ISSN 2500-4255

УДК 343.71; 343.72
DOI 10.17150/2500-4255.2020.14(4).601-612

РАЗЛИЧНЫЕ ПОДХОДЫ К ОЦЕНКЕ СПОСОБОВ ХИЩЕНИЙ БЕЗНАЛИЧНЫХ ДЕНЕЖНЫХ СРЕДСТВ В УСЛОВИЯХ СОВРЕМЕННОГО ИНФОРМАЦИОННОГО ОБЩЕСТВА

М.И. Третьяк, Л.В. Рябова
Северо-Кавказский федеральный университет, г. Ставрополь, Российская Федерация

Информация о статье

Дата поступления
26 февраля 2020 г.

Дата принятия в печать
19 августа 2020 г.

Дата онлайн-размещения
31 августа 2020 г.

Ключевые слова

Компьютерная информация; хищение безналичных денежных средств; тайный способ хищения; мошенничество; электронное средство платежа

Аннотация. В результате широкого распространения в сегодняшних условиях разнообразных способов незаконного изъятия безналичных денежных средств с применением информационных технологий появляется необходимость в поиске более совершенных подходов к оценке таких деяний. Рассматривая разные подходы к определению способов хищений в информационной сфере, специалисты исследуют мнения ученых, существующие в доктрине уголовного права, а также законодательные и судебные положения, принятые в течение всего периода действия Уголовного кодекса РФ (с 1997 по 2020 г.). Авторы предлагаемой статьи обращают особое внимание на подходы к оценке способов хищения безналичных денежных средств, получивших распространение в настоящее время, имеющиеся в теории, законодательной сфере и на практике. Отмечается, что в действующем уголовном законодательстве нашел закрепление выработанный современной теорией и практикой новый подход к оценке хищений в информационной сфере. Также указывается, что в современной теории уголовного права сложилось три основных направления в оценке способов хищения безналичных денежных средств в информационной сфере. Эти направления состоят в криминализации новой формы хищения, новых видов преступлений гл. 21 или 28 УК РФ; в рассмотрении такого хищения как разновидности традиционных форм хищения и других корыстных преступлений против собственности; в применении существующих норм о традиционных преступлениях гл. 21 и 28 УК РФ. Авторы статьи также отмечают, что с момента принятия уголовного законодательства незаконное изъятие безналичных денежных средств в информационной сфере оценивалось по-разному: как разновидность традиционного обманного хищения в форме мошенничества; в качестве отдельно выделенных видов мошенничества в зависимости от способа; в качестве отдельно выделенных видов мошенничества в зависимости от способа и кражи. Исходя из детального анализа содержания новых уголовно-правовых норм и разработанных теоретических (судебных) положений, выявлены положительные и отрицательные моменты, позволяющие сформулировать авторское видение эффективности закрепленного в действующем уголовном законодательстве нового подхода к оценке информационных хищений безналичных денежных средств.

VARIOUS APPROACHES TO ASSESSING THE METHODS OF STEALING CASHLESS MONEY IN THE MODERN INFORMATION SOCIETY

Maria I. Tretiak, Liliya V. Ryabova
North-Caucasus Federal University, Stavropol, the Russian Federation

Article info

Received
2020 February 26

Accepted
2020 August 19

Available online
2020 August 31

Keywords

Computer information; theft of cashless funds; secret method of theft; fraud; electronic means of payment

Abstract. A wide spread of various illegal methods of stealing cashless funds using modern information technologies makes it necessary to search for more advanced approaches to assessing such actions. Specialists examine different approaches to determining methods of theft in the information environment and analyze the opinions of scholars presented in the doctrine of criminal law, as well as legislative and court statutes adopted during the whole period that the Criminal Code of the Russian Federation has been in force (from 1997 to 2020). The authors of the article pay special attention to the approaches of assessing the widespread methods of stealing cashless money in the theory, legislative sphere and practice. It is noted that current criminal legislation reflects a new approach to assessing theft in the information environment, developed on the basis of modern theory and practice. The authors point out that in modern criminal law theory there are three main trends in assessing the methods of stealing cashless money in the information environment.

They are: criminalization of the new form of theft, new types of crimes in Ch. 21 or 28 of the Criminal Code of the Russian Federation; viewing this theft as a variety of traditional forms of theft and other acquisitive crimes against property; application of the existing norms of traditional crimes in Ch. 21 and 28 of the CC of the RF. The authors also note that in the period following the adoption of criminal legislation, the illegal acquisition of cashless funds in the information environment has been assessed differently: as a type of traditional theft by deceit in the form of fraud; as separate types of fraud depending on the method; as separate types of fraud depending on the method and theft. The authors conduct a detailed analysis of the contents of new criminal law norms and the developed theoretical (court) statutes, identify their positive and negative features, and present their own understanding of the effectiveness of the new approach to assessing online theft of cashless money incorporated in current criminal legislation.

Сегодня в различных источниках регулярно сообщается о разнообразных постоянно видоизменяющихся способах хищения в основном безналичных денежных средств с использованием усложняющихся технических средств вычислительной техники, телефонов, электронных средств платежа. Считаем, что в этих условиях наиболее важным вопросом является определение и изучение более эффективных подходов к оценке способов таких деяний, имеющихся в теории, законодательной сфере и на практике.

В течение всего периода действия Уголовного кодекса РФ 1996 г. (с 1997 по 2020 г.) ученые высказывали различные мнения по поводу оценки корыстных преступлений в сфере высоких технологий, в том числе деяний, связанных с хищением безналичных денежных средств. Среди существующих позиций авторов по этому вопросу в первую очередь следует выделить позицию большой группы ученых, считающих, что в уголовном законодательстве отсутствуют нормы, которые с достаточной степенью точности отражали бы специфические признаки способов совершения корыстных преступлений в сфере высоких технологий, и в связи с этим предлагающих криминализировать данные корыстные деяния в виде:

– новой формы хищения [1; 2, с. 15];

– новой формы хищения с выделением отягчающего хищения с банковских счетов и электронных денежных средств [3];

– нового корыстного преступления гл. 21 УК РФ [4][1];

– корыстного преступления гл. 28 УК РФ в качестве мошенничества и подлога [5; 6].

Способы совершения этих видов преступлений авторами определялись по-разному, например:

– путем указания обобщенного воздействия с выделением конкретных его форм, в частности как вмешательство в функционирование компьютера или компьютерной системы путем ввода, изменения, удаления или блокирования компьютерных данных [7, с. 13];

– одной конкретной формы воздействия на компьютерную информацию, например в виде модификации результатов автоматизированной обработки данных компьютерной системы [8];

– средства (орудия) совершения преступления в виде использования компьютерной информации (технологий) [9];

– предмета воздействия, которым выступает компьютерная информация [10, с. 22–24];

– объекта преступления — информационной сферы [11].

