Коновалова Ксения Владимировна
магистрант
Ермакова Татьяна Николаевна
канд. юрид. наук, доцент
ФГБОУ ВО «Вятский государственный университет»
г. Киров, Кировская область

DOI 10.21661/r-113210

МОШЕННИЧЕСТВО В СФЕРЕ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ И СЕТИ ИНТЕРНЕТ – СОВРЕМЕННАЯ УГРОЗА

***Аннотация**: в статье дается криминологическая характеристика одного из самых распространенных преступлений современности – мошенничества в сфере компьютерных технологий. В работе рассматриваются различные формы проявления мошенничества, а также меры, необходимые для защиты от мошенничества.*

***Ключевые слова**: преступление, имущество, обман, злоупотребление доверием, истина, фальсификация, сделка, оборот, электронная почта, мошенничество, злоумышленник, модификация, фишинговые письма.*

Издавна мошенничество являлось одним из самых распространенных преступлений в большинстве стран мира. Россия в этом отношении не является исключением, тем более учитывая тот факт, что мошенничество отличается способностью быстро изменять формы проявления и проникать, практически во все сферы общественной жизни [1, с. 96]. Не обошло стороной мошенничество и сферу информационно-коммуникационных технологий. Рассматривая мошенничество в данной сфере, мы также берем за основу общее понятие мошенничества – хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.

При этом под обманом понимается как сознательное искажение истины (активный обман), так и умолчание об истине (пассивный обман). В обоих случаях обманутая жертва сама передает свое имущество мошеннику [5].

Форма мошеннических обманов очень разнообразна. Обман может совершаться в виде устного или письменного сообщения, либо заключаться в совершении каких-либо действий: фальсификации предмета сделки, применение шулерских приемов при игре в карты или «в напёрсток», подмена отсчитанной денежной суммы фальсифицированным предметом («куклой»), обвести т. п. Очень часто обман действием сочетается со словесным [4].

Мошенники действуют практически в каждой сфере деятельности, но с приходом в жизнь человека различных средств коммуникации, деятельность мошенников приобрела новые обороты. Постоянное нахождение в социальных сетях, общение через электронную почту, покупка товаров через интернет. Зачастую люди не задумываясь, выкладывают свои персональные данные в сеть, к примеру, для поиска работы. Все это, конечно же, привлекает преступников.

Современное общество настолько компьютеризировалось, что пользователи совершенно забывают об элементарной безопасности в сети. Если раньше, совершая покупку в магазине, не говоря уже об уличных ларьках, человек был осторожен, то сейчас, покупая в интернете, он не задумываясь отправляет денежные средства на непроверенные счета и не получает товар, за который, зачастую, платит немаленькие деньги. По данным Европейской комиссии, количество фиктивных операций с покупками в интернете выросло в полтора раза.

Очень успешным инструментом в руках преступников является электронная почта. Многие не раз видели у себя на электронной почте письма с предложениями сомнительных финансовых операций и быстрого заработка через сеть Интернет. Большинство из них, конечно же, являются махинациями. Потребители должны быть очень внимательными в отношении всех, кто предлагает им легкие деньги или бесплатные услуги. Издержки от них могут оказаться очень большими.

Ярким примером такого мошенничества является предложение работы на дому или на удаленном доступе. Мошенник предлагает потенциальному работнику за определенную сумму перепечатать текст, который отправляется ему на электронную почту, после выполнения. Результат работы отправляется на уже

известный адрес, после чего, происходит перечисление заработной платы. Казалось бы, схема практически прозрачная, и, в случае, если даже мошенник-работодатель ничего не заплатит, работник не понесет никаких убытков, кроме собственных сил. Но зачастую, после согласия работника, «работодатель» присылает письмо, в котором говорится, что для продолжения сотрудничества необходимо внести определенную сумму на «счет издательства», чтобы получить гарантию в том, что работник действительно выполнит задание, денежные средства обещают вернуть с первой же выплатой зарплаты. В действительности, после перечисления денежных средств работником, «работодатель» больше не выходит на связь.

