

ИВАНОВА Л.В.,
кандидат юридических наук, доцент,
ivanova_liliya@mail.ru
Кафедра уголовного права и процесса;
Тюменский государственный университет,
625000, г. Тюмень, ул. Ленина, 38

IVANOVA L.V.,
Candidate of Legal Sciences,
associate professor,
ivanova_liliya@mail.ru
Chair of criminal law and procedure;
Tyumen State University,
Lenina St. 38, Tyumen, 625000,
Russian Federation

ХИЩЕНИЕ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ: ПРОБЛЕМЫ КВАЛИФИКАЦИИ

Аннотация. В статье анализируются проблемы уголовно-правовой оценки неправомерного завладения чужими безналичными и электронными денежными средствами, ответственность за которое в настоящее время предусмотрена несколькими нормами уголовного закона. Выделены типичные ситуации хищения таких средств, в рамках которых рассматриваются проблемы и ошибки, возникающие при квалификации содеянного. Сохраняющаяся неточность в понимании признаков составов преступлений, предусматривающих ответственность за разные формы хищения безналичных, электронных денежных средств, порождает неверную квалификацию деяний, что свидетельствует о необходимости дальнейшего совершенствования уголовно-правовых норм. Автор обосновывает необходимость исключения из Уголовного кодекса Российской Федерации пункта «г» части 3 статьи 158, статьи 159.3 и статьи 159.6 с одновременным введением самостоятельного состава преступления «Хищение с использованием информационных технологий», охватывающего все формы хищения, совершаемого определенным способом. При этом дифференциация ответственности должна проводиться в зависимости от размера похищенных средств.

Ключевые слова: хищение; электронные денежные средства; информационные технологии; компьютерное мошенничество; квалификация преступлений.

USING INFORMATION TECHNOLOGIES TO COMMIT THEFT: PROBLEMS CONCERNING THE QUALIFICATION

Annotation. The problems concerning the criminal legal assessment of illegal acquisition of other people's non-cash and electronic funds, responsibility for which is currently provided by several criminal law norms, are analyzed in the article. Typical situations of the theft of such funds are distinguished. Within the framework of such situations the problems and errors that arise when qualifying the offence are considered. The continuing inaccuracy in understanding the peculiarities of the elements of crimes that provide the responsibility for various forms of theft of non-cash and electronic funds leads to the incorrect qualification of the act, which indicates the need for further improvement of criminal law norms. The author substantiates the need to exclude the paragraph "g" of part 3 of Article 158, Article 159.3 and Article 159.6 of the Criminal Code of the Russian Federation and, simultaneously, to introduce a separate category of crime "Using information technologies to commit theft", covering all forms of theft committed in a certain way. In this case, the differentiation of responsibility should be carried out depending on the amount of the stolen funds.

Keywords: theft; electronic cash; information technology; computer fraud; qualification of crimes.

Цифровизация практически всех сфер жизнедеятельности, несмотря на положительные моменты ее применения, такие как облегчение и ускорение решения повседневных бытовых и профессиональных задач, вызывает и негативные последствия в части использования цифрового пространства для совершения преступления, что способствует более быстрому достижению преступной цели, широкому охвату круга потенциальных потерпевших.

Данные официальной статистики показывают неуклонный рост преступлений, которые совершаются с использованием информационных технологий. Например, в 2019 году было зарегистрировано 294 409 преступлений, совершаемых с использованием компьютерных и телекоммуникационных технологий, — на 68,5 % больше, чем в 2018 году (174 674 преступления), что, в свою очередь, на 92,8 % больше показателей 2017 года, в котором было зарегистри-

ровано всего 90 587 таких преступлений*. Важно отметить, что в статистических данных МВД России показатели преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий, получили отражение лишь с 2017 года, ранее фиксировались данные только о преступлениях в сфере компьютерной информации. При этом в УК РФ перечень преступлений, совершаемых с использованием информационных технологий, с 2016 года значительно расширился**.

