реализации (носителя информации) создает возможность увеличения числа передаваемых информационных потоков [1].

Предлагаемые СКК на основе шумовых носителей позволяют уплотнять информационные потоки без использования дополнительных частотных и временных ресурсов, обеспечивая при этом высокую структурную скрытность систем передачи информации (СПИ).

В работе приводится синтез и математическое моделирование устройств формирования и обработки шумовых сигналов на основе корреляционно-временного уплотнения информационных потоков для помехозащищенных СПИ. Показано влияние помех на качество выделения информационных потоков, даны оценки качественных характеристик СПИ, использующих предлагаемые СКК.

Литература

1. Ипатов В.П. Широкополосные системы и кодовое разделение сигналов. Принципы и приложения. М., 2007.

ПОДХОД К ВЫЯВЛЕНИЮ АППАРАТНЫХ НЕДЕКЛАРИРОВАННЫХ ВОЗМОЖНОСТЕЙ В ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКЕ

В.И. ВОРОБЬЕВ, В.А. ПОПОВ, Ю.В. ШАМГИН

Известны способы и устройства [1] выявления аппаратных недекларированных возможностей (АНДВ) в вычислительной технике (ВТ). В докладе обосновывается целесообразность сосредоточения внимания на:

– поиске АНДВ, в первую очередь, во внешних устройствах и аксессуарах основного оборудования ВТ;

– анализе возможностей использования в исследуемом оборудовании АНДВ, работающих в официально выделенном для интерфейсов Wi-Fi и Bluetooth частотном диапазоне.

Предложения связаны с тем, что внешние устройства и аксессуары основного оборудования ВТ весьма удобны для быстрой установки в них и обеспечения электропитания камуфлированных под стандартные элементы и узлы АНДВ. в частотном же диапазоне, используемом интерфейсами Wi-Fi и Bluetooth, сравнительно просто маскировать маломощные электромагнитные сигналы АНДВ. Поиск демаскирующих работу АНДВ сигналов целесообразно осуществлять на всех входах и выходах основного оборудования ВТ, подключаемых к внешним проводным линиям, включая линию электропитания. Важным средством выявления АНДВ следует считать визуальный осмотр и даже разборку аксессуаров и внешних устройств ВТ. Поиск информативных радиоизлучений исследуемого оборудования в каждом конкретном случае требует индивидуального подхода.

Литература

1. Халяшин Д.Б. Защита информации. Вас подслушивают? Защищайтесь. М., 2004. 432 с.

МЕТОД ОБНАРУЖЕНИЯ СКРЫТОЙ ПЕРЕДАЧИ ДАННЫХ, ИСПОЛЬЗУЮЩЕЙ СТЕГАНОГРАФИЧЕСКИЙ МЕТОД КОХА-ЖАО

А.И. ДЕМИДЧУК, Ю.А. ЧЕРНЯВСКИЙ

Жао Цянь и Экхард Кох предложили выполнять встраивание скрываемого сообщения в процессе JPEG-сжатия [1]. В каждом блоке дискретно-косинусного преобразования из 8-ми среднечастотных коэффициентов выбираются три

коэффициента ДКП и подвергаются следующей модификации: для кодирования 1 и 0 коэффициенты изменяются так, чтобы два из них были больше или меньше третьего на определенное пороговое значение *D*.

Анализу подвергаются все коэффициенты ДКП из области модификации каждого блока (8 коэффициентов). Для этого в каждом блоке вычисляется среднеквадратичное отклонение (СКО) и формируется массив коэффициентов СКО. для полученного массива строится гистограмма распределения коэффициентов, по которой находится значение наиболее часто встречающееся — s_{max}. для пустых контейнеров и контейнеров заполненных с порогом $D>1$ значение s_{max} будет больше ς=0,354. для случая $D=1$ вычисляется отношения количества наиболее часто встречающихся значений к общему количеству коэффициентов СКО. Полученное значение отношения сравнивается со значениями вероятности нахождения скрытой информации по таблице значений, полученных эмпирическим путем.

Предложенный критерий стеганографического анализа JPEG-изображений дает высокий процент (порядка 90%) верных результатов в случае порога $D>1$. Оценка с порогом встраивания $D=1$ дает результат с ошибкой второго рода равной 15,6%. для пустых контейнеров ошибка первого рода примерно равна 20%. Использование предложенного метода оценки изображения в формате JPEG на предмет определения наличия скрытой информации методом Коха–Жао обеспечивает эффективное решение задач стегоанализа.

Литература

1. Zhao J., Koch E. // IEEE Workshop on Nonlinear Signal and Image Processing. Greece, 1995. P. 123–132.

УСТРОЙСТВО СИНТЕЗА РЕЧЕПОДОБНЫХ СИГНАЛОВ НА РАЗНЫХ ЯЗЫКАХ

О.Б. ЗЕЛЬМАНСКИЙ

Задачей предлагаемого устройства защиты речевой информации является генерирование речеподобных сигналов на разных языках и в режиме реального времени, маскирующих речь участников переговоров. Работа устройства осуществляется следующим образом.

Блок формирования псевдотекста составляет псевдотекст на выбранном языке или нескольких языках с использованием их статистики, получаемой, например, от баз русского, арабского и английского языков. Блок компиляции аллофонов в зависимости от диктора и выбранного языка выбирает необходимые базы аллофонов и озвучивает полученный псевдотекст. в результате получается шумовой речеподобный сигнал, который поступает на управляемый усилитель.

В случае, если требуется синтезировать речеподобный сигнал непосредственно из речи участников переговоров, речевой сигнал, поступающий от встроенного или выносного микрофона, фиксируется блоком детектирования речи. Далее он поступает в блок верификации диктора по голосу, а также в блоки сегментации и классификации с целью формирования аллофонов, которые в свою очередь заносятся в базу аллофонов соответствующего диктора. В базу аллофонов какого диктора следует занести каждый аллофон определяется блоком верификации диктора по голосу, который распознает и подтверждает личность каждого из участников переговоров на основании уникальной информации, выделенной из их речи заранее в процессе регистрации до начала переговоров. Кроме того данный блок позволяет выбрать уже имеющуюся базу аллофонов конкретного диктора для использования в блоке компиляции аллофонов.