УДК 343.34 DOI 10.51980/2542-1735_2023_2_23

Ольга Владимировна ЕРМАКОВА,
профессор кафедры уголовного права
и криминологии Барнаульского
юридического института МВД России,
кандидат юридических наук, доцент
ermakova_alt@mail.ru

ВОПРОСЫ ОБОСНОВАННОСТИ ЗАКОНОДАТЕЛЬНОЙ РЕГЛАМЕНТАЦИИ ПРЕСТУПЛЕНИЙ ПРОТИВ СОБСТВЕННОСТИ, СОВЕРШАЕМЫХ В СФЕРЕ IT-ТЕХНОЛОГИЙ

ISSUES OF REASONABLENESS OF LEGISLATIVE REGULATION OF CRIMES AGAINST PROPERTY COMMITTED IN THE IT-SPHERE

В статье рассматривается законодательная регламентация преступлений против собственности, совершаемых в сфере IT-технологий. Автором детально анализируется юридическое выражение обязательных признаков составов кражи с банковского счета или в отношении электронных денег, мошенничества с использованием электронных средств платежа и мошенничества в сфере компьютерной информации. Выявленные недостатки законодательной регламентации подтверждаются анализом судебной практики. В частности, автором доказывается необходимость законодательного закрепления юридического статуса электронных денег, поскольку в правоприменительной деятельности существует проблема признания таковыми бонусов организаций, разъясняются недостатки отсутствия указания на способ совершения деяния в составе мошенничества с использованием электронных средств платежа, поскольку действующая редакция ст. 159.3 УК РФ не позволяет отграничить данное преступление от смежных. Кроме того, автором приводятся аргументы недопустимости использования в рамках состава преступления, предусмотренного ст. 159.6 УК РФ, при обозначении деяния термина «мошенничество» в связи с несоответствием сущности данного преступления общему составу мошенничества.

The legislative regulation of crimes against property committed in the IT sphere is considered in the article. The author analyzes in detail the legal expression of the mandatory elements of theft from a bank account or e-money thefts, electronic payment fraud and computer and Internet fraud. The revealed shortcomings of legislative regulation are confirmed by the analysis of judicial practice. The author proves the need for legislative consolidation of the legal status of electronic money, since in law enforcement there is a problem of recognizing organizations' bonuses as e-money. The author also explains the shortcomings of the lack of regulation of the method of committing an act as part of fraud using electronic payment instruments, since the current version of Art. 159.3 of the Criminal Code of the Russian Federation does not allow distinguishing this crime from related offenses. In addition, the author provides arguments for the inadmissibility of using the term «fraud» within corpus delicti under Art. 159.6 of the Criminal Code of the Russian Federation when designating the crime due to the discrepancy between the essence of this crime and the characteristics of fraud.

Ключевые слова: преступления против собственности, преступления в сфере IT-технологий, кража электронных денег, мошенничество с использованием электронных средств платежа, мошенничество в сфере компьютерной информации.

Keywords: *crimes against property, crimes in the IT sphere, electronic money theft, electronic payment fraud, computer fraud .*

Глобализация сети Интернет, масштабная цифровизация общества, развитие электронных систем и коммуникаций привели к появлению преступлений в сфере информационно-телекоммуникационных технологий. Так, по данным Генеральной Прокуратуры РФ, удельный вес преступлений, совершенных с применением сети Интернет, мобильной связи, расчетных карт, компьютерной техники, программных средств, в январе – ноябре 2022 г. составил 25,8%[1].

