УДК

Р.А. Оценова

ПРОБЛЕМЫ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ, СОВЕРШЕННЫХ ГРУППОЙ ЛИЦ ПО ПРЕДВАРИТЕЛЬНОМУ СГОВОРУ И ОРГАНИЗОВАННОЙ ГРУППОЙ

Совершение преступлений в сфере компьютерной информации группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ или их сети (УК КР ч.II ст. 289). [1].

Одним из квалифицирующих признаков состава преступления, предусматривающего ответственность за неправомерный доступ к компьютерной информации, является совершение данного преступления группой лиц по предварительному сговору.

Совершение преступления группой лиц по предварительному сговору - это совершение его двумя или более лицами, заранее договорившимися о совместном совершении преступления (ч. 2 ст. 33 УК КР). Применительно к несанкционированному доступу к компьютерной информации совершение преступления группой лиц должно выражаться в совместном участии нескольких лиц в совершении деяния, запрещенного ст. 289 УК КР.

Каждый участник группы должен полностью или частично выполнять действия, образующие объективную сторону состава рассматриваемого преступления.

Для неправомерного доступа к охраняемой законом компьютерной информации уголовным законом не предусмотрено такого квалифицирующего признака, как совершение деяния простой группой (т. е. без предварительной договоренности), что скорее всего обусловлено такой степенью общественной опасности этого вида соучастия, которая не позволяет выделять его в качестве квалифицирующего обстоятельства. Несмотря на это обстоятельство, совершение неправомерного доступа группой лиц возможно и без предварительного сговора между соучастниками, хотя надо признать, что встречается это крайне редко.

Особенность соучастия в преступлении без предварительного сговора заключается в том, что соглашение о совместном участии в посягательстве достигается после начала выполнения объективной стороны, т.е. на стадии покушения на преступление.

Такого рода соисполнительство при совершении анализируемого деяния имеет место в том случае, когда оно начинается одним лицом, а затем уже в процессе неправомерного доступа к компьютерной информации к его действиям присоединяется другое лицо, пожелавшее участвовать в совершении начатого преступления. В этом случае имеет место не простое совпадение действий виновных во времени и пространстве, - преступление совершается сообща, путем объединения усилий для достижения единого, общего для всех соучастников преступного результата.

Действия соисполнителей неправомерного доступа к компьютерной информации, объединенных между собой без предварительного сговора, не образуют признаков, характерных для квалифицированного состава этого преступления и, следовательно, уголовная ответственность за их совершение должна наступать по ч.II п. 1 ст. 289 УК КР. Для оценки деяния, ответственность за которое предусмотрена ч. II ст. 289 УК КР, как совершенного группой лиц по предварительному сговору, в каждом конкретном случае необходимо установить, что договоренность о совместном совершении преступления будущими соисполнителями была достигнута до непосредственного осуществления действий, образующих объективную сторону состава этого преступления. При этом промежуток времени между сговором и началом совершения конкретных общественно опасных действий не имеет решающего значения.

Сговор может иметь место задолго до совершения таких действий, либо непосредственно перед началом осуществления таковых, но не в процессе их совершения [2].

Таким образом, по смыслу закона, достижение соглашения на совершение подобных действий следует отождествлять со стадией приготовления к неправомерному доступу к компьютерной информации.

Дискуссионным является вопрос о том, должны ли все участники неправомерного доступа, совершаемого по предварительному сговору группой лиц, быть исполнителями (соисполнителями) этого преступления. Полагаем, что ответ на него должен быть только утвердительным, несмотря на то, что п. 2 ст. 33 УК КР непосредственно не характеризует участников данного вида группового преступления как исполнителей (соисполнителей).

В связи с этим следует согласиться с аргументом В.С. Комиссарова, который, отстаивая аналогичную заявленной нами точку зрения, утверждает, что в случаях, когда группа лиц по предварительному сговору предусматривается в Особенной части УК КР как квалифицирующий признак, она должна состоять только из соисполнителей [3].

