

Суркова А.В.

магистрант

3 курс, кафедра «Уголовно-правовых дисциплин»

Институт права

Челябинский государственный университет

Россия, г. Челябинск

Научный руководитель: Штефан А.В., кандидат юридических наук,

доцент, доцент кафедры «Уголовно-правовых дисциплин»

Челябинский государственный университет

Россия, г. Челябинск

**О НЕКОТОРЫХ ПРОБЛЕМАХ КВАЛИФИКАЦИИ
МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ,
СВЯЗАННЫХ С ОТГРАНИЧЕНИЕМ ОТ СМЕЖНЫХ СОСТАВОВ
ПРЕСТУПЛЕНИЙ**

Аннотация: Статья посвящена исследованию некоторых проблем квалификации мошенничества в сфере компьютерной информации, связанных с отграничением от смежных составов преступлений. Рассматриваются основные критерии, по которым ст.159.6 УК РФ отличается от иных смежных составов преступлений. Автором предложены способы совершенствования действующего законодательства по вопросу квалификации мошенничества в сфере компьютерной информации.

Ключевые слова: проблемы квалификации преступления, способы совершения преступлений, компьютерная информация, мошенничество в сфере компьютерной информации.

Annotation: The article is devoted to the study of some problems of fraud qualification in the field of computer information related to the separation from

related crimes. The main criteria by which Article 159.6 of the Criminal Code of the Russian Federation differs from other related crimes are considered. The author suggests ways to improve the current legislation on the qualification of fraud in the field of computer information.

Key words: *problems of crime qualification, methods of committing crimes, computer information, fraud in the field of computer information.*

Проблема отграничения мошенничества в сфере компьютерной информации от иных хищений, в том числе от других специальных видов мошенничества является одним из наиболее важных вопросов, возникающих при квалификации указанного преступного деяния и заслуживает особого внимания. В настоящее время традиционно вызывают сложности отграничения мошенничества в сфере компьютерной информации от общего состава мошенничества, кражи, в том числе кражи с банковского счета, а равно в отношении электронных денежных средств, а также от специальных видов мошенничества: мошенничества с использованием электронных средств платежа и мошенничества в сфере страхования, присвоения и растраты.

В первую очередь предлагаем рассмотреть проблемы отграничения мошенничества в сфере компьютерной информации от общего состава мошенничества, предусмотренного ст. 159 УК РФ, ввиду особой взаимосвязи указанных норм. Специальным признаком, позволяющим отграничить специальную норму, предусматривающую ответственность за совершение мошенничества в сфере компьютерной информации от общей нормы, регламентирующей ответственность за совершение мошенничества выступает способ совершения преступления¹. Так, специальный состав мошенничества характеризуется наличием такого специфического способа совершения преступления как ввод, удаление, блокирование, модификация

¹ Ногинов В.О., Засеева Д.Д. Проблемы правоприменительной практики при квалификации мошенничества в сфере оборота компьютерной информации // Материалы Всероссийской научно-практической конференции: «Стратегии устойчивого развития: социальные, экономические и юридические аспекты. Чебоксары.: «Издательский дом «Среда». С. 308-309.

компьютерной информации, либо иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. При этом обращаем внимание, что обман или злоупотребление доверием в качестве способа совершения преступления не характерен для исследуемого состава преступления¹.

На особенности отграничения мошенничества в сфере компьютерной информации от общего состава мошенничества указывает и п.21 Постановления Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», который отмечает, что «если хищение чужого имущества или приобретение права на чужое имущество осуществляется путем распространения заведомо ложных сведений в информационно-телекоммуникационных сетях, включая сеть интернет (например, создание поддельных сайтов благотворительных организаций, интернет-магазинов, использование электронной почты), то такое мошенничество следует квалифицировать по статье 159, а не 159.6 УК РФ».

В этой связи также стоит указать, что использование лицом похищенных, но достоверных персональных данных (логинов, паролей, кодов доступа) при совершении мошенничества в сфере компьютерной информации подлежит квалификации по ст. 159.6 УК РФ, поскольку указанные действия не содержат признаков способа совершения преступления - обмана. Кроме того, действия, содержащие признаки мошенничества в сфере компьютерной информации, в том числе связанные с введением в заблуждение лица с целью получения информации о банковской карте также подлежат квалификации по ст.159.6 УК РФ, если изъятие денежных средств осуществлялось посредством ввода компьютерной информации.

