Гриб Д.В.

СОЦИАЛЬНАЯ ОБУСЛОВЛЕННОСТЬ НОРМ УГОЛОВНОГО ЗАКОНОДАТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ И РЕСПУБЛИКИ БЕЛАРУСЬ, ПРЕДУСМАТРИВАЮЩИХ ОТВЕТСТВЕННОСТЬ ЗА ХИЩЕНИЯ, СОВЕРШАЕМЫЕ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Цель: Изучить особенности уголовной ответственности за хищения, совершаемые с использованием информационных технологий, по законодательству Российской Федерации и Республики Беларусь, а также выделить факторы, обусловившие криминализацию формы хищений.

Медотология: Использовались системный анализ, формально-юридический, сравнительно-правовой и другие методы познания.

Результаты: В статье на основе ранее проведенных теоретических исследований относительно ключевых факторов криминализации деяний рассмотрены факторы, обусловливающие необходимость уголовно-правовой охраны хищений, совершаемых с использованием информационных технологий. На основе статистических данных представлены показатели, характеризующие преступления, совершаемые с использованием информационных технологий. Внимание акцентируется на значимости фактора общественной опасности деяния как одной из важных составляющих необходимости его криминализации.

Новизна/**оригинальность**/**ценность**: Статья обладает определенной научной и практической ценностью, поскольку в ней рассмотрены актуальные проблемы науки уголовного права, а также указаны основные факторы повышенной общественной опасности хищений, совершаемых с использованием информационных технологий.

Ключевые слова: социальная обусловленность, криминализация, уголовный закон, общественная опасность, хищения, совершаемые с использованием информационных технологий.

Gryb D.V.

SOCIAL CONDITIONALITY OF THE CRIMINAL LEGISLATION OF THE RUSSIAN FEDERATION AND THE REPUBLIC OF BELARUS ON THE THEFT COMITTED USING INFORMATION TEHNOLOGIES

Purpose: To study the peculiarities of criminal liability for theft committed using information technologies under the laws of the Russian Federation and the Republic of Belarus, and also to identify the factors that led to the criminalization of this form of theft.

Methodology: Formal, comparative and systematic approaches were used by thr authors among different methods of cognition.

Results: In the paper, the factors causing the need for criminal law protection of theft committed using information technologies are considered on the basis of previously conducted theoretical studies on the key factors of criminalization of acts. On the basis of statistical data, indicators characterizing crimes committed using information technologies are presented. Attention is focused on the significance of the social danger factor of the criminal act, as one of the important components in determining the need for its criminalization.

Novelty/**originality**/**value:** The article has certain scientific and practical value, since it deals with the actual problems of the science of criminal law, and also indicates the main factors of increased public danger of theft committed using information technologies.

Keywords: social purpose, criminalization, criminal law, public danger, theft committed using information technology.

Как отмечается в специальной литературе, в узком смысле криминализация представляет собой признание в уголовном законе деяния общественно опасным и объявление его уголовно наказуемым. Общим основанием криминализации тех или иных деяний является переоценка степени их общественной опасности вследствие воздействия на волю законодателя объективных факторов развития общества и государства, тогда как причинами криминализации деяний выступает, как правило, отсутствие закрепления в уголовном законе новых, сравнительно недавно возникших угроз объектам (обособленным сферам общественных отношений), находящимся под уголовно-правовой охраной [1, с. 59; 2, с. 271; 3, с. 28].

Н.Ф. Кузнецова на основе анализа норм Особенной части УК России и всех признаков составов предусмотренных в них преступлений в совокупности приходит к выводу, что общественная опасность представляет собой специфическое свойство преступления, которое позволяет отграничивать преступления от непреступных правонарушений и малозначительных деяний [4, с. 68]. Говоря о значении общественной опасности как специфического свойства преступления, автор неоднократно повторяет тезис о том, что именно

общественная опасность позволяет отграничивать преступления от непреступных правонарушений и малозначительных деяний [5, с. 265].

Н.Е. Крылова также придерживается той позиции, что лишь преступления обладают таким уровнем «вредоносности», которую законодатель именует общественной опасностью. Другие же правонарушения ею не обладают [6, с. 724]. По мнению Е.В. Епифановой, «именно общественная опасность выступает в роли признака, позволяющего отграничить преступления от иных правонарушений: административные правонарушения, гражданско-правовые деликты являются вредными для общества или конкретного лица, асоциальными, но не общественно опасными» [7, с. 37].

