### МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

## «САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

# ЗАХМАТОВА МАРИЯ ВАСИЛЬЕВНА ДИСТАНЦИОННЫЕ МОШЕННИЧЕСТВА ПОД ПРЕДЛОГОМ БЛОКИРОВКИ БАНКОВСКИХ КАРТ

Направление подготовки 40.03.01 — «Юриспруденция» юридического факультета СГУ им. Н.Г.Чернышевского

Автореферат бакалаврской работы

Научный руководитель д.ю.н, профессор кафедры уголовного, экологического права и криминологии

Н.Т. Разгельдеев

Зав. кафедрой уголовного, экологического права и криминологии д.ю.н, профессор

Н.Т. Разгельдеев

Саратов 2020

### Введение

исследования. Мошенничество, Актуальность темы как ВИД преступлений, является актуальным в первую очередь из-за личности самого преступника, которого можно охарактеризовать, как хитрого человека, умеющего находить психологический контакт с потенциальной жертвой, манипулировать ею, желая добиться результата, а именно, принадлежащего потерпевшему имущества в собственность преступника. В развитием информационно-телекоммуникационных связи резким технологий, переходом товарно-денежных отношений в сеть Интернет, при котором потенциальная жертва и преступник друг друга не видят, а так же с развитием кредитно-банковской системы, в результате которой денежные средства граждан хранятся на их счетах и платежных (банковских) картах, особую актуальность, в последнее время, представляют раскрытие и расследование дистанционных мошенничеств. Как показывает практика, при совершении дистанционного мошенничества, преступник и потерпевший в большинстве своем находятся в разных регионах РФ. Как пример, житель Саратовской области на сайте «Авито» выставляет объявление о продаже Преступник, обнаружив какого-либо имущества. данное объявление, сообщает продавцу, что готов приобрести данное имущество, предлагая при этом перевести продавцу задаток, при этом выясняя номер карты, срок ее действия и иные необходимые для подключения к онлайн-банку клиента данные. После подключения к онлайн-банку, преступник дистанционно с принадлежащего ему компьютера, либо сотового телефона, похищает денежные средства потерпевшего.

Так же данная тема актуальна в силу того, что установить преступника, совершившего данное преступление, очень сложно ввиду его географической отдаленности от потерпевшего, частые смены SIM-карт и сотовых аппаратов, а так же принудительные смены IP-адреса в момент выхода в сеть Интернет, при просмотре страниц бесплатных объявлений, в том числе при хищении денежных средств с онлайн-банка клиента.

Если рассматривать личность потерпевшего, то в большинстве случаев, эти люди - социально незащищенные -пенсионеры, жители деревенских глубинок, незнакомые с банковской системой, неосведомленные о возможности дистанционного перевода денежных средств, привыкшие хранить денежные средства «по-старинке».

Сама проблема дистанционных мошенничеств возникла сравнительно недавно, приблизительно в 2008 году. За это время произошло много изменений в Уголовном Кодексе РФ, а так же выделен отдельный вид преступлений, а именно «кража, совершенная с банковского счета, а равно в отношении электронных денежных средств», предусмотренный п. «г» ч.3 ст.158 УК РФ. Неоднократно возникавшие споры о месте окончания преступления, месте возбуждения уголовного дела и предварительного расследования уголовного дела были устранены Постановлением Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 "О судебной практике по делам о мошенничестве, присвоении и растрате". 2

**Степень научной разработанности темы**. Основоположниками в изучении в изучении различных аспектов хищения, в том числе мошенничества являются такие ученые, как И.Н. Багера, Р.В. Кудрявцев, Г.А. Качмазов, Н.С. Таганцев, Н.Е. Мерецкий.

**Цель исследования** - выявление существующих проблем квалификации и расследования дистанционного мошенничества под предлогом блокировки банковских карт, а также всестороннее исследование теоретических и практических вопросов, связанных с применением действующего законодательства в области применения статьи 159.3 УК РФ.

Исходя из цели исследования и для всестороннего ее достижения, были поставлены следующие задачи:

 $<sup>^1</sup>$  Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 07.04.2020) (с изм. и доп., вступ. в силу с 12.04.2020) // Собрание законодательства РФ.1996. № 25. Ст. 2954. Статья 158. Кража

<sup>&</sup>lt;sup>2</sup> Постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 "О судебной практике по делам о мошенничестве, присвоении и растрате" [Электронный источник] / http://www.garant.ru (дата обращения 11.11.2019 г.)

