УДК 343.7
DOI 10.36511/2078-5356-2019-4-226-230

Сердюк Павел Леонидович
Pavel L. Serdyuk

кандидат юридических наук, старший преподаватель
Уфимский юридический институт МВД России (450103, Республика Башкортостан, Уфа, ул. Муксинова, 2)

candidate of sciences (law), senior teacher
Ufa Law Institute of the Ministry of Internal Affairs of Russia (2 Muksinova st., Ufa, Republic of Bashkortostan, Russian Federation, 450103)

E-mail: pavel.ser@mail.ru

Особенности правовой оценки дистанционного мошенничества

Features of the legal assessment of remote fraud

В статье рассматриваются наиболее сложные вопросы, возникающие при квалификации дистанционного мошенничества в сфере компьютерной информации. Исследуются вопросы отношения к составу мошенничества таких способов обмана и злоупотребления доверием, как уничтожение, блокирование, модификация либо копирование компьютерной информации с целью хищения чужого имущества или получения права на чужое имущество. Проводится отграничение исследуемого состава мошенничества от таких смежных составов, как мошенничество с использованием электронных средств платежа (ст. 159^3 УК РФ), мошенничество в сфере страхования (ст. 159^5 УК РФ) и др. Рассматривается роль социальной сферы при определении степени опасности компьютерного мошенничества, а также возможные ошибки при квалификации статьи 159^6 УК РФ в совокупности с другими статьями Уголовного кодекса РФ.

Ключевые слова: дистанционное мошенничество, компьютерное мошенничество, информационный обман, компьютерное хищение, блокирование информации.

The article discusses the most difficult issues arising in the qualification of remote fraud in the field of computer information. The article examines the relationship to the composition of fraud of such methods of fraud and breach of trust, such as the destruction, blocking, modification or copying of computer information in order to steal someone else's property or obtain the right to someone else's property. The investigated composition of fraud is distinguished from such adjacent compositions as fraud using electronic means of payment (art. 159^3 of the Criminal code of the Russian Federation), fraud in the insurance industry (art. 159^5 of the Criminal code of the Russian Federation), etc. The role of the social sphere in determining the degree of danger of computer fraud as well as possible errors in the qualification of art. 159^6 in conjunction with other articles of the Criminal code of the Russian Federation.

Keywords: remote fraud, computer fraud, information fraud, computer theft, blocking information.

Проблема дистанционного мошенничества сегодня является особенно актуальной в связи с распространением этого преступления, сложностью его квалификации и предупреждения. В большей степени это относится к компьютерному мошенничеству, но значительное место занимает также мошенничество в сфере банковских технологий, связанных с использованием поддельных банковских карт.

Вопрос об особенностях компьютерного мошенничества рассматривался российскими учеными еще 20 лет назад. Исследуя состав этого преступления в Уголовном кодексе ФРГ в 1998 году, профессор Б.В. Волженкин писал: «санкции за компьютерное и за обычное мошенничество в этом Кодексе практически совпадают, поэтому законодатель, вероятно, выделил компьютерное мошенничество в самостоятельный состав преступления, имея в виду необычность

способа совершения преступления с использованием компьютерной техники, когда в "заблуждение" вводится электронно-вычислительная машина» [1, с. 21].

В Уголовный кодекс РФ состав компьютерного мошенничества был введен только в 2012 году. Размер наказания части 1 статьи 159[6] УК РФ фактически не отличается от санкции части 1 статьи 159 УК РФ, где в обоих случаях предусмотрен максимальный штраф до 120 тыс. рублей при отсутствии лишения свободы. Это говорит о том, что Б.В. Волженкин был прав. Мы видим, что основное отличие состава компьютерного мошенничества от общего состава статьи 159 УК РФ заключается не в степени опасности этих преступлений, а исключительно в способе совершаемого обмана. В свою очередь, способ зависит от той социальной сферы и тех технических условий, в которых совершается преступление. Использование электронно-вычислительных средств при совершении мошеннических действий создает специфику данного преступления, требующую специальных знаний при квалификации такого рода преступлений и их доказывании.

В этом случае для совершения обмана не требуется ни подделка документов, ни какие-то иные действия, которые направлены на введение потерпевшего в заблуждение. Преступник использует технические возможности компьютера или иных устройств, содержащих информацию в электронном виде. В основе обмана лежит исключительно информация и возможности электронной техники.