Представители второй группы ученых, также многочисленной, рассматривали эти преступления как одну из разновидностей предусмотренных УК РФ традиционных форм хищения и других корыстных преступлений против собственности, например:

– в качестве квалифицированных составов кражи (присвоения и растраты) с применением компьютерной информации [12];

– в виде квалифицированного состава мошенничества с использованием результата автоматизированной обработки данных [13, с. 7];

– в качестве конкретной нормы о компьютерном мошенничестве, состоящем в завладении чужим имуществом путем обмана, злоупотребления доверием, присвоения, растраты либо в причинении имущественного ущерба путем обмана или злоупотребления доверием, совершенном с использованием ЭВМ, системы ЭВМ или их сети [14];

[1] Например, вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, совершенное с корыстной целью либо без таковой.

– как разновидность преступления, закрепленного в ст. 165 УК РФ [15].

Способы использования различных компьютерных технологий в этих случаях являлись либо основанием для ужесточения уголовной ответственности, либо критерием для выделения определенного вида преступления против собственности (отнесения к существующему виду преступлений гл. 21 УК РФ).

Также в теории уголовного права имеются мнения ученых, полагающих, что в отношении подобных деяний следует применять существующие *нормы о традиционных преступлениях против собственности и преступлениях гл. 28 УК РФ* [9; 16, с. 22; 17].

Следовательно, разработанные теоретические положения уголовного права являются подтверждением того, что в доктрине сложилось три основных направления в оценке способов хищения безналичных денежных средств в информационной сфере, состоящих:

– в криминализации новой формы хищения, новой формы хищения с выделением отягчающего хищения с банковских счетов и электронных денежных средств, новых видов преступлений гл. 21 или 28 УК РФ;

– в рассмотрении хищения безналичных денежных средств в информационной сфере как разновидности традиционных форм хищения, корыстного посягательства на собственность, объединяющего различные формы хищения и иные корыстные деяния, других отдельных корыстных преступлений против собственности;

– в применении существующих норм о традиционных преступлениях гл. 21 и 28 УК РФ.

С принятием УК РФ 1996 г. в гл. 28 кодекса впервые получила закрепление разновидность преступлений в сфере компьютерной информации, совершаемых путем неправомерного доступа к компьютерной информации или создания, использования и распространения вредоносных компьютерных программ. Однако корыстная направленность не предусматривалась в качестве обязательного субъективного признака ни основных, ни квалифицированных составов[2] этих преступлений. В гл. 21 УК РФ, в которой располагались корыстные преступления против собственности в виде кражи, мошенничества[3] [18, с. 5–13] и других преступных деяний, наоборот, отсутствовали нормы, предусматривающие корыстные деяния, выступающие способами совершения преступлений в сфере компьютерной информации.

В правоприменительной практике в период с 1997 по 2007 г. различные способы воздействия на компьютерную информацию с помощью *средств вычислительной техники, платежных карт* находили отражение лишь в судебных решениях по конкретным уголовным делам. Однако именно на основании этих решений был выработан один из первых подходов к оценке таких деяний, который впоследствии нашел закрепление в пп. 12 и 13 постановления Пленума Верховного Суда РФ от 27 декабря 2007 г. № 51. Смысл его состоял в том, что исключительно к традиционному обманному мошенничеству (ст. 159 УК РФ)[4] относились различные способы обращения денежных средств, находящихся на счетах в банках, при этом не совершалось неправомерного доступа к компьютерной информации или не использовались (не распространялись) созданные вредоносные программы (ст. 272 и 273 УК РФ). В случае обращения денежных средств, находящихся на счетах в банках, с использованием указанных способов они оценивались как совокупность мошенничества и преступлений в сфере компьютерной информации. К обманному мошенничеству было также отнесено и использование похищенной или поддельной кредитной либо расчетной карты для оплаты товаров или услуг в торговом или сервисном центре при условии, если лицо ставит подпись в чеке на покупку вместо законного владельца карты либо

[2] Только в 2011 г. федеральным законом от 7 декабря № 420-ФЗ в ст. 272, 273 УК РФ была предусмотрена корыстная заинтересованность в качестве квалифицирующего признака (ч. 2). С этого момента отдельная часть предусмотренных ст. 165 УК РФ преступлений, совершенная способами, предусмотренными в ст. 272 и 273 УК РФ, стала квалифицироваться только по нормам гл. 28 УК РФ (см.: Приговор по уголовному делу 1-130/2015 Пугачевского районного суда Саратовской области от 18 ноября 2015 г. URL: http://судебныерешения.рф). Другая часть таких преступлений, совершенная иными способами вмешательства в компьютерные системы, продолжала оцениваться по ст. 165 УК РФ (см.: Постановление судьи Советского района г. Махачкалы Республики Дагестан от 14 марта 2012 г. по апелляционной жалобе на приговор мирового судьи судебного участка № 14 Советского района г. Махачкалы. URL: http://судебныерешения.рф).

[3] Тайные и обманные способы совершения преступлений против собственности предусматривались в российском законодательстве с древнейших времен.

[4] Возможно и в виде причинения имущественного ущерба путем обмана.

предъявляет поддельный паспорт на его имя. Использование заранее похищенной или поддельной платежной карты для получения наличных денежных средств посредством банкомата без участия уполномоченного работника кредитной организации оценивалось как тайное хищение (кража).

Затем положения, предусмотренные в пп. 12 и 13 указанного постановления, послужили основанием для выделения в 2012 г. в уголовном законодательстве[5] двух самостоятельных норм, регламентирующих ответственность за такие виды мошенничества: с использованием платежных карт (ст. 159.3 УК РФ) и в сфере компьютерной информации (ст. 159.6 УК РФ). Содержание первой из этих норм было сформулировано как хищение чужого имущества, в основном безналичных денежных средств, совершенное с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты путем обмана уполномоченного работника кредитной, торговой или иной организации. Определение содержания обманного способа этого вида мошенничества не раскрывалось вплоть до принятия новых официальных разъяснений высшей судебной инстанцией в 2017 г.

