DOI 10.37882/2223–2974.2020.04.22

МОШЕННИЧЕСТВО В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ КАК УГРОЗА ЭКОНОМИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ: АКТУАЛЬНЫЕ ВОПРОСЫ КВАЛИФИКАЦИИ

COMPUTER INFORMATION FRAUD: CURRENT QUALIFICATION ISSUES

S. Kropachev

Summary. The article discusses current issues of countering illegal acts that pose a threat to economic activity, in this regard, in modern conditions, it is extremely important to study the criminal law aspects of fraud in the field of computer information. Particular attention is paid to the analysis of qualification of crimes in terms of the ratio of related fraud, for which liability is provided for in Articles 159, 159.3, 159.6 of the Criminal Code. As a result of the work, the key features of fraud in the field of computer information were identified that affect the correct qualification of a crime.

Keywords: fraud, computer information, qualification, electronic means of payment, common and special norms, crime.

Кропачев Сергей Юрьевич
Адъюнкт, Нижегородская академия МВД России
skropach@mail.ru

Аннотация. В статье рассматриваются актуальные вопросы противодействия противоправным деяниям, представляющим угрозу экономической деятельности, в этой связи в современных условиях представляется крайне важным исследование уголовно-правовых аспектов мошенничества в сфере компьютерной информации. Особое внимание уделяется анализу вопросов квалификации преступлений в части соотношения смежных составов мошенничества, ответственность за которые предусмотрена статьями 159, 159.3, 159.6 УК РФ. В результате проведенной работы были установлены ключевые особенности мошенничества в сфере компьютерной информации, влияющие на правильную квалификацию преступления.

Ключевые слова: мошенничество, компьютерная информация, квалификация, общая и специальная нормы, преступление.

Современная реальность характеризуется ростом инновационных технологий, которые с одной стороны способствуют развитию общества, с другой стороны открывают новые возможности для совершения преступлений, особенно мошенничества, все чаще совершающегося в виртуальном мире.

В 2017 году в России из-за действий киберпреступников потери в финансовой сфере составили порядка 116 млрд. рублей, при этом пострадала каждая пятая организация. Не избежали участи быть атакованными хакерами как государственные структуры, так и военные ведомства. Эксперты считают, что в ближайшие годы рост преступлений с использованием информационно-телекоммуникационных технологий может увеличиться в четыре раза со совокупными потерями, превышающими два триллиона рублей [1].

Подобная ситуация характерна не только для нашей страны, во всем мире наблюдается рост экономических потерь от деятельности мошенников, происходят сбои непрерывности функционирования и дезорганизация управления финансовым рынком. В свою очередь увеличение количества способов и средств совершения мошенничества вследствие стремительного развития IT-сферы требует от государства своевременного предупреждения и профилактики совершения преступлений, оперативности реагирования, использования современных информационных технологий и методов работы, так как страны с наиболее защищенной кредитно-финансовой сферой являются более предпочтительными для потенциальных инвесторов, что представляет собой один из факторов экономического развития.

Основными факторами риска в экономической сфере являются:

- потери финансовых средств вследствие мошеннических действий снижают доверие к современным информационных технологиям в экономической сфере;
- понесенные финансовые потери для некоторых организаций могут быть критичными для их дальнейшей деятельности;
- перебои предоставления финансовых услуг и снижение надежности операций в экономической сфере способствуют нанесению ущерба репутации государства, как регулятора финансового рынка, и росту социальной напряженности в обществе;
- возможность системного кризиса вследствие действий злоумышленников в ведущих организациях финансового рынка.

Законодатель не оставил без внимания опасную тенденцию и своевременно внес изменения в ст. 159–159.6 УК РФ [2], но к сожалению, в практической деятельности органов правопорядка нередко возникают проблемы правильной квалификации преступных деяний в соответствии с введенными нормами уголовного законодательства.

Как правило, не составляет особых затруднений применение общей нормы, указанной в ст. 159 УК РФ, вследствие наличия обширной практики и накопления значительного опыта ее применения. И совсем иначе обстоит дело с квалифицированными составами, установленными ст. 159.1–159.3, 159.5–159.6 УК РФ, по которым практика применения значительно различается по регионам, вследствие того, что современные информационно-телекоммуникационные технологии, используемые злоумышленниками при совершении мошенничеств, зачастую граничат с составами преступлений, установленными ст. 158, ст. 159, ст. 159.3, ст. 159.6 УК РФ.

Исходя из этого, мы считаем необходимым проанализировать особенности квалификации мошенничества, совершенного с использованием информационно-телекоммуникационных технологий.