Таким образом, можно утверждать, что криминализация хищений, совершаемых с использованием информационных технологий, обусловлена возросшей в последние годы степенью общественной опасности данной категории преступлений. В свою очередь информационные технологии используются во многих сферах преступной деятельности, при этом в абсолютном большинстве случаев лица не знают друг друга в реальной жизни, и их взаимодействие реализуется посредством виртуальных средств идентификации [8, с. 18].

В частности, В.В. Белокопытов и В.М. Филиппенков обращают внимание на то, что сегодня одновременно с ускорением процессов получения и обмена информацией происходит создание новых и усовершенствование уже известных способов и средств совершения преступлений и применяемых при этом технических устройств. В отношении хищений это выражается в том, что если традиционно основным способом совершения данной категории общественно опасных деяний являлось применение насилия или угроза его применения, то в современном мире «пальма первенства» принадлежит такому способу совершения преступлений, как использование лжи или обмана [9].

Так, согласно статистическим данным Генеральной прокуратуры Российской Федерации, общее число преступлений в сфере информационно-телекоммуникационных технологий в 2017 году увеличилось с 65 949 до 90 587, а их доля от числа всех зарегистрированных в России преступных деяний составляет 4,4 %, т. е. это почти каждое двадцатое преступление. Одновременно весьма существенно увеличилось число преступлений, предусмотренных ст. 159.3 УК РФ (мошеннические действия, совершенные с использованием электронных средств платежа): их количество в первом полугодии 2018 г. возросло в 7 раз [10].

По данным Министерства внутренних дел Республики Беларусь, более 2/3 преступлений (2318, или 74,8 %), выявленных в сфере высоких технологий в 2017 году, относятся к хищениям путем использования компьютерной техники (ст. 212 УК РБ). В 2018 году хищения путем использования компьютерной техники составили 75,8 % от общего числа преступлений, выявленных в сфере высоких технологий, а их число увеличилось до 2996. При этом сумма установленного материального ущерба от преступлений, совершенных с использованием компьютерных технологий, в 2018 году составила 1 170 200 белорусских рублей [11].

Отдельно следует отметить, что довольно высокий удельный вес киберпреступлений совершается несовершеннолетними и при их соучастии: по данным МВД Беларуси, в 2017 и 2018 годах их число составило 116 и 55 соответственно. Н.И. Лимож и М.В. Косович обращают внимание на то, что совершение рассматриваемых преступлений несовершеннолетними осуществляется с использованием глобальной компьютерной сети Интернет, поскольку возможности удаленного доступа облегчают совершение преступлений и помогают скрыть следы преступного деяния. Характерным примером могут послужить действия несовершеннолетнего, который, действуя в сговоре с неустановленным лицом, с использованием реквизитов банковских пластиковых карточек, эмитированных банками Италии и США, совершил хищение денежных средств на общую сумму 22,7 млн белорусских рублей посредством интернет-ресурса, принадлежащего обществу с ограниченной ответственностью. Преступники вводили в компьютерную систему процессингового центра заведомо ложную информацию о распоряжении денежными средствами, находящимися на банковских счетах, якобы уполномоченными на это лицами, что было сопряжено с несанкционированным доступом к компьютерной информации о банковских счетах. Хищение совершалось путем перевода денежных средств с карт-счетов указанных банковских карточек на счета абонентов операторов мобильной связи Республики Беларусь [12].

В этой связи подчеркнем, что в ч. 2 ст. 27 УК Беларуси хищение путем использования компьютерной техники включено в перечень преступлений, нижний порог возраста уголовной ответственности за которые установлен в 14 лет. Однако российский уголовный закон (ч. 2 ст. 20 УК России) не рассматривает составы, предусмо-

тренные ст. 159.3 и 159.6, в качестве преступления, за которое уголовная ответственность наступает с 14 лет.