В ст. 159.6 УК РФ впервые был закреплен способ мошенничества, заключающийся только в непосредственном воздействии на компьютерную информацию, отражающую сведения об имуществе либо праве на него. Он состоял во вмешательстве в функционирование средств компьютерной информации или информационно-телекоммуникационных сетей в виде ввода, удаления, блокирования, модификации компьютерной информации или иных способов воздействия на нее. Определив как мошенничество преступление, для которого нехарактерен традиционный обман, предполагающий непосредственное участие конкретного собственника имущества, законодатель создал неоднозначную ситуацию с определением формы этого хищения. Если исходить из названия ст. 159.6 УК РФ, то хищение является отдельной мошеннической формой; если учитывать только содержание способа, закрепленного в диспозиции статьи, то она может быть либо тайной, либо вообще иной формой хищения. Если же при определении формы хищения рассматриваемого преступления одновременно учитывать название статьи и содержание диспозиции закона (ст. 159.6 УК РФ), то она в одних случаях может быть обманной, в других — безобманной (тайной), в третьих — иной формой хищения[6].

Кроме того, после принятия таких изменений уголовного закона в судебной практике в течение пяти лет (с 2012 по 2017 г.) сохранялось отношение к такому роду преступлений как к разновидности традиционного мошенничества (ст. 159 УК РФ), поскольку до принятия постановления Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48[7] продолжало действовать постановление Пленума Верховного Суда РФ от 27 декабря 2007 г. № 51, в котором, как уже было отмечено выше, данные преступные деяния рассматривались как мошенничество, предусмотренное ст. 159 УК РФ.

Что же касается конкретной судебной практики в период с 2012 по 2017 г., то, согласно внесенным в УК РФ изменениям, как хищение с использованием платежных карт оценивался:

– обман уполномоченного лица при использовании принадлежащей другому лицу платежной карты для оплаты товаров или услуг в торговом (сервисном) центре[8];

– обман уполномоченного лица кредитной организации при получении доступа (авторизации карты) к денежным средствам и их последующее получение с использованием принадлежащей другому лицу карты[9];

[5] О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации [Электронный ресурс] : федер. закон от 29 нояб. 2012 г. № 207 // СПС «КонсультантПлюс».

[6] Обращая внимание на отсутствие в диспозиции закона указания на обманный, тайный способы, считаем возможным предположить, что речь идет о самостоятельной форме хищения.

[7] О судебной практике по делам о мошенничестве, присвоении и растрате [Электронный ресурс] : постановление Пленума Верхов. Суда РФ от 30 нояб. 2017 г. № 48 // СПС «КонсультантПлюс».

[8] Приговор Центрального районного суда г. Комсомольска-на-Амуре Хабаровского края по уголовному делу № 1-290/2015 от 15 апреля 2015 г. URL: https://sudact.ru/regular/doc/c0UCCGfv3B5x/?regular-txt ; Приговор мирового судьи судебного участка № 38 г. Кургана Курганской области по уголовному делу № 1-18/14 от 26 марта 2014 г. URL: https://rospravosudie.com/act-q/section-acts/sort-date.

[9] Приговор мирового судьи судебного участка № 2 Нижнетуринского судебного района г. Нижняя Тура Свердловской области по уголовному делу № 1-84/2014 от 24 ноября 2014 г. ; Приговор мирового судьи судебного участка Волоконовского района Белгородской области по уголовному делу № 1-4/2015 от

– обман уполномоченного лица кредитной организации на этапе завладения кредитной картой[10] для последующего изъятия (обращения) денежных средств с использованием этой карты[11].

К вмешательству, выступающему способом мошенничества в сфере компьютерной информации, относились разнообразные случаи:

– хищения безналичных денежных средств с использованием виновным лицом телефона[12] (компьютера[13]), подключенного к услуге «Мобильный банк», путем ввода конфиденциальной информации держателя платежной карты, предоставляющей доступ к этим деньгам и переданной злоумышленнику самим держателем платежной карты под воздействием обмана;

– хищения безналичных денежных средств с использованием виновным лицом телефона потерпевшего (которым оно завладело обманным путем), подключенного к услуге «Мобильный банк»[14], или с использованием собственного телефона, подключенного к услуге «Мобильный банк», и сим-карты, ошибочно привязанной к лицевому банковскому счету потерпевшего[15] путем ввода учетных данных собственника имущества;

– хищения безналичных денежных средств с помощью созданных поддельных сайтов благотворительных организаций, интернет-магазинов;

– хищения безналичных денежных средств с использованием виновным лицом специализированных программ[16] для вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей[17]. Чаще всего это компьютерные программы по оформлению кредитных договоров, договоров о выпуске кредитных карт, ведомостей о заработной плате, документов (накладных) о цене (количестве) товара. Также в судебной практике имелись менее распространенные случаи применения для совершения преступных деяний программ, созданных для работы с сим-картами, абонентскими номерами, файлами настроек принимаемых купюр в программном обеспечении банкомата.

В ситуациях, когда мошенничество в сфере компьютерной информации было сопряжено с преступлениями, предусмотренными в гл. 28 УК РФ, судебная практика продолжала оценивать их по совокупности.

Изучение конкретной судебной практики по уголовным делам за 2012–2017 гг. позволяет сделать вывод о том, что мошенничеством с использованием платежных карт признавались как случаи обмана уполномоченного лица при использовании злоумышленником принадлежащей другому лицу платежной карты, так и случаи обмана уполномоченного лица кредитной организации при авторизации виновным лицом чужой платежной карты или на этапе завладения этой картой. К мошенничеству в сфере компьютерной информации относились любые случаи вмешательства в функци-

16 февраля 2015 г. URL: https://rospravosudie.com/act-q/section-acts/sort-date.

[10] Независимо от использования банковской карты для оплаты товаров (услуг) в торговом (сервисном) центре либо получения наличных денег через банкомат или перечисления безналичных денег на счет виновного (или другого) лица.

[11] Такие виды обмана в судебной практике встречались реже (см.: Постановление Копейского городского суда Челябинской области по уголовному делу № 1-166/2015 от 4 марта 2015 г. ; Приговор мирового судьи судебного участка № 2 г. Ельца Липецкой области по уголовному делу № 1-27/2015 от 27 мая 2015 г. URL: https://rospravosudie.com/act-q/section-acts/sort-date).

[12] Приговор мирового судьи судебного участка № 2 Ленинского района г. Ульяновска по уголовному делу № 1-25/13 от 5 июня 2013 г. URL: http://судебныерешения.рф.

[13] Постановление Президиума Алтайского краевого суда от 3 сентября 2013 г. по делу № 44у-224/13 [Электронный ресурс] // СПС «КонсультантПлюс» ; Приговор по уголовному делу № 1-82/2013 от 13 июня 2013 г. Грачевского районного суда Ставропольского края. URL: http://www.gcourts.ru/case/14183520 ; Приговор по уголовному делу № 1-232/13 от 23 апреля 2013 г. Подольского городского суда Московской области. URL: http://www.gcourts.ru/case/14183520 ; Апелляционное определение Московского городского суда от 6 мая 2013 г. № 10-2076 [Электронный ресурс] // СПС «КонсультантПлюс».

