Гайфутдинов Рамиль Рустамович. Понятие и квалификация преступлений против безопасности компьютерной информации: диссертация ... кандидата Юридических наук: 12.00.08 / Гайфутдинов Рамиль Рустамович;[Место защиты: ФГАОУ ВО «Казанский (Приволжский) федеральный университет»], 2017.- 243 с.

|  |
| --- |
|  |
| |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  |  |  | | --- | --- | --- | --- | | |  | | --- | | **Содержание к диссертации**  Введение  **Глава 1. Основные положения теории квалификации преступления и их интерпретация к уголовно-правовой оценке деяний против безопасности компьютерной информации 19**  1. Понятие квалификации преступления, ее виды, содержание и правовые основы 19  2. Состав преступления, его виды и алгоритм квалификации преступного деяния 28  3. Правила квалификации преступления и критерии деления их на виды 34  **Глава 2. Социально-правовая обусловленность уголовной ответственности за посягательства на безопасность компьютерной информации 41**  1. Понятие компьютерной информации и преступления против ее безопасности  2. Проблемы криминализации посягательств на безопасность компьютерной информации: сравнительно-правовой аспект 57  **Глава 3. Реализация общих положений теории квалификации преступлений применительно к преступлениям против безопасности компьютерной информации 72**  1. Особенности установления объекта преступления и предмета посягательства при квалификации содеянного 72  2. Выявление признаков объективной стороны названных составов преступлений и деяний в процессе их квалификации 97  3. Законодательное описание признаков субъективной стороны составов преступлений и проблемы ее установления в процессе квалификации содеянного 122  4. Уголовно-правовая характеристика субъекта преступления и его установление в ходе квалификации посягательств против безопасности компьютерной информации 138  5. Особенности уголовно-правовой оценки содеянного при наличии квалифицирующих и особо квалифицирующих признаков составов рассматриваемых составов преступлений 143  **Глава 4. Применение специальных правил квалификации преступлений против безопасности компьютерной информации 150**  1. Понятие и квалификация неоконченной преступной деятельности, направленных против безопасности компьютерной информации 150  2. Особенности квалификации преступлений против безопасности компьютерной информации, совершенных в соучастии 161  3. Квалификация преступлений против безопасности компьютерной информации при их множественности и способы преодоления конкуренции уголовно-правовых норм 167  Заключение 183  Список сокращений и условных обозначений 192  Список использованной литературы   * [Состав преступления, его виды и алгоритм квалификации преступного деяния](http://www.dslib.net/kriminal-pravo/ponjatie-i-kvalifikacija-prestuplenij-protiv-bezopasnosti-kompjuternoj-informacii.html#7701281) * [Проблемы криминализации посягательств на безопасность компьютерной информации: сравнительно-правовой аспект](http://www.dslib.net/kriminal-pravo/ponjatie-i-kvalifikacija-prestuplenij-protiv-bezopasnosti-kompjuternoj-informacii.html#7701282) * [Выявление признаков объективной стороны названных составов преступлений и деяний в процессе их квалификации](http://www.dslib.net/kriminal-pravo/ponjatie-i-kvalifikacija-prestuplenij-protiv-bezopasnosti-kompjuternoj-informacii.html#7701283) * [Особенности квалификации преступлений против безопасности компьютерной информации, совершенных в соучастии](http://www.dslib.net/kriminal-pravo/ponjatie-i-kvalifikacija-prestuplenij-protiv-bezopasnosti-kompjuternoj-informacii.html#7701284)  Состав преступления, его виды и алгоритм квалификации преступного деяния Как отмечалось ранее, состав преступления как законодательная модель (конструкция) позволяет отграничивать один вид преступления от другого. Так, в главе 28 УК РФ содержится описание (указание на признаки) четырех видов преступлений против безопасности компьютерной информации. Система признаков, свойственная каждому из них, образует законодательную модель определенного вида преступления. С их помощью (на их основе) они отграничиваются друг от друга. К примеру, лицом может быть создана вредоносная компьютерная программа (далее - ВКП), а затем распространена. С позиции обывателя совершается несколько преступлений. Однако, по правилам квалификации с учетом признаков непосредственного объекта и в особенности объективной стороны состава преступления, такое деяние рассматривается в качестве единичного, хотя и сложного по характеристике преступления.  