Министерство общего и профессионального образования

Курганский государственный университет

# Кафедра уголовно-правовых дисциплин

Реферат на тему:

## Преступления в сфере компьютерной информации

Выполнил студент гр. 2040

Андреев А. Б.

Проверил: Осыченко К.А.

Курган, 2002

### Преступления в сфере компьютерной информации

Преступления в области компьютерной информации являются новеллой УК, однако динамика роста такова, что скоро они смогут начать соперничать с традиционными видами преступлений - по сравнению с 1998 г. количество зарегистрированных преступлений в 1999 г. увеличилось в 12 раз.

Компьютерная информация - в соответствии со ст. 2 Федерального закона от 20.02.95 N 24-ФЗ "Об информации, информатизации и защите информации" под информацией понимаются сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления, но применительно к комментируемым статьям под компьютерной информацией понимаются не сами сведения, а форма их представления в машиночитаемом виде, т.е. совокупность символов, зафиксированная в памяти компьютера, либо на машинном носителе (дискете, оптическом, магнитооптическом диске, магнитной ленте либо ином материальном носителе). При рассмотрении дел следует учитывать, что при определенных условиях и физические поля могут являться носителями информации.

Программа для ЭВМ - объективная форма представления совокупности данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств с целью получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения.

ЭВМ (компьютер) - устройство или система (несколько объединенных устройств), предназначенное для ввода, обработки и вывода информации. Сеть ЭВМ - совокупность компьютеров, средств и каналов связи, позволяющая использовать информационные и вычислительные ресурсы каждого компьютера, включенного в сеть, независимо от его места нахождения. База данных - это объективная форма представления и организации совокупности данных (например, статей, расчетов), систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью ЭВМ.

#### Неправомерный доступ к компьютерной информации

Объективную сторону данного преступления составляет неправомерный доступ к охраняемой законом компьютерной информации, который всегда связан с совершением определенных действий 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.

Неправомерным признается доступ к компьютерной информации лица, не обладающего правами на получение и работу с данной информацией либо компьютерной системой. Причем в отношении этой информации либо системы должны приниматься специальные меры защиты, ограничивающие круг лиц, имеющих к ней доступ. Неправомерный доступ к компьютерной информации является наиболее распространенным видом преступлений, связанных с компьютерной информацией.

Под охраняемой законом информацией понимается информация, для которой в специальных законах установлен специальный режим ее правовой защиты, например государственная, служебная и коммерческая тайна, персональные данные и т.д.

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

уничтожение информации - удаление информации или изменение ее параметров, повлекшее за собой невозможность использования данной информации, вне зависимости от возможности ее восстановления;

блокирование информации - совершение действий, приводящих к ограничению или закрытию доступа к компьютерной системе и предоставляемым ею информационным ресурсам;

модификация информации - внесение изменений в программы, базы данных, текстовую информацию, находящуюся на материальном носителе;

копирование информации - перенос информации на другой материальный носитель, при сохранении неизмененной первоначальной информации;

нарушение 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.

Важным является установление причинной связи между несанкционированным доступом и наступлением последствий. При функционировании сложных компьютерных систем возможны уничтожение, блокирование и нарушение работы ЭВМ в результате технических неисправностей или ошибок в программных средствах. В этом случае лицо, совершившее неправомерный доступ к компьютерной информации, не подлежит ответственности из-за отсутствия причинной связи между действиями и наступившими последствиями.

Данное преступление считается оконченным с момента наступления предусмотренных данной статьей последствий.

С субъективной стороны данное преступление может быть совершено только умышленно. Совершая неправомерный доступ к компьютерной информации, виновный осознает неправомерность своих действий, предвидит, что в результате его действий могут наступить предусмотренные в данной статье последствия, и желало либо сознательно допускало возможность их наступления. Совершение действий по неправомерному доступу к компьютерной информации предполагает наличие специальных знаний и опыта по работе с компьютерами, а сами современные компьютерные системы имеют достаточно высокий уровень программной защиты от случайных ошибок. В случае 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.

По общему правилу субъектом может быть лицо, достигшее 16-летнего 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.

**Создание, использование и распространение вредоносных программ для ЭВМ**

Под вредоносными программами в смысле ст. 273 УК понимаются программы, специально созданные для нарушения нормального функционирования компьютерных систем и программ. Под нормальным функционированием имеется в виду выполнение операций, для которых эти программы предназначены, что должно быть определено в документации на программу. Наиболее распространенные виды вредоносных программ: "компьютерные вирусы", "логические бомбы", "троянские кони", "черви" и т.д.

"Компьютерные вирусы" - это программы, которые умеют воспроизводить себя в нескольких экземплярах, модифицировать (изменять) программу, к которой они присоединились, и тем самым нарушать ее нормальное функционирование. "Логические бомбы" - умышленное изменение кода программы, частично или полностью выводящее из строя программу либо систему ЭВМ при определенных заранее условиях, например наступлении определенного времени. Принципиальное отличие "логических бомб" от "компьютерных вирусов" состоит в том, что они изначально являются частью программы и не переходят в другие программы, а "компьютерные вирусы" являются динамичными программами и могут распространяться даже по компьютерным сетям. "Троянские кони" - это специально разработанные вредоносные программы, с помощью которых можно по сети получить доступ к ресурсам зараженной машины вне зависимости от места ее нахождения. "Черви" - это специально разработанные вредоносные программы, обладающие способностью к неограниченному копированию собственного кода через компьютерные сети скрытно от пользователя сети с использованием различных способов преодоления защиты.

