ПРИЗНАКИ МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Барсукова А.А.

Научный руководитель: Инюшкин А.А.

Россия, г. Самара,
Самарский национальный исследовательский университет
имени академика С.П. Королева

Аннотация. *В статье рассматривается один из видов мошенничества, а именно мошенничество в сфере компьютерной информации. Будут рассмотрены признаки состава мошенничества в сфере компьютерной информации, способы противоправного завладения чужим имуществом, особенности данной статьи, также квалификация, и отграничение от смежных составов. Автор приходит к мнению, что мошенничество в сфере компьютерной информации – это самостоятельный вид мошенничества.*

Ключевые слова*: мошенничество, компьютерная информация, судебная практика по мошенничеству в сфере компьютерной информации, способ совершения мошенничества.*

Мошенничество известно с момента основания российского государства. При росте и развитии государства увеличивался и рост мошенничества. Увеличение количества норм, предусматривающих ответственность за преступления в сфере мошенничества, может указывать о повышенном уровне общественной опасности и распространения преступления [1].

В современном мире практически вся деятельность человека связана с компьютерами. Компьютер позволяет хранить, передавать, обрабатывать большой объем информации. В связи с этим имеет место быть злоупотребление компьютерной информацией со стороны киберпреступников, в частности.

Не так давно был введен закон о мошенничестве в сфере компьютерной информации.

Стоит отметить, что вопрос мошенничества в сфере компьютерной информации начал активно обсуждаться в начале 2000-х годов. Ученые предложили дополнить УК РФ нормой об ответственности как «незаконное безвозмездное приобретение имущественных благ в значительном размере путем использования компьютеров, компьютерных систем или их сетей» [2].

Только в ноябре 2012 года этот состав преступлениябыл включен в Уголовный кодекс. А именно Федеральным законом от 29.11.2012 г. N 207-ФЗ года была введена статья 159.6 «Мошенничество в области компьютерной информации»: мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокировки, изменения компьютерной информации или иного вмешательства в функционирование средств хранения, обработки или передачи

компьютерной информации или информационных и телекоммуникационных сетей.

В то же время после введения этой статьи возникли новые взгляды на корректировку этой статьи. А именно сменить на «воровство в сфере компьютерной информации». В этом случае автор расширяет это правило. Поскольку кража – это общее понятие, а мошенничество – это вид (поскольку мошенничество – это форма воровства).

Что касается динамики преступности, то, по данным 2018 года, суды вынесли приговоры 7,7 тысячам человек за мошенничество в сфере компьютерной информации, что на 20% больше, чем в 2017 году. Экономические преступления относятся к категории преступлений, которые с каждым годом только увеличиваются.

Согласно судебной статистике Судебного департамента Верховного Суда РФ в докладе о функционировании федеральных судов общей юрисдикции и мировых судей за 1 полугодие 2020 года сказано, что было возбуждено 19 849 дел, но по факту было вынесено всего 9 328 приговоров. То есть обвинительных приговоров в два раза меньше, чем возбужденных дел. Это говорит о том, что доказать такое преступление в наши дни крайне сложно.

Диспозиция статьи 159.6 УК РФ бланкетная. В частности, ссылка на ФЗ № 27.07.2006 «Об информации 149-ФЗ информационных технологиях и защите информации»; 4 часть Уголовного кодекса РФ и другие.

Основания для введения такого рода преступлений:

- рост преступности различными способами совершения преступления;
- в литературе считают, что простое мошенничество (ч. 4 ст. 159 УК РФ) не учитывает особенности отношений, а потому фактически не позволяет защитить потерпевших [3].

Можно выделить значимые характеристики данной статьи.

1. Положение в соответствии со статьей 159.6 не совершается путем обмана или злоупотребления доверием (как и в статье 159 УК РФ), а путем получения доступа к компьютерной системе и осуществления ввода, удаления, блокировки или изменения компьютерной информации или иного вмешательства в работу средств хранения, обработки или передачи компьютерной информации или телекоммуникационных сетей.

2. Объективная часть вносит изменения в традиционный способ совершения типичного факта хищения, поскольку без ведома жертвы мошенник вмешивается в компьютерную информацию, манипулируя личной идентификационной информацией жертвы, что нарушает верховенство права, установленное в информационном пространстве, обеспечение его безопасного использования участниками информационных отношений, которые являются их дополнительным объектом.