Следует заметить, что нет различий и в определении суммы значительного ущерба гражданину. В примечании к статье 159[1] УК РФ этот размер ущерба определяется по общему указанию закона в сумме не менее 10 тыс. рублей. Крупный и особо крупный размеры ущерба определены, соответственно, в сумме 1 млн 500 тыс. и 6 млн рублей.

Проблема организации борьбы с преступлениями в сфере высоких технологий на международном уровне в 2005 году получила отражение в Бангкокской декларации по результатам XI Конгресса ООН по предупреждению преступности и уголовному правосудию. Был сделан вывод о том, что преступления в этой сфере приобрели организованный, транснациональный характер и представляют серьезную угрозу всем странам мира. На это обратил внимание и Совет Европы, который призвал страны к объединению в борьбе с данными преступлениями в целях защиты от них общества и выработки общей уголовной политики. Направление особого внимания к проблемам киберпреступности было отражено и в Дохийской декларации по результатам XIII Конгресса ООН по предупреждению преступности и уголовному правосудию в 2015 году.

Есть множество примеров применения способов компьютерного мошенничества, рассчитанных на малограмотных и доверчивых граждан. В последние годы компьютер используется отдельными лицами и группами не только по корыстным мотивам, но и в целях вовлечения молодежи в экстремистские группировки и даже в совершение суицида. Но надо заметить, что компьютер при завладении чужим имуществом используется не только в качестве средства обмана потерпевших. Хорошо известны также завладения чужими денежными средствами без непосредственного контакта с хозяином денежных средств, с применением дистанционного обмана. Это происходит с использованием таких способов, которые, например, указаны в части 1 статьи 159[6] УК РФ: ввода, удаления, блокирования, модификации компьютерной информации, вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

По мнению некоторых авторов, данные способы мало похожи на мошенничество. В частности, О.Е. Борунов при рассмотрении этого вопроса пишет: «само понятие обмана предполагает, что потерпевший (собственник) вследствие применения к нему обмана сам выводит имущество из своего владения, то есть добровольно передает его преступнику, предоставляя последнему в отношении имущества правомочия владения, пользования и даже распоряжения. Указанный признак также отличает хищение в сфере компьютерной информации от мошенничества, поскольку невозможно говорить о добровольности передачи имущества в том случае, когда потерпевший даже не догадывается о такой передаче» [2; 3; 4, с. 34].

Думается, с данной позицией нельзя согласиться. Хотя, действительно, хищения с помощью компьютера в той части, когда преступник не соприкасается с потерпевшим, похожи на кражу, но нельзя не признать, что здесь в основе преступного завладения чужими средствами лежит дистанционный обман. Особенно этот способ данного преступления выражается в том, что с помощью современных технических возможностей происходит завладение не только чужой собственностью, но и правом на

эту собственность, что характерно для мошенничества.

«Неправильное понимание сути хищений при завладении чужим имуществом путем манипулирования компьютерными данными на практике приводит к ошибкам в квалификации», пишет Ю.П. Фадина. Автор считает, что статья 159[6] УК РФ «не выдерживает никакой критики». По ее мнению, наличие данной статьи в УК РФ «не будет способствовать разрешению борьбы с рассматриваемыми преступлениями» [5, с. 120].

Т. Тропина приходит к выводу, что мошенничество, совершаемое с помощью компьютера, вообще не может квалифицироваться ни по статье 158, ни по статье 159 УК РФ, так как эти составы неполно охватывают действия преступника [6].

Имеется и другое, на первый взгляд, более рациональное предложение: включить мошенничество, совершаемое с помощью компьютера, в составы статей 158, 159 и 163 УК РФ в качестве квалифицирующих обстоятельств. По мнению авторов, высказывающих это предложение, манипуляции с компьютерной информацией при посягательстве на чужое имущество или право на имущество могут быть способами и кражи, и мошенничества, и выступать в форме вымогательства с использованием компьютерного шантажа.

