УДК 343.72

Скоморохова Маргарита Сергеевна
Уральский государственный юридический университет имени В.Ф. Яковлева
Институт прокуратуры
Россия, Екатеринбург
margsko@yandex.ru
Skomorokhova Margarita
Ural State Law University named after V. F. Yakovlev
Institute of Procuracy
Russia, Ekaterinburg

ПРОБЛЕМЫ КВАЛИФИКАЦИИ МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Аннотация: актуальность исследования обусловлена динамичным ростом совершения преступлений, квалифицируемых по ст. 159.6 УК РФ. Автором рассмотрены основные законодательные положения, продемонстрированы основные проблемы квалификации: сложность выбора квалификации в судебной практике, пересечение составов ст. ст. 159.6, 272, 274 УК РФ, предложен путь решения проблем.

Ключевые слова: Уголовный Кодекс, мошенничество, компьютерная информация, IT-мошенничество, хищение.

THE PROBLEMS OF FRAUD QUALIFICATION IN THE FIELD OF COMPUTER INFORMATION

Annotation: the relevance of the study is due to the dynamic increase in the commission of crimes classified under Article 159.6 of the Criminal Code of the Russian Federation. The author considers the main legislative provisions, demonstrates the main problems of qualification: the difficulty of choosing qualifications in judicial practice, the intersection of the constitutions of Articles 159.6, 272, 274 of the Criminal Code of the Russian Federation, and suggests a way to solve the problems.

Key words: Criminal Code, fraud, computer information, IT fraud, theft.

Актуальность данной статьи обусловлена частотой совершения преступлений, предусмотренных ст. 159.6 УК РФ. Подобная динамика напрямую связана с ускоренной цифровизацией общества, которая порождает новые общественные отношения, нуждающиеся в правовом регулировании. В частности экономическое взаимодействие людей с использованием информационных технологий является с одной стороны способом оптимизации отношений собственности, а с другой стороны благоприятной средой для возникновения компьютерного мошенничества и других компьютерных преступлений. Обратимся к статистическим данным, которые будут являться самым очевидным свидетельством актуальности заявленной темы.

По данным Министерства Внутренних дел РФ прирост числа таких преступлений (среди которых можно выделить и мошенничество в сфере компьютерной информации) в России за прошлый год составил 29,7% в сравнении с предыдущим, общее количество таких преступлений за 2023 год составило более 600 тыс. Анализируя динамику прироста за время существования ст. 159.6 УК РФ, можно увидеть, что в 2012 году, когда в Уголовный кодекс Российской Федерации Федеральным законом от 29 ноября 2012 г. N 207-ФЗ были введены нормы, регулирующие ответственность за мошенничество в сфере компьютерной информации количество таких преступлений составляло чуть меньше 6 тыс., что в 2 раза меньше, чем в 2014 году и почти в 11 раз меньше чем в 2023 году [8].

Анализируя компьютерное мошенничество, как явление в целом и как преступление в частности, необходимо обратить внимание на дефиницию «компьютерной информации», которая содержится непосредственно в примечании к ст. 272 УК РФ, а именно «сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи».

Особого внимания заслуживает так же способ совершения преступления, как обязательный элемент объективной стороны состава. Способом совершения мошенничества в ст. 159 УК РФ, является обман или злоупотребление доверием. Очевидно, что подобный способ не возможно представить применительно к искусственному интеллекту, поскольку он лишен сознания, и законодатель предусмотрел иной способ для совершения компьютерного мошенничества, а именно «ввод, удаление, блокирование, модификацию компьютерной информации либо иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей».

При этом в научной среде сформировалось разное отношение к выделению мошенничества в сфере компьютерной информации в отдельную норму. Южин А. А. полагает, что необходимо ввести в гл. 21 УК РФ новую норму о хищении с помощью компьютерной информации, согласно которой, соответственно и будут квалифицироваться подобные деяния [5, с. 144]. Тогда как Болсуновская Л. М. считает, что в статье 159.6 предусмотрена самостоятельная форма хищения путем использования компьютерных технологий, и представляется логичным исключение нормы о мошенничестве в сфере компьютерной информации [2, с. 17].

