МЕТОДЫ И СРЕДСТВА ФОРМИРОВАНИЯ И ИССЛЕДОВАНИЯ СЛУЧАЙНЫХ И ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

УДК 681.324.067

А. А. ТОРБА, канд. техн. наук, С. Г. ЕЛАКОВ, А. З. СТЕПЧЕНКО

ГЕНЕРАЦИЯ РАВНОВЕРОЯТНЫХ СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ОСНОВЕ ФИЗИЧЕСКИХ ДАТЧИКОВ

Применение физических датчиков позволяет генерировать случайные последовательности, которые не будут коррелированны на сколь угодно длинном расстоянии. Такие последовательности действительно являются случайными, т.к. они не могут быть воспроизведены в заданном порядке, не могут быть повторены в следующем опыте и являются полностью непредсказуемыми.

Для генерации случайных последовательностей достаточно внесение одного какого-нибудь случайного (непредсказуемого) параметра в детерминированный процесс. Простейшим примером является считывание состояний детерминированного счетчика в случайные моменты времени. Обязательным условием для генерации случайных последовательностей является многократное переполнение счетчика между считываниями. Известен пример генерации случайных чисел при считывании состояний счетчика в таймере IBM PC в моменты нажатий произвольных клавиш. Для набора случайного числа длиной 512 бит необходимо нажать 32 клавиши. Это занимает много времени (до одной минуты), однако такой метод может быть реализован на программном уровне и не требует дополнительного оборудования.

Физические датчики шума (резисторы, полупроводниковые и вакуумные электронные приборы) генерируют случайные последовательности импульсов различной амплитуды и с широким частотным спектром. Наиболее удобно применять в вычислительных устройствах физические датчики шума на основе полупроводниковых приборов с Зенеровским пробоем (стабилитронов).

Генераторы шума КГ401А при токе 50...100 мкА формируют случайные импульсы амплитудой 0,1...1 В с максимальной частотой до 3-х МГц (график Uшд на рис. 1, а). Преобразование этих импульсов в логические уровни цифровых микросхем (график Uтш на рис. 1, б) реализуется усилителями-ограничителями (компараторами) с небольшим гистерезисом на входе – триггерами Шмитта (TS).

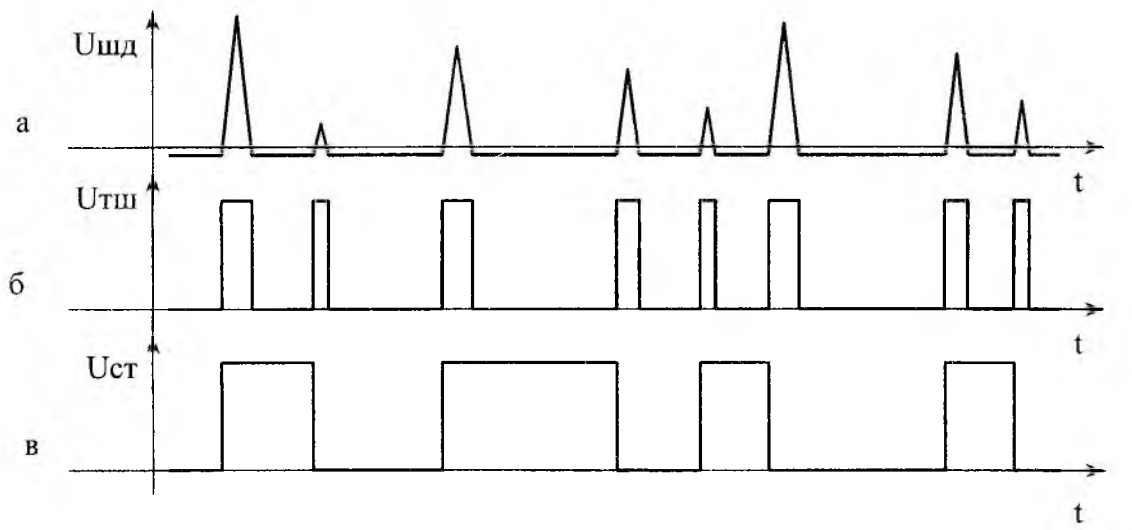

Рис. 1

В выходном сигнале триггера Шмитта (график Uтш на рис. 1, б) преобладает уровень логического нуля. При считывании этого сигнала в произвольные моменты времени формируемая случайная последовательность будет содержать значительно больше нулевых битов, чем единичных.

