УДК 343.2

Доронина А.А.,
Студентка магистратуры 2 курса кафедры «Уголовное право»
Волгоградский Государственный Университет,
Россия, Волгоград

ПРОБЛЕМЫ КВАЛИФИКАЦИИ МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Аннотация. *Статья посвящена исследованию нового специального состава мошенничества — мошенничества в сфере компьютерной информации. Рассмотрены основные проблемы квалификации мошенничества в сфере компьютерной информации.*

Ключевые слова: *компьютерное мошенничество, компьютерная информация, мошенничество, хищение, чужое имущество, дополнительная квалификация.*

PROBLEMS OF COMPUTER INFORMATION FRAUD QUALIFICATION

Annotation. *The article is devoted to the study of a new special composition of fraud - fraud in the field of computer information. The main problems of qualification of fraud in the field of computer information are considered.*

Keywords: *computer fraud, computer information, fraud, theft, other people's property, additional qualification.*

С каждым годом идет бурное развитие и совершенствование компьютерных технологий, в связи с чем возрастает вероятность совершения преступлений в данной сфере. С учетом намеченной тенденции развития криминальных отношений, в Уголовный кодекс Российской Федерации

Федеральным законом от 29 ноября 2012 г. N207-ФЗ закреплены нормы, которые регулируют ответственность за мошенничество в сфере компьютерной информации. Однако, изучив научную литературу, можно сделать вывод, что среди ученных, данное изменение вызвало немало споров.

Суть проблемы, в первую очередь, в том, что некорректно сформулированная диспозиция компьютерного мошенничества имеет противоречия с общим пониманием мошенничества и тем самым создает большое количество проблем применения данной нормы на практике, начиная с того, что в данной норме законодателем прямо не указан способ совершения мошенничества — обман, заканчивая разграничением данного преступного деяния с составами компьютерных преступлений.

Первостепенным объектом мошенничества в сфере компьютерной информации является собственность, как экономико-правовая категория. Необходимо отметить, что в исключительных случаях, исходя из специфики способов и средств исследуемого общественно опасного деяния, в качества дополнительного объекта может выступать также и безопасность в сфере компьютерных технологий.

Объективная сторона данного состава преступления выражена в хищении чужого имущества или приобретении 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.

Как видно из диспозиции, особенностью мошенничества в сфере компьютерной информации является перенос обмана в виртуальный мир. Само понятие компьютерной информации содержится в примечании 1 к ст. 272 УК, где под ней понимаются «сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи».

Тем самым, преступник осуществляет какие-либо операции с компьютерной информацией, при этом корректирует ее так, чтобы обратить в свою пользу, против воли собственника или законного владельца чужое имущество или право на чужое имущество.

Рассмотрим примеры операций, которые совершены с грубым нарушением закона.

Во-первых, это ввод компьютерной информации, которая изначально не соответствует действительности.

Во-вторых, в удалении, когда информация уничтожается, например, о владельце ценных бумаг или искажении, в этом случае вторая часть информации будет недостаточной.

В-третьих, в блокировании, когда информация не уничтожается и не искажается, однако, доступ к ней либо вообще запрещен, либо даже ограничен.

И, в-четвертых, в модификации. В этом случае лицом могут вноситься другие данные, например о состоянии банковского счета права на чужое имущество. Преступление может быть совершено и еще одним способом, который законодатель тоже относит к обману, хотя следует говорить о краже, в частности путем иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Прямо говоря, здесь обман-то отсутствует.

Любой вид мошенничества всегда характеризуется обманом человека, а сама терминология «обмана» означает наличие отношений между двумя сторонами, в котором потерпевший гражданин вводится в заблуждение, и здесь четко прослеживается совершение кражи путем махинаций с виртуальными документами, поэтому выделение данного вида мошенничества, далеко не бесспорно [6]. Отсюда возникает много различных дискуссий и мнений авторов. Проанализируем основные взгляды авторов.

А.Ю. Чупрова выделяет некоторые особенности диспозиции рассматриваемой нормы:

1) отсутствуют способы мошенничества — обман и злоупотребление доверием, а вместо них законодатель использует термины, которые мы ранее рассмотрели,

2) происходит контакт человека с компьютером с помощью специальных программ,

3) мошенничество не сопряжено с добровольной передачей имущества или права на имущество, преступник обращает их в свою пользу тайным способом,

4) субъект расширяет тайный способ совершения преступления, присущий краже, потому что потерпевший не знает о том, что злоумышленник осуществляет вмешательство в компьютерную информацию, манипулируя личной идентифицирующей информацией потерпевшего, чем нарушает установленный правопорядок в информационной сфере, обеспечивающий его безопасное использование сторонами информационных отношений, выступающий в качестве их дополнительного объекта [3].

Предметом исследования является не отдельный вид мошенничества, а отдельная форма хищения чужого имущества исключительными способами совершения общественно опасного деяния.

По мнению А.А. Южина следует изменить название рассматриваемой нормы, при этом указав, что этой новый способ хищения — хищение с помощью компьютерной информации либо переместить в главу, которая посвящена компьютерным преступлениям.

Обратим внимание на то, что при расследовании уголовных дел, использование понятия — «электрический сигнал» доставляет серьезные трудности. В первую очередь это связано тем, что на законодательном уровне не определено, что такое электрический сигнал, а во-вторых, изобретаются новые технологии без электронных устройств (нанотехнологии).

