УДК 343.140.02

Попова Д.В.,
магистрантка
2 курс, юридический факультет
Высшая школа экономики, управления и права
Северный (Арктический) федеральный университет им. М.В. Ломоносова,
Россия, г. Архангельск

ВИНОВНОСТЬ ЛИЦА, КАК ОБСТОЯТЕЛЬСТВО ПОДЛЕЖАЩЕЕ УСТАНОВЛЕНИЮ ПО УГОЛОВНЫМ ДЕЛАМ О МОШЕННИЧЕСТВЕ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Аннотация: *в статье рассматриваются вопросы доказывания виновности лица по уголовным делам о мошенничестве в сфере компьютерной информации.*

Ключевые слова: *мошенничество, компьютерная информация, виновность, доказывание.*

Abstract: *the article discusses the issues of proving the guilt of a person in criminal cases of computer information fraud.*

Keywords: *fraud, computer information, guilt, proving.*

Так, согласно статье 73 УПК РФ, одним из обстоятельств, подлежащих доказыванию, является виновность лица, совершившего деяние, форма его вины и мотивы деяния. Доказать виновность обвиняемого − значит установить, было ли преступление совершено данным лицом при наличии умысла или по неосторожности (субъект и субъективная сторона состава преступления), а так же факты необходимые для признания лица так называемого специального субъекта преступления. В качестве непосредственных обстоятельств, характеризующих личность обвиняемого подразумеваются: формальные (установочные) данные о личности (фамилия, имя, отчество, год рождения и т.д.)

и данные, которые отражают его общественный статус, «характеризующие его как члена общества» [5].

И.М. Комаров отмечает следующие положительные стороны введения в УК РФ ст. 159.6: «Практика правоприменения свидетельствует о том, что, оценив криминальную ситуацию с использованием преступниками компьютерных способов и средств, законодатель в ноябре 2012 года существенно изменил соответствующее уголовное законодательство и «упростил» уголовно-правовую характеристику установления преступного факта по ряду противоправных деяний, которые до этого требовали от органа предварительного расследования проведения дополнительных следственных мероприятий, связанных с доказыванием виновности лица в совершении компьютерного преступления. Это оптимизировало процесс расследования и позволило значительно сократить доказательственные процедуры, что в свою очередь сказалось на сроках предварительного расследования в сторону их сокращения, а также собственно на результатах расследования» [4, с. 120].

Субъект преступления по ст. 159.6 УК РФ − общий (вменяемое физическое лицо, достигшее 16-летнего возраста), за исключением компьютерного мошенничества, совершённого лицом с использованием своего служебного положения (ч. 3 ст. 159.6 УК РФ) [3]. Последнее характеризуется наличием специального субъекта − должностного лица, обладающего признаками, предусмотренными Примечанием 1 к ст. 285 УК РФ, государственного или муниципального служащего, который не является должностным лицом, а также иного лица, отвечающего требованиям, предусмотренным Примечанием 1 к ст. 201 УК РФ (п. 29 Постановления Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате»).

Отсюда, субъективная сторона характеризуется прямым умыслом (ч. 2 ст. 25 УК РФ): виновный должен осознавать степень общественной опасности своих действий по вводу, удалению, блокированию, модификации компьютерной информации или иному вмешательству в функционирование

средств хранения, обработки или передачи компьютерной информации либо информационно-телекоммуникационных сетей, предвидеть возможность или неизбежность наступления общественно опасных последствий в виде причинения ущерба собственнику или иному владельцу чужого имущества и желать их наступления. Мотив здесь − чаще всего корыстный, т.е. побуждение к получению материальной выгоды для виновного либо других лиц или избавлению от материальных затрат (абз. 1 п. 11 Постановления Пленума Верховного Суда РФ от 27 января 1999 г. № 1 «О судебной практике по делам об убийстве (ст. 105 УК РФ)»). Реже бывает мотив самоутверждения. Цель − во всех случаях корыстная.

Уголовное право, и разъяснения Пленума Верховного Суда РФ только лишь в общих чертах ориентирует следователя на то, какие обстоятельства нужно доказать для установления события преступления, в том числе компьютерного мошенничества. Так, например, только заявление потерпевшего о том, что он передал свое имущество или право на имущество под влиянием обмана, является доказательством того, что он был обманут.