Указание на состав преступления как систему объективных и субъективных признаков позволяет рассматривать их как взаимосвязанные между собой. Нередко уголовно-правовая характеристика отдельно взятого признака (к примеру, субъективного) состава преступления позволяет раскрыть содержание другого (к примеру, субъективного) признака состава преступления. Такой подход позволяет выявить структуру состава конкретного вида преступления в полном объеме.  Структуру состава преступления образуют ряд уголовно-правовых признаков 36 , которые характеризуют внешнюю и внутреннюю сторону конкретного деяния. В теории их принято группировать по таким элементам состава преступления, как объект преступления и его объективная сторона, субъект и субъективная сторона. Законодатель использует различные способы формирования состава преступления как информационной модели для квалификации преступления. С учетом этого составы преступлений классифицируются по различным основаниям.  Одним из оснований такой классификации является оценка законодателем степени общественной опасности определенного деяния. Поэтому их подразделяют на основные, привилегированные, квалифицированные и особо квалифицированные составы преступлений. Первый вид состава преступления заключает в себе сущностные (общие) признаки, отражающие специфику данного вида преступления по отношению к другим. Законодательное описание признаков основного состава преступления обычно излагается в начальных (первых) частях соответствующих статей Особенной части УК РФ. Однако законодатель не всегда следует этому подходу. Квалифицированные составы преступлений (с отягчающими обстоятельствами) содержат помимо сущностных признаков обстоятельства, существенно повышающие общественную опасность деяния (обычно это вторые части составов преступлений). Особо квалифицированные составы преступления - обстоятельства, придающие совершенному деянию особую опасность (обычно части третьи и последующие). Привилегированные составы преступлений (со смягчающими обстоятельствами) содержат в себе признаки, уменьшающие степень общественной опасности преступления. Так, состав преступления, изложенный в ч. 1 ст. 272 УК РФ, является основным составом неправомерного доступа к компьютерной информации. В то же время в ст. 2741 УК РФ характеристика основных составов излагается законодателем в частях 1, 2 и 3 данной статьи. Состав преступления, изложенный в ч. 2 ст. 272 УК РФ, является квалифицированным. Составы преступлений, сформулированные в ч. и ч. 4 ст. 272 УК РФ, - особо квалифицированными. Привилегированных составов рассматриваемых нами преступлений законодательство не содержит.  По особенностям конструирования объективной стороны составы преступлений подразделяют обычно на формальные и материальные. Некоторые авторы выделяют среди первых усеченные составы преступления37. Обычно их рассматривают как самостоятельные виды.  Для материального состава преступления характерно, что в качестве обязательного признака их объективной стороны предусматриваются общественно опасные последствия деяния, которые предполагают установление причинной связи между деянием и данным последствием. Объективная сторона преступления в формальных составах описывается путем указания только на само действие (или бездействие) 38 , т.е. содержит описание самого уголовно-наказуемого поступка.  Четыре основных состава преступления против безопасности компьютерной информации, признаки которых излагаются в ч. 1 ст. 272, ч.1 ст. 274 УК РФ, части 2 и 3 ст. 2741 УК РФ, являются по своей конструкции материальными, а два основных состава, изложенных в ч. 1 ст. 273 УК РФ, ч. 1 ст. 2741 УК РФ, -формальными.  В литературе принято считать, что установление вида состава преступления с учетом специфики конструирования законодателем их объективной стороны (формальный, материальный или усеченный состав преступления) способствует установлению момента юридического окончания преступления, времени совершения преступления, установление возможности добровольного отказа от доведения преступления до конца, определения формы вины, множественности преступлений, исчисления сроков давности и т.