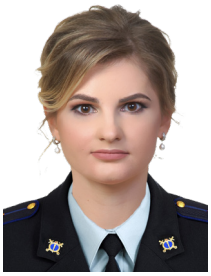
УДК 343.2



Елена Николаевна КУРИЛОВА,
старший преподаватель кафедры уголовно-правовых дисциплин Белгородского юридического института МВД России имени И.Д. Путилина,
кандидат юридических наук
Alkut_91@mail.ru

Николай Борисович КУТЕРГИН,
профессор кафедры физического воспитания и спорта Белгородского государственного технологического университета им. В.Г.Шухова,
кандидат педагогических наук, профессор
kutergin-nb@rambler.ruu

ПРОБЛЕМНЫЕ ВОПРОСЫ ПРИВЛЕЧЕНИЯ К УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА МОШЕННИЧЕСТВО В СФЕРЕ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА

PROBLEM ISSUES OF BRINING TO CRIMINAL LIABILITY FOR FRAUD IN THE FIELD OF ELECTRONIC PAYMENT

В статье рассматриваются способы совершения мошенничества с использованием электронных средств платежа. Опыт формирования уголовного законодательства в России иллюстрирует, что понимание мошенничества как уголовной категории видоизменялось не раз. Данное обстоятельство обусловило появление определенных практических и доктринальных вопросов, некоторые из которых не разрешены до сих пор. Актуальность выбранной темы исследования также усиливается вследствие недостаточной проработанности уголовно-правовых норм, регламентирующих мошенничество как форму хищения. Авторы аргументируют необходимость признания потерпевшими от такого вида преступлений кредитных организаций, а не физических лиц, от чьего имени оформлены кредитные обязательства, предлагают измененную редакцию статьи 159.3 УК РФ.

The article considers ways of committing fraud using electronic means of payment. The experience of forming criminal legislation in Russia illustrates that the understanding of fraud as a criminal category has been modified more than once. This circumstance has stipulated the emergence of certain practical and doctrinal issues, some of which have not yet been resolved. The topicality of the theme under research is strengthened in consideration of insufficient development of criminal and legal norms regulating fraud as a form of embezzlement. The authors argue the necessity to recognize credit organizations as victims of this type of crime rather than individuals on behalf of whose loan obligations are issued; the modified Article 159.3 of the Criminal Code of the RF is proposed.

Ключевые слова: мошенничество, электронные средства платежа, кредитные организации, потерпевшее лицо, хищение.

Keywords: *fraud, electronic means of payment, credit organizations, victim, embezzlement.center, suspects, accused, convicted.*

Банковская система – одна из основных звеньев финансово-кредитной составляющей Российской Федерации. Именно поэтому она является объектом, который привлекает мошенников. Этот факт подрывает авторитет банковских учреждений как финансовых посредников, гарантирующих сохранение и накопление средств клиентов: населения, государства и субъектов хозяйствования. В современном мире способы мошенничества меняются, количество схем хищения денежных средств увеличивается. Информационные технологии преобразовывают жизнь человека и в то же время модифицируют способы совершения преступлений. Банковская сфера не является исключением. Распространение информационных технологий в ней имеет как положительные (упрощение банковских операций), так и негативные последствия (распространение мошеннических действий).

Мы придерживаемся мнения, что под мошенничеством понимается введение в заблуждение (обман, ложь, обещание, данное без какого-либо намерения его выполнения, простое замалчивание, другие мошеннические меры и т.п.) и завладение через это чужим имуществом (правом на имущество). Для мошенничества основным предметом преступления выступают денежные средства.

Финансовое мошенничество накладывает отпечаток на работу банковского учреждения, что связано с возникновением угроз, рисков и др. Для банковских учреждений такое мошенничество имеет ряд негативных последствий, в том числе нарушение операционной деятельности, прямые финансовые убытки, наложение санкций, уплата штрафов, а при условии повторения – потеря банковских лицензий и банкротство. Но данный перечень не является исчерпывающим и указывает не только на финансовые потери. В то время как реальная цена [4, с. 129] вышеуказанных преступных действий – это потеря доверия клиентов и репутации, расторгнутые коммерческие предложения, потеря доли банковского рынка и перспектив. Банковские платежные системы, имеющие слабую защиту, могут терять клиентов, поскольку они могут стать объектами мошенничества. Привлечение широких слоев населения к осуществлению безналичных операций и возможность получения ими убытков превращает банковское мошенничество не только в проблему банков, но и в социальную проблему.

