УДК 343

Кульчунова К.Т.

ИЮИ КГЮА

УГОЛОВНО-ПРАВОВАЯ ЗАЩИТА КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Материал, изложенный в статье, не решает всех проблем в предотвращении и профилактике компьютерных преступлений. Но признание такого рода проблемы обретает существенный предостерегающий, предупреждающий шаг.

Уголовно-правовая защита компьютерной информации в Кыргызском уголовном законодательстве введена впервые в Уголовный кодекс в 1997 году. Изменения, происходящие в экономической жизни Кыргызстана – создание финансово-кредитной системы, предприятий различных форм собственности и т.п., – оказывают существенное влияние на вопросы защиты информации. Долгое время в нашей стране существовала только одна собственность – государственная, которая охранялась мощными спецслужбами. Проблемы информационной безопасности постоянно усугубляются процессами проникновения практически во все сферы деятельности общества технических средств обработки и передачи данных, и, прежде всего, вычислительных систем. Это дает основание поставить проблему компьютерного права, одним из основных аспектов которой являются так называемые компьютерные посягательства. Об актуальности проблемы свидетельствует обширный перечень возможных способов компьютерных преступлений.

Различают криминологические группы компьютерных преступлений: экономические компьютерные преступления, компьютерные преступления против личных прав и неприкосновенности частной сферы, компьютерные преступления против общественных и государственных интересов. Наиболее опасные и распространенные экономические компьютерные преступления включают компьютерное мошенничество (неправомерное обогащение за чужой счет путем злоупотребления с использованием автоматизированных информационных систем), компьютерный экономический шпионаж и кража программ, компьютерный саботаж, кража услуг и «компьютерного времени», самовольное проникновение в автоматизированную систему, традиционные экономические преступления, совершаемые с помощью компьютеров.

Экономические компьютерные преступления совершаются чаще всего по корыстным мотивам служащими организации, в которой используется компьютер, но могут совершаться и другими лицами, например, в случаях злоупотребления с использованием банковских счетов на компьютерных носителях, получения незаконных выплат в виде зарплаты, социальных пособий, гонораров и т.п., краж программ (компьютерное пиратство), неправомерного получения услуг, краж компьютерного времени. Эти преступления широко распространены в западных странах и составляют значительную часть компьютерной преступности. Компьютерные преступления впервые попали в сферу социального контроля в начале 70-х годов.

Компьютерные преступления против личных прав и неприкосновенности частной сферы чаще всего заключаются во введении в компьютерную систему неправильных и некорректных данных о лице, незаконном собирании данных, иных незаконных злоупотреблениях с информацией на компьютерных носителях и неправомерном разглашении информации (разглашение, например, банковской или врачебной тайны, торговля банками данных о своих клиентах, полученных путем изучения расходов, сделанных при помощи кредитной карточки).

Компьютерные преступления против интересов государства и общества включают преступления против государственной и общественной безопасности, нарушение правил передачи информации за границу, дезорганизации работы оборонных систем, злоупотребления с автоматизированными системами подсчета голосов на выборах и при принятии парламентских решений и др. Если «обычные» хищения попадают под действие существующего уголовного закона, то проблема хищения информации

значительно сложнее. Присвоение активной информации, в том числе программного обеспечения, путем неправомерного копирования не квалифицируется как хищение, поскольку хищение сопряжено с изъятием ценностей из фондов организации. Не очень далека от истины шутка, что у нас программное обеспечение распространяется только путем краж и обмена краденным. При неправомерном обращении в собственность машинная информация может не изыматься из фондов, а копироваться. Следовательно, как уже отмечалось выше, машинная информация должна быть выделена, как самостоятельный предмет уголовно правовой охраны. Собственность на информацию, как и прежде, не закреплена в законодательном порядке. Последствия этого момента еще заявят о себе.

Первоначально столкнувшись с компьютерной преступностью, органы уголовной юстиции начали борьбу с ней при помощи традиционных правовых норм об ответственности за кражу, мошенничество, злоупотребление доверием и др. Однако такой подход оказывается недостаточно эффективным, поскольку многие компьютерные преступления не охватываются составами традиционных преступлений. Так, простейший вид компьютерного мошенничества – перемещение денег с одного счета на другой путем «обмана компьютера» - не охватывается ни составом кражи (ввиду отсутствия предмета кражи – материального имущества – так как «деньги» существуют тут не в виде вещей, а в виде информации на компьютерном носителе), ни составом мошенничества, поскольку обмануть компьютер в действительности можно лишь в том смысле, в какой можно обмануть и замок у сейфа. Ни будет и признаков уничтожения или повреждения имущества в случае, например, уничтожения или повреждения имущества или уничтожение информационного элемента компьютерной системы. Подробные действия могут причинить весьма значительный имущественный ущерб.

Первым опытом Кыргызского уголовного законодательства о компьютерных преступлениях является глава 28 Уголовного кодекса КР «Преступления в сфере компьютерной информации», где предусмотрена ответственность за:

- неправомерный доступ к охраняемой законом компьютерной информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети (ст. 289 УК КР);
- 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, а равно использование либо распространение таких программ или машинных носителей с такими программами (ст. 290 УК КР);
- нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 291 УК КР).

Объективную сторону преступления характеризует неправомерное действие, нарушающее чужое право на неприкосновенность информации в компьютерной системе или сети, заключающееся в создании (включая изменение существующей программы) вредоносной программы, использовании или распространении носителей с такими программами.

Под **вредоносной программой** в законе понимается программа, приводящая к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети. Достаточно, если программа рассчитана хотя бы на единичное достижение этого результата.

Несанкционированное достижение результата означает достижение его без разрешения владельца компьютерной системы и иного законного полномочия. Не охватывается составом этого преступления создание, использование и распространение программ, предназначенных для копирования информации с защищенных дискет в нарушение авторских прав. Такое копирование или модификация информации не может рассматриваться в качестве несанкционированного, если осуществляется в соответствии с

волей владельца компьютерной системы.

Под **использованием** вредоносной программы понимается использование ее с целью несанкционированного уничтожения, блокирования, модификации либо копирования информации, нарушения работы компьютерной системы.

Распространение вредоносной программы означает как распространение ее с помощью средств компьютерной связи, так и простую передачу ее любому другому лицу.

Распространение машинных носителей вредоносной программы – означает передачу носителя другому лицу, включая копирование или дозволение копирования программы на носитель другого лица.

Субъективная сторона преступления характеризуется прямым умыслом. Лицо осознает, что создает вредоносную программу или носитель с такой программой во вред подлежащим правовой охране интересам и желает совершить эти действия.

Тяжкими последствиями могут быть: смерть человека, причинение вреда здоровью, реальная опасность технологической или военной катастрофы, дезорганизации работы транспорта или связи, причинение крупного имущественного ущерба и др.

Блокирование информации означает создание препятствий для правомерного доступа к этой информации.

Модификация информации означает изменение охраняемой законом информации.

Копирование информации влечет ответственность вне зависимости от того, копируется ли информация с помощью технических средств, либо копирование производится вручную (например, с дисплея).

Литература

1. Уголовный кодекс КР (от 1 октября 1997г.) – Б.: НАКР, 1997. -168 с.
2. Закон «Об информатизации» от 24 января 2002 г. № 10.
3. Анин Б.Ю. Защита компьютерной информации. – СПб.: БХВ-Санкт-Петерберг, 2000. -384 с.

Вехов В.Б. Компьютерные преступления: Способы совершения и раскрытия \
Под ред. акад. Б.П. Смагоринского –М.: Право и Закон, 1996. -182 с.