Компьютерные преступления

Выполнил студент гр. НБо-20-2
Кузнецова Ульяна Александровна

Понятие компьютерных преступлений

Компьютерная информация — в соответствии со ст.2 закона “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 комментируемой статье 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).

Классификация компьютерных преступлений

Способы совершения компьерных преступлений

Основные виды преступлений, связанных с вмешательством в работу компьютеров:

«За хвост» — злоумышленник подключается к линии связи законного пользователя и дожидается сигнала, обозначающего конец работы.

«Компьютерный абордаж» — злоумышленник вручную или с использованием автоматической программы подбирает код (пароль) доступа к КС системе с использованием обычного телефонного аппарата:

«Неспешный выбор» — преступник изучает и исследует систему защиты от НСД, ее слабые места, и вводит дополнительные команды, разрешающие доступ;

«Маскарад» — злоумышленник проникает в компьютерную систему, выдавая себя за законного пользователя с применением его кодов (паролей) и других идентифицирующих шифров;

«Мистификация» — злоумышленник создает условия, когда законный пользователь осуществляет связь с нелегальным терминалом, будучи абсолютно уверенным в том, что он работаете нужным ему законным абонентом.

«Аварийный» — злоумышленник провоцирует сбои или других отклонений в работе СВТ. При этом включается особая программа, получающая доступ к наиболее ценным данным. В этом режиме возможно «отключение» всех имеющихся в компьютерной системе средств защиты информации.

Сферы компьютерных преступений

Юридическая ответственность

Уголовный кодекс РФ предусматривает различные наказания за компьютерные преступления, а также разделяет преступления на группы:

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

С помощью компьютера можно совершить любые преступления, поэтому количество статей, к которым они могут быть отнесены, велико.

Международная борьба

Первый документ Совета Европы – Рекомендации №9 Комитета Министров Совета Европы о преступлениях с компьютерами. К перечисленным правонарушениям, рекомендованных для включения в национальное законодательство, отнесены:

- -компьютерное мошенничество
- компьютерный подлог
- причинение ущерба компьютерным данным и программам
- компьютерный саботаж
- несанкционированный доступ
- несанкционированный перехват
- несанкционированное воспроизведение микросхем.

Вскоре появилась международная «Конвенция о киберпреступности». Она содержит множество процессуальных положений. Россия является участником «Соглашения о сотрудничестве государств-участников СНГ в борьбе с преступностью в сфере компьютерной информации».

Формы сотрудничества: обмен информации, скоординированные мероприятия, подготовка квалифицированных кадров, создание информационных систем, обмен нормативно-правовыми актами

Заключение

Как известно – наиболее опасные преступления – это те, которые носят экономический характер. Преступления в сфере компьютерной информации имеют, на мой взгляд, как бы двоякий смысл, и поэтому требуют специальных статей в Уголовном кодексе. Принятый в недавнем прошлом кодекс содержит целую главу, включающую в себя три статьи, что, на мой взгляд, несколько мало. Даже исходя из дословного толкования, позволю себе сказать, что они уже несколько устарели по смысловому значению, и требуют обновлений.

Спасибо за внимание