ИНИЦИАЛИЗАЦИЯ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ В АВТОНОМНЫХ УСТРОЙСТВАХ

П. Л. Чечет
Кафедра автоматизированных систем обработки информации, Гомельский государственный университет имени Франциска Скорины
Гомель, Республика Беларусь
E-mail: pchechet@gsu.by

Существует большое число алгоритмов, использующих для своей работы датчики псевдослучайных чисел. Для повышения разнообразия генерируемых последовательностей псевдослучайных значений большую роль играет начальная инициализация датчиков (генераторов) псевдослучайных чисел. В автономных устройствах как правило, не так много возможностей для получения различных случайных значений, которые могут быть использованы для начальной инициализации датчиков псевдослучайных чисел. В данной работе рассмотрены некоторые приёмы получения начальных значений, что актуально для встраиваемых устройств и/или автономных устройств с ограниченным набором внешних аппаратных средств.

Введение

Во многих алгоритмах важным является наличие именно различных псевдослучайных последовательностей. Эта задача просто решается при работе алгоритма в полноценной вычислительной системе. В такой системе начальные значения для датчиков псевдослучайных чисел могут быть получены с использованием различных доступных из программы аппаратных средств. Чаще всего это часы реального времени и различные аппаратные счётчики. Но во многих автономных системах нет подобных устройств, в том числе устройство может включаться «по требованию» для снижения энергопотребления, что усложняет получение уникальных значений для различной инициализации датчиков псевдослучайных чисел при каждом запуске.

I. Сложности получения начальных значений

Встроенные автономные устройства часто функционируют без полноценной операционной системы, а так же часто не имеют в своём составе часов реального времени. Поэтому возможности для получения начальных значений для инициализации датчиков псевдослучайных чисел получаются ограниченными. Возможные варианты функционирования таких устройств приведены в таблице 1.

Таблица 1 – Варианты функционирования устройства

№ п.п	Питание	Выполнение алгоритма, требующего псевдослучайные числа
1	Постоянно	Постоянно
2	Постоянно	По запросу пользователя/ при наступлении события
3	Разово	По запросу пользователя/ при наступлении события

При постоянном функционировании устройства (варианты №№1 и 2 в таблице 1) возможна организация переполняемого счётчика времни работы устройства путём использования аппаратного таймера микроконтроллера, тактируемого с определённой частотой. В этом случае при выполнении задачи, требующей датчика псевдослучайных чисел, может быть считано текущее значение таймера и, непосредственно или путём преобразований (нормирование, разбиение на несколько значений сдвиговыми операциями и др.), это значение может быть использовано для начальной инициализации датчика псевдослучайных чисел. Это позволит получать в общем случае различные начальные значения и, следовательно, псевдослучайные последовательности, для каждого выполнения алгоритма.

II. Инициализация датчика при включении устройства

Сложнее задача получения значений в случае №3 (таблица 1). В этом случае устройство «не знает», в какое время оно было включено и задача получения различных начальных значений для инициализации датчиков псевдослучайных чисел усложняется. В качестве начальных значений в таком случае может быть использована, например, некоторая количественная информация об окружающей среде. Это может быть значение температуры, если устройство имеет соответствующий датчик, влажности, давления, освещения [1].

Если устройство взаимодействует с человеком, то появляется возможность использовать его физиологические показатели (реакция, скорость) для получения различных начальных значений для начальной инициализации датчиков псевдослучайных чисел. Даже при использовании устройства одним и тем же пользователем, числа будут получаться различными, так как физиологические характеристики одного и того

же человека непостоянны и зависят от множества факторов, а как отмечено в [2], значения такой системы имеют стохастическую природу.

III. Получение начальных значений по действию пользователя

Для практической проверки был реализован алгоритм получения числового значения, связанного со временем нажатия кнопки устройства. Схематично алгоритм работы программы микроконтроллера представлен на рисунке 1.

Рис. 1 – Упрощённая схема алгоритма

Устройство, реализованное с использованием микроконтроллера, находится в спящем (sleep) режиме, при котором все узлы микроконтроллера выключены, за исключением системы обработки внешних прерываний, что позволяет организовать пробуждение устройства нажатием кнопки. В практическом варианте, предназначенном для проверки функционирования этого способа получения начальных значений для инициализации датчика псевдослучайных чисел, алгоритм, использующий псевдослучайные числа, был заменён выводом в порт микроконтроллера полученного значения (рисунок 2).

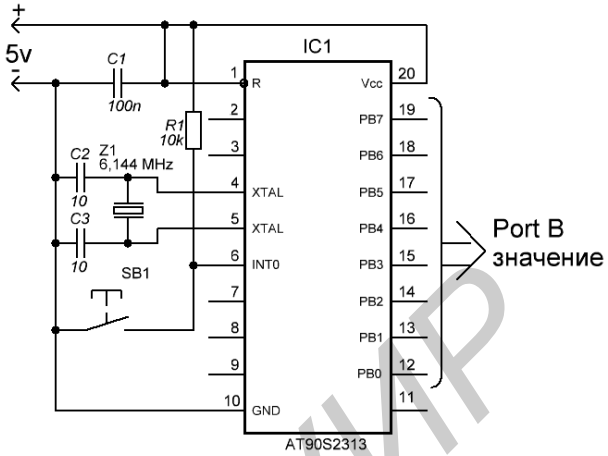

Рис. 2 – Схема включения микроконтроллера

Аппаратный таймер микроконтроллера сконфигурирован так, что его переполнение в процессе работы возникает с частотой примерно 94 Гц. Система прерывания микроконтроллера настроена на обработку переполнения таймера 0, что позволяет измерять время нажатия кнопки SB1 (рисунок 2), а так же выполнять отсчёт времени для выключения устройства путём перевода микроконтроллера в «спящий»режим с пониженным энергопотреблением. Числовое значение, полученное с помощью алгоритма (рисунок 1), выводится в порт B микроконтроллера (выводы 12–19, рисунок 2).

Для применения описанного здесь способа начальной инициализации датчиков псевдослучайных чисел в ответственных алгоритмах требуется провести дополнительные исследования числовой последовательности, получаемой данным способом. Не исключено, что значения, используемые для начальной инициализации датчиков псевдослучайных чисел, окажутся «недостаточно» случайными. Возможно, придётся откорректировать разрешающую способность таймера, или ввести дополнительные преобразования получаемых значений.

1. Чечет, П. Л. Аппаратно-программная реализация адаптивной яркости в устройствах отображения / П. Л. Чечет // Известия Гомельского государственного университета имени Ф. Скорины. – № 6(75), 2012. – С.128–133.
2. Приём шумоподобных сигналов на МК. – Режим доступа: http://nauchebe.net/2011/05/priyom-shumopodobnyx-signalov-na-mk/. – Дата доступа: 02.09.2015 г.