Общественная опасность рассматриваемых преступлений также обусловлена тем, что использование лжи и обмана при совершении хищений может обладать различной степенью общественной опасности, при этом она многократно повышается за счет использования преступниками потенциала программно-технического комплекса. В частности, специальный состав хищения, предусмотренный ст. 212 УК РБ и ст. 159.3 УК РФ, будет иметь место в преступных действиях, направленных на получение PIN-кодов пользователей банковских карт и электронных кошельков потерпевших. В данном случае злоумышленники считывают данные банковских карт клиентов, а также изготавливают их дубликаты, которые впоследствии продают по низкой цене в другие регионы, минимизируя тем самым риски обнаружить себя [13].

Таким образом, повышенная общественная опасность хищений, совершаемых с использованием компьютерных технологий, обусловлена их транснациональным характером. Кроме того, о повышенной общественной опасности данной разновидности хищений свидетельствуют такие факторы, как высокая латентность такого рода посягательств и объективные сложности уголовно-процессуального доказывания [9].

В этой связи обратим внимание на различие подходов белорусского и российского законодателей к уголовно-правовой регламентации хищений с использованием информационных технологий. Российский уголовный закон использование компьютерной техники рассматривает в качестве особого способа (средства) совершения преступления против собственности, причем данный критерий используется для выделения не отдельной формы хищения, а самостоятельной разновидности мошенничества. Одновременно в Беларуси хищение с помощью компьютерной техники оценивается как самостоятельная форма хищения, о чем свидетельствует содержание ст. 212 УК Беларуси, а также п. 1 примечаний к главе 24 уголовного закона.

Подход российского законодателя заключается в следующем: фактически хищение путем использования компьютерной техники по своей объективной стороне сводится к такой форме хищения, как мошенничество. При этом в п. 20 постановления Пленума Верховного Суда Республики Беларусь от 21 декабря 2001 г. № 15 «О применении судами уголовного законодательства по делам о хищениях имущества» также разъясняется, что в любом случае данное хищение возможно лишь посредством компьютерных манипуляций, заключающихся в обмане потерпевшего или лица, которому имущество вверено или под охраной которого оно находилось, с использованием системы обработки информации [14]. Таким образом, приведенная позиция Верховного Суда Республики Беларусь, по сути, сводит все возможные формы хищения, по которым уголовная ответственность наступает по ст. 212 УК Беларуси, к мошенничеству.

В то же время не до конца ясно, почему российский законодатель ограничился выделением специальных составов только для мошенничества, тогда как иные формы хищения (вымогательство, грабеж), совершаемые с использованием компьютерных технологий, квалифицируются в рамках соответствующих частей ст. 161, 163 УК РФ. С одной стороны, широкая распространенность мошенничества посредством использования современных информационных технологий обусловлена, в частности, тем, что, используя возможности сети Интернет, злоумышленники получают доступ к гораздо более широкому кругу потенциальных жертв, а также удаленный доступ к серверам, хранилищам данных, базам данных и информационным ресурсам большого числа компаний, банков, финансовых учреждений и т. д. С другой стороны, санкции за «традиционное» мошенничество и мошенничество в сфере компьютерной информации, предусмотренные ст. 159, 159.3 и 159.6 УК РФ, в большинстве своем совпадают.

Принимая во внимание данные обстоятельства, можно утверждать, что единственным критерием для обособления специальных составов хищения с использованием компьютерной техники (ст. 212 УК Беларуси), мошенничества с использованием электронных средств платежа (ст. 159.3 УК России) и мошенничества в сфере компьютерной информации (ст. 159.6 УК России) является способ совершения преступления.

Обобщая вышеизложенное, можно сделать вывод о том, что установление уголовной ответственности за хищения, совершаемые с использованием информационных технологий, в России и Белоруссии обусловлено таким их признаком, как общественная опасность. Данный признак присущ преступлениям, является их ключевой характеристикой, тогда как иные правонарушения подобной степенью вредоносности по отношению к охраняемым уголовным законом общественным отношениям не обладают.

Более того, хищения, совершаемые с использованием информационных технологий, относятся к преступлениям против собственности, а их криминализация обусловлена значимостью отношений собственности и ее правовой природой как абсолютного вещного права, гарантированного Конституцией. Соответственно, в настоящее время российским и белорусским законодателем установлен общий уголовно-правовой запрет. Необходимость установления уголовной ответственности за хищения, совершаемые с использованием информационных технологий, обусловлена спецификой способов и средств совершения данных преступлений против собственности, их совершением группой лиц, в том числе – с вовлечением в преступную деятельность несовершеннолетних. Кроме того, о повышенной общественной опасности данной разновидности хищений свидетельствуют такие факторы, как их транснациональный характер, высокая латентность такого рода посягательств на отношения собственности и объективные сложности уголовно-процессуального доказывания.