Безналичные платежи быстро набрали обороты [7, с. 867], что послужило развитию платежной инфраструктуры и возникновению новых видов преступлений. В связи с этим Уголовный кодекс РФ был дополнен ст. 159.3 «Мошенничество с использованием электронных средств платежа». Под электронным средством платежа понимается «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»[1].

В современной глобализированной экономике развитие системы безналичных платежей способствует увеличению объемов потребления различных финансовых продуктов. Хищения, совершаемые с использованием информационно-телекоммуникационных технологий, связываются со следующими ключевыми признаками: введение в заблуждение (обман, ложь, обещание, данное без какого-либо намерения его выполнения, простое замалчивание, другие мошеннические меры и т.п.) и завладение через это чужим имуществом (правом на имущество) с помощью информационно-телекоммуникационных технологий.

Отдельные квалифицирующие признаки мошенничества являются сквозными для всех норм уголовного законодательства Российской Федерации. Речь идет о соучастии в со-

1 О национальной платежной системе : Федеральный закон от 27.06.2011 N 161-ФЗ (ред. от 24.07.2023) (с изм. и доп., вступ. в силу с 21.10.2023), ст. 3 п. 19 // СПС «КонсультантПлюс».

вершении мошенничества, множественности совершения мошенничеств и других имущественных преступлений, общественно опасных последствиях и способах совершения мошенничеств (в том числе и с использованием электронных средств платежа). Выделяют также отдельные квалифицированные признаки мошенничества, такие как влияние на вещи первой необходимости, совершение путем подделки подписи, манипуляции с электронными документами, влияние на активы и т.п.

Операции с платежными картами являются основой функционирования мировой банковской системы, учитывая инновационную платежную функцию денег. Мошенничество как специфический вид деятельности с платежными картами имеет значительное негативное влияние на экономику любой страны мира.

Согласно статистическим данным МВД России, в 2021 году были зарегистрированы 32 627 преступлений против собственности, из них 26 396 – мошенничества, в том числе и с электронными средствами платежа, что составило около 80%. За 2022 год из 32 478 зарегистрированных преступлений против собственности мошенничества составили 27 055 преступлений[1], т.е. более 83%. Как видим, доля мошенничеств составляет подавляющее количество среди преступлений против собственности, к тому же при снижении количества зарегистрированных преступлений против собственности наблюдается рост мошенничеств.

Так, по данным судебной статистики Российской Федерации, в 2021 году по ч. 1 ст. 159.3 УК РФ были осуждены 135 лиц, по ч. 2 ст. 159 – 232, по ч. 3 ст. 159.3 – 8, по ч. 4 ст. 159.3 – 5 человек. В 2022 году по ч. 1 ст. 159.3 УК РФ были осуждены 37 лиц, по ч. 2 ст. 159.3 – 61, по ч. 3 ст. 159.3 – 14, по ч. 4 ст. 159.3 – 1 человек[2]. Количество лиц, привлеченных к уголовной ответственности, уменьшилось, однако снижения преступности не произошло.

Правоохранительные органы проводят с клиентами банков профилактические беседы о мошенничествах, банковские сотрудники предупреждают о нераспространении информации по электронным счетам в ходе телефонных разговоров, однако жертвы все равно попадают под воздействие мошенников.

Так, в сентябре 2023 г. УМВД России по г. Белгороду обратилась гражданка Б. с заявлением о том, что ей на сотовый телефон с абонентского номера оператора связи IP-телефонии звонил неизвестный, который, представившись сотрудником финансового учреждения, введя в заблуждение заявительницу, под предлогом пресечения попытки подозрительных транзакций и перевода финансовых активов на безопасный банковский счет обманным путем завладел денежными средствами в сумме 1 009 000 рублей, которые она самостоятельно перевела на счет неустановленного лица.

Платежные и банковские карты следует считать электронными платежными средствами. Определяющую роль для наличия состава преступления имеют потери материального характера, которые претерпевает собственник или держатель банковской карты.

Приведем пример мошенничества, совершенного дистанционным способом. В дежурную часть УМВД России по г. Белгороду обратился М. с заявлением о том, что в период с 10.08.2023 по 13.09.2023 неустановленные лица с использованием сети Интернет, введя в заблуждение заявителя, под предлогом получения дополнительного дохода от инвестиций на финансовой бирже «известного банка Т.» мошенническим путем завладели денежными средствами в сумме 1 292 085 рублей, которые он самостоятельно перевел на счета данным неустановленным лицам.

Наибольшее количество случаев банковских хищений, совершаемых с использованием информационно-телекоммуникационных технологий, осуществляются с использованием методов социальной инженерии, реализу-

1 Состояние преступности в России за 2021-2022 г. URL: https://xn--b1aew.xn--p1ai/dejatelnost/statistics (дата обращения: 22.11.2023).