д.39 С этим следует согласиться. Проблемы криминализации посягательств на безопасность компьютерной информации: сравнительно-правовой аспект Под общественными отношениями понимаются обычно социальные связи, возникающие между людьми, обществом и государством. Причинить вред объекту возможно только путем воздействия на вещи материального мира либо разрыва социальных связей в общественных отношениях160. Считается, что структура общественных отношений включает в себя 1) носителей (субъектов) отношения; 2) предмета, по поводу которого существуют отношения; 3) общественно значимой деятельности (социальной связи) как содержания отношений161. Опираясь на указанную структуру, механизм причинения вреда общественным отношениям выглядит как посягательство на перечисленные элементы общественных отношений либо как разрыв связей между названными элементами.  Поэтому под объектом преступления следует понимать охраняемое уголовным законом общественное отношение, на которое направлено преступное посягательство и которому причиняется ущерб либо создается угроза его причинения162.  Объекты преступлений принято разделять по вертикали и горизонтали. Мы придерживаемся четырехзвенного деления объекта по вертикали на общий, родовой, видовой (который также именуют в качестве группового или специального)163 и непосредственный.  Общий объект уголовно-правовой охраны находит свое отражение в ч. 1 ст. 2 УК РФ. Д. А. Калмыков предлагает его дополнить специальным указанием на охрану информационной безопасности164. Это предложение весьма убедительно. Указание информационной безопасности наряду с другими основными объектами представляется актуальным, ибо служит предпосылкой ее выделения в качестве самостоятельного родового объекта уголовно-правовой охраны. Родовой объект преступления представляет собой совокупность однородных общественных отношений, охраняемых единым комплексом уголовно-правовых норм. Под родовым объектом иногда понимается определенная сфера общественных отношений, которая включает в себя социальные ценности, блага и интересы. Родовой объект лежит в основе деления УК РФ на разделы, одним из которых является «Общественная безопасность и общественный порядок» (раздел IX УК РФ), содержащий в себе вид (группу) преступлений против безопасности компьютерной информации (гл. 28 УК РФ).  Законодатель, расположив главу 28 в разделе IX УК РФ, фактически признал, что родовым объектом изучаемых нами в настоящем исследовании преступлений следует рассматривать общественную безопасность и общественный порядок. Такого мнения (с некоторой конкретизацией) придерживаются А. В. Наумов, Т. М. Лопатина, В. Г. Степанов-Егиянц, А. И. Коробеев, А. С. Червоткин, Д. М. Молчанов и другие ученые165.  На наш взгляд, если на период принятия УК РФ в 1996 г. такой вывод был достаточно обоснован, то сейчас такое положение не в полной мере отражает сущность изучаемого нами явления. Так, в одном разделе каждая из глав должна образовывать единое целое. Однако группа рассматриваемых нами преступлений (гл. 28 УК РФ) качественно выделяется среди других преступлений против общественной безопасности и общественного порядка. Существующее законодательное положение не учитывает активное проникновение информационных отношений во все сферы общественных отношений. Именно поэтому вышеуказанный подход к определению родового объекта преступлений против безопасности компьютерной информации представляется уязвимым. В связи с этим полагаем необходимым пересмотреть такой подход к его оценке.  Нам близка точка зрения Д. А. Калмыкова, который в своей работе обосновал не только существование в действующем Уголовном кодексе объекта уголовно-правовой охраны в виде информационной безопасности, выявил его распространенность наряду с другими объектами уголовно-правовой охраны, но и пришел к выводу, что «преступное посягательство на любой объект уголовно -правовой охраны с точки зрения формальной логики (в самом общем смысле) означает, в том числе, и нарушение информационного компонента соответствующего объекта»166. Однако, как нам представляется, Д. А. Калмыков не рассматривает информационную безопасность ни в качестве родового объекта преступлений, ни в качестве группового объекта. Так, в качестве родового объекта преступлений, расположенных в гл. 28 УК РФ, исходя из теории о четырехзвенной структуры объекта преступления, которой придерживается автор, им признается совокупность всех охраняемых уголовным законом общественных отношений в области компьютерной информации, а группового - общественная безопасность и общественный порядок в области информационных отношений167. Другие ученые также признают наличие такого объекта уголовно-правовой охраны в виде информационной безопасности168.  