ДВУХУРОВНЕВОЕ ТЕСТИРОВАНИЕ СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С ДЛИНАМИ 192 И 1024 БИТ

Н.Г. Киевец

Широкое распространение получили электронные пластиковые карты (ЭПК), имеющие встроенный генератор случайных чисел (ГСЧ), который применяется для выработки криптографических ключей.

Оценка качества работы ГСЧ ЭПК может быть выполнена на основе двухуровневого тестирования вырабатываемых ГСЧ случайных последовательностей (СП), что позволяет также выполнить проверку статистических свойств отдельных сгенерированных СП, предназначенных для создания ключей.

Ранее автором было выполнено двухуровневое тестирование СП с длинами 128 и 256 бит, полученных от ГСЧ четырех ЭПК с микроконтроллером K5004 BE2 [1, 2]. Полученные результаты показали высокое качество работы ГСЧ ЭПК.

В докладе обсуждаются результаты двухуровневого тестирования СП с длинами практически используемых ключей 192 и 1024 бит. СП получены от ГСЧ двух ЭПК с микроконтроллером K5004 BE2, при тестировании применялся частотный тест. Полученные результаты представлены в виде таблиц и гистограмм. Выводы, сделанные по результатам тестирования СП с длинами 192 и 1024 бит, соответствуют выводам, сделанным ранее, и подтверждают возможность использования ГСЧ ЭПК для криптографических приложений.

Литература

1. Киевец Н.Г., Корзун А.И. Двухуровневое тестирование случайных последовательностей длиной 128 и 256 бит // Доклады БГУИР. – 2017. – № 3 (105). – С. 78–83.

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