УДК:34:51:659

Кульчунов Б.Т., Кульчунова К.Т.

ИЮИ КГЮА г. Каракол

КОМПЬЮТЕРНАЯ ПРЕСТУПНОСТЬ И КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

Изменения, происходящие в экономической жизни КР – 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, поэтому информация и секреты были тоже государственные, которые охранялись мощными спецслужбами.

Проблемы информационной безопасности постоянно усугубляется 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.

Объектами посягательства могут быть сами технические средства (компьютеры и периферия) как материальные объекты, программное обеспечение и базы данных, для которых технические средства являются окружением.

В этом смысле компьютер может выступать, и как предмет посягательств, и как инструмент, если разделять два последних понятия, то термин компьютерное преступление как юридическая категория не имеет особого смысла. Если компьютер – только объект посягательства, то квалификация правонарушения может быть произведена по существующим нормам права. Если же - только инструмент, то достаточен только такой признак, как «применение технических средств». Возможно объединение указанных понятий, когда компьютер одновременно и инструмент и предмет. В частности, к этой ситуации относится факт хищения машинной информации. Если хищение информации связано с потерей материальных и финансовых ценностей, то этот факт можно квалифицировать как преступление. Так же если с данным фактом связываются нарушения интересов национальной безопасности, авторства, то уголовная ответственность прямо предусмотрена в соответствии с законами КР.

Каждый сбой работы компьютерной сети это не только «моральный» ущерб для работников предприятия и сетевых администраторов. По мере развития технологий платежей электронных, «безбумажного» документооборота и других, и серьезный сбой локальных сетей может просто парализовать работу целых корпораций и банков, что приводит к ощутимым материальным потерям. Не случайно что защита данных в компьютерных сетях становится одной из самых острых проблем в современной информатике. На сегодняшний день сформулировано три базовых принципа информационной безопасности, которая должна обеспечивать: целостность данных – защиту от сбоев, ведущих к потере информации, а также не авторизованного создания или уничтожения данных; конфиденциальность информации и, одновременно, ее доступность для всех авторизованных пользователей.

Следует также отметить, что отдельные сферы деятельности (банковские и финансовые институты, информационные сети, системы государственного управления, оборонные и специальные структуры) требуют специальных мер безопасности данных и предъявляют повышенные требования к надежности функционирования информационных систем, в соответствии с характером и важностью решаемых ими задач.

Компьютерная преступность.

Ни в одном из уголовных кодексов союзных республик не удается найти главу под названием «Компьютерные преступления». Таким образом компьютерных преступлений специфических в юридическом смысле не существует.

Попытаемся кратко обрисовать явление, которое как социологическая категория получила название «компьютерная преступность». Компьютерные преступления условно можно подразделить на две большие категории – преступления, связанные с вмешательством в работу компьютеров, и, преступления, использующие компьютеры как необходимые технические средства.

Перечислим основные виды преступлений, связанных с вмешательством в работу компьютеров.

1. несанкционированный доступ к информации, хранящейся в компьютере.

Несанкционированный доступ осуществляется, как правило, с использованием чужого имени, изменением физических адресов технических устройств, использованием информации остававшейся после решения задач, модификацией программного и информационного обеспечения, хищением носителя информации, установкой аппаратуры записи, подключаемой к каналам передачи данных.

Хакеры «электронные корсары», «компьютерные пираты» – так называют людей, осуществляющих несанкционированный доступ в чужие информационные сети для забавы. Набирая наудачу один номер за другим, они терпеливо дожидаются, пока на другом конце провода не отзовется чужой компьютер. После этого телефон подключается к приемнику сигналов в собственной ЭВМ, и связь установлена. Если теперь угадать код (а слова, которые служат паролем часто банальны), то можно внедриться в чужую компьютерную систему.

2. Ввод в программное обеспечение «логических бомб», которые срабатывают при выполнении определенных условий и частично или полностью выводят из строя компьютерную систему.

«временная бомба» – разновидность «логической бомбы», которая срабатывает по достижении определенного момента времени.

3. Разработка и распространение компьютерных вирусов.

«Троянские кони» типа «сотри все данные этой программы, перейди в следующую и сделай тоже самое» обладают свойствами переходить через коммуникационные сети из одной системы в другую, распространяясь как вирусное заболевание.

Выявляется вирус не сразу: первое время компьютер «вынашивает инфекцию», поскольку для маскировки вирус нередко используется в комбинации с «логической бомбой» или «временной бомбой». Вирус наблюдает за всей обрабатываемой информацией и может перемещаться, используя пересылку этой информации. Все происходит, как если бы он заразил белое кровяное тельце и путешествовал с ним по организму человека.

4. Подделка компьютерной информации.