Мы считаем, что завладение чужими средствами с помощью компьютерных технологий справедливо признано законодателем одним из особых видов мошенничества. Обман потерпевшего в данном случае происходит в завуалированном, дистанционном и на первой его стадии скрытом виде. В этом заключается специфика данного преступления, где способ обмана и злоупотребления доверием связан с новыми техническими возможностями преступника при совершении манипуляций в сфере электронной информации. Поэтому исследуемый нами состав мошенничества вполне оправданно существует обособленно от других норм, предусматривающих уголовную ответственность за хищение с применением обмана и злоупотребления доверием.

Под компьютерной информацией закон определяет «сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи» (прим. к ст. 272 УК РФ). Охраняемой законом является информация особого статуса — ограниченного доступа, завладение которой может причинить существенный вред ее частному владельцу или государственной организации, либо даже государству в целом. Незаконные посягательства на эту информацию происходят с применением преступных способов, предусмотренных специальными нормами Уголовного кодекса РФ. К таким нормам относятся: статья 272 УК РФ «Неправомерный доступ к компьютерной информации» (в ред. Федеральных законов от 7 декабря 2011 г. и от 28 июня 2014 г.); статья 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ» (в ред. Федерального закона от 7 декабря 2011 г.); статья 274 УК РФ «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» (в ред. Федерального закона от 7 декабря 2011 г.); статья 274[1] УК РФ «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации» (введена Федеральным законом от 26 июля 2017 г.).

Интернет предоставляет свободный доступ к инструкциям по применению компьютерных программ, поэтому работа с компьютерной информацией доступна не только специалистам, связанным с высокими технологиями, но практически любому гражданину. Это значительно затрудняет профилактику и предупреждение данного рода преступности. Кроме того, невысокий уровень расследования данных преступлений связан со сложностью их доказывания, что во многом объясняет слабую борьбу с данными преступлениями. Но главные трудности возникают на стадии квалификации этих преступлений. Например, выявление ложных информационных сведений, введенных преступником в имеющуюся информационную программу, возможно только с привлечением специалиста.

Практика показывает, что наиболее сложным для квалификации является определение проникновения в компьютерные сети путем «взлома» систем защиты информации. Данный способ наиболее часто применяется сегодня для осуществления хищений чужого имущества или приобретения права на чужое имущество с использованием электронной техники.

Не менее сложным при квалификации дистанционного мошенничества является установление такого способа, как ввод вредоносной компьютерной программы в электронную память компьютера или иных электронных устройств, способных выполнять прием, обработку, хранение и выдачу информации в электронном виде. Под иными электронными устройствами

понимаются: телефоны, смартфоны, бортовые компьютеры транспортных средств, банкоматы, контрольно-кассовые машины и т. п.

Под блокированием информации понимается постоянное или временное закрытие (или ограничение) доступа к ней. Это также технический прием при совершении в том числе и хищения денежных средств либо при достижении цели завладения правом на чужое имущество. Блокирование информации не позволяет использовать информацию полностью или в требуемом режиме.

Модификация информации означает изменение ее содержания, что не позволяет ее воспроизведение в первоначальном виде. Сюда не относится изменение технического обеспечения информации. Обман непосредственно к потерпевшему в данном случае также не применяется.

Особую общественную опасность представляет копирование компьютерной информации. Это выражается в получении возможности использования ценной информации в нежелательных для владельца целях. Копирование информации может осуществляться и путем ее переписывания от руки, срисовывания, фотографирования и т. д. Однако надо заметить, что копирование информации может быть и вполне законным и даже полезным, если это совершается в целях надежности ее сохранения.

Не меньший вред может причинять такой способ преступления, как удаление (уничтожение) компьютерной информации, независимо от того, возможно ее восстановление или нет. В этом случае полостью исключается ее получение с соответствующего носителя электронной памяти компьютера, иного устройства или интернет-сайта. Данный способ применяется часто при незаконном завладении правом на чужое имущество.

Следующим способом компьютерного мошенничества является создание вредоносной программы. Общественная опасность этого способа заключается в том, что вредоносный код может внедряться в уже существующую программу, нарушая ее нормальную работу путем изменения ее алгоритма либо путем удаления из нее (или внесения в нее) отдельных фрагментов.

Распространение вредоносных программ совершается также иными способами, например, путем их проката, продажи и т. д.

Правовую базу нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации телекоммуникационных сетей (ст. 274 УК РФ) представляет Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 18.03.2019), а также постановление Правительства РФ от 24 ноября 2009 года № 953 (ред. от 20.04.2017) «Об обеспечении доступа к информации о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти».