¹ Замалева С.В. О некоторых проблемах квалификации мошенничества // Право и государство: теория и практика.2022. № 7 (211). С.133-134.

Одной из проблем, возникающих при квалификации мошенничества в сфере компьютерной информации и требующей особого внимания со стороны законодателя является проблема отграничения мошенничества в сфере компьютерной информации от кражи (ст. 158 УК РФ), в том числе с банковского счета, а равно в отношении электронных денежных средств (п. «г» ч. 3 ст. 158 УК РФ). Так, анализируя составы вышеуказанных преступлений, стоит отметить, что конструкции составов указанных преступлений во-многом схожи, поэтому зачастую в практической деятельности встречаются случаи, когда содеянное переqualифицируется со ст. 159.6 на п. «г» ч. 3 ст. 158 УК РФ. Схожесть вышеуказанных составов обусловлена тем, что объектом преступного посягательства, как в отношении кражи, так и мошенничества в сфере компьютерной информации выступает право собственности, а предметом – чужое имущество. Отличие же указанных преступлений стоит проводить также по способу совершения преступления¹.

Отметим также, что в настоящее время несмотря на имеющиеся в доктрине уголовного права разъяснения относительно отграничения мошенничества в сфере компьютерной информации от кражи с банковского счета, а равно в отношении электронных денежных средств судебная практика по вопросу разграничения указанных преступлений не сформировалась, и суды квалифицируют одинаковые обстоятельства по-разному. К примеру, приговором Ступинского городского суда Московской области действия С. квалифицированы по п. «а,б» ч.4 ст. 158 УК РФ, в результате совершения им в составе организованной группы действий по незаконному присоединению к контролеру управления банкоматом через USB – переходник, заранее подготовленного ноутбука с программой для удаленного доступа через информационно-телекоммуникационную сеть «Интернет» в целях подачи команды диспенсеру банкомата на выдачу наличных денежных средств в

¹ Белоногова А.В. Проблемы квалификации мошенничества в сфере компьютерной информации // Научно-практический электронный журнал «Аллея Науки». 2022. № 12 (75). С.110-119.

особо крупном размере, находящихся в его кассетах¹. Указанный пример на наш взгляд демонстрирует, что на практике действия, подпадающие под признаки мошенничества в сфере компьютерной информации, нередко квалифицируются как кража. Считаем, что признаком, позволяющим отличить кражу от мошенничества в сфере компьютерной информации, является также признак тайности совершения противоправных действий: при мошенничестве преступник действует открыто, при краже – тайно. В соответствии с п.2 Постановления Пленума Верховного Суда Российской Федерации «О судебной практике по делам о краже, грабеже и разбое» тайность означает, что «изъятие и обращение имущества происходят скрытно, незаметно для собственника или иного владельца либо других лиц»².

Относительно отграничения мошенничества в сфере компьютерной информации от кражи с банковского счета, а равно в отношении электронных денежных средств заметим также, что ученые-теоретики при разграничении указанных деяний сходятся во мнении, что кража с банковского счета, а равно в отношении электронных денежных средств в отличие от мошенничества в сфере компьютерной информации зачастую производятся без применения особых знаний и навыков³.

В продолжение исследования вопроса отграничения мошенничества в сфере компьютерной информации от иных смежных составов преступлений обратим внимание на особенности отграничения от другого специального вида мошенничества, ответственность за которое предусмотрена ст.159.3 УК РФ (мошенничество с использованием электронных средств платежа). Сложности в отграничении указанных составов зачастую обусловлены тем,

¹ Приговор Октябрьского районного суда г.Владимира от 4 июня 2019 г. № 1-95/2019 URL: <https://sudact.ru/regular/doc/v59eyhN7lzJq/> (дата обращения: 02.11.2023)

² О судебной практике по делам о краже, грабеже и разбое: постановление Пленума Верховного Суда РФ № 29 от 27 декабря 2022 года. URL: https://www.consultant.ru/document/cons_doc_LAW_40412/?ysclid=lov5jbugbb214811256 (дата обращения 08.11.2023)

³ Миралиев Ф.С., Хаснутдинов Р.Р. Некоторые проблемы квалификации мошенничества в сфере компьютерной информации // Российская наука: актуальные исследования и разработки. 2019. № 2. С.359-363.

