Содержание:

Введение

Научно-техническая революция повлекла за собой серьезные социальные изменения, наиболее важным из которых является появление нового вида общественных отношений и общественных ресурсов — информационных. Информация стала первоосновой жизни современного общества, предметом и продуктом его деятельности, а процесс ее создания, накопления, хранения, передачи и обработки в свою очередь стимулировал прогресс в области орудий ее производства: электронно-вычислительной техники (ЭВТ), средств телекоммуникаций и систем связи.

Появление на рынке в 1974 году компактных и сравнительно недорогих персональных компьютеров, по мере совершенствования которых стали размываться границы между мини- и большими ЭВМ, дали возможность подключаться к мощным информационным потокам неограниченному кругу лиц. Встал вопрос о контролируемости доступа к информации, ее сохранности и доброкачественности. Организационные меры, а также программные и технические средства защиты оказались недостаточно эффективными.

Особенно остро проблема несанкционированного вмешательства дала о себе знать в странах с высокоразвитыми технологиями и информационными сетями.

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 комментируемым статьям 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). При рассмотрении дел следует учитывать, что при определенных условиях и физические поля могут являться носителями информации.

Быстрый количественный рост преступности и ее качественные изменения, обусловленные обострением противоречий в различных областях общественной жизни, частой реорганизацией системы правоохранительных органов, несовершенство законодательства и частое его изменение, серьезные упущения в правоприменительной практике, способствуют ускорению процессов развития компьютерной преступности как социального явления.

Отсутствие четкого определения компьютерной преступности, единого понимания сущности этого явления значительно затрудняют определение задач правоприменительных органов в выработке единой стратегии борьбы с ней.

Компьютерные преступления условно можно подразделить на две большие категории — преступления, связанные с вмешательством в работу компьютеров, и преступления, использующие компьютеры как необходимые технические средства. Не будем касаться «околокомпьютерных» преступлений, связанных с нарушением авторских прав программистов, незаконным бизнесом на вычислительной технике и т.п., а также физического уничтожения компьютеров.

Способы совершения компьютерных преступлений

Подходить к классификации компьютерных преступлений наиболее оправданно с позиций составов преступлений, которые могут быть отнесены к разряду компьютерных. Хотя состав компьютерных преступлений в настоящее время четко не определен, можно выделить ряд видов противоправных деяний, которые могут быть в него включены. Перечислим некоторые основные виды преступлений, связанных с вмешательством в работу компьютеров:

- «за дураком» — физическое проникновение в производственные помещения.
- «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, выявляет участки, имеющие ошибки или неудачную логику программного строения, разрывы программ (брешь, люк) 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 создает условия для возникновения сбоев или других отклонений в работе СВТ. При этом включается особая программа, позволяющая в аварийном режиме получать доступ к наиболее ценным данным. В этом режиме возможно «отключение» всех имеющихся в компьютерной системе средств защиты информации.
- манипуляция данными и управляющими командами

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

Но с помощью компьютера можно совершить любые преступления кроме изнасилования, поэтому количество статей, к которым они могут быть отнесены, велико.

1. ст. 129 Клевета
2. ст. 130 Оскорбление
3. ст. 137 Нарушение неприкосновенности частной жизни

4. ст. 138 Нарушение тайны переписи, телефонных переговоров, почтовых, телеграфных и иных сообщений.
5. ст. 146 Нарушение авторских и смежных прав
6. ст. 147 Нарушение изобретательных и патентных прав
7. ст. 158 Кража
8. ст. 159 Мошенничество
9. ст. 163 Вымогательство
10. ст. 165 Причинение имущественного ущерба путем обмана или злоупотребления доверием
11. ст. 167 Умышленное уничтожение или повреждение имущества
12. ст. 168 Умышленное уничтожение или повреждение имущества по неосторожности
13. ст. 171 Незаконное предпринимательство
14. ст. 182 Заведомо ложная реклама
15. ст. 183 Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну
16. ст. 200 Обман потребителя
17. ст. 242 Незаконное распространение порнографических материалов или предметов
18. ст. 276 Шпионаж
19. ст. 280 Публичные призывы к осуществлению экстремистской деятельности
20. ст. 282 Возбуждение национальной, расовой или религиозной вражды
21. ст. 283 Разглашение государственной тайны
22. ст. 354 публичные призывы к развиванию агрессивной войны

Тенденции развития экономической преступности в России

Уровень компьютерной преступности определяется во многом объективными причинами и напрямую зависит от общего уровня информатизации общества. Большинством зарубежных и отечественных исследователей отмечается отставание России в вопросах компьютеризации от развитых стран в среднем на 20 лет. Если в США первое компьютерное преступление было зафиксировано в 1966 г., то в бывшем СССР — в 1979 г[1]. Поэтому тенденции развития компьютерной преступности в России могут заметно отличаться от таковых в развитых странах. По мнению экспертов в данной области, следует, прежде всего, ожидать

значительного количественного роста компьютерных преступлений. Этому способствует ряд причин, среди которых основными можно считать: во-первых, резкий рост безработицы и падение уровня жизни среди так называемой «беловоротничковой» прослойки населения на фоне общего экономического кризиса и кризиса неплатежей; во-вторых, массовая неконтролируемая компьютеризация и использование новейших электронных средств во всех сферах деятельности, прежде всего финансовых, банковских и кредитных учреждениях всех форм собственности; в-третьих, отсутствие соответствующей правовой базы, препятствующей в сколько-нибудь заметной мере распространению и пресечению компьютерных преступлений.

Среди положительных тенденций можно прогнозировать сокращение числа краж собственно компьютерной техники и периферии, ввиду существенного падения цен на них и относительной доступности, а также сокращение незаконного использования машинных ресурсов и машинного времени.

Заключение

На современном этапе развития ИТ в России назрела необходимость детального изучения проблемы основ криминалистического исследования компьютерной преступности. Следует отметить, что при совершении компьютерных преступлений, так же как и при совершении любых других общеизвестных видов преступлений, остаются «следы», обнаружение, фиксация и исследование которых является непременным условием при расследовании и раскрытии, как данного вида преступлений, так и в борьбе с «техногенной» преступностью в целом.