ВЕСТНИК ЮГОРСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА
2017 г. Выпуск 1 (44). С. 117–121

УДК 343.72:004.738.5

Ю. П. Фадина

УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА МОШЕННИЧЕСТВА В СЕТИ ИНТЕРНЕТ

Мошенничество является одним из распространенных преступлений против собственности, в связи с чем ему уделено достаточно много внимания в специальной литературе. В то же время способы мошенничества постоянно меняются, появляются новые средства совершения преступлений такого рода, что требует и изменений законодательства.

Чрезвычайно актуальным в этой области является: исследование особенностей уголовной ответственности за преступления в сфере компьютерной информации, выявление пробелов в данной сфере и предложение возможных путей их решения.

Ключевые слова: мошенничество, Интернет, фишинг, вишинг, нигерийские письма.

CRIMINAL-LEGAL CHARACTERISTIC OF FRAUD ON THE INTERNET

Fraud is one of the most common crimes against property, so, it is paid enough attention to it in the literature. At the same time the methods of fraud are constantly changing, and new means of committing crimes of the kind that requires changes in legislation.

The study of peculiarities of criminal liability for crimes in sphere of the computer information, identification of gaps in this area and offer possible ways of their solutions is extremely relevant.

Key words: fraud, Internet, phishing, vishing, Nigerian letter.

До недавних пор любое хищение путем обмана или злоупотребления доверием охватывалось ст. 159 УК РФ. Однако появление новых способов хищения потребовало от законодателя своевременной и адекватной реакции, чем обусловлено введение в УК РФ новых статей 159.1–159.6 УК РФ, а также внесение дополнительных частей в ст. 159 УК РФ.

Изменение законодательства требует целенаправленного изучения мошенничества. Кроме того, несмотря на модернизацию уголовного закона в сфере регулирования мошенничества, имеется достаточно нерешенных проблем. На сегодняшний день множество людей ежедневно, не выходя из дома, покупают различные товары через Интернет. В России огромными темпами растет количество пользователей Интернета, поэтому количество «электронных» покупателей тоже растет. Электронные магазины помогают сэкономить на содержании обычного магазина. Они позволяют покупателю покупать любой товар в любое время в любой стране, в любом городе. Это дает электронным магазинам неоспариваемое преимущество перед обычными магазинами. Немалое количество людей попадается в руки «электронных» мошенников.

Родовым объектом мошенничества выступают общественные отношения в сфере экономики. Видовым объектом исследуемого преступления, исходя из буквального толкования уголовного закона и названия главы 21 УК РФ «Преступления против собственности», где это посягательство описано, признается «собственность».

Отношения собственности регулируются разделом II «Право собственности и другие вещные права» (ст.ст. 209–306 Гражданского кодекса Российской Федерации).

Непосредственным объектом мошенничества в сети Интернет являются отношения собственности, в частности конкретная форма собственности: государственная, муниципальная или частная [6, 242]. К примеру, в декабре 2015 года в Межмуниципальный отдел МВД России «Ханты-Мансийский» поступили материалы дела о совершении мошенничества посредством сети Интернет, в результате которого житель города Тольятти лишился денежных средств в общей сумме около 10 000 рублей.

В ходе проверки полицейские установили, что неустановленное лицо в неустановленном месте, имея умысел на хищение чужого имущества, умышленно из корыстных побуждений,

под предлогом возврата ножа в онлайн-игре путем обмана и злоупотребления доверием похитил у пострадавшего деньги.

Полицейские установили личность подозреваемого в совершении данного преступления: им оказался ранее несудимый житель города Ханты-Мансийска 1995 года рождения, который в содеянном признался.

По факту мошенничества в МО МВД России «Ханты-Мансийский» возбуждено уголовное дело по признакам состава преступления, предусмотренного ч. 1 ст. 159 Уголовного кодекса Российской Федерации (мошенничество), санкция которой предусматривает наказание в виде лишения свободы на срок до 2 лет [4]. Из указанного примера видно, что объектом мошенничества в сети Интернет послужила частная собственность жителя г. Тольятти.

Практика показывает, что наиболее распространенными видами преступлений в сети Интернет, связанных с хищениями, являются так называемые нигерийские письма, фишинг и вишинг.

Нигерийские письма являются распространенным видом киберпреступности, который получил наибольшее развитие с появлением массовых рассылок по электронной почте (т. н. «спама»). Нигерийские письма впервые появились в Нигерии, причем распространялись они в бумажной форме по обычной почте [1, 28].