Для выравнивания вероятностей "0" и "1" выходной сигнал триггера Шмитта подается на счетный триггер (см. рис. 2). Выходной сигнал счетного триггера (график Uст на рис. 1, в) с равной веро-

ятностью принимает значения «логического нуля» и «логической единицы» в произвольные моменты времени. Считывание случайных битов можно производить в детерминированные моменты времени.

Достоинством данного метода формирования случайных битов является малая зависимость параметров формируемых последовательностей от режимов первичного генератора шумовых импульсов и закона распределения во времени случайных импульсов. Обязательным условием независимости элементов генерируемых случайных последовательностей является многократное срабатывание счетного триггера в течение интервала времени между считываниями.

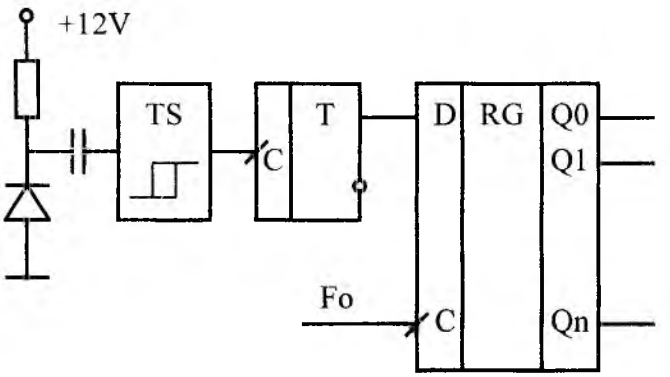

Рис. 2

Состояния счетного триггера считываются с частотой Fo сдвигающим регистром RG (рис. 2). Частота Fo выбирается в 5...10 раз меньше, чем средняя частота шумовых импульсов на выходе триггера Шмитта. Это необходимо для многократного срабатывания счетного триггера между соседними считываниями случайных битов. При этом исключается взаимное влияние вероятности появления очередного бита от состояния предыдущего бита.

Реальная средняя частота шумовых случайных импульсов диода КГ401А составляет 2...3 МГц, поэтому детерминированная частота считывания Fo выбирается около 200 кГц (период формирования случайных битов – 5 мкс). При этом время формирования случайного слова (длиной 16 бит) равно 80 мкс. Время формирования ключа длиной 512 бит составит – 2,56 мс.

Одноканальная схема формирования случайных битов, включающая шумовой диод, усилитель-ограничитель (триггер Шмитта) и счетный триггер (см. рис. 2), не обеспечивает необходимую надежность генерации равновероятных битов в случае изменения параметров источника шума или усилителя-ограничителя на основе триггера Шмитта. Повышение надежности канала формирования случайных битов достигается горячим резервированием, то есть параллельной работой нескольких каналов [1]. На рис. 3 приведена схема генератора случайных последовательностей с двумя каналами формирования случайных битов (первый канал выделен на рис. 3 пунктиром). Возможно применение трех и более аналогичных каналов формирования случайных битов.

Выходные равновероятные случайные логические сигналы всех каналов объединяются схемой ИСКЛЮЧАЮЩЕЕ ИЛИ (схемой суммирования по модулю 2) и считываются в сдвигающий регистр с частотой Fo (см. рис. 3).

