OSTIS-2011
(Open Semantic Technologies for Intelligent Systems)

УДК 62-83:621.3

СИСТЕМА ФАЗОВОЙ СИНХРОНИЗАЦИИ КАК ГЕНЕРАТОР ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Л.Ю. Шилин (*kaftoe@bsuir.by*)
Белорусский государственный университет информатики и радиоэлектроники, г.Минск, Республика Беларусь

Д.Л. Шилин (*dimashilin@gmail.com*)
Белорусский государственный университет информатики и радиоэлектроники, г.Минск, Республика Беларусь

Все чаще в качестве носителя информации используются хаотические процессы, что имеет ряд достоинств и недостатков[1]. Существуют различные способы ввода полной информации в хаотическую составляющую, но поскольку для хаотического сигнала отсутствует понятие амплитуды, то информационный сигнал может быть восстановлен только при помощи аналогично хаотического сигнала, что реализуется на основе синхронного хаотического генератора. При этом синхронизация генераторов может быть осуществлена внешним сигналом.

Основной задачей в этом случае выступает создание хаотического генератора с требуемыми техническими характеристиками [1]. Авторами предлагается использовать в качестве такого генератора систему фазовой синхронизации, работающую в режиме детерминированного хаоса.

Анализ режимов работы систем фазовой синхронизации (СФС) показывает, что при определенных параметрах системы в ней могут возникать специфические режимы работы – кратные захваты, NT-периодические и режимы детерминированного хаоса [2]. Эти режимы до сих пор рассматривались как нежелательные и при проектировании СФС определялись параметры, при которых системы находились в области устойчивости [2] и обеспечивали стабильную работу без возникновения нерабочих режимов.

На рис. 1 приведена обобщенная схема СФС, где ФД − фазовый детектор; ФК − цепи фильтрации и коррекции; ОУ − объект управления; ОС − цепь обратной связи.

Сигналы y(t) и u(t) − входной сигнал и сигнал обратной связи, могут быть аналоговыми, импульсными или цифровыми; что определяется частотным диапазоном, функциональным назначением и другими факторами при проектировании системы; ε(t) − сигнал фазового рассогласования; z(t), ω(t) − выходной сигнал без учета и с учетом возмущающего воздействия g(t). Математическая модель СФС построена для аналоговых и дискретных систем и описывает блоки ФК и ОУ в пространстве переменных состояния [3], фазовый детектор − набором неравенств или аналитическими функциями. Фазовый детектор и объект управления задаются в виде нелинейных элементов.

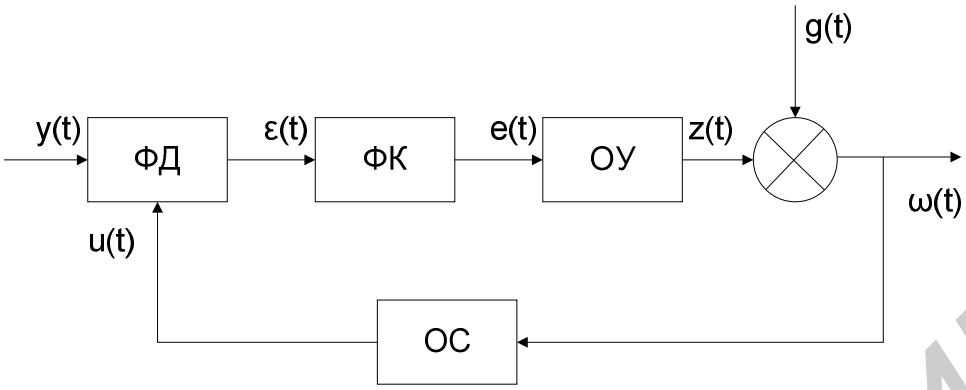

Рисунок 1 - Структурная схема СФС

Далее описывается СФС с разомкнутой петлей обратной связи системой разностно-итерационных уравнений, которая дополняется уравнением замыкания обратной связи:

$$\int_{nT+\tau_n}^{nT+kT+\tau_{n+k}} \varpi(t)dt = 2\pi jN \,, \qquad (1)$$

где

$$\varpi(t) = z(t) + g(t) \,,$$

nT – начало времени отсчета исследуемого интервала времени; τ_n – отрезок времени от nT до до момента, когда начальная фаза сигнала цепи ОС равна нулю; kT – время, в течении которого начальная фаза цепи ОС не достигла нуля; τ_{n+k} – отрезок времени, определяющий когда начальная фаза цепи ОС достигла 360□; T – период входного сигнала на исследуемом шаге; $N_д$ – коэффициент деления цепи ОС; j – целое число периодов выходного сигнала за анализируемое время.

