ISSN 2500-4255

Научная статья
УДК 343.71; 343.72
DOI 10.17150/2500-4255.2021.15(5).592-604

ОТЛИЧИТЕЛЬНЫЕ ОСОБЕННОСТИ МЕР ЗАЩИТЫ ОТ КОРЫСТНЫХ КОМПЬЮТЕРНЫХ ПОСЯГАТЕЛЬСТВ НА БЕЗНАЛИЧНЫЕ (ЭЛЕКТРОННЫЕ) ДЕНЕЖНЫЕ СРЕДСТВА В СОВРЕМЕННОМ УГОЛОВНОМ ЗАКОНОДАТЕЛЬСТВЕ БЕЛОРУССИИ И РОССИИ

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

Информация о статье

Дата поступления
6 марта 2021 г.

Дата принятия в печать
3 ноября 2021 г.

Дата онлайн-размещения
25 ноября 2021 г.

Ключевые слова

Дистанционная деятельность; безналичные денежные средства; мошенничество; компьютерные преступления; доступ к компьютерной информации; хищение; кража

Аннотация. Преобладание дистанционного формата деятельности в современных условиях привело к еще большему увеличению объема операций с безналичными (электронными) денежными средствами, что обусловило рост уровня корыстной преступности в виртуальном пространстве. Рассматривая уголовно-правовые меры защиты от корыстных посягательств на безналичные (электронные) денежные средства в компьютерной информационной сфере, автор производит правовой анализ предписаний о корыстных преступных деяниях против собственности и информационной безопасности, получающих отражение в уголовном законодательстве Белоруссии и России. Обращается особое внимание на отличительные особенности мер защиты от корыстных компьютерных преступлений в отношении безналичных (электронных) денежных средств в современном уголовном законодательстве Белоруссии и России. Отмечается, что в действующем уголовном законодательстве Белоруссии дифференциация уголовной ответственности осуществляется с учетом единых критериев (способа и размера имущества) в рамках одного состава трех преступлений гл. 24 и 31 Уголовного кодекса Республики Беларусь. В российском законодательстве дифференциация уголовной ответственности осуществляется с учетом трех критериев (размера, вида денежных средств или способа хищения) в рамках пяти составов преступлений гл. 21 и 28 Уголовного кодекса Российской Федерации. В статье отдельно указывается, что применение дифференцированного подхода к закреплению ответственности за компьютерные хищения безналичных денежных средств в нормах российского уголовного закона приводит, во-первых, к серьезным трудностям при установлении форм, отличительных критериев таких хищений, а во-вторых, к различию в применении более строгих (менее строгих) мер наказания за тождественные деяния. На основании детального сравнительного анализа современного уголовного законодательства Белоруссии и России в компьютерной сфере в части корыстных посягательств на безналичные (электронные) денежные средства делается вывод о применении в российском законе положения, которое позволяло в полном объеме учитывать различные особенности дистанционного способа посягательства на безналичные (электронные) денежные средства и применять единые критерии для дифференциации уголовной ответственности в рамках одного состава преступления, например в виде совершения хищения в сфере компьютерной информации, способ совершения которого детально описан в одной из норм о компьютерных преступлениях в ст. 159.6 Уголовного кодекса России.

Original article

SPECIFIC FEATURES OF PROTECTION AGAINST COMPUTER-AIDED CRIMINAL INFRINGEMENTS ON CASHLESS (ELECTRONIC) FUNDS IN CONTEMPORARY CRIMINAL LEGISLATIONS OF BELARUS AND RUSSIA

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

Article info

Received
2021 March 6

Abstract. The dominance of a distance form of interactions in modern conditions resulted in an increase in operations with cashless (electronic) funds, which led to a growth of the number of acquisitive cybercrimes. The author examines criminal law measures of protecting cashless (electronic) funds against criminal infringements in the

ISSN 2500-4255

Accepted
2021 November 3
Available online
2021 November 25

Keywords
Distance activities; cashless funds; fraud; cybercrime; access to computer information; larceny; theft

cybersphere and conducts legal analysis of regulations on acquisitive crimes against property and information security reflected in criminal legislations of Belarus and Russia. Special attention is paid to the characteristic features of protection measures against acquisitive cybercrimes involving cashless (electronic) funds in modern criminal legislations of Belarus and Russia. Current Belarus legislation differentiates criminal liability using unified criteria (method and property size) within the same corpus delicti of three crimes in Ch. 24 and 31 of the Criminal Code of the Republic of Belarus. In the Russian legislation, the differentiation of criminal liability is based on three criteria (size, type of money or method) within five corpora delicti in Ch. 21 and 28 of the Criminal Code of the Russian Federation. The author specifically states that the use of such a differentiation approach in determining liability for online theft of cashless money in the norms of Russian criminal law leads, firstly, to considerable difficulties in determining the forms and specific criteria of such theft and, secondly, to the application of more (or less) severe measures of punishment for identical crimes. Using a detailed comparative analysis of modern criminal legislations of Belarus and Russia regarding online criminal infringements against cashless (electronic) money, the author draws a conclusion on the use of regulations in the Russian law that would make it possible to fully take into account various specific features of online infringements on cashless (electronic) money and to apply unified criteria for the differentiation of criminal liability within one corpus delicti, for example, in the form of theft in the sphere of computer information whose modus operandi is thoroughly described in one of the norms on computer crimes in Art. 159.6 of the Criminal Code of Russia.

В связи с многократным увеличением объема всевозможных операций с безналичными (электронными) денежными средствами в безграничном виртуальном пространстве и стремительным ростом корыстной преступности в области высоких технологий в 2018 г. в Уголовном кодексе России произошло ужесточение уголовной ответственности за хищения в таких формах, как кража и мошенничество в сфере компьютерных технологий, совершенные в отношении безналичных (электронных) денежных средств. На сегодняшний день применение кризисных санитарно-эпидемиологических правил в различных государствах, ограничивающих перемещение людей как внутри определенной страны, так и между странами, преобладание дистанционного формата деятельности в разных сферах приводят к еще большему возрастанию количества операций с безналичными (электронными) денежными средствами и нарастанию уровня[1] корыстной преступности в виртуальном пространстве[2]. Считаем, что в этих условиях особое значение приобретает вопрос выявления эффективности тех или иных предписаний (мер) уголовного законодательства в противодействии корыстным компьютерным посягательствам на безналичные (электронные) денежные средства таких стран, как Белоруссия и Россия, имеющих богатый опыт совместной борьбы с преступностью.

При первом обращении к уголовному законодательству Белоруссии следует констатировать, что, в отличие от УК РФ, в нем отсутствуют специальные положения о корыстных компьютерных посягательствах на безналичные (электронные) денежные средства. В частности, в Уголовном кодексе Республики Беларусь (УК РБ) 1999 г.[3] нормы о корыстных компьютерных преступлениях содержатся в гл. 24 разд. VIII «Преступления против собственности и порядка осуществления экономической деятельности» и гл. 31 разд. XII «Преступления против информационной безопасности». В первом случае интересы владельцев денежных средств выступают основным объектом, а во втором — только дополнительным. В гл. 24 УК РБ рассматривается общее определение хищения и выделяются как традиционные его формы, так и хищения, совершенные с использованием компьютерной техники. Уголовная ответственность за само-

[1] В России за 2020 г. наибольшее распространение получили мошенничества в сфере информационно-телекоммуникационных технологий или компьютерной информации, на них приходится около 70 % всех хищений, совершенных путем обмана или злоупотребления доверием (+73,4 %, 237,1 тыс.). При совершении 25,8 тыс. (42,4 %) мошенничеств использовались электронные средства платежа. См.: Генеральная прокуратура РФ. Портал правовой статистики. URL: http://crimestat.ru/analytics.

