УДК 343.72

Э. Е. Гензюк
Институт сферы обслуживания и предпринимательства (филиал) ДГТУ в г. Шахты, Шахты, e-mail: Shpigunova96@mail.ru

ОСОБЕННОСТИ КВАЛИФИКАЦИИ МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Ключевые слова: преступление, информация, объект преступления, компьютерная безопасность, компьютерное мошенничество.

В статье рассматриваются специальные признаки предмета мошенничества, совершаемого в сфере компьютерной безопасности, а именно в различных видах вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, совершаемые в целях обогащения или выгоды. условиях поступательного движения современной России к постиндустриальному обществу, постепенного перехода нашей страны к использованию высоких технологий опасность компьютерного мошенничества растет с каждым днем. В связи с этим еще одним специальным видом мошенничества, выделенным в отдельную норму УК РФ (ст. 159.6 УК РФ), стало мошенничество в сфере компьютерной информации. Данная статья призвана защитить отношения собственности, имущественные интересы, отношения, обеспечивающие охрану компьютерной информации и безопасность информационно-телекоммуникационных сетей. Схема компьютерного мошенничества заключается в том, что преступник умышленно с целью хищения имущества потерпевшего осуществляет доступ к защищенной информации, не имея на это правомочий.

E. E. Genzyuk
Institute of Service and Entrepreneurship (branch) of DGTU in Shakhty, Shakhty, e-mail: Shpigunova96@mail.ru

FEATURES OF QUALIFICATIONS FRAUD IN THE SPHERE OF COMPUTER INFORMATION

Keywords: crime, information, objects of crime, computer security, computer fraud.

The article deals with the special features of the subject of fraud committed in the field of computer security, namely in various types of interference in the functioning of the means of storage, processing or transmission of computer information or information and telecommunication networks, committed for enrichment or benefit. under the conditions of the progressive movement of modern Russia to the post-industrial society, the gradual transition of our country to the use of high technologies, the danger of computer fraud is growing every day. In this regard, another special type of fraud, allocated to a separate rule of the criminal code (Art. 159.6 of the criminal code), was fraud in the field of computer information. This article is intended to protect property relations, property interests, relations that ensure the protection of computer information and the security of information and telecommunication networks. The scheme of computer fraud is that the offender deliberately for the purpose of theft of the victim's property provides access to protected information without having the authority to do so.

В условиях поступательного движения современной России к постиндустриальному обществу, постепенного перехода нашей страны к использованию высоких технологий опасность компьютерного мошенничества растет с каждым днем. В связи с этим еще одним специальным видом мошенничества, выделенным в отдельную норму УК РФ (ст. 159.6 УК РФ), стало мошенничество в сфере компьютерной информации. Данная статья призвана защитить отношения собственности, имущественные интересы, отношения, обеспечивающие охрану компьютерной информации и безопасность информационно-телекоммуникационных сетей. Дополнительным непосредственным объектом мошенничества в сфере компьютерной информации выступает общественная безопасность. Юридически это подтверждается, в частности, тем обстоятельством, что по действующему уголовному законодательству России преступления в сфере компьютерной информации (гл. 28 УК РФ) представляют собой разновидность посягательств на общественную безопасность, что,

в свою очередь, объясняет способность подобного рода деяний наносить большой материальный ущерб.

Еще одним отличием от других специальных видов мошенничества является то, что предметом преступления, предусмотренного ст. 159.6 УК РФ, может выступать и имущество, и право на него. Аналогичный подход к определению предмета преступления имеет место в общем составе мошенничества (ст. 159 УК РФ). В качестве разновидностей имущества как предмета мошенничества в сфере компьютерной информации чаще всего выступают денежные средства в безналичной форме. В отдельных делах фигурирует иное имущество, имеющее овеществленную форму. Право на имущество, в свою очередь, представлено правомочиями собственника или иного владельца в отношении конкретного имущества. Оно может быть закреплено различных документах (в дарственной на квартиру, именной сберкнижке и т. д.). В судебной практике право на имущество рассматривается как право собственности на недвижимое имущество, право на долю в уставном капитале, право требования денежных средств и т. п.

Потерпевшими в данном преступлении могут быть любые лица. В других видах мошенничества, за исключением основного состава, чаще встречались специальные потерпевшие. Объективную сторону мошенничества в сфере компьютерной информации составляет хищение чужого имущества или приобретение права на чужое имущество. Средствами, с помощью которых совершается само преступление, то есть происходит хищение или приобретение права на чужое имущество, выступают компьютерная информация и средства хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

При квалификации мошенничества в сфере компьютерной информации необходимо обратиться к примечанию ст. 272 УК РФ: «Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи». То есть сущность компьютерной информации сводится к ее природе, выраженной в электрических сигналах. Однако подобное понимание компьютерной информации как «электронной информации» в современном мире вызывает нарекания. Такую информацию, по мнению В.М. Елина, следует рассматривать лишь как один из видов компьютерной информации. Подобной позиции придерживается и П.С. Яни. Однако если непосредственно оценивать сущность компьютерной информации как средства мошенничества в компьютерной сфере, то в качестве ее выступают команды, вводимые с клавиатуры или с помощью звуковых сигналов, различного рода «вирусные» программы, а также иная информация, способная осуществить неправомерное воздействие на предмет хищения.

