Правовая ответственность за компьютерные преступления

Первым человеком, применившим ЭВМ для совершения налогового преступления на сумму 620 тыс. долларов и в ***1969 г.*** представшим за это перед американским судом, стал Альфонсе Конфессоре.
Дальнейшая история компьютерных преступлений отмечена такими наиболее "яркими" событиями:
конец 70-х - "ограбление" "Секьюрити пасифик бэнк" (10,2 млн. долларов);
1979 г. - компьютерное хищение в Вильнюсе (78584 руб.);
1984 г. - сообщение о первом в мире "компьютерном вирусе";
1985 г. - вывод из строя при помощи "вируса" электронной системы голосования в
конгрессе США;
1987-1988 гг. - появление первого "компьютерного вируса" в СССР;
1989 г. - блокировка американским студентом 6000 ЭВМ Пентагона;
международный съезд компьютерных "пиратов" в Голландии с демонстрацией
возможности неограниченного внедрения в системы ЭВМ;
1991 г. - хищение во Внешэкономбанке на сумму в 125,5 тыс. долларов;
1992 г. - умышленное нарушение работы АСУ реакторов Игналинской АЭС;
1993 г. - неоконченное электронное мошенничество в Центробанке России (68 млрд. руб.);
1995 г. - попытка российского инженера украсть из Сити - банка 2,8 млн. долларов.

В настоящее время только в Москве с помощью поддельной кредитной карточки для электронных расчетов за один раз похищается порядка **300 тыс. долларов.** Ежедневно только американские "крекеры" (специалисты по "взлому" программного обеспечения ЭВМ) крадут около 4 млн. долларов (в 2 раза больше, чем во всех остальных кражах). Годовой мировой ущерб от компьютерных преступлений составляет более 5 млрд. долларов.

Вредоносное использование вычислительной техники, естественно, потребовало разработки мер защиты от компьютерных преступлений. Основным средством борьбы должна была стать система соответствующего законодательства, в первую очередь - уголовного. В передовых странах Запада процесс этот идет уже не один десяток лет: в США - с конца 70-х гг., в Великобритании - с конца 80-х. Примечательно, что лоббированием данного вопроса в законодательных органах занимаются, прежде всего, представители промышленности и бизнеса, а также программисты.

Российские правоведы уже давно ставили вопрос о необходимости законодательного закрепления правоотношений, вытекающих из различных сфер применения средств автоматической обработки информации. Определенным этапом на пути реализации этих пожеланий стало принятие в 1992 г. ***Закона РФ "О правовой охране программ для электронно - вычислительных машин и баз данных".*** Закон содержал положение о том, что выпуск под своим именем чужой программы для ЭВМ или базы данных либо незаконное воспроизведение или распространение таких произведений влечет уголовную ответственность. Однако соответствующих изменений в УК РСФСР так и не было внесено.

Под компьютерными преступлениями понимаются те предусмотренные уголовным законом общественно опасные деяния, в которых машинная информация представляет собой предмет преступного посягательства. Именно поэтому новый УК содержит такое понятие, как "компьютерная информация", под которой понимается информация на машинном носителе, в ЭВМ, системе ЭВМ или их сети.

Последствия неправомерного использования информации могут быть самыми разнообразными: это не только нарушение неприкосновенности интеллектуальной собственности, но и разглашение сведений о частной жизни граждан, имущественный ущерб в виде прямых убытков и неполученных доходов, потеря репутации фирмы, различные виды нарушений нормальной деятельности предприятия, отрасли и т.д. Поэтому совершенно оправданно то, что преступления данного вида помещены в раздел IX "Преступления против общественной безопасности и общественного порядка".

Первоначально в проекте УК РФ глава о компьютерных преступлениях содержала 5 статей. Однако в дальнейшем в силу замечаний, высказанных как теоретиками уголовного права, так и практиками компьютерного дела, первые три статьи были объединены, и в настоящее время глава предстает в следующем составе:

- **ст. 272**. ***Неправомерный доступ к компьютерной информации;***
- **ст. 273**. ***Создание, использование и распространение вредоносных программ для ЭВМ***;
- **ст. 274**. ***Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети***.

Неправомерный доступ к компьютерной информации

Появление **ст. 272** и ее расположение в главе на первом месте было вызвано поистине катастрофическим положением, сложившимся на отечественном рынке компьютерной информации и вызванным свободным доступом пользователей ПК к информационным ресурсам и бесконтрольным копированием последних. Достаточно сказать, что около 98% копий программных продуктов производится в настоящее время у нас в стране именно таким путем.

Состав преступления, сформулирован как материальный, причем если деяние в форме действия определено однозначно (неправомерный доступ к охраняемой законом компьютерной информации), то последствия, хотя и обязательны, могут быть весьма разнообразны:

1) уничтожение информации,
2) ее блокирование,
3) модификация,
4) копирование,
5) нарушение работы ЭВМ,
6) то же - для системы ЭВМ,
7) то же - для их сети.

Субъектом преступления, указанного в ч. 1 ст. 272, может быть любое вменяемое физическое лицо, достигшее 16 лет, кроме, конечно, легального пользователя данной компьютерной информации. Санкция основного состава альтернативно предусматривает три вида наказаний: штраф, исправительные работы и лишение свободы. Первый, в свою очередь, может быть двух видов: кратный минимальному размеру оплаты труда (от 200 до 500) и кратный размеру зарплаты или иного дохода осужденного (период от 2 до 5 месяцев). Исправительные работы могут быть назначены в размере от 6 месяцев до 1 года, а лишение свободы - от 6 месяцев до 2 лет.