[14] Приговор Братского городского суда Иркутской области № 1-17/2015 1-17/2015(1-640/2014; 1-640/2014 от 12 января 2015 г. URL: https://sudact.ru/regular/doc.

[15] Приговор Талицкого районного суда Свердловской области по уголовному делу № 1-31/2015 от 24 февраля 2015 г. URL: http://судебныерешения.рф.

[16] Виновное лицо может правомерно (неправомерно) использовать различные компьютерные программы. Если это воздействие будет связано с созданием, использованием и распространением вредоносных компьютерных программ, возникает необходимость квалификации по ст. 273 УК РФ.

[17] Приговор мирового судьи судебного участка № 2 Богдановичского судебного района Свердловской области по уголовному делу № 1-20/2014 от 3 марта 2014 г. URL: http://судебныерешения.рф.

онирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей: это как простой ввод информации с использованием различных информационных технологий (например, чужой сим-карты, чужого телефона с наличием в нем сим-карты и др.) для изъятия имущества, так и ввод (удаление, блокирование, модификация) информации с применением специализированных программ, оказывающих влияние на другое программное обеспечение, установленное в различных информационных средствах.

Существенные изменения в оценке конкретных способов хищения безналичных денежных средств с использованием различных информационных технологий, выработанных практикой в период с 2012 по 2017 г., произошли с принятием постановления Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48.

В частности, согласно пп. 17 и 21 постановления, кроме хищения наличных денежных средств с использованием заранее похищенной или поддельной платежной карты без участия уполномоченного лица, к простому виду кражи были отнесены такие его виды:

– хищение безналичных денежных средств с использованием необходимой для получения доступа к ним конфиденциальной информации держателя платежной карты, переданной злоумышленнику самим держателем платежной карты под воздействием обмана или злоупотребления доверием;

– хищение безналичных денежных средств с использованием учетных данных собственника или иного владельца имущества независимо от способа получения доступа к таким данным, если при этом виновный не оказывает незаконного воздействия на программное обеспечение серверов, компьютеров или на сами информационно-телекоммуникационные сети.

Что касается хищения, совершенного путем распространения заведомо ложных сведений в информационно-телекоммуникационных сетях, включая сеть Интернет, то оно стало признаваться традиционным видом мошенничества (ст. 159 УК РФ). К мошенничеству в сфере компьютерной информации отнесены лишь способы незаконного воздействия программных и (или) программно-аппаратных средств на программное обеспечение серверов, компьютеров или на сами информационно-телекоммуникационные сети, исключающие обманное воздействие на потерпевшего[18]. Теперь в соответствии с п. 1 названного постановления мошенничество в сфере компьютерной информации не отнесено к видам мошенничества, для которых характерен обманный способ хищения.

В п. 17 постановления понятие обманного способа мошенничества с использованием платежных карт раскрыто как сообщение уполномоченному лицу заведомо ложных сведений о принадлежности виновному лицу такой карты на законных основаниях либо умолчание о незаконном владении им платежной картой. Это определение позволяет утверждать, что к хищению с использованием платежных карт может быть отнесена только одна разновидность обманного использования принадлежащей другому лицу платежной карты — в случае *оплаты с помощью этой карты товаров или услуг в торговом (сервисном) центре*, поскольку только в этих примерах обман уполномоченного лица осуществляется при непосредственном использовании уже имеющейся у виновного лица чужой платежной карты. Другие ситуации, когда обман уполномоченного лица кредитной организации осуществляется при авторизации карты или на этапе завладения этой платежной картой[19], как и конфиденциальной информацией держателя платежной карты, должны оцениваться только как приготовление к хищению[20], а не как обманный способ хищения. Последующее изъятие (обращение) безналичных (наличных) денежных средств с использованием полу-

[18] При условии, если оно нарушает установленный процесс обработки, хранения, передачи компьютерной информации, что позволяет виновному или иному лицу незаконно завладеть чужим имуществом или приобрести право на него (см.: О судебной практике по делам о мошенничестве, присвоении и растрате : постановление Пленума Верхов. Суда РФ от 30 нояб. 2017 г. № 48. П. 20).

[19] На наш взгляд, обман уполномоченного лица кредитной организации, осуществляемый на этапе предоставления виновным лицом конфиденциальных данных другого лица (например, использования чужого паспорта) с целью вначале завладеть кредитной картой другого лица, а уже затем изъять (обратить) безналичные (наличные) денежные средства с использованием этой карты, может оцениваться как простое мошенничество при условии, что преступление окончено с момента получения кредитной карты независимо от изъятия (обращения) безналичных (наличных) денежных средств с использованием этой карты.

[20] О судебной практике по делам о мошенничестве, присвоении и растрате : постановление Пленума Верхов. Суда РФ от 30 нояб. 2017 г. № 48. П. 17, абз. 3.

ченной от уполномоченного лица карты может быть квалифицировано как кража[21].

Важно отметить, что в судебной практике в 2017 г. в связи с принятием указанного выше постановления произошли серьезные изменения в оценке конкретных способов исследуемых преступлений. Они состояли в следующем: наиболее точно определены обманные способы мошенничества с использованием платежных карт, в зависимости от способа вмешательства в функционирование информационных технологий выделены новые виды тайного и обманного хищения безналичных денежных средств, конкретизированы способы мошенничества в сфере компьютерной информации. В связи с этим отдельные виды хищения, которые ранее признавались компьютерным мошенничеством (ст. 159.6 УК РФ), были отнесены к тайному хищению (ст. 158 УК РФ) и традиционному обманному мошенничеству (ст. 159 УК РФ). Исходя из этого, информационное мошенничество, содержащееся в ст. 159.6 УК РФ, является самостоятельной отдельно выделенной формой хищения.

В 2018 г. в результате изменений уголовного закона[22] произошло установление отдельной уголовной ответственности за хищение с банковского счета, а равно в отношении электронных денежных средств, в виде:

– конкретного состава мошенничества с использованием электронного средства платежа (ст. 159.3 УК РФ);

– квалифицированных видов кражи и мошенничества в сфере компьютерной информации с банковского счета, а равно в отношении электронных денежных средств (п. «г» ч. 3 ст. 158 и п. «в» ч. 3 ст. 159.6 УК РФ).

Но в связи с реформированием уголовного законодательства сложилась следующая ситуация в определении отличительных способов этих новых видов хищений.