В связи с указанными особенностями УК РФ был подвержен значительным изменениям. В частности, многие основные и квалифицированные составы преступлений против собственности стали содержать указание на сферу информационных технологий. При этом законодательная регламентация данных преступлений имеет отличительные особенности, заключающиеся в том, что указание на сферу IT-технологий осуществляется опосредованно и данный вывод можно сделать только лишь путем толкования признаков составов преступлений, закрепленных в главе 21 УК РФ. Например, в составе кражи выделен квалифицирующий признак (п. «г» ч. 3 ст. 158 УК РФ) по особенностям предмета преступления, а именно электронных денег; в составе преступления, предусмотренного ст. 159.3 УК РФ, обязательным признаком выступает средство совершения преступления – электронное средство платежа; для специального вида мошенничества, закрепленного в ст. 159.6 УК РФ, принципиально важным представляется способ в виде различных операций с компьютерной информацией.

Регламентация обозначенных составов преступлений против собственности, совершаемых в сфере IT-технологий, существенно отличается, что вызывает вопросы относительно ее обоснованности, поскольку, несмотря на уникальность каждого преступления, данные разновидности относятся к группе хищений.

Решение вопросов обоснованности законодательных конструкций преступлений против собственности, совершаемых в сфере IT-технологий, имеет несомненное практическое значение, поскольку от качества нормативных предписаний зависит эффективность правоприменительной деятельности. Тем более, что выделенные для исследования составы главы 21 УК РФ вызывают множественные проблемы в квалификации и отграничении друг от друга.

Вывод об обоснованности той или иной конструкции может быть представлен только посредством детального анализа обязательных признаков каждого из обозначенных составов преступлений против собственности с выявлением проблем правоприменительной деятельности.

1. Регламентация состава кражи с банковского счета, а также электронных денежных средств (п. «г» ч. 3 ст. 158 УК РФ) и проблемы правоприменения.

Рассматриваемый квалифицированный состав выделен по особенностям предмета преступления, толкование которого представляется достаточно затруднительным. Закрепление такого вида предмета преступления предопределило изменение представления об имуществе в рамках составов хищений исключительно как физического предмета, что, по нашему мнению, является новым направлением, развивающим традиционное учение о формах и видах хищения. В научной литературе в отдельных исследованиях отождествляются электронные деньги и безналичные [3, с. 60-68]. Исходя из разъяснений, содержащихся в Памятке Банка России, электронные денежные средства – это безналичные деньги[2].

Отдельными авторами данные понятия не отождествляются. Например, А.В. Архипов разделяет понятия электронных и безналичных денежных средств [1, с. 4-9].

Поддерживая обозначенную позицию, отметим, что понятие безналичных денег в законодательстве отсутствует. Однако в соответствии со ст. 140 ГК РФ платежным сред-

1 Портал правовой статистики Генеральной Прокуратуры РФ. URL: http://crimestat.ru/analytics (дата обращения: 16.02.2023).

2 Приложение к информационному письму Банка России от 11.03.2016 N ИН-017-45/12 // СПС «КонсультантПлюс» (дата обращения: 16.02.2023).

ством на территории Российской Федерации выступает рубль. При этом платежи могут осуществляться путем наличных и безналичных расчетов. Статья 861 ГК РФ определяет порядок безналичных расчетов, осуществляемых путем перевода банком денежных средств, находящихся на счете конкретного лица. Таким образом, безналичные деньги всегда «привязаны» к счету.

Иное содержание имеют электронные деньги. В Федеральном законе от 27 июня 2011 г. N 161-ФЗ «О национальной платежной системе» под ними понимаются денежные средства, которые предварительно предоставлены одним лицом другому без открытия банковского счета. Очевидно, что в отличие от безналичных электронные деньги могут располагаться вне банковского счета в любых платежных системах.

При этом если судебная практика по безналичным денежным средствам достаточно устоявшаяся, то правовая природа электронных денег вызывает в научной литературе дискуссии. В частности, остается не ясным, следует ли относить к электронным денежным средствам криптовалюту, бонусы торговых организаций и т.д. К.А. Мира для обозначения указанных разновидностей использует термин «имущество в виде информационного объекта» [7, с. 170-176].