Часть 2 ст. 272 предусматривает в качестве квалифицирующих признаков несколько новых, характеризующих объективную сторону и субъект состава. Это совершение деяния: 1) группой лиц по предварительному сговору; 2) организованной группой; 3) лицом с использованием своего служебного положения; 4) лицом, имеющим доступ к ЭВМ, их системе или 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 автоматизированных рабочих мест и т.д.

Санкция за эти квалифицированные виды данного преступления ужесточена: в нее введен новый вид наказания (арест на срок от 3 до 6 мес.), размеры остальных увеличены: штраф от 500 до 800 минимальных размеров оплаты труда или зарплаты за период от 5 до 8 месяцев; исправительные работы от 1 года до 2 лет; лишение свободы до 5 лет.

Обязательными признаками объективной стороны ч. 1 ст. 273 будут два, характеризующих способ и средство совершения преступления. Это, во-первых, то, что последствия должны быть, несанкционированными, во-вторых, наличие самой вредоносной программы или изменения в программе. Последними, кроме названного компьютерного вируса, могут быть хорошо известные программистам "троянский конь", "логическая бомба", "люк", "асинхронная атака" и другие. В свою очередь, сами вирусы очень разнообразны и могут быть, в зависимости от: 1) сложности - простыми и раздробленными, 2) степени изменчивости - олигоморфными, полиморфными, пермутирующими, 3) среды обитания - сетевыми, файловыми, загрузочными, комбинированными, 4) метода действий - резидентными и нерезидентными, 5) особенностей алгоритма - "спутниками", "червями", "призраками", "невидимками", "паразитическими", "студенческими" и т.д., 6) деструктивных возможностей - безвредными, неопасными, опасными, очень опасными.

Санкция предусматривает один основной вид наказания (лишение свободы на срок до 3 лет) и один дополнительный (штраф в размере 200 - 500 минимальных размеров оплаты труда или зарплаты либо иного дохода лица за период 2 - 5 мес.).

Частью 2 ст. 273 криминализируется более опасное преступление: те же деяния, повлекшие тяжкие последствия. Это - преступление с материальным составом и с двумя формами вины: по отношению к действиям присутствует умысел, а к общественно опасным последствиям - неосторожность, легкомыслие или небрежность.

Санкция данной части - относительно - определенная: лишение свободы на срок от 3 до 7 лет. Таким образом, именно это преступление из всей главы относится к категории тяжких. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или сети. Целью действия ст. 274 должно быть предупреждение невыполнения пользователями своих профессиональных обязанностей, влияющих на сохранность хранимой и перерабатываемой информации. Непосредственный объект преступления, предусмотренного этой статьей, - отношения по соблюдению правил эксплуатации ЭВМ, системы или их сети, т.е. конкретно аппаратно-технического комплекса.

Под таковыми правилами понимаются, во-первых, Общероссийские временные санитарные нормы и правила для работников вычислительных центров, во-вторых, техническая документация на приобретаемые компьютеры, в-третьих, конкретные, принимаемые в определенном учреждении или организации, оформленные нормативно и подлежащие доведению до сведения соответствующих работников правила внутреннего распорядка.

Правонарушение может быть определено как преступление только при наступлении существенного вреда. Под последним следует понимать, прежде всего, вред, наносимый информации в ее значимой, существенной части. Это, например, уничтожение, блокирование, модификация ценной информации (относящейся к объектам особой важности, либо срочной, либо большого ее объема, либо трудно восстановимой или вообще не подлежащей восстановлению и т. д.); уничтожение системы защиты, повлекшее дальнейший ущерб информационным ресурсам; широкое распространение искаженных сведений и т.п.

Санкция ч. 1 ст. 274 состоит из трех альтернативных видов наказания: лишение права занимать определенную должность или заниматься определенной деятельностью на срок до 5 лет, обязательные работы от 180 до 240 часов и ограничение свободы до 2 лет.

Часть 2 - состав с двумя формами вины, предусматривающий в качестве квалифицирующего признака наступление по неосторожности тяжких последствий. Содержание последних, очевидно, аналогично таковому для ч. 2 ст. 273. Санкция нормы существенно отличается от предыдущей: только лишение свободы до 4 лет.

ССЫЛКИ НА ПРАВОВЫЕ АКТЫ

ЗАКОН РФ от 23.09.1992 N 3523-1
"О ПРАВОВОЙ ОХРАНЕ ПРОГРАММ ДЛЯ ЭЛЕКТРОННЫХ ВЫЧИСЛИТЕЛЬНЫХ МАШИН И БАЗ ДАННЫХ»

ФЕДЕРАЛЬНЫЙ ЗАКОН от 20.02.1995 N 24-ФЗ
"ОБ ИНФОРМАЦИИ, ИНФОРМАТИЗАЦИИ И ЗАЩИТЕ ИНФОРМАЦИИ"
(принят ГД ФС РФ 25.01.1995)

"УГОЛОВНЫЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ" от 13.06.1996 N 63-ФЗ
(принят ГД ФС РФ 24.05.1996)

ФЕДЕРАЛЬНЫЙ ЗАКОН от 13.06.1996 N 64-ФЗ
"О ВВЕДЕНИИ В ДЕЙСТВИЕ УГОЛОВНОГО КОДЕКСА РОССИЙСКОЙ ФЕДЕРАЦИИ"
(принят ГД ФС РФ 24.05.1996)
Законность, N 1, 1997