Как правило, мошенники просят у получателя письма помощи во многомиллионных денежных операциях, обещая солидные проценты с сумм. Если получатель согласится участвовать, у него постепенно выманиваются крупные суммы денег якобы на оформление сделок, уплату сборов, взятки чиновникам, а потом и штрафы.

Фишинг (англ. phishing, от fishing – рыбалка) является разновидностью интернет-мошенничества. Цель фишинга заключается в получении доступа к таким конфиденциальным данным пользователей, как логин и пароль. Фишинг выполняется при помощи массовой рассылки электронной почты. Чаще всего рассылка производится от имени банков (к примеру, банк Тинькофф, Альфа-банк), интернет-сервисов (Рамблер, Яндекс), социальных сетей (Фэйсбук, ВКонтакте, Одноклассники). В письме обычно содержится прямая ссылка на сайт, который внешне неотличим от настоящего, либо на сайт с редиректом. Этот сайт создается для того, чтобы пользователь ввел свой логин и пароль. После ввода логина и пароля мошенники получают доступ к аккаунтам и банковским счетам. К примеру, в полицию г. Когалыма обратилась жительница города, которая рассказала, что в августе этого года она решила приобрести сотовый телефон на одном из Интернет-сайтов, для чего перечислила в качестве предоплаты денежные средства в сумме около двадцати восьми тысяч рублей. Спустя некоторое время ей на электронную почту пришло письмо о том, что по техническим причинам заказ не может быть выполнен, и для возврата денег ей необходимо направить заявление. После того, как когалымчанка направила письмо, ей позвонил мужчина, представившийся сотрудником интернет-магазина, и сообщил, что оно принято к рассмотрению, а пока она может оформить заказ повторно. Потерпевшая не стала дожидаться возврата денег и оформила второй заказ. На этот раз она перечислила, в качестве предоплаты, около двадцати девяти тысяч рублей. Однако спустя несколько дней сайт оказался недоступен. Все попытки дозвониться по телефону также оказались безуспешными [2].

Вишинг (vishing – voice phishing) является распространенной разновидностью сетевого мошенничества. Вишинг схож с фишингом. Отличие вишинга от фишинга состоит в том, что при вишинге используется телефон. Схема обмана при вишинге состоит в том, что в сообщении содержится просьба позвонить на определенный городской номер. При этом зачитывается сообщением, в котором потенциальную жертву просят сообщить свои конфиденциальные данные. К примеру, ввести номер карты, пароли, PIN-коды, коды доступа или другую личную информацию в тоновом наборе [1, 28].

Между тем с точки зрения уголовного закона хищение так называемых электронных денег есть не что иное, как кража, совершенная с использованием информационно-телекоммуникационных сетей, поскольку здесь нет никакого обмана либо злоупотребления доверием и потерпевший не сам отдает свои кровные сбережения, а они тайно похищаются таким своеобразным способом. О компьютерном мошенничестве, пожалуй, стоит говорить в

случаях, когда, например, потенциальный покупатель или потребитель услуг, доверившись интернет-рекламе, перечисляет на соответствующий счет определенную сумму денег, не получая взамен ни товаров, ни услуг.

Неправильное понимание сути хищения и различных форм его проявления приводит к законодательным ошибкам в процессе правоприменения статьи 159.6 УК РФ.

Нужно сказать, что правоприменительная практика по делам о преступлениях, предусматривающих ответственность за компьютерное мошенничество, крайне скудна.

Возникает вопрос: надо ли было вводить в УК РФ отдельный состав о компьютерном мошенничестве? Ведь случаи хищения чужого имущества, которые совершаются с использованием информационно-телекоммуникационных сетей, вполне укладываются в имеющиеся составы преступлений против собственности.

Следует сказать, что о необходимости выделения такой нормы говорилось во многих исследованиях.