- проанализировать состав преступления, предусмотренного статьей 159.3 УК РФ;
- провести сравнительный анализ составов статей 159 УК РФ и 159.3 УК РФ с целью определения причин, послуживших основанием для 21 УК РΦ дополнения главы самостоятельным составом, предусматривающим наступление уголовной ответственности за совершение мошенничества с использованием электронных средств платежа, а также установить, имеется ЛИ В действительности конкуренция общей специальной нормы;
- показать проблематику в области правоприменения статьи 159.3 УК РФ;
- рассмотреть основы методики и особенности тактики следственных действий при расследовании дистанционного мошенничества под предлогом блокировки банковских карт;
- выявить особенности проведения следственных действий и оперативно-розыскных мероприятий, вызывающих затруднения для субъектов расследования мошенничества;

**Объектом исследования** выступают общественные отношения, складывающиеся в процессе квалификации дистанционного мошенничества под предлогом блокировки банковских карт.

**Предметом исследования** выступают актуальные вопросы уголовноправовой характеристики мошенничества, правовые и криминалистические проблемы расследования дистанционного мошенничества.

Степень разработанности темы. Исследование проблематики квалификации и расследования данной категории дел носят значимый теоретический и практический характер для практики борьбы с мошенничеством под предлогом блокировки банковских карт.

**Методологической основой** дипломной работы послужили методы: логический, сравнительно-правовой, историко-правовой метод, методы системного анализа, метод теоретико-правового прогнозирования.

## Основное содержание работы

В первой главе бакалаврской работы рассматривается уголовноправовой анализ мошенничества с использованием банковских карт ст. 159.3 УК РФ.

В частности первый параграф посвящен понятиям и общей характеристике.

Вторая глава «Актуальные вопросы в определении места совершения и места предварительного расследования дистанционного мошенничества».

Третья глава «Организация раскрытия и расследования дистанционного мошенничества под предлогом блокировки банковских карт».

В четвертой главе представлены процессуальные документы уголовного дела по ст. 159.3 УК РФ.

### Заключение

Подводя итоги вышесказанного, необходимо отметить, что в настоящее время законодательство Российской Федерации в сфере раскрытия и расследования преступлений в сфере дистанционного мошенничества, да и преступлений в сфере IT-технологий требует значительных изменений.

Так необходимо внести изменения в статью 26 ФЗ № 395-1 "О банках и деятельности"<sup>1</sup>, где необходимо расширить представителей органов власти, которым бы выдавалась информация о владельце банковского счета, движении денег, а именно, закрепить данное право за сотрудниками органа дознания, в чьем производстве находится материал доследственной проверки И дознавателей ОВД, чьем производстве находится уголовное дело по делам небольшой тяжести. Необходимо на федеральном уровне устранить противоречия в уголовнопроцессуальном законодательстве, при толковании норм права расследовании и последующем направлении в суд уголовных дел по дистанционным мошенничествам и кражам денежных средств с банковских карт и счетов граждан и организаций.

<sup>&</sup>lt;sup>1</sup> См: Собрание законодательства РФ, 05.02.1996, N 6, ст. 492; 2019, N 52 (часть I), ст. 7825.

Необходимо обязать на законодательном уровне представителей операторов сотовой связи и SIP-телефонии, предоставлять услуги связи только лишь авторизированным пользователям.

Например, существует положительный опыт республики Казахстан. При покупке сотового телефона и сим-карты, собственник должен в специальной программе ввести индивидуальный номер, так называемый ИИН (индивидуальный идентификационный номер), после чего связать абонентский номер сим-карты, ІМЕІ мобильной трубки. В случае перестановки сим-карты в другой сотовый телефон, услуги предоставляться не будут. Таким образом, можно будет добиться снижения количества незарегистрированных пользователей услуг телефонной связи, сим-карты которых используют совершении при дистанционных мошенничеств.

Отдельным пунктом хотелось бы отметить совершение мошенничеств при использовании услуг IP (SIP) - телефонии. Преступления данной категории в настоящее время практически невозможно раскрыть, в силу использования преступниками подменных номеров, динамических IP-адресов, либо статических IP-адресов, которые выделяются одновременно тысячам пользователей сети Интернет. В данном случае, назрела острая необходимость обязать компании - провайдеры предоставлять IP-адреса исключительно единичным, зарегистрированным пользователям.

Таким образом, используя опыт зарубежных стран, анализируя проблемы, возникающие в процессе раскрытия и расследования уголовных дел по фактам совершенных дистанционных мошенничеств, необходимо в корне менять подход к имеющимся проблемам, не позволяющим в полной мере воспользоваться гражданам своими правами и свободами, закрепленными в Конституции Российской Федерации.