УДК 343.72

Белоногова А.В.
Студентка магистратуры 3 курса кафедры
«Уголовное право и криминология»
Алтайский государственный университет
Россия, Барнаул

ПРОБЛЕМЫ КВАЛИФИКАЦИИ МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Аннотация: *Статья посвящена рассмотрению проблем квалификации ст. 159.6 УК РФ «Мошенничество в сфере компьютерной информации».*

Ключевые слова: *мошенничество, компьютерное мошенничество, компьютерная информация, хищение чужого имущества, отграничение ст. 159.6 УК РФ от 158 УК РФ.*

PROBLEMS OF QUALIFYING FRAUD IN THE SPHERE OF COMPUTER INFORMATION

Annotation: *The article is devoted to the problems of qualification of Article 159.6 of the Criminal Code of the Russian Federation "Fraud in the field of computer information".*

Keywords: *fraud, computer fraud, computer information, theft of other people's property, delineation of Article 159.6 of the Criminal Code of the Russian Federation from 158 of the Criminal Code of the Russian Federation.*

Быстрый рост и развитие современных технологий, использование которых повсеместно распространено во всех областях человеческой деятельности, порождает развитие преступных посягательств корыстного характера на чужое имущество в указанной сфере.

Статистика МВД России позволяет оценить количество зарегистрированных преступлений в сфере информационных технологий, которое по состоянию на конец декабря 2021 года составило 517 722, а на конец ноября 2022 года – 470 143 [12].

Статья 159.6 УК РФ «Мошенничество в сфере компьютерной информации» в Уголовный кодекс Российской Федерации [1] была введена Федеральным законом от 29.11.2012 № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» [2].

В науке уголовного права высказывались критические замечания по поводу введения рассматриваемой статьи.

Непосредственным объектом ст. 159.6 УК РФ являются охраняемые уголовным законом общественные отношения в сфере собственности, дополнительным - общественные отношения, обеспечивающие информационную безопасность.

Предметом мошенничества в сфере компьютерной информации является имущество и право на имущество, а также бездокументарные ценные бумаги в виде электронной записи на носителе.

Мошенничество в сфере компьютерной информации совершается путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Уголовный закон не раскрывает указанные способы. Методические рекомендации Генеральной прокуратуры Российской Федерации,

разработанные для ст. ст. 272 - 274 УК РФ, содержат описание ряда способов. Рекомендации не содержат понятия «удаление», однако содержат понятие «уничтожение», долгое время в науке уголовного права производились попытки отграничений указанных понятий.

Считаем, что решением вопроса стало принятие Пленумом Верховного Суда Российской Федерации 15 декабря 2022 года постановления № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет», согласно которому уточнено понятие уничтожение компьютерной информации, применительно к преступлениям, предусмотренным главой 28 УК РФ, в частности, понятие дополнено указанием на то, что «приведение ее в непригодное состояние должно совершаться с целью утраты возможности ее восстановления» [4].

Таким образом, с учетом вышесказанного, считаем, что «уничтожение» и «удаление» компьютерной информации являются самостоятельными понятиями, различающихся своей сутью, ключевое различие состоит в невозможности восстановления информации при ее уничтожении, и возможности при удалении.

Следует, рассмотреть соотношение мошенничества в сфере компьютерной информации и кражи, так как нередко возникают сложности отграничения именно указанных составов.

Отграничение вышеуказанных составов, прежде всего, следует проводить по способу совершения преступления. При этом, несмотря на отсутствие прямого контакта злоумышленника и потерпевшего, скрытого характера действий с компьютерной информацией, это не позволяет сделать вывод о том, что указанные действия являются тайными по смыслу ст. 158 УК РФ.

Пункт 21 постановления Пленума Верховного Суда РФ от 30.11.2017 N

48 «О судебной практике по делам о мошенничестве, присвоении и растрате» приводит основание разграничения данных составов [5].

До принятия Пленумом Верховного Суда РФ в 2017 году данного постановления суды часто ошибочно квалифицировали содеянное не по ст. 158 УК РФ (кража), а по ст. 159.6 УК РФ.

