информации, что позволит познакомить их с фундаментальными основами теории защиты информации, общей схемой обеспечения информационной безопасности, со структурой унифицированной концепции и стратегией защиты информации. Рассмотрение фундаментальных основ теории защиты информации позволит сформировать представление о подходах к защите информации, инвариантных относительно развития разных информационных технологий [1].

Обучение основам защиты информации в рамках курсов переподготовки по ИТ-специальностям можно разделить на два направления: программное и техническое. Если технические методы защиты информации рассматриваются слушателями в рамках курса «Компьютерные сети», то программные методы защиты информации в рамках специальности не рассматриваются. В настоящее время прорабатывается возможность введения в рамках курса, где слушатели изучают основы алгоритмизации и программирования, темы «Основы защиты информации», в которой будут рассматриваться как основы защиты информации на уровне программного обеспечения, так и основные алгоритмы шифрования данных (например: AES, DES, RSA, RC4), будут описываться основные преимущества и недостатки и приводится варианты их применения на практике. Для закрепления полученных знаний слушателям, в рамках практических занятий, будет предложено реализовать один из алгоритмов шифрования. Полученные теоретические и практические навыки в дальнейшем помогут выпускникам переподготовки быть более конкурентоспособными на рынке труда.

Список литературы

1. Димов Е.Д. Методика обучения студентов вузов технологиям защиты информации в условиях фундаментализации образования: автореф. дис. ... канд. пед. наук. Москва, 2013. 25 с.

МОНИТОРИНГ ЭЛЕКТРОМАГНИТНЫХ ПОЛЕЙ, СОЗДАВАЕМЫХ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКОЙ

В.А. Попов, А.В. Потапович, П.Л. Прудников

В условиях стремительно развивающейся современной вычислительной техники, переноса на ЭВМ большинства количества и видов анализа и обработки информации, возникла и начала развиваться киберпреступность. Одной из ее разновидностей является перехват обрабатываемой на ЭВМ информации путем внедрения в агрегаты вычислительной машины аппаратной закладки, считывающей обрабатываемые в памяти компьютера данные и передаче ее по радиоканалу с помощью встроенных в вычислительную технику недекларированных возможностей. Встроенные недекларированные возможности в вычислительную технику могут быть организованы как программным путем с использованием не основных по функциональному назначению свойств элементной базы, так и аппаратно-программным путем. Такие встроенные недекларированные возможности вычислительной техники могут эпизодически кратковременно организовывать передачу информации в сжатом виде на некоторой частоте по радиоканалу. Исходя из этого, становится очевидным один из методов обнаружения подобных устройств несанкционированного съема информации – мониторинг электромагнитного излучения вычислительной техники.

Важнейшим показателем мониторинга электромагнитного излучения является выбор необходимого диапазона частот. При выборе частотного диапазона мониторинга исходили из предпосылок наиболее простого и доступного метода организации получения информации. Частотный диапазон предлагается выбрать от 10 МГц до 10 ГГц с разбиением его на 10 октавных полос.

Устройство мониторинга может применяться на рабочих местах, в машинных залах предприятий, осуществляющих обработку конфиденциальной информации на ЭВМ. Сигнал тревоги от устройства мониторинга послужит основанием для выполнения работ с целью проверки узлов и агрегатов ЭВМ на предмет наличия недекларированных возможностей.