УДК 517.518.23

ОСОБЕННОСТИ АППАРАТНОГО ДАТЧИКА СЛУЧАЙНЫХ ЧИСЕЛ

Колыбельников А. И.

Московский физико-технический институт

Доклад посвящен проблемным вопросам, которые возникают при создании аппаратного датчика случайных чисел. Подобного рода датчики широко востребованы в различных системах защиты информации, там они применяются для выработки ключей шифрования, случайных чисел, обеспечивающих уникальность блоков информации. Кроме того, случайные последовательности могут применяться для моделирования различных случайных процессов в других приложениях.

Итоговой целью работы было построить датчик случайных чисел на небольшом устройстве с интерфейсом USB, скорость получения чисел на выходе устройства не должна была быть менее 100Мбит/сек, полученная последовательность должна была полностью соответствовать требованиям тестов NIST и DIEHARD для случайных последовательностей.

В качестве физического генератора случайной последовательности был выбрана пара стабилитронов КГ401В. Поскольку эти стабилитроны являются аналоговыми, то схема приобрела деление на аналоговую часть и цифровую. Кроме того, такое деление потребовало отдельного питания на выходе стабилизаторов устанавливалось напряжение +12(±0,1)В и -12(±0,1)В – что не невозможно обеспечить на автономном USB-устройстве так как питание на USB порте +5(±0,1)В и -5(±0,1)В. В ходе экспериментов было обнаружено, что этот вопрос можно решить использованием батарей в качестве источника постоянного тока для питания аналоговой части схемы.

Выбранные стабилитроны генерируют шум Шоттки (дробовой шум). Спектральная плотность этого типа шума зависит от тока I_0, протекающего через барьер. Выражается спектральная плотность формулой Шоттки: $i^2(f) = 2qI_0$, где $q = 1.610^{-19}$ – заряд электрона. Таким образом, $i(f) = \sqrt{2qI_0}$=17.9рА. С входного тока I_0. Для генерации шума стабилитронами такого типа необходимо использовать малые токи. В приведенной ниже схеме использовался ток $I_0 = 50\text{мкА}$, среднее напряжение на диоде в таком режиме составляет ~ 8,35В.

Что бы обеспечить отсутствие навязывания закона формирования последовательности применялся целый ряд фильтров изображенных на рисунке 1. Часть из них является избыточной, часть – следствие неправильного выбора АЦП. Для аналого-цифрового преобразования в данной схеме использовалась широко распространённая микросхема FT232RL. Она имеет ряд недостатков для использования в качестве АЦП для оцифровки шума, она имеет узкую полосу приема сигнала и механизм нормирования принятого сигнала, что отрицательно сказывается на качестве оцифрованной последовательности.

Схем генерации случайных чисел, было реализовано две. Схемы были эквивалентными, после прохождения процедуры оцифровки, полученные данные суммировались при помощи операции XOR. Эта операция была нужна для приведения

итоговой последовательности к равномерному распределению. До ее осуществления так же выполнялась операция взятия по модую 16.

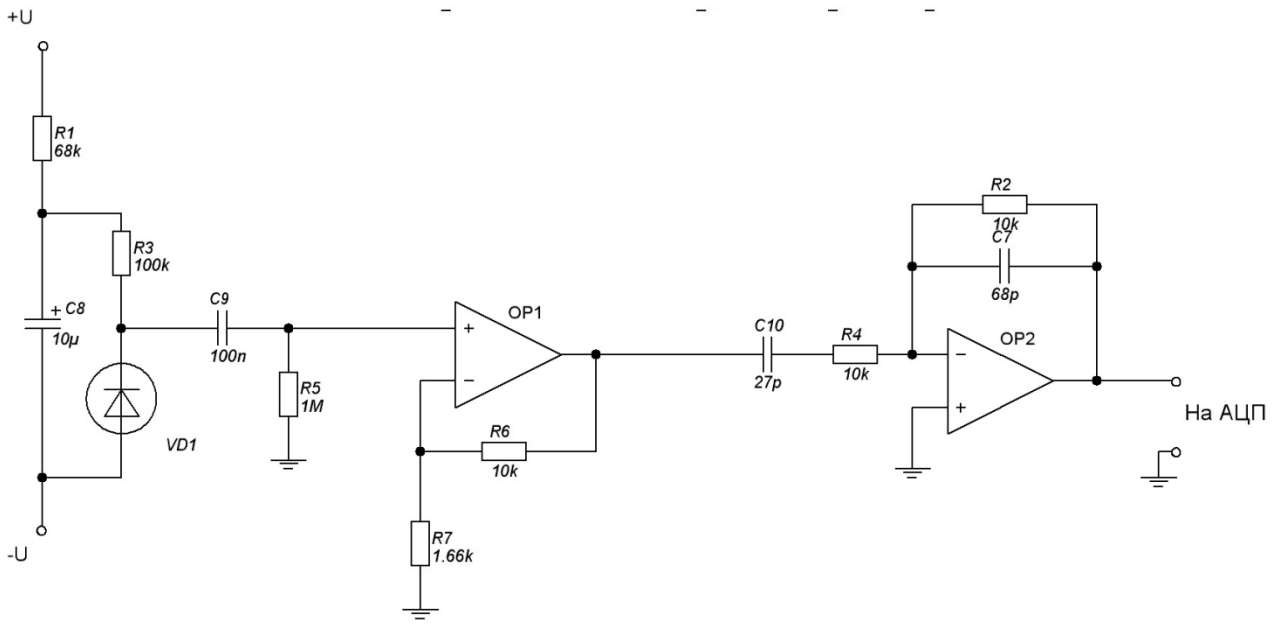

Рисунок 1. Схема генерации случайных чисел (аналоговая часть)

Эти преобразования, XOR и mod 16 были необходимы для нивелирования недостатков цифровой последовательности, которые возникали из-за недоработанной схемы. Таким образом, терялось до половины сгенерированных бит, падала скорость работы. При увеличении значения модуля, датчик переставал проходить тесты NIST и DIEHARD. Максимальная скорость, которая была достигнута при указанных параметрах – 82Мбит/сек.

Исходя из вышеизложенного был сделан вывод о необходимости замены АЦП на широкополосный, с меньшим количеством регистров.

ЛИТЕРАТУРА

Бобнев М. П. «Генерирование случайных сигналов и измерение их параметров». — М.: Энергия, 1966. — 120 с.

Григорьев А.А. Лекции по теории сигналов. –М.:МФТИ, 2013