Рассматриваемые преступления сегодня имеют небольшой процент в статистике общей преступности, но их число постоянно увеличивается. В большей степени это относится к преступлениям экономической направленности, где преступники используют электронные средства. Кроме того, если эти преступления касаются государственных интересов крупного экономического или производственного характера, они могут повлечь серьезные негативные последствия. Однако жертвами данных преступлений могут стать и отдельные организации, и обычные граждане, так как они могут касаться как банковских и коммерческих тайн, так и авторских, изобретательских и других прав граждан.

При квалификации разных видов мошенничества, если преступление совершается с использованием компьютерной информации в качестве способа обмана, надо иметь в виду, что определяющим признаком квалификации является не способ мошенничества, а та сфера, в которой совершается преступление. Например, мошенничество в сферах использования кредитных карт или страхования происходит с использованием модификации компьютерной информации, и квалификация должна осуществляться по соответствующим статьям 159^3 и 159^5 УК РФ.

Ошибочной иногда является квалификация мошенничества с применением компьютерной информации в совокупности с другими статьями УК РФ. Когда делается неверный вывод о том, что состав статьи 159^6 УК РФ не охватывает признаки этих преступлений. К таким составам, в частности, относится статья 272 УК РФ «Неправомерный доступ к компьютерной информации», если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации. Это относится также к составу статьи 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ». Дополнительная квалификация при мошеннических действиях в данном случае не нужна по той причине, что данные нарушения компьютерной информации выступают

в качестве способа совершения преступления, предусмотренного статьей 159[6] УК РФ.

В заключение следует отметить, что борьба с дистанционным мошенничеством с использованием электронной техники требует обратить внимание на необходимость специальной подготовки оперативных и следственных кадров, осуществляющих раскрытие и расследование данных преступлений.

Примечания

1. Волженкин Б.В. Мошенничество. СПб., 1998.

2. Борунов О.Е. Проблемы квалификации хищения денежных средств со счетов банка с использованием средств компьютерной техники // Российский судья. 2004. № 6. С. 87—90.

3. Кузнецова Е.Г. Мошенничество в сфере компьютерной информации: вопросы квалификации // Правопорядок: история, теория, практика. 2017. № 4 (15). С. 87—90.

4. Майоров А.В. Уголовно-правовая характеристика мошенничества: вопросы квалификации // Наука ЮУрГУ: сборник материалов 68-й научной конференции. Челябинск: Минобрнауки России; Южно-Уральский государственный университет, 2016.

5. Фадина Ю.П. Уголовно-правовая характеристика мошенничества в сети Интернет // Вестник Югорского государственного университета. 2017. № 1 (44).

6. Тропина Т. Компьютерное мошенничество: вопросы квалификации и законодательной техники. URL: http://www.connekt/ru/artift.asp?id=7004 (дата обращения: 05.04.2019).

7. Минин А.Я. О специфике противодействия киберпреступности // Российский следователь. 2013. № 8. С. 37—39.

References

1. Volzhenkin B.V. Fraud. St. Petersburg, 1998. (In Russ.)

2. Borunov O.E. Qualification problems of embezzlement of funds from bank accounts using computer technology. *Russian judge*, 2004, no. 6, pp. 87—90. (In Russ.)

3. Kuznetsova E.G. Computer information fraud: qualification issues. *Law and order: history, theory, practice,* 2017, no. 4 (15), pp. 87—90. (In Russ.)

4. Mayorov A.V. The criminal law characteristic of fraud: qualification issues // Science SUSU: collection of materials of the 68th scientific conference. Chelyabinsk: Ministry of Education and Science of Russia; South Ural State University, 2016. (In Russ.)

5. Fadina Yu.P. The criminal law characteristic of fraud on the Internet. *Bulletin of Ugra State University*, 2017, no. 1 (44). (In Russ.)

6. Tropina T. Computer fraud: qualification issues and legislative technology. URL: http: //www.connekt/ru/artift.asp?Id=7004 (accessed 05.04.2019). (In Russ.)

7. Minin A.Ya. On the specifics of countering cybercrime. *Russian Investigator*, 2013, no. 8, pp. 37—39. (In Russ.)