ЗАЩИТА МОБИЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ ОТ УТЕЧКИ ИНФОРМАЦИИ ПО КАНАЛАМ ПЭМИ

М.В. ЖАЛКОВСКИЙ, А.В. СИДОРЕНКО

Новейшие разработки в области электроники и информационных технологий позволили реализовать в мобильном исполнении вычислительные системы с производительностью, ранее доступной только стационарным комплексам. В свою очередь, мобильность вычислительных систем сделала еще более актуальной проблему защиты информации от утечки по каналам побочных электромагнитных излучений (ПЭМИ), так как мобильную систему невозможно однозначно соотнести с физической средой, в которой она работает. В каждом новом месте работы мобильной системы будут уникальными электромагнитная обстановка и физические свойства среды распространения радиоволн, что делает невозможным расчет или прогноз степени защищенности.

Для защиты информации в мобильных вычислительных системах целесообразно использовать комбинированный метод защиты информации от ПЭМИ, который включает в себя элементы активного и пассивного методов [1]. Основными мероприятиями пассивного метода защиты являются максимальное снижение уровней ПЭМИ в источнике излучений, уменьшение длины излучающих элементов (кабелей питания, интерфейсных и др.) экранирование вычислительных систем, применение радиопоглощающих материалов и покрытий.

В качестве основного элемента активной системы защиты предлагается использовать разработанный мобильный генератор электромагнитного шума. Питание генератора осуществляется от порта USB, который де-факто стал стандартным в любой вычислительной системе. Спецификация USB 2.0 определяет максимальный ток потребления 500 мА при напряжении 5 В [2], что является достаточным для устойчивой работы всех систем генератора шума.

Излучающим элементом генератора выбрана всенаправленная штыревая антенна. Данный тип антенны позволяет добиться стабильности отношения сигнал/шум при изменении взаимного расположения вычислительной системы и генератора.

Разработанный генератор электромагнитного шума и методика его применения, могут быть использованы в качестве основного средства защиты мобильных вычислительных систем от утечки информации по каналам ПЭМИ.

Литература

1. *Зайцев А.П., Шелупанов А.А. и др.* Технические средства и методы защиты информации. 7-е изд., испр. М., 2012.

2. *Garney J.* Universal Serial Bus Specification. Revision 2.0. Intel Corporation, 2000. P. 178–183.

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННОГО КОМПЛЕКСА ANSYS ДЛЯ ПОСТРОЕНИЯ МОДЕЛИ СИСТЕМЫ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО АКУСТИЧЕСКОМУ КАНАЛУ

И.В. САВЧЕНКО, Г.В. ДАВЫДОВ

При создании программной модели для защиты речевой информации целесообразно использовать программную среду ANSYS, в основе которой лежит система конечно-элементного анализа. Процедура типового расчета а программе ANSYS проводится в три основных этапа: построение модели, приложение нагрузок и получение решения, просмотр и анализ результатов.

Первый этап включает определение типов конечных элементов, их констант, свойств и геометрии модели. Программа ANSYS содержит более 80 типов конечных элементов, каждый из которых определяет применимость элемента к той или иной области расчетов. Разработанная геометрическая модель для защиты речевой информации должна представлять

собой конечно-элементную модель, состоящую из узлов и элементов, соответствующих требуемым характеристикам модели.

На втором этапе выбирается тип анализа, производится установление его опций, прикладываются нагрузки, определяются опции для выбора шага по нагрузке и инициируется решение. Тип анализа учитывает основные характеристики, условия функционирования и реакцию системы, которую предполагается оценивать. Информация о нагрузках для последующего расчета содержится в базе данных программы ANSYS, в которой может храниться только один набор результатов, тогда как в файлах могут содержаться результаты для всех вариантов решения.

На третьем этапе для просмотра результатов может быть применим общий постпроцессор, используемый для анализа результатов одного шага решения (оценки погрешности счета, проведения вычислений на основе полученных данных и др.), и постпроцессор процесса нагружения, применимый для просмотра результатов в указанных точках расчетной модели на каждом шаге решения, что позволяет получить график результатов или выполнить алгебраические вычисления.

Таким образом, программа ANSYS является наиболее приемлемым программным продуктом для построения модели системы защиты речевой информации от утечки по акустическому каналу.

АНАЛИЗ ХАРАКТЕРИСТИК ИЗМЕРИТЕЛЬНЫХ КОМПЛЕКСОВ ДЛЯ ОЦЕНКИ ЗАЩИЩЕННОСТИ РЕЧЕВОЙ АКУСТИЧЕСКОЙ ИНФОРМАЦИИ

В.А. ТРУШИН, А.В. ИВАНОВ

Доклад посвящен требованиям к характеристикам комплексов оценки защищенности речевой акустической информации. Проведено рассмотрение существующих программно-аппаратных комплексов, их измерительных и функциональных характеристик. Предложено сформировать требования к данным комплексам, основываясь на характеристиках органов слуха и артикуляции человека, потому что, даже при использовании всевозможных технических средств разведки, конечным «анализатором» речевой информации всегда является человек. Проведен ряд экспериментов для получения данных характеристик. Сформированы требования к элементам программно-аппаратных комплексов, а так же предложены различные варианты схем создания подобных комплексов.

По результатам исследований получены следующие результаты: частотный диапазон должен составлять от 90 до 10000 Гц, тип полосового разбиения — соответствующий «критическим» полосам слуха, динамический диапазон от 30 дБ (обычный уровень фоновых шумов в помещениях) до 110 дБ (с учетом возможности завышения уровня тестового сигнала для снижения влияния на результат фоновых шумов), человеческое ухо способно различать разницу амплитуд акустических сигналов в 1 дБ (относительно порога слышимости 20 мкПа). Чувствительность микрофона, разрядность аналогово-цифрового преобразователя (АЦП) и коэффициент усиления предусилителя, в совокупности, должны позволять реализовать измерения с заданным разрешением. Поставленная цель требует создания комплекса на базе специализированного под задачи защиты информации (ЗИ) шумомера. С учетом всех требований, предлагается несколько схем реализации комплекса (с использованием АЦП) для оценки защищенности речевой информации, стоимость создания которых оказывается на порядок ниже стоимости существующих на рынке комплексов.