АЛГОРИТМЫ СРАВНЕНИЯ СЛУЧАЙНЫХ ЧИСЛОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Репка М.В., Херсонский И.В.
Научный руководитель – д.т.н., проф. Антипов И. Е.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Ленина,14, каф. Радиоэлектронных устройств,
тел. (057) 702-14-44)

Algorithms of comparing random number sequences can be used to protect information. Method of information protection, presented in this paper is based on the random characteristics of the meteor-burst channel for the formation of random number sequences as the encryption keys.

Способ защиты информации, который рассмотрен в данной работе, основан на использовании случайных характеристик метеорного радиоканала для формирования случайных числовых последовательностей в качестве ключей шифрования. В данной работе рассмотрен самый простой с точки зрения технической реализации способ формирования случайной числовой последовательности, основанный на измерении интервалов между метеорными радиоотражениями.

В каждом из пунктов размещения корреспондентов в эфир непрерывно излучаются зондирующие сигналы с периодом. Количество излучённых сигналов непрерывно считается счётчиками. В момент приёма зондирующего сигнала от удалённого корреспондента (одновременно в обоих пунктах), происходит считывание состояния счётчиков, затем их обнуление и начало нового счёта. Считанная информация (одинаковая в обоих пунктах) равна времени, прошедшему от начала последнего метеорного следа до начала текущего, выраженному в количестве интервалов. Не исключены ситуации, когда результаты единичного измерения в одном из пунктов будут отличаться от результатов измерений в другом. Это неизбежно из-за шума, помех и возможных аппаратурных сбоев. Чтобы удостовериться в идентичности сформированных последовательностей в каждом из сеансов связи необходимо применить кодирование сформированных ключей и их обмен по каналу связи. Даже в случае перехвата закодированного ключа криптоаналитиком, это не позволит ему вычислить ключ. А корреспонденту, который обладает ключами шифрования, сравнение закодированных ключей позволит установить факт их идентичности. В случае несовпадения вычисленного и принятого закодированного ключа, данные текущего измерения игнорируются в обоих пунктах. Также такие меры позволят исключить влияние постановщиков помех. Если злоумышленник, пытаясь поставить помеху, направляет антенну на метеорный след, который является «полезным» для легального пользователя и злоумышленника, то бла-

годаря применению кодирования ключей пользователь сможет определить ложность полученных результатов измерений.

Помехоустойчивое кодирование представляет собой метод обработки сообщений, предназначенный для повышения надежности передачи по каналам связи. Существует два больших класса корректирующих кодов – блочные и сверточные. Определяющее различие между этими кодами состоит в отсутствии или наличии памяти кодера. Блочное кодирование удобно использовать в тех случаях, когда исходные данные по своей природе уже сгруппированы в какие-либо блоки или массивы. При передаче по радиоканалам чаще используется свёрточное кодирование, которое лучше приспособлено к побитовой передаче данных. Кроме этого, при одинаковой избыточности сверточные коды, как правило, обладают лучшей исправляющей способностью. Основными характеристиками сверточных кодов являются параметры – размер кадра информационных символов, размер кадра кодовых символов, длина памяти кода, информационная длина слова, кодовая длина блока [1].

Кодовая длина блока - это длина кодовой последовательности, на которой сохраняется влияние одного кадра информационных символов.

Сверточный код имеет еще один важный параметр – скорость, которая характеризует степень избыточности кода, вводимой для обеспечения исправляющих свойств кода. Сверточные коды могут быть систематическими и несистематическими и обозначаются как линейные сверточные коды.

Систематическим сверточным кодом является такой код, для которого в выходной последовательности кодовых символов содержится без изменения породившая его последовательность информационных символов. В противном случае сверточный код является несистематическим. Сверточные коды являются частным случаем итеративных или рекуррентных кодов [2]. При рекуррентном кодировании разбиение кодируемой последовательности информационных символов на блоки не производится, а кодовые символы вычисляются. Используя представление сверточного кода с помощью порождающих многочленов, можно задавать сверточный код посредством последовательностей коэффициентов производящих многочленов, записанных в двоичной или восьмеричной форме. Сверточные коды используются для надежной передачи данных: видео, мобильной связи, спутниковой связи.

Литература:

1. Шульгин В.И. Основы теории передачи информации (пособие) Часть 2. Харьков. 2003. – 87 с.

2. Никитин Г. И. Сверточные коды: Учебное пособие. С-П.: Сов. радио, 2001. – 78 с.