УДК 34
ББК 67
DOI 10.24411/2414-3995-2020-10017

© Д.В. Гриб, 2020

Научная специальность 12.00.08 — уголовное право и криминология; уголовно-исполнительное право

ОБЪЕКТИВНЫЕ ПРИЗНАКИ ХИЩЕНИЯ, СОВЕРШАЕМОГО С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ПО ЗАКОНОДАТЕЛЬСТВУ РЕСПУБЛИКИ БЕЛАРУСЬ И РОССИЙСКОЙ ФЕДЕРАЦИИ

Денис Вячеславович Гриб,
адъюнкт кафедры уголовного права
Московский университет МВД России имени В.Я. Кикотя (117437, Москва, ул. Академика Волгина, д. 12)
E-mail: denisgrib83@gmail.com
Научный руководитель и рецензент: А.П. Дмитренко, доктор юридических наук, профессор кафедры уголовного права Московского университета МВД России имени В.Я. Кикотя

Аннотация. Предметом исследования выступают нормы уголовного права, устанавливающие ответственность за хищения, совершаемые с использованием информационных технологий. Целью настоящей статьи является проведение сравнительного анализа объективной стороны хищений, осуществляемых с помощью компьютерных технологий как специального вида преступлений по законодательству Российской Федерации и Республики Беларусь. Выводы автора позволяют выявить направления трансформации действующих положений уголовного законодательства Республики Беларусь и Российской Федерации в части хищений, совершаемых с использованием информационных технологий.

Ключевые слова: мошенничество, хищение, информационные технологии, предмет преступления, совершенствование уголовного законодательства.

OBJECTIVE CHARACTERISTICS OF THE THEFT COMMITED WITH THE USE OF INFORMATION TECHNOLOGIES, BY THE LAW OF THE REPUBLIC OF BELARUS AND RUSSIAN FEDERATION

Denis V. Grib,
adjunct of the Department of Criminal Law
Moscow University of the Ministry of Internal affairs of Russia named after V.Ya. Kikot' (117437, Moscow, ul. Akademika Volgina, d. 12)

Abstract. The subject of the study is the criminal law, establishing liability for theft committed with the use of information technology. The purpose of this article is to conduct a comparative analysis of the objective side of thefts carried out using computer technology as a special type of crime under the laws of the Russian Federation and the Republic of Belarus. The author's conclusions allow us to identify the directions of transformation of the existing provisions of the criminal legislation of the Republic of Belarus and the Russian Federation regarding theft committed using information technology.

Keywords: fraud, theft, information technology, the subject of the crime, improvement of legislation.

Citation-индекс в электронной библиотеке НИИОН

Для цитирования: Гриб Д.В. Объективные признаки хищения, совершаемого с использованием информационных технологий, по законодательству Республики Беларусь и Российской Федерации. Вестник экономической безопасности. 2020;(1):99-103.

В настоящее время информационные технологии все активнее проникают во все сферы человеческой деятельности, что позволяет говорить о процессе всеобщей информатизации, при этом данный масштабный процесс несет с собой новые угрозы, с которыми ранее общество не сталкивалось. Речь идет о том, что информация, добываемая и используемая при помощи информационных технологий, становится объектом преступных деяний.

В связи с чем, детальное исследование основных компонентов содержания объективной стороны хищения, осуществляемого с помощью информационных технологий, играет важную роль для одинакового понимания сути данного явления. Более того, объект преступления помогает определить границу действия уголовно-правовой нормы, природу и характер общественной опасности содеянного [1, с. 136], а также имеет решающее значение для конструкции отдельных составов преступлений [2, с. 111].

Применительно к хищениям, совершаемым с использованием информационных технологий как преступлениям против собственности родовым объектом, по мнению И.О. Грунтова, являются от-

ношения собственности, т.е. отношения по поводу владения, пользования и распоряжения имуществом или правом на имущество [3]. Иначе говоря, преступления, предусмотренные этой статьей, посягают на определенную часть имущественных отношений — отношения собственности, связанные с применением информационных технологий. В качестве дополнительного объекта преступлений, предусмотренных ст. 159.6 УК России и ст. 212 УК Белоруссии, по нашему мнению, выступает совокупность общественных отношений в сфере компьютерной информации.

Характеризуя предмет хищений, совершаемых с использованием информационных технологий, отдельное внимание следует обратить на то обстоятельство, что в диспозиции ч. 1 ст. 159.6 УК России в качестве непосредственного объекта преступления прямо упоминается чужое имущество и право на такое имущество, однако право на имущество не позволяет владеть и распоряжаться имуществом.

