

Моторов А.А.,

магистрант

2 курс, факультет «Юридический»

Ивановский государственный университет

Россия, г. Иваново

ЕСТЬ ЛИ СВЯЗЬ МЕЖДУ ФИШИНГОМ И МОШЕННИЧЕСТВОМ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ?

***Аннотация:** Статья посвящена проблемам, возникающим при квалификации преступлений, совершенных посредством фишинга. Рассматриваются примеры из судебной практики, касающиеся юридической оценки деяний, в ходе которых применялись фишинговые атаки. Предлагаются варианты квалификации указанных преступлений с учетом разъяснений постановления Пленума Верховного Суда РФ от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате».*

***Ключевые слова:** фишинг, мошенничество в сфере компьютерной информации, кража, мошенничество.*

***Annotation:** The article is devoted to the problems arising in the qualification of crimes committed through phishing. Examples from judicial practice concerning the legal assessment of acts during which phishing attacks were used are considered. The variants of the qualification of these crimes are proposed, taking into account the explanations of the resolution of the Plenum of the Supreme Court of the Russian Federation No. 48 dated 30.11.2017 "On judicial practice in cases of fraud, assignment and embezzlement".*

***Key words:** phishing, fraud in the field of computer information, theft, fraud.*

С увеличением количества людей, использующих сеть «Интернет» и цифровые технологии, растет и количество киберпреступлений. Эти преступления представляют серьезную угрозу как для граждан, так и для организаций, поскольку могут нанести значительный экономический ущерб физическим лицам, компаниям и государству в целом. Преступники, используя новые информационные технологии, формируют новые способы хищения денежных средств. Законодатель зачастую попросту не успевает своевременно адаптировать уголовно – правовые нормы для их соответствия произошедшим информационным изменениям. В связи с этим в науке и следственно – судебной практике отсутствует единообразное понимание признаков составов преступлений, связанных с компьютерными технологиями, в частности мошенничества в сфере компьютерной информации.

Так, некоторые ученые относят к способам совершения мошенничества в сфере компьютерной информации так называемый фишинг. Так, например, Шевелева С.В. указывает следующее: «Если выполнение объективной стороны мошенничества в сфере компьютерной информации происходит с участием лица, который заблуждается в истинности информации, например, фишинг, такое деяние необходимо оценивать как мошенничество в сфере компьютерной информации[1, с. 232]. Абдульмянова Т.В. в качестве одного из способов интернет мошенничества выделяет фишинг, указывая, что в таком случае жертва добросовестно передает свои данные[2, с. 139]. Поддерживает указанную позицию и Степанова К.В., отмечая, что мошенничество в сфере компьютерной информации может осуществляться путем фишинга и вишинга[3, с. 74]. Шумихин В.Г. в свою очередь указывает, что способ должен проявляться в незаконном воздействии на программное обеспечение серверов, компьютеров или на сами информационно – телекоммуникационные сети[4, с. 735]. Различные точки зрения на способы мошенничества в сфере компьютерной информации обусловлены отсутствием классического обмана

