PROBLEMS OF QUALIFICATION OF FRAUD ON THE INTERNET

Kuzmina P.G. Email: Kuzmina52@scientifictext.ru

Kuzmina Polina Gennadievna – Student,
FACULTY OF LAW,
A.A. KHMYROV KUBAN STATE UNIVERSITY, KRASNODAR

Abstract: *nowadays information technologies are rapidly merging into everyday life of every inhabitant of our planet. The growth of technical innovations replaces human labor in many ways, but at the same time facilitates its existence and makes it possible to touch the future technogenic reality. Information space changes people's lives, modernizes the model of governance of the state. All this suggests that the era of high technology is not far off, and the makings of its development are visible today. The article is devoted to the problems of qualification of the crime provided for by article. 159.6 OF THE CRIMINAL CODE. On the basis of the analysis of judicial and investigative practice it is reasoned inexpediency of criminalization of this act, options of improvement of the criminal legislation in the sphere of counteraction to plunder with use of computer technologies are offered.*
Keywords: *internet, law, problems, fraud, information.*

ПРОБЛЕМЫ КВАЛИФИКАЦИИ МОШЕННИЧЕСТВА В ИНТЕРНЕТЕ

Кузьмина П.Г.

Кузьмина Полина Геннадиевна – студент,
юридический факультет им. А.А. Хмырова,
Кубанский Государственный университет, г. Краснодар

Аннотация: *в настоящее время информационные технологии стремительно вливаются в обыденную жизнь каждого жителя нашей планеты. Рост технических новинок заменяет во многом человеческий труд, но вместе с тем облегчает его существование и дает возможность прикоснуться к будущей техногенной реальности. Информационное пространство меняет жизнь людей, модернизирует и модель управления самого государства. Все это говорит о том, что эра высоких технологий не за горами, а задатки ее развития видны уже сегодня. Статья посвящена проблемам квалификации преступления, предусмотренного ст. 159.6 УК РФ [1]. На основании анализа судебно-следственной практики аргументируется нецелесообразность криминализации этого деяния, предлагаются варианты совершенствования уголовного законодательства в сфере противодействия хищениям с использованием компьютерных технологий.*
Ключевые слова: *интернет, право, проблемы, мошенничество, информация.*

Рост информационных технологий дал толчок к развитию законотворческой деятельности уполномоченных на то органов. Сразу же возникают вопросы, касающиеся характера регулирования отношений в сети, ответственность за несоблюдение обязательств, совершения преступлений и т.д. Интернет право в целом отрасль очень молодая, имеющая большое количество пробелов, которые дают возможность мошенникам совершить то или иное противоправное действие. Мы считаем, что сейчас в сфере интернет ресурсов острым вопросом является нарушение авторских прав. Сегодня в интернете можно найти абсолютно любые книги, аудио и видео материалы, статьи, а так же и другую информацию, размещенную с нарушением прав создателя.

Сейчас мошенничество проникло во все сферы, в которых присутствуют имущественные отношения, включая цифровое пространство. Данное преступление в классическом виде включает в себя любые деяния, представляющие собой хищение чужого имущества или приобретение права на него путем обмана или злоупотребления доверием. Глобальная сеть очень часто используется для совершения правонарушений. А именно: распространение компромата, программ-вирусов, порнографии, недобросовестной рекламы, разжигания религиозных, расовых конфликтов. Еще одним популярным видом правонарушений является электронная коммерция. Электронная коммерция это способ организации бизнеса, основанный на электронных средствах коммуникации. Где, не смотря на множество систем безопасности и трудности их взлома, количество интернет мошенников не перестает увеличиваться.

Судебная практика тому подтверждение:

«Так, приговором Грачевского районного суда (Ставропольский край) от 13 июня 2013 г. Н. признана виновной в совершении преступления, предусмотренного ч. 1 ст. 159.6 УК РФ. Н., получив на мобильный телефон электронное сообщение посредством услуги «Мобильный банк» о доступном лимите денежных средств на не принадлежащем ей банковском счете, открытом на имя Ш., имея умысел на хищение указанной суммы и реализуя его, используя принадлежащий ей мобильный телефон и сим-

карту, зарегистрированную на имя Д., к которой ошибочно подключена услуга «Мобильный банк» Сбербанка России, предоставляющая право распоряжаться денежными средствами, находящимися на расчетном счету на имя Ш., путем ввода компьютерной информации в форме электрических сигналов — «СМС сообщения» на номер «900», посредством телекоммуникационной сети оператора сотовой связи «Билайн» перечислила денежные средства, находившиеся на расчетном счету Ш., на счёт, принадлежащей Н. сим-карты» [2].

Одним из громких интернет преступлений можно назвать взлом системы MasterCard.Компания MasterCard на протяжении многих лет занимается электронной валютой и обладает высочайшим уровнем безопасности. В 2005 году, хакерам удалось взломать процессинговый центр CardSystem и таким образом они получили доступ к информации о платежах различных фирм и банков. После внедрения вируса в эту систему, им удалось получить данные более чем на 40 млн. пластиковых карт, каждую из которых они могли использовать по собственному назначению. Общий объем убытков от действий этой группы мошенников составил более 3 млн. долларов, и вплоть до сегодняшнего дня, это преступление является самым «громким» по количеству украденных личных данных.

Пожалуй, стоит упомянуть и наших соотечественников из Челябинска, которым удалось похитить более 25 млн долларов с карт обычных граждан. При данной хакерской атаке, пострадало множество крупных компаний, таких как Paypal и WesternUnion. Правоохранительные органы долго не могли найти мошенников, и удалось им это только после того, как они создали фиктивную компанию, посредствам которой «заманили» злоумышленников на территорию США.