[2] Global operation sees a rise in fake medical products related to COVID-19. URL: https://www.interpol.int/en/News-and-Events/News/2020/Global-operation-sees-a-rise-in-fakemedical-products-related-to-COVID-19.

[3] Уголовный кодекс Республики Беларусь 1999 г. состоит из Общей части (разд. I–V, гл. 1–16) и Особенной части (разд. VI–XV, гл. 17–37). См.: Уголовный кодекс Республики Беларусь от 9 июля 1999 г. № 275-З. URL: https://online.zakon.kz/Document/?doc_id=30414984.

стоятельную форму хищения с использованием компьютерной техники[4] [1, с. 153–158] в зависимости от вида дистанционного способа его совершения и размера похищенного имущества (ущерба) устанавливается в ст. 212 гл. 24 УК РБ [2], в ч. 1 которой закреплено хищение имущества путем изменения (введения) информации, а в ч. 2 — это же деяние, сопряженное с несанкционированным доступом к компьютерной информации. В ст. 216 УК РБ, предусматривающей уголовную ответственность за традиционное преступление против собственности в виде причинения имущественного ущерба в значительном и крупном размере, не связанного с хищением, одновременно с обманом и злоупотреблением доверием закрепляется такой способ воздействия на компьютерную информацию, как модификация. Следует сразу же отметить: предусмотрев уголовную ответственность за названные виды преступлений в зависимости от способа их совершения и размера похищенного имущества (причиненного ущерба), хотя и без дифференциации ответственности с учетом разновидностей предмета преступления, законодатель таким образом закрепил в УК РБ меры защиты владельцев (собственников) безналичных (электронных [3]) денежных средств, позволяющие правоприменителю при преступном завладении чужим имуществом, в том числе и безналичными (электронными) денежными средствами в крупном и особо крупном размере применять к виновным лицам более строгие меры воздействия, чем за аналогичные преступные деяния, не причинившие ущерб в указанных размерах. Кроме названных предписаний гл. 24, в гл. 31 УК РБ закреплена норма (ст. 349) о несанкционированном доступе к компьютерной информации, в ч. 2 которой предусмотрена ответственность за квалифицированный вид указанного деяния, совершенного из корыстной заинтересованности, наказуемый менее строго[5], чем преступные деяния, содержащиеся в ст. 212 и 216 УК РБ.

Следовательно, в УК РБ наряду со способом преступления крупный, особо крупный размер хищения чужого имущества, без выделения безналичных (электронных) денежных средств в качестве особой его разновидности, с использованием компьютерной техники является одним из критериев применения более строгих мер воздействия; а значительный, крупный размер причинения ущерба без признаков хищения путем модификации компьютерной информации выступает одним из критериев признания деяния преступным либо назначения более строгой меры наказания.

При установлении особенностей мер защиты имущественных интересов собственников безналичных (электронных) денежных средств особую значимость имеет вопрос об особенностях способов совершения корыстных компьютерных преступлений, одновременно предусмотренных в гл. 24 и 31 УК РБ, и мерах наказаний, установленных за их совершение. В ч. 1 ст. 212 УК Белоруссии способ совершения преступления представлен в виде двух самостоятельных разновидностей: во-первых, в «изменении информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных»; во-вторых, во «введении в компьютерную систему ложной информации».

В ст. 216 УК Белоруссии о причинении ущерба без признаков хищения модификация одновременно с обманом (злоупотреблением доверием) указывается без выделения таких способов, как изменение и введение (внесение) компьютерной информации, исключающие контакт с потерпевшим. Примечательным является то, что две эти разновидности[6] модификации компьютерной информации одновременно признаются способами совершения самостоятельного преступления, закрепленного в ст. 350 гл. 31 УК РБ о преступлениях против информационной безопасности, при обязательном условии отсутствия в этом деянии признаков преступлений против собственности. Следовательно, исходя из предписаний ст. 212, 216 и 350 УК РБ при наличии признаков преступлений, предусмотренных ст. 212 и 216, модификация компьютерной информации оценивается как преступление против собственности и, наоборот, при их отсутствии — как преступление против информационной безопасности (ст. 350 УК РБ).

[4] Понятия форм хищения в виде кражи, грабежа, разбоя, вымогательства, мошенничества, присвоения и растраты в ч. 1 ст. 205–209, 211 гл. 24 УК РБ в целом не отличаются от предусмотренных таких же преступлений в УК РФ, т.е. использования высоких технологий как способа совершения преступления в основных и квалифицированных составах этих преступлений не содержится.

[5] В частности, согласно санкции ст. 349 УК РБ, максимальный размер наиболее строгого наказания в виде лишения свободы — до двух лет, а за компьютерное хищение имущества по ч. 1 ст. 212 УК РФ — до трех лет.

[6] В УК РФ ввод информации не выступает способом модификации компьютерной информации.

Мошенничество путем обмана или злоупотребления доверием, уголовная ответственность за которое предусматривается в ст. 209 УК РБ[7], если оно совершено путем модификации компьютерной информации, оценивается как компьютерное хищение, закрепленное в ст. 212 УК РБ.

Наряду с модификацией компьютерной информации действия по уничтожению (приведению в непригодное состояние компьютерной информации или программы), блокированию, копированию информации выступают способами совершения умышленных преступлений, предусмотренных ст. 350 («Модификация компьютерной информации»), ст. 351 («Компьютерный саботаж»), ст. 352 («Неправомерное завладение компьютерной информацией»), или последствием неосторожного преступления, содержащегося в ст. 350 гл. 31 УК РБ. С учетом размера[8] санкций умышленное уничтожение, блокирование компьютерной информации, совершенное из корыстных побуждений, будет оцениваться по ч. 1 ст. 351 УК РБ, а если оно сопряжено с несанкционированным доступом к компьютерной информации и не повлекло причинения имущественного ущерба в особо крупном размере — по ч. 2 этой статьи. Если преступление, предусмотренное ст. 352 УК РБ («Неправомерное завладение компьютерной информацией»), выступает способом совершения преступлений против собственности, то с учетом размера санкций ч. 1 ст. 352 и ч. 1 ст. 212 (216) УК РБ оно охватывается основными составами этих преступлений против собственности. Модификация компьютерной информации, совершенная из корыстных побуждений, как уже было отмечено, полностью оценивается как преступление против собственности (гл. 24 УК РБ). Иные действия в виде разработки, использования либо распространения вредоносных программ, закрепленные в ст. 354 УК РБ, рассматриваются только как компьютерное преступление. Если же оно выступает способом совершения преступлений против собственности, то с учетом размера санкций ч. 1 ст. 354 и ч. 1 ст. 212 (216) УК РБ оно охватывается основными составами этих преступлений против собственности.

