1. Г.Реклейтис, А.Рейвиндран, К.Рэгсдел «Оптимизация в технике», книга 1, Москва, 1986
2. Г.Реклейтис, А.Рейвиндран, К.Рэгсдел «Оптимизация в технике», книга 2, Москва, 1986

КОМПЬЮТЕРНАЯ РЕАЛИЗАЦИЯ СИСТЕМЫ ЗАСЕКРЕЧИВАНИЯ ИНФОРМАЦИИ С ПОМОЩЬЮ ФУНКЦИЙ НЕПРОПОРЦИОНАЛЬНОСТЕЙ

Левченко Е.В., Авраменко В.В.

Рассматривается возможность нового подхода для решения задачи засекречивания и рассекречивания информации, имеющей вид аналогового сигнала (функции времени) и сигнала, представленного в виде последовательности символов из заданного алфавита, с помощью функций непропорциональностей[1,2].

Для осуществления шифрования информации на передающем конце необходимы: сообщение, подлежащее засекречиванию, представленное в виде функции $y(t)$, эталонная функция $f(t)$, с помощью которой осуществляется шифрование сообщения, производная эталонной функции $f'(t)$ и дополнительный элемент засекречивания – $y(0)$ – начальное значение функции $y(t)$, принятый согласно договорённости отправляющей и принимающей сторон. Эталонная функция $f(t)$ должна быть гладкой и $f(t) \neq 0$, ни при каких значениях t.

Засекречиваемая функция $y(t)$ в процессе кодирования сообщения заменяется её непропорциональностью $z(t)$ (13) [2] по эталонной функции $f(t)$, которая в принятых обозначениях имеет вид:

$$z(t) = @d^{(1)}_{f(t)} y(t) = \frac{y(t)}{f(t)} - \frac{y'_t(t)}{f'_t(t)}. \qquad (1)$$

Полученная таким образом непропорциональность $z(t)$ передается по каналу связи.

На приемном конце по функции $z(t)$, эталонной функции $f(t)$ и по известному начальному значению $y(0)$, осуществляется восстановление засекреченной функции $y(t)$. Для этого из формулы (1) получаем дифференциальное уравнение:

$$y'(t) = y(t) \cdot \frac{f'(t)}{f(t)} - z(t) \cdot f'(t) \cdot \qquad (2)$$

Его решение при заданном значении $y(0)$ позволяет найти $y(t)$.

Дифференциальное уравнение (2) решается аналитически и численно. Аналитическое решение приводиться для контроля численного метода решения данной задачи.

Обычно $y(t)$ имеет такой вид, для которого аналитически решить уравнение (2) очень сложно или вообще невозможно. Поэтому, как правило, задача решается только численным методом.

Результатом работы являются компьютерные программы шифрования и дешифрования информации. Применение такого подхода приводит к тому, что каждый символ в сообщении засекречивается различными числами действительного типа, в зависимости от того, в какой части сообщения он расположен. Это значительно усложняет процесс взлома данной криптосистемы.

[1] Авраменко В.В. Характеристики непропорциональности числовых функций. – Деп. в ГНТБ Украины 19.01.98, №59 Ук98.

[2] Авраменко В.В. Характеристики непропорциональностей и их применения при решении задач диагностики// Вестник СумГУ. – 2000. №16.

РАСЧЕТ ВОЛЬТ-АМПЕРНЫХ ХАРАКТЕРИСТИК В ПОЛУИЗОЛИРУЮЩИХ МАТЕРИАЛАХ ДЛЯ СЛУЧАЯ НЕОДНОРОДНОГО РАСПРЕДЕЛЕНИЯ ЛОВУШЕК

Е.О.Гончаренко студ., А.С. Опанасюк доц., Н.В. Тыркусова доц.,Сумский государственный университет, Сумы