Основная проблема, на которую хотелось бы обратить внимание заключается в разграничении ст. 159. 6 УК РФ и п. «г» ч. 3 ст. 158 УК РФ. Пленум Верховного Суда РФ в постановлении от 30.11.2017 № 48 совершил первый шаг к решению проблемы, указав, что в случае, «если хищение совершается путем использования учетных данных собственника или иного владельца имущества независимо от способа получения доступа к таким данным, такие действия подлежат квалификации как кража, если виновным не было оказано незаконного воздействия на программное обеспечение серверов, компьютеров или на сами информационно-телекоммуникационные сети». Однако, несмотря на то, что постановление было введено в 2017 году сложности в разграничении квалификаций возникают до сих пор. Об этом свидетельствует относительно свежий приговор суда (от 2020 года, т.е. позже, чем вступило в силу Постановление Пленума ВС РФ №48). По материалам дела лицо, посредством имеющегося у него компьютера, используя ранее найденную им банковскую карту и мобильный телефон, принадлежащие потерпевшему, не имея каких-либо законных оснований, используя «Интернет», «Мобильный банк», путем ввода данных карты потерпевшего, оплатил заказанные ранее для себя товары, приобретенные в интернет – магазине, списав с лицевого счета потерпевшего, денежные средства в размере ... руб., которые перевел в счет оплаты товаров, причинив потерпевшему значительный материальный ущерб. Изначально действия обвиняемого квалифицировали по ст. 159.6 УК РФ, однако признаков объективной стороны компьютерного мошенничества в совершенном деянии не содержится, поскольку лицо не осуществляло мошеннических действий, и не оказало необходимого для совершения деяния воздействия на компьютерное обеспечение. Содеянное было переквалифицировано на п. «в» ч. 2 ст. 158 УК РФ, что представляется более точным применительно к описанному деянию [6].

При этом для сравнения представляется необходимым привести в пример приговор суда, согласно которому действия осужденного квалифицировались по ч.3 ст. 272, ч.3 ст. 272, ч.1 ст.159.6, УК РФ. Осужденный путем неправмерного доступа к компьютерной информации без согласия абонента, на счету которой находились денежные средства в размере 11600 руб перевыпустил ее сим-карту. В последующем он совершил деяние, квалфиицированное судом именно по ч. 1 ст. 159.6 УК РФ, выразившееся в том, что в последующем, заполучив новую сим-карту, осужденный вставил ее в сотовый телефон и посредством отправки СМСсообщения с абонентского номера потрепевшей на подконтрольный себе номер перевел денежные средства. Данная квалфикация представляется не противоречащей приведенному ранее Постановлению Пленума Верховного суда [7].

Еще одна проблема заключается в том что, компьютерное мошенничество совершается способами, которые по своей сути и исходя из норм Уголовного Кодекса РФ является последствиями деяний, квалифицируемых по ст. ст. 272 УК РФ и 274 УК РФ, т. е., присутствет «полное пересечение составов» по ряду признаков, что в свою очередь порождает ряд проблемных вопросов [4, с. 605]. Получается, что деяние — или неправомерный доступ, или нарушение правил эксплуатации — влечет за собой <u>уничтожение</u>, <u>блокирование</u>, <u>модификацию</u> либо <u>копирование</u> компьютерной информации. Способы, перечисленные в ст. 159.6 УК РФ ранее в статье уже упоминались, представляется уместным лишь указать на то, что блокирование и модификация тоже указаны в данной статье, но уже в качестве способов. Получается, что состав неправомерного доступа к компьютерной информации в данном случае является частью компьютерного мошенничества, следовательно выполняется полностью.