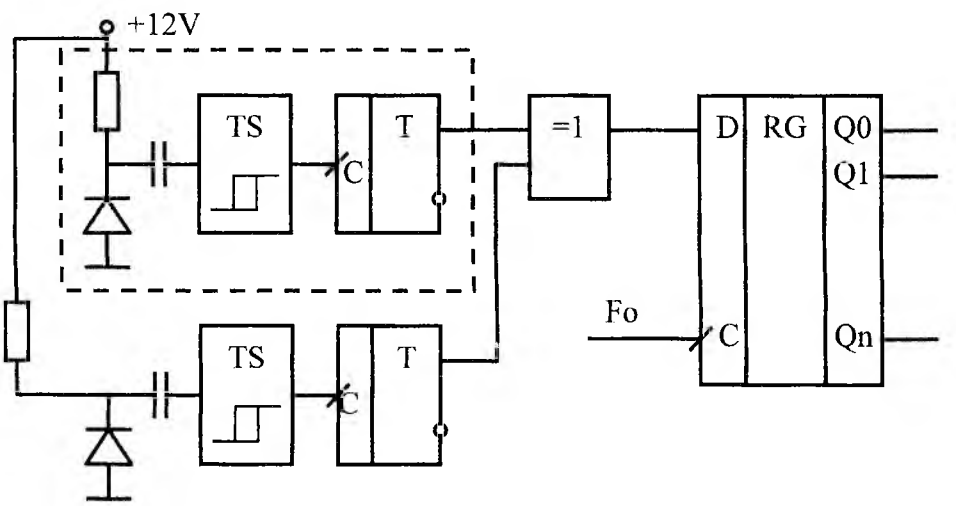

Рис. 3

Функционирование генератора случайных последовательностей (см. рис. 2 или 3) возможно только в составе программно-аппаратного комплекса, включающего в себя:

- собственно генератор равномерно распределенных случайных чисел,
- программный драйвер считывания случайных чисел,
- программы тестирования случайных последовательностей.

При экспериментальных исследованиях генераторов случайных последовательностей (см. рис. 2 или 3), реализованных на микросхемах ТТЛШ, было обнаружено, что при частоте входных импульсов шумового генератора около 2 МГц вероятность «нулевых» битов превышает вероятность «единичных» битов на величину примерно:

$$\Delta P = P(0) - P(1) = 0{,}001.$$

При увеличении входной частоты шумовых импульсов – разность вероятностей ΔР также увеличивается.

Это объясняется особенностями схемотехники выходного каскада микросхем ТТЛШ. Выходное сопротивление каскада в состоянии «логическая единица» значительно больше выходного сопротивления каскада в режиме «логический нуль». Поэтому время перезарядки «паразитных емкостей» нагрузки элемента ТТЛШ через выходное сопротивление каскада будет различным. В результате: счетный триггер дольше переходит из состояния "0□1", чем "1□0". Поэтому в выходной последовательности генераторов случайных чисел в среднем на 1000 «нулей» формируется примерно 999 «единиц».

Существует несколько алгоритмов выравнивания вероятностей случайных битовых последовательностей.

Первый алгоритм позволяет значительно уменьшить разность вероятностей генерируемых случайных битов. Для этого из двух последовательных случайных битов формируется их логическая функция ИСКЛЮЧАЮЩЕЕ ИЛИ. Промежуточный регистр RG1 запоминает два последних генерируемых случайных бита (рис. 4). В выходной регистр RG2 записывается логическая функция ИСКЛЮЧАЮЩЕЕ ИЛИ этих битов, но с частотой в два раза меньше, чем Fo (счетный триггер Т2 делит частоту считывания Fo на два). Вероятность единичного формируемого бита на *входе регистра RG1* обозначим P(1), а вероятность нулевого – P(0) = P(1) + Δ.