Со своей стороны, белорусский законодатель в качестве объекта хищения, ответственность за которое наступает по ст. 212 УК Беларуси, указывает в дефиниции данной статьи уголовного закона лишь имущество. В связи с чем, в правоприменительной практике возникают проблемы с квалификацией указанных преступлений, а именно с моментом окончания хищений с использованием информационных технологий. Однако следует учесть, что, по своей сути, данная форма преступления заключается в хищении безналичных денежных средств, в связи с чем, необходимо в диспозицию ст. 212 УК РБ включить понятие «право на имущество» с целью расширения предмета преступления. Однако на сегодняшний день в уголовном законодательстве России и Белоруссии отсутствует четкое определение дефиниции право на имущество.

Тем не менее, по мнению исследователей М.М. Ветошкина [4, с. 9], Безверхова А.Г. [5, с. 127], в уголовно-правовом контексте право на имущество, может рассматриваться исключительно как имущественное право. Данная концепция исходит из того, что поскольку в уголовном праве под имуществом рассматриваются вещи, то под правом на имущество следует понимать право на вещь не в вещно-правовом, а в обязательственно-правовом смысле, то есть рассматривать право на имущество в качестве имущественного права объекта гражданских прав.

Сторонники другого подхода Г.Н. Борзенков [6, с. 19], А.П. Севрюков [7, с. 35], полагают, что под правами на имущество понимаются субъективные права участников правоотношений, связанные с владением, пользованием и распоряжением имуществом.

В этой связи отметим, что состав хищения, по общему правилу, является материальным: согласно п. 33 постановления Пленума Верховного Суда Республики Беларусь от 21 декабря 2001 г. № 15 «О применении судами уголовного законодательства по делам о хищениях имущества» [8], а также согласно п. 6 постановления Пленума Верховного Суда Российской Федерации от 27 декабря 2002 г. № 29 «О судебной практике по делам о краже, грабеже и разбое» [9].

Кроме того, ключевым элементом характеристики хищений, совершаемых с применением компьютерных технологий, является совокупность сведений, отражающих типичные способы их реализации. В уголовном праве РФ условно выделяют восемь способов совершения мошенничества в сфере компьютерной информации: ввод, удаление, блокирование, модификация, вмешательство в функционирование средств хранения, вмешательство в функционирование средств обработки, вмешательство в функционирование средств передачи компьютерной информации и вмешательство в функционирование информационно-телекоммуникационной сети.

Белорусский законодатель предусмотрел только два способа совершения подобных преступлений: 1) изменение информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям; 2) введение к компьютерной системы ложной информации [10].

Вместе с тем, судебная практика свидетельствует о том, что дать исчерпывающий перечень способов совершения хищения, совершаемого с помощью компьютерных технологий, вряд ли возможно. Более того, позиция белорусских законодателей, согласно конструкции диспозиции ст. 212 УК РБ будет более правильной, так как, например, совершение мошенничества в сфере информационных технологий только с помощью удаления информации

осуществить невозможно, при этом данный способ может дублироваться и другой уголовно-правовой нормой — уничтожение компьютерной информации. В связи с чем, приходим к выводу, что невозможно в диспозиции указать все существующие способы хищений в сфере информационных технологий в современных условиях жизни, при этом необходимо понимать в каких условиях и обстоятельствах совершается информационное преступление для правильного соотношения компьютерных терминов с уголовно-правовыми нормами.

Кроме того, согласно диспозиции ст. 159.6 УК РФ обман выступает не как способ совершения преступления, а как средство для противоправного завладения имуществом. Однако в результате хищение путем использования компьютерной техники обману подвергается не сам человек, а информационная программа. По нашему мнению, более справедливой является позиция белорусского законодателя.

В качестве примера судебной практики следует указать приговор суда № 01-0207/2016 по ч. 3 ст. 159.6 УК РФ, согласно которому осужденный Ч. в период с 13.02.2014 по 21.10.2014, используя свои служебные полномочия (должность менеджера по продвижению услуг технической поддержки Департамента консалтинга и технической поддержки корпоративных заказчиков), путем ввода логина и пароля (известного только ему), имея доступ к электронной системе заказа железнодорожных билетов, заказал проездные железнодорожные билеты, заведомо не намереваясь осуществлять поездки. Далее, осуществив возврат 255 билетов, Ч., оставил себе полученное денежное вознаграждение, причинив тем самым крупный материальный ущерб [11].

В белорусской судебной практике также зафиксированы подобные случаи. Житель П. Минской области, работая в одном из коммерческих банков, в период с 2014 г. по 2016 г., имея доступ в автоматизированную банковскую систему и используя ноутбук и 3G-модем, изменял суммы размеров овердрафта по имеющимся у него кредитным договорам. Похищенные денежные средства использовал в личных целях. Суд признал его виновным по ч. 4 ст. 212 УК РБ и умышленном уничтожении компьютерной информации (ч. 1 ст. 351 УК РБ) и назначил ему наказание в виде лишения свободы сроком на семь лет с конфискацией имущества [12].

