ПРОБЛЕМЫ КВАЛИФИКАЦИИ ХИЩЕНИЙ БЕЗНАЛИЧНЫХ ДЕНЕГ

А.С. Фархутдинова, *студент*
Д.В. Чукаева, *студент*
Научный руководитель: *Р.Н. Нурмухаметов, ассистент*
Уфимский университет науки и технологий
(Россия, г. Уфа)

DOI:10.24412/2500-1000-2023-12-5-120-123

Аннотация. *В статье рассматриваются проблемные аспекты привлечения к уголовной ответственности за хищение безналичных и электронных денег. Современное состояние правового регулирования защиты от подобного рода преступлений имеет ряд недостатков и требует дальнейшего совершенствования. Также отмечаются пробелы и коллизии в правоприменении, предложение решений по дальнейшему совершенствованию законодательства в данной области.*

Ключевые слова: *уголовное право, ответственность, хищение, банковские карты, безналичные денежные средства, мошенничество, квалификация.*

В современном цифровом мире хищение безналичных денег становится все более распространенным и серьезным преступлением. С развитием технологий и переходом к электронным платежам, преступники находят новые способы обманных действий, чтобы получить доступ к финансовым средствам людей и организаций.

Эта проблема имеет глобальный масштаб и требует внимания не только со стороны правоохранительных органов, но и от самих пользователей электронных платежных систем. В данной статье мы рассмотрим различные методы хищения безналичных и электронных денег, а также предложим практические рекомендации по защите своих финансовых активов от подобного рода преступлений. Данный вопрос очень актуален в современных реалиях, безналичные операции с каждым годом растут по всему миру, преступный мир в свою очередь придумывает все больше и больше методов хищения.

Методы хищения безналичных средств представляют собой разнообразные способы незаконного завладения электронными деньгами и ресурсами. Среди них можно выделить фальсификацию платежных документов, использование украденных банковских данных для совершения транзакций. Это может быть осуществлено через взлом компьютерных систем, фишинг, вредоносное программное обеспечение или другие технические устройства.

Согласно отчетам правоохранительных органов, мы видим значительный рост числа киберпреступлений в 50 раз до 510 тыс.(с 2014 г.) [1]. Киберпреступники используют различные методы для доступа к банковским аккаунтам и цифровым кошелькам, включая фишинг, вредоносное программное обеспечение (malware) и социальную инженерию.

Анализ статистики данных позволяют сделать вывод, что за последние 10 лет примерно в 7 раз увеличилось количество преступлений, совершенных с использованием платежных карт [2]. Проблематика заключается в том, что чаще всего преступник остается анонимным при совершении преступления, ему необходим лишь доступ к сети Интернет из любой точки мира. По данным Генеральной прокуратуры РФ, каждая пятая кража, совершаемая в стране, связана с хищением денежных средств с банковского счета [3].

В целях защиты безналичных денежных средств граждан (с использованием которых, по оценкам современных финансистов, в РФ совершается более 75% расходных операций [4]) Федеральным законом (далее – ФЗ) от 23.04.2018 № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» ч. 3 ст. 158 УК РФ была дополнена п. «г»: «кража, совер-

шенная с банковского счета, а равно в отношении электронных денежных средств».

Для борьбы с этой проблемой требуется постоянное обновление систем безопасности и повышение осведомленности пользователей о возможных угрозах. Организации также должны активно работать над предотвращением атак на свои платежные системы и приложения для финансовых операций. Кроме того, важно разработать механизмы защиты безналичных денежных средств от кражи. Это может включать в себя использование двухфакторной аутентификации при осуществлении электронных платежей, шифрование данных и многоуровневую систему проверки личности клиента.

На данный момент раскрываемость данных преступлений (п. «г» ч. 3 ст. 158 УК РФ) низкая (47,7%) [5], что не может не являться проблематикой в уголовном праве. Также спорная квалификация кражи с банковского счета, а равно в отношении электронных денег, совершаемой с использованием новых технологий; отграничения деяния, закрепленного в п. «г» ч. 3 ст. 158 УК РФ, от деяния, указанного в ст. 159.3 УК РФ.

В уголовном праве и правоприменительной практике возникают проблемы квалификации хищения электронных средств платежа, к числу таковых относятся сложности разграничения анализируемых деяний. В самой диспозиции п. «г» ч. 3 ст. 158 УК закреплена необходимость отграничения признаков кражи от мошенничества. Ранее в первом и втором абзацах п. 17 Постановления Пленума Верховного Суда РФ № 48 от 30.11.2017 г., содержался ряд положений, позволяющих отграничивать данные составы преступлений, однако 29 июня 2021 г. данные критерии для квалификации были исключены. Согласно исключенным положениям, мошенничеством признавался обман лишь уполномоченных сотрудников банковских, торговых, кредитных организаций, тем самым круг объекта обмана был конкретизирован, на данный момент мошенничеством признается обман не только уполномоченных сотрудников, но и других граждан.

В уголовном праве хищение безналичных денег рассматривается как преступление против собственности. Родовым объектом исследуемого состава, как и всех преступлений против собственности следует признать экономические обеспечивающие материальное благосостояние отношения, личности, общества государства. Предметом состава преступления, предусмотренная п. «г» ч. 3 ст. 158 УК РФ являются электронные денежные средства, размещенные на банковском счете. Предметом преступлений по ст. 159.3 УК РФ являются денежные средства в целом.

Главное в этом случае - это намеренное завладение чужим имуществом путем обмана или злоупотребления доверием. Важно отметить, что для квалификации деяния как хищения необходимо наличие умысла на присвоение имущества.

