Андрей БЕЛОУСОВ

Исследователь Центра исследования компьютерной преступности

(Запорожье, Украина)

ОБЪЕКТИВНАЯ И СУБЪЕКТИВНАЯ СТОРОНА КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Квалификация компьютерных преступлений имеет ряд особенностей. Одной из них является то, что достаточно затруднено выявление объективной стороны преступления, т. е. конкретных действий, приведших к наказуемым последствиям. Это затруднение связано с большой сложностью компьютерных систем, скрытностью процессов, в них протекающих, и большим кругом лиц, имеющих прямое или косвенное отношение к последствиям преступления. Особенно это касается неосторожных преступлений, а также тех деяний, в которых последствия не совпадают с первичной целью.

Другой особенностью квалификации компьютерных преступлений является сложность установления субъективной стороны состава преступления. Если программист изменил последовательность операторов, в результате чего остановился конвейер завода, то доказать, что имел место умысел, а не ошибка, весьма сложно.

Основная сложность состоит в том, что безошибочных программ не бывает, а презумпция невиновности – на стороне программиста.

Иногда трудно определить предмет преступления. Так, например, предполагаемое преступление против конкретного компьютера в конечном итоге может быть направлено на более глобальную инфраструктуру, с которой он был связан сетью.

Объектом значительной части компьютерных преступлений являются отношения общественной безопасности.

Если сформируется особая "компьютерная" группа общественных отношений, то логично превратить такие отношения компьютерной безопасности в объект специальной уголовно-правовой, а в более широком контексте юридической (в том числе и международно-правовой) охраны.

Участниками отношений компьютерной безопасности являются лица, управляющие компьютеризованными системами, иным образом эксплуатирующие, а также обслуживающие их (персонал). Связи между ними опосредуются функционированием компьютеризованных систем, образующим предметную сторону данных отношений.

Среди компьютерных посягательств можно выделить:

1) посягательства на связи и отношения людей, опосредующих применение и использование компьютерной техники;
2) посягательства на вещественный элемент отношений компьютерной безопасности (заметим, что сюда могут входить и технические линии связи);
3) посягательства на надежность персонала компьютеризованных систем.

Недопустимо устанавливать уголовную ответственность за ошибку программиста, ибо программ без ошибок не бывает. Но ответственность за неосторожную модификацию файлов, которая повлекла за собой существенный ущерб, исключать нельзя.

Наконец, о субъекте. Обычно "преступления в области использования техники – это в основном и главным образом преступления со специальными субъектами". Но для компьютерных преступлений это не совсем так. И чем выше уровень компьютеризации общества, чем больше создается телекоммуникационных компьютерных сетей, тем чаще компьютерные преступления будут учиняться общими субъектами.

Особое место среди компьютерных преступлений занимают деяния, связанные с несанкционированным вторжением в компьютеризованные системы.

При расследовании компьютерных преступлений зачастую трудно установить как объективную, так и субъективную сторону преступления. Вспомним, что объективная сторона увязывает действие, последствия и их причинно-следственную связь, а субъективная сторона показывает наличие умысла (прямого, косвенного) или неосторожности.

В чем здесь заключается сложность для следствия? Дело в том, что преступник очень часто находится в условиях глубокой априорной неопределенности, т. е. "работает" в "вероятностном пространстве", а следствие всегда находится, как говорят математики, в "апостериорной области". Действительно, очень часто преступник не может в полной мере представить себе последствия своей деятельности. Это касается не только изобретателей и распространителей вирусов, а значительно более широкой категории компьютерных преступников. Такая неопределенность часто возникает, например, при попытках несанкционированного доступа в компьютерные сети. Преступник не всегда правильно представляет себе ценность копируемой, уничтожаемой или искажаемой информации, а тем более цепную реакцию, к которой могут привести его действия. Надо сказать, что одни и те же действия приводят к разным последствиям при различных (и часто совершенно неизвестных преступнику) состояниях вычислительной системы, ее загрузки, степени надежности и защищенности, связи с другими системами. Если перейти к терминологии, используемой в теории игр, то преступник зачастую неосознанно оптимизирует свою стратегию с учетом противодействия разумного или безразличного

противника. При этом он старается минимизировать риск от принятия неправильных решений, т. е. попасть в так называемую седловую точку, но, как правило, его не очень беспокоит совокупный ущерб, нанесенный его действиями. Все это приводит к сложности не только в установлении причинно-следственных связей, но даже в определении всех последствий преступления, не говоря уж об отличении умысла от неосторожности.

Таким образом, работа следователя по раскрытию компьютерных преступлений обладает целым рядом особенностей и требует специальной подготовки. Вопрос учета этих особенностей мог бы решаться, например, путем введения соответствующих специализаций в юридических вузах, училищах и академии МВД, учебных заведениях СБУ и Министерства обороны, а также юридическим профилированием студентов-программистов.

Техническое оснащение следователей, занимающихся расследованием компьютерных преступлений, в настоящее время практически отсутствует. Представляется целесообразным провести разработку и ввести в практику пакет прикладных программ следователя.

Можно не сомневаться, что область программирования, ориентированная на раскрытие и затруднение компьютерных преступлений, будет развиваться самыми быстрыми темпами, но еще не скоро достигнет своего расцвета.