Определенные квалифицирующие признаки мошенничества можно увидеть в преступлениях, связанных с хищением денежных средств с банковских карт, когда потерпевшие лица добровольно передавали злоумышленникам свои личные сведения, открывая доступ к личным счетам. Более того, в абсолютном большинстве случаев лица не знают друг друга в реальной жизни и их взаимодействие реализуется посредством виртуальных средств идентификации [13, с. 18].

Так, по приговору суда РФ № 1-144/2017 Д., используя сим-карту оператора «М» отправил смс-сообщение незнакомому лицу следующего содержания: «Ваша банковская карта заблокирована…..., для ее разблокировки позвоните на номер…». Будучи введенный в заблуждение, что разговор осуществляется с работником банка, потерпевший сообщил Д., номер банковской карты и пин-код к ней. В результате преступник перевел с банковской карты потерпевшего на подконтрольный лицевой счет сумму в размере 499 980 рублей [14].

Следует отметить, что белорусский законодатель еще ранее решил разграничить понятия «мошенничества при хищении путем использования компьютерной техники» и «хищений с использованием компьютерной техники». В частности согласно п. 12 Пленума Верховного суда Республики Беларусь лицо, изготовившее фиктивный документ с помощью компьютерной техники, а затем использовало его для завладения имуществом, вводя в заблуждение потерпевшую сторону, квалифицируется как мошенничество [15].

В судебной практике также можно обнаружить преступления, предусмотренные ст. 159.6 УК РФ и 212 УК РБ, с явными признаками хищения, где компьютерная техника выступает лишь инструментом упрощающим процесс его осуществления. К примеру, П., реализуя свой план хищения денежных средств, используя найденный паспорт другого лица, установил номер банковской карты и сотового оператора с целью получения доступа к системе мобильный банк. Далее восстановив сим-карту оператора (заявив о ее утере, введя в заблуждение сотрудника компании-оператора), П., осуществил перевод денежных средств с банковской карты потерпевшего на номер сотового оператора «Б» [16].

Таким образом, как показывает судебная практика, проблематика квалификации подобного рода хищений указывает на то, что способ совершения преступлений с использованием информационных технологий является самостоятельным составом в Уголовном кодексе и применение принципа совокупности преступлений по не нему не требуется. Однако остается нерешенным вопрос относительно определения первичной квалификации «хищение» или «мошенничество». Анализируя ст. 159.6 УК РФ, можем отметить отсутствие четкого соотнесения данного вида преступления к мошенничеству, так как фактически нет указаний на обман, злоупотребление доверием, ввод в заблуждение самого человека. Получается, что состав преступления по ст. 159.6 УК РФ по своей сути не может определяться как мошенничество. В данном правовом контексте правильным будет видение белорусского законодателя, которые согласно диспозиции ст. 212 УК РБ, установил данный вид преступлений, как хищения с использованием компьютерной техники.

Однако, поскольку российский законодатель, установил более широкий и конкретный перечень информационных технологий, с помощью которых могут осуществляться подобные преступления, то целесообразнее будет назвать данный состав «Хищение с использованием информационных технологий». Также законодателю следует проводить различие между мошенничеством в сфере компьютерной информации как преступлением, связанным с нарушением имущественных прав, произошедшим вследствие нарушения установленного процесса ввода, обработки, хранения, передачи компьютерной информации, и иными формами хищений, которые подразумевают обращение виновного лица к компьютерной информации, но не влекущее вмешательство в компьютерную информацию.

Если отталкиваться от сложившегося подхода российского законодателя и позиции Пленума Верховного Суда Российской Федерации, основным критерием разграничения такой особой формы хищения должно послужить совершение действий, перечисленных в действующей редакции ч. 1 ст. 159.6 УК России, однако в качестве ее квалифицированных составов необходимо дополнить эту новую специальную норму признаками, позволяющими дифференцировать уголовную ответственность и наказания за хищения с использованием информационных технологий, объективная сторона которых содержит признаки различных «традиционных» форм хищения (кража, мошенничество, грабеж, разбой, вымогательство). В эту же статью целесообразно перенести специальный состав кражи как тайного хищения имущества, предметом которого выступают безналичные денежные средства и электронные средства платежа.

Аналогичный подход, как нам представляется, целесообразно использовать и для оптимизации положений ст. 212 УК Беларуси, что позволит, во-первых, разграничить различные формы хищения с использованием компьютерной техники.

Одним из значительных недостатков в ст. 212 УК РБ, а также ст. 159 УК РФ видится оценка уровня материальных убытков. Это объясняется тем, что на современном этапе любая деятельность как необходимый элемент включает информационное обеспечение. Эффективность деятельности во многом зависит от количества и качества входной информации, поэтому искажения или уничтожения информации, имеющей сравнительно небольшую цену, способно причинить значительный ущерб в виде упущенной выгоды. Именно поэтому представляется правильным, кроме потери или уменьшения объема информации, которым владеет потерпевший, в размер материальных убытков от компьютерного преступления включать также и упущенную выгоду, которая может заключаться в заключении невыгодных договоров, падении авторитета, в невыполнении условий договоров.