Одним из ключевых условий правильной квалификации преступлений является изучение и уяснение содержания нормы с последующим ее отграничением от смежных составов преступлений. Это процесс имеет огромное значение в уголовно-правовом противодействии преступности, так как позволяет установить характер и степень вины злоумышленника, тяжесть преступления, определить его индивидуальную ответственность, и назначить справедливое наказание. На практике это представляет собой разграничение предполагаемой для применения правовой нормы, расположенной в Особенной части УК РФ, от смежных и конкурирующих составов преступлений. К конкурирующих нормам относятся те, которые содержат сходные основные признаки деяния, но различающиеся по дополнительным признакам, присутствующим в одной норме и отсутствующим в другой, и наоборот. Как считает Л. В. Иногамова-Хегай при конкуренции уголовно-правовых норм, в части соотношения по объему подчинения, общая норма является более объемной и содержит множество видов, а специальная норма является ничем иным, как одним из таких видов [2, с. 7]. При этом, исходя из устоявшегося в уголовно-правовой науке понимания, при конкуренции общей и специальной норм, применению подлежит именно специальная, как частный случай общей нормы.

В данной статье мы рассматриваем особенности квалификации преступлений, ответственность за которые устанавливается статьей 159.6 УК РФ, конкурирующей со статьями ст. 159 и 159.3 УК РФ.

Законодатель посредством принятия Федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» [3] устанавливая ответственность за дифференцированные виды мошенничества, указанные в ст. 159.1–159.6 УК РФ, совершенно очевидно, преследовал цель не криминализировать новые виды преступлений, а более четко разделить составы мошенничества в зависимости от сферы совершения преступных деяний, что должно было значительно повысить качество квалификации и расследования преступлений.

Из пояснительной записки к Федеральному закону «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» следует, что ст. 159 УК РФ уже предусмотрены все деяния, связанные с хищением чужого имущества или приобретением на него права путем обмана или злоупотребления доверием [4]. Введение дополнительного состава, предусмотренного ст. 159.6 УК РФ, связано с выделением, в силу специфики способа совершения злоумышленником преступного деяния, посредством воздействия разными способами на работу средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей [5, с. 96].

Таким образом, вполне очевидно то, что состав преступления, установленный ст. 159.6 УК РФ является специальным по отношению к ст. 159 УК РФ, которая представляет собой общую норму.

Тем не менее, следует обратить внимание на то, что, несмотря на выделение способов совершения мошенничества в сфере компьютерной информации, по нашему мнению, в преступном деянии, предусмотренном ст. 159.6 УК РФ обязательно должен присутствовать обман и злоупотребление доверием. И только тогда при совершении злоумышленником мошенничества посредством специальных способов, предусматривающих ввод, удаление, блокирование, модификацию компьютерной информации или другим воздействием на работу средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей при установлении факта обмана или злоупотребления доверием, преступное деяние подлежит квалификации по ст. 159.6 УК РФ.

Однако в научном сообществе присутствуют иные точки зрения на соотношение общей и специальной нормы применительно к рассматриваемым статьям УК РФ. Например, Т. В. Кленова, исходя из того, что

ст. 159.1–159.6 УК РФ устанавливаются более низкие санкции, чем те, которые предусмотрены ст. 159 УК РФ, считает, что таким образом законодатель криминализировал новые составы мошенничества с другим характером и степенью общественной опасности, а вследствие недостаточной проработанности новых норм предполагаемая конкуренция норм не удалась [6, с. 29].

По мнению, В. Г. Шумихина, отсутствие в диспозиции ст. 159.6 УК РФ основного признака мошенничества, а именно способа совершения преступления посредством обмана и злоупотребления доверием, указывает на то, что мошенничество в сфере компьютерной информации не представляет собой специальную норму по отношению к общей норме, указанной в ст. 159 УК РФ, так как отсутствует совпадение объективной стороны состава преступления, ответственность за которое устанавливается данными статьями [7, с. 230]. Вследствие этого ученый делает вывод о том, что мошенничество в сфере компьютерной информации является самостоятельной формой хищения.

Рассмотренные мнения теоретиков уголовно-правовой науки относительно конкуренции норм за мошенничество представляются нам не совсем верными, и мы придерживаемся позиции, которую занимают другие ученые, например, Л. Гаухман [8, с. 25], о том, что ст. 159.1–159.6 УК РФ необходимо рассматривать как привилегированные составы преступлений по отношению к общей норме ст. 159.6 УК РФ.

По нашему мнению, отсутствие в диспозиции статьи указания основных способов мошенничества не является основанием для исключения их в качестве признаков мошенничества в сфере компьютерной информации, так как название нормы само по себе предполагает их наличие.

Мы уже рассмотрели, что состав мошенничества в сфере компьютерной информации, введенный в УК РФ, отличается по способу совершения преступного деяния от других видов мошенничества. В основе правильной квалификации мошенничества лежит точное определение способа хищения.