В новой редакции нормы, предусмотренной в ст. 159.3 УК РФ, мошенническое хищение с использованием электронного средства платежа закрепляется без указания традиционных способов его совершения. В данном случае при определении способа этого специального вида мошенничества следовало бы исходить из общей нормы ст. 159 УК РФ[23] и, соответственно, признать обман и злоупотребление доверием его способами[24], а предметом — «чужое имущество» или «право на чужое имущество» [19]. Однако в п. «г» ч. 3 ст. 158 УК РФ используется формулировка «при отсутствии признаков преступления, предусмотренного статьей 159.3 УК РФ»[25], в которой речь идет о признаках (без конкретизации их вида и содержания), указанных не в ст. 159 УК РФ, а только в *ч. 1 ст. 159.3 УК РФ*[26]. Такая трактовка позволяет лишь предположить, что для мошенничества с использованием электронных средств платежа характерен особый предмет (только безналичные денежные средства) и строго определенный способ обмана, который присущ только этому виду мошенничества. Либо способ, вообще не связанный ни с обманным, ни с тайным изъятием, как это имеет место при определении способа мошенничества в ст. 159.6 УК РФ [там же], которое, согласно п. 1 названного постановления, не было отнесено к видам мошенничества, для которых характерен обманный способ хищения. Исходя из сказанного, считаем, что предусмотренные в п. «г» ч. 3 ст. 158 и в ст. 159.3 УК РФ положения не предоставляют возможности точ-

[21] Например, виновное лицо использовало платежную карту для совершения интернет-покупок, получения посредством банкомата наличных денег либо перевода безналичных денег на свой (иной) банковский счет. На наш взгляд, это будет оцениваться как мошенничество с использованием платежных карт, если виновное лицо затем совершит обман уже представителя торговой организации в процессе покупки с использованием чужой платежной карты.

[22] О внесении изменений в Уголовный кодекс РФ [Электронный ресурс] : федер. закон РФ от 23 апр. 2018 г. № 111-ФЗ // СПС «КонсультантПлюс».

[23] В связи с этим используемая законодателем формулировка «при отсутствии признаков преступления, предусмотренного статьей 159.3 УК РФ» в п. «г» ч. 3 ст. 158 УК РФ для отграничения кражи с банковского счета, а равно в отношении электронных денежных средств, от мошенничества, на наш взгляд, является неточной, поскольку обман и злоупотребление доверием как способы совершения мошенничества, которые позволяют отграничивать его от кражи, указаны не в ст. 159.3 УК РФ, а в ч. 1 ст. 159 УК РФ. Кроме того, формулировка «при отсутствии признаков преступления, предусмотренного статьей 159.3 УК РФ» устанавливает только факт отсутствия признаков, не определяя их вида и содержания.

[24] Как это уже было в уголовном законодательстве до 2012 г., когда мошенничество с использованием платежных карт рассматривалось в качестве одной из разновидностей традиционного мошенничества (ст. 159 УК РФ).

[25] Вероятно, при формулировании этого положения законодатель допустил определенную неточность, наряду со ст. 159.3 не указав ст. 159 УК РФ.

[26] Позволяющие отграничивать такое мошенничество от специального вида кражи.

но и конкретно определить отличительные признаки способов этих видов преступлений.

Признаками вновь выделенных квалифицированных видов преступлений, предусмотренных в п. «г» ч. 3 ст. 158 и п. «в» ч. 3 ст. 159.6 УК РФ, служащими основанием для ужесточения уголовной ответственности, названы в одном случае местонахождение (хранение) денежных средств — банковский счет, а в другом — определенная форма предмета преступления — электронные денежные средства. Однако указанные признаки позволяют отграничивать только хищения, предусмотренные основным и квалифицированным составом преступления, но не хищения, закрепленные в п. «г» ч. 3 ст. 158 и п. «в» ч. 3 ст. 159.6 УК РФ. Тайный способ и способы вмешательства, закрепленные в ч. 1 ст. 158 и в ст. 159.6 УК РФ, которые присущи всем квалифицированным видам краж и мошенничествам в сфере компьютерной информации, в том числе безналичных средств, не могут служить критерием для отграничения этих видов преступлений, поскольку для мошенничества в сфере компьютерной информации также характерна обстановка тайности изъятия безналичных денежных средств, а способы, указанные в ч. 1 ст. 159.6 УК РФ, могут быть, в свою очередь, присущи и краже.

Выделение квалифицированного вида кражи и компьютерного мошенничества без конкретизации способов воздействия на информацию в п. «г» ч. 3 ст. 158 и п. «в» ч. 3 ст. 159.6 УК РФ приводит к установлению в законе иных правил квалификации этих деяний. В частности, квалифицированному виду кражи, согласно п. «г» ч. 3 ст. 158 УК РФ, присущи любые способы тайного воздействия на информацию, а для безобманного мошенничества в сфере компьютерной информации характерны способы тайного воздействия на информацию, лишь указанные в ч. 1 ст. 159.6 УК РФ. Это позволяет утверждать, что нормы, закрепленные в п. «г» ч. 3 ст. 158 и п. «в» ч. 3 ст. 159.6 УК РФ, соотносятся как общая и специальная. Тогда в соответствии с ч. 3 ст. 17 УК РФ квалификация хищения безналичных денежных средств с использованием необходимой для получения доступа к ним конфиденциальной информации держателя платежной карты или учетных данных собственника (иного владельца) имущества должна во всех случаях осуществляться только по специальной норме, т.е. по п. «в» ч. 3 ст. 159.6 УК РФ. Пункт «г» ч. 3 ст. 158 УК РФ следует применять только в ограниченных ситуациях, не связанных с применением средств, указанных в ч. 1 ст. 159.6 УК РФ, например при использовании преступником принадлежащего другому лицу платежного средства для перевода денежных средств или оплаты различных услуг посредством банкомата. Ввиду этого предложенные правила квалификации в судебных разъяснениях в пп. 17 и 21 обозначенного выше постановления не подкрепляются внесенными при реформировании законодательными положениями. Получается, что отличительные признаки способов хищений, содержащихся в п. «г» ч. 3 ст. 158 и п. «в» ч. 3 ст. 159.6 УК РФ, также не получают конкретного отражения в законе.

Следовательно, в результате изменений, внесенных в УК РФ, в 2018 г. был применен подход к определению тайного и мошеннического хищения безналичных денежных средств (п. «г» ч. 3 ст. 158, ст. 159.3 и п. «в» ч. 3 ст. 159.6 УК РФ) без конкретизации их отличительных способов.

Проведенный анализ практики и уголовного закона с точки зрения подходов к оценке изъятия безналичных денежных средств в информационной сфере свидетельствует о признании такого изъятия в качестве:

– разновидности только традиционного обманного хищения в форме мошенничества;

– формы хищения в виде мошенничества, отдельно выделенной в зависимости от способа: обмана с использованием платежных карт и различных способов вмешательства в функционирование информационных средств (сетей);

– формы хищения в виде кражи и мошенничества: мошенничества с использованием электронных средств платежа, квалифицированного вида традиционной кражи и мошенничества в сфере компьютерной информации.