в диспозиции статьи 159.6 УК РФ. Для этого состава преступления не характерно введение лица в заблуждение при непосредственном устном или письменном контакте. При исследовании компьютерного мошенничества об обмане можно говорить весьма условно, правильнее указывать, что происходит преодоление средств программно – технической защиты. В свою очередь, под фишингом необходимо понимать получение доступа к информации, чаще всего личной или имеющей юридическое значение, путем выдачи себя за доверенное лицо или организацию. В большинстве случаев фишинг осуществляется посредством смс – рассылки или через электронную почту, сообщения в социальных сетях или веб – сайты, которые имитируют официальные страницы банков, онлайн магазинов, благотворительных организаций и других сервисов. Следует согласиться с Батюшкиным М.В., который указывает, что фишинг осуществляется путем обмана или с использованием методов социальной инженерии[5, с. 91]. Необходимо отметить, что сам по себе, фишинг не является уголовно – наказуемым деянием на территории Российской Федерации. Важно понимать, что при фишинге не происходит никакого вмешательства в компьютерную информацию или информационно – телекоммуникационную сеть. Данный способ состоит в том, что злоумышленник создает сайт, сходный до такой степени, что обычный, а иногда даже опытный пользователь интернета, не увидит никаких различий между подлинной и поддельной веб – страницей, предназначенной для получения данных жертвы. Далее различным путями преступник привлекает людей на такой сайт, например посредством рассылки сообщений на электронную почту. В некоторых случаях пользователь может случайно зайти на такой веб – сайт, найдя его в строке поискового запроса своего браузера. И самое главное – жертва добровольно введет, передаст свои данные злоумышленнику, заблуждаясь в подлинном характере интернет сайта, воздействия на компьютерную информацию потерпевшего не

произойдет. Единообразная практика по данному вопросу отсутствует и в решениях судов.

Так судом было установлено, что подсудимый нашел в социальной сети гражданку А., с которой ранее не встречался. Обманывая ее относительно своих настоящих целей, он предложил оформить банковскую карту под предлогом перевода заработной платы иностранным работникам. Не раскрыв своих настоящих намерений, он заверил А., что она получит денежное вознаграждение за оформление карты, на что она согласилась. После этого виновный передал полученную карту своим соучастникам. Затем неустановленный соучастник, используя данные банковской карты, полученные путем фишинговой атаки во время пребывания потенциальной жертвы в интернете на поддельном сайте банка, инициировал операцию по переводу средств с карты А. на карту подсудимого. Впоследствии второй соучастник обналичил похищенные деньги через банкомат. Действия виновного были квалифицированы по ч. 2 ст. 159.6 УК РФ. Раскрывая объективную сторону, суд лишь указал, что имело место вмешательство в функционирование средств хранения, обработки и передачи компьютерной информации, дальнейшая конкретизация данного способа отсутствует[6].

В другом случае, Октябрьским районным судом города Ижевска установлено, что Канус В.Н. и Шигапов Э.Р., знали диапазон телефонных номеров клиентов ООО "Т2 Мобайл" в Ямало-Ненецком автономном округе. Используя ноутбук "ACER" и программу, предназначенную для массовой отправки SMS-сообщений и электронного маркетинга, они воспользовались коммутатором со слотами для сим-карт и совершили массовую рассылку SMS (фишинг) гражданам на их телефонные номера. Сообщения содержали заведомо недостоверную информацию о блокировке банковских карт, а также указывали абонентский номер для получения дополнительной информации. Одно из подобных SMS-сообщений было доставлено на абонентский номер, который использовал К.О.А.. В тот же день К.О.А. позвонил по указанному в

сообщении абонентскому номеру с целью выяснения причин блокировки его банковской карты. В ходе разговора виновные представились сотрудниками департамента безопасности банка и сообщили заведомо ложные сведения о блокировке банковской карты К.О.А.. Продолжая свои преступные действия, Шигапов Э.Р. пояснил К.О.А., что для разблокировки его банковской карты последний должен сообщить все реквизиты своей банковской карты. В то же время, К.О.А., полагая, что последний действительно является сотрудником департамента безопасности банка, сообщил все реквизиты своей банковской карты, а также согласился сообщить одноразовые пароли, необходимые для получения доступа к безналичным денежным средствам. После чего виновные, зайдя на Интернет сайт банка, авторизовались под имеющимися данными и осуществили перевод денежных средств со счета потерпевшего на счет банковской карты, которая находилась в пользовании подсудимых. Действия виновных были квалифицированы по п.п. «а», «в» ч. 2 ст. 158 УК РФ[7].