Способы мошенничества, указанные в диспозиции ст. 159.6 представляют собой несколько приемов вмешательства, а именно ввод, удаление, блокирование, модификация компьютерной информации или иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, и представляют собой самостоятельные способы хищения. Со стороны Верховного суда РФ поступили разъяснения [9, с. 7], что способы мошенничества в сфере компьютерной информации основаны на противоправном воздействии на программные алгоритмы обработки и работы с информацией серверов, компьютеров или на сами информационно-телекоммуникационные сети. Данное разъяснение является ключевым для отграничения мошенничества в сфере компьютерной информации от мошенничества с использованием электронных средств платежа, ответственность за которое предусмотрена ст. 159.3 УК РФ, и кражи с банковского счета, в том числе и в отношении электронных денежных средств, закрепленной в ч. 3 ст. 158 УК РФ [10, с. 9].

Рассмотрим вышеуказанные способы мошенничества подробнее для определения ключевых особенностей, влияющих на правильную квалификацию преступного деяния.

Под вводом компьютерной информации в практической деятельности длительное время принимался весьма обширный и неопределенный круг действий, вплоть до способа хищения чужих денежных средств посредством отправки sms-сообщений на служебные номера кредитных организаций, предназначенные для информирования клиентов и совершения денежных переводов. Такое мнение встречается и среди ученых-правоведов, так, например, М. И. Третьяк, считает, что ввод компьютерной информации представляет собой последовательность действий, в которую входят ввод данных об адресате, идентификацию их системой и получение результата [11]. В свою очередь Пленум Верховного Суда РФ трактует такие действия, как кражу чужого имуществах [9, с. 11]. По нашему мнению, под вводом компьютерной информации в качестве способа совершения мошенничества необходимо рассматривать противоправное воздействие на программные алгоритмы обработки и работы с информацией электронно-вычислительных машин или технологические системы, предназначенные для передачи информации по линиям связи.

Вторым способом совершения мошенничества в сфере компьютерной информации является удаление компьютерной информации, которое первоначально в практике российских судов квалифицировалось как воздействие на информацию с целью изменения ее исходного состояния до момента, при котором она утрачивает возможность существования, восприятия и анализа. Самим законодателем понятие «удаления» информации не раскрывается. Так, например, в Федеральном законе от 27 июля 2006 года № 152-ФЗ «О персональных данных» вводится понятие уничтожения информации как действий, в результате которых восстановление данных в информационной системе становится невозможным. Мы считаем, что удаление компьютерной информации

представляет собой незаконные действия посредством программного обеспечения над накопителями информации в результате которых информация утрачивает свой формализованный вид (цифровую форму), позволяющую автоматизировать её сбор, хранение и дальнейшую обработку в ЭВМ.

Третьим способом совершения мошенничества в диспозиции ст. 159.6 УК РФ указывается блокирование компьютерной информации. В нормативных правовых актах данное понятие впервые раскрывается в

ст. 3 Федерального закона «О персональных данных», где под блокированием компьютерной информации понимается временное прекращение обработки данных, за исключением тех случаев, когда обработка необходима для уточнения данных. В уголовно-правовой науке встречается понимание блокирования компьютерной информации как действия, направленного на ограничение или прекращение доступа к данной информации и вследствие этого отсутствием возможности распоряжаться ей законным владельцем, но без причинения собственнику прямого материального ущерба [11]. Данная позиция представляется нам слишком расплывчатой и представляется более верным считать блокированием компьютерной информации итог воздействия на компьютерную информацию или технику, в результате которого в течение определенного периода времени или постоянно отсутствовала возможность производить требуемые операции над искомой информацией, то есть целенаправленная реализация приемов вмешательства в функционирование программно-технического оборудования, влекущее за собой ограничение или закрытие доступа законным пользователям к расположенным на этом оборудовании информационным ресурсам.

Четвертым способом совершения мошенничества в сфере компьютерной информации является модификация компьютерной информации. Доктринальное и судебное толкование данного способа подразумевало любые изменения имеющейся программы для ЭВМ [12, с. 41], за исключением адаптации программы в целях работы на конкретных технических устройствах. На наш взгляд под модификацией компьютерной информации необходимо понимать целенаправленное воздействие на информацию, хранящуюся в ЭВМ, сети или на машинных носителях, с целью изменения первоначального содержания файлов.