В ч. 2 ст. 212 УК РБ отягчающим обстоятельством признается совершение компьютерного хищения, если оно «сопряжено с несанкционированным доступом к компьютерной информации»[9] [4, с. 85; 5, с. 16; 6, с. 46–54], одновременно в ч. 2 ст. 349 гл. 31 УК РБ устанавливается ответственность за несанкционированный доступ к компьютерной информации[10] [7, с. 41; 8, с. 22], совершенный из корыстной заинтересованности[11]. На наш взгляд, эти нормы соотносятся между собой как общая (ч. 2 ст. 349 УК РБ) и специальная (ч. 2 ст. 212 УК РБ). В соответствии с правилами квалификации общей и специальной норм, сформулированных в ч. 2 ст. 42 УК РБ, к преступлениям против собственности, совершенным путем использования компьютерной техники с корыстной целью, может быть применена только ч. 2 ст. 212 УК РБ. В ст. 216 УК РБ («Причинение имущественного ущерба без признаков хищения»), наоборот, нет указания на этот способ, но в санкции этой статьи предусматривается более строгое наказание, чем в ч. 2 ст. 349 УК РБ. Следовательно, и в этом случае применение данной нормы также не требуется.

Сравнительный анализ способов и мер наказаний за компьютерные преступления, предусмотренные гл. 24 и 31 УК Белоруссии, показывает, что компьютерным преступным деяниям против собственности, обозначенным в гл. 24 УК РБ, присущи строго определенные способы воздействия на компьютерную информацию (в виде изменения или введения компьютерной информации), отличительная особенность которых состоит в следующем:

[7] Размер наказания в виде лишения свободы установлен по ч. 1 сроком до трех лет, по ч. 2 — до четырех лет, по ч. 3 — от двух до семи лет, по ч. 4 — от трех до десяти лет.

[8] За умышленное уничтожение, блокирование компьютерной информации в ч. 1 ст. 351 УК РБ установлено максимальное наказание в виде лишения свободы на срок от одного года до пяти лет; в ч. 1 ст. 212 (216) УК РБ — лишение свободы на срок до трех лет; в ч. 2 ст. 351 — лишение свободы на срок от трех до десяти лет; в ч. 3 ст. 212 — лишение свободы на срок от двух до семи лет; в ч. 2 ст. 216 — лишение свободы на срок до пяти лет.

[9] Субъектом хищения, сопряженного с несанкционированным доступом к компьютерной информации, выступает не только лицо, не имеющее доступ к информации, но и лицо, имеющее такой доступ, но осуществляющее его с нарушением установленного порядка доступа либо выходящее за рамки идентификации.

[10] По мнению российских специалистов, данный термин следует признать более точным при характеристике запрещенного уголовным законом действия, поскольку правомерность доступа к информации фактически означает его санкционированность (разрешенность) обладателем информации.

[11] Кроме этого, в ч. 2 ст. 350 УК РБ — за модификацию компьютерной информации, сопряженную с несанкционированным доступом к компьютерной информации без указания корыстного мотива.

1. При совместном совершении действий по модификации компьютерной информации и несанкционированному доступу к компьютерной информации (неправомерному завладению компьютерной информацией или разработке, использованию (распространению) вредоносных программ) не образуется совокупность преступлений гл. 24 и 31 УК РБ, данные действия оцениваются как единые преступления, предусмотренные гл. 24 УК РБ. Например, последовательность совершаемых преступных действий по неправомерному доступу к информации, получению (копированию) информации, проникновению в систему с использованием этой информации, совершению операций по изменению (введению) информации, приводящая к изъятию определенного имущества, в соответствии с законом (ч. 2 ст. 212 УК РБ) оценивается в судебной практике как единое преступление[12].

2. В случае одновременного совершения с модификацией компьютерной информации таких действий, как уничтожение[13], блокирование[14] компьютерной информации, наоборот, возникает необходимость в дополнительном применении предписаний гл. 31 УК Белоруссии (ст. 351 «Компьютерный саботаж»). Умышленное уничтожение, блокирование компьютерной информации, совершенные из корыстных побуждений, оцениваются исключительно как компьютерное преступление, предусмотренное гл. 31 УК РБ (ч. 1 и 2 ст. 351), в случае отсутствия воздействия на компьютерную информацию в виде модификации.

3. В гл. 24 УК Белоруссии ужесточение уголовной ответственности происходит за хищение путем модификации компьютерной информации в случаях, когда оно сопряжено с несанкционированным доступом к компьютерной информации (ч. 2 ст. 212), в гл. 31 происходит усиление ответственности за такие действия, как умышленное уничтожение (приведение в непригодное состояние) и блокирование компьютерной информации (ч. 1 ст. 351), а также в случае, когда они сопряжены с несанкционированным доступом к компьютерной системе либо сети (ч. 2 ст. 351) [9, с. 112; 10].

Все названные особенности являются основанием для утверждения, что признание в УК Белоруссии хищения чужого имущества путем использования компьютерной техники самостоятельной формой хищения с присущими только ей специфическими признаками исключает возможность отождествления ее признаков с традиционными формами хищения (например, с тайным, обманным хищением, присвоением и др.) и компьютерными преступлениями против информационной безопасности. И, самое главное, позволяет одновременно регулировать общественные отношения, возникающие по поводу наличных и (или) безналичных денежных средств с учетом различных особенностей дистанционного способа совершения преступления (либо их сочетания) и размера похищенного имущества, без создания многочисленных норм о корыстных компьютерных посягательствах на безналичные денежные средства. Размеры санкций, установленные за компьютерные преступления против собственности, в основном являются более строгими, чем за преступления против информационной безопасности, и не отличаются от традиционных преступлений против собственности в форме кражи и мошенничества[15]. Наиболее строгое наказание в виде лишения свободы установлено за компьютерное хищение в крупном и особо крупном размере. Уничтожение, блокирование компьютерной информации, в отличие от УК РФ, признаются только способами совершения компьютерного преступления в виде саботажа (гл. 31 УК РБ).

В Уголовном кодексе РФ 1996 г. до 2012 г. собственность в сфере высоких технологий защищалась нормами о традиционных корыстных посягательствах против собственности и (или) о преступлениях в сфере компьютерной

[12] Приговор Центрального районного суда г. Минска по уголовному делу от 25 августа 2020 г. URL: court.gov.by/ru/minskij/gorodskoj/sud/press_sluzhba.

[13] Допускаем, что этот способ воздействия на компьютерную информацию может рассматриваться как разновидность модификации компьютерной информации в качестве способа совершения преступлений либо признаваться приготовительными действиями к преступлениям, предусмотренным гл. 24 УК РБ, или как самостоятельный способ совершения преступлений, содержащихся в гл. 31 УК РБ.

[14] Блокирование компьютерной информации по УК Белоруссии может признаваться приготовительными действиями к преступлениям против собственности в сфере компьютерной информации или выступать в качестве альтернативного способа самостоятельного преступления, предусмотренного гл. 31 УК РБ.

[15] Хотя минимальный размер наказания за компьютерное хищение в особо крупном размере гораздо выше, чем за традиционные формы хищения. Полагаем, что в случае компьютерного хищения в особо крупном (сверхкрупном) размере безналичных денежных средств имеется возможность назначить более строгое наказание, чем за традиционные хищения.

информации без специального выделения разновидности деяний, совершаемых в отношении безналичных (электронных) денежных средств[16] [11; 12, с. 111–117]. Лишь в 2012 г.[17] в гл. 21 УК РФ в числе специальных разновидностей хищений в форме мошенничества (включая и мошенничества в сфере компьютерной информации) впервые было предусмотрено положение о защите от посягательств в основном на безналичные (электронные) денежные средства в виде мошенничества с использованием платежных карт (ст. 159.3). Затем в 2018 г. в связи с вновь внесенными изменениями[18] в гл. 21 УК РФ появились новые специальные положения о защите интересов владельцев безналичных (электронных) денежных средств, которые обусловили в этой главе наряду с традиционным критерием (размером денежных средств) применение нового критерия для дифференциации ответственности в виде разновидности денежных средств. На сегодняшний день среди норм о корыстных компьютерных преступлениях гл. 21 и 28 УК РФ имеются:

1. Предписания о преступлениях, предметом которых выступают безналичные (электронные) денежные средства, в виде квалифицированного состава традиционной кражи (п. «г» ч. 3 ст. 158), специального вида мошенничества с использованием электронных средств платежа (ст. 159.3), квалифицированного состава мошенничества в сфере компьютерной информации (п. «в» ч. 3 ст. 159.6[19] [13, с. 32]).

