Зайцев Владимир Сергеевич
магистрант
Горбань Владимир Сергеевич
канд. юрид. наук, доцент, заместитель декана
Институт сервиса, туризма и дизайна (филиал)
ФГАОУ ВО «Северо-Кавказский федеральный университет»
г. Пятигорск, Ставропольский край

DOI 10.21661/r-114506

ПРОБЛЕМЫ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЯ, ПРЕДУСМОТРЕННОГО СТ. 272 УК РФ

Аннотация: *в данной статье рассматриваются проблемы квалификации преступных деяний, связанных с незаконным доступом к охраняемой законом информации, для которой законодательно установлен специальный режим ее правовой защиты. В работе раскрыты основные особенности таких проблем квалификации преступления, предусмотренного ст. 272 УК РФ, как трактовка понятия «неправомерный доступ к компьютерной информации», определение в деянии лица вины в виде умысла. В заключение авторами предложены пути решения исследованных проблем.*

Ключевые слова: *неправомерный доступ, компьютерная информация, квалификации преступных деяний, преступление.*

Неправомерный доступ к компьютерной информации, если такой доступ стал причиной уничтожения, блокирования, модификации либо копирования информации, а также нарушения работы вычислительных систем, влечет за собой наступление ответственности за указанное противозаконное деяние, предусмотренной согласно Уголовному кодексу Российской Федерации (далее – УК РФ) ст. 272 УК РФ. Указанная статья защищает права лиц на неприкосновенность информации в используемой ими системе. Согласно ч.4 ст.1280 Гражданского кодекса Российской Федерации лицо, которое правомерно использует услуги по обработке информации как собственник вычислительной системы, либо лицо,

которое приобрело право использования системы или информации, является владельцем информационной вычислительной системы и содержащейся в ней информации. Под сферу защиты данной статьи подпадает компьютерная информацию любых предприятий, учреждений, организаций и частных лиц. Диспозиция соответствующей нормы заключается в неправомерном доступе к охраняемой законом компьютерной информации.

Из чего следует, что для наступления ответственности по ст. 272 УК РФ, преступное деяние должно состоять в неправомерном доступе к охраняемой законом компьютерной информации, который всегда связан с совершением определенных действий. Так, он может быть осуществлено как проникновение в компьютерную систему путем использования специальных технических или программных средств, которые позволяют преодолеть установленные системы защиты; незаконное применение действующих паролей или маскировка под видом законного пользователя для проникновения в компьютер; хищение носителей информации, при условии принятия мер по их охране, а само преступное деяние повлекло уничтожение или блокирование информации.

Информацию, для которой законодательно установлен специальный режим ее правовой защиты, например – государственная, служебная и коммерческая тайна, персональные данные и другие, – следует считать охраняемой законом информацией [1]. А неправомерным доступом к охраняемой законом информации является доступ, который противоречит действующим правовым нормам, актам управления, приказам, распоряжениям и иным актам, регулирующим отношения по доступу лиц (группы лиц) к информации [2]. Помимо этого доступ к информации будет являться неправомерный в том случае, если лицом для возможности использования информации были незаконно использованы специальные технические средства для проникновения в устройство или его сеть, такие как модификация программы, снятие пароля, в обход имеющемуся на устройстве и так далее. Самовольное получение информации без разрешения ее собственника или владельца так же следует рассматривать как неправомерный доступ к охраняемой законом компьютерной информации.

Одна из трудностей, с которой приходится сталкиваться при квалификации общественно опасных деяний, ответственность за которые предусмотрена ст. 272 УК РФ, связана как раз-таки с трактовкой понятия «неправомерный доступ к компьютерной информации».

На первый взгляд, исходя из диспозиции ст. 272 УК РФ, выделяются следующие обязательные признаки объективной стороны неправомерного доступа к охраняемой законом компьютерной информации: наступление общественно опасных последствий в виде уничтожения или блокирования, а модификация данных при копировании компьютерной информации, нарушения работы ЭВМ или их сети, и обязательное наличие причинно-следственной связи между, то есть взаимосвязь между совершенным деянием и наступившими последствиями. При отсутствии одного из указанных признаков, уголовная ответственность за общественно опасное деяние, предусмотренная ст. 272 УК РФ, исключается. Но как указано ранее необходимым условием для верной квалификации указанного деяния является четкая трактовка понятия «неправомерный доступ к компьютерной информации».