В заключительном примере виновный совершал аналогичные действия по рассылке смс – сообщений (фишинг) гражданам. Потерпевшая, будучи введенной в заблуждение, сообщила данные своей банковской карты, а также одноразовые пароли. Далее, подсудимый с помощью сервиса «UBANK» ввел все реквизиты банковской карты, необходимые для перечисления с лицевого счета банковской карты потерпевшей денежных средств на баланс сим-карты оператора сотовой связи ООО «Т2 Мобаил», используемой виновным в своих преступных целях. Действия подсудимого были переклассифицированы с ч. 2 ст. 159 УК РФ на п. «в» ч. 2 ст. 158 УК РФ. Суд обосновал свою позицию тем, что обман был направлен на завладение конфиденциальными данными держателя карты, а не на завладение его денежными средствами[8].

В таком случае возникает вопрос – как правильно квалифицировать содеянное, если оценка по ст. 159.6 УК РФ не представляется возможной. С одной стороны мы имеем первый абзац 21 пункта Постановления Пленума

Верховного Суда от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении, растрате». При анализе этого пункта можно сделать вывод, что содеянное необходимо квалифицировать как кражу. Однако следующий абзац этого же пункта гласит иное: «Если хищение чужого имущества или приобретение права на чужое имущество осуществляется путем распространения заведомо ложных сведений в информационно-телекоммуникационных сетях, включая сеть "Интернет" (например, создание поддельных сайтов благотворительных организаций, интернет – магазинов, использование электронной почты), то такое мошенничество следует квалифицировать по статье 159, а не 159.6 УК РФ»[9]. С одной стороны, аналогичные деяния могут квалифицироваться по разным статьям Особенной части УК РФ. С другой стороны, при более детальном анализе данных разъяснений можно сделать иной вывод. В тех случаях, когда лицо создает, например, поддельный сайт интернет магазина, предполагается что потерпевший сам, лично переведет деньги на счет злоумышленника, оплачивая какую – либо покупку. Следовательно, такие действия необходимо оценивать как мошенничество, предусмотренное ст. 159 УК РФ. В случае если фишинг был направлен за владение данными держателя карты, перечисление денежных средств со счета потерпевшего осуществлялось виновным, содеянное необходимо квалифицировать по ст. 158 УК РФ.

Литература:

1. Шевелева С.В. Мошенничество в сфере компьютерной информации: особенности квалификации и конкуренции со смежными составами преступлений // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2017. №4. С. 229-234.
2. Абдульмянова Т.В., Асанова И.П., Данилов В.В. Мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ): понятие, уголовно-

правовая характеристика и некоторые особенности расследования // Вопросы российского и международного права. 2021. № 1. С. 134-145.

3. Степанова К.В. Мошенничество в сфере компьютерной информации: российский и зарубежный опыт // Имущественные отношения в Российской Федерации. 2022. № 8. С. 32-38.

4. Шумихин В.Г. Судебное и доктринальное толкования способа мошенничества в сфере компьютерной информации // Пермский юридический альманах. Ежегодный научный журнал. 2019. № 2. С. 733–740.

5. Батюшкин М.В. "Фишинг" - компьютерное мошенничество? // Символ науки: международный научный журнал. 2021. № 1. С. 90-93.

6. Приговор Преображенского районного суда г. Москвы от 05.03.2014 по делу № 1-74/2014. URL: <https://sudact.ru/regular/doc/jA8GpwXbeVmJ/> (дата обращения: 03.11.2023).

7. Приговор Октябрьского районного суда г. Ижевска от 26.11.2018 по делу № 1-308/2018. URL: <https://sudact.ru/regular/doc/GyMZf1QVGXVC/> (дата обращения: 04.11.2023).

8. Приговор Ленинского районного суда г. Ижевска от 13.11.2018 по делу № 1-282/2018. URL: <https://sudact.ru/regular/doc/UZrPj5SIRamY/> (дата обращения: 04.11.2023).

9. О судебной практике по уголовным делам о мошенничестве, присвоении и растрате: Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 // Бюллетень Верховного Суда РФ. 2018. № 2.