Представление об информационной безопасности как родовом объекте уголовно-правовой охраны, на наш взгляд, предполагает отнесение к ним преступлений, посягающих на информационную сферу Российской Федерации. Следовательно, в структуре УК РФ необходимо выделить раздел «Преступления против информационной безопасности». До этого времени в действующем уголовном законодательстве преступления против информационной безопасности характеризуются, как представляется, наличием дополнительного объекта уголовно-правовой охраны в виде безопасности информационной сферы.  При этом под информационной сферой следует понимать общественные отношения, заключающие в себе совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети Интернет, сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений169.  Информационная безопасность рассматривается как составляющая национальной безопасности Российской Федерации наряду с другими ее видами: государственной, общественной, экологической, экономической, транспортной, энергетической и безопасностью личности. Поэтому информационная безопасность России, охватывая все сферы человеческой жизнедеятельности, оказывает влияние на обороноспособность страны, государственную и общественную безопасность, экономический рост, развитие науки, технологии и образования, качество здравоохранения, в том числе и экологию. Это значит, что информационная безопасность проявляется себя не только как один из видов безопасности, но и как срез экономической, социальной, политической, военной, духовно-культурной и иных видов безопасности, т.е. тех видов безопасности, в которых информационные процессы занимают существенное место. Выявление признаков объективной стороны названных составов преступлений и деяний в процессе их квалификации На наш взгляд, не следует признавать общественно опасным копирование информации в пределах одной компьютерной техники. Так, правоприменителем в качестве уничтожения, модификации и копирования квалифицировано создание зашифрованного архива, копирование папок и файлов в пределах одного магнитного жесткого диска и удаление системных файлов администратора с сервера274.  Под несанкционированным уничтожением, блокированием, модификацией, копированием компьютерной информации (ст. 273 УК РФ) следует понимать действия, осуществляемые вопреки воле других лиц, которые не могут ими управляться, контролироваться, т.е. в отсутствии их разрешения и уведомления.  Поэтому для признания деяния преступным важно учитывать характер отношений правообладателя информации с лицом, осуществляющим посягательство на компьютерную информацию. Это позволяет отличать уголовно-наказуемое деяние от правомерных действий лиц. Такими лицами могут быть специалисты антивирусных компаний или специальных служб, разрабатывающие способы противодействия вредоносным компьютерным программам, выявляющие свойства и признаки таких компьютерных программ, или работники сервисных служб, обслуживающие компьютерную и периферийную техники. При ином толковании уголовного закона уголовной ответственности могли бы подлежать вышеуказанные лица.  В. Б. Вехов верно выделяет наиболее значимые признаки, которые позволяют определить характер несанкционированности действия компьютерной программы. Такая программа, по его мнению, не предполагает предварительного уведомления лица о характере действий и не запрашивает согласия у него на реализацию своего назначения275. К примеру, в качестве несанкционированного признаются действия по модификации программного обеспечения из демонстрационной версии в версию, использование которой возможно лишь при наличии лицензионного соглашения с правообладателем276.  Под нейтрализацией средств защиты компьютерной информации (ст. 273 УК РФ) следует понимать такое нарушение функционирования средств защиты компьютерной информации, при котором они прекращают выполнять свои функции. Некоторые исследователи считают нецелесообразным включение такого признака в конструкцию объективной стороны преступления по той причине, что он охватывается приготовительными действиями к неправомерному доступу к компьютерной информации277. Однако, исходя из представлений о стадиях совершения преступлений против безопасности компьютерной информации, каждое из деяний, описанных ст.