Т. Тропина считает, что «манипуляции с компьютерными данными в целях завладения чужим имуществом или правом на чужое имущество не попадают как под действие статьи 158, так и статьи 159 УК РФ. И квалификация «компьютерных» хищений по совокупности статей 159 и 272 УК РФ противоречит одному из основных принципов уголовного права – nullum crimen, nullum poena sine lege, поскольку представляет собой применение уголовного закона по аналогии, что недопустимо» [5]. Т. Тропина считает, что дополнение ст. 159 УК РФ таким квалифицирующим признаком, как «деяние, совершенное с использованием манипулирования компьютерной информацией» либо расширение диспозиции ст. 159 УК РФ путем указания в ней признака совершения деяния, в том числе «с использованием компьютерных технологий», не решит проблемные вопросы квалификации компьютерных преступлений. Она предлагает дополнить УК РФ специальной статьей, в которой будет криминализирован вопрос приобретения прав на чужое имущество путем манипуляций с компьютерными данными [5].

Конкретные предложения о дополнении действующего УК РФ статьей о «компьютерном мошенничестве» уже вносились некоторыми учеными. Так, Д. А. Зыков предлагал ввести в УК РФ специальную статью 159-1 «Компьютерное мошенничество» – «завладение чужим имуществом путем обмана, злоупотребления доверием, присвоения, растраты либо причинение имущественного ущерба путем обмана или злоупотребления доверием, совершенное с использованием ЭВМ, системы ЭВМ или их сети» [3, 37].

Были и предложения о дополнении статей 158, 159 и 163 УК РФ таким квалифицирующим признаком, как совершение деяния с несанкционированным доступом к компьютерной системе и информационно-коммуникационным сетям, в том числе и Интернету.

На наш взгляд, достойны внимания и те, и другие варианты. Если учитывать, что совершение преступлений против собственности с использованием информационно-телекоммуникационных сетей с точки зрения учения о составе преступления не более чем способ или средство совершения указанных преступлений, логично было бы не изобретать новых составов, а дополнить уже существующие основные либо квалифицированные составы соответствующим признаком, тем более что, как уже отмечалось, многочисленные случаи хищений через Интернет или другие средства связи никак не укладываются только в рамки состава мошенничества.

В любом случае действующая на сегодняшний момент уголовно-правовая норма о компьютерном мошенничестве – статья 159.6 УК РФ не выдерживает никакой критики с точки зрения ни законодательной техники, ни ее соответствия базовым признакам хищения. Создается впечатление, что из всех предлагаемых вариантов законодатель выбрал наихудший.

Подобный, мягко говоря непрофессиональный, подход, на наш взгляд, не будет способствовать разрешению проблемы борьбы с рассматриваемыми преступлениями, прежде всего по причине сложности установления наличия в совершенных деяниях всех признаков состава того или иного преступления, в первую очередь – субъекта преступления (в силу его анонимности, объективной стороны деяния – по причине его виртуального характера; субъективной стороны – по причине сложности установления формы вины, мотива и цели). В этом

направлении необходимы глубокие исследования как теоретиков уголовного права, так и специалистов в области информационно-коммуникационных технологий [1, 30].

Разрешение данной проблемы требует всестороннего и компетентного обсуждения с привлечением широкого круга лиц – специалистов в области права, высоких технологий, общественности, иначе переложить общие принципы, подходы к противодействию киберпреступности на язык уголовного закона, не нарушая его целостности, системности, базовых положений, будет чрезвычайно трудно. Непродуманные же законодательные шаги приведут (и уже привели) к появлению в УК РФ еще целого ряда так называемых неработающих («мертвых») норм, наличие которых не только не улучшит ситуацию по противодействию преступлениям, совершаемым с использованием информационно-коммуникационных технологий, но и еще более ее усугубит.

При квалификации преступления необходимо установить наличие обязательных признаков субъекта преступления, к которым уголовный закон относит следующие:

- физическое лицо;
- вменяемое лицо;
- лицо, достигшее возраста уголовной ответственности.

При отсутствии хотя бы одного из указанных признаков лицо, совершившее общественно опасное деяние, не может быть привлечено к уголовной ответственности в качестве субъекта преступления.

Анализ ст.ст. 20, 21 УК РФ приводит к выводу, что субъект мошенничества в сети Интернет общий, т. е. вменяемое физическое лицо, достигшее возраста 16 лет.

С субъективной стороны мошенничество в сети Интернет характеризуется прямым умыслом на незаконное получение чужого имущества или приобретение права на него путем обмана или злоупотребления доверием, который возник до совершения названных действий, а также корыстной целью. К примеру, в приговоре Октябрьского районного суда г. Барнаула от 12 мая 2016 года по делу №1-154/2016 указывается, что по факту мошенничества в отношении потерпевшего П. виновность Щетинина О. С. подтверждается следующими доказательствами.