2. Предписания о преступлениях, предметом которых могут выступать наличные денежные средства и иное имущество, исключающее безналичные (электронные) денежные средства[20] [14, с. 12–17], в качестве основного и квалифицированного вида мошенничества в сфере компьютерной информации (ч. 1 и 2 ст. 159.6).

3. Предписания о преступлениях, предметом которых, наряду с наличными денежными средствами и иным имуществом, могут выступать и безналичные денежные средства, в виде создания, использования и распространения вредоносных компьютерных программ или неправомерного доступа к компьютерной информации, совершенных из корыстной заинтересованности (ч. 2 ст. 272[21] и 273 УК РФ), а также традиционных корыстных преступлений против собственности, предметом которых, наряду с наличными денежными средствами и иным имуществом, могут выступать и безналичные денежные средства.

Важно заметить, что выделение специальных посягательств на безналичные денежные средства с использованием компьютерных технологий в различных нормах гл. 21 УК РФ и использование разных подходов к ужесточению уголовной ответственности за их совершение привели к появлению противоречивой ситуации — признание основанием ужесточения ответственности в одном случае размера и вида денежных средств (ст. 159.3), а в другом — только вида похищенных средств (п. «г» ч. 3 ст. 158, п. «в» ч. 3 ст. 159.6), т.е. за мелкое и крупное хищение безналичных (электронных) денежных средств могут быть назначены одинаковые сроки наказания. В частности, за квалифицированные виды тайного (п. «г» ч. 3 ст. 158 УК РФ) и мошеннического (п. «в» ч. 3 ст. 159.6 УК РФ) хищений безналичных (электронных) денежных средств независимо от размера (мелкий либо крупный) может быть назначено наказание до шести лет лишения свободы. За мошенническое хищение с использованием электронного платежного средства[22] такое наказание может быть назначено лишь в случае хищения безналичных денежных средств в крупном размере. Кроме

[16] Развитие уголовного законодательства России осуществлялось в направлении более широкого понимания традиционных норм о преступлениях против собственности в форме мошенничества и кражи.

[17] О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации : федер. закон от 29 нояб. 2012 г. № 207-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_138322.

[18] О внесении изменений в Уголовный кодекс Российской Федерации : федер. закон от 23 апр. 2018 г. № 111-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_296451.

[19] Выделение квалифицированного вида компьютерного мошенничества в отношении безналичных (электронных) денежных средств в ст. 159.6 УК РФ, по мнению Е.А. Русскевича, привело к аннулированию ч. 1 и ч. 2 этой статьи, поскольку этот вид компьютерного преступления, так или иначе, всегда посягает на безналичные или электронные деньги.

[20] Некоторые современные авторы выделяют отдельные разновидности преступлений против собственности, предметом которых выступают в одном случае вещи, а в другом — электронные денежные средства.

[21] Приговор Марксовского городского суда Саратовской области № 1-40/2020 от 10 июля 2020 г. по уголовному делу № 1-40/2020. URL: https://sudact.ru/regular/doc/yJaz4xdlOxLQ.

[22] Либо за квалифицированные виды хищений (ст. 159, 159.1, 159.2, 159.5 и 160 УК РФ) наличных и безналичных денежных средств.

этого, имеется возможность признания мошенничества с использованием электронного средства платежа (ч. 1 ст. 159.3 УК РФ) в соответствии со ст. 158.1 УК РФ и ст. 7.27 КоАП РФ мелким хищением либо административным правонарушением. В отношении тайного и мошеннического хищения безналичных (электронных) денежных средств (п. «г» ч. 3 ст. 158, п. «в» ч. 3 ст. 159.6 УК РФ) такая возможность исключается.

Закрепление в гл. 21 и 28 УК РФ как традиционных корыстных преступлений, так и их специальных видов, предметом которых выступают безналичные (электронные) денежные средства, приводит к необходимости установления характерных особенностей способов их совершения. Предмет в виде безналичных (электронных) денежных средств предполагает дистанционный способ управления денежными средствами, который может осуществляться как без участия самого собственника (владельца)[23] в процессе преступного завладения средствами, так и с его участием. Отличительные признаки исключающего любое участие собственника дистанционного способа отражены в законе: в одном случае в виде квалифицированного вида традиционного тайного хищения — кражи, в другом — квалифицированного специального вида хищения — компьютерного мошенничества, а в третьем — специальной разновидности традиционного хищения — мошенничества. Дистанционный способ хищения, указанного в ч. 1 ст. 159.3 УК РФ, характерен как для менее (ст. 158.1, ч. 1 и 2 ст. 159.3 УК РФ), так и для более (ч. 3 и 4) наказуемых его видов и определяется как мошенничество[24] [15–17] с использованием электронных средств платежа без указания конкретных традиционных мошеннических способов [18]. Исходя из общего определения мошенничества, содержащегося в ст. 159 УК РФ, способами совершения рассматриваемого в ст. 159.3 хищения могут выступать обман или злоупотребление доверием. Хотя, если обратиться к ранее действовавшему законодательству и судебной практике, следует отметить, что с 2012 г. в законе, а затем с 2017 по 2020 г. в судебных разъяснениях основным способом его совершения признавался только обман[25] [19; 20], содержание которого состояло в обманном воздействии на уполномоченных лиц различных организаций в процессе перечисления денежных средств виновным лицом с помощью принадлежащего другому лицу электронного средства платежа за товар (работу (услугу)) в отсутствие владельца этих денежных средств[26] [21]. В настоящее время в связи с изменениями, внесенными в уголовный закон в 2018 г., Верховный Суд РФ с сентября 2020 г.[27] такое хищение с использованием электронного средства платежа оценивает как тайное хищение в форме кражи[28] (п. «г» ч. 3 ст. 158) [17; 22], а содержание обманного способа мошенничества, предусмотренного ст. 159.3 УК РФ, конкретно в судебной практике пока на сегодняшний момент не определено[29].

Дистанционный способ совершения двух строго наказуемых хищений в виде кражи и компьютерного мошенничества, предусмотренных п. «г» ч. 3 ст. 158 и п. «в» ч. 3 ст. 159.6 УК РФ, непосредственно в законе не конкретизируется, однако, согласно ч. 1 и п. «г» ч. 3 ст. 158 УК РФ, такой способ хищения определяется как тайный, не включающий признаков

[23] Например, продавец (уполномоченное лицо) только присутствует при оплате виновным лицом товара чужими безналичными денежными средствами и передает купленный товар, но перечисление средств осуществляется другим лицом в отсутствие их собственника.

[24] Согласны с мнением многих авторов о том, что использованный термин «мошенничество» в названии ст. 159.3 УК РФ не отражает содержание способа, указанного в ее диспозиции. Единственным термином, отвечающим требованию юридической техники, является «хищение».

[25] В доктрине уголовного права позиция о признании в содеянном мошенничестве отстаивается авторитетным ученым П.С. Яни.