ст. 273, 274, ч. 3 ст. 2741 УК РФ, может выступать в качестве приготовления к неправомерному доступу к компьютерной информации. Поэтому такое положение не должно служить основанием для исключения даже какого-то одного предусмотренного законом признака. В судебной практике под нейтрализацией средств защиты, например, признается возможность использовать программу без аппаратного ключа доступа278. Проблемы при квалификации преступлений с учетом рассматриваемого признака также встречаются. Так, в качестве нейтрализации средств защиты компьютерной информации возможно было признать созданную ВКП, которая обладала правами администратора операционной системы, что давало возможность активировать функцию защиты от удаления данного вредоносного программного обеспечения279. Однако правоприменителем такая квалификация не отражена.  Преступление, предусмотренное ч. 1 ст. 274 УК РФ, является оконченным при наступлении последствия в виде причинения крупного ущерба. Согласно прим. 2 к ст. 272 УК РФ, крупным ущербом признается ущерб, сумма которого превышает один миллион руб. Как справедливо отметил Московский городской суд, по делу, квалифицированному по ч. 1 ст. 274 УК РФ, законодатель не устанавливает критериев причиненного ущерба, за исключением его размера, – суммы, превышающий один миллион руб., тем самым, отнеся его к категории оценочных понятий, зависящих и подлежащих определению в каждом отдельном конкретном случае как потерпевшим, так и уполномоченными на то участниками уголовного судопроизводства с учетом всех обстоятельств дела. Ущерб может быть причинен моральный, материальный, деловой репутации. К ущербу могут быть также отнесены вынужденные финансовые потери и затраты на восстановление рабочего состояния средств хранения, обработки или передачи охраняемой информации280. Например, Лефортовским районным судом г. Москвы установлено, что своими действиями А. причинил крупный ущерб ООО «Приват Трэйд» на общую сумму 1 155 600 руб.281.  Причинение вреда КИИ РФ является последствие деяния, ответственность за которое предусмотрено ч. 2 ст. 2741 УК РФ. Вред может наступать в результате уничтожения, блокирования, модификации, копирования, распространения компьютерной информации, содержащейся в КИИ РФ. Если неправомерный доступ к охраняемой компьютерной информации, содержащейся в КИИ РФ, повлекший уничтожения, блокирования, модификации, копирования, не приводит к причинению вреда КИИ РФ, то деяние следует квалифицировать по ч. 1 ст. 272 УК РФ. Особенности квалификации преступлений против безопасности компьютерной информации, совершенных в соучастии Статья 32 УК РФ содержит понятие соучастия, согласно которому им признается умышленное совместное участие двух или более лиц в совершении умышленного преступления.  Понятие содержит в себе субъективные и объективные признаки соучастия в преступлении. Субъективными признаками соучастия являются умышленный характер деятельности соучастников, возможность совершения в соучастии только умышленного преступления, взаимная осведомленность каждого из участников. Объективными признаками соучастия являются участие в деятельности двух или более лиц, наличие вклада (физического или интеллектуального) в преступную деятельность каждого из участников (совместность деятельности).  Определение видов и форм совместного участия в преступной деятельности непосредственно связано с квалификацией преступлений. Как справедливо отмечается в литературе, установление вида соучастника способствует установлению его роли в ходе подготовки и совершения конкретного преступления376 . В качестве видов соучастников в преступлении наряду с исполнителем, в ч. 1 ст. 33 УК РФ законодатель выделяет организатора, пособника и подстрекателя.  Установленные уголовным законом в ст. 33 УК РФ правила квалификации преступлений, совершаемых лицами с распределением ролей, предписывают ссылаться правоприменителю в принимаемом акте не только на пункт, часть и статью Особенной части УК РФ, по которой деяния квалифицируется, но и в зависимости от роли такого лица на соответствующую часть статьи 33 УК РФ. Такая особенность связана с тем, что при сложном соучастии (с распределением ролей) лицо не выполняет объективную сторону преступления. Поэтому исключением из этого правила являются случаи, когда организатор, подстрекатель или пособник является одновременно соисполнителем преступления377.  Характерные способы совершения преступления в виде форм соучастия находят отражение в ст. 35 УК РФ, которая делит их на совершение преступления группой лиц, группой лиц по предварительному сговору, организованной группой, преступным сообществом (преступной организацией). Выделение форм соучастия в виде организованной группы и преступного сообщества (преступной организации) в науке дискуссионен. С. А. Балеев убедительно доказывает, что соучастие в преступлении в форме преступного сообщества (преступной организации) не является одним из видов форм соучастия по той причине, что целью такого вида совместной преступной деятельности является не совершение единичного преступления, а организованная преступная деятельность378.  