Подобное понимание соисполнительства, при совершении преступления вытекает и из систематического толкования норм Общей части уголовного закона, которыми установлены признаки соучастия. Если признать пособника или подстрекателя участником преступной группы, образованной по предварительному сговору, законодательное обособление сложного соучастия с распределением ролей теряло бы смысл. Такую точку зрения занимают и авторы, подготовившие монографию о расследовании неправомерного доступа к компьютерной информации [4]. Это не означает, что между соучастниками квалифицированного неправомерного доступа вообще не может быть распределения ролевых функций. Соисполнительство не исключает распределения исполнительских функций между участниками, не влияющего на квалификацию содеянного [3].

Действия соисполнителей квалифицируются без ссылки на ст. 30 УК КР.

При совершении неправомерного доступа к компьютерной информации группой лиц по предварительному сговору распределение ролевых функций между различными соучастниками также сводится к совершению действий, которые состоят в частичном выполнении объективной стороны состава этого преступления и не содержат признаков материального пособничества или иной формы сложного соучастия. Например, один из соучастников "взламывает" закрытую компьютерную сеть и передает управление тому лицу, которое произведет поиск и уничтожение (либо блокирование, копирование, модификацию) интересующей виновных информации. Подобные ситуации могут возникать при неправомерном доступе в компьютерные сети банков, с последующим несанкционированным перечислением денежных средств. Одни лица занимаются взломом защиты компьютерной сети банка, а другие - внесением изменений фальсификаций в бухгалтерскую информацию.

Лица, непосредственно не участвовавшие в совершении неправомерного доступа, а исполнявшие роль организатора, подстрекателя или пособника, должны нести ответственность по соответствующей части ст. 30 УК КР и ст. 289 УК КР.

Деятельность двух или более лиц по совершению данного преступления не может быть признана групповой, в смысле квалифицирующего признака неправомерного доступа к компьютерной информации, если одно лицо выступает в качестве подстрекателя, а другое - непосредственного исполнителя, т.к. участники этой группы не являются соисполнителями. Действия исполнителя в данном случае должны квалифицироваться по п. 1 ст. 289 УК КР. со ссылкой на п. 3 ст. 30 УК КР (исполнитель). Подстрекатель же должен отвечать по п. 1 ст. 289 УК КР со ссылкой на п. 5 ст. 30 УК КР (подстрекатель). Если лицо сообщает виновному пароль доступа к информации, то его действия должны быть квалифицированны по п. 1 ст. 289 УК КР со ссылкой на п. 6 ст. 30 УК КР (пособник).

На практике преступлений в России имели место случаи, когда при осуществлении неправомерного доступа осуществлялось чисто техническое распределение ролей, т.е. действия некоторых участников по своим внешним чертам соответствовали признакам пособничества. Эти действия выполнялись одновременно с осуществлением неправомерного доступа к компьютерной информации. Так, сотрудник коммерческого банка, вступив в преступный сговор с другим лицом, в заранее обусловленное время блокирует систему защиты с тем, что бы его соучастник проник в компьютерную сеть банка. При рассмотрении такой ситуации необходимо иметь в виду, что при совершении конкретного преступления в пределах объективной стороны внутри группы лиц по предварительному сговору вполне возможно "техническое" распределение ролей, не влияющее на квалификацию [5] , то же самое можно сказать и

о неправомерном доступе к компьютерной информации. Распределение ролей при совершении этого преступления может быть связано с технологией выполнения действий, образующих его объективную сторону, что не влияет на квалификацию деяния так же, как не влияет на квалификацию действий соисполнителей при совершении групповой кражи распределение между ними различных ролевых функций, ни одна из которых не содержит признаков материального пособничества или какой-либо другой формы сложного соучастия (взлом помещения, изъятие имущества, обеспечение тайности изъятия имущества и т. п.) [5].

