств совершаются с помощью использования продвинутых информационных технологий и иных инноваций в области инженерии, сотрудникам правоохранительных органов необходимо обладать специальными познаниями в сфере компьютерной информации.

Целесообразным приходится организация различных конференций и круглых столов как для начинающих, так и для опытных сотрудников с целью обмена практическим опытом между отделами, а также с целью выявления и опережения новых преступных схем.

Подобные круглые столы необходимо проводить и в судебном сообществе, чтобы упорядочить судебную практику в разных районах одного субъекта, а также между субъектами государства в целом.

Устранение пробелов в законодательстве путем приведенных методов позволит устранить ошибочную квалификацию совершенных преступлений, а также систематизирует судебную практику по аналогичным делам во всей стране. Это поможет справедливо, объективно и законно назначать наказания виновным лицам, а также поможет содействию в восстановлении социальной справедливости, исправлении осуждённого и предупреждении совершения им новых преступлений.

ЗАКЛЮЧЕНИЕ

В данной научном исследовании были проанализированы преступления, связанные с использованием электронных средств платежа в Российской Федерации и в Республике Казахстан. Подвергся детальному анализу понятийный аппарат двух государств, разработанный, в том числе, для защиты общественных отношений в сфере собственности.

Так, были выявлены значительные различия в формулировках терминов. Стало понятно, что Российскому законодателю стоит обратить внимание на емкую и лаконичную формулировку терминов в Республике Казахстан в целях устранения недопонимания как со стороны представителей власти, так и со стороны обычных граждан.

На основе анализа были выявлены сходства и различия в объективных и субъективных сторонах рассматриваемых преступлений. Объективная сторона рассматриваемых в исследовании видов краж и мошенничеств характеризуется активными действиями, воздействующими либо на информационную систему (актуально для законодательства Республики Казахстан), либо на банковский счет пользователя посредством использования электронных средств платежа (актуально для законодательства Российской Федерации) и факультативными признаками, которые де-юре разнятся в России и Казахстане в связи с разным понятийным аппаратом, но де-факто представляют собой одни и те же действия лиц, направленные на хищения денежных средств с банковских карт. Стоит отметить сходства материальной конструкции объективной стороны. И в Российской Федерации, и в Республике Казахстан, такие преступления могут быть признаны оконченными только тогда, когда виновный получил реальную возможность свободно распоряжаться украденными деньгами. Если же говорить о субъективной стороне преступлений в двух странах, то требования уголовного закона обеих стран совпадает в связи с аналогичными условиями уголовной ответственности. Это должно быть вменяемое физическое лицо, достигшее возраста, установленного Уголовным кодексом: шестнадцати лет (для

мошенничеств) и четырнадцати лет (для краж), а совершаются преступления лишь с прямым умыслом и корыстной целью.

Исследование показало, что преступления, связанные с использованием электронных средств платежа, чаще совершают мужчины (67,42 %), чем женщины (32,58 %). Большинство преступников данной категории относятся к возрастной группе от 30 до 49 лет. Преступное поведение взрослых является более общественно опасным, чем у молодых преступников, так как они имеют больший жизненный опыт, сформировавший их характер и потребности [Лещенко В.П., с. 117]. В этом возрасте формируется модель криминальной активности, начатая в более юном возрасте. Большинство преступников, занимающихся незаконным использованием электронных средств платежа, имеют средний уровень образования. Отсутствие постоянного законного дохода является экономической причиной, объясняющей представленные данные. Неоспорим и тот факт, что отсутствие стабильного источника доходов способствует увеличению преступности.

В рамках исследования было детально проанализировано конкретное дело, которое ярко продемонстрировало наличие недостаточной квалификации правоохранительных органов, а также присутствие пробелов в законодательстве. В связи с выявлением проблематики были предложены эффективные пути решения для ее устранения.

В первую очередь выявлена потребность в принятии нового Постановления Пленума Верховного Суда Российской Федерации или же введение новых положений в имеющееся Постановление с целью разъяснения объема преступных деяний, связанных с хищениями, совершенных с использованием электронных средств платежа. Целью новых разъяснений должно стать разграничение и устранение такой тонкой грани между рассматриваемыми составами преступлений: кража с банковского счета, а равно в отношении электронных денежных средств и мошенничество, совершенное с использованием электронных средств платежа.