Необходимо разграничивать составы преступления, а именно п. «г» ч. 3 ст. 158 УК РФ от мошенничества, совершаемым с использованием электронных средств платежа (ст. 159.3 УК РФ).

Выбор способа обналичивания денег напрямую влияет на дальнейшую квалификацию преступных действий виновного лица: если в процесс вовлечен сотрудник банка, которому были сообщены ложные (или не сообщены достоверные) сведения о принадлежности банковской карты – то действия подлежат квалификации как мошенничество по ст. 159.3. УК РФ, а если снятие наличных денежных средств осуществлено виновным лицом через банкомат без участия сотрудников банка - уголовная ответственность наступает по ст. 158 УК РФ.

Данный вопрос регламентируется п. 17 Постановления Пленума Верховного Суда РФ от 30.11.2017 № 48 определяет, что преступные действия лица следует квалифицировать по ст. 159.3 Уголовного кодекса Российской Федерации, только если виновный совершил хищение посредством сообщения «заведомо ложных сведений о принадлежности указанному лицу такой карты на законных основаниях либо путем умолчания о незаконном владении им платежной картой» [6]. Можно сделать вывод о том, что основным разграничением бу-

дет являться способ совершения преступления.

При производстве следственных действий необходимо обращать внимание на то, что при допросе подозреваемого (обвиняемого) следует выяснить обстоятельства возникновения умысла на хищение денежных средств; время, характер и способ хищения; источник получения информации о состоянии их счетов, наличии средств на их банковских счетах; наличие навыков, позволяющих создавать вредоносное программное обеспечение; наличие технических средств [7].

К материалам уголовного дела следует приобщать копии документов, подтверждающих полученные сведения (распечатки sms-сообщений, сведения о движении денежных средств, чеки, подтверждающие факт оплаты за товар или услугу и т.д.).

При совершении кражи путем обмана или злоупотреблением доверием, действия будут квалифицироваться по ст. 159 УК РФ. Именно способ совершения преступления лежит в основе разграничения данных составов преступлений.

Как тайное хищение следует квалифицировать действия и тогда, когда виновным потерпевший введен в заблуждение или обманут, под воздействием чего он сам передает злоумышленнику свою карту или сообщает персональный идентификационный номер – пин-код, а снятие денег с банкомата происходит без потерпевшего.

Вместе с тем, если виновный открыто похищает непосредственно банковскую карточку, знает или при помощи применения насилия к потерпевшему узнает пин-код, такие действия, несмотря на последующее снятие денежных средств посредством банкомата в отсутствие потерпевшего, надлежит квалифицировать в зависимости от конкретных обстоятельств по ст. 161 или ст. 162 УК РФ [8].

Основными проблемами уголовной ответственности за совершение хищения с использованием банковских карт являются:

- разграничение кражи от мошенничества;

- определение предмета и средств совершенного преступления.

Таким образом, анализируя вышеизложенное, следует отметить, что ряд аспектов уголовной ответственности за кражу в отношении электронных денежных средств остается неурегулированным. Существует трудность разграничения квалификации деяний, а именно п. «г» ч. 3 ст. 158 УК РФ, со смежными составами преступления, сложность расследования и раскрытия.

Для борьбы с этими угрозами необходимо разработать единые международные стандарты по защите электронных денег и координацию усилий между различными правоохранительными органами. Также необходимо повысить осведомленность пользователей о методах предотвращения кражи безналичных и электронных денег, таких как использование надежного пароля, двухфакторной аутентификации и регулярная проверка выписок по счетам.

Библиографический список

1. Киберпреступность и киберконфликт: Россия // Портал «TAdviser», 12 октября 2022 (дата обращения: 20.11.2023).

2. Боровых Л.В. Направленность обмана в составе мошенничества с использованием платежных карт / Л.В. Боровых, Е.А. Корепанова // Вестник Пермского университета. Юридические науки. – 2016. – № 1. – С. 98-104.

3. Газета «Известия», 13 октября 2020 (дата обращения: 20.11.2023).

4. Безналичные платежи в России // Портал «TAdviser», 12 октября 2021. (дата обращения: 20.11.2023).

5. Криминогенная обстановка под контролем // Газета «Сельская новь», 26 ноября 2022 (дата обращения: 20.11.2023).

6. О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного Суда РФ от 30.11.2017 № 48. Доступ из СПС «КонсультантПлюс» (дата обращения: 20.11.2023).

7. Филимонов С.А. Проблемы борьбы с киберпреступлениями, совершаемыми с использованием банковских карт / С.А. Филимонов // Современное право. – 2015. – № 3. – С. 119-124.

8. Долгих Т.Н. Ответственность за хищение денежных средств с банковской карты // Правовой Сервер КонсультантПлюс. [Электронный ресурс] (дата обращения: 20.11.2023).

THEFT OF NON-CASH AND ELECTRONIC MONEY

A.S. Farkhutdinova, *Student*
D.V. Chukaeva, *Student*
Supervisor: *R.N. Nurmukhametov, Assistant*
Ufa University of Science and Technology
(Russia, Ufa)

Abstract. *The article discusses the problematic aspects of criminal liability for theft of non-cash and electronic money. The current state of legal regulation of protection against this type of crime has a number of shortcomings and requires further improvement. Gaps and conflicts in law enforcement are also noted, and solutions are proposed for further improvement of legislation in this area.*

Keywords: *criminal law, liability, theft, bank cards, non-cash funds, fraud, qualification.*