Пристатейный библиографический список

1. Коробеев А.И. Советская уголовно-правовая политика: проблемы криминализации и пенализации. Владивосток: Изд-во Дальневост. ун-та, 1987.
2. Лопашенко Н.А. Уголовная политика: монография. М.: Волтерс Клувер, 2009.
3. Лопашенко Н.А. Основы уголовно-правового воздействия: уголовное право, уголовный закон, уголовно-правовая политика. СПб.: Юрид. центр Пресс, 2004.
4. Энциклопедия уголовного права. Т. 3: Понятие преступления. СПб.: Издание профессора Малинина, 2005.
5. Полный курс уголовного права: в 5 т. / под ред. А.И. Коробеева. Т. 1: Преступление и наказание. СПб.: Юридический центр Пресс, 2008.
6. Крылова Н.Е. Существует ли уголовное право «в широком смысле слова» // Научные основы уголовного права и процессы глобализации: материалы V Российского конгресса уголовного права, 27–28 мая 2010 г. М.: Проспект, 2010. С. 721–727.
7. Епифанова Е.В. Общественная опасность как научная категория, законодательная дефиниция: история и современность: монография. М.: Юрлитинформ, 2012.
8. Дмитренко А.П., Русскевич Е.А. О нетипичных аспектах соучастия в преступлениях, совершаемых с использованием информационно-коммуникационных технологий // Вестник Академии Генеральной прокуратуры Российской Федерации. 2017. № 5 (61). С. 18.
9. Белокопытов В.В., Филиппенков В.М. Особенности совершения и предупреждения киберпреступлений // ИБ «Комментарии законодательства». Минск: ООО «ЮрСпектр», 2019. Доступ из справ.-правовой системы «КонсультантПлюс Беларусь».
10. О преступлениях, совершаемых с использованием современных информационно-коммуникационных технологий, коммуникационных технологий [Электронный ресурс]. URL: http://genproc.gov.ru/smi/news/genproc/news-1431104.
11. Официальный сайт Министерства внутренних дел Республики Беларусь [Электронный ресурс]. URL: http://mvd.gov.by/main.aspxguid-3311.
12. Лимож Н.И., Косович М.В. Криминологические и уголовно-правовые аспекты преступлений, связанных с несовершеннолетними // ИБ «Комментарии законодательства». Минск: ООО «ЮрСпектр», 2019. Доступ из справ.-правовой системы «КонсультантПлюс Беларусь».
13. Хилюта В.В. Отграничение состава преступления, предусмотренного ст. 212 Уголовного кодекса Республики Беларусь, от иных составов преступлений // ИБ «Комментарии законодательства». Минск: ООО «ЮрСпектр», 2019. Доступ из справ.-правовой системы «КонсультантПлюс Беларусь».
14. О применении судами уголовного законодательства по делам о хищениях имущества: Постановление Пленума Верховного Суда Республики Беларусь от 21 декабря 2001 г. № 15 // Национальный реестр правовых актов Республики Беларусь. 2002. № 8, 6/311.

References (transliterated)