Получение доступа к чужому имуществу при совершении преступления осуществляется путем совершения определенных в законе действий. Следовательно, обязательным признаком данного состава выступает способ совершения преступления. Специфика способа указанного преступления состоит, прежде всего, в различных видах вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, а именно:

1) хищения чужого имущества или приобретения права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации;

2) хищения чужого имущества или приобретения права на чужое имущество путем иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей [8, 96].

Способы воздействия в виде действий по «вводу», «удалению», «блокированию», «модификации» компьютерной информации аналогичны способам преступлений, которые предусмотрены главой 28 УК РФ. В связи с этим определения этих способов, разработанные применительно к компьютерным преступлениям, в неизменном виде в юридической литературе используются и в отношении компьютерного мошенничества.

Тем не менее мы считаем чрезвычайно важным с учетом уже наработанной судебной практики более точно установить содержание этих понятий.

Термином «ввод компьютерной информации» определяется в литературе как любой (определенный), так и неопределенный алгоритм действий по набору и электронной обработке сведений (сообщений, данных) для их дальнейшего распознания и использования компьютерной системой. Понимание «ввод» как введение любых исходных данных означает наступление любых результатов. Следовательно, он своим содержанием охватывает все способы, которыми можно совершить компьютерное преступление, в том числе и компьютерное мошенничество. Однако, исходя из содержания диспозиции ст. 159.6 УК РФ, где совместно с понятием «ввод» отдельно названы другие термины: «удаление», «блокирование», «модификация» и «иное вмешательство», его следует рассматривать и как определенное действие, и как результат. То есть, как верно замечает М.И. Третьяк, ввод компьютерной информации как признак компьютерного мошенничества есть определенный алгоритм действий по набору данных об адресате (номера его лицевого счета, мобильного телефона, данных мобильного кошелька и др.), сведений о сумме денежных средств (данных о ценной бумаге) и непосредственному переводу их указанному адресату (операции «перевести», «отправить», «исполнить»), далее их обработка, распознание компьютерной системой и наступление результата – поступление денежных средств (ценной бумаги) адресату [8, 111].

Удаление компьютерной информации понимается как действия по изменению ее первоначального состояния (полная либо частичная деинсталляция информации с машинных носителей), при котором она перестает существовать в силу утраты основных качественных признаков. Изменение состояния компьютерной информации на практике осуществляется путем совершения операции «delete» либо другой комбинаций действий, приводящей к исчезновению полностью или части записи. Следовательно, исчезновение записи полностью либо частично является моментом окончания деяния. К примеру, с момента удаления виновным лицом информации из компьютерной базы предприятия об объеме произведенной продукции у него появляется возможность распорядиться имуществом по своему усмотрению. Фактическое же завладение такой продукцией находится за рамками состава преступления.

Блокирование компьютерной информации представляет собой действия, которые приводят к ограничению либо закрытию доступа к компьютерной информации и характеризуются недоступностью ее использования по прямому назначению со стороны законного владельца (собственника). Оно осуществляется путем совершения действий по изменению либо установлению пароля, логина, в результате чего доступ к информационным ресурсам становится ограниченным (закрытым). Моментом окончания данного действия выступает отсутствие доступа к компьютерной информации в определенный промежуток времени либо постоянно. Все другие действия, которые могут быть на практике совершены, находятся за рамками состава преступления. Поэтому ущерб определяется размером выгоды, полученной только в результате совершения действий по блокированию. Однако он выражается не в виде прямого реального ущерба, а в виде упущенной выгоды, что, как мы видим, не соответствует классической трактовке мошенничества и в целом хищения. Полагаем, что на практике оно чаще всего будет выступать в качестве дополнения к другому действию, например, к вводу компьютерной информации. Следует заметить, что применения только одного этого способа недостаточно для причинения прямого реального ущерба. Модификация заключается в любых действиях по изменению первоначального состояния компьютерной информации. Модификация компьютерной информации при совершении мошенничества осуществляется путем действий по изменению номера sim-карты, записи на лицевом счете, персональных данных потерпевшего, цены товара, внесения изменений в программу и других действий, результатом которых являются видоизмененные данные на лицевом счете виновного лица, сведения о sim-карте и т. д.

