диапазонов. Показателем качества работы алгоритмов было определено количество срывов сопровождения на 1000 кадров видеопоследовательности. Срывом сопровождения считалось отсутствие перемещения строба сопровождения в направлении движения объекта интереса в течении более 2 с.

Проведенный анализ показал существенное улучшение работы корреляционного алгоритма с комплексированием первичной видеоинформации по сравнению с типовым алгоритмом (от 33 до 83%). Результаты проведенных исследований планируется применить в автомате сопровождения системы «Адунок».

ПРОВЕРКА КАЧЕСТВА РАБОТЫ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ЧИСЕЛ ЭЛЕКТРОННЫХ ПЛАСТИКОВЫХ КАРТ В ДИАПАЗОНЕ РАБОЧИХ ТЕМПЕРАТУР

А.М. Ярук, Н.Г. Киевец, А.В. Босак, Э.В. Машкович

В соответствии со стандартом информационных технологий и безопасности [1] одним из наиболее важных требований по генерации случайных чисел является использование физических генераторов для получения криптографических ключей. Одним из устройств, содержащих физические генераторы случайных чисел (ГСЧ), является электронная пластиковая карта (ЭПК). Интерес к применению ЭПК в криптографических системах вызван их дополнительными преимуществами: ЭПК защищены от посторонних атак и используют стандартные команды.

Так как в основе функционирования ГСЧ ЭПК лежит физический процесс, в их работе возможны сбои и отказы, возникающие в том числе под воздействием температуры окружающей среды. Для проверки качества работы генераторов ЭПК требуется статистическое тестирование их выходных последовательностей.

Для ЭПК стандартом [2] определен диапазон рабочих температур от 0 ˚С до 50 ˚С. В докладе приводятся результаты тестирования случайных последовательностей, полученных из ЭПК при температурах 0 ˚С, 20 ˚С и 50 ˚С. Для проверки статистических свойств последовательностей применены системы тестов FIPS 140-2 и NIST. Полученные результаты могут быть использованы при выборе ЭПК для генерации криптографических ключей.

Литература

1. Информационные технологии и безопасность. Требования безопасности к программным средствам криптографической защиты информации: СТБ 34.101.27-2011. Введ. 01.03.12. Минск: Госстандарт, 2012. – 33 с.

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