При совершении рассматриваемого преступления группой лиц по предварительному сговору распределение ролевых функций между различными соучастниками также сводится к совершению действий, которые состоят в частичном выполнении объективной стороны состава этого преступления и не содержат признаков материального пособничества или иной формы сложного соучастия.

В данном случае имеет место соисполнительство с распределением ролей, если виновные объединены предварительной договоренностью на совершение неправомерного доступа к защищаемой законом компьютерной информации.

Для признания неправомерного доступа к компьютерной информации, совершенным по предварительному сговору группой лиц не требуется, чтобы все соисполнители в полном объеме принимали участие в совершении этого преступления. Для признания участника такой группы соисполнителем преступления, ответственность за которое предусмотрена п. 2 ст. 289 УК КР, достаточно совершения им действия, которое непосредственно направлено на достижение общего преступного результата. Например, одно лицо "взламывает" защиту информации, а другое выполняет какие либо манипуляции с ней (уничтожает, блокирует, модифицирует или копирует), либо первый соучастник начинает уничтожение информации, а второй его заканчивает. Важным в данном случае является лишь наличие предварительного сговора о совершении этого деяния до момента выполнения объективной стороны преступления.

Особого внимания заслуживает вопрос об участии в групповом совершении неправомерного доступа к компьютерной информации двух лиц, если одно из них во время совершения преступного деяния не отвечает признакам субъекта преступления (вменяемость, возраст уголовной ответственности).

Одни авторы полагают, что действия лица, соответствующего признакам субъекта, участвовавшего вместе с подростком в совершении преступления, предусмотренного ст. 289 УК КР, образуют групповой способ посягательства только в том случае, если подросток обладал общими признаками субъекта преступления, то есть, вменяемое лицо, достигшее шестнадцатилетнего возраста выступает в качестве единственного исполнителя этого деяния и квалификации по п. 2 ст. 289 УК КР не требуется [6].

Другие авторы вкладывают в понятие "группа" не только юридический, но и социальный смысл [7].

Нам представляется, что более объективным было бы решение данного вопроса с учетом значимости участия лица, не подпадающего под признаки субъекта, в достижении совместного преступного результата. Так, если участие лица в выполнении объективной стороны преступления оказывало существенное влияние на достижение результатов преступления, то вполне логичным было бы квалифицировать деяние виновного, соответствующего признакам субъекта, как совершенное в составе группы лиц. Если же участие лица, не достигшего возраста уголовной ответственности

являлось не существенным (при совершении неправомерного доступа это лицо занималось лишь разархивацией данных), то полагаем, что нет необходимости в квалификации деяния, совершенного взрослым участником группы по п. 2 ст. 289 УК КР.

Здесь достаточно будет квалифицировать содеянное по п. 1 ст. 289 УК КР и ст. 156 УК КР (вовлечение несовершеннолетнего в совершение преступления).

Степень значимости участия в совершении преступления должна определяться в зависимости от всех обстоятельств дела, в том числе от обстановки, места совершения преступления, технической оснащенности, профессиональной подготовленности лица, особенностей неправомерного доступа к компьютерной информации в каждом конкретном случае.

Квалификация преступлений в сфере компьютерной информации, совершенных организованной группой, вызывает большую сложность, представляет определение системы признаков организованной группы применительно к неправомерному доступу к компьютерной информации (п. 2 ст. 289 УК КР).

В ст. 33 УК КР преступление признается совершенным организованной группой, если создавшее организованную группу или руководившее ею, несёт ответственность за все совершённые этой группой преступления, которые охватывались его умыслом.

Таким образом, уголовный закон определяет только два признака организованной группы: умысел, особая цель ее образования (совершение одного или нескольких преступлений), что не дает достаточно четкого представления о ее отличии от группы лиц, действующих по предварительному сговору. В практике высших судебных органов неоднократно предпринимались попытки дать разъяснение признаков организованной группы, которое позволило бы более четко отграничить таковую от других объединений.

