**Лекция на тему: «Преступления в сфере компьютерной информации»**

Развитие современного общества, основанного на использовании огромного количества самой разнообразной информации, немыслимо без широкого внедрения в управленческий процесс и многие другие сферы электронно-вычислительной техники. Она служит не только для хранения и обработки соответствующей информации на уровне органов государственной власти и местного самоуправления или коммерческих организаций и используется как средство связи и коммуникации между гражданами, но и является одним из важнейших элементов в обеспечении внутренней и внешней безопасности государства. Все это обуславливает разработку правовых норм, обеспечивающих регулирование общественных отношений, которые связаны с использованием компьютерной техники.

В этой связи следует упомянуть Закон РФ от 23 сентября 1992 года «О правовой охране программ для электронно-вычислительных машин и баз данных», Федеральные законы от 20 февраля 1995 года «Об информации, информатизации и защите информации» и от 10 января 2002 года «Об электронной цифровой подписи». Определенную роль в этом играют и нормы главы 28 УК РФ «Преступления в сфере компьютерной информации».

Согласно УК РФ преступлениями в сфере компьютерной информации являются: неправомерный доступ к компьютерной информации (ст. 272 УК РФ); создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК РФ); нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК РФ). Указанные преступления представляют собой общественно опасные деяния, посягающие на безопасность информации и систем обработки информации с использованием ЭВМ. Это означает, что преступные деяния, совершаемые с помощью электронно-вычислительной техники, статьями главы 28 УК РФ не охватываются и подлежат квалификации как самостоятельные посягательства (например, в качестве преступления против собственности - мошенничества, как преступление против основ конституционного строя и безопасности государства - шпионаж).

Физическое повреждение или уничтожение компьютерной техники, незаконное завладение ПЭВМ или ее компонентами, а равно машинными носителями информации (дискетами, CD-R дисками, электронными «накопителями») как предметами, обладающим материальной ценностью, квалифицируются в качестве посягательства на чужую собственность по статьям главы 21 УК РФ. Преступления в сфере компьютерной информации сопряжены с посягательством на иной своеобразный предмет - информацию, сосредоточенную внутри компьютера (в файлах, программах или базах данных).

Объективная сторона рассматриваемых преступлений по общему правилу представляет собой деяние в форме действия. Бездействие возможно только как несоблюдение установленных правил эксплуатации ЭВМ, систем или сетей ЭВМ (ст. 274 УК РФ). Особенностью конструкции составов этих преступлений является то, что преимущественно они сконструированы по типу материальных - предполагают наступление общественно опасных последствий в виде вреда для пользователей ЭВМ. Согласно уголовному закону этот вред состоит в нарушении нормального функционирования ЭВМ или сетей ЭВМ.

Субъектом преступлений в сфере компьютерной информации могут быть не только лица, в обязанности которых входит соблюдение правил хранения и обработки информации либо иных правил безопасности информационных систем (специальный субъект), но и любые иные лица, противоправно получившие доступ к информации с помощью персонального компьютера, а также создавшие, использовавшие или распространившие вредоносные программы для ЭВМ.

Бывают следующие виды преступлений в сфере компьютерной информации:

1. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ).

Объективная сторона преступления состоит в неправомерном доступе к охраняемой законом компьютерной информации, т. е. информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети.

Процесс неправомерного доступа к такой информации непременно сопряжен с «взломом» систем защиты ЭВМ, однако при этом повреждения защитных электронных компонентов не требуется.

Способы получения такого доступа различны: с использованием чужого имени (пароля), изменением физических адресов технических устройств, модификацией программного и информационного обеспечения и др.

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, систем ЭВМ или их сети. Это означает, что сам по себе просмотр информации, хранящейся в оперативной памяти компьютера или на машинном носителе (гибком диске - дискете, CD-R диске), состава преступления не образует. Необходимо, по крайней мере, внесение изменений в соответствующие файлы (каталоги) или создание на базе имеющихся новых каталогов, затрудняющих законному пользователю информации доступ к ней, т. е. вызывающих уничтожение, блокирование информации или нарушение работы ЭВМ (систем ЭВМ, их сети) (последствия преступления).

Под уничтожением информации понимается не простое удаление файлов, а только такое, которое приведет к невозможности их восстановления. Модификация информации также понимается как существенное ее видоизменение, затрудняющее законное пользование ею.