что для изготовления либо пользования платежной картой виновное лицо может использовать компьютерную информацию. В теории уголовного права разграничение указанных составов преступлений производят по двум основным признакам. Во-первых, обязательным элементом мошенничества с использованием электронных средств платежа выступает средство совершения преступления – поддельная или принадлежащая другому лицу кредитная, расчетная или иная платежная карта (в ст. 159.6 УК РФ такой признак отсутствует). Во-вторых, в отличие от мошенничества в сфере компьютерной информации способом совершения мошенничества с использованием электронных средств платежа выступает обман уполномоченного работника кредитной, торговой или иной организации, кроме случаев, когда хищение денежных средств осуществлялось автоматически¹.

Приведем пример из судебной практики, где действия злоумышленника были квалифицированы как мошенничество с использованием электронных средств платежа. Так, приговором Миасского городского суда Челябинской области гражданин У., находясь в гостях у своего знакомого, тайно завладел дебетовой картой и путем обмана работников торговой организации произвел безналичный расчет с данной карты, причинив при этом значительный вред потерпевшему. Судом действия гражданина У. были квалифицированы по ч.2 ст. 159.3 УК РФ – мошенничество с использованием электронных средств платежа с причинением значительного ущерба потерпевшему, поскольку работник организации не осознает незаконность действий гражданина У., и, соответственно, не раскрывает обмана².

Вопрос отграничения исследуемого состава преступления от мошенничества в сфере страхования (ст.159.5 УК РФ) также вызывает

¹ Герасимова Е.В. Перспективы развития законодательства, устанавливающего уголовную ответственность за мошенничество с использованием сети Интернет и мобильной связи // Вопросы российского и международного права. 2018. № 8А. С.148-155.

² Приговор Миасского городского суда от 30 декабря 2019 г. № 1-765/2019. URL: <https://sudact.ru/regular/doc/vG70dKMsd6Yj/?ysclid=lov71veq4n533921182> (дата обращения 15.11.2023).

некоторые сложности на практике, несмотря на исчерпывающие разъяснения, представленные в п.8 Постановления Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате». Так, согласно указанному постановлению «неправомерное завладение денежными средствами, иным чужим имуществом или приобретение права на него путем предъявления (представления) чужих личных или иных официальных документов (например, паспорта, пенсионного удостоверения, свидетельства о рождении ребенка) в зависимости от непосредственного объекта посягательства и иных обстоятельств дела квалифицируется как мошенничество соответственно по статьям 158.1, 159, 159.1, 159.2, 159.3, 159.5 УК РФ». Тем самым, законодательством устанавливается, что в независимости от того, в какой форме были поданы документы (нарочно или электронным способом) и не зависимо от того, контактировал ли злоумышленник с работником страховой организации или нет, деяние следует квалифицировать по ст.159.5 УК РФ.

В данном случае дискуссионным вопросом при квалификации содеянного выступает вопрос оценки действий злоумышленника, когда решение о выплате осуществляется компьютерной программой автоматически. На этот счет в доктрине уголовного права общепринятой является позиция, в соответствии с которой действия злоумышленника при данном условии стоит оценивать, как мошенничество в сфере компьютерной информации, поскольку злоумышленником в данном случае был использован специальный способ совершения мошенничества в сфере компьютерной информации (ввод, модификация компьютерной информации). Следовательно, отличать исследуемый состав преступления от мошенничества в сфере страхования необходимо также по способу совершения преступления.

Сложности могут возникнуть и при его отграничении мошенничества в сфере компьютерной информации от присвоения или растраты (ст. 160 УК

РФ). Это обусловлено тем, что в настоящее время деятельность хозяйствующих субъектов неразрывно связана с активным использованием современных информационных технологий, и, зачастую, уполномоченные должностные лица (например, главный бухгалтер) совершают хищение денежных средств с использованием информационных технологий, в частности, компьютера. Например, путем отправки подложного платежного поручения в электронной форме. Вопрос правильной квалификации подобных действий указанных лиц остается дискуссионным.

