ОЦЕНКА КАЧЕСТВА РАБОТЫ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ЧИСЕЛ, ВЫРАБАТЫВАЮЩИХ ПОСЛЕДОВАТЕЛЬНОСТИ ДЛИНОЙ 512 БИТ

Н.Г. Киевец, А.М. Ярук

От качества работы генераторов случайных чисел (ГСЧ), используемых для создания криптографических ключей, зависит безопасность передачи зашифрованной информации. В связи с этим задача оценки качества работы ГСЧ является актуальной. Оценка качества работы ГСЧ может выполняться на основе двухуровневого тестирования вырабатываемых генераторами случайных последовательностей (СП) с длинами, равными длинам практически используемых криптографических ключей [1].

В докладе обсуждаются результаты двухуровневого тестирования СП длиной 512 бит, выработанных ГСЧ пяти электронных пластиковых карт (ЭПК) с микроконтроллером К5004 ВЕ2. Двухуровневое тестирование выполнялось по частотному тесту и тесту кумулятивных сумм. Для указанных тестов автором были получены теоретические распределения тестовых статистик для СП длиной 512 бит в соответствии с методикой [2]. Все ГСЧ ЭПК успешно прошли тестирование, что свидетельствует об их высоком качестве работы.

Литература

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

2. Киевец Н.Г., Корзун А.И. Методика нахождения эталонных законов распределения вероятностей, получаемых при статистическом тестировании последовательностей ключей // Доклады БГУИР. 2014. № 5 (83). С. 38–43.