Форму соучастия в виде совершения преступления группой лиц без предварительного сговора законодатель, а также разновидность стечения лиц в одном преступлении в виде организованной группы, законодатель не указывает в качестве квалифицирующих основные составы преступлений против безопасности компьютерной информации.  В судебной практике имеются случаи квалификации действий лиц, совершивших преступления против безопасности компьютерной информации, преступным сообществом (преступной организацией). Как справедливо отмечает С. А. Балеев, возможность совершения преступления преступным сообществом (преступной организацией) не предусматривается в качестве квалифицирующего ни в одной статье Особенной части УК379. Поэтому такие действия находят отражение в квалификации как совокупности компьютерных преступлений со ст. 210 УК РФ с учетом позиции Пленума Верховного Суда РФ, изложенной в постановлении от 10.06.2010 г. № 12 «О судебной практике рассмотрения уголовных дел об организации преступного сообщества (преступной организации) или участии в нем (ней)»380.  Так, Замоскворецким районным судом г. Москвы действия подсудимых Б., К., Пал., Поп., Г., Ф. квалифицированы по ч. 2 ст. 210 УК РФ (в ред. Федерального закона от 27.12.2009 № 377-ФЗ) как участие в преступном сообществе (преступной организации) в целях совместного совершения тяжких преступлений. Судом было отмечено, что указанное преступное сообщество (преступная организация) характеризуется устойчивостью, сплоченностью, единым умыслом ее участников, длительностью противоправной деятельности, а также отработанной системой совершения преступлений и масштабностью преступной деятельности, затронувшей территорию ряда субъектов Российской Федерации. Кроме этого, данное преступное сообщество (преступная организация) характеризуется знаниями о вредоносном программном обеспечении и его назначении, правилах и порядке его установки и способах модификации, механизма регистрации собственного веб-ресурса и порядка его администрирования, а также использованием полученных навыков работы с вредоносным программным обеспечением в дальнейшей преступной деятельности по хищению денежных средств. Получаемый от этой преступной деятельности доход использовался участниками преступной организации в качестве основного источника существования и обогащения3  Повышенная опасность совместного совершения рассматриваемых преступлений при различных групповых формах соучастия отражается также в квалифицированных и особо квалифицированных признаках составах этих преступлений. Признаки совершения преступления группой лиц по предварительному сговору и организованной группой являются квалифицирующими преступления, ответственность за которые предусмотрена ч. 1 ст. 272, ч. 1 ст. 273 УК РФ, ч.ч. 1-3 ст. 2741 УК РФ.  Из статистических сведений следует, что доля лиц, совершивших преступления группой лиц, среди лиц, осужденных по гл. 28 УК РФ, в 2013-2016 гг. стабильна и не превышает 6% (см. Приложение 8).  Определение совершения преступления группой лиц по предварительному сговору дается в ч. 2 ст. 35 УК РФ, согласно которому таким преступлением признается, если в нем участвовали лица, заранее договорившиеся о совместном совершении этого преступления. «Заранее» означает предварительную договоренность между лицами о совершении преступления, т.е. до начала выполнения действий неправомерного доступа (ч. 2 ст. 272 УК РФ), создания, распространения или использования ВКП либо иной компьютерной информации подобного рода(ч. 2 ст. 273 УК РФ), неправомерного воздействия на КИИ РФ (ч.1-3 ст. 2741 УК РФ).  В групповых преступлениях умыслом каждого из соучастников должны охватываться определенные в законе последствия: уничтожение, блокирование, модификация либо копирование компьютерной информации (ч. 2 ст. 272 УК РФ) или возможность причинение вреда КИИ РФ (ч. 2-3 ст. 2741 УК РФ), либо осознанность или понимание предназначенности, используемых ВКП или иной компьютерной информации подобного рода для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации (ч. 2 ст. 273 УК РФ) или неправомерного воздействия на КИИ РФ (ч. 1 ст. 2741 УК РФ). | |  | |  | | |  | | |  |
|  |  |