Ст.272 УК РФ
Неправомерный доступ к компьютерной информации

Выполнил: Браславский Никита

Статья 272 УК предусматривает ответственность за неправомерный доступ к компьютерной информации (информации на машинном носителе, в ЭВМ или сети ЭВМ), если это повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы вычислительных систем.

Данная статья защищает право владельца на неприкосновенность информации в системе. Владельцем информационной вычислительной системы может быть любое лицо, правомерно пользующееся услугами по обработке информации как собственник вычислительной системы (ЭВМ, сети ЭВМ) или как лицо, приобретшее право использования компьютера.

Данное неправомерное деяние наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

То же деяние, совершенное **группой лиц** по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, - наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

Режим доступа к конфиденциальной информации может быть установлен как ее собственником, так и непосредственно в соответствии с действующим законодательством. Исчерпывающий Перечень сведений конфиденциального характера определены в Указе Президента РФ от 6 марта 1997 г. N 188 "Об утверждении Перечня сведений конфиденциального характера": а) персональные данные; б) сведения, составляющие тайну следствия и судопроизводства; в) служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с ГК РФ и федеральными законами (служебная тайна); г) сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и иными федеральными законами (врачебная, нотариальная и адвокатская тайны, тайны переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и др.); д) сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с ГК РФ и иными федеральными; е) сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них .

Неправомерным является доступ, если лицо не имеет права на доступ к данной информации, либо имеет право на доступ, но осуществляет его помимо установленного порядка.

Важным является наличие причинной связи между несанкционированным доступом и наступлением предусмотренных статьей 272 последствий, поэтому простое временное совпадение момента сбоя в компьютерной системе, которое может быть вызвано неисправностями или программными ошибками, и неправомерного доступа не влечет уголовной ответственности.

Состав данного преступления имеет материальный характер и предполагает обязательное наступление одного из следующих последствий:

1. уничтожения информации — удаление информации на материальном носителе и невозможность ее восстановления на нем;
2. блокирования информации — совершение действий, приводящих к ограничению или закрытию доступа к компьютерной системе и предоставляемым ею информационным ресурсам;
3. модификации информации — внесение изменений в программы, базы данных, текстовую информацию, находящуюся на материальном носителе;
4. копирования информации — перенос информации на другой материальный носитель, при сохранении неизмененной первоначальной информации;
5. нарушения работы ЭВМ, системы ЭВМ или их сети — нарушение работы как отдельных программ, баз данных, выдача искаженной информации, так и при нештатном функционировании аппаратных средств и периферийных устройств, либо нарушении нормального функционирования сети.

Объектом неправомерного доступа к компьютерной информации, как преступления являются права на информацию ее владельца и третьих лиц. По делам о данном преступлении должно быть установлено, что компьютерная информация, к которой осуществлен доступ, *охраняется законодательством* о государственной тайне, о собственности, об авторском праве или др. Под охраной закона находятся также частная жизнь человека, коммерческая тайна, тайна сообщений.

Объективную сторону данного преступления составляет неправомерный доступ к охраняемой законом компьютерной информации, который всегда связан с совершением определенных действии и может выражаться в проникновении в компьютерную систему путем:
использования специальных технических или программных средств, позволяющих преодолеть установленные системы защиты, незаконного использования действующих паролей или кодов для проникновения в компьютер либо совершение иных действий в целях проникновения в систему или сеть под видом законного пользователя, хищения носителей информации, при условии, что были приняты меры к их охране, если это деяние повлекло уничтожение или блокирование информации.

Субъективная сторона данного преступления характеризуется только прямым умыслом. В случае, если в результате неправомерного доступа к системе ЭВМ, управляющей процессами, связанными с повышенной опасностью (например, система управления атомной станцией), в результате уничтожения, блокирования, модифицирования информации была нарушена работа реактора, что привело к тяжким последствиям, даже если наступление этих последствий не охватывалось умыслом лица, уголовная ответственность за такие последствия наступает и тогда, когда лицо предвидело возможность наступления последствий, но, без достаточных к тому оснований, самонадеянно рассчитывало на их предотвращение, или в случае, если лицо не предвидело, но должно было и могло предвидеть возможность наступления этих последствий.

Субъект

По общему правилу субъектом может быть лицо, достигшее шестнадцатилетнего возраста. Однако ч. 2 ст. 272 УК предусматривает наличие специального субъекта, совершившего данное преступление с использованием своего служебного положения, а равно лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети. Под доступом в данном случае понимается фактическая возможность использовать ЭВМ, при отсутствии права на работу с защищенной информацией. Например, инженер по ремонту компьютерной техники имеет доступ к ЭВМ в силу своих служебных обязанностей, но вносить какие-либо изменения в информацию, находящуюся в памяти ЭВМ, не имеет права.