МОШЕННИЧЕСТВО В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ: ПРОБЛЕМЫ КВАЛИФИКАЦИИ ХИЩЕНИЯ ДЕНЕЖНЫХ СРЕДСТВ С ИСПОЛЬЗОВАНИЕМ СЕТИ ИНТЕРНЕТ

С.А. Горовой
Алтайский государственный университет, г. Барнаул

Перечень компьютерных преступлений не ограничен главой 28 Уголовного кодекса Российской Федерации (далее – УК РФ) [2]. Федеральным законом РФ от 29.11.2012 № 207-ФЗ в главу 21 УК РФ была введена статья 159.6 УК РФ, предусматривающая уголовную ответственность за мошенничество в сфере компьютерной информации [4]. С включением ст. 159.6 УК РФ в российское национальное законодательство был разрешен вопрос об участии Российской Федерации в мировых интеграционных процессах в сфере борьбы с киберпреступностью, вектор которых определяется положениями Европейской Конвенции о киберпреступности (раздел «Offences against the confidentiality, integrity and availability of computer data and systems») [1]. Вместе с тем, практика применения указанного состава преступления выявляет ряд проблем, порожденных, главным образом, неточностью законодательной регламентации.

В связи с изменениями, внесенными в УК РФ Федеральным законом от 23.04.2018 № 111-ФЗ, ч. 3 ст. 158 и ст. 159.6 УК РФ были дополнены новым квалифицирующим признаком «совершение хищения с банковского счета, а равно в отношении электронных денежных средств». Также была изменена полностью редакция ч. 1 ст. 159.3 УК РФ [3]. Применение и разграничение указанных норм на практике весьма затруднительно. Так, проблемы при квалификации вызывают случаи снятия денежных средств со счета потерпевшего через банкомат посредством его платежной карты, безналичный расчет платежной картой за товары, услуги путем её предъявления уполномоченному работнику кредитной, торговой или иной организации либо путем использования платежного терминала. В науке обозначенные проблемы не нашли должного решения.

Согласно диспозиции нормы ст. 159.6 УК РФ преступлением является хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации, либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Формулировка диспозиции воспроизводит установление ст. 8 Конвенции.

Общеизвестно, что видовым объектом мошенничества, как одной из форм хищения, являются общественные отношения в сфере собственности, а непосредственным - конкретная форма собственности. Уголовно-правовой запрет, содержащийся в ст. 159.6 УК РФ, охраняет сразу несколько объектов, которые предусмотрены разными главами УК РФ – и отношения собственности, и отношения в сфере компьютерной информации [8, 47].

Предмет рассматриваемого деяния составляет чужое имущество или право на чужое имущество, не принадлежащее виновному лицу [6]. Анализ складывающейся судебной практики позволяет сделать вывод о том, что чаще всего предметом хищения, совершаемого с использованием компьютерной информации или информационно-телекоммуникационных сетей выступают электронные денежные средства, хранящиеся в виртуальных кошельках, таких как «QIWI-кошелек», электронных счетах и расчетных счетах.

Некоторые авторы ошибочно называют предметом мошенничества, предусмотренного ст. 159.6 УК РФ, компьютерную информацию, то есть сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от их хранения, обработки и передачи [6]. Однако же, компьютерные и

телекоммуникационные технологии в данном виде хищения выступают в качестве средств совершения противоправного деяния, дающих возможность для получения денежных средств, либо оплаты с их помощью товаров и услуг.

Потерпевшим выступает собственник имущества. Примечательно, что согласно теории уголовного права, в мошенничестве потерпевший под влиянием обмана или злоупотребления доверием сам передает виновному лицу предмет преступления [7, 200]. Следовательно, вопреки традиционному пониманию мошенничества в составе мошенничества в сфере компьютерной информации законодатель предусмотрел возможность направленности обмана не на потерпевшего (при совершении преступления потерпевший вообще чаще всего не присутствует).

Оценка объективной стороны состава мошенничества в сфере компьютерной информации также показывает, что оно не в полной мере соответствует признакам мошенничества как хищения. Обман и злоупотребление доверием в данном случае должны являться способами совершения мошенничества. Между тем, в диспозиции нормы статьи 159.6 УК РФ указания на обман и злоупотребление доверием вообще нет. Согласно диспозиции данной статьи способами мошенничества названы следующие:

- «ввод, удаление, блокирование, модификация компьютерной информации либо
- иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей».