Даже в тех немногочисленных приговорах, где имеется упоминание про данные виды предмета, они таковыми не признаются. Например, А., работая на АЗС в качестве оператора, зная о проведении акции «Топливо за бонусы», путем обмана зарегистрировала на вымышленных лиц карты лояльности и начисляла при оплате клиентами на них бонусы, которые впоследствии применяла при расчете за топливо. Судом в приговоре в качестве предмета хищения признано топливо[1].

Полагаем, решение обозначенной проблемы возможно только путем внесения изменений в российское законодательство и определения статуса электронных денег [подр.: 5, с. 128-131].

Не отличается единообразием размер электронных денег, необходимый для привлечения виновного к уголовной ответственности [6, с. 38-42]. Исходя из предписания, закрепленного в ст. 7. 27 КоАП РФ, наличие квалифицированного состава нивелирует значение размера похищенного предмета. Однако во многих регионах Российской Федерации отказывают в возбуждении уголовного дела, если денежная сумма менее 500, 1000 рублей и т.д., применяя нормы о малозначительности деяния.

В отдельных случаях судом вообще не усматривается наличие электронных денежных средств. В частности, такая ситуация имеет место при снятии по чужой карте денег посредством банкомата.

Например, Ю., зная пин-код от банковской карты Ш., снял посредством банкомата 5000 рублей. По мнению Судебной коллегии по уголовным делам Красноярского краевого суда, квалификация по п. «г» ч. 3 ст. 158 УК РФ проведена неверно, поскольку данный признак имеется только при хищении в рамках формы безналичных расчетов[2].

Полагаем ограничение действия п. «г» ч. 3 ст. 158 УК РФ исключительно сферой безналичных расчетов и переводов денежных средств виновным по своему усмотрению не соответствует целям введения данного квалифицированного состава, в связи с чем предлагаем осуществлять квалификацию по данному квалифицирующему признаку как в случаях безналичных расчетов, так и при использовании банковской карты, не принадлежащей виновному.

Однако с целью разрешения вопросов соответствия этого предложения нормам уголовного закона полагаем необходимым дополнить содержание квалифицированного состава, закрепленного в п. «г» ч. 3 ст. 158 УК РФ, указанием на альтернативный спо-

1 Приговор Котовского городского суда Тамбовской области от от 29.06.2015 N 1-47/2015.. URL: https://sudact.ru/regular/doc/GNUZ0dhTlGLT/ (дата обращения: 16.02.2023).

2 Апелляционное определение Красноярского краевого суда от 18.12.2018 по делу N 22-7584/2018 // Сайт Красноярского краевого суда. URL: https://kraevoy--krk.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=7998836&delo_id=4&new=4&text_number=1 (дата обращения: 16.02.2023).

соб в виде использования электронного средства платежа, под которым следует понимать электронные кошельки и предоплаченные банковские карты, предназначенные для перевода электронных денежных средств.

Обязательным признаком кражи электронных денег выступает способ, т.е. тайность изъятия и обращения данного предмета. Анализ судебной практики позволяет выделить типичные ситуации тайного хищения, позволяющие унифицировать судебную практику по применению п. «г» ч. 3 ст. 158 УК РФ:

1 ситуация – виновное лицо осуществляет перевод денежных средств безналичным способом с использованием необходимой информации держателя карты. При этом данная информация могла быть известна ему заранее либо получена любым способом от самого потерпевшего;

2 ситуация – оплата покупки чужой картой при отсутствии обмана. Виновный может найти банковскую карту, а может похитить ее у собственника;

3 ситуация – хищение посредством мобильного банка, когда потерпевший, подключая услугу, неверно сообщил номер телефона, присоединив, принадлежащую ему банковскую карту к чужому номеру. В свою очередь, виновный, воспользовавшись этим, перевел денежные средства с расчетного счета потерпевшего [подр.: 8, с. 12].

При этом ранее судебная практика квалифицировала подобные случаи хищения с использованием мобильного банка либо приложения «Сбербанк онлайн» как мошенничество в сфере компьютерной информации, объясняя данное решение наличием способа в виде ввода, иного вмешательства в средства хранения, обработки компьютерной информации.

