

*Желтухина Е.В.,  
студент магистратуры,  
2 курс, факультет «Юридический», филиал Северо-Кавказского  
федерального университета, в г. Пятигорске.*

*Россия, г. Пятигорск*

*Суховеева Ю.Ю.,  
студент магистратуры,  
3 курс, факультет «Юридический», филиал Северо-Кавказского  
федерального университета, в г. Пятигорске.*

*Россия, г. Пятигорск*

## **ОТДЕЛЬНЫЕ АСПЕКТЫ КВАЛИФИКАЦИИ ХИЩЕНИЙ В СЕТИ «ИНТЕРНЕТ» И НЕПРАВОМЕРНОГО ДОСТУПА К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ**

***Аннотация:** в статье раскрываются вопросы квалификации хищений совершаемых с использованием сети интернет. Проводится анализ квалификации указанных преступлений по совокупности с неправомерным доступом к компьютерной информации. При этом выявляются определенные проблемы квалификации и указываются пути их решения.*

***Ключевые слова:** квалификация, хищения, интернет, компьютерная информация, неправомерный доступ, кража, мошенничество.*

***Abstract:** the article deals with the issues of qualification of thefts committed using the Internet. The analysis of qualification of the specified crimes on set with illegal access to the computer information is carried out. At the same time, certain problems of qualification are identified and ways of their solution are indicated.*

***Keywords:** qualification, theft, Internet, computer information, unauthorized access, theft, fraud.*

В правоприменительной практике встречаются случаи квалификации по реальной совокупности преступлений, действий, направленных на посягательство на собственность и сферу экономической деятельности. Нередко путем воздействий тем или иным способом на безопасность компьютерной информации лицам удается похищать денежные средства. В таких случаях действия в зависимости от конкретных обстоятельств, которые мы рассмотрим, будут подлежать квалификации либо по ст. 158 УК РФ, либо по ст. 159<sup>6</sup> УК РФ<sup>1</sup>.

При установлении в таких действиях наличия признаков состава преступления, ответственность за которое предусмотрено ст. 158 УК РФ, следует обратить внимание на следующие обстоятельства. Установлено, что С., неправомерно получив доступ к электронному почтовому ящику, воспользовавшись логином и паролем к «ДеньгиMail.Ru», который был «привязан» к электронному почтовому ящику потерпевшего, перечислил денежные средства в общем размере 4 321 руб. 17 коп.<sup>2</sup> Такие действия С. судом были квалифицированы по ст. 158 УК РФ до введения состава компьютерного мошенничества (ст. 159<sup>6</sup> УК РФ).

Следует отличать случаи образования действиями лица реальной совокупности преступлений, ответственность за которые предусмотрена ст.ст. 158 и 272 УК РФ. Такие случаи могут образовываться, когда неправомерный доступ к компьютерной информации является одной из подготовительных стадий для дальнейшего хищения денежных средств без использования компьютерной информации. Так, Верховный суд Республики Татарстан правильно обратил внимание на обстоятельство использования полученной информация в последующем для похищения денежных средств, поэтому действия Г. были правильно квалифицированы по реальной совокупности преступлений, ответственность за которые предусмотрена ст.ст. 158, 272 УК

---

<sup>1</sup> Гайфутдинов Р.Р. Понятие и квалификация преступлений против безопасности компьютерной информации: дис. ... канд. юрид. наук. Казань, 2017. С. 132.

<sup>2</sup> Материалы уголовного дела № 917417 МВД по РТ ГСУ СЧ // Архив Советского районного суда г. Казани Республики Татарстан. // <http://sovetsky.tat.sudrf.ru/> (дата обращения: 17.07.19).

РФ<sup>3</sup>. Так, Г. в составе группы лиц по предварительному сговору путем установки на банкоматы «скиммеров» (технических средств для негласного получения информации) собирал компьютерную информацию, находящуюся на магнитных полосах банковских карт, принадлежащих другим лицам, изготавливал дубликаты таких банковских карт («белый пластик»), на которые записывалась собранная информация, являющаяся банковской тайной, и с них денежные средства снимались в банкоматах под видом настоящих<sup>4</sup>.

Более того, при квалификации деяний лица по совокупности преступлений, ответственность за которые предусмотрена ст. 158 УК РФ, с преступлениями против безопасности компьютерной информации необходимо обратить внимание на наличие разъяснений, данных Пленумом Верховного Суда РФ от 27.12.2002 г. № 29 «О судебной практике по делам о краже, грабеже и разбое»<sup>5</sup>.

Позиции о возможности квалификации одного деяния лица по совокупности преступлений, ответственность за которые предусмотрена ст.ст. 159<sup>6</sup> и 272 УК РФ, весьма различны как в литературе, так и в судебной практике. Так, Самарский областной суд неоднократно в принимаемых постановлениях рассматривал вопрос о возможности квалификации деяния по совокупности преступлений как компьютерное мошенничество и неправомерный доступ к компьютерной информации (ст.ст. 159<sup>6</sup>, 272 УК РФ). Например, по одному из дел установлено, что поскольку действия по хищению чужого имущества путем модификации компьютерной информации сопряжены с неправомерным доступом к охраняемой законом компьютерной информации, повлекшим модификацию такой информации, судом правильно квалифицированы действия Х. по совокупности вышеуказанных преступлений. Одно действие подсудимых находит квалификацию по совокупности преступлений и в других рассмотренных делах.