Мы склоняемся к мнению, что понятие, которое применяется в процессе уголовного судопроизводства должно содержать в себе все признаки информации ЭВМ, в том числе с учетом «всех лазеек», то есть совершенствования или появления новых информационных технологий.

Проблема также заключается и в совокупности преступлений. Данная проблема возникает в связи с тем, что новые виды мошенничества совершаются способами, составляющими самостоятельные преступления. Во всех четырех статьях гл. 28 УК законодатель использует понятия «уничтожение, блокирование, модификация либо копирование компьютерной информации».

Вопрос дополнительной квалификацией по ст. ст. 274.1 УК РФ, по нашему мнению, необходим в связи с тем, что в ней содержится особый объект - критическая информационная инфраструктура, а в ст. 159.6 он не предусмотрен вообще.

В случае если составом мошенничества в сфере компьютерной информации не охватывается создание вредоносных программ, думается, что необходима квалификация по ч. 2 ст. 273 УК по признаку корыстной заинтересованности. Однако гораздо сложнее с составами ст. ст. 272 и 274 УК.

Таким образом, деяние - или неправомерный доступ, или нарушение правил эксплуатации - влечет за собой уничтожение, блокирование или модификацию компьютерной информации. Абсолютно то же самое мы имеем и в ст. 159.6 УК, только помимо этого преступник таким образом еще и завладевает чужим имуществом или правом на него.

Можно сказать, что состав неправомерного доступа всегда полностью выполняется в мошенничестве в сфере компьютерной информации, является его частью. Полностью охватывается компьютерным мошенничеством и нарушение правил эксплуатации компьютерных систем, с учетом того только, что оно в качестве самостоятельного состава преступно при наступлении крупного ущерба.

Исходя из изложенного, можем сделать вывод, что дополнительная квалификация компьютерного мошенничества по ст. ст. 272 и 274 УК не требуется, кроме ситуации связанной с последствиями в виде копирования, не предусмотренными ст. 159.6 УК РФ и не связанного с хищением.

В науке уголовного права данный вопрос является спорным. Основная масса ученных утверждают, что компьютерное мошенничество необходимо дополнительно квалифицировать по 272 или ст. 273 УК РФ [1].

Невозможно не согласиться. Однако, возникает очередная проблема, что по правилам квалификации преступлений это совершенно неверно. Когда признаки одного состава преступления полностью входят в число признаков другого преступного посягательства, предусматривающего и дополнительные признаки, должен применяться только последний состав. Законодателем это определено как совокупность деяний, а нормы предусмотренные в ст. 272 (274) УК и ст. 159.6 УК, конкурируют между собой как часть и целое.

Таким образом, получается, что законодатель сам себе противоречит, устанавливая меньшее наказание за то деяние, которое содержит признаки двух преступлений, нежели наказание за преступления, являющиеся его частью [4].

Исходя из изложенного, постараемся кратко сформулировать вывод. Новый состав мошенничества сформулирован крайне неудачно и противоречит понятию мошенничества, и это влечет достаточно большое количество проблем применения данной нормы на практике, в связи с чем наблюдается ее отсутствие. Исходя из смысла, вложенного законодателем в содержание ст. 159.6 УК РФ, следует, что предметом анализа является не специальный состав мошенничества, а самостоятельная форма хищения чужого имущества с присущими ей неповторимы способами совершения преступления.

Мы, абсолютно обоснованно, соглашаемся с мнением многих ученых, что необходимо ввести в гл. 21 УК РФ новую норму, которая будет

предусматривать ответственность за совершение хищения с использованием компьютерной информации.

Использованные источники:

1. Болсуновская, Л.А. Анализ способов совершения мошенничества в сфере компьютерной информации / Л.А. Болсуновская.—Текст: непосредственный // Уголовное право.— 2016.— № 2.—С. 12–16.

2. Лопашенко, А.А. Компьютерное мошенничество — новое слово в понимании хищения или ошибка законодателя? / А.А. Лопашенко.—Текст: непосредственный // Пермский юридический альманах. Ежегодный научный журнал.— 2019.— № 1.—С. 598–609.

3. Чупрова, А.Ю. Проблемы квалификации мошенничества с использованием информационных технологий / А.Ю. Чупрова.—Текст: непосредственный // Уголовное право.— 2015.— № 5.—С. 131–134.

4. Шарапов Р.Д. Актуальные вопросы квалификации новых видов мошенничества. // Проблемы квалификации и расследования преступлений, подследственных органам дознания / Р.Д. Шарапов.— Текст: непосредственный // всеросс. науч.-практ. конф..—Тюмень: Тюменский институт повышения квалификации, 2013.—С. 3–5.

5. Шеслер А.В. Мошенничество: проблемы реализации законодательных новелл / А.В. Шеслер.—Текст: непосредственный // Уголовное право.— 2013.— № 2.—С. 67–71.

6. Южин А.А. Мошенничество и его виды в российском уголовном праве: специальность 40.03.01 «Юриспруденция»: диссертация на соискание ученой степени кандидата педагогических наук / Южин А.А., Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный юридический университет имени О.Е. Кутафина (МГЮА)».—Москва, 2017.— 238 с.—Текст: непосредственный.