**Юсько Алина**

Магистрант

**Направление:** Юриспруденция

**Магистерская программа:** Уголовное право, криминология, уголовно-исполнительное право

# Проблемы квалификации неправомерного доступа к компьютерной информации

**Аннотация.** В статье раскрывается содержание объективных и субъективных признаков преступлений в сфере компьютерной информации, регламентируемых гл. 28 Уголовного кодекса РФ. Рассмотрены некоторые особенности квалификации и основания освобождении от уголовной ответственности за совершение общественно опасных деяний, предусмотренных ст. 272 УК РФ «Неправомерный доступ к компьютерной информации».

**Ключевые слова:** неправомерный доступ, компьютерная информация, преступление, компьютер.



Уголовный кодекс Российской Федерации в 28 главе содержит нормы, которые предусматривают уголовную ответственность за преступления в сфере компьютерной информации [7, с. 270]. Данная глава появилась в УК РФ в связи с кардинальным преобразованием в стране общественных отношений и появлением открытого информационного общества. Преступления в сфере компьютерной информации общественно опасны в связи с тем, что компьютеры и другие современные устройства и данные, которые они накапливают и передают, затрагивают все сферы жизнедеятельности современного общества. Преступные вмешательства в компьютерную информацию могут помешать осуществлению банковских операций, социальному обеспечению, оборонной способности, транспортной

инфраструктуры и даже национальной безопасности. В связи с этим уголовное законодательство защищает законные процессы сбора, обработки, накопления, хранения, поиска, распространения (передачи) информации.

Под компьютерной техникой понимаются как традиционные персональные компьютеры и ноутбуки, так и планшеты, смартфоны, кассовые аппараты, банкоматы, терминалы по приему платежей и другие устройства, оперирующие с компьютерной информацией [1, с. 183].

Операции с любой информацией, включая компьютерную считаются законными, если есть согласие и допуск со стороны собственника либо оператора, соблюдены требования к обработке и передаче данных и к эксплуатации компьютеров, их систем и сетей.

В соответствии с разд. IX УК РФ родовым объектом преступлений в сфере компьютерной информации является совокупность общественных отношений, которые направлены на охрану общественной безопасности и общественного порядка. Видовым объектом в свою очередь выступают общественные отношения, которые возникают в процессе создания любых видов воздействия на компьютерную информацию.

Понятие «компьютерная информация» не регламентировано ни одним специальным нормативным актом и законодательно определено лишь в примечании к ст. 272 УК РФ, где указывается, что это сведения (сообщения, данные), которые представлены в форме электрических сигналов, независимо от средств их хранения, обработки и передачи [6, с. 33]. Очевидно, что это определение является производным от общего понятия информации, которое содержится в Федеральном законе РФ «Об информации, информационных технологиях и о защите информации».

Непосредственным объектом преступления, регламентированного ст. 272 УК РФ «Неправомерный доступ к компьютерной информации» являются общественные отношения, которые обеспечивают безопасность и правомерное использование компьютерной информации. В свою очередь дополнительным объектом могут выступить отношения, обеспечивающие сохранность

соответствующего вида тайны (налоговой, коммерческой, банковской), а факультативным объектом – отношения, охраняющие собственность или интересы государственной службы и службы в коммерческих организациях. Предметом же данного преступления является охраняемая законом компьютерная информация.

Согласно Федеральному закону РФ «Об информации, информационных технологиях и о защите информации» информация может свободно использоваться любым лицом и передаваться одним лицом другому лицу, при условии, что федеральными законами не установлены ограничения доступа к информации или другие требования к порядку ее предоставления либо распространения [4, с. 33].

Порядок и условия доступа к информации, правила ее использования (в том числе путем распространения) и передачи определяет обладатель такой информации. Также обладатель и устанавливает ограничения либо дает разрешение на осуществление каких-либо действий с информаций, а в случае незаконного ее получения либо использования другими лицами вправе обратиться в соответствующие органы для защиты своих интересов.

Доступом к компьютерной информации называется возможность получения информации и ее использования, т. е. любая форма проникновения в источник информации с использованием средств (вещественных и интеллектуальных) в виде электрических сигналов, позволяющая манипулировать полученной информацией (копировать, модифицировать, блокировать либо уничтожать ее) [3].

Неправомерным становится доступ, который осуществляется без разрешения ее законного владельца и в нарушение порядка, который установлен законодательством. Владелец может установить ограничения доступа посредством правовых, организационных, технических мер либо другим способом. Следовательно, неправомерным можно считать доступ к конфиденциальной информации или информации, которая составляет государственную тайну, лица, не обладающего необходимыми полномочиями

(без согласия собственника или его законного представителя), при условии обеспечения специальных средств ее защиты [5].