Вытекающая отсюда проблема - построение «согласованных санкций», на которую указывала Лопашенко. Простой состав неправомерного доступа к компьютерной информации, равно как и простой состав нарушения правил эксплуатации влекут, в числе прочего, наказание в виде лишения свободы на срок до двух лет, в то время как компьютерное мошенничество без квалифицирующих признаков может быть максимально наказано арестом до четырех месяцев [4, с. 606]. При этом, как нами было замечено ранее, неправомерный доступ к компьютерной информации является лишь частью компьютерного мошенничества, следовательно на данный момент с теоретической точки зрения наказание за преступление (ст. 159.6 УК РФ) мягче, чем за его часть (ст. ст. 272, 274 УК РФ).

Способы устранения данной проблемы активно обсуждаются на данный момент в научном обществе. Большинство ученых утверждают, что компьютерное мошенничество необходимо дополнительно квалифицировать по ст. 272 или ст. 273 УК РФ, однако если признаки одного состава преступления полностью входят в число признаков другого преступного посягательства, предусматривающего и дополнительные признаки, то должен применяться только последний состав. Такой же позиции придерживается Пленум Верховного суда РФ в п. 20 постановления от 30.11.2017 №48. В данной совокупности деяний нормы конкурируют между собой как часть и целое [4, с. 607].

Автор разделяет позицию, согласно которой, выделение отдельных статей для пяти видов мошенничества - это казуистичный подход, от которого необходимо отказаться, несмотря на его популярность в европейских странах [3, с. 508]. В заключение представляется нужным отметить, что вызывает сомнение необходимость существования специальных составов мошенничества, учитывая то, что основного признака мошенничества - обмана и злоупотребления доверием в данном составе не присутствует, тогда как присутствует такой признак кражи, как тайность. В связи с этим, ст. 159.6 представляется лишней в Уголовном Кодексе Российской Федерации. Представляется необходимым ее исключить, а в ст. 158 УК РФ ввести в качестве квалифицирующего признака кражи (ст. 158 УК РФ) новый способ, выделив его внутри статьи как п. «д» ч. 2, сохранив при этом выделенные законодателем и присущие хищению в сфере компьютерной информации способы.

Список литературы:

1. Постановление Пленума Верховного Суда РФ от 130.11.2017 N 48 "О судебной практике по делам о мошенничестве, присвоении и растрате" // "Бюллетень Верховного Суда РФ", N 2, февраль, 2018.

2. Болсуновская Л. М. Криминализация мошенничества в сфере компьютерной информации в российском праве / Л. М. Болсуновская // Библиотека криминалиста. — 2016. — № 3. — С. 15–20.

3. Лопашенко Н. А. Законодательная реформа мошенничества: вынужденные вопросы и вынужденные ответы / Н. А. Лопашенко // Криминологический журнал Байкальского государственного университета экономики и права. — 2015. — Т. 9, № 3. — С. 504–513.

4. Лопашенко Н. А. Компьютерное мошенничество — новое слово в понимании хищения или ошибка законодателя? / Н. А. Лопашенко // Пермский юридический альманах. Ежегодный научный журнал. — 2019. — № 1. — С. 598–609.

5. Южин А.А. Специфика мошенничества в сфере компьютерной информации: теория и практика / А. А. Южин // Известия Юго-Западного государственного университета – 2015 – Т.1 – № 3 (60) – С. 143-147.

6. Приговор суда по ч. 2 ст. 159.6 УК РФ № 1-417/2017 [Электронный ресурс] // sud-praktika.ru: сайт. URL https://sud-praktika.ru/precedent/ (дата обращения: 20.03.2024)

7. Приговор суда по ч. 3 ст. 272, ч. 3 ст. 272, ч. 1 ст. 159.6 УК РФ № 1-336/2017 [Электронный ресурс] // sudact.ru: сайт. URL https://sudact.ru/regular/doc/ (дата обращения: 20.03.2024)

8. tadviser.ru [Электронный ресурс] // URL: http://sudact.ru