[26] В доктрине уголовного права имелось и другое мнение о том, что к обманному способу совершения преступления (ст. 159.3 УК РФ) следует отнести еще обманное получение необходимой для доступа к счету конфиденциальной информации держателя платежной карты.

[27] Определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 29 сентября 2020 г. № 12-УДП20-5-К6. URL: https://legalacts.ru/sud/opredelenie-sudebnoi-kollegii-po-ugolovnym-delam-verkhovnogo-suda-rossiiskoi-federatsii-ot-29092020-n-12-udp20-5-k6.

[28] Данная позиция Верховного Суда РФ в оценке такого деяния, как кража, была поддержана отдельными авторами, в частности М.А. Филатовой, С.А. Петровым.

[29] Только можно предположить, что к нему, возможно, будут относиться случаи, которые с 2017 г. в судебной практике оценивались как традиционное мошенничество и были связаны с непосредственным воздействием на держателя электронного платежного средства. В этом случае, на наш взгляд, отпадает необходимость в выделении этой нормы в качестве специальной.

преступления, предусмотренного ст. 159.3 УК РФ[30]. В ч. 1 ст. 159.6 УК РФ, в которой способ совершения компьютерного хищения определяется как вмешательство в функционирование информационных средств (сетей) путем ввода, удаления, блокирования, модификации компьютерной информации либо иным образом[31] [23, с. 108–110], не содержится указания на традиционный обманный либо тайный [24, с. 600] способ совершения преступления. Следовательно, отличительная особенность дистанционного способа совершения хищений безналичных (электронных) денежных средств, содержащегося в п. «г» ч. 3 ст. 158[32] [25] и п. «в» ч. 3 ст. 159.6 УК РФ, заключается не в тайном или традиционном обманном способе хищения, а в особом характере воздействия на информацию. В связи с тем что в п. «г» ч. 3 ст. 158 УК РФ конкретно не определяется дистанционный способ, этому квалифицированному виду кражи присущи любые способы воздействия на информацию, а, согласно ч. 1 ст. 159.6 УК РФ, для мошенничества в сфере компьютерной информации, указанного в п. «в» ч. 3 ст. 159.6 УК РФ, характерны способы воздействия на информацию, лишь названные в ч. 1 ст. 159.6 УК РФ [26]. Получается, что к способам тайного хищения (п. «г» ч. 3 ст. 158 УК РФ) необходимо отнести все способы воздействия, за исключением воздействия[33], присущего традиционному и специальным видам мошенничества, содержащимся в ст. 159, 159.3 и 159.6 УК РФ. Согласно действующим разъяснениям высшей судебной инстанции, одна часть деяний с компьютерной информацией, совершаемых виновным лицом путем использования конфиденциальной информации о держателе платежной карты, полученной обманом (злоупотреблением доверием) потерпевшего (держателя платежной карты), либо учетных данных собственника (иного владельца) имущества независимо от способа получения доступа к таким данным, оценивается как тайное вмешательство в форме кражи. Другая часть таких деяний с применением программных (программно-аппаратных) средств оценивается как разновидность компьютерного мошеннического вмешательства. Тогда в целом тайный способ хищения (п. «г» ч. 3 ст. 158 УК РФ) состоит в безобманном[34] использовании принадлежащего другому лицу электронного средства платежа[35], сим-карты[36], конфиденциальной информации о держателе платежной карты, предварительно полученной путем обмана[37] (злоупотребления доверием) потерпевшего (держателя платежной карты), или учетных данных собственника (иного

[30] Согласно этому законодательному положению, в судебной практике дистанционный способ тайного хищения рассматривается как использование конфиденциальной информации держателя платежной карты, переданной виновному лицу самим держателем платежной карты путем его обмана (злоупотребления доверием). См.: О судебной практике по делам о мошенничестве, присвоении и растрате : постановление Пленума Верхов. Суда РФ от 30 нояб. 2017 г. № 48. П. 17. URL: http://www.consultant.ru/document/Cons_doc_LAW_283918.

[31] В доктрине уголовного права есть мнение, что единственным способом совершения компьютерного мошенничества является «ввод» информации, в связи с этим предлагается реформировать норму о данном преступлении.

[32] Нельзя не согласиться с мнением отдельных специалистов, что в этом случае имеется излишняя криминализация хищения безналичных (электронных) денежных средств в виде кражи.

[33] Это обманное или иное воздействие. При обманном воздействии собственник денежных средств под влиянием обмана, совершенного в отношении него виновным лицом, сам осуществляет перечисление денежных средств со своего банковского счета с использованием электронного платежного средства на счет виновного лица. Иное воздействие в этом случае охватывает дистанционные способы, заключающиеся в действиях с манипуляцией (вводом, модификацией и др.) информацией и иным программным вмешательством в информационные системы (сети), характерные для компьютерного мошенничества. См.: Приговор Советского районного суда г. Томска Томской области № 1-25/2019 1-377/2018 от 9 декабря 2019 г. по уголовному делу № 1-275/2018. URL: https://sudact.ru/regular/doc/hktokOrwZgbO ; Приговор Волжского городского суда Волгоградской области № 1-23/2018 1-782/2017 по уголовному делу № 1-23/2018 от 5 февраля 2018 г. URL: https://sudact.ru/regular/doc/uytRBHbkIwC.

[34] Приговор Моршанского районного суда Тамбовской области № 1-121/2020 от 3 июля 2020 г. по уголовному делу № 1-121/2020. URL: https://sudact.ru/regular/doc/01VVEqSdUqda.

[35] Приговор Тобольского городского суда Тюменской области № 1-347/2020 от 30 июля 2020 г. по уголовному делу № 1-347/2020. URL: https://sudact.ru/regular/doc/uuHneWw7CA1J.

[36] Приговор Миллеровского районного суда Ростовской области № 1-242/2020 от 30 июля 2020 г. по уголовному делу № 1-242/2020. URL: https://sudact.ru/regular/doc/XjBQFaqjxbNv.

[37] Приговор Вурнарского районного суда Чувашской Республики по уголовному делу № 1-6/2019 1-90/2018 от 30 января 2019 г. URL: https://rospravosudie.com/act-q/section-acts/sort-date.

владельца) имущества[38] независимо от способа получения доступа к таким данным[39] [26]. Компьютерное мошенничество заключается в любых формах вмешательства, связанного с программным (программно-аппаратным) воздействием на программное обеспечение информационных систем (сетей), нарушающим установленный процесс обработки (хранения, передачи) компьютерной информации[40]. В соответствии с рассмотренными разъяснениями часть деяний, которые ранее признавались компьютерным мошенничеством, стали считаться кражей, а к мошенничеству стал относиться узкий круг деяний, связанных только с воздействием на программные (программно-аппаратные) и другие средства.

Следует заметить, что приведенное распределение деяний между кражей и мошенничеством, содержащимися в п. «г» ч. 3 ст. 158 и п. «в» ч. 3 ст. 159.6 УК РФ, нельзя признать четким, бесспорным, поскольку указание на получение доступа к учетным данным собственника (иного владельца) имущества независимо от его способа в одной разновидности тайного хищения[41] служит основанием для утверждения, что воздействие на программное обеспечение информационных систем (сетей) может являться и его альтернативным способом[42]. Получается, что в законе имеется две нормы, которые с одинаковой степенью точности описывают признаки одного деяния.

