ПРИМЕНЕНИЕ ТЕСТА «СТОПКА КНИГ» ДЛЯ ОЦЕНКИ КАЧЕСТВА РАБОТЫ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ЧИСЕЛ

Н.Г. Киевец

Учреждение образования «Белорусская государственная академия связи», Минск, Беларусь

В докладе рассматривается оценка качества работы генераторов случайных чисел (ГСЧ) электронных пластиковых карт (ЭПК) на основе методики двухуровневого тестирования [1].

В докладе обсуждаются результаты двухуровневого тестирования ГСЧ пяти ЭПК на базе микроконтроллера К5004 ВЕ2 с применением теста «стопка книг» [2]. Для проведения исследования от каждой ГСЧ получено по 500 случайных последовательностей (СП) длиной 2048 бит. На первом уровне тестирования к каждой из СП применен тест «стопка книг», в котором СП разбивалась на непересекающиеся блоки длиной два бита. На втором уровне тестирования выполнена проверка равномерности распределения вероятностей превышения полученных для каждой из СП тестовых статистик.

Применение теста «стопка книг» позволило в дополнение к тестам NIST проверить соответствие вырабатываемых генераторами СП равномерно распределенным случайным последовательностям и сделать выводы о качестве работы ГСЧ ЭПК.

Список литературы

1. Киевец, Н. Г. Применение духуровневого тестирования для оценки качества работы генераторов случайных чисел / Н. Г. Киевец // Проблемы инфокоммуникаций. – 2017. – № 1 (5). – С. 19–23.

2. Рябко, Б. Я. «Стопка книг» как новый статистический тест для случайных чисел / Б. Я. Рябко, А. И. Пестунов // Проблемы передачи информации. – 2004. – Т. 40, вып. 1. – С. 73–78.