---

<sup>3</sup> Апелляционное постановление Верховного Суда Республики Татарстан по делу № 22-7630 от 01.11.16 г. // ГАС «Правосудие». URL: <http://vs.tat.sudrf.ru/> (дата обращения: 17.07.19).

<sup>4</sup> Там же.

<sup>5</sup> Бюллетень Верховного Суда РФ. 2003. № 2.

Вместе с тем необходимо тщательно устанавливать обстоятельства возможности квалификации указанных преступлений, образующих идеальную совокупность. Так, органами предварительного расследования Г. вменяли совокупность рассматриваемых преступлений в связи с тем, что последний через систему дистанционного банковского обслуживания «Сбербанк ОнЛ@йн» осуществлял денежные переводы с личных кабинетов потерпевших на банковскую карту, находящуюся в его распоряжении. Ошибка в квалификации указанных действий по совокупности преступлений состояла в том, что 1) предварительным следствием не установлено причинение вреда охраняемому объекту - нарушению безопасности информации и работы ЭВМ банка; 2) действия подсудимого не повлекли вменяемого последствия в виде модификации - т.к. изменение данных по движению денежных средств по лицевому счету не является модификацией информации, поскольку автоматизированная система «Филиал-Сбербанк» в результате этого не претерпела каких-либо изменений, зафиксировав лишь факт доступа к лицевым счетам и факты перевода денежных средств .

Таким образом, при квалификации деяния по признакам составов преступлений, ответственность за которые предусмотрена ст.ст. 159<sup>б</sup> и 272 УК РФ, *следует иметь в виду, что ответственность по данным статьям предусмотрена за совершение различных противоправных действий, с учетом различной объективной стороны преступлений.* При совершении лицом деяния, имеющего все признаки компьютерного мошенничества путем удаления, блокирования, модификации либо копирования компьютерной информации, необходимо установить наличие неправомерного доступа к охраняемой законом компьютерной информации. Если такие признаки установлены (в рамках последствий, наступивших в результате компьютерного мошенничества), то необходима квалификация действия лица как идеальной совокупности преступлений.

В пользу необходимости квалификации совершенного лицом рассматриваемого нами одного деяния по совокупности преступлений

свидетельствуют установленная законодателем оценка степени тяжести вреда, причиняемой собственности и сфере компьютерной информации. Как следует из положения ст. 159<sup>б</sup> УК РФ, основным объектом уголовно-правовой охраны является собственность, а дополнительным - компьютерная безопасность. Частью первой рассматриваемой статьи максимальный размер наказания установлен в виде четырех месяцев ареста.

Посягательство на объект в виде компьютерной безопасности, являющийся дополнительным в компьютерном мошенничестве, сопряженным с неправомерным доступом к охраняемой законом компьютерной информации (ч. 1 ст. 272 УК РФ), наказуемо лишением свободы до 2 лет. Однако при осуществлении компьютерного мошенничества санкции необходимо сопоставлять с частью второй ст. 272 УК РФ, а не частью первой, как совершаемое с корыстной заинтересованностью, за которое максимальная санкция установлена в размере до 4 лет лишения свободы.

Таким образом, нельзя ставить знак равенства между компьютерным мошенничеством, совершенным путем удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование компьютерной техники (в т.ч. копирования компьютерной информации), и неправомерным доступом к компьютерной информации (ст. 272 УК РФ). Поэтому квалификация деяния только по ч. 1 ст. 159<sup>б</sup> УК РФ не отражает в полной мере общественную опасность совершаемого деяния и требует, как уже говорилось, квалификации по совокупности преступлений при наличии соответствующих оснований. Такое положение полностью отражает актуальность данного разъяснения в п. 12 постановления Пленума Верховного Суда РФ от 27.12.2007 № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате», в котором говорится о необходимости квалификации по совокупности преступлений, ответственность за которые предусмотрена ст.ст. 159 и 272 УК РФ (до дополнения УК РФ ст. 159<sup>б</sup> УК РФ), вопреки имеющимся позициям в литературе.

## Библиографический список

1. Уголовный Кодекс Российской Федерации от 13 июня 1996 Г. № 63-ФЗ (ред. от 19.09.2019) // Собрание законодательства РФ. 1996. № 25, ст. 2954.
2. Бюллетень Верховного Суда РФ. 2003. № 2.
3. Апелляционное постановление Верховного Суда Республики Татарстан по делу № 22-7630 от 01.11.16 г. // ГАС «Правосудие». URL: <http://vs.tat.sudrf.ru/> (дата обращения: 17.07.19).
4. Гайфутдинов Р.Р. Понятие и квалификация преступлений против безопасности компьютерной информации: дис. ... канд. юрид. наук. Казань, 2017.
5. Материалы уголовного дела № 917417 МВД по РТ ГСУ СЧ // Архив Советского районного суда г. Казани Республики Татарстан. // <http://sovetsky.tat.sudrf.ru/> (дата обращения: 17.07.19).