Как видно, предложенный в 2018 г. в законе дифференцированный подход к хищениям безналичных (электронных) денежных средств привел к ситуации, когда появилась норма (ст. 159.3 УК РФ), которая не будет в полной мере применяться в судебной практике, а все виды дистанционного способа будут распределяться (оцениваться) между двумя нормами (ст. 158 и 159.6 УК РФ), четкие отличительные критерии которых ни в законе, ни в положениях судебной практики не получили точного отражения. По существу, одному преступному деянию посвящено две нормы закона.

Дистанционный способ с участием самого собственника (иного владельца) в большинстве случаев характерен для таких корыстных преступлений против собственности, как мелкое хищение, грабеж, разбой, традиционные и специальные виды мошенничества [27–29] (за исключением его компьютерного вида), вымогательство. В последнее время среди названных деяний получают широкое распространение мошеннические посягательства путем создания поддельных сайтов различных организаций, интернет-магазинов, использования электронной почты, телефонной связи. Степень их общественной опасности оценивается в пределах санкции за указанные традиционные преступления. Например, когда потерпевший под влиянием обмана (насилия), совершенного в отношении него виновным лицом, сам[43] оформляет распоряжение, а затем на его основании со счета потерпевшего переводятся безналичные денежные средства на счет преступника. Обращает на себя внимание и тот факт, что за все виды обманных

[38] Приговор Краснодарского гарнизонного военного суда Краснодарского края № 1-30/2020 от 30 июля 2020 г. по уголовному делу № 1-30/2020. URL: https://sudact.ru/regular/doc/h7erPsTIg7rB ; Приговор Полярного районного суда Мурманской области № 1-25/2020 от 30 июля 2020 г. по уголовному делу № 1-25/2020. URL: https://sudact.ru/regular/doc/NbvnwB3M0mUE.

[39] О судебной практике по делам о мошенничестве, присвоении и растрате : постановление Пленума Верхов. Суда РФ от 30 нояб. 2017 г. № 48. П. 21. URL: http://www.consultant.ru/document/Cons_doc_LAW_283918. Следует заметить, что разновидность этих деяний до 2017 г. в судебной практике оценивалась как компьютерное мошенничество (ст. 159 УК РФ). Именно этот подход к квалификации деяний, по нашему мнению, был более правильным, так как не возникала необходимость ничем не различающиеся деяния, связанные с «вводом» информации как отдельной разновидностью вмешательства, в одном случае оценивать как кражу, а в другом — как компьютерное мошенничество. Предполагаем, что тайный способ (п. «г» ч. 3 ст. 158 УК РФ) должен состоять в безобманном использовании принадлежащего другому лицу электронного средства платежа, сим-карты или предварительно полученной конфиденциальной информации о держателе платежной карты.

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

[41] Там же. П. 2120.

[42] Например, ситуация, связанная с получением виновным лицом путем копирования данных о собственнике денежных средств с применением специальной вредоносной программы, а затем с осуществлением незаконного доступа к информации и совершением действий по перечислению денежных средств потерпевшего на банковский счет виновного лица, в судебной практике оценивается как кража по п. «г» ч. 3 ст. 158 УК РФ. См.: Приговор Ленинского районного суда г. Саратова Саратовской области № 1-196/2018 от 8 июня 2018 г. по уголовному делу № 1-196/2018. URL: https://sudact.ru/regular/doc/9exBIa5BZaln.

[43] Либо сам преступник, получающий путем насилия конфиденциальную информацию от собственника и в его присутствии совершающий перечисление денежных средств.

и тайных хищений любого чужого имущества, в том числе и безналичных денежных средств, в особо крупном размере устанавливается одинаково строгое наказание в виде лишения свободы до десяти лет.

Для преступлений, закрепленных в ст. 272 и 273 гл. 28 УК РФ, в отличие от преступлений гл. 21, единственным критерием ужесточения уголовной ответственности продолжает оставаться только способ посягательства [30–32]. Например, за создание, использование и распространение вредоносных компьютерных программ, совершенных из корыстной заинтересованности, максимальное наказание может быть назначено в виде лишения свободы сроком до пяти лет, а за неправомерный доступ к компьютерной информации, совершенный по таким же мотивам, — до четырех лет. Видимо, законодатель посчитал, что в этом случае нет необходимости выделять в качестве квалифицирующего признака завладение безналичными (электронными) денежными средствами. При сравнении размера наказаний за корыстные компьютерные преступления в отношении безналичных (электронных) денежных средств (гл. 21 и 28 УК РФ) можно отметить, что за компьютерные хищения безналичных (электронных) денежных средств (гл. 21) устанавливаются более строгие наказания, чем за корыстные деяния, предусмотренные гл. 28 УК РФ, поэтому совокупность этих деяний в данном случае отсутствует.

Проведенный анализ особенностей способов и мер наказаний за корыстные компьютерные преступления, получающие закрепление в УК Белоруссии и УК РФ, показывает, что установление уголовной ответственности в гл. 21 УК РФ за компьютерные хищения в зависимости от размера и вида денежных средств приводит к следующим противоречивым ситуациям в законе и на практике:

1. Применение в 2018 г. в законе избыточной дифференциации уголовной ответственности в отношении хищений безналичных (электронных) денежных средств по такому критерию, как их размер, создало ситуацию, когда появилась норма о мошенничестве с использованием электронного платежного средства (ст. 159.3 УК РФ), которая в дальнейшем не будет в полной мере применяться в судебной практике, так как обманные хищения, совершаемые в отношении безналичных (электронных) денежных средств и с использованием электронного средства платежа, уголовная ответственность за которые ранее дифференцировалась в зависимости от размера похищенных денежных средств, стали признаваться в судебной практике квалифицированными видами тайного хищения в зависимости уже от вида денежных средств, предусмотренного п. «г» ч. 3 ст. 158 УК РФ.

2. Выделение специальных посягательств на безналичные денежные средства с применением компьютерных технологий в виде квалифицированных тайных, мошеннических хищений и использование вида денежных средств как единственного основания для ужесточения уголовной ответственности за их совершение привели к появлению в законе двух норм (п. «г» ч. 3 ст. 158 и п. «в» ч. 3 ст. 159.6 УК РФ), содержащих описание признаков двух не различающихся по предмету, способу и, соответственно, форме хищений.

3. Имеется возможность признания мошенничества с использованием электронного средства платежа (ч. 1 ст. 159.3 УК РФ) в соответствии со ст. 158.1 УК РФ и ст. 7.27 КоАП РФ мелким хищением либо административным правонарушением. Такая возможность исключается в отношении тайного и мошеннического хищения безналичных (электронных) денежных средств (п. «г» ч. 3 ст. 158 и п. «в» ч. 3 ст. 159.6 УК РФ).

4. За квалифицированные виды тайного (п. «г» ч. 3 ст. 158 УК РФ) и мошеннического (п. «в» ч. 3 ст. 159.6 УК РФ) хищений безналичных (электронных) денежных средств независимо от размера (мелкий либо крупный) похищенных денежных средств может быть назначено наказание до шести лет лишения свободы. За мошенническое хищение с использованием электронного платежного средства такое наказание может быть назначено лишь в случае хищения безналичных денежных средств в крупном размере.