Использование информационных технологий возможно при совершении многих преступлений, посягающих на отношения собственности, безопасность личности, общества и государства, что в соответствии с УК РФ выступает либо конструктивным, либо квалифицирующим признаком (в частности, «использование электронных или информационно-телекоммуникационных сетей») состава преступле-

* Состояние преступности в России за январь — декабрь 2019 года; Состояние преступности за январь — декабрь 2018 года; Состояние преступности за январь — декабрь 2017 года // МВД России: официальный сайт. URL: <https://мвд.рф>

** О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности: федер. закон от 6 июля 2016 г. N 375-ФЗ; О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в части установления дополнительных механизмов противодействия деятельности, направленной на побуждение детей к суицидальному поведению: федер. закон от 7 июня 2017 г. N 120-ФЗ; О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»: федер. закон от 26 июля 2017 г. N 194-ФЗ; О внесении изменений в Уголовный кодекс Российской Федерации: федер. закон от 23 апр. 2018 г. N 111-ФЗ; О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации: федер. закон от 27 июня 2018 г. N 157-ФЗ // Официальный интернет-портал правовой информации. URL: <http://www.pravo.gov.ru>

ния. Признавая целесообразность дифференциации уголовной ответственности при совершении преступления с использованием информационных технологий, отметим, что введение соответствующего признака в смежные составы преступлений может повлечь сложности в правоприменительной практике при разграничении схожих составов преступлений.

В частности, уголовная ответственность за хищение с использованием информационных технологий в настоящее время предусмотрена тремя статьями: п. «г» ч. 3 ст. 158 УК РФ содержит особо квалифицированный состав — кража с банковского счета, а равно в отношении электронных денежных средств, ст. 159.3 УК РФ устанавливает ответственность за мошенничество с использованием электронных средств платежа. До внесения в 2018 году изменений в УК РФ*** диспозиция ст. 159.3 УК РФ имела иную формулировку: совершение деяния связывалось с обманом работника кредитной, торговой или иной организации, а предметом преступления выступала только платежная карта. Федеральным законом от 23 апреля 2018 г. N 111-ФЗ был введен новый квалифицирующий признак кражи и изменена ст. 159.3 УК РФ, а ст. 159.6 УК РФ «Мошенничество в сфере компьютерной информации» была дополнена новым квалифицирующим признаком, аналогичным названному новому квалифицирующему признаку в составе кражи.

В связи с этим возникает закономерный вопрос о соотношении и разграничении данных составов преступлений.

Кража с банковского счета, электронных денежных средств и мошенничество с использованием электронных средств платежа являются формами хищения (тайное хищение и хищение посредством обмана или злоупотребления доверием), их объединяет одинаковый родовой, видовой и непосредственный объект преступления, субъективная сторона, представленная прямым умыслом и корыстной целью, а также отмечается схожесть в предмете преступления [1, с. 26].

*** О внесении изменений в Уголовный кодекс Российской Федерации: федер. закон от 23 апр. 2018 г. N 111-ФЗ // Там же.

Категории «электронные денежные средства», «электронные средства платежа» подробно и довольно сложно раскрываются в Федеральном законе от 27 июня 2011 г. N 161-ФЗ «О национальной платежной системе»*. Иначе говоря, электронные денежные средства — это безналичные денежные средства, учитываемые кредитными организациями без открытия банковского счета и переводимые с использованием электронных средств платежа**.

К электронным средствам платежа, с помощью которых переводятся электронные денежные средства, относятся электронные кошельки, доступ к которым осуществляется с использованием компьютеров, мобильных устройств, в том числе посредством специального программного обеспечения, а также банковские предоплаченные карты — платежные карты, которые предоставляются клиенту оператором электронных денежных средств и используются для перевода электронных денежных средств и иных операций.

Таким образом, электронные денежные средства представляют собой разновидность безналичных денежных средств, но последние привязаны к конкретному банковскому счету, а электронные денежные средства — нет. При этом перечисление электронных денежных средств возможно лишь посредством электронных средств платежа, а операции с безналичными денежными средствами могут совершаться как с использованием таких способов, так и без них (например, посредством личного обращения в кредитную организацию).

Основное различие названных преступлений проводится по способу совершения преступления. Кража предполагает тайный способ хищения. Мошенничество — обман или злоупотребление доверием.

* О национальной платежной системе: федер. закон от 27 июня 2011 г. N 161-ФЗ: ред. от 2 авг. 2019 г. // Собр. законодательства Рос. Федерации. 2011. N 27. Ст. 3872; Официальный интернет-портал правовой информации. URL: <http://www.pravo.gov.ru>

** Информационное письмо Банка России от 11 марта 2016 г. N ИН-017-45/12 «О предоставлении клиентам — физическим лицам информации об особенностях оказания услуг по переводу электронных денежных средств» // Вестник Банка России. 2016. N 27.