По-видимому, этот вид компьютерной преступности является одним из наиболее свежих. Он является разновидностью несанкционированного доступа с той разницей, что пользоваться им может, как правило, не посторонний пользователь, а сам разработчик, причем имеющий достаточно высокую квалификацию.

Идей преступления состоит в подделке выходной информации компьютеров с целью имитации работоспособности больших систем, составной частью которых является компьютер. При достаточно ловко выполненной подделке зачастую удается сдать заказчику заведомо неисправную продукцию.

К подделке информации можно отнести также подтасовку результатов выборов, голосованию, референдумов и т.п.

5. Хищение компьютерной информации.

Если «обычные» хищения подпадают под действие существующего уголовного закона, то проблема хищения информации значительно более сложна. Присвоение машинной информации, в том числе программного обеспечения, путем несанкционированного 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 краденными. 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, на закреплена в законодательном порядке. На мой взгляд, последствия этого не замедлят сказаться.

Предупреждение компьютерных преступлений.

При разработке компьютерных систем, выход из строя или ошибки в работе которых могут привести к тяжелым последствиям, вопросы компьютерной безопасности становятся первоочередными. Известного много мер, направленных на предупреждение преступления. Выделим из них технические, организационные и правовые.

К техническим можно отнести защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев, установку оборудования обнаружения и тушения пожара, принятие конституционных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания, оснащения помещения замками, установку сигнализации и многое другое.

К организационным моментам отнесем охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра после выхода его из строя, организацию обслуживания вычислительного центра посторонней организацией или лицами, незаинтересованными в сокрытии фактов нарушения работы центра, универсальность средств защиты от всех пользователей.

К правовым мерам следует отнести разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства. К правовым мерам относятся также вопросы общественного контроля за разработчиками компьютерных систем и принятие международных договоров об их ограничениях, если они влияют или могут повлиять на военные, экономические и социальные аспекты жизни стран, заключающих соглашение.

Защита данных в компьютерных сетях.

При рассмотрении проблем защиты данных в сети прежде всего возникает вопрос о классификации сбое и нарушений прав доступа, которые могут привести к уничтожению или нежелательной модификации данных. Среди таких потенциальных «угроз» можно выделить:

1. Сбои оборудования (сбои кабельной системы; перебои электропитания; сбои дисковых систем; сбои работы серверов, рабочих станций и т.д.).
2. Потери информации из-за некорректной работы ПО (потеря или изменение данных при ошибках ПО; потери при заражении системы компьютерными вирусами).
3. Потери, связанные с несанкционированным доступом (несанкционированное копирование, уничтожение или подделка информации; ознакомление с конфиденциальной информацией, составляющей тайну, посторонних лиц).

Концентрация информации в компьютерах – аналогично концентрации денег в банках – заставляет все более усиливать контроль в целях защиты информации.

Юридические вопросы, частная тайна, национальная безопасность – все эти соображения требуют усиления внутреннего контроля в коммерческих и правительственных организациях. Работы в этом направлении привели к появлению новой дисциплины: безопасность информации. Специалист в области безопасности информации отвечает за разработку, реализацию и эксплуатацию системы обеспечения информационной безопасности, направленной на поддержание целостности, пригодности и конфиденциальности накопленной в организации информации. В его функции входит обеспечение физической (технические средства, линии связи и удаленные компьютеры) и логической (данные, прикладные программы, операционная система) защиты информационных ресурсов.

Сложность создания системы защиты информации определяется тем, что данные могут быть похищены из компьютера и одновременно оставаться на месте; ценность некоторых данных заключается в обладании им, а не в уничтожении или изменении.

Обеспечение безопасности информации – дорогое дело, и не столько из-за затрат на закупку или установку средств, сколько из-за того, что трудно квалифицированно определить границы разумной безопасности и соответствующего поддержания системы в работоспособном состоянии

В заключении хотелось бы подчеркнуть, что никакие аппаратные, программные и любые другие решения не смогут гарантировать абсолютную надежность и безопасность данных в компьютерных сетях. В то же время свести риск потерь к минимуму возможно лишь при комплексном подходе к вопросам безопасности.

Литература:

1. Рааб М. Защита сетей: наконец-то в центре внимания. - М., 1994. -№ 29. -18 с.
2. Векслер Д. Наконец-то надежно обеспечена защита данных в радиосетях. - М., 1994. -№ 17. -13-14 с.
3. Сухова С.В. Система безопасности. Сети, 1995, № 4, 60-70 с.
4. Беляев В. Безопасность их распределенных системах. /Открытые системы. - М., 1995. - № 3, 36-40 с.
5. Материалы с сайта http://referat2000.bizforum.ru/