Нарушение работы ЭВМ (систем ЭВМ, их сети) включает в себя сбои в работе машины, выведение на дисплей неверной информации, отказ в выдаче информации, отключение элементов компьютерной системы (серверов, модемов и т. д.).

При ненаступлении указанных вредных последствий состав рассматриваемого преступления отсутствует, даже если состоялся доступ к весьма конфиденциальной (в том числе и государственно значимой) информации.

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

Субъект - лицо, достигшее возраста 16 лет.

Квалифицированный состав данного преступления образует неправомерный доступ к компьютерной информации, совершенный 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.

Групповой способ совершения преступления будет налицо, если предварительный сговор имел место между лицами, которые совместными усилиями непосредственно обеспечили неправомерное проникновение в память компьютера или сеть ЭВМ. Понятие организованной группы в данном случае ничем не отличается от традиционного (ч. 3 ст. 35 УК РФ).

Лицо, использующее свое служебное положение или имеющее доступ к ЭВМ, системе ЭВМ или компьютерной сети, - это законный пользователь информации, как непосредственно работающий в режиме

пользования или обработки баз данных, так и по роду своей деятельности имеющий право временно эксплуатировать ЭВМ или знакомиться с хранящейся в них информацией.

1. Создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК РФ).

Объективную сторону этого преступления образуют несколько самостоятельных действий: 1) создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети; 2) использование таких программ; 3) распространение таких программ или машинных носителей с такими программами.

Состав преступления формальный, так как способность уничтожать, блокировать, модифицировать информацию и т. д. характеризует не общественно опасные последствия деяния, а сами по себе создаваемые или видоизменяемые программы (их свойства). Фактически деяние в данном случае выражается в разработке так называемых «вирусных» программ, т. е. таких, которые способны выполнять деструктивную функцию - стереть файл, зашифровать или сделать его недоступным для пользователя, полностью уничтожить информацию, содержащуюся в оперативной памяти компьютера, и т. д. Наступление реальных последствий в виде уничтожения, блокирования, модификации либо копирования информации, нарушения работы ЭВМ пользователями вредоносных программ не требуется.

Использование «вирусных» программ означает их установку (введение в память компьютера) в процессе технического обслуживания ЭВМ, обмена программами и др.

Распространением программ такого рода признается любая форма их реализации - как на коммерческой, так и на иной основе, как с обозначением сущности программы, так и без этого, путем, как дублирования, так и реализации отдельных машинных носителей (флоппи-дисков, CD-R дисков) либо посредством модема или передачи по компьютерной сети.

Окончено преступление с момента создания программы-«вируса» либо ее использования или распространения.

Субъективная сторона преступления характеризуется прямым умыслом.

Субъект преступления - лицо, достигшее возраста 16 лет.

Квалифицированный состав преступления налицо при наступлении в результате совершения деяний, предусмотренных ч. 1 ст. 273 УК РФ, по неосторожности тяжких последствий. Под таковыми следует понимать крупный материальный или моральный ущерб пользователям ЭВМ, дезорганизацию деятельности государственного органа, коммерческой организации или учреждения, аварию, катастрофу и др.

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст.274 УК РФ).

Объективная сторона преступления заключается в нарушении установленных правил эксплуатации ЭВМ, системы ЭВМ или их сети, если это повлекло причинение существенного вреда (материальный состав).

Фактически это выражается в несоблюдении или прямом игнорировании определенных правил, обеспечивающих безопасность компьютерной системы или сети (например, требования о проверке посторонних машинных носителей информации на наличие «вирусов», регулярном обновлении используемых «антивирусных» программ).

Существенный вред - оценочное понятие, которым охватывается как материальный, так и иной (например, моральный) вред. Он должен быть прямым следствием уничтожения, блокирования или модификации охраняемой законом информации ЭВМ, происходящих по вине пользователя.

Субъективная сторона преступления характеризуется виной в форме умысла или неосторожности.

Однако если умышленная вина включает цель подрыва экономической безопасности и обороноспособности РФ, то при определенных обстоятельствах содеянное охватывается ст. 281 УК РФ (диверсия).

Субъект преступления специальный, т. е. лицо, имеющее доступ к ЭВМ, системе ЭВМ или их сети (законный пользователь).

Наступление тяжких последствий в результате совершения этого деяния охватывается ч. 2 ст. 274 УК РФ.

Помощник прокурора города А.А. Попов