Так, судом первой инстанции Н. признан виновным в совершении преступления, предусмотренного ч. 2 ст. 159 УК РФ. «Н., дезинформировал С., С., не догадываясь о преступных намерениях Н., выполнил при помощи карты и банкомата операции, указанные Н., тем самым предоставил ему на двух выданных банкоматом квитанциях полную информацию о банковской карте и о находящихся на ней денежных средствах. Н., используя указанные данные при помощи компьютера и автоматизированной системы перевел денежные средства, находящиеся на банковской карте С. в размере 12 000 рублей, на банковскую карту своего знакомого З. Далее Н., через банкомат по банковской карте З. снял данные денежные средства.

Кассационным определением судебной коллегии по уголовным делам Алтайского краевого суда действия Н. переквалифицированы на п. «в» ч. 2 ст. 158 УК РФ.

Президиум Алтайского краевого суда решение кассационной инстанции о переквалификации действий Н. с ч. 2 ст. 159 УК РФ на ч. 2 ст. 158 УК РФ признал ошибочным, мотивировав свои выводы тем, что действие осужденного по изъятию денежных средств является тайным, а обман потерпевшего явился средством облегчения совершения хищения. При этом кассационной инстанцией не учтен особый способ совершения хищения, выделенный законодателем в отдельный состав преступления и являющийся специальной нормой по отношению к ст. 159 УК РФ»[6]. Президиумом указано, что описанный способ хищения свидетельствует о вмешательстве в функционирование средств хранения, обработки, передачи компьютерной информации, что подпадает под действие ст. 159.6 УК РФ. В данном случае

злоумышленник использовал обман потерпевшего для дальнейшего тайного завладения его денежными средствами, а поэтому содеянное необходимо квалифицировать по ст. 158 УК РФ (кража).

Если после хищения денежных средств с банковского счета похитителем изменяется логин и пароль, то в этом случае содеянное должно квалифицироваться по ст. 158 УК РФ и ст. 272 УК РФ.

Федеральным законом от 23 апреля 2018 года № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации ч. 3 ст. 158 УК РФ была дополнена новым особо квалифицирующим признаком совершения кражи: «с банковского счета, а равно в отношении электронных денежных средств» [3].

В пояснительной записке к законопроекту [7] указано на то, что он направлен на повышение уголовно-правовой защиты граждан и организаций путем усиления уголовной ответственности за хищение чужого имущества, совершенное с банковского счета, а равно электронных денежных средств.

«Авторы законопроекта указывали на то, что хищение денежных средств в электронной форме либо с банковского счета клиента, как правило, сопряжено с профессионализмом преступников, их оснащенностью и, как следствие, повышенной общественной опасностью»[11]. Судебная практика показывает, что хищения производятся без применения особых знаний и навыков. Так, «ФИО1 в ходе распития спиртного заметил на лавочке сотовый телефон, он взял телефон и убрал в карман своей одежды, после посредством услуги «мобильный банк» за два раза перевел на свою карту денежные средства, принадлежащие Ш.» [10].

Для исправления сложившейся ситуации необходимо исключить вышеназванный квалифицирующий признак ст. 158 УК РФ.

Считаем, что как мошенничество в сфере компьютерной информации, следует квалифицировать действия злоумышленника путем ввода и модификации компьютерной информации в программном обеспечении

банкомата в случае неправомерного подключения к нему вследствие которых происходит изъятие денежных средств, то есть реализуется способом, составляющим объективную сторону ст. 159.6 УК РФ.

Так, по приговору Октябрьского районного суда г. Владимира о действия гражданина Л. были квалифицированы по ч. 3 ст. 159.6 УК РФ. «Используя электронный шуруповерт и фрезу к нему, Л. вскрыл корпус банкомата, проделав в нем два отверстия, через которые достал USB-провод и подключил к нему имеющиеся при нем удлинитель с клавиатурой, а также USB-hab (разветвитель) и получил непосредственный доступ к ЭВМ (системному блоку). Далее Л. подключил к системному блоку банкомата флешнакопитель с установленной на нем вредоносной компьютерной программой. Запустив указанную вредоносную компьютерную программу, модифицировал компьютерную информацию в накопителе на жестких магнитных дисках (НЖМД) системного блока банкомата, нейтрализовал средства защиты компьютерной информации и инициировал автоматическую выгрузку денежных средств из банкомата. В результате противоправных действий Л. оборудование банкомата необоснованно выдало ему денежные средства, которые привели к ущербу в крупном размере»[8].

