**Уголовная ответственность за неправомерный доступ к компьютерной информации**

Статьей 272 УК РФ предусмотрена уголовная ответственность за  неправомерный доступ к компьютерной информации.

Непосредственным объектом преступления является право владельца компьютерной системы на неприкосновенность содержащейся в ней информации.

Объективная сторона данного преступления состоит в неправомерном доступе к охраняемой законом компьютерной информации, т.е. к информации на машинном носителе , в ЭВМ, системе ЭВМ или их сети, если это деяние повлекло уничтожение. Блокирование, модификацию, либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети.

Под информацией в данном случае понимаются сведения о лицах, предметах, фактах, событиях, явлениях и процессах, содержащиеся в информационных системах. Эта информация должна быть чужой для осуществляющего неправомерный доступ лица и защищенной от произвольного копирования.

"Доступ" к охраняемой законом компьютерной информации - это приобретение и использование лицом возможности получать информацию, вводить ее либо влиять на процесс обработки информации.   
"Неправомерным" следует считать такой доступ, когда лицо действует без разрешения владельца этой системы или сети или другого законного полномочия.

Обязательным признаком объективной стороны этого преступления является наступление вредных последствий для собственника или хранителя информации в виде уничтожения, блокирования, модификации либо копирования информации, нарушения работы ЭВМ, системы ЭВМ или их сети. Это означает, что сам по себе просмотр информации, хранящейся в оперативной памяти компьютера или на машинном носителе (дискете, CD-R диске), состава преступления не образует.

Под уничтожением информации понимается не простое удаление файлов, а только такое, которое приведет к невозможности их восстановления.  
Модификация информации - существенное ее видоизменение, совершенное без согласия собственника информации и затрудняющее законное пользование ею.

Блокирование информации - это создание препятствий к свободному ее использованию при сохранности самой информации.  
Нарушение работы ЭВМ, системы ЭВМ или их сети имеет место в случае, если компьютерная система не выполняет своих функций, выполняет их не должным образом или в случае заметного уменьшения производительности системы. Между действиями и последствиями обязательно должна быть установлена причинная связь.

Вопрос о том, когда окончено данное деяние, должен решаться так - моментом его окончания является момент отсылки пользователем последней интерфейсовой команды вызова хранящейся информации, независимо от наступления дальнейших последствий. Однако преступлением это деяние станет лишь при наличии последнего условия. При ненаступлении указанных последствий, все совершенные до этого действия будут подпадать под признаки неоконченного преступления.

Субъективная сторона преступления характеризуется виной в форме умысла: лицо сознает, что осуществляет неправомерный (несанкционированный) доступ к охраняемой законом компьютерной информации, предвидит, что в результате производимых им действий могут наступить или неизбежно наступят указанные в законе вредные последствия, и желает (прямой умысел) или сознательно допускает (косвенный умысел) их наступления либо относится к ним безразлично.

Мотивы и цели этого преступления могут быть разными: корыстный мотив, желание получить какую-либо информацию либо желание причинить вред. Мотив и цель не являются признаками состава данного преступления и не влияют на квалификацию.

Субъект - лицо, достигшее 16-летнего возраста.  
Квалифицирущие признаки:

1. совершение данного преступления группой лиц по предварительному сговору;

2. совершение данного преступления организованной группой;

3. совершение данного преступления лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети.

Если описание первых двух признаков дано в ст. 35 УК, то специальный субъект двух последних можно трактовать как отдельных должностных лиц, программистов, операторов ЭВМ, наладчиков оборудования, специалистов-пользователей специализированных рабочих мест и т.д.

Лицом, «имеющим доступ к ЭВМ, системе ЭВМ или их сети» является как лицо, которому в силу разрешения владельца системы или служебного полномочия разрешено получать информацию в компьютерной системе, вводить ее или производить с ней операции, так и лицо, осуществляющее техническое обслуживание компьютерного оборудования и на иных законных основаниях имеющее допуск к компьютерной системе. Лицо, имеющее допуск к компьютерной системе может совершить это преступление лишь в случае доступа к информации, допуска к которой оно не имеет. В случае, когда существенный вред причиняется действиями лица имеющего правомерный доступ имеющее допуск к компьютерной информации, ответственность наступает по ст. 274 УК РФ.