Вот еще один пример мошенничества, особо распространенный в США. Некий «спецназовец» просил получателей послания помочь ему вывезти найденные наличные с территории Афганистана, обещая за это солидный процент от общей суммы. Дождавшись, когда жертва клюнет на приманку, жулики через какое-то время сообщают, что для перевода или перевозки денег нужны дополнительные расходы на адвокатов, налоги, разрешения и т. п., требуя, чтобы новые «партнеры» взяли на себя эти «непредвиденные» расходы. Получив деньги, они бесследно исчезают [3].

Только в США жертвами таких схем стали 2,6 тыс. человек. Из них 16 американцев расстались с 345 тысячами долларов, двое потеряли по 70 тысяч долларов.

Но в данных случаях пострадавшие сами идут на риск и поддаются влиянию мошенников.

Зачастую, люди даже не знают, что с помощью их аккаунтов либо паролей доступа к каким-либо данным, могут совершаться мошеннические действия. Например, ввод логина и пароля зарегистрированного пользователя и получение таким образом легального доступа к ресурсам локальной сети предприятия, чтобы в дальнейшем осуществить хищение чужого имущества.

Так же мошенники могут модифицировать компьютерную информацию, например: подмена платежных реквизитов для незаконного получения денежных средств.

Чаще всего мошенники используют сразу несколько способов для совершения преступного деяния, к примеру: отправка сообщения легальному пользователю с целью заражения компьютера. Троянская программа, содержащаяся в письме, осуществляет сбор информации (логины, пароли), удаление правил безопасности межсетевого экрана и модификацию таблицы разрешенных ip-адресов. Затем нарушитель получает полный доступ к информационным ресурсам путем ввода полученного логина и пароля со своего компьютера [2].

Так же очень распространен такой вид мошенничества как фишинговые письма [6]. Это один из наиболее активно развивающихся видов мошенничества. Фишинговые письма представляют собой электронные сообщения от злоумышленника, оформленные, как официальные письма от банка, университета, провайдера. Они направляются с целью получения логина и пароля пользователя к информационной системе с целью присвоения денежных средств, либо других ценных ресурсов. Такие письма содержат ссылки на сайт-копию организации, от имени которой якобы отправлено это письмо. Пользователь вводит свои данные на поддельном сайте, чем в результате и пользуются злоумышленники. Благодаря невнимательности и халатному отношению пользователей, фишинговые письма используются мошенниками довольно успешно.

В заключении хотелось бы отметить, что как бы ни были законодательно урегулированы меры ответственности за совершение такого рода преступлений, внимательность пользователей компьютерной техники всегда будет играть большую роль. Излишнее проявление доверия к незнакомым людям, письмам с неизвестных адресов, SMS и звонкам, приводит к негативным последствиям. Чтобы их избежать, необходимо проявлять бдительность и осознавать возможные риски своих действий.

Список литературы

1. Ермакова Т.Н. Мошенничество в кредитно-банковской сфере [Текст] / Т.Н. Ермакова // Вестник Вятского государственного гуманитарного университета. – 2010. – №3 (1). – С. 96–100.

2. Информационная справка по видам мошенничества [Электронный ресурс]. – Режим доступа: http://muuo.ucoz.ru/Novosti/Novosti2/novosti3/novosti2015/pamjatka_ot_moshennikov.pdf

3. Ловушка в интернете [Электронный ресурс]. – Режим доступа: http://palm.newsru.com/world/24May2002/inet_36.html

4. Прокуратура Нагорского района Кировской [Электронный ресурс]. – Режим доступа: http://prokurornagorsk.ucoz.ru/publ/o_moshennichestve/1–1-0–430

5. Уголовный кодекс Российской Федерации: Федер. закон: принят Гос. Думой РФ 13.06.1996] // Консультант Плюс. СЗ РФ. – 17.06.1996. – №25. – Ст. 2954.

6. Фишинг – что это. Методы и способы защиты [Электронный ресурс]. – Режим доступа: http://pro-spo.ru/informaczionnaya-bezopasnost/3624-metody-mirovogo-fishinga