2 Судебная статистика РФ. URL: https://stat.апи-пресс.рф/stats/ug/t/14/s/17(дата обращения: 22.11.2023).

емых среди Card-Not-Present, т.е. без наличия карты и физического присутствия пользователя. Злоумышленники получают данные банковской карты и идентификационные данные клиентов. Мошенники используют фишинг (отправка мошеннических электронных писем, предположительно исходящих от законных компаний, с целью хищения личных данных, таких как банковские реквизиты и пароли) и прекстинг, сущностью которых является «выманивание» данных платежных карт клиентов, получение доступа к счетам и хищение средств.

Необходимо отметить, что хищения с использованием электронных средств платежа – это преступления, которые в большинстве совершаются повторно, превращаются в конкретную преступную деятельность и имеют широкий круг лиц. Данные лица могут как являться участниками мошенничества, так и не осознавать, что имеют какую-либо роль в преступлении. Это связано с тем, что мошенники чаще всего не связывают себя непосредственно с деньгами, которые похищают. Эти средства на промежуточном этапе поступают на счета вышеуказанных лиц и лишь потом мошенники завладевают ими. Оказывая влияние путем обмана, преступники действуют так, чтобы лицо не отдавало себе отчета и не могло проинформировать посторонних лиц, в результате чего происходит потеря денежных средств [1, с. 136].

Хищения, совершаемые с использованием информационно-телекоммуникационных технологий, ставят актуальный вопрос установления потерпевшего по уголовным делам, где предметом хищения являются кредитные денежные средства, полученные физическими лицами путем оформления кредитов в банке. В таких преступлениях именно банк выступает жертвой мошеннических действий или инструментом в руках злоумышленников.

Так, злоумышленники звонят гражданам и под предлогом предотвращения несанкционированного доступа к банковским счетам со стороны третьих лиц, предлагают потерпевшим устанавливать на телефоны различные программы, которые предоставляют возможность удаленного управления мобильными приложениями банков, позволяющими в том числе оформлять заявки на получение кредита, в дальнейшем переводить кредитные денежные средства на различные банковские счета, к которым лица, совершающие преступление, имеют доступ.

Так, в ОП-1 УМВД России по г. Белгороду обратился Т., который пояснил, что в период с 10 час. по 12 час. неустановленное лицо, представившись сотрудником банка, под предлогом перевода денежных средств на безопасный банковский счет мошеническим путем завладело денежными средствами в сумме 721 000 рублей (кредит).

В таких ситуациях гражданин, от имени которого заключен кредитный договор, не знает о его существовании, получение заемных денежных средств и дальнейшее распоряжение ими происходит без его участия. Преступление совершается в отношении денежных средств кредитной организации, сотрудники которой введены в заблуждение относительно личности заемщика и его осведомленности о происходящем, действия мошенников направлены на хищение денежных средств кредитора [2, с. 108], а не лица, на которого оформлены кредитные обязательства, не выполняющего никаких действий по получению денежных средств и их дальнейшей передаче. На наш взгляд, в данном случае потерпевшим должна быть признана кредитная организация.

Зачастую лица, совершившие преступление, осуществляют звонки гражданам и сообщают о необходимости для сохранности денежных средств, находящихся на принадлежащих им банковских счетах, заключать кредитные договоры [3, с. 108]. Такие действия граждане выполняют как с использованием мобильных приложений банков, так и при посещении отделений банков.

Злоумышленниками добросовестные граждане вводятся в заблуждение, в момент заключения кредитного договора полагают, что действуют в целях сохранения своих денежных средств, не понимают существенные условия договора кредитования, сообщают

банковским работникам о необходимости кредитных денежных средств, фактически не нуждаясь в них. Зачастую кредитные денежные средства выдаются населению, не способному вернуть долг.

Так, в дежурную часть ОМВД по Белгородскому району обратился О. с заявлением о том, что неустановленное лицо, представляясь сотрудником финансового учреждения, под предлогом предотвращения несанкционированного списания денежных средств убедило его установить на мобильный телефон приложение «Поддержка В.», после чего через программу удаленного доступа совершило оформление кредита в сумме 2 870 000 рублей.

Изучением возбужденных уголовных дел установлено, что банками принимались решения о выдаче денежных средств по заключенным кредитным договорам, по которым сумма платежа значительно превышала ежемесячный доход клиента банка.