Уничтожением информации, как общественно опасным последствием, понимается приведение ее или ее части в непригодное для использования состояние независимо от возможности ее восстановления. Однако обыкновенное переименование файла, а также автоматическая замена старой версии файлов новой уничтожением информации не считается. В свою очередь перенос информации на другой носитель уничтожением компьютерной информации не будет являться лишь в том случае, если в результате этих действий доступ правомерных пользователей к информации не затруднен либо исключен.

Блокированием информации называется результат такого воздействия, последствием которого является постоянное либо временное отсутствие возможности осуществлять над компьютерной информацией операции. Блокирование приводит к ограничению или полному прекращению доступа к компьютерному оборудованию и находящимся на нем ресурсам, не связанному с уничтожением компьютерной информацией.

Модификацией информации является ее изменение либо изменение ее параметров. Модификация считается легальной и не влечет ответственности, если она осуществляется законным владельцем или пользователем информации с целью исправления ошибок, обеспечения функционирования программы, базы данных на каком-либо устройстве либо для налаживания взаимодействия нескольких программ.

Копированием информации называется перенос ее на другое обособленное устройство (носитель) при сохранении неизменной первоначальной версии, а также воспроизведение информации в любой материальной форме путем переписывания от руки, фотографирования, а также считывания (перехвата).

Между деянием и перечисленными последствиями должна присутствовать причинно-следственная связь. Важно установить, что причиной

стали целенаправленные действия, а не технические неисправности и ошибки в работе программного обеспечения. Для признания преступления оконченным достаточно наступления хотя бы одного из перечисленных в диспозиции статьи последствий. Наличие совокупности нескольких последствий на квалификацию не влияет [2, с. 56].

Неправомерный доступ может состоять в модификации программ, от которых зависит функционирование каких-либо сайтов в сети Интернет и демонстрация на них информации, в том числе рекламного, оскорбительного или порнографического характера.

Большинство исследователей считает, что субъективная сторона преступления характеризуется умышленной формой вины. Виновный осознает общественную опасность деяния в виде неправомерного доступа, предвидит возможность или неизбежность наступления последствий в виде уничтожения, блокирования, модификации либо копирования информации и либо желает наступления этих последствий, либо не желает, но сознательно допускает их наступление или относится к их наступлению безразлично.

Субъект данного преступления общий – физическое вменяемое лицо, достигшее 16-летнего возраста. Законодательством установлена повышенная ответственность, если помимо обозначенных в ч. 1 ст. 272 УК РФ последствий был причинен крупный ущерб (превышает один миллион рублей) или деяние было совершено из корыстной заинтересованности.

В части 3 ст. 272 УК РФ предусмотрена ответственность за совершение анализируемого преступления группой лиц по предварительному сговору, организованной группой либо лицом с использованием своего служебного положения. Для квалификации по указанной части достаточно одного из перечисленных признаков [2, с. 57]. Неправомерный доступ будет считаться совершенным группой лиц по предварительному сговору, если в его осуществлении участвовали два или более исполнителей, предварительно договорившихся о совместном совершении преступления.

В силу того, что преступления, предусмотренные ч. 1-3 ст. 272 УК РФ, относятся к категории небольшой и средней тяжести, виновный может быть освобожден от уголовной ответственности в связи с деятельным раскаянием, в связи с примирением с потерпевшим или с назначением судебного штрафа. Однако необходимо учитывать, что в соответствии с п. 25.5 постановления Пленума Верховного Суда РФ «О применении судами законодательства, регламентирующего основания и порядок освобождения от уголовной ответственности» судья принимает решение об удовлетворении ходатайства о прекращении уголовного дела и назначении меры уголовно-правового характера в виде судебного штрафа при отсутствии обстоятельств, препятствующих освобождению лица от уголовной ответственности.

**Литература**

1. Казакова В.А., Кораблева С.Ю. Уголовное право Российской Федерации. Общая и Особенная части: учебник. М.: Юстиция, 2021.

2. Квалификация преступлений: Учебное пособие / Под ред. О.С. Капинус. М.: Юрайт, 2020.

3. Комментарий к Уголовному кодексу Российской Федерации (постатейный). Последняя актуальная редакция от 01.07.2021 [Электронный ресурс] // Режим доступа: http://ukrfinfo.ru/comms/ (дата обращения: 17.12.2021).

4. Корабельников С.М. Преступления в сфере информационной безопасности: Учебное пособие. М.: Юрайт, 2020.

5. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации (утв. Генпрокуратурой России) [Электронный ресурс] // Режим доступа: https://www.garant.ru/products/ipo/prime/doc/70542118/#review (дата обращения: 17.12.2021).

6. Попов А.Н. Преступления в сфере компьютерной информации: Учебное пособие. СПб.: Санкт-Петербургский юридический институт (филиал) Университета прокуратуры Российской Федерации, 2020.

7. Уголовное право. Особенная часть: Учебник / Под ред. В.Б. Боровикова. М.: Юрайт, 2020.