Так, Ч. в отделении «Сбербанка» нашел в мусорном контейнере чек, содержащий конфиденциальную компьютерную информацию, а именно логин и пароль для входа в «Сбербанк онлайн» на имя ранее ему незнакомого К. Реализуя свой преступный умысел на хищение чужого имущества путем вмешательства в средства хранения компьютерной информации, Ч. осуществил перевод денежных средств[1].

Полагаем, изменение в судебной практике квалификации таких действий и вменение не ст. 159.6, а п. «г» ч. 3 ст. 158 УК РФ абсолютно обоснованно, поскольку все перечисленные частные случаи объединяет тайный способ изъятия, что полностью соответствует составу кражи.

Нельзя не обратить внимание на то, что постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. N 48 конкретизировало момент окончания данного преступления. Так, если предметом являются электронные денежные средства, то хищение признается оконченным с момента изъятия денег с банковского счета. Такие разъяснения были внесены в обозначенный документ только 29 июня 2021 г., а до этого момента для признания кражи электронных денег оконченной требовалось получение виновным этих денег в свое обладание, т.е. приобретение возможности пользоваться или распоряжаться похищенным.

Учитывая, что перевод денег может в отдельных случаях осуществляться длительный период, задержание виновного до момента завершения операции подлежало квалификации как покушение со ссылкой на ч. 3 ст. 30 УК РФ с ограничением, соответственно, наказания – санкции статьи. Полагаем, такое решение не соответствует конструкции состава хищения (примечание 1 к ст. 158 УК РФ), поскольку момент окончания по прямому указанию закона должен связываться с причинением имущественного ущерба собственнику, который наступает в момент снятия денег у него со счета. В свою очередь, факт зачисления их на счет виновного для потерпевшего в принципе безразличен. Поэтому изменение разъяснений Верховным Судом РФ момента окончания хищения применительно к особому предмету в виде электронных денег следует признать обоснованным и правильным.

1 URL: https://rospravosudie.com/court-sudebnyj-uchastok-88-samarskoj-oblasti-s/act-239015612 (дата обращения: 08.04.2022).

При разъяснении вопросов квалификации нельзя не акцентировать внимание на проблеме отграничения единичного продолжаемого хищения и совокупности преступлений. Так, на практике вызывает вопросы квалификация действий при совершении покупок по одной и той же похищенной или найденной карте.

Полагаем, что в первую очередь необходимо установить наличие единого умысла на совершение тождественных действий. Только тогда возможно утверждать о продолжаемом преступлении. Например, такая ситуация имеется в случае, если виновный сообщает о желании потратить все средства на полученной банковской карте. Если же умысел конкретизированный, направлен на хищение определенной суммы, а повторный факт совершается с вновь возникшим умыслом, то налицо совокупность преступлений (к примеру, лицо похищает карту только для расчета за проезд и долгое время не пользуется ею).

2. Регламентация мошенничества с использованием электронных средств платежа (ст. 159.3 УК РФ)

Среди всех специальных составов мошенничества разновидность, закрепленная в ст. 159.3 УК РФ, выступает наиболее сложной для толкования и правоприменения. Это объясняется тем, что диспозиция ч. 1 ст. 159.3 УК РФ лишь называет деяние, не отражая признаки, ему присущие.

При этом в первоначальной редакции 2012 г. данная диспозиция содержала указание на способ – обман уполномоченного работника кредитной, торговой, иной организации. Исключение в последующей редакции из диспозиции способа совершения преступления дестабилизировало судебную практику, а после введения квалифицирующего признака, предусмотренного п. «г» ч.3 ст. 158 УК РФ, вообще привело к неприменению ст. 159.3 УК РФ.

В отдельных случаях суды переквалифицировали действия лица с квалифицированного состава кражи (п. «г» ч.3 ст. 158 УК РФ) на мошенничество с использованием электронных средств платежа (ст. 159.3 УК РФ) и в силу недостаточности имущественного ущерба (менее 2500 рублей) выносили оправдательные приговоры[1].