Применение дифференцированного подхода к закреплению ответственности за компьютерные хищения безналичных (электронных) денежных средств в нормах российского уголовного закона при отсутствии возможности установления отличительных их признаков, более точного определения форм этих видов хищений в нормах закона [27], наличии законодательного положения, не применяемого в полной мере в судебной практике, существовании ситуации, когда применение более строгих (менее строгих) мер наказания возможно в отношении одной части хищений, но исключается для другой части ничем не различающихся таких же деяний, не может восприниматься без серьезной критики. Считаем, что такая ситуация требу-

ет выработки и принятия иного подхода (иных мер) в части защиты отношений собственности в сфере обращения безналичных (электронных) денежных средств. В этом случае стоит обратить внимание на положения, получающие закрепление в УК Белоруссии в виде самостоятельной формы хищения чужого имущества с присущими только ей специфическими признаками либо альтернативного способа основного состава традиционного корыстного преступления против собственности с характерными для него признаками. Именно это позволяет в полном объеме учитывать различные особенности дистанционного способа совершения преступления[44] и применять единые критерии для дифференциации уголовной ответственности в рамках одной формы хищения[45]. Важно отметить, что в УК Белоруссии размеры санкций, установленные за компьютерные преступления против собственности, в основном являются более строгими, чем за преступления против информационной безопасности, и не отличаются от традиционных преступлений против собственности в форме кражи и мошенничества.

Следовательно, более эффективными в защите общественных отношений, возникающих по поводу обращения наличных и (или) безналичных (электронных) денежных средств либо иного имущества, на наш взгляд, являются те положения, которые позволяют в полном объеме учитывать различные особенности дистанционного способа совершения преступления и применять единые критерии для дифференциации уголовной ответственности в рамках одного состава преступления. Именно такое положение должно находить применение в современном российском уголовном законодательстве в виде хищения в сфере компьютерной информации, способ совершения которого в общем виде сформулирован в ст. 159.6 УК РФ.

[44] Всевозможное сочетание его способов как между собой, так и с другими обманными и тайными способами, характерными для корыстных преступлений.

[45] Отдельного традиционного корыстного преступления без признаков хищения, альтернативным способом совершения которого выступает воздействие (модификация) на компьютерную информацию.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Щербаков В.П. Уголовная ответственность за хищения в законодательстве зарубежных государств: вопросы уголовно-правовой теории и проблемы правоприменительной практики / В.П. Щербаков // Вестник экономической безопасности. — 2017. — № 4. — С. 153–159.

2. Кочои С.М. Преступления против собственности в законодательстве Латвии, Белоруссии, Азербайджана / С.М. Кочои // Законодательство. — 2001. — № 2. — С. 59–62.

3. Пасынков А.В. Предмет хищения путем использования компьютерной техники / А.В. Пасынков // Известия Гомельского государственного университета имени Ф. Скорины. — 2016. — № 2 (95). — С. 103–109.

4. Пасынков А.В. Субъект хищения путем использования компьютерной техники / А.В. Пасынков // Вестник Гродненского государственного университета имени Янки Купалы. Сер. 4, Правоведение. — 2011. — № 1. — С. 85.

5. Дворецкий М.Ю. Преступления в сфере компьютерной информации (уголовно-правовое исследование) : автореф. дис. … канд. юрид. наук : 12.00.08 / М.Ю. Дворецкий. — Волгоград, 2001. — 23 с.

6. Богомолов М.В. Уголовная ответственность за неправомерный доступ к охраняемой законом информации / М.В. Богомолов. — Красноярск, 2002. — 58 с.

7. Ахраменка Н. Аспекты доступа в преступлениях против информационной безопасности / Н. Ахраменка // Юстиция Беларуси. — 2006. — № 3. — С. 40–42.

8. Зинина У.В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве : автореф. дис. … канд. юрид. наук : 12.00.08 / У.В. Зинина. — Москва, 2007. — 33 с.

9. Семыкина О.И. Противодействие киберпреступности за рубежом / О.И. Семыкина // Журнал зарубежного законодательства и сравнительного правоведения. — 2016. — № 6. — С. 104–113.

10. Русскевич Е.А. Законодательные подходы к криминализации деяний, связанных с неправомерным доступом к компьютерной информации в странах Содружества Независимых Государств / Е.А. Русскевич // Журнал зарубежного законодательства и сравнительного правоведения. — 2018. — № 1. — С. 116–121.

11. Хилюта В.В. Хищение с использованием компьютерной техники или компьютерное мошенничество? / В.В. Хилюта // Библиотека криминалиста. — 2013. — № 5 (10). — С. 55–65.

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

13. Русскевич Е.А. Новые нормы УК об «электронном» мошенничестве и коррупционных преступлениях / Е.А. Русскевич // Уголовный процесс. — 2018. — № 7. — С. 26–33.

14. Иванова О.М. Хищение чужого имущества как уголовно-правовая категория : дис. … канд. юрид. наук : 12.00.08 / О.М. Иванова. — Самара, 2020. — 318 с.

15. Архипов А.В. Мошенничество с использованием электронных средств платежа (ст. 159.3 УК) / А.В. Архипов // Уголовное право. — 2019. — № 5. — С. 16–20.

16. Русскевич Е.А. Отграничение кражи с банковского счета или в отношении электронных денежных средств от смежных составов преступлений / Е.А. Русскевич // Уголовное право. — 2019. — № 2. — С. 59–64.

17. Филатова М.А. Хищение с использованием чужой банковской карты в магазине образует состав кражи / М.А. Филатова // Законность. — 2020. — № 12. — С. 34–38.

18. Третьяк М.И. Способ мошенничества, предусмотренного ст. 159[3] УК РФ / М.И. Третьяк // Уголовное право. — 2020. — № 4. — С. 61–68.

19. Яни П.С. Хищение с использованием чужой банковской карты в магазине следует квалифицировать как мошенничество / П.С. Яни // Законность. — 2020. — № 12. — С. 39–43.

20. Яни П.С. Мошенничество с использованием электронных средств платежа / П.С. Яни // Законность. — 2019. — № 4. — С. 30–35.

21. Иванов И.С. Современный подход к определению мер уголовной ответственности за хищение денежных средств, находящихся на банковском счете, и электронных денежных средств / И.С. Иванов, С.В. Рязанцева // Российский следователь. — 2018. — № 8. — С. 46–50.

22. Петров С.А. Проблемы квалификации хищений безналичных денег / С.А. Петров // Законность. — 2020. — № 7. — С. 42–45.

23. Болсуновская Л.М. Анализ способов совершения мошенничества в сфере компьютерной информации / Л.М. Болсуновская // Бизнес в законе. — 2015. — № 6. — С. 108–111.

24. Лопашенко Н.А. Компьютерное мошенничество — новое слово в понимании хищения или ошибка законодателя? / Н.А. Лопашенко // Пермский юридический альманах. — 2019. — № 2. — С. 598–609.

25. Русскевич Е.А. Об избыточности и пробельности реформирования уголовного законодательства в целях обеспечения защиты цифровой экономики / Е.А. Русскевич // Пермский юридический альманах. — 2019. — № 2. — С. 708–715.

26. Третьяк М.И. Различные подходы в 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.

27. Hussain M. Corporate fraud: the human factor / M. Hussain. — London : Bloomsbury, 2014. — 175 p.

28. O'Gara J.D. Corporate fraud: case studies in detection and prevention / J.D. O'Gara. — New York : Wiley, 2004. — 202 p.

29. Gregor Urbas. An overview of cybercrime legislation and cases in Singapore / Gregor Urbas // ASLI Working Paper. — 2008. — № 101. — URL: https://www.researchgate.net/publication/237222362_An_Overview_of_Cybercrime_Legislation_and_Cases_in_Singapore.

30. Bazelon D.L. Computer Crimes / D.L. Bazelon, Y.J. Choi, J.F. Conaty // American Criminal Law Review. — 2006. — Vol. 43, iss. 2. — P. 259–310.