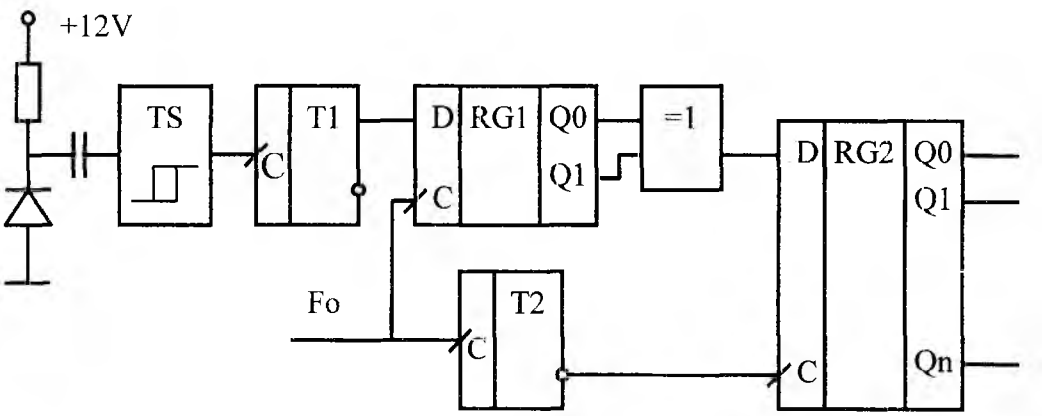

Рис. 4

Сумма вероятностей P(0) + P(1) всегда равна единице.

Запишем все комбинации битов на *выходе промежуточного регистра RG1* и вероятности этих комбинаций (с учетом полной статистической независимости генерируемых соседних случайных битов) (см. табл. 1).

Таблица 1

Q1	Q2	Вероятности
0	0	[P(1) + Δ] * [P(1) + Δ]
0	1	[P(1) + Δ] * P(1)
1	0	P(1) * [P(1) + Δ]
1	1	P(1) * P(1)

На выходе схемы ИСКЛЮЧАЮЩЕЕ ИЛИ (см. рис. 4) формируется логический нуль при комбинациях, соответствующих первой и последней строкам табл. 1. Поэтому вероятность "нулей" P(0)' на выходе схемы ИСКЛЮЧАЮЩЕЕ ИЛИ равна:

$$P(0)' = [\,P(1) + \Delta\,] * [\,P(1) + \Delta\,] + P(1) * P(1).$$

Логической единице на выходе схемы ИСКЛЮЧАЮЩЕЕ ИЛИ будут соответствовать две средние строки в таблице 1, поэтому вероятность "единиц" P(1)' будет равна:

$$P(1)' = [\,P(1) + \Delta\,] * P(1) + P(1) * [\,P(1) + \Delta\,].$$

Разность вероятностей на выходе схемы ИСКЛЮЧАЮЩЕЕ ИЛИ равна:

$$\Delta' = P(0)' - P(1)' = \Delta^2.$$

Учитывая малую величину разности вероятностей Δ (примерно 0,001), можно утверждать, что ее квадрат будет значительно меньше.

К недостаткам этого метода (метода «Дельта-квадрат») можно отнести в два раза меньшую скорость формирования случайных битов и, хотя и маленькую, но не нулевую, разность вероятностей "0" и "1".

Второй метод еще в два раза уменьшает скорость формирования случайных последовательностей, но позволяет выровнять вероятности "0" и "1". Идея этого метода понятна из анализа табл. 1. Вероятности второй и третьей строк равны. Поэтому при комбинации сигналов на выходах промежуточного регистра RG1, соответствующей второй строке, в выходной регистр RG2 записывается нулевой бит, а при комбинации, соответствующей третьей строке, – единичный бит. Комбинации сигналов, соответствующие первой и последней строкам, не используются.

Для этого нулевой логический сигнал с выхода логической схемы ИСКЛЮЧАЮЩЕЕ ИЛИ (контролирующей выходы промежуточного регистра RG1) запрещает запись в выходной регистр RG2 (см. рис. 5) при комбинациях, соответствующих первой и последней строкам табл. 1.

Описанные схемы формирователей случайных последовательностей (рис. 4 и 5) обладают относительно небольшой скоростью генерации случайных бит, которая при частоте шумовых импульсов кремниевого диода КГ401А около 2МГц – не превышает десятков килогерц.