Показаниями подозреваемого Щетинина О. С. подтверждается, что ДД.ММ.ГГГГ он приехал в <адрес> на постоянное место жительства. ДД.ММ.ГГГГ около 16 часов в квартире, расположенной по адресу: <адрес>, встретившись с Ф., он согласился арендовать указанное жилое помещение. В этот же день около 18 часов он вместе с Ш. и ребенком приехал в квартиру по указанному адресу, где с Ф. заключил договор аренды, подписанный им и Ф. от имени Ч. За первый месяц проживания в квартире он перечислил Ф. 9000 рублей. В дальнейшем, нуждаясь в денежных средствах, он решил пересдать квартиру третьим лицам. С этой целью в сети Интернет на сайте «без посредников» разместил объявление о сдаче вышеуказанной квартиры в аренду. ДД.ММ.ГГГГ около 13 часов в квартиру по адресу: <адрес> приехал П., чтобы ее посмотреть. Он, обманывая последнего, пояснил, что приобрел квартиру несколько месяцев назад, документы на которую находятся у родителей. Чтобы более заинтересовать мужчину, он сообщил, что П. может снимать квартиру до лета 2016 года, а если внесет предоплату в размере 10000 рублей, то сумма арендной платы будет составлять 5000 рублей в месяц. Около 19 часов этого же дня в указанной квартире он собственноручно написал договор, в котором указал, что сдает однокомнатную меблированную квартиру по адресу: <адрес> П., оплата произведена за два месяца в сумме 10000 рублей. Далее около 19 часов 30 минут ДД.ММ.ГГГГ П. передал ему деньги в сумме 10000 рублей, о чем он (Щетинин О. С.) написал расписку. ДД.ММ.ГГГГ около 14 часов П. он передал ключи от указанной квартиры, после чего уехал. Он понимал, что данная квартира ему не принадлежит, и распоряжаться ею ему никто не разрешал (л.д. 126–131, 153–154)

Показаниями обвиняемого Щетинина О. С. подтверждается, что последний свою вину в совершении преступления, предусмотренного ч. 2 ст. 159 УК РФ, признал полностью, пояснив, что 16 ноября путем обмана он похитил у П. денежные средства в сумме 10000 рублей,

сдав ему квартиру, расположенную по адресу: <адрес>, не имея на то права. Вырученные денежные средства потратил на собственные нужды (л. д. 167–168) [7].

Как видим из указанного примера, Щетинин О. С., зная о том, что квартира была заранее арендована, умышленно путем обмана сдал квартиру заново другому лицу.

Таким образом, объективная сторона мошенничества в сети Интернет характеризуется обманом. Субъект преступления общий, а субъективная сторона характеризуется прямым умыслом и корыстной целью.

Литература

1. Гладких, В. И. Компьютерное мошенничество: а были ли основания его криминализации? [Текст] / В. И. Гладких // Российский следователь. – 2014. – № 22. – С. 25–31.

2. Две жительницы Когалыма стали жертвами Интернет-мошенников на 60 тысяч рублей [Электронный ресурс]. – Режим доступа: http://www.ugrapro.ru/2015/09/09/internet-moshenniki-polyubili-kogalyim-hmao-za-zhenskiy-pol/ (дата обращения 05.02.2017).

3. Минин, А. Я. О специфике противодействия киберпреступности [Текст] / А. Я. Минин // Российский следователь. – 2013. – № 8. – С. 37–39.

4. Полицейские Ханты-Мансийска раскрыли интернет-мошенничество [Электронный ресурс]. – Режим доступа : https://86.мвд.рф/news/item/7891330 (дата обращения 05.02.2017).

5. Тропина, Т. Компьютерное мошенничество: вопросы квалификации и законодательной техники [Электронный ресурс]. – Режим доступа: http://www.connect.ru/article.asp?id=7004 (дата обращения 05.02.2017).

6. Уголовное право. Особенная часть [Текст] : учебник / отв. ред. И. Я. Козаченко, Г. П. Новоселов. – 4-е изд., изм. и доп. – Москва : Норма, 2008. – 1008 с.

7. Приговор Октябрьского районного суда г. Барнаула от 12 мая 2016 года по делу № 1-154/2016 [Электронный ресурс]. – Режим доступа: http://sudact.ru/regular/doc/9Tug2D2AqPUp/ (дата обращения 05.02.2017).