

ЗАКОНОДАТЕЛЬНОЕ РЕГУЛИРОВАНИЕ МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

© Юлия Сергеевна КАУФМАН

Тамбовский государственный университет им. Г.Р. Державина,
г. Тамбов, Российская Федерация, аспирант, кафедра уголовного права
и криминологии, e-mail: vera1705@mail.ru

Раскрывается характеристика состава мошенничества в сфере компьютерной информации, общественно-опасные последствия, специфика информационных отношений, а также проблемы квалификации данного вида преступлений. Указанное деяние находится в одном ряду с мошенничеством в сфере кредитования, при получении выплат, с использованием платежных карт, в области предпринимательской деятельности, в области страхования. Включение указанной статьи в уголовное законодательство способствует конкретизации компьютерных преступлений, наряду с преступлениями в сфере компьютерной информации выделяя преступления, осуществляемые с использованием компьютерных средств. Однако включение данного состава преступления в уголовное законодательство Российской Федерации порождает также ряд проблем. Необходимость криминализации компьютерного мошенничества назрела давно, обоснованность принятия данной статьи раскрывается рядом научных статей, отражается в существующей практике.

Ключевые слова: мошенничество в сфере компьютерной информации; информация; хищение.

Федеральным законом № 207-ФЗ от 29 ноября 2012 г. в действующий Уголовный кодекс Российской Федерации внесены изменения. Гл. 21 была дополнена шестью новыми составами, среди которых ст. 159.6 «Мошенничество в сфере компьютерной информации». Данная статья призвана защитить отношения собственности, имущественные интересы, отношения, обеспечивающие охрану компьютерной информации и безопасность информационно-телекоммуникационных сетей. Уголовная ответственность предусмотрена за хищение чужого имущества или приобретение права на чужое имущество посредством ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей [1].

Мошенничество в сфере компьютерной информации является закономерным шагом интеграции российского законодательства о борьбе с компьютерными преступлениями в международное законодательство. До настоящего времени основная деятельность в указанной сфере осуществлялась в рамках требований ст. 272-274 УК РФ. Прослеживается схожесть объективной стороны деяний ст. 159.6 УК РФ и ч. 2 ст. 272 УК РФ, предусматривающей неправомерный доступ к компьютерной информации, совершенный из

корыстной заинтересованности. Однако если при мошенничестве ввод, удаление, блокирование, модификация либо иное вмешательство являются способами преступления, то, по смыслу диспозиции ст. 272 УК РФ, уничтожение, блокирование, модификация либо копирование информации выступают скорее обязательными последствиями [2].

Положениями п. 166 Резолюции X Конгресса ООН по предупреждению преступности и обращению с правонарушителями, состоявшегося 10–17 апреля 2000 г. в Вене, определено: «если компьютерные данные поддаются идентификации и контролю по конкретному носителю данных, то с юридической точки зрения они могут рассматриваться как единый и осязаемый материальный предмет» [3].

Преступление, предусмотренное ч. 1 ст. 159.6 УК РФ, является преступлением небольшой степени тяжести, преступления, предусмотренные ч. 2 и 3 ст. 159.6 УК РФ, – преступлениями средней тяжести, а преступления, предусмотренные ч. 4 указанной статьи, – отнесены к тяжким [4].

Анализ указанной статьи позволяет сделать следующие выводы.

Включение мошенничества в сфере компьютерной информации в состав гл. 21 УК РФ предусматривает в качестве видового объекта отношения собственности, непосредственным объектом выступает чужое имущество или права на него.

Объективную сторону мошенничества в сфере компьютерной информации составляет хищение чужого имущества или приобретение права на чужое имущество.

Способом совершения преступления выступает:

1) ввод, удаление, блокирование, модификация компьютерной информации;

2) иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Субъект – общий, по ч. 3 ст. 159.6 УК РФ – специальный, квалифицирующим признаком выступает совершение преступления группой лиц по предварительному сговору либо организованной группой.

