ГЕНЕРАТОР СЛУЧАЙНЫХ ЧИСЕЛ НА ОСНОВЕ МОДЕЛИ ЛОРЕНЦА

А.М. Ярук, Н.Г. Киевец

В криптографической области важным предметом для изучения и усовершенствования являются генераторы случайных чисел (ГСЧ), которые должны формировать надежные ключи.

Конструкция и технология ГСЧ должна позволить формировать непредсказуемые последовательности чисел на его выходе. Помимо этого, к ним предъявляются следующие требования: выходной поток битовой последовательности чисел должен соответствовать статистическим критериям случайности; следующий бит последовательности чисел должен быть случайным (неопределенным); должна быть исключена возможность воспроизведения одного и того же битового потока последовательности случайных чисел.

Рассматривается формирование случайных чисел с помощью ГСЧ, в состав которого входит блок, построенный на основе хаоса. Блок относится к диссипативным динамическим системам, в которых хаос обусловлен наличием странных аттракторов [1]. Примерами таких реализаций являются: входной источник шума и дискретизация с использованием двух генераторов с джиттером, хаотические генераторы с дискретным и непрерывным временем.

В основе ГСЧ лежит физическая случайность, энтропия которой увеличивается благодаря использованию блока, построенного на основе хаоса. Таким образом, начальными условиями для работы блока динамического хаоса служит физическая случайность. Это приводит к возникновению сложной системы: при изменении начальных условий системы образуется эрготичность (хаос) значений.

Реализация ГСЧ выполнена с использованием хаотического генератора на основе модели Лоренца, математически описываемой тремя дифференциальными уравнениями первого порядка. При этом в ГСЧ устанавливается хаотический режим с непрерывными случайными числами на выходе. Показано, что использование рассмотренного ГСЧ улучшает процесс случайности и непредсказуемости результата.

Литература

1. Кузнецов С.П., Динамический хаос / С.П. Кузнецов. – М: Физматлит, 2001.

Библиотека БГУИР