Кроме того, необходимы разъяснения, касающиеся посягательств на различные электронные бонусы, которые нельзя признать денежной единицей, но благодаря которым можно частично или полностью производить расчеты в тех или иных организациях.

Также, как уже отмечалось, российскому законодателю стоит обратить внимание на понятийный аппарат, касающийся аналогичных вопросов, Республики Казахстан. Заимствование идеи термина «информационная система» в российское законодательство позволило бы избежать ошибок в квалификации некоторых преступлений.

Наряду с указанным, прослеживается потребность и в разъяснениях, касающихся способов совершения мошенничеств, ведь спорным остается вопрос о наличии обмана или злоупотребления доверием в случае возникновения «компьютерной», системной программной ошибки. Говорить об обмане или злоупотреблении доверием в таком случае представляется ошибочным.

Все более частое использование альтернативных наличным деньгам вариантов платежных средств людьми навязывает необходимость детального изучения сущности обращения с ними. Также в связи с актуальностью использования альтернативных денежным средствам вариантов стоит повышать грамотность не только специалистов, но и обычных граждан, использующих такие методы в своих расчетах.

Не последнее место в вопросе противодействия преступлениям, совершаемым с использованием электронных средств платежа, занимает грамотно организованная система подготовки кадров правоохранительных органов. На сегодняшний день уровень подготовки лиц, непосредственно осуществляющих раскрытие и расследование рассматриваемых деяний, недостаточен, поэтому повышение их квалификации «извне» приходится уместным. Предлагается проведение конференций и круглых столов. Подобные мероприятия необходимо проводить и в судебском сообществе, чтобы упорядочить судебную практику в разных районах одного субъекта, а также между субъектами государства в целом.

Устранение пробелов в законодательстве путем приведенных методов позволит устранить ошибочную квалификацию совершенных преступлений, а также систематизирует судебную практику по аналогичным делам во всей стране. Это поможет справедливо, объективно и законно назначать наказания виновным лицам, а также поможет содействию в восстановлении социальной справедливости, исправлении осуждённого и предупреждении совершения им новых преступлений.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Нормативные правовые источники:

1. Конституция Российской Федерации от 12 декабря 1993 г.: с изменениями, одобренными в ходе общероссийского голосования 01 июля 2020 г. // Официальный интернет-портал правовой информации <http://www.pravo.gov.ru>. 2020.
2. Уголовный кодекс Российской Федерации: Федеральный закон от 13 июня 1996 г. (ред. от 01 июля 2021 г.) № 63-ФЗ // Собрание законодательства Российской Федерации. 1996. №25. Ст.2954.
3. Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V (с изменениями и дополнениями по состоянию на 20.05.2023).
4. О национальной платежной системе: Федеральный закон от 27.06.2011 года № 161-ФЗ // Собрание законодательства Российской Федерации. - 2011. - № 27. - С. 3872.
5. О внесении изменений в Уголовный кодекс Российской Федерации: Федеральный закон от 23.04.2018 года № 111-ФЗ // Собрание законодательства Российской Федерации. - 2018. - № 27. - С. 4256.
6. Гражданский кодекс Российской Федерации (часть первая): от 30.11.1994 № 51-ФЗ (ред. от 16.12.2019) // Собрание законодательства РФ. – 05.12.1994. – № 32. – Ст. 3301.
7. Закон Республики Казахстан от 26 июля 2016 года «О платежах и платежных системах» года № 11-VI ЗРК.
8. Закон Республики Казахстан от 1 декабря 2022 года «О республиканском бюджете на 2023-2025 годы» № 163-VII.
9. Закон Республики Казахстан от 24 ноября 2015 года «Об информатизации» № 418-V.

