

одной или более частей сообщения (но не всех) и ее расшифровывание не дает возможности получить все сообщение целиком.

Литература

1. Freier A. The Secure Sockets Layer (SSL) Protocol Version 3.0 – August 2011.

МОДЕЛИРОВАНИЕ АКУСТИЧЕСКИХ ЗАДАЧ С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНОГО СРЕДСТВА

И.В.Савченко

Одним из подходов к решению проблема защиты речевой информации от утечек по акустическому каналу является разработка базовой программной модели, которая основана на адаптации физической модели под программную реализацию. Для разработки программного средства определены входные и выходные параметры базовой физической модели, критерии выбора среды разработки и непосредственно сама среда разработки программного средства, а также предложена архитектура программного средства.

Входные величины и параметры, которыми будет оперировать разрабатываемая программная реализация акустической модели, основываются на наборе математических формул и уравнений акустики, описывающих физические процессы в рамках заданного класса акустических задач.

С учетом требований к программной реализации и исследуемой физической модели, оптимальным языком программирования является Java, позволяющий создавать программы в соответствии с концепциями объектно-ориентированного программирования в рамках распространенных паттернов проектирования.

Архитектура программного средства представлена в виде набора шаблонов проектирования, оптимальным из которых является шаблон проектирования «Мост». При реализации базовой архитектуры приложения через шаблон «Мост», изменение структуры интерфейса не мешает изменению структуры реализации.

На основании разработанной архитектуры реализован прототип программного средства, демонстрирующий работу описанного выше алгоритма в рамках выбранной математической модели. В качестве входных параметров заданы: размер помещения и взаимное расположение стен; источник звука, являющийся центром исходящих лучей; точность расчета, включающая в себя количество лучей и количество отражений. Чтобы итерационно продемонстрировать принцип работы алгоритма, при работе с программой изменялись значения, определяющие точность заданных параметров.

ЗАЩИТЫ ДАННЫХ НА ОСНОВЕ ВЕКТОРНОЙ СХЕМЫ РАЗДЕЛЕНИЯ СЕКРЕТА В РАСПРЕДЕЛЕННОЙ СИСТЕМЕ ХРАНЕНИЯ ИНФОРМАЦИИ

С.Б. Саломатин, Т.А. Андриянова

Распределенные системы хранения информации широко используются в современных инфокоммуникационных системах. При этом появляется возможность использовать пространственно-временную избыточность распределенных систем для защиты информации.

Один из методов защиты данных может быть основан на схеме разделения секрета среди группы пользователей (агентов) распределенной информационной сети.

Векторная пороговая схема, использующая геометрию точек в пространстве.

Сообщение определяется как точка в n -мерном пространстве. Каждое уравнение в пороговой схеме – это уравнение $(n - 1)$ - мерной гиперплоскости, содержащей эту точку.

Защищаемые массивы данных, разбиваются на несколько отображений. Коэффициенты отображений выбираются случайным образом из множества целых чисел меньших модуля P или используются элементы массива данных. Матричное представление