Учитывая разъяснения Пленума Верховного Суда Российской Федерации***, ст. 159.6 УК РФ применяется в случае целенаправленного воздействия программных или программно-аппаратных средств на серверы, средства вычислительной техники (компьютеры) или на информационно-телекоммуникационные сети, нарушающего установленный процесс обработки, хранения, передачи компьютерной информации, то есть если имеет место противоправное вмешательство со стороны виновного в работу информационных систем и сетей, что способствует хищению безналичных денежных средств. Но если речь идет о техническом воздействии, то в данном случае не происходит обман или злоупотребление доверием.

Мошенничество традиционно рассматривается как форма хищения, отличающаяся способом его совершения в виде обмана или злоупотребления доверием. Однако в данном случае происходит «обман машины». А по смыслу общей нормы ст. 159 УК РФ мошенничество представляет собой обман, который может быть реализован только при непосредственном взаимодействии двух людей [2, с. 42], что не позволяет говорить о мошенничестве в чистом виде применительно к ст. 159.6 УК РФ. Снятие денег по чужой карте в банкомате также будет образовывать состав кражи, в то время как предъявление такой карты сотруднику банка или торговой организации и распоряжение таким образом чужими денежными средствами расценивается как мошенничество. При этом суды квалифицируют по ст. 159.6 УК РФ любые деяния, по своим признакам больше подпадающие под кражу или присвоение (например, бухгалтер совершает хищение денежных средств посредством отправления подложного платежного поручения, используя сервисы интернет-банка), если способ их совершения связан с использованием компьютерной информации, либо в качестве технических средств совершения преступления использованы компьютерные технологии [3, с. 23].

*** О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного Суда Российской Федерации от 30 нояб. 2017 г. N 48 // Рос. газ. 2017. N 280.

Действующая редакция ст. 159.3 УК РФ расширяет предмет преступления, так как категория «электронные средства платежа» включает не только платежные карты, и это законодательное нововведение заслуживает положительной оценки. Развитие технологий безналичных расчетов позволяет использовать, помимо карты, и иные устройства, которых со временем будет становиться больше [4, с. 7].

Для рассмотрения особенностей и проблем квалификации хищений посредством высоких технологий считаем возможным выделить несколько типичных ситуаций такого неправомерного завладения чужими средствами.

Во-первых, виновный использует поддельную или принадлежащую другому лицу банковскую карту и, сообщая ложные сведения (либо умалчивая о незаконном владении картой) сотруднику кредитной, торговой или иной организации, завладевает чужими денежными средствами. Как показывает анализ судебной практики, в основном это случаи использования чужой банковской карты для оплаты товаров в магазинах, что квалифицируется по ст. 159.3 УК РФ, как и до изменения данной нормы*. Бесспорно, платежная карта также является электронным средством платежа, тем более что сейчас возможна функция бесконтактного платежа. А использование электронных средств платежа как раз и предполагает бесконтактную форму взаимодействия клиента и оператора электронного средства платежа. Однако, как справедливо отмечает П.С. Яни, иногда суды квалифицируют подобные ситуации по п. «г» ч. 3 ст. 158 УК РФ, обосновывая такое решение тем, что работник торговой организации не осознает незаконности изъятия имущества и обмана, так как не знает истинного владельца банковской

карты. При предъявлении банковской карты сотруднику торговой организации без документа, удостоверяющего личность, владелец карты не обманывает сотрудника и не вводит его в заблуждение, хотя и умалчивает о своей личности [5, с. 34].

Во-вторых, виновный использует поддельную или принадлежащую другому лицу платежную карту и получает в распоряжение чужие средства, сняв их в банкомате. Такие случаи традиционно квалифицируются как кража. В настоящее время необходимо вменять квалифицирующий признак «с банковского счета, а равно в отношении электронных денежных средств». При этом тайное хищение безналичных и электронных денежных средств приравнивается к краже в крупном размере, исходя из санкции ч. 3 ст. 158 УК РФ, хотя хищение и наличных, и безналичных, и электронных денежных средств по характеру и степени общественной опасности одинаково [4, с. 6]. В результате внесенных в 2018 году изменений произошло уравнивание максимального наказания за кражу с банковского счета, а также в отношении электронных средств платежа и за компьютерное мошенничество в отношении аналогичного квалифицирующего признака. Однако мошенничество с использованием электронных средств платежа дифференцируется и в зависимости от размера похищенного. И если по п. «г» ч. 3 ст. 158 УК РФ максимальное наказание в виде лишения свободы составляет 6 лет, то по ч. 1 ст. 159.3 УК РФ — всего 3 года, что представляется несправедливым при тайном хищении сумм менее крупного размера. Кроме того, банкомат также можно рассматривать как электронное средство платежа, поскольку он предоставляет возможность дистанционной выдачи распоряжения оператору по переводу денежных средств [6, с. 25].

