МЕТОД КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ВИДЕОИНФОРМАЦИИ В СРЕДСТВАХ ОБРАБОТКИ ДАННЫХ

А.В. ХИЖНЯК, А.В. ИГНАТЧЕНКО

Предлагаемый метод криптографической защиты видеоинформации может быть использован для создания защищённых средств обработки данных (СОД) от утечки информации за счёт побочного электромагнитного излучения (ПЭМИ).

Прохождение электрических сигналов по цепям средства обработки данных и соединительным кабелям сопровождается возникновением побочных электромагнитных излучений в окружающей среде. Распространение побочных электромагнитных излучений за пределы контролируемой территории создает предпосылки для утечки информации, так как возможен ее перехват с помощью специальных технических средств контроля. В СОД, как например, персональная ЭВМ (ПЭВЭМ), основными источниками электромагнитных излучений являются устройства ввода и вывода информации совместно с их адаптерами (монитор, принтер, клавиатура, печатающее устройство и т.д.), а также центральный процессор. Утечке информации в ПЭВМ способствует применение коротких видеоимпульсов прямоугольной формы и высокочастотных коммутирующих сигналов. Исследования показывают, что излучение видеосигнала монитора является достаточно мощным, широкополосным и охватывает диапазон метровых и дециметровых волн.

Для уменьшения уровня побочных электромагнитных излучений применяют специальные средства защиты информации — экранирование, фильтрацию, заземление, электромагнитное зашумление, а также средства ослабления уровней нежелательных электромагнитных излучений и наводок при помощи различных резистивных и поглощающих согласованных нагрузок.

В отличие от известных методов и средств защиты информации от утечки за счёт ПЭМИ, предлагаемый метод позволил создать модель системы криптографической защиты видеоинформации в СОД с секретной передачей ключа, обеспечивающей теоретическую стойкость шифра по Шеннону, что позволяет с уверенностью говорить о несостоятельности решения при криптоанализе. Использование данного метода позволяет впервые не говорить о контролируемой территории для данного канала утечки, так как её значение сводится к нулю. Отсутствует также необходимость в использовании экранирующих материалов и всевозможных фильтрующих устройств в канале передачи видеоинформации.

Важным достоинством метода является так же то, что он позволяет создать модель криптосистемы, которая не только защищает видеоинформацию в средствах обработки данных, но и осуществляет информационное противодействие по каналу ПЭМИ, в целях полного или частичного дезинформирования злоумышленника.