Так, существует мнение, что доступ к информации, содержащейся на устройстве и в его системе, следует считать неправомерным, когда к ресурсам ЭВМ и их сети несанкционировано обращается лицо, которое право доступа к указанному ЭВМ, его ресурсам и ресурсам его сети вообще не имеет. А.Ю. Красиковым предложено следующее, на наш взгляд, более точное определение данного понятия: «неправомерным доступ считается не только при отсутствии такого права, но и при отсутствии правил защиты компьютерной информации».

Следовательно, преступление, квалифицирующееся по ст. 272 УК РФ, следует считать оконченным, если совершено несанкционированное преодоление программных средств защиты информации. Попытку же несанкционированного проникновения к охраняемой законом информации следует рассматривать как покушение на неправомерный доступ. А сами действия лица, которые так или иначе связаны с осуществлением неправомерного доступа к компьютерной ин-

формации, но которые не повлекли нарушения работы ЭВМ или их сети по причине возникновения обстоятельств, независящих от лица этот доступ совершающего следует квалифицировать по ст.272 УК РФ со ссылкой на ч. 3 ст. 30 УК РФ.

Состав преступления, ответственность за совершение, которого предусмотрена ст. 271 УК РФ, является материальный, причем деяние, согласно диспозиции статьи, определено в форме действия и предполагается обязательное наступление одного из следующих последствий:

– полное либо частичное уничтожения информации, под которым понимается удаление либо стирание информации, содержащейся на материальном носителе, при осуществлении которого невозможно ее восстановление;

– осуществление блокировки информации, то есть совершение таких действий, которые привели к ограничению или закрытию доступа к компьютерной системе и предоставляемым ею информационным ресурсам;

– внесение различных изменений в: программы, базы данных, текстовую информацию, находящуюся на материальном носителе, то есть так называемая модификация как самого устройства, так и содержащегося на нем программного обеспечения и информации;

– перенос информации на иной материальный носитель, при сохранении неизмененной первоначальной информации, то есть копирование информации;

– совершение действий, ведущих к нарушению работы ЭВМ, системы ЭВМ или их сети, выражающемся в нарушении работы как отдельных программ, баз данных, выдаче искаженной информации, так и нештатном функционировании аппаратных средств и периферийных устройств, либо нарушении нормального функционирования сети.

Как нами отмечалось ране особо важным для квалификации деяния как неправомерный доступ к компьютерной информации несомненно является установление причинной связи между самими несанкционированным доступом и наступившими из-за него последствиями. Уничтожение и блокирование информации, нарушение работы ЭВМ может происходить в результате технических

неисправностей или ошибок в программных средствах. В таком случае лицо, совершившее неправомерный доступ к компьютерной информации, ответственности за предпринятые им действия не подлежит по причине отсутствия причинно-следственной связи между действиями и наступившими последствиями.

Преступление, ответственность за которое наступает согласно ст. 272 УК РФ, считается оконченным в момент наступления предусмотренных в данной статье последствий. Следовательно, все действия, выполненные до формальной подачи последней команды, образовывают состав неоконченного преступления.

Мотивы и цели совершения рассматриваемого преступного деяния могут быть любыми. К ним можно отнести и корыстный мотив, и месть, и зависть, и цель получить какую-либо информацию, и желание причинить вред или проверить свои профессиональные способности, либо самоутвердится.

Квалификация деяния, ответственность за осуществление которого предусмотрена ст. 272 УК РФ, существенно затрудняется на этапе определения в деянии лица вины в виде умысла, по причине того, что при различных состояниях вычислительной системы, зачастую преступнику предварительно неизвестных, одни и те же действия могут приводить к различным последствиям. То есть одни и те же действия, с одним и тем же умыслом могут приводить к неожиданным для виновного последствиям.

Но, при подобном подходе к квалификации деяния отмечается явное наличие противоречий нормам, закрепленным ст.24 УК РФ, согласно которой деяние, совершенное только по неосторожности, признается преступлением лишь в том случае, когда это специально предусмотрено соответствующей статьей Особенной части УК РФ. Согласно которой, в рассматриваемом случае, неправомерный доступ к охраняемой законом компьютерной информации, содержащий признаки неосторожной формы вины, преступлением не является.