Объективную сторону данного преступления составляет факт создания 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, а равно использование либо распространение таких программ или носителей с такими программами, например дискет, CD-ROM, оптических дисков и т.д.

Использование программы означает выпуск в свет, воспроизведение, распространение и иные действия по их введению в оборот. Использование может осуществляться путем записи программы в память ЭВМ, на материальный носитель, распространение по сетям либо путем иной передачи другим лицам. 5. Данный состав преступления формальный и не требует наступления каких-либо последствий, уголовная ответственность наступает в результате создания программы, независимо от того, использовалась эта программа или нет. По смыслу ст. 273 УК наличие исходных текстов вирусных программ является основанием для привлечения к ответственности. Однако следует учитывать, что в ряде случаев использование подобных программ не будет уголовно наказуемым. Это относится к деятельности организаций, осуществляющих разработку антивирусных программ и имеющих лицензию на деятельность по защите информации, выданную Государственной технической комиссией при Президенте РФ ,при условии, что эта деятельность осуществляется с целью анализа вредоносных программ и разработки по борьбе с ними.

Формой совершения данного преступления может быть только действие, связанное с созданием вредоносных программ для ЭВМ, внесением изменений в уже существующие программы, а равно использование либо распространение таких программ. Распространение машинных носителей с такими программами полностью покрывается понятием распространения.

С субъективной стороны преступление, предусмотренное ч. 1 ст. 273 УК, может быть совершено только с прямым умыслом.

Часть 2 ст. 272 УК в отличие от ч. 1 в качестве квалифицирующего признака предусматривает наступление тяжких последствий по неосторожности. Разработка вредоносных программ доступна только квалифицированным программистам, которые в силу своей профессиональной подготовки должны предвидеть возможные последствия использования этих программ. Однако уголовная ответственность по ч. 2 ст. 273 УК может наступить в том случае, если указанные специалисты самонадеянно рассчитывают на предотвращение последствий либо не предвидели возможности наступления общественно опасных последствий своих действий, хотя при необходимой внимательности и предусмотрительности должны и могли их предвидеть.

В случае если установлен прямой умысел, охватывающий и наступление тяжких последствий, то действия виновного должны квалифицироваться по совокупности преступлений, предусмотренных ч. 1 ст. 273 УК и соответствующей статьи УК, предусматривающей ответственность за умышленное преступление.

Субъектом данного преступления может быть любой гражданин, достигший 16 лет.

##### Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

Данная норма - бланкетная и отсылает к конкретным инструкциям и правилам, устанавливающим порядок работы с ЭВМ в ведомстве или организации. Эти правила должны устанавливаться управомоченным лицом, в противном случае каждый работающий с компьютером будет устанавливать свои правила эксплуатации.

Применительно к данной статье под сетью понимается только внутренняя сеть ведомства или организации, на которую может распространяться его юрисдикция. В глобальных сетях типа Интернет отсутствуют общие правила эксплуатации, их заменяют этические Кодексы поведения, нарушения которых не могут являться основанием для привлечения к уголовной ответственности.

Объективная сторона данного преступления состоит в нарушении правил эксплуатации ЭВМ, повлекших уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ при условии, что в результате этих действий был причинен существенный вред.

Между фактом нарушения и наступившим существенным вредом должна быть установлена причинная связь и полностью доказано, что наступившие последствия являются результатом нарушения правил эксплуатации, а не программной ошибкой либо действиями, предусмотренными в ст. 272, 273 УК.

Существенный вред, указанный в диспозиции данной статьи, должен устанавливаться судом в каждом конкретном случае, исходя из обстоятельств дела, однако этот вред должен быть менее значительным, чем тяжкие последствия.

Субъективная сторона ч. 1 ст. 274 УК характеризуется наличием умысла, направленного на нарушение правил эксплуатации ЭВМ. В случае наступления тяжких последствий ответственность по данной статье наступает только в случае неосторожных действий.

Например, программист, работающий в больнице, поставил полученную по сетям программу без предварительной проверки на наличие в ней компьютерного вируса. В результате указанных действий произошел отказ в работе систем жизнеобеспечения реанимационного отделения. Умышленные действия должны квалифицироваться по соответствующим статьям УК.

Субъект данного преступления - специальный, это лицо, в силу должностных обязанностей имеющее доступ к ЭВМ, системе ЭВМ и их сети и обязанное соблюдать установленные для них правила эксплуатации.

**Литература**.

1. Федеральный закон от Федерального закона от 20.02.95 N 24-ФЗ "Об информации, информатизации и защите информации"
2. 2. Комментарий к Уголовному кодексу Российской Федерации. Под ред. Лебедева, М., 2001