ДАТЧИК СЛУЧАЙНЫХ ЧИСЕЛ НА ОСНОВЕ ЭЛЕКТРОННЫХ ПЛАСТИКОВЫХ КАРТ

Н.Г. Киевец, П.Б. Капля, А.И. Корзун

Генерация случайного числа в интеллектуальной карте (ИК) на основе К5004 ВЕ1 начинается от датчика шума. Датчиком служит полупроводниковый прибор. Шум усиливается операционным усилителем до уровня опорного напряжения схемы непрерывного во времени хаоса. Сигнал с выхода схемы непрерывного хаоса модулирует частоту высокочастотного генератора, выход которой поступает на вход схемы выборки. На второй вход схемы выборки поступает сигнал с низкочастотного нестабильного релаксационного генератора. Таким образом, для генерации случайного числа используется три физических явления: временная нестабильность периода выходных колебаний релаксационного генератора, тепловой шум интегральных полупроводниковых приборов и непрерывный во времени хаос.

Полученное случайное число подвергается обработке по специальному алгоритму. При первом обращении к ДСЧ (при подаче питания) начальное состояние

соответствующих автоматов "заполняется" с физического датчика с обязательной начальной прокруткой в течение 8 периодов.

При постоянном нахождении микроконтроллера в рабочем состоянии текущие состояния соответствующих автоматов сохраняются в оперативной памяти и используются при каждой последующей выработке случайной последовательности (8 байт).

Для выработки массива случайных чисел создана установка на основе компьютера, к которому по USB подключается карт-ридер, осуществляющий обмен с картой по протоколу ISO 7816. Написана программа, по которой компьютер получает доступ к данным, генерируемым картой. Сгенерированные данные накапливаются в виде файла данных, доступного к чтению программой MATLAB. Массив данных обрабатывается в MATLAB для оценки качества случайных чисел. Благодаря универсальности протокола взаимодействия с картами имеется возможность сравнить качественные показатели и возможности генерации массивов данных картами различных производителей.