Фактически в данной статье употребляется терминология составов преступлений, предусмотренных статьями 272 - 274 УК РФ.

С точки зрения формального подхода в виду отсутствия указания на обман или злоупотребление доверием хищение электронных денежных средств есть не что иное, как кража, совершенная с использованием информационно-телекоммуникационных сетей: потерпевший не сам отдает свое имущество или право на имущество, а оно похищается тайным способом.

Субъект мошенничества в сфере компьютерной информации – это физическое, вменяемое лицо, достигшее возраста 16 лет, не являющееся законным владельцем предмета рассматриваемого преступления.

Субъективная сторона состава преступления, предусмотренного ст. 159.6 УК РФ характеризуется прямым конкретизированным умыслом. Умысел на мошенничество проявляется в том, что лицо сознательно осуществляет ввод, удаление, блокирование, модификацию компьютерной информации либо иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, и не намеревается в последующем возместить потерпевшему изъятое у него имущество.

На наш взгляд, неправильное понимание сути хищения и форм его проявления приводит к ошибкам в процессе применения статьи 159.6 УК РФ. Примечательно, что с момента введения в действие изменений, внесенных ФЗ от 23.04.2018 №111-ФЗ Алтайским краевым судом в апелляционном порядке дела изучаемой категории не пересматривались и не оценивались, поэтому новой судебной практики с учетом введения квалифицирующих признаков пока не сложилось. В настоящее время практика рассмотрения уголовных дел данной категории в судах находится в стадии формирования.

Обратимся к имеющимся примерам судебной практики Алтайского края.

1. Н. обратился к незнакомому С. с просьбой воспользоваться его банковской картой с целью установления исправности функционирования системы интернет-обслуживания, тем самым дезинформировал С. относительно своих преступных намерений. С., выполнил просьбу Н., при помощи банковской карты выполнил

операции, указанные Н, тем самым предоставив на двух выданных банкоматом квитанциях полную информацию о банковской карте и находящихся на ней денежных средствах. Н. забрал указанные квитанции, приехал домой, где при помощи сети «Интернет» и автоматизированной системы «Сбербанк ОнЛайн», имея в наличии полную информацию с указанием персональных данных о банковской карте, принадлежащей С., произвел операцию по переводу денежных средств на банковскую карту своего знакомого З. После этого Н. произвел операцию по снятию с банковской карты З. денежных средств, которыми распорядился по собственному усмотрению.

Первоначально суд усмотрел в данном случае признаки ч.2 ст.159 УК РФ. Определением судебной коллегии по уголовным делам приговор был изменен. Содеянное Н. было переквалифицировано на п. «в» ч.2 ст.158 УК РФ. Не согласившись с решениями судов первой и второй инстанции, Президиум краевого суда переквалифицировал действия Н. на ч.2 ст.159.6 УК РФ. В своем постановлении указал, что описанный в судебных решениях способ хищения свидетельствует о вмешательстве в функционирование средств хранения, обработки, передачи компьютерной информации [9].

2. Другое решение было принято в отношении Т. по обвинению в совершении преступления, предусмотренного п. «б» ч.4 ст.158 УК РФ. Согласно приговору Т. Был признан виновным в тайном хищении имущества потерпевшей Ю. на сумму 1 068 000 рублей. Осужденный, обнаружив в квартире потерпевшей Ю. банковские чеки, на которых был указан логин, пароль, одноразовые пароли для входа в личный кабинет Ю. в автоматизированной системе «Сбербанк ОнЛайн», тайно похитил указанные пароли и коды доступа. Затем, находясь в интернет-кафе, используя пароли и коды, с помощью компьютера вошел в личный кабинет Ю. и перевел со счета ее банковской карты денежные средства на счет банковской карты, оформленной на его имя на сумму 18 000 рублей. На следующий день он повторил операцию и перевел аналогичным образом на счет своей карты денежные средства в сумме 100 000 рублей.

Приговор в части квалификации его действий был оставлен без изменения. Апелляционная инстанция в своем решении указала, что действия осужденного по изъятию денежных средств носили тайный характер и были совершены без вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей [11].

