ПРИМЕНЕНИЕ ДВУХУРОВНЕВЫХ ТЕСТОВ ДЛЯ ОЦЕНКИ КАЧЕСТВА РАБОТЫ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ЧИСЕЛ В ДИАПАЗОНЕ РАБОЧИХ ТЕМПЕРАТУР

Н.Г. Киевец

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

Для различных приложений широко применяются электронные пластиковые карты (ЭПК) со встроенными физическими генераторами случайных чисел (ГСЧ), вырабатывающими случайные последовательности (СП). Поскольку СП используются для создания криптографических ключей и от их статистических свойств зависит безопасность передаваемых данных, актуальной является задача оценки качества работы ГСЧ ЭПК.

В связи с тем, что ЭПК эксплуатируются при различных температурах, представляет интерес проверка качества работы ГСЧ ЭПК во всем диапазоне рабочих температур от 0º до 50º в соответствии со стандартом [1].

Была поставлена задача выполнить оценку качества работы ГСЧ пяти ЭПК с микроконтроллерами К5004 ВЕ2 при температурах 0º, 21º и 50º с использованием методики двухуровневого тестирования СП [2].

Для решения поставленной задачи от ГСЧ каждой ЭПК получено 12 тыс. СП длиной 256 бит – по 4 тыс. СП при каждой из трех температур. Далее выполнено двухуровневое тестирование СП каждого массива из 4 тыс. СП. В эксперименте использовались частотный тест, тест на подпоследовательности одинаковых бит, тест на самые длинные подпоследовательности единиц в блоках, тест аппроксимированной энтропии и тест кумулятивных сумм.

Полученные результаты тестирования показали высокое качество работы ГСЧ ЭПК во всем диапазоне рабочих температур и пригодность ГСЧ ЭПК для генерации криптографических ключей длиной 256 бит.

Список литературы

1. Карточки идентификационные. Карточки с интегральными схемами контактные. Ч. 1: СТБ 1211.1-2000 (ИСО/МЭК 7816-1:1998). Введ. 01.07.2000. Минск: Госстандарт, 2000. 4 с.

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