ПРОБЛЕМЫ КВАЛИФИКАЦИИ МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ ПО УК РФ

Е. А. ЦЫГАНКОВА,

канд. юрид. наук, доц. кафедры юридических и специальных дисциплин Ставропольского филиала Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации

Современная жизнь обосновывает необходимость развития уголовного законодательства в части противодействия мошенничеству. Диспозиция ст. 159 УК РФ предусматривает определение мошенничества, сформированное еще в советские времена, однако изменение социально-экономической обстановки в стране требует переосмысления данного деяния, учитывая отношения, ранее не существовавшие.

Как справедливо отмечают Н. А. Моисеев и Н. Г. Новоселов, «в настоящее время мошеннические действия являются преступлениями новой формации, становятся дистанционными и совершаются в большей мере с использованием информационно-коммуникационных систем. Также сегодня увеличивается количество способов их совершения, усложняются схемы и механизмы преступных действий, что в полной мере затрудняет противодействие данному виду преступлений» [1, с. 26].

Характеризуя личность современного преступника-мошенника следует отметить его стремление к материальному обогащению, к упрочению собственных позиций, уверенность в собственном превосходстве на фоне других представителей криминального мира. Достаточно часто мошенничество относят к преступности «белых воротничков», высокотехнологичной преступности. Криминологическая характеристика мошенника указывает на то, что последний, как правило имеет высшее образование, хорошо ориентируется в законодательстве, обладает коммуникативными бизнес-связями, на момент привлечения к ответственности имеет высокий социальный статус и стабильный доход.

В связи с принятием Федерального закона РФ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» [2], законодатель дифференцировал ответственность за мошенничество в зависимости от сферы деяния (ст. 159^1, 159^2, 159^3, 159^5, 159^6 УК РФ). Однако, отсутствие какого-либо пояснения о применении этих норм вынудило правоохранительные органы самостоятельно толковать

признаки специальных составов преступлений о мошенничестве, что породило разрозненную, порой неоднозначную практику.

Данная проблема была частично устранена в результате принятия Постановления Пленума Верховного Суда РФ от 30.11.2017 № 48 (ред. от 15.12.2022) «О судебной практике по делам о мошенничестве, присвоении и растрате» [3].

В тоже время остается ряд неоднозначных вопросов относительно правил квалификации обозначенных деяний, что предопределяет актуальность рассматриваемой проблемы.

Расширение основного состава мошенничества путем принятия ряда норм права, предусматривающих ответственность за специальные виды мошеннических действий, было неоднозначно воспринято научной общественностью, поскольку создало трудности в вопросах квалификации и отграничения простого мошенничества от смежных составов.

Обратимся к рассмотрению такого специального вида рассматриваемого преступного деяния как мошенничество в сфере компьютерной информации, закрепленное ст. 159.6 УК РФ. Криминализация данного деяния и выделение его в качестве самостоятельного состава явилось следствием усиливающейся цифровизации экономики в государственном и частном секторе [4, с. 2].

Сразу обращает на себя внимание, что данная статья отличается способом совершения преступного деяния как от основного состава мошенничества, так и от иных видов. Согласно диспозиции, способом совершения хищения является «ввод, удаление, блокирование, модификации компьютерной информации либо иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей». В основном же составе мошенничества способом совершения является обман или злоупотребление доверием. Исходя из этого, ряд исследователей отмечают, что, по сути, мошенничество в сфере компьютерной информации есть совершенно новый состав хищения, никак не связанный с основным составом мошенничества [5, с. 21].

Для того, чтобы согласиться с данным мнением или отказаться поддерживать его, необходимо остановится на вопросе наличия проблем, с которыми сталкиваются правоприменители при разрешении дел.

В статье 272 УК РФ «Неправомерный доступ к компьютерной информации», уже содержатся такие понятия как «уничтожение», «блокирование», «модификация» компьютерной информации. Определения указанных понятий содержатся в методических рекомендациях по осуществлению прокурорского надзора при расследовании преступлений в сфере компьютерной

информации, которые рассчитаны на применение в отношении статей 272-274 УК РФ.