Так, в диспозиции ст. 272 УК РФ законодателем явно указано, что осуществляемые в отношении компьютерной информации, которая охраняется законом, действия обязаны носить неправомерный характер, то есть лицо должно не иметь

права на доступ к информации, либо лицо право на доступ к данной информации имеет, однако осуществляет его помимо установленного порядка, с нарушением правил ее защиты. В случае если лицо совершает доступ к компьютерной информации, осознавая, что не имеет для этого законных оснований тем самым нарушая режим доступа к информации, такое лицо поступает общественно опасно. В этом случае неправомерные действия виновного рассматриваются и легко подпадают под формулу прямого или косвенного умысла. То есть лицо, осуществляющее вышеуказанные действия, предвидит возможность наступления указанных в законе общественно опасных последствий и желает их наступления или допускает эти последствия (прямой умысел), либо относится к ним безразлично (косвенный умысел).

Действия, ответственность за совершение которых может квалифицироваться по ст. 272 УК РФ признаются совершенными не с прямым умыслом, а по неосторожности, если лицо, осознает факт неправомерности доступа в отношении компьютерной информации, находящейся под охраной закона, но самонадеянно рассчитывает на их предотвращение – легкомыслие; либо не проявило необходимой внимательности и предусмотрительности – небрежность. Подобные ситуации предусмотрены ст. 274 УК РФ, заключаются в выраженном умышленном характере рассматриваемого деяния, и в диспозиции ст. 272 УК не указано обратное. Таким образом, при неправомерном доступе к компьютерной информации законодатель не связывает совершение умышленных действий с не осторожным наступлением последствий, поэтому субъективная сторона этого состава выражается только в форме умысла.

Следовательно, что касается субъективной стороны преступления, ответственность за совершение которого наступает по ст. 272 УК РФ, данные деяния характеризуются наличием прямого умысла (осознание неправомерного доступа, предвидение наступления вредных последствий и желание их наступления) или косвенного умысла (осознание неправомерного доступа, предвидение наступления вредных последствий и сознательное допущение их наступления

либо безразличное отношение к наступлению последствий). То есть неправомерный доступ к компьютерной информации по своей сути является умышленное деяние, поскольку в диспозиции ст.272 УК не указано обратное [2].

При выявлении признаков неправомерного доступа к компьютерной информации и для отграничения данного преступного деяния от иных, смежных преступлений необходимо, на наш взгляд, обращаться к различным методам анализа, которые позволяют рассмотреть конкретное преступление с различных сторон и раскрыть его конструктивные признаки, к коим относятся и экспертные методы. Так же важно установить, на что посягают осуществленные преступником действия, чему они причиняют вред или создают угрозу его причинения.

Таким образом, суть общественно опасного деяния, ответственность за которое предусмотрена ст. 272 УК РФ, заключается в неправомерном доступе к компьютерной информации. Причем следует отличать деяние – «неправомерный доступ к компьютерной информации» от «создание, использование и распространение вредоносных программ для ЭВМ», ответственность за которое регламентируется ст. 273 УК РФ. Состав преступления, предусмотренного ст. 272 УК РФ, материальный и считается оконченным в случае наступления общественно опасных последствий, лежащих в причинно-следственной связи с поведенческим актом виновного.

Список литературы

1. Дворецкий М.Ю. Преступления в сфере информации: Научно-практический комментарий к гл.28.Уголовного кодекса РФ/ М.Ю. Дворецкий. – М., 2005.

2. Маляров А.И. Объект преступления в сфере электронно-цифровой (компьютерной) информации и вопросы квалификации (российский и зарубежный опыт) / А.И. Маляров // Общество и право. – 2012. – №2.

3. Уголовный кодекс Российской Федерации от 13.06.1996 №63-ФЗ (ред. от 06.07.2016) // Информационно-справочный портал «Консультант плюс».

4. Уголовное право России: Учебник для вузов: В 2 т. / Под ред. д-ра юрид. наук, проф. А.Н. Игнатова и д-ра юрид. наук, проф. Ю.А. Красикова. – Т. 1: Общая часть. – М.: Норма, 2005.

5. Зайцева Е.В. Преступления в сфере компьютерной информации: уголовно-правовой и криминологический анализ [Электронный ресурс]. – Режим доступа: http://www.uchit.net/catalog/Gosudarstvo_i_pravo/156914/