Некоторые авторы делают попытку разобраться в этом понятии и предлагают под признаком устойчивости подразумевать умысел соучастников на совершение нескольких преступлений или даже одного, но требующего тщательного планирования совместных действий, распределения ролей между участниками, оснащения их орудиями, средствами, техникой, а равно наличия организатора или руководителя группы [8]. Полагаем, что данное разъяснение также не дает четкого представления об устойчивости организованной группы.

Таким образом, несмотря на неоднократные попытки разъяснить содержание системы признаков организованной группы в сфере компьютерных преступлений, достаточного представления о данном виде криминального сотрудничества ни в теории уголовного права, ни на практике применения уголовного закона не сложилось.

Исходя из современных научных представлений о данной форме преступных объединений и руководящих разъяснений высших судебных органов Кыргызской Республики, нам представляется возможным выделить отдельные признаки совершения неправомерного доступа к охраняемой законом информации организованной группой. Такая группа должна отличаться наличием организатора или руководителя.

Именно организатор, как справедливо отмечают Л. Д. Гаухман и С.В. Максимов, создает группу, осуществляет подбор соучастников, распределяет роли между ними, устанавливает дисциплину и т.п., а руководитель обеспечивает целенаправленную, спланированную и слаженную деятельность как группы в целом, так и каждого ее участника [9].

В организованную группу могут входить лица, выполняющие управленческие функции в коммерческих или иных организациях, а также должностные лица, равно как и иные служащие. Участие таковых в организованной группе может заметно облегчить подготовку и совершение неправомерного доступа к компьютерной информации, а также сокрытие этого преступления. При этом использование ими своего служебного положения в целях непосредственного совершения этого преступления, либо в целях содействия другим участникам организованной группы в совершении неправомерного доступа, должно учитываться при назначении им наказания.

В отличие от участников преступной группы лиц, действующих по предварительному сговору, отдельные участники организованной группы могут быть не только соисполнителями преступления, но и выполнять функции организатора, либо пособника. Их действия должны квалифицироваться как соисполнительство при совершении преступления организованной группой (по п. 2 ст. 289 УК КР) без ссылки на ст. 30 УК КР. Однако при совершении неправомерного доступа к компьютерной информации организованной группой, как и при совершении других преступлений в соучастии указанного вида, все же возможно и сложное соучастие. Например, когда лицо, не являющееся участником организованной группы, выступает пособником совершения такого деяния, в частности, оказывая помощь участникам организованной группы путем предоставления необходимой для совершения преступления информации.

ЛИТЕРАТУГА

1. Расследование неправомерного доступа к компьютерной информации. Под ред. Н.Г. Шурухнова. –М., 1999. –С. 86.

2. Кригер Г.А. Квалификация хищений социалистического имущества. –М., 1974. – С. 217.

3. См. Курс уголовного права. Общая часть: Учебник для вузов /Под ред. Н.Ф. Кузнецовой. –М., 1999.-Том 1: Учение о преступлении. –С. 417.

4. См. Расследование неправомерного доступа к компьютерной информации /Под ред. Н.Г. Шуруханова. –М., 1999. –С. 83.

5. Лавров В.В. Уголовная ответственность за легализацию (отмывание) денежных средств или иного имущества. –М., 1999. –С. 216.

6. Расследование неправомерного доступа к компьютерной информации /Под ред. Н.Г. Шуруханова. –М., 1999. –С.90.

7. Куринов Б.А. Научные основы квалификации преступления. –М., 1984. –С. 141-142; Практикум по уголовному праву: Учебное пособие /Под ред. Л.Л. Кругликова. –М., 1997. –С. 111.

8. О практике применения судами законодательства об ответственности за бандитизм: Постановление пленума Верховного суда РФ от 17.01.97. №1 //Российская газета, 1997. 30 января.

9. Гаухман Л.Д., Максимов С.В. Уголовная ответственность за организацию преступного сообщества (преступной организации), -М., 1997. –С.9.