Еще одним видом преступной деятельности в сети является интернет-попрошайничество [3, с. 134-136].

Мошенники давят на жалость и отправляют письма с просьбой о помощи якобы от благотворительных организаций или нуждающихся людей. В действительности такие сообщения содержат ссылки на реальные организации и фонды, но реквизиты для перечисления денежных средств указываются ложные. Стоит запомнить, что благотворительные организации не рассылают письма пользователям, они используют другие методы и способы привлечения инвестиций.

Мошенники, занимающиеся кражей данных содержащихся на банковских картах, ловко научились подделывать свои письма под официальные сообщения от всевозможных организаций. Они используют логотипы этих компаний и копируют стиль легальной корреспонденции. В письме может содержаться просьба о переходе по предложенной в тексте документа ссылке, где необходимо будет ввести ваши персональные данные, якобы для обеспечения безопасности данных пользователя. Пройдя по указанной в уведомлении ссылке, вы попадаете на сайт мошенников, который выглядит, как настоящий. Вы, ничего не подозревая, вводите свой логин и пароль, после этого персональные данные отправляются злоумышленникам, а пользователь перенаправляется на реальный сайт. Данные способы мошенничества являются сейчас самыми популярными не только в нашей стране, но и во всем мире [4, с.12].

Однако уже сегодня можно констатировать существование некоторых проблем при реализации уголовно-правовых норм о мошенничестве, обусловленных избыточностью криминализации этого деяния. Среди них следует выделить, прежде всего, такие проблемы, как:

- конкуренцию уголовно-правовых норм, предусматривающих различные виды мошенничества;
- отграничение мошенничества от смежных составов преступлений;
- квалификацию мошенничества по совокупности с другими преступлениями, предусмотренными УК РФ;
- определение содержания новых терминов, раскрывающих признаки специальных видов мошенничества;
- дифференциацию уголовного наказания за различные виды мошенничества.

Прежде всего, стоит отметить проблемы разграничения специальных видов мошенничества и общего состава мошенничества, предусмотренного ст. 159 УК РФ. На первый взгляд, эта проблема должна решаться по правилу конкуренции общей и специальной норм, которое предусмотрено ч. 3 ст. 17 УК РФ. Однако неудачная редакция новых составов мошенничества не всегда позволяет сделать такой однозначный вывод.

Стоит также отметить проблему разграничения мошенничества и смежных составов преступления. Причем речь должна идти не о ранее существовавшей проблеме отграничения мошенничества от других преступлений, например, от причинения имущественного ущерба путем обмана или злоупотребления доверием, предусмотренного ст. 165 УК РФ. Возникли новые аспекты этой проблемы, в частности, вопрос о разграничении преступлений, предусмотренных ст. 159.1 и 176 УК РФ, так как обе статьи предусматривают кредитный обман.

В УК РФ указаны шесть составов, которые касаются интернет преступлений: мошенничество в сфере кредитования (ст. 159.1 УК РФ), при получении выплат (ст. 159.2 УК РФ), с использованием платежных карт (ст. 159.3 УК РФ), в сфере предпринимательской деятельности (ст. 159.4 УК РФ), в сфере страхования (ст. 159.5 УК РФ), в сфере компьютерной информации (ст. 159.6 УК РФ). Также, стоит

отметить, что ч. 4 ст. 159 УК РФ дополнена таким квалифицирующим признаком, как мошенничество, повлекшее лишение права гражданина на жилое помещение [5].

Законодательством РФ предусмотрена уголовная ответственность за преступления совершенные в сети Интернет. Глава 28 УК РФ регламентирует порядок назначения наказания за данную категорию правонарушений. Например, по ст. 272 «Неправомерный доступ к компьютерной информации» лица, взломавшие вашу страницу в социальных сетях, электронную почту или незаконно сменившие пароли понесут наказание в виде штрафа, размер которого составляет от 200 до 500 МРОТ. За те же нарушения, совершенные несколькими лицами (по большей части мошенники работают в группе) предусмотрено наказание в виде штрафа, составляющего от 500 до 800 МРОТ. Также наказан будет и тот, кто прочтет закрытую от всех информацию в социальных сетях или на других Интернет-ресурсах (путем взлома или другим незаконным способом).

Современное общество не представляет свою жизнь без использования Интернета, а мошенники активно этим пользуются. Сколько бы законодатели не ужесточали ответственность за преступления во Всемирной Паутине, мошенников от этого меньше не становится. Так как наши соотечественники очень доверчивы и любую информацию принимают за чистую монету, преступники не перестают изобретать новые и совершенствовать старые способы обмана населения. Число лиц, пострадавших от интернет-преступлений, ежегодно увеличивается.

По словам же самих чиновников в последние годы в России происходят положительные изменения в обеспечении сохранности личной информации пользователей в сети Интернет. Это только на словах. В действительности преступлений в сети Интернет меньше не становиться, просто чиновники научились замалчивать это, как и многое другое.

Список литературы / References

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 21.07.2014) // Собрание законодательства РФ, 1996. № 25. Ст. 2954.
2. О судебной практике по делам о мошенничестве, присвоении и растрате: Постановление Пленума Верховного Суда РФ от 27.12.2013 № 51 // Российская газета. 2013.
3. *Ермакова О.В*. Специальные виды мошенничества (ст. 159.1–159.6 УК РФ): некоторые вопросы квалификации // Вестник Алтайской академии экономики и права, 2014. № 3 (35). С. 134-136.
4. *Медведев С.С*. Мошенничество в сфере высоких технологий: автореф. дис. канд. юрид. наук. Краснодар, 2008. С. 12.
5. О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации: Федеральный закон от 29.11.2012 № 207-ФЗ // Собрание законодательства РФ, 2012. № 49. Ст. 6752.