10. Указ Президента РФ от 09.05.2017 г. № 203 «О Стратегии развития информационного общества на 2017-2030 годы» // Собрание законодательства Российской Федерации. - 2017. - № 20. - Ст. 2901.
11. Указ Президента РФ от 19.12.2012 г. № 1666 «О Стратегии государственной национальной политики Российской Федерации на период до 2025 г.» // Собрание законодательства Российской Федерации. - 2012. - N 52. - Ст. 7477; СЗ РФ - № 50. - Ст. 7739.
12. Об утверждении Концепции правовой политики Республики Казахстан до 2030 года // Указ Президента Республики Казахстан от 15 октября 2021 года № 674.
13. Об утверждении Концепции кибербезопасности ("Кибершит Казахстана") // Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407
14. Об утверждении Государственной программы "Цифровой Казахстан" // Постановление Правительства Республики Казахстан от 12 декабря 2017 года № 827.
15. Послание Конституционного Совета Республики Казахстан "О состоянии конституционной законности в Республике Казахстан" (оглашено на совместном заседании Палат Парламента Республики Казахстан 21 июня 2021 года).
16. Указание Банка России от 14.09.2011 N 2694-У "О порядке уведомления Банка России оператором электронных денежных средств о начале деятельности по осуществлению перевода электронных денежных средств" (Зарегистрировано в Минюсте России 21.09.2011 N 21854).

2. Научная литература:

1. Анисимов В. Ф. Ответственность за преступления против собственности с признаками хищения: состояние, сущность и проблемы квалификации // докт. юрид. наук. — СПб. — 2007. — 381 с.;

2. Архипов А.В. Проблемы применения нормы о мошенничестве с использованием платёжных карт // Уголовное право. 2017. № 1 (январь-февраль) С. 4—11.
3. Бегишев, И. Р. Преступления в сфере обращения цифровой информации / И. Р. Бегишев, И. И. Бикеев. - Казань : Познание, 2020. - 300 с.
4. Бойцов А.И. Преступления против собственности. – СПб.: Юридический центр Пресс, 2012. – С. 773.
5. Голунский С. А., Шавер Б. М. Криминалистика. Методика расследования отдельных видов преступлений // С. А. Голунский, Б. М. Шавер. — М., 1939. — 372 с.
6. Голованова Н.А. Уголовно-юрисдикционная деятельность в условиях цифровизации : монография // Н.А. Голованова. М. : ИЗИСП, Контракт, 2019. С. 82.
7. Головин А.Ю. Проблемы и пути совершенствования методик расследования отдельных видов преступлений // Известия Тульского государственного университета. Экономические и юридические науки. 2014. № 3-2. С. 3-10.
8. Здравомыслов Б.В. Уголовное право России. Общая часть: учебник. – М.: Юрист, 2015. – С. 217.
9. Иванчина С. А. Оконченное преступление: закон, теория, практика // канд. юрид. наук. Саратов, 2012. 25 с.
10. Караваева Ю.С. «Значение социального статуса и роли личности для целей криминологического прогнозирования индивидуального преступного поведения». Вестник Саратовской государственной юридической академии 2020 (133): - С. 177-184.
11. Коростелев М.А.оборот электронных денежных средств: гражданско-правовые вопросы // Журнал российского права. 2013. № 12. С. 130135.
12. Креховец А.В., Степанова М.А., Царёв Е.В. Проблемы квалификации преступления, предусмотренного п. «г» ч. 3 ст. 158 Уголовного кодекса Российской Федерации // Вестник Российского нового университета. - 2021. - № 1. - С. 158-165.