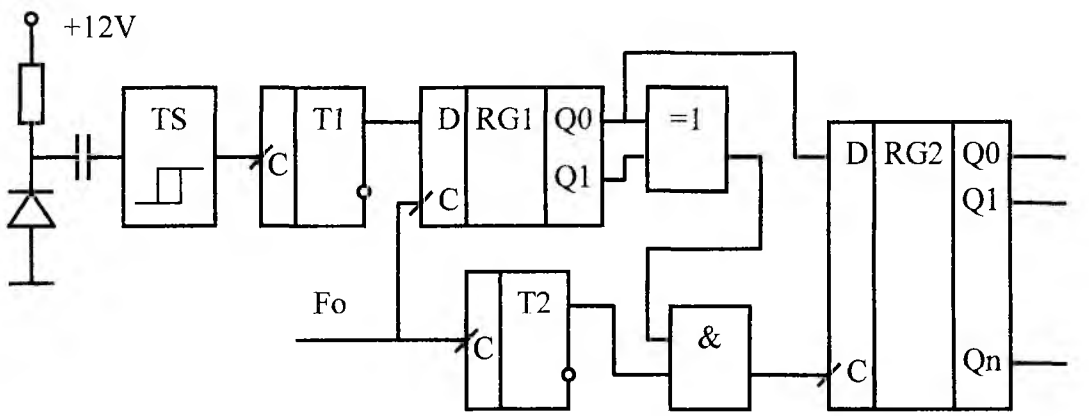

Рис. 5

Значительно повысить скорость формирования случайных битов позволяет схема генератора псевдослучайных последовательностей на основе сдвигающего регистра с обратными связями и случайным инвертированием входного сигнала регистра при помощи элемента ИСКЛЮЧАЮЩЕЕ ИЛИ (рис. 6) [2].

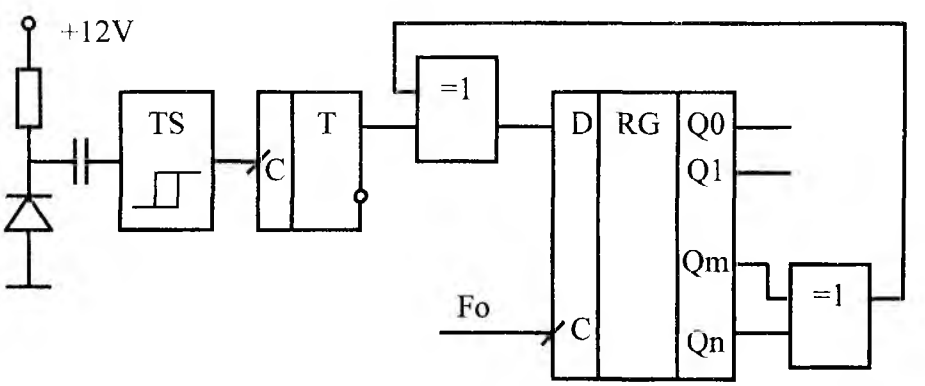

Рис. 6

Частота генерации случайных бит Fo может многократно превышать среднюю частоту датчика шума. Реально максимальное значение частоты Fo ограничено быстродействием элементов сдвигающего регистра и может превышать 100 МГц (для современных КМОП микросхем).

Для увеличения надежности генераторов случайных последовательностей методом "горячего резервирования" в схемы на рис. 4, 5 и 6 необходимо ввести многоканальные формирователи случайных битов [1].

Применение современных интегральных микросхем в значительной степени определяет массогабаритные параметры устройства. Генераторы случайных последовательностей реализованы на логических микросхемах средней степени интеграции микромощных серий ТТЛШ и сопряжением с каналом персонального компьютера через ISA-слот, а также на программируемых логических интегральных схемах (ПЛИС) и сопряжением через слот PCI.

Разработан программный драйвер для сопряжения формирователей с вычислительной системой и программы тестирования случайных последовательностей.

При тестировании генератора проверялось соответствие генерируемой случайной последовательности условиям:

- равновероятности с использованием критерия Пирсона;
- случайности по критерию серий;
- некоррелированности по коэффициентам корреляции разрядов байтов случайной последовательности;
- независимости по методу сопряженности признаков;
- однородности по методу проверки гипотезы о совпадении распределений.

Результаты экспериментальных исследований подтвердили равновероятный закон распределения генерируемых случайных последовательностей.

Экспериментально проверена эффективность горячего резервирования для двух каналов генерации случайных битов. На вход элемента ИСКЛЮЧАЮЩЕЕ ИЛИ (см. рис. 3) вместо одного из каналов генерации случайных битов подавались:

- постоянные логические уровни "0" или "1";
- прямоугольный сигнал детерминированного генератора.