В-третьих, лицо обманным или иным путем завладевает личными данными держателя карты (номер карты, код ее верификации, логин, пароль и т.п.) и получает доступ к безналичным средствам потерпевшего. Верховный Суд Российской Федерации предлагает такие случаи также квалифицировать как кражу. Однако с введением п. «г» ч. 3 ст. 158 УК РФ возникает вопрос о необходимости вменения данно-

* См., например: Приговор Череповецкого городского суда N 1-344/2019 от 16 апр. 2019 г. по делу N 1-344/2019; постановление Президиума Верховного Суда Республики Татарстан по делу N 44у-99 от 22 мая 2019 г.; постановление Югорского районного суда N 1-41/2019 от 29 апр. 2019 г. по делу N 1-41/2019; приговор Промышленного районного суда г. Ставрополя N 1-704/2019 от 29 апр. 2019 г. по делу N 1-704/2019 // Судебные и нормативные акты Российской Федерации: сайт. URL: <http://sudact.ru>

го признака в подобных ситуациях. Иногда в судебной практике имеют место ошибки при квалификации подобных деяний.

Например, Енисейский районный суд Красноярского края переквалифицировал с п. «г» ч. 3 ст. 158 УК РФ на п. «в» ч. 2 ст. 158 УК РФ действия Б., который перевел денежные средства при помощи услуги «Сбербанк Онлайн» с банковского счета потерпевшего на банковский счет продавца криптовалюты, оплатив приобретение биткоинов, поступивших на электронный кошелек Б.* При этом в обоснование своего решения суд указал на отсутствие незаконного воздействия на банковский счет потерпевшего, в связи с чем содеянное не может квалифицироваться как кража с банковского счета. Представляется, что в данном случае произошло неправомерное смешение в обосновании разграничения кражи и мошенничества в сфере компьютерной информации. Как правильно отмечается, имеющаяся в законе оговорка «при отсутствии признаков преступления, предусмотренного ст. 159.3» как раз и свидетельствует о том, что неправомерный доступ к счету получен и осуществлен без применения специальных информационных технологий [7, с. 46].

Кроме того, не всякое завладение чужими средствами, совершенное с использованием учетных данных, можно квалифицировать как кражу. Если распоряжение на списание денежных средств было отправлено в присутствии третьих лиц, осознававших противоправный характер совершаемой операции, или если возможность пользования телефоном потерпевшего возникла во время нападения с целью хищения и манипуляции с мобильным банком были осуществлены непосредственно в процессе нападения, то содеянное должно квалифицироваться соответственно как грабеж или разбой [8, с. 124-125].

В-четвертых, виновный обманным путем воспользовался телефоном или иным устройством потерпевшего, подключенного к электронному банку, и осуществил перевод денежных средств на свою карту.

Согласно позиции Верховного Суда Российской Федерации такие ситуации также образуют состав кражи, несмотря на то, что владелец соответствующего устройства был введен в заблуждение. Критерием для разграничения мошенничества в сфере компьютерной информации и «компьютерной кражи» является использование или неиспользование виновным такого способа хищения, который можно охарактеризовать как «компьютерный взлом» [9, с. 20].

В-пятых, возможно использование специальных программ, позволяющих незаконно подключаться к системам интернет-банка или мобильного банка либо создавать обманные сайты, получая возможность распоряжения чужими денежными средствами. Последний случай необходимо отличать от ситуаций распространения ложных данных в информационно-телекоммуникационной сети (создание поддельных сайтов благотворительных организаций, интернет-магазинов, использование электронной почты), что должно квалифицироваться по общему составу мошенничества**. В данном случае потерпевший вводится в заблуждение и сам перечисляет свои денежные средства виновным лицам. Способы компьютерного мошенничества включают взлом паролей, кражу банковских реквизитов: преступник умышленно осуществляет доступ к защищенной информации, не имея на это полномочий [10, с. 111]. В ситуациях хищения денежных средств посредством незаконного воздействия на устройства, информационно-телекоммуникационные сети требуется квалификация по п. «в» ч. 3 ст. 159.6 УК РФ, а также при наличии признаков и по составам преступлений, предусмотренных главой 28 УК РФ.