13. Курбатов А.Я. Правовое регулирование электронных платежных систем по законодательству Российской Федерации // *Хозяйство и право*. 2007. № 9. С. 68-84.
14. Лещенко В.П. Мошенничество, совершенное с использованием средств электронного платежа в системе имущественных преступлений против собственности В.П. Лещенко // *Гуманитарные, социально-экономические и общественные науки*. 2021.
15. Лещенко В.П. Предмет Мошенничество, совершенное с использованием средств электронного платежа в системе имущественных преступлений против собственности В.П. Лещенко // *Гуманитарные, социально-экономические и общественные науки*. 2019.
16. Лихолетов А. О. Проблемы разграничения мошенничества / А. О. Лихолетов // *Российская юстиция*. — 2017. — № 6. — С. 35—37.
17. Малянова К. П. Методика расследования преступлений, связанных с незаконным образованием (созданием, реорганизацией) юридического лица: — Ростов н/Д., 2018. — С. 264.
18. Маркова, Е. А. Мошенничество с использованием электронных средств платежа: вопросы теории и практики / Е. А. Маркова // *Аграрное и земельное право*. – 2019. – № 5 (173). – С. 112–117 (1,13 п.л.).
19. Маршева, К. С. Объективные признаки мошенничества с использованием электронных средств платежа / К. С. Маршева. — Текст: непосредственный // *Молодой ученый*. — 2021. — № 50 (392). — С. 262-265.
20. Мельникова, В. Е. Объект преступления / В. Е. Мельникова // *Уголовное право России. Общая часть* / под ред. Б. В. Здравомыслова. - М. : Юрист, 1996. – С. 512.
21. Нугаева Э. Д. Особенности расследования мошенничества при оказании оккультных услуг: дис. ... канд. юрид. наук / Э. Д. Нугаева. — Уфа, 2018. — С. 269.

22. Осипова М.А. Понятие и сущность криминалистической характеристики преступлений, совершаемых в сфере банковской деятельности // Известия Иркутской государственной экономической академии. 2012. № 2. С. 39.
23. Прозументов Л.М. Криминологическая характеристика и предупреждение наркопреступности. // Томск: Издательство научно-технической литературы, 2020, С. 54.
24. Рарог А.И. Уголовное право России. Общая часть. - М.: Проспект, 2009. – С. 841.
25. Русскевич Е.А. Отграничение мошенничества с использованием электронных средств платежа (ст. 159.3 УК РФ) от смежных составов преступлений // Уголовное право. — 2019. — № 5. — С. 16—20.
26. Саблина Т. И., Никитенко И. В. Мошенничество с использованием платежных карт: вопросы теории, законодательства и практики его применения / Т. И. Саблина, И. В. Никитенко // Молодой ученый. — 2017. — № 48 (182). — С. 274—276.
27. Скляр С. В. К вопросу о конкуренции норм, предусматривающих уголовную ответственность за кражу, совершенную с банковского счета, и мошенничество с использованием электронных средств платежа / С. В. Скляр // Вестник Университета прокуратуры Российской Федерации. — 2019. — № 4 (72). — С. 17—22.
28. Скопин А. Ю. (2019). Авторская концепция и Стратегия пространственного развития России: критический анализ // Россия: тенденции и перспективы развития. №14-2, С. 14.
29. Степанов М. В. Особенности квалификации преступлений, предусмотренных ст. 159.1—159.6 УК РФ: метод. рек. // М. В. Степанов. — Н. Новгород: Нижегородская академия МВД России, 2014. — 23 с.
30. Тимошин Н. В. Новые нормы о мошенничестве в УК РФ: рекомендации по применению / Н. В. Тимошин // Уголовный процесс. — 2013. — № 1. — С. 10—15.

31. Третьякова Е.И. Новые виды мошенничества: о необходимости формирования методики расследования // Деятельность правоохранительных органов в современных условиях: Сборник материалов XXIII международной научно-практической конференции. В 2-х томах. 2018. С. 122-125.
32. Филиппов М. Н. Расследование краж и мошенничеств, совершенных с использованием банковских карт и их реквизитов : автореф. дис. // М., 2012. С. 30.
33. Ямалов А.О. Методические рекомендации о порядке действий в случае выявления хищения денежных средств в системах дистанционного банковского обслуживания, использующих электронные устройства клиента // Вестник Ассоциации российских банков. 2017. № 1. С. 22-23.
34. Яни П. С. Специальные виды мошенничества / П. С. Яни // Законность. — 2015. — № 5. — С. 42—46.

3. Материалы практики:

1. Постановление Пленума Верховного суда от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате».
2. Нормативное постановление Верховного Суда Республики Казахстан от 29.06.2017 года № 6 «О судебной практике по делам о мошенничестве».
3. Определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 29.09.2020 № 12-УДП20–5-К6.
4. Определение Конституционного Суда РФ от 9 июля 2021 г. № 1374-О «О прекращении производства по делу о проверке конституционности пункта "г" части третьей статьи 158 и статьи 159.3 Уголовного кодекса Российской Федерации в связи с запросом Железнодорожного районного суда города Рязани». – Доступ из справочно-правовой системы «КонсультантПлюс» (дата обращения 04.02.2023).

