DOI: 10.17117/na.2016.10.01.384

<http://ucom.ru/doc/na.2016.10.01.384.pdf>

Поступила (Received): 02.10.2016

**Лукьянчикова Е.Ф., Мальцева Н.Н., Морозова Е.А.
Мошенничество в сфере компьютерной информации:
некоторые проблемы квалификации и
соотношения со ст. 272, 273 УК РФ**

**Lukyanchikova E.F., Maltseva N.N., Morozova E.A.
Fraud in the sphere of computer information: some issues of
qualification and relation to Articles 272, 273 of the Criminal Code**

Статья посвящена исследованию мошенничества, осуществляемого в сфере компьютерной информации, а также наиболее актуальных проблем его соотношения с такими видами преступлений как неправомерный доступ к компьютерной информации и создание, использование и распространение вредоносных компьютерных программ

Ключевые слова: мошенничество, компьютерная информация, компьютерные преступления

The article investigates fraud, carried out in the sphere of computer information, as well as the most urgent problems of its relationship with these types of crimes like illegal access to computer information and the creation, use and distribution of malicious computer programs

Key words: fraud, computer information, computer crime

Лукьянчикова Елена Федоровна

Кандидат юридических наук, доцент
Белгородский государственный национальный
исследовательский университет
г. Белгород, ул. Победы, 85

Lukyanchikova Elena Fedorovna

Candidate of Juridical Sciences, Associate Professor
Belgorod state national research university
Belgorod, Pobedy st., 85

Мальцева Наталья Николаевна

Студент
Белгородский государственный национальный
исследовательский университет
г. Белгород, ул. Победы, 85

Maltseva Natalia Nikolaevna

Student
Belgorod state national research university
Belgorod, Pobedy st., 85

Морозова Екатерина Александровна

Студент
Белгородский государственный национальный
исследовательский университет
г. Белгород, ул. Победы, 85

Morozova Ekaterina Alexandrovna

Student
Belgorod state national research university
Belgorod, Pobedy st., 85

На сегодняшний день, мошенничество в сфере телекоммуникационных сетях, в том числе и интернет-мошенничество, получили повсеместное распространение не только в России, но и по всему миру. Этому активно способствует как онлайн платежные операции с реальными и даже виртуальными деньгами, так и привлекательность ИТ-технологий для ввода в заблуждение и скрывтия

следов преступления. Особую опасность виртуальные мошенники представляют для пользователей, у которых нет достаточного опыта деятельности в сфере финансовой информации [5, с. 14].

Необходимо отметить, что на сегодняшний день в Уголовном кодексе РФ существует ст. 159.6 «Мошенничество в сфере компьютерной информации», предусматривающая ответственность за «хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей» [1].

Несмотря на то, что введение данного специализированного вида мошенничества было необходимым и обусловлено потребностями современного общества, в отношении нее существует множество дискуссионных вопросов. В частности, многие правоведы отмечают ее спорное содержание, так как обязательный признак объективной стороны рассматриваемого преступления является самостоятельным деянием, подпадающим под санкцию ст. 272 УК РФ «Неправомерный доступ к компьютерной информации» [2, с. 58]. При этом если максимально возможная санкция по ч. 1 ст. 159.6 составляет арест на срок до четырех месяцев, до по ч. 1 ст. 272 УК РФ – лишение свободы на срок до двух лет. Справедливо утверждать, что подобная ситуация обуславливает противоречивое толкование и применение уголовного законодательства в части квалификации содеянного: по ст. 159.6, ст. 272 или по совокупности указанных деяний.

В.М. Елин придерживается позиции, согласно которой содеянное следует квалифицировать по совокупности преступлений [4, с. 7].

Мы категорически не согласны с данным утверждением, так как подобная квалификация представляет собой не что иное как двойное вменение, что в соответствии с принципом гуманизма уголовного закона, неприемлемо. Аргументируем мы свою позицию тем, что лицо, совершая мошенничество в сфере компьютерной информации, осознает, что сначала ему необходимо осуществить иное преступление – неправомерный доступ к компьютерной информации. В связи с этим мы солидарны с мнением И.Р. Бегишева, который предлагает внести изменения в ст. 159.6 так, чтобы «способ совершения данного вида мошенничества не ограничивался только неправомерным доступом к компьютерной информации (так как доступ может носить и правомерный характер), но и предусматривал другие возможности применения компьютерной техники» [3, с. 29].

Неоднозначный характер носит и соотношение ст. 159.6 и ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ». Обуславливается это тем, что мошенничество в сфере компьютерной информации может и осуществляться с помощью специально созданных для этого программ, которые дают преступнику возможность вводить, удалять, блокировать необходимую ему информацию из компьютера потерпевшего, или передавать необходимую информацию в сети «Интернет». В соответствии с диспозицией ст. 273 УК РФ, под вредоносной программой понимается программа, которая заведомо предназначена для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств компьютерной защиты [1]. Анализируя приведенные

определения, возможно констатировать, что мошеннические программы по методу воздействия на компьютерную информацию, целям и мотивам их создания аналогичны вредоносным программам. Таким образом, возникает вопрос, аналогичный рассмотренному ранее: как квалифицировать мошенничество, если для его осуществления применялась специально-разработанная для этого компьютерная вредоносная программа. На наш взгляд, квалификация по обеим статьям также противоречит принципу гуманизма и демонстрирует собой двойное вменение, являющееся недопустимым. Мы считаем, что указанное преступление следует квалифицировать по ч. 1 ст. 159.6 УК РФ, так как диспозиция данной статьи охватывает собой разработку, распространение и применение вредоносной компьютерной программы, однако для этого необходимо внести соответствующие изменения.

Констатируя вышеизложенное, считаем необходимым обратить внимание на проблемы соотношения ст. 159.6 и ст.ст. 272, 273 УК РФ, так как ввиду наличия сходных черт, на практике возникают определенные проблемы при квалификации совершенного мошенничества в сфере компьютерной информации. На наш взгляд, единственным выходом из данной ситуации является корректировка действующего уголовного законодательства в целях устранения указанных противоречий и приведения практики применения указанных статей «к одному знаменателю».

Список используемых источников:

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 06.07.2016) // Российская газета. 1996, 25 июня.
2. Александрова И.А. Новое уголовное законодательство о мошенничестве // Уголовное право. 2013. № 12. С. 55 – 63.
3. Бегишев И.Р. Некоторые вопросы противодействия мошенничеству в сфере компьютерной информации // Юридические науки. 2016. № 3. С. 28 – 34.
4. Елин В.М. Мошенничество в сфере компьютерной информации как новый состав преступления // Государство и право. 2013. № 2. С. 1 – 9.
5. Манохина, О.В. Компьютерная преступность // Киберпреступность. 2015. № 5. С. 13 – 17.

© 2016, Лукьянчикова Е.Ф., Мальцева Н.Н.,
Морозова Е.А.

Мошенничество в сфере компьютерной информации: некоторые проблемы квалификации и соотношения со ст. 272, 273 УК РФ

© 2016, Lukyanchikova E.F., Maltseva N.N.,
Morozova E.A.

Fraud in the sphere of computer information: some issues of qualification and relation to Articles 272, 273 of the Criminal Code