Однако и в подобных ситуациях допускаются ошибки в квалификации. Например, действия участников организованной группы были квалифицированы по п. «а» ч. 4 ст. 158 УК РФ. Вместе с тем хищение денежных средств осуществлялось посредством заражения смартфонов операционной системы «Андроид»

* Постановление N 1-22/2019 от 18 янв. 2019 г. по делу N 1-186/2018 // Судебные и нормативные акты Российской Федерации: сайт. URL: <http://sudact.ru>

** О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного Суда Российской Федерации от 30 нояб. 2017 г. N 48 // Рос. газ. 2017. N 280.

вредоносной компьютерной программой с получением доступа к СМС-сервису «Мобильный банк» держателей банковских карт ПАО «Сбербанк», вследствие чего осуществлялись переводы денежных средств с их счетов на счета банковских карт, оформленных на третьих лиц, находящихся у участников организованной группы, посредством направления СМС-сообщений на сервисный номер «900»*. Представляется, что в данном случае происходило техническое вмешательство в функционирование платежной системы, а следовательно, прослеживаются признаки составов преступлений, предусмотренных ст. 159.6 УК РФ и ст. 273 УК РФ.

Возможны и ситуации, когда потерпевший сам переводит денежные средства под воздействием убеждающих речей виновного в качестве подтверждения намерения приобрести «товар», факта пользования терминалом самообслуживания или уплаты налога за получение приза в денежном эквиваленте взамен самого приза и т.п., что квалифицируется как мошенничество. При этом, несмотря на то, что в данном случае используются информационно-телекоммуникационные сети для перечисления денежных средств виновному лицу, подобные ситуации нельзя рассматривать как специальный вид мошенничества — с использованием электронных средств платежа, так как в данном случае важен способ хищения — обман или злоупотребление доверием, а то, каким образом потерпевший передает свое имущество (лично или осуществляя безналичный перевод), значения для квалификации не имеет. Однако если потерпевший переводит денежные средства виновному под угрозой применения насилия, опасного для жизни или здоровья, то способ хищения меняется и речь должна идти уже о другом составе преступления.

Таким образом, до сих пор сохраняются трудности в квалификации хищений безналичных, в том числе электронных, денежных средств, несмотря на разъяснения высшей судебной инстанции. Посредством интернет-технологий чужими

денежными средствами можно завладеть любым способом.

Учитывая неточности в понимании признаков составов преступлений, предусматривающих ответственность за различные формы хищения безналичных, электронных денежных средств, и проблемы квалификации анализируемых составов преступлений, представляется необходимым исключение п. «г» ч. 3 ст. 158, ст. 159.3 и ст. 159.6 из УК РФ с одновременным введением самостоятельного состава преступления «Хищение с использованием информационных технологий».

В соответствии с Федеральным законом от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»** информационные технологии — это процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов. Предлагаемый состав будет объединять все случаи неправомерного завладения чужими денежными средствами, находящимися на банковском счете, либо электронными денежными средствами любыми способами, которые стали возможны благодаря высоким технологиям, от использования чужих данных доступа к электронному банку до создания специальных программ для перечисления чужих средств на свой банковский счет или электронный кошелек.

Следует отметить, что вопрос о введении отдельного состава преступления за хищение с использованием компьютерной информации [11, с. 133] либо за хищение с использованием компьютерных технологий и об исключении статей 159.3 и 159.6 УК РФ обоснованно поднимался на страницах печати еще до введения в 2018 году квалифицирующего признака кражи с банковского счета, а равно в отношении электронных денежных средств [12, с. 8]. Однако предлагаемая редакция, по сути, повторяла положения ст. 159.6 УК РФ в части способа совершения преступления, что представ-

* Приговор Центрального районного суда г. Новосибирска N 1-12/2019 от 25 февр. 2019 г. по делу N 1-12/2019 // Судебные и нормативные акты Российской Федерации: сайт. URL: <http://sudact.ru>

** Об информации, информационных технологиях и о защите информации: федер. закон от 27 июля 2006 г. N 149-ФЗ: ред. от 1 мая 2019 г. // Собр. законодательства Рос. Федерации. 2006. N 31 (ч. I). Ст. 3448; Официальный интернет-портал правовой информации. URL: <http://www.pravo.gov.ru>

ляется ограничивающим возможность ее распространения на иные формы хищений.