5. Дело № 1-266/2021 Сургутского городского суда Ханты-Мансийского автономного округа – Югры от 05.04.2021. – Доступ из справочно-правовой системы «КонсультантПлюс» (дата обращения 04.02.2023).
6. Приговор № 1-224/2021 1-24/2022 от 18 февраля 2022 г. по делу № 1-224/2021 Ярцевский городской суд. – Доступ из справочно-правовой системы «КонсультантПлюс» (дата обращения 04.02.2023).
7. Приговор № 1-92/2022 от 11 февраля 2022 г. по делу № 1-92/2022 Шадринский районный суд. – Доступ из справочно-правовой системы «КонсультантПлюс» (дата обращения 04.02.2023).
8. Приговор № 1-378/2020 от 8 мая 2020 г. по делу № 1-378/2020 Энгельсский районный суд. – Доступ из справочно-правовой системы «КонсультантПлюс» (дата обращения 04.02.2023).
9. Приговор № 1-3-5/2020 от 8 мая 2020 г. по делу № 1-3-5/2020 Сухиничский районный суд. – Доступ из справочно-правовой системы «КонсультантПлюс» (дата обращения 04.02.2023).
10. Приговор № 1-59/2020 от 7 мая 2020 г. по делу № 1-59/2020 Ермаковский районный суд. – Доступ из справочно-правовой системы «КонсультантПлюс» (дата обращения 04.02.2023).

4. Иные источники:

1. Информация пресс-центра Банка Русский стандарт. URL: <https://www.rsb.ru/press-center/news/2023/290323/> (дата обращения 04.02.2023).
2. Данные IT-компании Эватор, размещенные в открытом доступе. URL: <https://evotor.ru/research/k-kontsu-2022-goda-dolya-beznalichnyh-platezhej-v-malom-biznese-vyros-la-do-rekordnyh-68/> (дата обращения 04.02.2023).
3. Обзор статистики по безналичным карточным операциям за 2022 год Аналитического центра АФК. URL: <https://plusworld.ru/articles/50580/> (дата обращения 04.02.2023).

4. Официальный сайт Президента Республики Казахстан. Стратегии и программы. URL:https://www.akorda.kz/ru/official_documents/strategies_and_programs (дата обращения 04.02.2023).
5. Сайт Turan Times // Об индексе преступности в разных странах URL: <https://turantimes.kz/obschestvo/40843-v-rejtinge-stran-po-urovnju-prestupnosti-kazahstan-zanjal-48-e-mesto-iz-142.html> (дата обращения 04.02.2023).
6. Сводные статистические сведения о состоянии судимости в России за 2020 год. Судебный департамент при Верховном Суде РФ. 2020. URL: <http://www.cdep.ru/index.php?id=79&item=5669>. (дата обращения 04.02.2023).
7. Краткие Правила бонусной программы в открытом доступе. URL: <https://media.utair.ru/status> (дата обращения 04.02.2023).
8. Полные правила программы «Utair Status», URL: https://eu-s3.beelinecloud.ru/utairlog/%D0%9F%D1%80%D0%B0%D0%B2%D0%B8%D0%BB%D0%B0%20Status_2023.pdf?AWSAccessKeyId=d2149677-4252-4a8694fe434ee1b6e1e8&Signature=8ii%2BIL91MX4D568rbDBBsoNpft0%3D&Expires=4839539 (дата обращения 04.02.2023).
9. Сводные статистические сведения о состоянии судимости в России за 2020 год. Судебный департамент при Верховном Суде РФ. 2020. URL: <http://www.cdep.ru/index.php?id=79&item=5669> (дата обращения 04.02.2023).
10. Сводные статистические сведения о состоянии судимости в России за 2022 год // Судебный департамент при Верховном Суде РФ. URL: <http://www.cdep.ru/index.php?id=79&item=7069> (дата обращения 04.02.2023).