Субъективная сторона 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 [5].

Состав, описанный в ст. 159.6 УК РФ, является специальным по отношению к составу ст. 159 УК РФ, к тому же основной состав (ч. 1 ст. 159.6 УК РФ) конкурирует с основными составами, предусмотренными ч. 1 ст. 272, ч. 1 ст. 273 УК РФ. Нельзя не отметить отсутствие системности законодательства, что проявляется в различных подходах к установлению наказания за преступное хищение, сопряженное с незаконным использованием компьютерной информации, и фактически за то же деяние в сфере компьютерной информации, но без признаков хищения: мошенничество, причинившее ущерб до 2,5 тыс. руб. (ч. 1 ст. 159.6 УК РФ), карается мягче, чем преступление, предусмотренное ч. 1 ст. 172 и ч. 1 ст. 173 УК РФ. Вместе с тем мошенничество, причинившее ущерб от 2,5 тыс. до 1 млн руб. (ч. 2 ст. 159.6 УК РФ), карается жестче, чем преступление, предусмотренное ч. 1 ст. 272, и соразмерно преступлению, описанному в ч. 2 ст. 273 УК РФ. Это противоречие тем более остро, что в случае, если деяние не завершено, умысел на хищение трудно установить. Кроме того, есть проблема с конкуренцией в применении норм, предусматривающих квалифицирующие и особо квалифицирующие признаки:

при совершении преступления, предусмотренного ч. 3 ст. 272 УК РФ, группой лиц по предварительному сговору с причинением значительного ущерба (до 2,5 тыс. руб.), совершенного из корыстной заинтересованности, и квалифицированного мошенничества в сфере компьютерной информации (ч. 2 ст. 159.6 УК РФ) [6].

Что касается общественно-опасных последствий, 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. Таким образом, особую актуальность приобретает проблема информации как вещи, имущества.

Между тем информация исключена из перечня объектов гражданских правоотношений с 1 января 2008 г. [7]. В силу ряда свойств, у информации нет собственника, а только обладатель, что нашло свое отражение в ряде законов информационной отрасли права. Применяя понятие информационного объекта, информационной вещи, следует иметь в виду, что информация, обладая стоимостью, не является имуществом, как совокупность вещей. Таким образом, вопрос о возможности рассмотрения информационной вещи в качестве предмета мошенничества, в настоящее время не может решаться однозначно и нуждается в дальнейшей проработке.

Подводя итог, можно констатировать, что формальное отнесение преступлений данной категории к преступлениям против собственности неминуемо породит правовые коллизии в связи с невозможностью правоохранительных органов ответить на вопросы:

- о собственнике информации;
- о размере ущерба;
- об имущественных характеристиках компьютерной информации;
- о взаимосвязи правомерных действий (ввода, удаления, блокирования, модификации компьютерной информации) и общественно-опасных последствий (хищение чужого имущества или приобретение права на чужое имущество);

– о разграничениях между ст. 159.6 УК РФ и смежными составами преступления и др. [5].

В настоящее время в диспозиции статьи никоим образом не учтены особенности правового регулирования информационных отношений, самого понимания феномена информации, что породит сложности в практике привлечения к уголовной ответственности за совершение компьютерного мошенничества.

Представляется необходимым выделить в российском уголовном кодексе раздел, посвященный компьютерным преступлениям, куда включить отдельными главами преступления в сфере компьютерной информации, преступления с использованием компьютерных технологий, преступления в отношении конфиденциальной информации, намеренно выделяя видовые объекты, что в значительной мере упростит понимание сущности данной категории преступлений и возможности правоприменения.