По-нашему мнению, отграничить действия, содержащие признаки мошенничества в сфере компьютерной информации от присвоения или растраты позволяет верное установление субъекта преступного посягательства – должностного лица. Вышеуказанный пример наглядно демонстрирует, что правоприменителю, при отграничении указанных преступлений следует обращать внимание на должностное положение субъекта преступления и на специфическое содержание предмета хищения – на момент изъятия имущество является вверенным виновному, а также на способ совершения преступления (при присвоении или растрате специальные способы мошенничества в сфере компьютерной информации не применяются).

Подводя итог вышесказанному, заметим, что норма уголовного закона, устанавливающая ответственность за совершение мошенничества в сфере компьютерной информации далека от совершенства, что неизбежно вызывает проблемы квалификации данного преступления в процессе правоприменительной деятельности, в частности, при отграничении мошенничества в сфере компьютерной информации от иных смежных составов преступлений. Трудности в отграничении мошенничества в сфере компьютерной информации от иных смежных составов преступлений порождают дополнительные трудности для правоохранительных органов и приводят к неоднородной судебной практике при квалификации

мошенничества в сфере компьютерной информации. Несвоевременная и неточная квалификация, а также дальнейшая переквалификация из одного состава преступления в другой приводит к волоките по делу и в целом оказывают негативное влияние на весь ход расследования, затягивая разбирательство по делу.

Представляется, что при квалификации мошенничества в сфере компьютерной информации правоприменителю в лице следственных и судебных органов необходимо четко представлять себе разграничительные линии между мошенничеством в сфере компьютерной информации и иными смежными составами преступлений информации от иных смежных составов преступлений.

Использованные источники:

1. Ногинов, В.О., Засеева, Д.Д. Проблемы правоприменительной практики при квалификации мошенничества в сфере оборота компьютерной информации / В.О. Ногинов, Д.Д. Засеева // Материалы Всероссийской научно-практической конференции: «Стратегии устойчивого развития: социальные, экономические и юридические аспекты. — Чебоксары.: «Издательский дом «Среда». — 2023. - С. 308-309.
2. Замалеева, С.В. О некоторых проблемах квалификации мошенничества / С.В. Замалеева // Право и государство: теория и практика. — 2022. № 7 (211). - С.133-134.
3. Белоногова, А.В. Проблемы квалификации мошенничества в сфере компьютерной информации / А.В. Белоногова // Научно-практический электронный журнал «Аллея Науки». —2022. № 12 (75). - С.110-119.
4. Приговор Октябрьского районного суда г. Владимира от 4 июня 2019 г.№ 1-95/2019 [Электронный ресурс].URL: <https://sudact.ru/regular/doc/v59eyhN7lzJq/> (дата обращения: 02.11.2023)

5. О судебной практике по делам о краже, грабеже и разбое: постановление Пленума Верховного Суда РФ № 29 от 27 декабря 2022 года. [Электронный ресурс].URL:https://www.consultant.ru/document/cons_doc_LAW_40412/?ysclid=lov5j6ugbb214811256 (дата обращения 08.11.2023)
6. Миралиев, Ф.С., Хаснутдинов, Р.Р. Некоторые проблемы квалификации мошенничества в сфере компьютерной информации / Ф.С. Миралиев, Р.Р. Хаснутдинов // Российская наука: актуальные исследования и разработки. — 2019. — № 2. - С.359-363.
7. Герасимова, Е.В. Перспективы развития законодательства, устанавливающего уголовную ответственность за мошенничество с использованием сети Интернет и мобильной связи / Е.В. Герасимова // Вопросы российского и международного права. — 2018. № 8А. - С.148-155.
8. Приговор Миасского городского суда от 30 декабря 2019 г. № 1-765/2019. [Электронный ресурс].URL:<https://sudact.ru/regular/doc/vG70dKMsd6Yj/?ysclid=lov71veq4n533921182> (дата обращения 15.11.2023).