Исследование положений, имеющихся в законе, теории и практических разъяснениях высшей судебной инстанции за период с 1997 по 2020 г., является подтверждением того, что в действующем уголовном законодательстве получил закрепление выработанный современной теорией и практикой новый подход к оценке хищений безналичных денежных средств в информационной сфере, заключающийся:

– во-первых, в отдельной регламентации ответственности за незаконное изъятие (обращение) безналичных денежных средств в информационной сфере в виде основного или квалифицированных составов, главным отграничивающим (отягчающим ответственность)

критерием (обстоятельством) которых признается предмет преступления (определенный вид и место его хранения (нахождения));

– во-вторых, в отождествлении данного рода хищения с традиционными его формами в виде двух специальных разновидностей мошенничества и кражи без конкретизации их специфических способов.

В чем заключаются преимущества и недостатки такого подхода?

Глобальное распространение дистанционного банковского обслуживания, преимущественно безналичная форма денежных средств, общеизвестное место их хранения — банковские счета или виртуальное пространство — позволяют в современных условиях активно использовать в преступных целях всевозможные способы дистанционного доступа к безналичным денежным средствам с применением информационных технологий [20]. Это свидетельствует о большей уязвимости, незащищенности, привлекательности для преступников безналичных денежных средств [21; 22; 23, p. 12–15] и, соответственно, об особом характере общественной опасности таких хищений [24] по сравнению с общественной опасностью хищений наличных денежных средств [3]. Поэтому положительным моментом является применение дифференцированного подхода при закреплении ответственности за информационное хищение безналичных денежных средств в нормах уголовного закона.

Однако одновременное выделение при реформировании уголовного закона различных видов информационного хищения безналичных денежных средств в гл. 21 УК РФ и их отождествление с традиционными формами хищения без конкретизации специфических способов совершения информационного хищения безналичных денежных привело к появлению и проблемных моментов:

– невозможности точно и конкретно определить способы совершения этих видов преступлений;

– закреплению тайной формы хищения в двух положениях закона (п. «г» ч. 3 ст. 158 и п. «в» ч. 3 ст. 159.6 УК РФ) без установления отличительных способов вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей;

– сохранению одновременно обманной, безобманной (тайной), а возможно, и иной формы хищения в одном и том же положении закона (ст. 159.6 УК РФ);

– установлению в законе (п. «г» ч. 3 ст. 158 и п. «в» ч. 3 ст. 159.6 УК РФ) совсем иных правил квалификации, чем те, что предложены в судебных разъяснениях (в пп. 17 и 21 обозначенного выше постановления).

Сказанное позволяет заключить, что основным недостатком при реформировании законодательства о хищениях безналичных денежных средств в информационной сфере выступает отказ от конкретизации отличительных способов и более точного определения форм этих видов хищений в нормах закона. Поэтому появляются серьезные сомнения в достаточной эффективности закрепленного в действующем уголовном законодательстве подхода к оценке хищений безналичных денежных средств в информационной сфере.

В связи с этим считаем возможным предложить свое видение усовершенствования нового подхода к оценке хищений безналичных денежных средств в информационной сфере в современном уголовном законодательстве. Оно состоит в осуществлении следующих изменений в уголовном законодательстве.

К видам краж, закрепленным в п. «г» ч. 3 ст. 158 УК РФ, могут быть отнесены деяния, способом совершения которых не может выступать, во-первых, незаконное воздействие программных средств на программное обеспечение компьютерных систем, во-вторых, обман. Такими деяниями являются изъятие безналичных денежных средств с применением предварительно полученной конфиденциальной информации о держателе платежной карты, сим-карты (телефона), о собственнике (ином владельце) имущества, и все случаи использования электронного средства платежа для хищения безналичных средств, в том числе деяния, рассматриваемые в качестве мошенничества в ст. 159.3 УК РФ. Полагаем, что обманный способ совершения преступления, содержащегося в ст. 159.3 УК РФ, не может служить критерием для выделения и признания его мошенничеством. Изъятие (обращение) безналичных денежных средств в этом случае осуществляется лишь путем одновременного использования электронного средства, информации (кода), компьютерной техники (POS-терминалов), связанных с программно-аппаратными комплексами — серверами. Сотрудник торговой (сервисной (иной)) организации только предоставляет

возможность использовать POS-терминал для перевода безналичных денежных средств самим виновным лицом, не зная при этом истинного владельца карты. Сходной точки зрения придерживаются Л.В. Боровых, Е.А. Корепанова, С.М. Кочои, а также Н.В. Тимошин [25; 26, с. 106; 27, с. 13].

Учитывая все сказанное, тайное хищение безналичных денежных средств, зафиксированное в п. «г» ч. 3 ст. 158 УК РФ, необходимо сформулировать в следующем виде: «Кража, совершенная с банковского счета, а равно в отношении электронных денежных средств, с использованием принадлежащего другому лицу электронного средства платежа, сим-карты (телефона) или предварительно полученной конфиденциальной информации о держателе платежной карты».

Следует заменить термин «мошенничество» в ст. 159.6 УК РФ на «вмешательство в функционирование информационных средств (сетей)», а в примечании к ст. 159.6 УК РФ необходимо закрепить понятие «вмешательство» аналогично тому, которое содержится в п. 20 постановления от 30 ноября 2017 г. № 48.

При реформировании уголовного законодательства законодатель был непоследователен в выделении квалифицированных видов только кражи и мошенничества в сфере компьютерной информации. Хищение безналичных денежных средств может быть совершено и обманными способами, например с помощью созданных поддельных сайтов благотворительных организаций, интернет-магазинов. Этот вид хищения в соответствии с п. 21 названного выше постановления отнесен к традиционному мошенничеству. Ввиду этого предлагаем предусмотреть в ст. 159 УК РФ уголовную ответственность за мошенничество, совершенное с банковского счета, а равно в отношении электронных денежных средств, в качестве квалифицированного состава преступления.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Яни П.С. Специальные виды мошенничества / П.С. Яни // Законность. — 2015. — № 9. — С. 9–12.

2. Алферова Ю.О. Проблемы квалификации компьютерного мошенничества / Ю.О. Алферова, О.М. Дементьев // Science Time. — 2014. — № 7. — С. 11–16.

3. Чернякова А.В. Актуальные аспекты уголовной ответственности за хищения, совершаемые с использованием информационно-коммуникационных технологий / А.В. Чернякова // Юридическая наука и правоохранительная практика. — 2019. — № 3 (49). — С. 124–130.