В то же время диспозиция ст. 159.6 УК РФ с учетом особенностей российского информационного законодательства должна определять мошенничество с использованием информационно-коммуникационных технологий или компьютерной информации как хищение чужого имущества или приобретение права на чужое имущество путем неправомерных действий, связанных с вводом, удалением, блокированием, модификацией компьютерной информации либо иным неправомерным вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

1. О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации: федеральный закон от 29.11.2012 г. № 207-ФЗ // Российская газета. 2012. 3 дек.
2. Маленкин А.С. Вопросы разграничения мошенничества в сфере компьютерной информации (ст. 159.6 УК РФ) и неправомерного доступа к компьютерной информации, совершенного из корыстной заинтересованности (ч. 2 ст. 272 УК РФ) // Противодействие преступности: от теории к практике день за днем: научно-практическая интернет-конференция Омской юридической академии. Омск, 2013.

3. Доклад 10 Конгресса ООН по предупреждению преступности и обращению с правонарушителями // 10 Конгресс ООН по предупреждению преступности и обращению с правонарушителями: сборник документов / сост. А.Г. Волеводев. М., 2001.
4. Комментарий к Уголовному кодексу Российской Федерации (постатейный) / под ред. А.И. Чучаева. М., 2013.
5. Елин В.М. Мошенничество в сфере компьютерной информации как новый состав преступления // Бизнес-информатика. 2013. № 2 (24). С. 70-76.
6. Александрова И.А. Новое уголовное законодательство о мошенничестве // Юридическая наука и практика. Вестник Нижегородской академии МВД России. 2013. № 21. С. 54-62.
7. Статья 128 ГК РФ (в ред. федерального закона от 18.12.2006 г. № 231-ФЗ). Доступ из информационно-правового портала «Гарант».

1. О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации: федеральный закон от 29.11.2012 г. № 207-ФЗ // Российская газета. 2012. 3 дек.
2. Маленкин А.С. Вопросы разграничения мошенничества в сфере компьютерной информации (ст. 159.6 УК РФ) и неправомерного доступа к компьютерной информации, совершенного из корыстной заинтересованности (ч. 2 ст. 272 УК РФ) // Противодействие преступности: от теории к практике день за днем: научно-практическая интернет-конференция Омской юридической академии. Омск, 2013.
3. Доклад 10 Конгресса ООН по предупреждению преступности и обращению с правонарушителями // 10 Конгресс ООН по предупреждению преступности и обращению с правонарушителями: сборник документов / сост. А.Г. Волеводев. М., 2001.
4. Комментарий к Уголовному кодексу Российской Федерации (постатейный) / под ред. А.И. Чучаева. М., 2013.
5. Елин В.М. Мошенничество в сфере компьютерной информации как новый состав преступления // Бизнес-информатика. 2013. № 2 (24). С. 70-76.
6. Александрова И.А. Новое уголовное законодательство о мошенничестве // Юридическая наука и практика. Вестник Нижегородской академии МВД России. 2013. № 21. С. 54-62.
7. Ст'я 128 GK RF (v red. federal'nogo zakona ot 18.12.2006 g. № 231-FZ). Dostup iz informatsionno-pravovogo portala "Garant".

Поступила в редакцию 28.12.2013 г.

UDC 343.72+004.056

LAW REGULATION OF FRAUD IN COMPUTER INFORMATION SPHERE

Yuliya Sergeyevna KAUFMAN, Tambov State University named after G.R. Derzhavin, Tambov, Russian Federation, Post-graduate Student, Criminal Law and Criminology Department, e-mail: vera1705@mail.ru

The characteristics of fraud in computer information sphere, social dangerous consequences, specificity of information relations and also problems of qualification of the given type of crimes are disclosed. This crime is the same as fraud in credit sphere, payment receiving, use of credit cards, entrepreneurship activity sphere, and insurance sphere. The inclusion of the given article in criminal legislation enables the concretization of computer crimes together with the crimes in computer information sphere pointing out the crimes with use of computer means. However, the inclusion of the given content of crime in the criminal legislation of the Russian Federation creates also some problems. The necessity of criminalization of computer fraud appeared long time ago, the prove of accepting of this article is disclosed by some scientific articles, and is reflected in present practice.

Key words: fraud in computer information sphere; information; steal.