31. Hancock D.H. To What Extent Should Computer Related Crimes be the Subject of Specific Legislative Attention? / D.H. Hancock // Albany Law Journal of Science & Technology. — 2001.

32. Heymann S.P. Legislating Computer Crime / S.P. Heymann // Harvard Journal on Legislation. — 1997.

REFERENCES

1. Scherbakov V.P. Criminal Liability for Plunders in the Legislation of the Foreign States: Questions of the Criminal and Legal Theory and Problem of law-Enforcement Practice. *Vestnik ekonomicheskoi bezopasnosti = Bulletin of Economic Security,* 2017, no. 4, pp. 153–159. (In Russian).

2. Kochoi S.M. Crimes against property in the legislations of Latvia, Belarus, Azerbaijan. *Zakonodatelstvo = Legislation*, 2001, no. 2, pp. 59–62. (In Russian).

3. Pasynkov A.V. Object of Theft by Using Computer Hardware. *Izvestiya Gomel'skogo gosudarstvennogo universiteta imeni F. Skoriny = Proceedings of Francisk Scorina Gomel State University*, 2016, no. 2, pp. 103–109. (In Russian).

4. Pasynkov A.V. The Use of Computer Technology in Committing Robbery. *Vestnik Grodnenskogo gosudarstvennogo universiteta imeni Yanki Kupaly. Seriya 4, Pravovedenie = Vesnik of Yanka Kupala State University of Grodno. Series 4, Jurisprudence,* 2011, no. 1, pp. 85. (In Russian).

5. Dvoretskii M.Yu. *Crimes in the sphere of computer information (a criminal law research). Cand. Diss. Thesis.* Volgograd, 2001. 23 p.

6. Bogomolov M.V. *Criminal liability for the illegal access to information protected by law.* Krasnoyarsk, 2002. 58 p.

7. Akhramenka N. Some aspects of access in crimes against information security. *Yustitsiya Belarusi = Justice of Belarus*, 2006, no. 3, pp. 40–42. (In Russian).

8. Zinina U.V. *Cybercrime in Russian and Foreign Criminal Law. Cand. Diss. Thesis*. Moscow, 2007. 33 p.

9. Semykina O.I. Combating Cybercrime in Foreign Countries. *Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniya = Journal of Foreign Legislation and Comparative Law*, 2016, no. 6, pp. 104–113. (In Russian).

10. Russkevich E.A. Legislative Approaches to the Criminalization of Acts Related to Illegal Access to Computer Information in the Countries of the Commonwealth of Independent States. *Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniya = Journal of Foreign Legislation and Comparative Law*, 2018, no. 1, pp. 116–121. (In Russian).

11. Khiluta V.V. A Theft Using Computer Equipment or Computer Fraud? *Biblioteka kriminalista = Library of a Criminalist*, 2013, no. 5, pp. 55–65. (In Russian).

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

13. Russkevich E.A. New Norms of the CC on Electronic Fraud and Corruption Crimes. *Ugolovnyi protsess = Criminal Procedure*, 2018, no. 7, pp. 26–33. (In Russian).

14. Ivanova O.M. *Property theft as a criminal law category. Cand. Diss*. Samara, 2020. 318 p.

15. Arkhipov A.V. Fraud Using Electronic Means of Payment (Article 159³ of the Criminal Code of the Russian Federation). *Ugolovnoe pravo = Criminal Law*, 2019, no. 5, pp. 16–20. (In Russian).

16. Russkevich Y.A. Differentiation of Bank Account Theft or in Relation to E-funds from Associated Elements of Crimes. *Ugolovnoe pravo = Criminal Law*, 2019, no. 2, pp. 59–64. (In Russian).

17. Filatova M.A. Theft Committed with the Use of Someone Else's Bank Card in a Store Constitutes Components of Larceny. *Zakonnost' = Legality*, 2020, no. 12, pp. 34–38. (In Russian).

18. Tretyak M.I. A Method of Fraud Defined by 159³ of the Criminal Code of the Russian Federation. *Ugolovnoe pravo = Criminal Law*, 2020, no. 4, pp. 61–68. (In Russian).

19. Yani P.S. Theft Committed with the Use of Someone Else's Bank Card in a Store should be Classified as a Fraud. *Zakonnost' = Legality*, 2020, no. 12, pp. 39–43. (In Russian).

20. Yani P.S. Online Payment Fraud. *Zakonnost' = Legality*, 2019, no. 4, pp. 30–35. (In Russian).

21. Ivanov I.S., Ryazantseva S.V. A Modern Approach towards Determination of Measures of Criminal Liability for Embezzlement of Money on a Bank Account and Electronic Money. *Rossiiskii sledovatel' = Russian Investigator*, 2018, no. 8, pp. 46–50. (In Russian).

22. Petrov S.A. The Problems of Classification of Embezzlement of Non-Cash Funds. *Zakonnost' = Legality*, 2020, no. 7, pp. 42–45. (In Russian).

23. Bolsunovskaya L.M. Analysis of the Methods of Committing Fraud in the Sphere of Computer Information. *Biznes v zakone = Business in Law*, 2015, no. 6, pp. 108–111. (In Russian).

24. Lopashenko N.A. Cybercrime: Advance in the Understanding of Fraud or a Lawmaker's Mistake? *Permskii yuridicheskii al'manakh = Perm Legal Almanac*, 2019, no. 2, pp. 598–609. (In Russian).

25. Russkevich E.A. On the Redundancy and Gaps of Reforming Criminal Legislation in Order to Protect the Digital Economy. *Permskii yuridicheskii al'manakh = Perm Legal Almanac*, 2019, no. 2, pp. 708–715. (In Russian).

26. 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. (In Russian). DOI: 10.17150/2500-4255.2020.14(4).601-612.

27. Hussain M. *Corporate Fraud: the Human Factor*. London, Bloomsbury, 2014. 175 p.

28. O'Gara J.D. *Corporate Fraud: Case Studies in Detection and Prevention*. New York, Wiley, 2004. 202 p.

29. Gregor Urbas. An overview of cybercrime legislation and cases in Singapore. *ASLI Working Paper*, 2008, no. 101. Available at: https://www.researchgate.net/publication/237222362_An_Overview_of_Cybercrime_Legislation_and_Cases_in_Singapore.

30. Bazelon D.L., Choi Y.J., Conaty J.F. Computer Crimes. *American Criminal Law Review*, 2006, vol. 43, iss. 2, pp. 259–310.

31. Hancock D.H. To What Extent Should Computer Related Crimes be the Subject of Specific Legislative Attention? *Albany Law Journal of Science & Technology*, 2001.

32. Heymann S.P. Legislating Computer Crime. *Harvard Journal on Legislation*, 1997.

ИНФОРМАЦИЯ ОБ АВТОРЕ

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.

INFORMATION ABOUT THE AUTHOR

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.

ДЛЯ ЦИТИРОВАНИЯ

Третьяк М.И. Отличительные особенности мер защиты от корыстных компьютерных посягательств на безналичные (электронные) денежные средства в современном уголовном законодательстве Белоруссии и России / М.И. Третьяк. — DOI 10.17150/2500-4255.2021.15(5).592-604 // Всероссийский криминологический журнал. — 2021. — Т. 15, № 5. — С. 592–604.

FOR CITATION

Tretiak M.I. Specific features of protection against computer-aided criminal infringements on cashless (electronic) funds in contemporary criminal legislations of Belarus and Russia. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2021, vol. 15, no. 5, pp. 592–604. (In Russian). DOI: 10.17150/2500-4255.2021.15(5).592-604.