Что касается вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, то им признается совокупность следующих факторов: во-первых, целенаправленное воздействие осуществляется посредством программных и (или) программно-аппаратных средств; во-вторых, воздействие оказывается на серверы, средства вычислительной техники (компьютеры), снабженные соответствующим программным обеспечением, или на информационно-телекоммуникационные сети; в-третьих, воздействие нарушает установленный процесс обработки, хранения, передачи компьютерной информации; в-четвертых, воздействие позволяет виновному либо иному лицу незаконно завладеть чужим имуществом или приобрести право на него. Также специфика способа обсуждаемого преступления характеризуется следующими особенностями: во-первых, воздействие осуществляется непосредственно на компьютерную информацию, а не на сознание потерпевшего; во-вторых, отсутствует обман, обязательным признаком которого является введение другого лица в заблуждение путем воздействия на сознание (психику) другого человека; в-третьих, отсутствует передача имущества или приобретение права на имущество с помощью потерпевшего; в-четвертых, орудием преступления признаются информация, средства хранения, передачи и обработки компьютерной информации, а не ложные сведения, передаваемые человеком. Что касается общественно-опасных последствий, то данное преступление, предусмотренное ст. 159.6 УК РФ, является преступлением с материальным составом, обязательным условием его совершения выступает хищение чужого имущества или приобретение права на чужое имущество. При этом возникает вопрос о том, что конкретно похищено в результате совершения преступления: деньги, информация, права или что-то еще. То есть, особую актуальность приобретает проблема информации как вещи, имущества. Как видим, анализ объективной стороны мошенничества в сфере компьютерной информации показывает, что оно в еще большей степени не соответствует признакам мошенничества как хищения чужого имущества или приобретения права на чужое имущество, совершенного путем обмана или злоупотребления. Обман и злоупотребление в данном случае являются способом совершения мошенничества. Между тем в диспозиции ст. 159.6 УК РФ указания на обман и злоупотребление доверием нет, а способами указанного деяния названы «ввод, удаление, блокирование, модификация компьютерной информации либо иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей», то есть фактически употребляется терминология составов преступлений, предусмотренных ст. 272–274 УК РФ. Субъективная сторона данного преступления предполагает прямой умысел. 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. Обязательным признаком является и корыстная цель, которая, как мы убедились, свойственна всем составам мошенничества.

Вместе с тем в постановлении Пленума Верховного Суда РФ №48 разъяснено, что не каждый факт ввода компьютерной информации с противоправным умыслом признается преступлением, предусмотренным ст. 159.6 УК РФ. Так, под названную статью не подпадает хищение посредством:

1) использования заранее похищенной или поддельной платежной карты для получения наличных денежных средств через банкомат (в такой ситуации применяется ст. 158 УК РФ);

2) использования учетных данных собственника или иного владельца имущества независимо от способа получения доступа к таким данным

(применяется ст. 158 УК РФ), за исключением случаев незаконного воздействия на программное обеспечение серверов, компьютеров или на сами информационно-телекоммуникационные сети;

3) распространения заведомо ложных сведений в информационно-телекоммуникационных сетях, включая сеть Интернет, например, посредством создания поддельных сайтов благотворительных организаций, интернет-магазинов, использования электронной почты (применяется ст. 159 УК РФ).

Кроме того, необходимо отметить, что мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по статье 272, 273 или 274.1 УК РФ. Субъект мошенничества в сфере компьютерной информации – общий, по ч. 3 ст. 159.6 УК РФ – специальный, квалифицирующим признаком выступает совершение преступления группой лиц по предварительному сговору либо организованной группой.

Таким образом, действующую на сегодняшний момент уголовно-правовую норму о мошенничестве в сфере компьютерной информации нельзя назвать удачной. В ней достаточно сложно установить наличие признаков состава, в первую очередь, субъекта преступления, в силу его анонимности, а также объективной стороны, по причине его виртуального характера, и субъективной стороны, по причине сложности установления. В связи с этим необходимы глубокие исследования в области информационно-коммуникационных технологий.

Библиографический список

1. Уголовный кодекс РФ от 13.06.1996 г. № 63-ФЗ // Собрание законодательства РФ. 17.06.1996. № 25. Ст. 2954.

2. Аминов Д.И., Шумов Р.Н., Борисов А.В., Борбат А.В. К вопросу о квалификации мошенничества в сфере жилищно-коммунального хозяйства // Российский следователь. 2017. № 8. С. 18.

3. Архипов А.В. Проблемы применения нормы о мошенничестве с использованием платежных карт // Уголовное право. 2017. № 1. С. 5.

4. Черняков С.А. К вопросу о детерминации мошенничества в сфере обеспечения исполнения обязательств банковскими гарантиями (по результатам проведенного исследования) // Российский следователь. 2014. № 21. С. 54–56.