Безусловно, сложившаяся проблема в уяснении правоприменителями признаков состава преступления, предусмотренного ст. 159.3 УК РФ, требует устранения в части совершенствования законодательного материала. Представленная регламентация обязательных признаков не пригодна для эффективного применения уголовно-правового запрета.

По справедливому замечанию А.В. Архипова, «ст. 159.3 УК РФ не была исключена из УК РФ, а значит, имеются все основания полагать, что действия, составлявшие объективную сторону рассматриваемого преступления при предыдущей редакции ст. 159.3 УК РФ, по-прежнему должны квалифицироваться по данной норме» [2, с. 16-20].

При разграничении составов преступлений, предусмотренных ст. 158 и 159.3 УК РФ, необходимо исходить из особенностей способа совершения хищения. Так, для мошенничества характерны такие способы, как обман или злоупотребление доверием, в соответствии с которыми виновный сообщает заведомо ложные сведения или умалчивает о них либо использует особые доверительные отношения при совершении преступления.

При отсутствии обмана или злоупотребления доверием действия виновного следует квалифицировать по п. «г» ч.3 ст. 158 УК РФ.

Например, такая квалификация должна иметь место при хищении посредством мобильного банка, когда потерпевший, подключая услугу, неверно сообщил номер телефона, присоединив принадлежащую ему банковскую карту к чужому номеру. В свою очередь, виновный, воспользовавшись этим, перевел денежные средства с расчетного счета потерпевшего.

Однако судебная практика не всегда руководствуется такими правилами. Так, по

1 URL: https://www.advgazeta.ru/novosti/opravdatelnyy-prigovor-grazhdaninu-oplativshemu-pokupki-chuzhoy-bankovskoy-kartoy-ustoyal-v-apellyatsii/ (дата обращения: 16.02.2023).

приговору Братского городского суда Иркутской области А. был признан виновным в совершении деяния, предусмотренного ч. 2 ст. 159.3 УК РФ. Согласно материалам уголовного дела А., нашедший на барной стойке чужую банковскую карту, оплачивал с ее помощью товары и услуги в нескольких магазинах[1].

Поскольку уголовная ответственность за рассматриваемый специальный вид мошенничества предусмотрена в самостоятельной статье УК РФ, а регламентация иных видов мошенничества всегда сопровождается указанием на обязательный способ совершения преступления, имеющий некие особенности в сравнении с обманом или злоупотреблением доверием, характерным для общего состава мошенничества, законодателю следует отразить особенности способа совершения преступления в диспозиции ст. 159.3 УК РФ. В этой части более рационально обратиться к предыдущей редакции рассматриваемой статьи, конкретизирующей способ совершения преступления.

3. Регламентация мошенничества в сфере компьютерной информации (ст. 159.6 УК РФ).

В отличие от всех специальных видов мошенничества данный состав содержит такой способ, как ввод, удаление, блокирование, модификацию компьютерной информации, иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Очевидно, что указанный способ не имеет никакого отношения к обману или злоупотреблению доверием, в связи с чем в научной литературе отмечается нелогичность отнесения данного преступления к разряду мошенничеств и предлагается изменить название статьи [4, с. 112-117].

Полагаем, предложенная законодателем регламентация мошенничества в сфере компьютерной информации необоснованна по следующим причинам: во-первых, для любого мошенничества особенностью, отражающей сущностную характеристику преступления, является способ в виде обмана или злоупотребления доверием. При несвойственности тому или иному деянию такого способа неверно признавать деяние мошенничеством. Учитывая, что при совершении манипуляций с компьютерной информацией, в результате которых осуществляется хищение чужого имущества, обман или злоупотребление доверием не используются, данное преступление нельзя признать мошенничеством. Во-вторых, предложенные в законе способы совершения преступления, предусмотренного ст. 159.6 УК РФ, также вызывают вопросы относительно обоснованности своего введения, поскольку в составе неправомерного доступа к компьютерной информации фактически аналогичные понятия употреблены законодателем для обозначения преступных последствий, что создает проблемы в отграничении указанных составов преступлений и нарушает единство предписаний уголовного закона. К тому же в отдельных случаях законодатель подменяет один термин синонимичным. Например, в диспозиции ст. 159.6 УК РФ употребляется термин «удаление», а в ст. 272 УК РФ – «уничтожение». Возникает вопрос о содержательной составляющей данных понятий и их соотношении между собой.