Таким образом, проведенное исследование позволяет сделать следующие выводы:

1. Сравнительный анализ объективных признаков преступления, предусмотренного нормами ст. 212 УК РБ и 159.6 УК РФ, свидетельствует о схожести интерпретации предмета преступления, признаков объективной стороны и непосредственного объекта.

2. Анализ судебной практики по рассматриваемому виду преступлений показал, что основная сложность при установлении ответственности лица и применения норм ст. 212 УК РБ и ст. 159.6 УК РФ заключается в определении способа совершения преступления. Известные на сегодня способы характеризуются значительным разнообразием и по-

стоянно расширяются. Это обусловлено как сложностью самих средств компьютерной техники, так и постоянным наращиванием новых информационных операций.

3. В контексте вышеописанных фактов, выделяя общие и закономерные недостатки норм уголовного закона белорусского и российского законодательства, предлагается изменить название данного состава преступлений на «Хищение с использованием информационных технологий», обосновав этом тем, что: хищение с использованием информационных технологий по своей юридической природе не могут относиться к мошенничеству, так как данное преступление совершается не путем обмана, либо злоупотребления доверием человека, а путем получения доступа к компьютерным программам, при этом перечень средств, которыми могут совершаться подобные преступления, выходит за рамки понятия «компьютерная техника» (ст. 212 УК РБ), в связи с чем применение термина российского законодателя «информационные технологии» (ст. 159.6 УК РФ) будет более приемлемым.

Литература

1. Кудрявцев В.Н. Общая теория квалификации преступлений. М., 2006.

2. Кригер Г.А. К вопросу о понятии объекта преступления в советском уголовном праве // Вестник Московского университета. Серия общественных наук. 1955. № 1.

3. Научно-практический комментарий к Уголовному кодексу Республики Беларусь / Н.Ф. Ахраменка [и др.]; под ред. А.В. Баркова, В.М. Хомича. 2-е изд., с изм. и доп. Минск: ГИУСТ БГУ, 2010.

4. Ветошкина М.М. Ценные бумаги как предмет хищений: автореф. дис. ... канд. юрид. наук: 12.00.08. Екатеринбург, 2001.

5. Безверхов А.Г. Имущественные преступления. Самара: Изд-во «Самарский университет», 2002.

6. Борзенков Г.Н. Ответственность за мошенничество (вопросы квалификации). М.: Юрид. лит, 1971.

7. Севрюков А.П. Хищение имущества: криминологические и уголовно-правовые аспекты. — М.: 2004.

8. 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.

9. О судебной практике по делам о краже, грабеже и разбое: постановление Пленума Верховного Суда Российской Федерации от 27 декабря 2002 г. № 29 // Российская газета, 18 января 2003 г., № 9.

10. Уголовный кодекс Республики Беларусь [Электронный ресурс]: Кодекс Респ. Беларусь, 9 июля 1999 г., № 275–З (в ред. от 9 января 2019 г. № 171-З)// ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. Минск, 2019.

11. Приговор суда по ч. 3 ст. 159.6 УК РФ № 01-0207/2016 | Судебная практика [Электронный ресурс]. Режим доступа: http://sud-praktika.ru/precedent/101982.html. Дата обращения: 23.08.2019.

12. Интернет-портал судов общей юрисдикции Республики Беларусь Верховный Суд Республики Беларусь [Электронный ресурс]. Режим доступа: http://court.gov.by/ru/justice/press_office/c97ba165467f5667.html?version=print. Дата обращения: 23.08.2019.

13. 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).

14. Приговор суда по ч. 3 ст. 159.6 УК РФ № 1-144/2017 | Мошенничество в сфере компьютерной информации [Электронный ресурс]. Режим доступа: http://sud-praktika.ru/precedent/356488.html. Дата обращения: 23.08.2019.

15. О применении судами уголовного законодательства по делам о хищениях имущества: Постановление Пленума Верховного суда Республики Беларусь от 21 декабря 2001 г. в ред. Пост. Пленума Верховного Суда Респ. Беларусь от 31.03.2016 г. // КонсультантПлюс: Беларусь. Технология 3000 [Электронный ресурс] / ООО «Юрспектр», Нац. центр правовой информации Респ. Беларусь. Минск, 2019.

16. Приговор суда по ч. 2 ст. 159.6 УК РФ № 1-221/2017 | Мошенничество в сфере компьютерной информации [Электронный ресурс]. Режим доступа: http://sud-praktika.ru/precedent/256201.html. Дата обращения: 23.08.2019.