Кроме того, спорным является приравнивание ввода, удаления, блокирования, модификации компьютерной информации к способам вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, на что обращалось внимание в научной литературе [13, с. 103]. М.Д. Фролов в рамках диссертационного исследования предлагает изменить ст. 159.6 УК РФ, сформулировав ее как «Хищение, совершенное с использованием информационно-телекоммуникационных технологий», под которым следует понимать хищение чужого имущества или приобретение права на чужое имущество, совершенное посредством ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей [14, с. 11].

Однако заметна терминологическая рассогласованность с понятийным аппаратом, используемым в специальном законодательстве, прежде всего в вышеназванном Федеральном законе от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации». В частности, закон оперирует такими понятиями, как информационные технологии и информационно-телекоммуникационные сети, не смешивая их. Кроме того, указание на способ совершения преступления сужает область применения нормы случаями целенаправленного противоправного воздействия на соответствующие средства и сети.

Введение отдельного состава хищения с использованием информационных технологий позволило бы объединить в одном составе все формы хищения по признаку совершения их определенным способом, повышающим общественную опасность содеянного, как это сделано применительно к хищению предметов, имеющих особую ценность, исходя из особенностей предмета посягательства. Под данный состав преступления будут подпадать случаи хищения безналичных и электронных денежных средств, совершенные тайно, путем обмана или злоупотребления доверием, в

случае открытого хищения, в том числе с применением насилия, опасного для жизни и здоровья, а также случаи присвоения или растраты вверенных безналичных денежных средств. Введение данного состава преступления позволит избежать ошибок в квалификации схожих ситуаций и будет способствовать единообразной правоприменительной практике.

Представляется, что хищение безналичных и электронных денежных средств в значительном размере и аналогичное хищение в крупном или особо крупном размере обладают различной степенью общественной опасности. Это необходимо учитывать при дифференциации уголовной ответственности и наказания и установления соответствующих квалифицирующих и особо квалифицирующих признаков в рамках предлагаемого состава преступления. При этом на степень общественной опасности содеянного влияет не только размер похищаемых средств, но и иные обстоятельства, которые в значительной степени повышают общественную опасность преступлений и являются типичными для такого рода деяний [15, с. 36-37]. Однако вопрос о дифференциации уголовной ответственности и наказания за хищения, совершаемые с использованием информационных технологий, безусловно, заслуживает отдельного самостоятельного исследования.

Таким образом, в настоящее время является проблематичным четкое разграничение кражи с банковского счета или электронных денежных средств, мошенничества с использованием электронных средств платежа и мошенничества в сфере компьютерной информации, совершенного с банковского счета, а равно в отношении электронных денежных средств, в силу схожести предмета посягательства и способа его совершения. В целях единообразного понимания и правильной квалификации неправомерного завладения безналичными, электронными денежными средствами предлагается исключить из УК РФ п. «г» ч. 3 ст. 158, ст. 159.3 и ст. 159.6 и одновременно дополнить его самостоятельным составом преступления «Хищение с использованием информационных технологий», который объединил бы в себе все формы хищения по признаку совершения их определенным способом, повышающим общественную опасность содеянного.