3. Преступление совершается частично или полностью в виртуальном пространстве.

4. Что касается объекта преступления, то речь идет о компьютерной информации и имуществе граждан.

5.Для преступления очень важен способ его совершения – это то, что отличает один состав от другого.

В соответствии со статьей 6 Федерального закона 149-ФЗ № 27.07.2006 «Об информации, информационных технологиях и защите информации» информационные ресурсы находятся в собственности юридических и физических лиц, включены в их имущество и подпадают под действие гражданского законодательства.

Основной объект – это собственность, дополнительная общественная безопасность.

В объективную сторону компьютерного мошенничества включены два факта:

1) хищение чужого имущества;

2) приобретение права на чужое имущество.

Деяние, предусмотренное в статье 159.6, имеет особые средства для осуществления хищения чужого имущества:

- ввод компьютерной информации, то есть выполнение действий по сбору и электронной обработке для распознавания, хранения и использования;

- удаление информации с компьютера, то есть исключение компьютерной информации из автоматических носителей;

- блокировка информации на компьютере, то есть выполнение действий, ограничивающих или закрывающих доступ к компьютерной информации (но не связанных с её удалением или уничтожением);

- изменение компьютерной информации, то есть любые первоначальные изменения информации (сообщения, данные), представляемой в виде электрических сигналов, независимо от их средств хранения, обработки, передачи;

- различное вмешательство в системы хранения, обработки или передачи компьютерной информации или телекоммуникационных сетей указывает прежде всего на открытый перечень способов вмешательства в ИТ и означает любые другие действия, нарушающие обработку, хранение, использование, передачу и другое управление ИТ-информацией.

Что же касается общественно-опасных последствий, то данное преступление является преступлением с материальным составом.

Мошенничество признается совершенным с того момента, когда имущество поступило в незаконное владение виновного или других лиц, и они получили реальную возможность пользоваться или распорядиться им по своему усмотрению.

Субъект – общий (физ. лицо, вменяемое, достигшее 16-летнего возраста).

Субъективная сторона всегда выражена в прямом умысле. Виновный осознает, что завладевает чужим имуществом или правами на него путем ввода, удаления, блокирования, модификации компьютерной информации либо иным вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

В каждом преступлении необходимо установить намерение злоумышленника использовать полученную информацию в корыстных целях.

Также данный довод подтверждается в п. 20 ПП ВС РФ от 30.11.2017 № 48, ст. 159.6: под вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей признается целенаправленное воздействие программных и (или) программно-аппаратных средств на серверы, средства вычислительной техники, в том числе переносные – ноутбуки, планшетные компьютеры, смартфоны, снабженные соответствующим программным обеспечением, или на информационно-телекоммуникационные сети, которое нарушает установленный процесс обработки, хранения, передачи компьютерной информации, что позволяет виновному или иному лицу незаконно завладеть чужим имуществом или приобрести право на него.

Рассмотрим квалификацию преступления и судебную практику.

В случае, если мошенничество совершенно посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, то необходимо квалифицировать его в совокупности со статьями 272, 273 или 274.1 УК [4].

По факту, если хищение чужого имущества или приобретение права на чужое имущество осуществляется путем распространения заведомо ложных сведений в информационно-телекоммуникационных сетях, то такое следует квалифицировать как мошенничество, а не мошенничество в сфере компьютерной информации [4].

Что касается судебной практики, в рамках подготовки статьи было проанализировано несколько дел.

Приговор суда по ч. 2 ст. 159.6 УК РФ № 1-221/2017.

Виновный обратился в телефонную организацию ЗАО «Теле2» с просьбой о восстановлении сим-карты, так как она была «утеряна». Получив восстановленную сим-карту, лицо, используя принадлежащий ему мобильный телефон и сим-карту с абонентским номером потерпевшего, с помощью сервиса мобильная коммерция перевело денежные средства, находящиеся на расчетном счете сим-карты оператора мобильной связи ЗАО «Теле2», на неустановленный расчетный счет платежной системы «Киви-Кошелек», таким образом, обратило денежные средства в свое пользование.