В связи с вышеуказанными обстоятельствами считаем, что потерпевшими в данном случае должны признаваться кредитные организации, т.к. физические лица находятся под воздействием обмана и хищение денежных средств происходит без их фактического участия.

Практика установления невозможности физическими лицами осознавать реальные последствия своих действий существует в виде проведения психолого-психиатрических экспертиз в ГСУ ГУ МВД России по г. Санкт-Петербургу и Ленинградской области, ГСУ ГУ МВД России по Кемеровской области.

Хотелось бы обратить внимание на то, что в постановлении Пленума Верховного Суда Российской Федерации «О судебной практике по делам о мошенничестве, присвоении и растрате»[1] необходимо более подробно расписать пассивный обман сотрудников торговой, кредитной или иной организации, который заключается в несанкционированном доступе злоумышленников к личным данным для оформления заявок на получение кредита, чтобы в дальнейшем переводить полученные денежные средства в пользование лиц, совершающих преступление.

В связи с изложенным считаем необходимым изложить ст. 159.3 УК РФ в следующей редакции:

«Статья 159.3 УК РФ. Мошенничество с использованием электронных средств платежа

Мошенничество с использованием электронных средств платежа, то есть хищение денежных средств путем обмана или злоупотребления доверием владельца имущества, работника торговой, кредитной или иной организации …».

Указание на хищение денежных средств путем обмана представителя организации раскрывается с позиции на кого направлено воздействие на завладение кредитными денежными средствами, полученными путем оформления кредитов в банке.

Считаем необходимым использовать положительный опыт проведения психолого-психиатрических экспертиз в территориальных подразделениях для констатирования наличия порока воли у потерпевшего физического лица при совершении юридически значимых действий, а также установления обстоятельств совершения сделок под влиянием обмана, когда граждане вслепую используются мошенниками для хищения денежных средств конкретного банка, который фактически является потерпевшим.

Исходя из вышеизложенного, считаем необходимым разъяснить в постановлении Пленума Верховного Суда Российской Федерации «О судебной практике по делам о мошенничестве, присвоении и растрате» правила квалификации мошенничеств с использованием электронных средств платежа на основании предложенной нами редакции ст. 159.3 УК РФ, что позволит разграничить конкурирующие составы преступлений, а также привлечь виновных лиц к установленной законом ответственности в зависимости от степени и характера общественной опасности деяния.

1 О судебной практике по делам о мошенничестве, присвоении и растрате : постановление Пленума Верховного Суда РФ от 30.11.2017 N 48 (ред. от 15.12.2022) // СПС «КонсультантПлюс».

Библиографический список

1. Вирясова, Н.В. Разграничение основного состава мошенничества от мошенничества при получении выплат / Н.В. Вирясова, М.М. Гурин // Развитие юридической науки и проблема преодоления пробелов в праве : сборник научных статей по итогам работы четвертого международного круглого стола. – М., 2019. – С. 135-136.

2. Гречишников, В.А. К вопросу о цене преступности. На примере мошенничества с использованием электронных средств платежа, статья 159.3 УК РФ / В.А. Гречишников // Государственная служба и кадры. – 2020. – N 1. – С. 108-110.

3. Дидидзе, М.А. Критерии разграничения мошенничества в сфере предпринимательской деятельности от иных видов мошенничества / М.А. Дидидзе // Юридическая наука: история и современность. – 2023. – N 4. – С. 106-110.

4. Каякина, Д.Н. Проблемы разграничения мошенничества при получении выплат с другими специальными составами мошенничества / Д.Н. Каякина // Юридический факт. – 2020. – N 120. – С. 127-130.

5. Клименко, А.К. Разграничение «электронной кражи» и «электронного мошенничества» между собой и «информационного мошенничества» с общеуголовными составами последних / А.К. Клименко // Право, его применение и реализация в эпоху глобальных вызовов и меняющейся реальности : материалы VI Тихоокеанского юридического форума. – Владивосток, 2021. – С. 248-252.

6. Репетий, Е.О. Способы мошенничества в интернете. методы распознавания интернет-мошенничества / Е.О. Репетий // Научный аспект. – 2023. – Т. 15. – N 4. – С. 1917-1923.

7. Степанова, К.В. О соотношении наказания за мошенничество и мошенничество в сфере компьютерной информации / К.В. Степанова, А.С. Федоров // Аллея науки. – 2018. – Т. 3. – N 6 (22). – С. 865-868.

8. Шавалеев, Б.Э. Особенности мошенничества с использованием электронных средств платежа в структуре современной российской преступности / Б.Э. Шавалеев // Ученые записки Казанского юридического института МВД России. – 2020. – N 1. – С. 36-39.