Однако, в ст. 272 УК РФ данные понятия отнесены к общественно опасным последствиям деяния; в рассматриваемой нами статье – к способу его совершения. Исходя из этого, получается, что законодатель применительно к нормам статей 159.6 УК РФ и 272 УК РФ вложил в данные понятия разный по существу смысл: как действия, процесса (ст. 159.6 УК РФ) и как состояния, результата данных процессов (статья 272 УК РФ). В тоже время, на практике, не возникает затруднений в применении содержания терминов относительно статьи 159.6 УК РФ.

Таким образом, методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации возможно использовать в качестве ориентира при применении статьи 159.6 УК РФ.

По смыслу статьи 159.6 УК РФ вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей признается целенаправленное воздействие программных и (или) программно-аппаратных средств на серверы, средства вычислительной техники (компьютеры), в том числе переносные (портативные) – ноутбуки, планшетные компьютеры, смартфоны, снабженные соответствующим программным обеспечением, или на информационно-телекоммуникационные сети, которое нарушает установленный процесс обработки, хранения, передачи компьютерной информации, что позволяет виновному или иному лицу незаконно завладеть чужим имуществом или приобрести право на него.

Мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по статье 272, 273 или 274.1 УК РФ.

Примером судебной практики является приговор Октябрьского городского суда Республики Башкортостан в отношении Д. [6], обвиняемой в совершении преступлений, предусмотренных ст. 159.6 ч. 3 п.п. «б», «в»; ст. 272 ч. 3 УК РФ. Судом было установлено, что обвиняемая, работая специалистом офиса обслуживания и продаж ПАО «Вымпелком», используя индивидуальный и конфиденциальный логин и пароль для работы в компьютерной программе «1С», содержащей персональные данные клиентов ПАО «Вымпелком» и персональные данные их лицевых счетов, используя свое служебное положение, из корыстной заинтересованности совершила неправомерный

доступ к охраняемой законом компьютерной информации, с целью ее модификации и хищение чужого имущества путем модификации компьютерной информации в крупном размере. Д. самостоятельно выбрала абонентский номер, с привязанными к ним лицевыми счетами, подделав заявления клиентов на замену СИМ-карт, производила перевыпуск СИМ-карт и модификацию компьютерной информации, получив возможность пользоваться лицевыми счетами с находящимися на них деньгами, принадлежащих ПАО «Вымпелком». Модифицировав компьютерную информацию, используя выпущенные СИМ-карты и свой сотовый телефон, с лицевых счетов абонентов в сети «Интернет» оплачивала покупки и переводила деньги на счет своей банковской карты. Данные деяния были совершены многократно в отношении различных клиентов ПАО «Вымпелком».

Суд пришел к выводу, что действия Д. следует квалифицировать по совокупности ст. 159.6 ч. 3 п.п. «б», «в» УК РФ; а также ст.272 ч. 3 УК РФ.

Таким образом, представляется целесообразным ввести в УК РФ специальную норму о мошенничестве в сфере компьютерной информации, и в целях исключения дополнительной квалификации постараться сконструировать норму путем идеальной совокупности преступлений по ст. 159.6 и 272 или 273 УК РФ.

ЛИТЕРАТУРА

1. Моисеев, Н. А., Новоселов, Н. Г. Исторический и правовой аспекты становление и развитие понятия «мошенничество» / Н. А. Моисеев, Н. Г. Новоселов // Вестник Белгородского юридического института МВД России имени И. Д. Путилина. – 2020. – № 2. – С. 26–29.
2. Федеральный закон от 29.11.2012 г. № 207-ФЗ (ред. 03.07.2016) «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» // [Электронный ресурс] Официальный интернет-портал правовой информации http://www.pravo.gov.ru.
3. Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 (ред. от 15.12.2022) «О судебной практике по делам о мошенничестве, присвоении и растрате» // [Электронный ресурс] Официальный интернет-портал правовой информации http://www.pravo.gov.ru.
4. Сухаренко, А. Н. Законодательное обеспечение информационной безопасности в России / А. Н. Сухаренко // Российская юстиция. – 2018. – № 2. – С. 2–7.
5. Кули-Заде, Т. А. Проблемы квалификации мошенничества в сфере компьютерной информации / Т. А. Кули-Заде // Российская юстиция. – 2019. – № 4. – С. 21–26.
6. Приговор Октябрьского городского суда Республики Башкортостан от 29.07.2020 г. по делу № 1-243/2020. [Электронный ресурс]. – URL: http://sudact.ru.