Достаточно спорным видится включение в перечень способов мошенничества в сфере компьютерной информации такого способа, как ввод, поскольку представляет собой любое размещение сведений для хранения и обработки информации. Иначе говоря, даже набор текста на телефоне уже образует ввод. Соответственно, способ в виде ввода не является отличительным и типичным для состава преступления, предусмотренного ст. 159.6 УК РФ. Возможность его применения в различных преступлениях (краже, мошенничестве) не позволяет провести отграничение мошенничества в сфере компьютерной информации от иных деяний.

Таким образом, закрепление в нормах, предусматривающих ответственность за преступления против собственности, отдельных

1 Приговор Братского городского суда Иркутской области от 09.06.2020 по делу N 1-196/2020. URL: https://bsr.sudrf.ru/bigs/portal.htm (дата обращения: 16.02.2023).

видов в сфере IT-технологий обеспечивает уголовно-правовую охрану новых экономических отношений. Регламентация данных составов требует совершенствования в следующих аспектах: определение статуса электронных денег, изменение юридического выражения способов совершения мошенничества с использованием электронных средств платежа и в сфере компьютерной информации. Предложенные трансформации указанных признаков позволят решить существующие вопросы квалификации преступлений, совершаемых с использованием информационно-телекоммуникационных технологий.

Библиографический список

1. Архипов, А.В. Ответственность за хищение безналичных и электронных денежных средств: новеллы законодательства / А.В. Архипов // Уголовное право. – 2018. – N 3. – С. 4-9.
2. Архипов, А.В. Мошенничество с использованием электронных средств платежа (ст. 159.3 УК РФ) / А.В. Архипов // Уголовное право. – 2019. – N 5. – С. 16-20.
3. Байбарин, А.А. Кража безналичных и электронных денег: об актуальных проблемах правоприменения / А.А. Байбарин, Д.Н. Садчикова // Вестник Сургутского государственного университета. – 2022. – N 1 (35). – С. 60-68.
4. Бегишев, И.Р. Некоторые вопросы противодействия мошенничеству в сфере компьютерной информации / И.Р. Бегишев // Вестник Казанского юридического института МВД России. – 2016. – N 3. – С. 112-117.
5. Ермакова, О.В. Мошенничество с использованием электронных средств платежа: вопросы толкования и разграничения со смежными составами / О.В. Ермакова // Актуальные проблемы уголовного законодательства на современном этапе : сборник научных трудов международной научно-практической конференции, Волгоград, 17 мая 2019 г. / редкол.: В.И. Третьяков, В.В. Намнясева, В.А. Канубриков [и др.]. – Волгоград: Тип. ИП «Слободчикова А. Д.», 2019. – С. 128-131.
6. Клименко, А.К. Хищения безналичных и электронных денежных средств: вопросы квалификации / А.К. Клименко // Российский следователь. – 2020. – N 5. – С. 38-42.
7. Мира, К.А. Имущество в виде информационного объекта, имеющего денежный эквивалент, как предмет хищения чужого имущества / К.А. Мира // Вестник Университета им. О.Е. Кутафина (МГЮА). – 2021. – N 2. – С. 170-176.
8. Проблемы квалификации отдельных видов преступлений : учебное пособие / О.В. Ермакова, И.В. Ботвин, Л.Я. Тарасова [и др.]. Барнаул: БЮИ МВД России, 2021. – 64 с.