Список литературы

1. Макаров А.В., Алешкова В.А. Особенности и проблемы квалификации мошенничества, совершенного с использованием электронных средств платежа // Российский судья. 2019. N 5. С. 24-29.
2. Шестало С.С. Новое в уголовном законодательстве о хищении безналичных денежных средств // Юрист. 2018. N 8. С. 39-44.
3. Кули-Заде Т.А. Проблемы квалификации мошенничества в сфере компьютерной информации // Российская юстиция. 2019. N 4. С. 21-23.
4. Архипов А.В. Ответственность за хищение безналичных и электронных денежных средств: новеллы законодательства // Уголовное право. 2018. N 3. С. 4-9.
5. Яни П.С. Мошенничество с использованием электронных средств платежа // Законность. 2019. N 4. С. 30-35.
6. Абрамова Е.Н. Электронное средство платежа как комплексный объект гражданских прав // Банковское право. 2018. N 1. С. 22-32.
7. Хисамова З.И. Об уголовной ответственности за хищения, совершенные с использованием IT-технологий: анализ изменений законодательства и правоприменительной практики // Российский следователь. 2018. N 9. С. 43-47.
8. Русскевич Е.А. Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий. М.: ИНФРА-М, 2019. 188 с.
9. Шарапов Р.Д. Постановление Пленума Верховного Суда России «О судебной практике по делам о мошенничестве, присвоении и растрате»: заметки на полях // Криминалист. 2018. N 4. С. 16-22.
10. Бархатова Е.Н. Особенности квалификации мошенничества в сфере компьютерной информации и его разграничение с иными составами преступлений // Современное право. 2016. N 9. С. 110-115.
11. Чупрова А. Проблемы квалификации мошенничества с использованием информационных технологий // Уголовное право. 2015. N 5. С. 131-134.
12. Иногамова-Хегай Л.В. Квалификация преступлений против личности и «компьютерных» преступлений по правилам совокупности преступлений и конкуренции уголовно-правовых норм // Вестник Академии Генеральной прокуратуры Российской Федерации. 2016. N 5 (55). С. 4-9.
13. Чернякова А.В. Некоторые вопросы квалификации преступлений в сфере компьютерной информации // Вестник Тюменского института повышения квалификации сотрудников МВД России. 2019. N 1 (12). С. 98-103.
14. Фролов М.Д. Уголовно-правовое и криминологическое противодействие мошенничеству в сфере компьютерной информации: автореф. дис. ... канд. юрид. наук: 12.00.08. М., 2019. 26 с.
15. Шеслер А.В. Уголовно-правовая политика. Новокузнецк: Кузбасский ин-т ФСИН России, 2018. 78 с.

References

1. Makarov A.V., Aleshkova V.A. Peculiarities and issues of classification of fraud committed using electronic payment means. Russian judge, 2019, no. 5, pp. 24-29. (In Russ.).
2. Shestalo S.S. Novelties of the criminal law on embezzlement of non-cash money. Lawyer, 2018, no. 8, pp. 39-44. (In Russ.).
3. Kuli-Zade T.A. Problems of qualification of fraud in the field of computer information. Russian justice, 2019, no. 4, pp. 21-23. (In Russ.).
4. Arhipov A.V. Liability for the theft of non-cash money and electronic money: legislative novels. Criminal law, 2018, no. 3, pp. 4-9. (In Russ.).
5. Yani P.S. Online payment fraud. Legality, 2019. no. 4, pp. 30-35. (In Russ.).
6. Abramova E.N. Electronic means of payment as a complex object of civil rights. Bank right, 2018, no. 1, pp. 22-32. (In Russ.).
7. Hisamova Z.I. About criminal liability for theft committed using IT-technologies: analysis of changes in legislation and law enforcement practices. Russian investigator, 2018, no. 9, pp. 43-47. (In Russ.).
8. Russkevich E.A. Criminal law response to information and communication technology crimes. Moscow, INFRA-M Publ., 2019. 188 p. (In Russ.).
9. Sharapov R.D. Resolution of the Plenum of the Supreme Court of Russia "On judicial practice in cases of fraud, misappropriation and embezzlement": notes in the fields. Criminalist, 2018, no. 4, pp. 16-22. (In Russ.).
10. Barhatova E.N. Features of qualification of fraud in the field of computer information and distinction with other criminal offences. Modern law, 2016, no. 9, pp. 110-115. (In Russ.).
11. Chuprova A. The problems of qualification of fraud related to use of information technologies. Criminal law, 2015, no. 5, pp. 131-134. (In Russ.).
12. Inogamova-Hegay L.V. Qualification of crimes against the person and "computer" crimes according to the rules of combination of crimes and competition of criminal law norms. Bulletin of the Academy of the Prosecutor General's Office of the Russian Federation, 2016, no. 5 (55), pp. 4-9. (In Russ.).
13. Chernyakova A.V. Some issues relating to the characterization of computer-related crime. Bulletin of the Tyumen Advanced Training Institute of the Ministry of the Interior of the Russian Federation, 2019, no. 1 (12), pp. 98-103. (In Russ.).
14. Frolov M.D. Criminal and criminological prevention of computer fraud. Autoabstract Cand. Diss. Moscow, 2019. 26 p. (In Russ.).
15. Shesler A.V. Criminal policy. Novokuznetsk, Kuzbass Institute of the Federal Penitentiary Service of Russia, 2018. 78 p. (In Russ.).