ТЕОРЕТИЧЕСКИЕ РАСПРЕДЕЛЕНИЯ СТАТИСТИК ТЕСТА КУМУЛЯТИВНЫХ СУММ ДЛЯ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С ДЛИНАМИ 192 И 1024 БИТА

Н.Г. Киевец

Для оценки качества работы генераторов случайных чисел (ГСЧ) электронных пластиковых карт (ЭПК) может использоваться двухуровневое тестирование вырабатываемых ГСЧ случайных последовательностей (СП).

В случае применения двухуровневого тестирования к СП с длинами практически используемых криптографических ключей требуется нахождение теоретического распределения тестовой статистики теста при каждой длине СП [1].

В докладе обсуждаются полученные автором теоретические распределения тестовых статистик теста кумулятивных сумм для СП с длинами 192 и 1024 бита. Теоретические распределения представлены в виде графиков. Приводятся результаты двухуровневого тестирования СП с длинами 192 и 1024 бита, выработанных ГСЧ десяти ЭПК с микроконтроллером К5004 ВЕ2. Полученные результаты свидетельствуют о высоком качестве работы ГСЧ ЭПК и подтверждают их пригодность для выработки криптографических ключей с длинами 192 и1024 бита.

Литература

1. Киевец, Н.Г. Оценка качества работы генераторов случайных чисел на основе двухуровневого тестирования // Проблемы инфокоммуникаций. 2017. № 1 (5). С. 19–23.