Необходимо точно установить, какая информация была им сообщена, в чем заключается «ложность» этой информации, как воспринимала жертва информацию, что было основанием для сомнения в «истинности». Для выдвижения версий о субъекте, о его виновности следователю дает основания детальный разбор средства совершения преступления, детали взаимоотношений между жертвой и исполнителем, физические данные потенциального виновного, профессиональные навыки, психологическое состояние на момент совершения преступления и т.д.

Исходя из диспозиции и квалифицирующих признаков ст. 159.6 УК РФ, ст. 61, 63 УК РФ, а также ст. 73 УПК РФ по делам о мошенничестве в сфере компьютерной информации установлению подлежат следующие обстоятельства: 1) тип программного обеспечения, которое используется потерпевшим, когда и кем оно установлено, кто мог иметь доступ к компьютерам; 2) какое программное обеспечение использовано лицами,

совершившими преступное деяние, какие возможности у данного обеспечения, откуда было получено; 3) каким компьютером пользовались, когда, в каких целях были осуществлены ввод, удаление, блокирование, модификация компьютерной информации либо иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей потерпевшего; 4) когда и как было осуществлено хищение чужого имущества или это было приобретением права на чужое имущество; 5) где находятся компьютеры и иное оборудование, документы, транспортные средства и т.п., все, что было использовано в процессе совершения преступления; 6) пострадавшая сторона, кому причинен материальный ущерб: лицо, чья компьютерная информация была подвергнута преступному воздействию или вред причинен другому лицу (лицам); 7) совершено ли было мошенничество единолично или группой лиц; 8) если действовала группа лиц, то какой состав этой группы, когда организована, кем, с какой целью, существуют ли роли в группе, все ли члены группы знали о способе совершения предстоящего преступления; 9) было ли у лица, совершившего мошенничество разрешенный (законный) доступ к компьютерной информации, (является ли данное лицо должностным); 10) имеет ли место предварительная договоренность о сумме хищения, о имуществе, все ли члены группы знали об этом, были ли согласны на хищение именно на эту сумму; 11) какой размер причиненного материального ущерба; 12) является ли для потерпевшего причиненный ущерб значительным с учетом материального положения потерпевшего и других юридически значимых обстоятельств; 13) где находится похищенное имущество, возможности изъятия; 14) если имущество уже растрачено и его изъятие невозможно, на какие цели, что именно приобретено на средства, добытые преступным путем, где теперь находится это имущество; 15) причины и условия, способствовавшие совершению преступления; 16) имеются ли обстоятельства, исключающие преступность и наказуемость деяния, смягчающие либо отягчающие наказание [5]. То, что именно эти обстоятельства входят в предмет доказывания по делам о

мошенничестве в сфере компьютерной информации, можно проиллюстрировать на примере одного из приговоров по ст. 159.6 УК РФ.

В приговоре Автозаводского районного суда г. Тольятти Самарской области от 18.06.2018 по № 1-452/2018 также видно, что по делам о мошенничестве необходимо устанавливать, какие компьютерные программы были использованы для совершения преступления, несмотря на то, что из приговора судом данные об этих программах изъяты, тем не менее, суд установил, что мошенничество совершено именно в сфере компьютерной информации, сослался на программы, которые были использованы.

Аналогичные обстоятельства были установлены судом при вынесении приговора в отношении Минитаевой А.А. по ч. 3 ст. 159.6 УК РФ [2]. В процессе судебного разбирательства суд установил, что: 1) хищение было совершено путём ввода, модификации компьютерной информации, выразившейся в том, что подсудимая, используя свое служебное положение, подключилась к лицевому счету МУ МВД России «Энгельское», с находящимися на нём денежными средствами, принадлежащими ПАО «МегаФон», и, убедившись, что на нем имеются денежные средства, в информационно-биллинговой системе изменила категорию клиента с «кредитный» на «предоплатный», статус клиента с «временно закрыт» на «действующий», класс клиента с «аннулированный» на «корпоративный»; 2) хищения были объединены единым умыслом, совершены в несколько этапов в период 03.01.2017 по 29.04.2017 г., по каждому из эпизодов было установлено время его совершения; 3) суд установил, что сумма ущерба составила 28 853 руб., ущерб причинен ПАО «Мегафон»; 4) похищенными деньгами подсудимая распорядилась на своеусмотрение; 5) преступление подсудимая совершила одна; 6) при определении меры наказания суд учел личность обвиняемой. Наличие смягчающих наказание обстоятельств, таких как признание вины, раскаяние, активное способствование раскрытию и расследованию преступления, добровольное возмещение причиненного материального ущерба, состояние здоровья подсудимой и членов ее семьи,

положительную характеристику подсудимой по месту жительства и прежнему месту работы.