4. Третьяк М.И. Проблема законодательной регламентации преступлений против собственности в сфере высоких технологий / М.И. Третьяк // Законность. — 2016. — № 7 (981). — С. 41–46.

5. Лопатина Т.М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности : автореф. дис. … д-ра юрид. наук : 12.00.08 / Т.М. Лопатина. — Москва, 2006. — 60 с.

6. Шепелов М.А. Основания криминализации мошенничества в сфере компьютерной информации / М.А. Шепелов // Актуальные вопросы современной науки. — 2015. — № 41. — С. 150–159.

7. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы : автореф. дис. ... канд. юрид. наук : 12.00.08 / Т.Л. Тропина. — Владивосток, 2005. — 26 с.

8. Хилюта В.В. Уголовная ответственность за хищения с использованием компьютерной техники / В.В. Хилюта // Журнал российского права. — 2014. — № 3. — С. 111–118.

9. Иванченко Р.Б. Проблемы квалификации мошенничества в сфере компьютерной информации / Р.Б. Иванченко, А.Н. Малышев // Вестник Воронежского института МВД России. — 2014. — № 1. — С. 194–200.

10. Петров С.А. Особенности квалификации хищений, совершенных с использованием компьютерной техники / С.А. Петров // Российский следователь. — 2008. — № 15. — С. 22–25.

11. Шебанов Д.В. О некоторых проблемах квалификации мошенничества в сфере компьютерной информации / Д.В. Шебанов, Л.С. Терещенко // Теория и практика общественного развития. — 2014. — № 4. — С. 240–242.

12. Лопашенко Н.А. Законодательная реформа мошенничества: вынужденные вопросы и вынужденные ответы / Н.А. Лопашенко. — DOI: 10.17150/1996-7756.2015.9(3).504-513 // Криминологический журнал Байкальского государственного университета экономики и права. — 2015. — Т. 9, № 3. — С. 504–513.

13. Медведев С.С. Мошенничество в сфере высоких технологий : автореф. дис. ... канд. юрид. наук : 12.00.08 / С.С. Медведев. — Краснодар, 2008. — 21 с.

14. Зыков Д.А. Виктимологические аспекты предупреждения компьютерного мошенничества : автореф. дис. ... канд. юрид. наук : 12.00.08 / Д.А. Зыков. — Нижний Новгород, 2002. — 27 с.

15. Безверхов А.Г. Отзыв на диссертацию С.А. Петрова «Хищение чужого имущества или приобретение права на него путем обмана: уголовно-правовая оценка и совершенствование правовой регламентации» / А.Г. Безверхов. — URL: http://www.agprf.org.

16. Гладких В. Компьютерное мошенничество: а были ли основания его криминализации? / В. Гладких // Российский следователь. — 2014. — № 22. — С. 25–31.

17. Шергин Р.Ю. Уголовная ответственность за компьютерное мошенничество: новое не всегда лучшее / Р.Ю. Шергин // Законность. — 2017. — № 5. — С. 47–49.

18. Елисеев С.А. Преступления против собственности в истории уголовного законодательства России : дис. ... д-ра юрид. наук : 12.00.08 / С.А. Елисеев. — Томск, 1999. — 337 с.

19. Архипов А.В. Ответственность за хищение безналичных и электронных денежных средств: новеллы законодательства / А.В. Архипов // Уголовное право. — 2018. — № S3. — С. 4–9.

20. Goodman M. Future Crimes: How Our Radical Dependence on Technology Threatens Us All / M. Goodman. — Canada : Anchor Canada, 2015. — 608 p.

21. Marbeth-Kubicki A. Computer- und Internetstrafrecht / A. Marbeth-Kubicki. — München : Verlag C.H. Beck, 2010. — 200 S.

22. Hilgendorf E. Computer- und Internetstrafrecht / E. Hilgendorf, B. Valerius. — Heidelberg : Springer, 2012. — 244 S.

23. Goodman M. Future Crimes / M. Goodman. — Canada : Anchor Canada, 2016. — 608 p.

24. Repräsentative Bevölkerungsbefragung im Rahmen des BaSiD-Teilvorhabens. Sicherheitsgefährdungen durch Kriminalität. Methodenbericht / S. Schiel, C. Dickmann, R. Gilberg, A. Malina. — Bonn, 2013. — 22 S.

25. Боровых Л.В. Проблема квалификации хищения с использованием банковских карт / Л.В. Боровых, Е.А. Корепанова // Российский юридический журнал. — 2014. — № 2. — С. 84–86.

26. Кочои С.М. Новые нормы о мошенничестве в УК РФ: особенности и отличия / С.М. Кочои // Криминологический журнал Байкальского государственного университета экономики и права. — 2013. — № 4. — С. 104–110.

27. Тимошин Н.В. Новые нормы о мошенничестве в УК РФ: рекомендации по применению / Н.В. Тимошин // Уголовный процесс. — 2013. — № 1. — С. 10–15.

REFERENCES

1. Yani P.S. Specific Types of Fraud. *Zakonnost' = Legality*, 2015, no. 8, pp. 9–12. (In Russian).

2. Alferova Yu.O., Dement'ev O.M. Problems of Qualification of Computer Fraud. *Science Time*, 2014, no. 7, pp. 11–16. (In Russian).

3. Chernyakova A.V. Actual Aspects of the Criminal Liability for Thefts Committed with the Use of Information and Communication Technologies. *Yuridicheskaya nauka i pravookhranitel'naya praktika = Legal Science and Law Enforcement Practice*, 2019, no. 3 (49), pp. 124–430. (In Russian).

4. Tretyak M.I. The Problem of Legal Regulation of Hi-Tech Property Crimes. *Zakonnost' = Legality*, 2016, no. 7 (981), pp. 41–46. (In Russian).

5. Lopatina T.M. *Kriminologicheskie i ugolovno-pravovye osnovy protivodeistviya komp'yuternoi prestupnosti. Avtoref. Dokt. Diss.* [Criminological and Criminal Law Basis of Counteracting Cybercrimes. Doct. Diss. Thesis]. Moscow, 2006. 60 p.

6. Shepelov M.A. Basics for the criminalization of fraud in the sphere of computer information. *Aktual'nye voprosy sovremennoi nauki = Actual Issues of Modern Science,* 2015, no. 41, pp. 150–159. (In Russian).

7. Tropina T.L. *Kiberprestupnost': ponyatie, sostoyanie, ugolovno-pravovye mery bor'by. Avtoref. Kand. Diss.* [Cybercrimes: Concept, Condition, Criminal Law Counteraction Measures. Cand. Diss. Thesis]. Vladivostok, 2005. 26 p.