Что же касается последнего способа совершения мошенничества, указанного в диспозиции ст. 159.6 УК РФ как иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно — телекоммуникационных сетей, то толкование этого способа среди ученых отличается в силу разного подхода к пониманию средств хранения, обработки или передачи компьютерной информации. Так, например, Ермакова О.В. считает, что под иным вмешательством нужно рассматривать незаконные приемы воздействия на процесс обработки, хранения, передачи, использования компьютерной информации, с целью нарушения его нормального функционирования, осуществляемые чаще всего посредством ввода информации [12, с. 42]. По мнению Шумихина В.Г. если рассматривать иное вмешательство как отдельный способ совершения преступления, то возникает проблема разграничения его от основных способов, таких как ввод, удаление, блокирование и модификация компьютерной информации [13]. По нашему мнению, под иным вмешательством следует понимать открытый, не ограниченный перечень приемов воздействия на средства вычислительной техники, которые влекут за собой нарушение установленного процесса обработки, хранения, передачи и иного обращения с компьютерной информацией.

На наш взгляд встречающееся в уголовно-правовой науке рассмотрение способа мошенничества в сфере компьютерной информации как совокупности самостоятельных способов [13] достаточно затруднительно для применения в части разграничения, так как, например, и блокирование и модификация информации включают в себя способы ввода и удаления компьютерной информации.

Пленум ВС РФ аналогично считает, что такого разграничения не требуется и для квалификации необходимо установить сочетание этих приемов вмешательства в любой вариации. На это в частности указывает Постановление Пленума Верховного суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», в котором способ совершения мошенничества в сфере компьютерной информации трактуется как один способ незаконного воздействия на программное обеспечение, включающий в себя пять приемов вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-коммуникационных сетей. При этом возможны различные варианты сочетания приемов и сами по себе, по отдельности, они не влекут за собой последствия причинения материального ущерба.

Мошенничество в сфере компьютерной информации, как разъясняет Пленум Верховного Суда РФ, необходимо считать оконченным с момента изъятия денежных средств потерпевшего с расчетного счета финансово-кредитной организации или электронных денежных средств, вследствие чего собственнику этих денежных средств причинен ущерб.

Таким образом, по нашему мнению, правильная квалификация мошенничества в сфере компьютерной информации основывается на разъяснениях Пленума ВС РФ от 30 ноября 2017 года и ключевого момента толкования способа совершения данного способа как совокупности пяти приемов вмешательства, указанных в ст. 159.6 УК РФ, заключающихся в целенаправленном незаконном воздействии на программное обеспечение серверов, компьютеров или на сами информационно-телекоммуникационные сети.

ЛИТЕРАТУРА

1. «РосБизнесКонсалтинг» [Электронный ресурс] Российские компании за год потеряли более 100 млрд. руб. из-за кибератак. URL: https://www.rbc.ru/technology_and_media/19/12/2017/5a38f3749a794710aa15581b (дата обращения: 26.02.2020).
2. Иногамова-Хегай Л. В. Концептуальные основы конкуренции уголовно-правовых норм: монография. М.: Норма, Инфра-М, 2015.— 288 с.
3. Федеральный закон «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» от 29.11.2012 № 207-ФЗ // Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 26.02.2020).
4. Пояснительная записка «К проекту федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации (в части усиления уголовной ответственности за хищение денежных средств с банковского счета или электронных денежных средств)»: [Электронный ресурс] Автоматизированная система обеспечения законодательной деятельности. URL: http://asozd.duma.gov.ru/ (дата обращения 26.02.2020)
5. Третьяк М. И. Проблемы квалификации новых способов мошенничества // Уголовное право. 2015. № 2. С. 94–98.
6. Кленова Т.В. О разграничении смежных и конкурирующих составов преступлений (на примере мошенничества) // Уголовное судопроизводство. 2014. № 1. С. 25–30.
7. Шумихин В. Г. Седьмая форма хищения чужого имущества // Вестник Пермского Университета. Юридические науки. 2014. № 2. С. 229–233.
8. Гаухман Л. Д. Мошенничество: новеллы уголовного законодательства // Уголовное право. 2013. № 3. С. 25–27
9. Постановление Пленума Верховного суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // Бюллетень Верховного Суда РФ. 2018. № 2. С. 7.
10. Архипов А. В. Ответственность за хищение безналичных и электронных денежных средств: новеллы законодательства // Уголовное право. 2018. № 3. С. 9.
11. Третьяк М. И. Проблемы понимания способа компьютерного мошенничества в судебной практике // Уголовное право. 2015. № 5. С. 109–110.
12. Ермакова О. В. Мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ): сложности толкования и квалификации // Уголовное право. 2016. № 3. С. 36–43.
13. Шумихин В. Г. Судебное и доктринальное толкования способа мошенничества в сфере компьютерной информации // Пермский юридический альманах. 2019. № 2. С. 733–740.

Журнал «Современная наука: актуальные проблемы теории и практики»