Т.е. установлена личность − сама причастность лица к совершению преступного деяния. Установлено психическое отношения лица к своему противоправному поведению и его последствиям, имеющего форму умысла. И мотив преступления − это непосредственная внутренняя побудительная причина преступного деяния. На стадии досудебного производства установлены обстоятельства, характеризующие личность обвиняемого, которые учтены судом при вынесении приговора.

Анализируя судебную практику, можно прийти к обоснованному выводу, что потерпевший может ничего не знать о передаче имущества или права на имущество и вообще не желать этого, т.е. здесь отсутствует обязательный волевой признак − добровольность. Так, приговором Кировского районного суда г. Курска от 15 мая 2014 года, С. был признан виновным по ч. 2 ст. 159.6 УК РФ. С. приобрел сим-карту, с подключенной бывшим ее владельцем услугой «Мобильный банк», на которую приходили смс-уведомления о движении денежных средств. С., понимая, что имеет доступ к компьютерной системе ОАО «Сбербанк России» и к управлению счетом банковской карты ОАО «Сбербанк России», зарегистрированной на другого человека, с последующей модификацией информации о состоянии счета, посредством мобильного телефона с использованием услуги «Мобильный банк» путем формирования и отправки смс-сообщения на специальный номер зачислил со счета указанной банковской карты на счет абонентского номера денежные средства в сумме 10 000 рублей [2].

Подобное деяние совпадает по объективным признакам с кражей, поскольку происходит тайное изъятие имущества, что характерно для данной формы хищения. Аналогичное мнение высказывает и профессор Н.А. Лопашенко: «…здесь надо говорить о специфическом тайном завладении чужим имуществом путем применения компьютерных технологий, т.е. о краже» [4].

Более того, суды сами, давая правовую оценку деянию, характеризуют его как тайное. В соответствии с материалами уголовного дела № 1-146/2013 мирового суда судебного участка Ковдорского района Мурманской области в декабре 2013 г. подсудимый Р. был признан виновным в мошенничестве в сфере компьютерной информации по ч. 1 ст. 159.6 УК РФ. В приговоре была использована формулировка: «продолжая реализовывать свой преступный умысел, направленный на тайное хищение чужого имущества, Р. 13 июня 2013 года, находясь в г. Ковдоре, с абонентского номера направил смс-сообщение на единый абонентский номер ОАО «Сбербанк России», с указанием кодовой команды, осуществив вмешательство в функционирование банковского сервера, на котором хранится информация о счетах клиентов ОАО «Сбербанк России» [2].

Сравнение статей 159.6 и ст. 272 УК РФ, позволяет сделать вывод, что в мошенничестве в сфере компьютерной информации указаны именно действия, которые должен осуществить виновный (ввод, удаление, блокирование, модификация, либо иное вмешательство), а в ст. 272 УК РФ говорится о необходимых последствиях (уничтожение, блокирование, модификация, копирование) в результате неправомерного доступа к охраняемой законом компьютерной информации. Получается, что, если в результате совершения мошенничества в сфере компьютерной информации (159.6 УК РФ) наступят последствия, указанные в ст. 272 УК РФ, а они, как правило, должны наступить, учитывая характер действий, то все равно потребуется дополнительная квалификация по ст. 272 УК РФ, как этого ранее требовалась до введения специальных видов мошенничества.