Ныне действующее постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» оба представленных случая предписывает квалифицировать как кражу (согласно действующей редакции - по п. «г» ч. 3 ст. 158 УК РФ) [5]. В п. 21 постановления указано, что в тех случаях, когда 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. Это значит, что по п. «г» ч. 3 ст. 158 УК РФ необходимо квалифицировать лишь случаи несанкционированного доступа к информации или системам ее хранения, когда самого противоправного воздействия на компьютерную информацию не происходит.

Так, приговором Алейского городского суда К. был осужден по совокупности преступлений, предусмотренных пунктами «в,г» ч.3 ст.158 и пунктом «г» ч.3 ст.158 УК РФ. Установлено, что у осужденного возник преступный умысел, направленный на систематическое неоднократное хищение денежных средств с банковских счетов ПАО «Сбербанк России», оформленных на имя Б., в крупном размере. В этих целях, используя личный компьютер и сим-карту, оформленную на потерпевшую, с

помощью сети «Интернет» К. осуществил вход в личный кабинет Б., где увидел, что к данному номеру телефона «привязаны» ее банковские карты. После чего совершил несколько операций по безналичному переводу денежных средств с одной карты потерпевшей на другую, поскольку имел к ней доступ. Желая довести умысел на хищение денег потерпевшей до конца, снял за несколько приемов в банкомате 321 587 руб. Аналогичным способом, с использованием удаленного доступа через сеть «Интернет» им были похищены с банковского счета денежные средства потерпевшей Л. в размере 5000 рублей [12].

Обращаясь к судебной практике других регионов, можно заметить, что по ст. 159.6 УК РФ, как правило, квалифицируются действия лиц, которые своими умышленными активными действиями вмешиваются в функционирование средств хранения, обработки или передачи компьютерной информации, т.е. в программные файлы, отвечающие за правильную работу самой системы. Примером такой тенденции может служить уголовное дело по обвинению Б. по ч.4 ст.159.6 УК РФ. Б. совместно с другим лицом оформляла на свое имя банковские карты, которые передавала специалистам в области компьютерного программирования. Те, в свою очередь, списывали со счетов физических и юридических лиц денежные средства, используя вирусы, встроенные в банковское приложение «Ява-Аплет» к системе дистанционного банковского обслуживания «Интернет Банк». Похищенные денежные средства поступали на расчетные счета банковских карт Б. и ее соучастника, затем обналичивались осужденными и тратились по своему усмотрению [10].

Осужденными при совершении преступления использовались технические средства – компьютеры для доступа в сеть Интернет, вредоносное программное обеспечение, а также средства сотовой связи. Следовательно, в совокупности с предыдущими примерами видится, что использования одного только формального признака - совершения преступления с использованием информационно-телекоммуникационных сетей при квалификации действий по ст.159.6 УК РФ явно недостаточно. Действительно, достаточно часто использование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей составляет часть способа совершения кражи (фактически происходит изъятие чужого имущества из правомерного владения собственника путем списания денежных средств с банковского счета потерпевшего). Как в случае со вторым приведенным примером из практики Алтайского края списание денежных средств не изменяет ни программное обеспечение компьютера, не меняет данных расчетного счета потерпевшего лица, т.е. на всем пути до достижения цели виновное лицо лишь использует предоставленные ему тем или иным способом ресурсы для получения доступа к расчетному счету потерпевшего. В этой связи отсутствие признаков модификации (изменения) программного обеспечения, отвечающего за правильное функционирование расчетного счета потерпевшего, свидетельствует об отсутствии признаков ст.159.6 УК РФ.

Специфика способа мошенничества в сфере компьютерной информации характеризуется следующими особенностями:

- воздействие осуществляется непосредственно на компьютерную информацию, а не на сознание потерпевшего;
- отсутствует обман, обязательным признаком которого является введение другого лица в заблуждение путем воздействия на сознание (психику) другого человека;
- отсутствует передача имущества или приобретение права на имущество с помощью потерпевшего;

- средством преступления признаются информация, средства хранения, передачи и обработки компьютерной информации, а не ложные сведения, передаваемые человеком.

Пленум Верховного Суда РФ в п. 20 постановления от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» указал, что 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 [5]. Таким образом, мошенничество, предусмотренное ст. 159.6 УК РФ, представляет собой не типичный вид мошенничества.