1. Korobeev A.I. Sovetskaya ugolovno-pravovaya politika: problemy` kriminalizacii i penalizacii. Vladivostok: Izd-vo Dal`nevost. un-ta, 1987.
2. Lopashenko N.A. Ugolovnaya politika: monografiya. M.: Volters Kluver, 2009.
3. Lopashenko N.A. Osnovy` ugolovno-pravovogo vozdejstviya: ugolovnoe pravo, ugolovny`j zakon, ugolovno-pravovaya politika. SPb.: Yurid. centr Press, 2004.
4. E`nciklopediya ugolovnogo prava. T. 3: Ponyatie prestupleniya. SPb.: Izdanie professora Malinina, 2005.
5. Polny`j kurs ugolovnogo prava: v 5 t. / pod red. A.I. Korobeeva. T. 1: Prestuplenie i nakazanie. SPb.: Yuridicheskij centr Press, 2008.
6. Kry`lova N.E. Sushhestvuet li ugolovnoe pravo «v shirokom smy`sle slova» // Nauchny`e osnovy` ugolovnogo prava i processy` globalizacii: materialy` V Rossijskogo kongressa ugolovnogo prava, 27–28 maya 2010 g. M.: Prospekt, 2010. S. 721–727.
7. Epifanova E.V. Obshhestvennaya opasnost` kak nauchnaya kategoriya, zakonodatel`naya definiciya: istoriya i sovremennost`: monografiya. M.: Yurlitinform, 2012.
8. Dmitrenko A.P., Russkevich E.A. O netipichny`x aspektax souchastiya v prestupleniyax, sovershaemy`x s ispol`zovaniem informacionno-kommunikacionny`x texnologij // Vestnik Akademii General`noj prokuratury` Rossijskoj Federacii. 2017. № 5 (61). C. 18.
9. Belokopy`tov V.V., Filippenkov V.M. Osobennosti soversheniya i preduprezhdeniya kiberprestuplenij // IB «Kommentarii zakonodatel`stva». Minsk: OOO «YurSpektr», 2019. Dostup iz sprav.-pravovoj sistemy` «Konsul`tantPlyus Belarus`».
10. O prestupleniyax, sovershaemy`x s ispol`zovaniem sovremenny`x informacionno-kommunikacionny`x texnologij, kommunikacionny`x texnologij [E`lektronny`j resurs]. URL: http://genproc.gov.ru/smi/news/genproc/news-1431104.

11. Oficial`ny`j sajt Ministerstva vnutrennix del Respubliki Belarus` [E`lektronny`j resurs]. URL: http://mvd.gov.by/main.aspxguid-3311.

12. Limozh N.I., Kosovich M.V. Kriminologicheskie i ugolovno-pravovy`e aspekty` prestuplenij, svyazanny`x s nesovershennoletnimi // IB «Kommentarii zakonodatel`stva». Minsk: OOO «YurSpektr», 2019. Dostup iz sprav.-pravovoj sistemy` «Konsul`tantPlyus Belarus`».

13. Xilyuta V.V. Otgranichenie sostava prestupleniya, predusmotrennogo st. 212 Ugolovnogo kodeksa Respubliki Belarus`, ot iny`x sostavov prestuplenij // IB «Kommentarii zakonodatel`stva». Minsk: OOO «YurSpektr», 2019. Dostup iz sprav.-pravovoj sistemy` «Konsul`tantPlyus Belarus`».

14. O primenenii sudami ugolovnogo zakonodatel`stva po delam o xishheniyax imushhestva: Postanovlenie Plenuma Verxovnogo Suda Respubliki Belarus` ot 21 dekabrya 2001 g. № 15 // Nacional`ny`j reestr pravovy`x aktov Respubliki Belarus`. 2002. № 8, 6/311.

Проведем оценку имущества для любых целей:

✓ Недвижимости для оспаривания кадастровой стоимости
✓ Ущерба от залива, пожара, действий третьих лиц, после ДТП
✓ Бизнеса, ценных бумаг, нематериальных активов
✓ Движимого и недвижимого имущества
✓ Машин и оборудования

Бесплатная консультация
Срок исполнения от 1 часа
Доставка отчетов курьером

Выполнение с учетом требований законодательства

Проведем профессиональную экспертизу:

Строительно-техническую
Землеустроительную
Инженерно-технологическую
Пожарно-техническую
Автотехническую
Почерковедческую
Подлинности документов
Оценочную
Товароведческую
Бухгалтерскую

Профессионализм экспертов и современные методики проведения исследований в сжатые сроки обеспечивают максимально достоверные результаты!

Входим в ТОП-70 крупнейших компаний России, работающих на рынке оценки. *

*По итогам 2017 года согласно рэнкингу Рейтингового агентства RAEX («Эксперт РА»)

Платинум
группа компаний

м. Электрозаводская,
г. Москва, пл. Журавлева, д. 2, стр. 2, офис 321
ocenka-m.com • info@ocenka-m.com
8 (800) 100-50-01 • 8 (495) 308-15-15