Однако в практике, ввиду отсутствия четких указаний, не выработалось единого мнения на этот счет. В одних ситуациях происходит дополнительная квалификация, а в других нет. Так, в соответствии материалами уголовного дела № 1-153/2014 Октябрьский районный суд г. Самары от 18 июня 2014 года, признал И. виновной в совершении преступлений, предусмотренных ч. 3 ст. 272, ч. 3 ст. 159.6 УК РФ. И., работая в должности специалиста офиса

продаж и обслуживания ООО «Л», являлась должностным лицом, решила совершить неправомерный доступ к охраняемой законом компьютерной информации, содержащей персональные данные клиентов ОАО «Л» и их лицевых счетов, из корыстной заинтересованности, сцелью получения выгоды имущественного характера. В отсутствие соответствующего заявления клиента произвела замену сим-карты, в результате чего у нее появилась возможность пользоваться лицевым счетом абонента и распоряжаться, находящимися на нем денежными средствами [2].

Таким образом, при доказывании виновности важная роль отводится знаниям компьютерно-технических технологий и соответствующей терминологии, так как имеет важное значение для правильной формулировки вопросов к лицам, совершившим такие преступления и к свидетелям, а также для получения правдивых ответов на поставленные вопросы.

При оценке выявленных первоначальных следственных ситуаций по этим делам, позволяющей правильно определить направление предстоящего расследования, важно, прежде всего, выявить в следственной картине, особенно при отсутствии каких-либо данных о преступнике, позволяющих судить о механизме его действий, сведения об уровне его криминального профессионализма, а также об уровне знаний и умений в области компьютерных технологий. Именно эта информация и позволит правильнее определить направление расследования. Необходимо знать особенности субъектов этих преступлений вообще и применительно к особенностям конкретного преступления. Без этого знания также трудно выстраивать нужную тактику допроса указанных лиц и общение с ними в ходе других следственных действий. Это следует учитывать и при решении вопроса о виновности/невиновности подозреваемого, а также в процессе доказывания вины в преступлении. Сложности выступают везде: поиск правильных методов и тактики допроса таких преступников, налаживание с преступниками психологического контакта, с целью получения от них необходимой информации для последующей проверки, установления вины и т.д.

В результате, как свидетельствует практика, следователи, недостаточно сведущие ввопросах IT-технологий, затрудняются в установлении профессионально-технического языка при контакте с преступниками. Это существенным образом мешает эффективности расследования таких преступлений, но показывает следователям такую необходимость [1, с. 197-218]. Знание криминологической характеристики субъектов компьютерных преступлений важно для выбора следователем специалистов, которые смогли бы оказать ему необходимую помощь в уяснении технико-технологических особенностей способа имеханизма деяния, помогли бы наметить путии вопросы, подлежащих выяснению при допросе таких преступников и, соответственно, важно для продумывания тактики их допроса.

При установлении личности виновного, доказывания вины следует использовать криминалистической тактикой, так как в ее задачи, прежде всего, входит выявление и изучение закономерностей логико-психологических и иных особенностей поведения преступниковв моменты подготовкии совершения преступлений, в процессе выбора способа совершения преступления и его поведения в ходе следствия. На основе анализа их поведения выявления личных особенностей осуществляется разработка приемов следственных действий в разных следственных ситуациях, позволяющих преодолевать выявленные проблемные моменты при поиске доказательств, в процессе доказывания и при контакте с подозреваемым. Необходимы методические рекомендации, где был бы дан анализ действий в конкретных ситуациях.

Использованные источники:

1. Анохин А.Г., Луковкин К.Е. О специфических особенностях мошенничества в сфере компьютерной информации // Энигма, 2019. Т. 1. № 9-1. С. 197-218.

2. Приговоры судов по ст. 159.6 УК РФ Мошенничество в сфере компьютерной информации. Режим доступа: http://sud-praktika.ru/ (дата обращения: 20.07.2020).

3. Статья 159.6 УК РФ. Мошенничество в сфере компьютерной информации. Уголовный Кодекс РФ с комментариями. Режим доступа: http://oukrf.ru/st159.6 (дата обращения: 20.07.2020).

4. Уголовно-правовая характеристика преступлений, предусмотренных ст. 159-159.6 УК РФ: учебное пособие Уголовно-правовые меры противодействия мошенничеству (ст.ст. 159-159.6 УК РФ) / Иванченко Р.Б., Колесников Р.В., Малышев А.Н., Шебанов Д.В. Воронеж, 2015. С. 120.

5. Улитин М.А. Обстоятельства, подлежащие установлению при расследовании мошенничества в сфере компьютерной информации // Молодой ученый, 2019. № 26 (264). С. 251-253.