В случае, когда виновное лицо использует различные средства хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационные сети для непосредственного воздействия на компьютерную информацию в виде манипуляции с собственными безналичными денежными средствами и сообщения заведомо ложных сведений оператору об изъятии своего имущества, однако воздействие на компьютерную информацию (на денежные средства банка) с помощью указанных средств под влиянием заведомо ложных сведений непосредственно осуществляет оператор путем зачисления на банковский счет виновного лица (владельца карты) денежных средств в качестве компенсации, вследствие того, что виновное лицо само не изымает чужие денежные средства, а их передает ему оператор, исследуемое деяние по ст. 159.6 УК РФ квалифицировать нельзя. В указанном случае основной частью способа совершения преступления является сообщение ложных сведений оператору об изъятии своего имущества. Остальные способы выступают его сопутствующей частью (либо предпосылкой, этапом, условием для него). Исходя из этого, для данного казуса необходимо рассматривать возможность применения общей нормы, предусмотренной в ст. 159 УК РФ.

Очевидно, что мошенничество в сфере компьютерной информации – особый состав преступления, особый вид мошенничества. Ныне в уголовном законодательстве сложилась следующая ситуация: если признать способы, которые указаны в ст. 159.6 УК РФ и ст. ст. 159.1, 159.2, 159.3 УК РФ, способами обмана, то следует сказать, что определение, содержащее в постановлении Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», не соответствует положениям УК РФ. В данном случае требуется либо отказаться от использования термина мошенничество в отдельных нормах либо сформулировать иное определение обмана для судебной практики. При сохранении прежнего определения обмана также становится непонятным, является ли норма, содержащаяся в ст. 159 УК РФ, общей по отношению к другим нормам о мошенничестве.

Для привлечения к уголовной ответственности за неквалифицированное мошенничество, неквалифицированную кражу имеет значение размер похищенного. В случае если сумма похищенных средств не превышает 2500 руб., лицо может быть привлечено к административной ответственности по ст.7.27 КоАП РФ. В свою очередь неверная квалификация хищения в сумме менее 2500 руб. может повлечь вынесение судом реабилитирующее решение.

Проведенное нами исследование показало, что правоприменительная практика по «компьютерному» хищению пока только складывается. Отсутствует комплексное представление о процессах незаконного обналичивания и транзита денег, а также единство подходов по их квалификации.

Библиографический список

1. Convention on Cybercrime, Budapest, 2001 [Электронный ресурс] // Official web-site of Council of Europe. URL: http:// conventions.coe.int./Treaty/en/Treaties/Html/185.htm.
2. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // Собрание законодательства РФ. – 1996. – № 25. – Ст. 2954.
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. О внесении изменений в Уголовный кодекс РФ и отдельные законодательные акты РФ : федеральный закон от 29.11.2012 № 207-ФЗ [Электронный ресурс] // URL: http://www.garant.ru/hotlaw/federal/432682/.
5. О судебной практике по делам о мошенничестве, присвоении и растрате : постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 // Российская газета. – 2017. – 4 декабря. – № 7446 (280).
6. Журавлева Г.В., Карпова Н.А. Мошенничество в сфере компьютерной информации: спорные вопросы теории и практики // Вестник Московского университета МВД России. - 2017. - №5. URL: https://cyberleninka.ru/article/n/moshennichestvo-v-sfere-kompyuternoy-informatsii-spornye-voprosy-teorii-i-praktiki.
7. Лопашенко, Н.А. Преступления против собственности: теоретико-прикладное исследование // М.: ЛексЭст - 2005. – 408 с.
8. Яни П.С. Специальные виды мошенничества // Законность. – 2015. – №5. – С.44.
9. Приговор Алейского городского суда от 28.09.2016 г. по обвинению Н. № 1-166/2016 // Архив Алейского городского суда за 2016 г.
10. Приговор Ленинского районного суда г. Екатеринбурга от 20.03.2017 г. по обвинению Б. № 1-144/2017 // Архив Алейского городского суда за 2017 г.
11. Приговор Локтевского районного суда от 20.07.2018 г. по обвинению Т. №1-75/2018 // Архив Локтевского районного суда за 2018 г.
12. Приговор Алейского городского суда от 23.10.2018 г. по обвинению К. № 1-171/2018 // Архив Алейского городского суда за 2018 г.