8. Khilyuta V.V. Criminal Liability for Theft with the use of Computer Equipment. *Zhurnal rossiiskogo prava = Journal of Russian Law*, 2014, no. 3, pp. 111–118. (In Russian).

9. Ivanchenko R.B., Malyshev A.N. The problems of qualification of fraud in the sphere of computer information. *Vestnik Voronezhskogo instituta MVD Rossii = Vestnik of Voronezh Institute of Ministry of the Interior of Russia*, 2014, no. 1, pp. 194–200. (In Russian).

10. Petrov S.A. Specific features of the qualification of thefts committed with the aid of computer equipment. *Rossiiskii sledovatel' = Russian Investigator,* 2008, no. 15, pp. 22–25. (In Russian).

11. Shebanov D.V., Tereshchenko L.S. Concerning Some Problems of Fraud Classification in the Computer Information Field. *Teoriya i praktika obshchestvennogo razvitiya = Theory and Practice of Social Development*, 2014, no. 4, pp. 240–242. (In Russian).

12. Lopashenko N.A. The Legislative Reform of Fraud: Forced Questions and Forced Answers. *Kriminologicheskii zhurnal Baikal'skogo gosudarstvennogo universiteta ekonomiki i prava = Criminology Journal of Baikal National University of Economics and Law*, 2015, vol. 9, no. 3, pp. 504–513. DOI: 10.17150/1996-7756.2015.9(3).504-513. (In Russian).

13. Medvedev S.S. *Moshennichestvo v sfere vysokikh tekhnologii. Avtoref. Kand. Diss.* [Fraud in the Sphere of High Technologies. Cand. Diss. Thesis]. Krasnodar, 2008. 21 p.

14. Zykov D.A. *Viktimologicheskie aspekty preduprezhdeniya komp'yuternogo moshennichestva*. *Avtoref. Kand. Diss.* [Victimological Aspects of Computer Fraud Prevention. Cand. Diss. Thesis]. Nizhny Novgorod, 2002. 27 p.

15. Bezverkhov A.G. *Otzyv na dissertatsiyu S.A. Petrova «Khishchenie chuzhogo imushchestva ili priobretenie prava na nego putem obmana: ugolovno-pravovaya otsenka i sovershenstvovanie pravovoi reglamentatsii»* [Review of the Dissertation. Petrov S.A. «Theft of Another's Property or the Acquisition of the Right to it by Deception: a Criminal-legal Assessment and Improvement of the Legal Regulation»]. Available at: http://www.agprf.org. (In Russian).

16. Gladkikh V.I. Computer fraud: if there were grounds for criminalization thereof? *Rossiiskii sledovatel' = Russian Investigator*, 2014, no. 22, pp. 25–31. (In Russian).

17. Shergin R.Yu. Criminal Liability for Cyber-crime: the New is not Always the Best. *Zakonnost' = Legality*, 2017, no. 5, pp. 47–49. (In Russian).

18. Eliseev S.A. *Prestupleniya protiv sobstvennosti v istorii ugolovnogo zakonodatel'stva Rossii. Dokt. Diss.* [Crimes Against Property under the Criminal Legislation of Russia. Doct. Diss.]. Tomsk, 1999. 337 p.

19. Arkhipov A.V. Liability for the theft of non-cash money and electronic money: legislative novels. *Ugolovnoe pravo = Criminal Law*, 2018, no. S3, pp. 4–9. (In Russian).

20. Goodman M. *Future Crimes: How Our Radical Dependence on Technology Threatens Us All*. Canada, Anchor Canada, 2015. 608 p.

21. Marbeth-Kubicki A. *Computer- und Internetstrafrecht*. München, Verlag C.H. Beck, 2010. 200 S.

22. Hilgendorf E., Valerius B. *Computer- und Internetstrafrecht*. Heidelberg, Springer, 2012. 244 S.

23. Goodman M. *Future Crimes*. Canada, Anchor Canada, 2016. 608 p.

24. Schiel S., Dickmann C., Gilberg R., Malina A. *Repräsentative Bevölkerungsbefragung im Rahmen des BaSiD-Teilvorhabens. Sicherheitsgefährdungen durch Kriminalität. Methodenbericht*. Bonn, 2013. 22 S.

25. Borovykh L.V., Korepanova E.A. A Problem of Qualification of Theft with the Use of Bank Card. *Rossiiskii yuridicheskii zhurnal = Russian Law Journal*, 2014, no. 2, pp. 84–86. (In Russian).

26. Kochoi S.M. New Regulations on Fraud in the Criminal Code of the Russian Federation: Special Features and Distinctions. *Kriminologicheskii zhurnal Baikal'skogo gosudarstvennogo universiteta ekonomiki i prava = Criminology Journal of Baikal National University of Economics and Law*, 2013, no. 4, pp. 104–110. (In Russian).

27. Timoshin N.V. New Regulations on Fraud in the Criminal Code of the Russian Federation: Recommendations. *Ugolovnyi protsess = Criminal Procedure*, 2013, no. 1, pp. 10–15. (In Russian).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Третьяк Мария Ивановна — доцент кафедры уголовного права и процесса Северо-Кавказского федерального университета, кандидат юридических наук, доцент, г. Ставрополь, Российская Федерация; e-mail: mariya62@mail.ru.

Рябова Лилия Викторовна — доцент кафедры уголовного права и процесса Северо-Кавказского федерального университета, кандидат юридических наук, доцент, г. Ставрополь, Российская Федерация; e-mail: liliya.ryabova.63@mail.ru.

ДЛЯ ЦИТИРОВАНИЯ

Третьяк М.И. Различные подходы к оценке способов хищений безналичных денежных средств в условиях современного информационного общества / М.И. Третьяк, Л.В. Рябова. — DOI: 10.17150/2500-4255.2020.14(4).601-612 // Всероссийский криминологический журнал. — 2020. — Т. 14, № 4. — С. 601–612.

INFORMATION ABOUT THE AUTHORS

Tretiak, Maria I. — Ass. Professor, Chair of Criminal Law and Procedure, North-Caucasus Federal University, Ph.D. in Law, Ass. Professor, Stavropol, the Russian Federation; e-mail: mariya62@mail.ru.

Ryabova, Liliya V. — Ass. Professor, Chair of Criminal Law and Procedure, North-Caucasus Federal University, Ph.D. in Law, Ass. Professor, Stavropol, the Russian Federation; e-mail: liliya.ryabova.63@mail.ru.

FOR CITATION

Tretiak M.I., Ryabova L.V. Various approaches to assessing the methods of stealing cashless money in the modern information society. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2020, vol. 14, no. 4, pp. 601–612. DOI: 10.17150/2500-4255.2020.14(4).601-612. (In Russian).