Постановление суда по ч. 2 ст. 159.6 УК РФ № 1-41/2017.

Виновный, зная, где находится сотовый телефон потерпевшего, несколько раз совершал хищение денежных средств с банковских карт путем ввода компьютерной информации – «СМС сообщений» на номер «900» в информационно-телекоммуникационны сети операторов сотовой связи. После совершения хищения денежных средств удалял из телефона потерпевшего «смс сообщение» с номера «900» о проведенной им вышеуказанной операции и клал телефон потерпевшего на прежнее место.

Также интерес вызвало Определение Первого Кассационного Суда общей юрисдикции от 24.12.2019 №77-58/2019, в котором была произведена переквалификация на ст.159.6 УК РФ с интересным обоснованием.

Лица по предварительному сговору договорились о хищении денежных средств из предназначенных для хранения и выдачи банкоматов.

Реализуя задуманное, лица у неизвестного лица получили технические средства и программное обеспечение, необходимое для подключения к банкоматам.

Так, суды первой, апелляционной инстанций признали в их действиях кражу. Но кассационный суд обратил внимание на то, что не был учтен способ совершения преступления, а именно, когда хищение сопряжено с преодолением компьютерной информации путем ввода, удаления, блокировки, модификации компьютерной информации или иного вмешательства в системы компьютерной информации.

Под вводом компьютерной информации понимается введение (установка) в электронную память компьютера программ, способных выполнять функцию приема, переработки, хранения и выдачи информации в электронном виде.

Также суд обратил внимание на то, что такие преступления совершаются не путем обмана или злоупотребления доверием, а путем получения доступа к компьютерной системе.

Многие авторы утверждают, что мошенничество в сфере современных экономических отношений повышает степень общественной опасности, так как субъект преступления может совершать мошенничество и причинять ущерб неограниченному кругу лиц, но по факту является недоступным для правоохранительных органов.

Таким образом, развитие и совершенствование компьютерных технологий, доступность компьютерной техники способствуют появлению новых видов и способов совершения преступления. Объектами преступления являются информация, информационно-телекоммуникационные ресурсы, а также денежные средства, находящиеся в обращении локальных компьютерных сетей. По статистике доля таких преступления только увеличивается, так как способы совершения данного преступления становятся более изощрёнными. С появлением сети «Интернет» получить информацию становится легче. С одной стороны, люди сами оставляют свои персональные данные третьим лицам, не задумываясь о последствиях. С другой стороны, используя современные технологии, профессионал легко может получить информацию. В связи с этим правоохранителям необходимо обращать внимание на данные преступления, повышать уровень грамотности не только правоохранителей, но и граждан. Тем самым, представляется возможным снизить количество совершенных преступлений мошенничества в сфере компьютерной информации [5].

Библиографический список

1. Южин А.А. Мошенничество и его виды в российском уголовном праве: автореф. дисс... канд. юрид. наук. Москва, 2016.

2. Безверхов А.Г. Развитие понятия мошенничества в отечественном праве // Уголовное право. 2001. № 4. С. 9-12.

3. Мусаелян М.Ф. О некоторых проблемах, связанных с введением в УК РФ специальных составов мошенничества // Российский следователь. 2016. № 10.

4. Постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» [Электронный ресурс]. URL: https://www.garant.ru/products/ipo/prime/doc/71723288/ (дата обращения: 25.11.2020).

5. Тураев М. Социально-экономическая обусловленность дифференциации уголовной ответственности за мошенничество в уголовном законодательстве России // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2014. №3 (27). С. 296-300.

SIGNS OF COMPUTER INFORMATION FRAUD

Barsukova A.A.

Scientific adviser: Inyushkin A.A.

Samara National Research University, Samara, Russia

Abstract. *The article deals with one of the types frauds, namely fraud in the sphere of computer information. The article provitedes information on features fraud in the sphere of computer information, methods misappropriation, special feature this article 159.6, qualification and dissociation from related trains. The author makes on a conclusion that fraud in the sphere of computer information is an independent form of theft of someone else's property.*

Keyswords: *fraud, computer information, judicial practice of computer information fraud, method of committing fraud.*