Приговором Ступинского городского суда Московской области действия С. квалифицированы по п. «а,б» ч.4 ст. 158 УК РФ. Так установлено, что «С. взламывал панель, находящуюся под монитором с левой стороны банкомата, через образовавшееся отверстие в банкомате незаконно подсоединил к контролеру управления банкоматом через USB - переходник заранее приготовленный планшет либо ноутбук программой для удаленного доступа к планшету либо ноутбуку, а затем, удаленно, посредством подключенного к контролеру управления банкомата компьютерного устройства через информационно-телекоммуникационную сеть «Интернет» подавать команды диспенсеру банкомата на выдачу наличных денежных

средств в крупном или особо крупном размерах, находящихся в его кассетах, которые похитил»[9].

Вышеуказанными примерами подтверждается, что судебная практика однозначно не сформировалась, и суды квалифицируют одинаковые обстоятельства по-разному.

При этом, актуальным остается вопрос: если согласится, что преодоление программой технических средств защиты с последующим изъятием похищаемого имущества в физическом смысле, т.е. с последующим изъятием наличных денежных средств, необходимо квалифицировать по 159.6 УК РФ, то в будущем практика предоставит довольно быстро такие примеры, когда представиться необходимым квалифицировать как мошенничество в сфере компьютерной информации совершение хищения имущества из квартиры путем предварительного определения кодовой комбинации замка и его открытия, взлома замка в квартиру, когда имеет место электронный замок. В данный перечень можно отнести и кражу транспортного средства, в случае его завладения по чужому аккаунту каршеринга.

Считаем, что следует квалифицировать также по ст. 159.6 УК РФ совершение посягательств на вещи в физическом смысле, если изъятие совершается физическим способом, даже в предварительном преодолении технической защиты, связанной с преодолением программно - технических средств защиты для того, чтобы устранить это техническое, физическое препятствие доступа к имуществу,

Подводя итог вышеуказанному, мошенничество в сфере компьютерной информации» стоит рассматривать как самостоятельный вид имущественного преступления, характеризующегося специфическими способами совершения противоправного хищения чужого имущества путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства. Статья 159.6 УК РФ обоснованного помещена в главу 21 УК РФ. Предложения по поводу переименования данной статьи, по ее

трансформированию с учетом имеющихся проблем квалификации, а также стремительным развитием информационных технологий расцениваем как положительное.

Использованные источники:

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // Собрание законодательства РФ. - 1996. - № 25. - Ст. 2954.
2. О внесении изменений в Уголовный кодекс РФ и отдельные законодательные акты РФ: федеральный закон от 29.11.2012 № 207-ФЗ [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_138322/.
3. О внесении изменений в Уголовный кодекс Российской федерации: Федеральный закон от 23.04.2018 №111-ФЗ // Российская газета. - 2018. – 25 апреля. - № 7551 (88).
4. Постановление Пленума Верховного Суда РФ от 15 декабря 2022 года № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» [Электронный ресурс]. URL: https://vsrf.ru/documents/own/31913/ (дата обращения: 26.12.2022).
5. Постановление Пленума Верховного Суда РФ от 30 ноября 2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_283918/ (дата обращения: 26.12.2022).
6. Постановление Президиума Алтайского краевого суда от 03.09.2013г. по делу № 44у-224/13. [Электронный ресурс]. URL: https://sudact.ru/regular/doc/qey190z0eFHg/ (дата обращения: 26.12.2022).

7. 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] // URL: https://www.consultant.ru (дата обращения: 26.12.2022).

8. Приговор Октябрьского районного суда г.Владимира от 04.06.2019 по делу 1-95/2019 [Электронный ресурс]. URL: https://sudact.ru/regular/doc/v59eyhN7lzJq/ (дата обращения: 26.12.2022).

9. Приговор Ступинского городского суда Московской области от 28.02.2020 по делу 1-36/2020 [Электронный ресурс]. URL: https://sudact.ru/regular/doc/45vvACxfKho8/ (дата обращения: 26.12.2022).

10. Приговор Читинского районного суда Забайкальского края от 24.02.2022 по делу 1-121/2022 [Электронный ресурс]. URL: https://sudact.ru/regular/doc/GKU2rcgTQ7lg/ (дата обращения: 26.12.2022).

11. Русскевич, Е.А. Актуальные проблемы противодействия хищениям в системах дистанционного банковского обслуживания / Е.А. Русскевич // Имущественные отношения в Российской Федерации. – 2022. – № 8(251). – С. 70-76.

12. Статистические сведения о состоянии преступности [Электронный ресурс]. URL: (https://мвд.рф/reports/item/34307225 дата обращения: 26.12.2022).