Тестирование выходных случайных последовательностей не выявили отклонений от равновероятного закона распределения во всех экспериментах.

Недостатком схем генераторов случайных последовательностей с сопряжением через ISA-слот или PCI-слот является необходимость разборки корпуса компьютера при инсталляции генератора (разборка компьютера в некоторых условиях эксплуатации не допускается).

Этот недостаток был устранен в генераторе случайных последовательностей с сопряжением через внешний COM-порт компьютера.

Значительно уменьшить габариты схемы удалось реализацией логических схем обработки случайных сигналов на однокристальном микроконтроллере.

Разработан программно-аппаратный комплекс генерации случайных последовательностей, который включает (рис. 7):

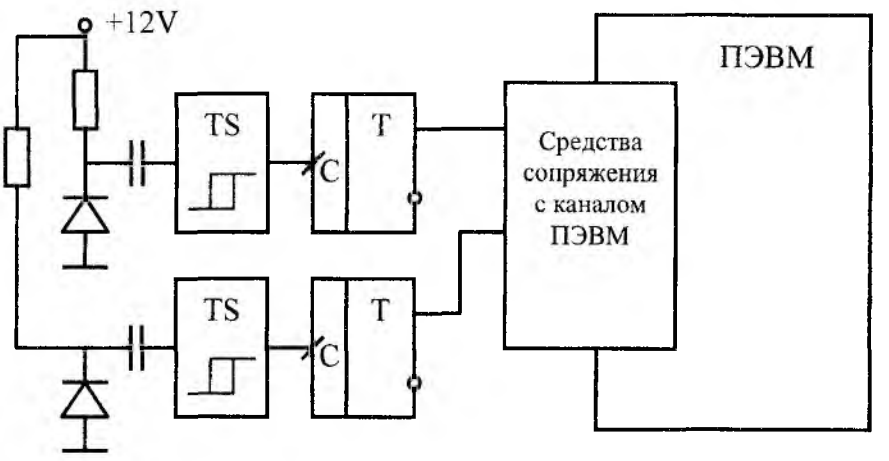

Рис.7

- два физических датчика случайного сигнала на основе шумовых диодов, работающих в режиме Зенеровского пробоя;
- два компаратора напряжения для преобразования аналоговых сигналов в логические уровни цифровых микросхем;
- два счетных триггера, преобразующих импульсы с выходов компараторов в сигналы, с равной вероятностью принимающие нулевые и единичные логические уровни;
- программно-аппаратные средства на основе однокристального микроконтроллера для сопряжения каналов формирования равновероятных битовых последовательностей с COM-портом ПЭВМ;
- программные средства для управления датчиком случайных последовательностей, его диагностики и тестирования.

Алгоритм функционирования такого генератора случайных последовательностей реализован на программном уровне в однокристальном микроконтроллере и полностью совпадает с логикой работы описанных генераторов. В этой схеме (см. рис. 7) также применяется "горячее резервирование" каналов формирования случайных битов.

Скорость генерации случайных последовательностей ограничена скоростью передачи COM-порта и составляет 9,6 Кбит/сек.

Тестирование случайных последовательностей на соответствие указанным выше условиям подтвердили равновероятный закон распределения. Экспериментально подтверждена эффективность "горячего резервирования" на случай отказа одного из генераторов шума.

Применение в формирователе случайных последовательностей микроконтроллеров позволяет реализовать на программно-аппаратном уровне средства защиты от несанкционированного доступа к аппаратным и программным ресурсам ПЭВМ.

Список литературы: **1**. *Патент Украины № 33361.* МКИ^{6} G 06F7/58, G 07C15/00. Генератор равномерно распределенных случайных чисел / *И.Д. Горбенко, А.А. Торба, С.Г. Елаков и др.* Опубл. Бюл. №1 от 15.02.2001. **2**. Заявка № 99116006 от 02.11.1999 (Решение на выдачу патента Украины от 26.05.2000). Способ генерации случайных чисел и устройство для его осуществления / *А.А. Торба.*

Харьковский государственный технический университет радиоэлектроники

Поступила в редколлегию 27.03.2001