Уравнение (1) является основным для всех типов СФС и определяет принцип моделирования. Разработанная модель позволяет определить области параметров системы, при которых разрабатываемая система устойчива. В зависимости от количества параметров математической модели рассматриваемого устройства области устойчивости имеют размерность равную количеству переменных. На границах этой области можно определить параметры, обеспечивающие режим детерминированного хаоса[2]. На рис. 2 приведен фазовый портрет СФС, представляющий собой странный аттрактор.

Авторами предлагается в качестве генератора псевдослучайных последовательностей использовать СФС в режиме детерминированного хаоса. Для того, чтобы убедиться в «случайности» генерируемой последовательности необходимо провести ряд тестов. Проверка была проведена при помощи: универсального алгоритма статистического тестирования; критерия Колмогорова-Смирнова; критерия частот; критерия интервалов; критерия монотонности; критерия максимум-t; критерия сериальной корреляции; критерия собирания купонов.

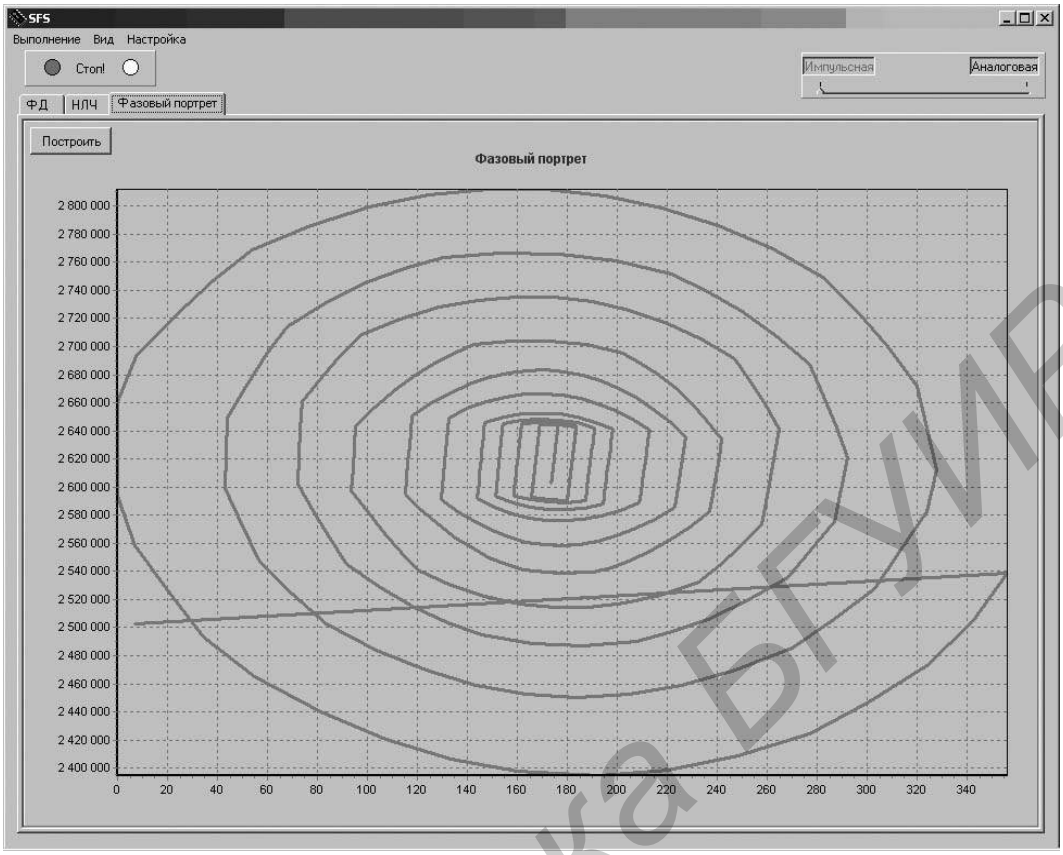

Рисунок 2 - СФС в режиме детерминированного хаоса

Для определения закона распределения последовательностей был построен группированный статистический ряд. Построение проводилось, как и принято в математической статистике, на основе подсчета частот встречаемости чисел, принадлежащих каждому из интервалов. Из гистограммы (рис. 3) сделан вывод о том, что распределение является равномерным. При тестировании количество элементов последовательности равнялось 5000.

Проведен анализ результатов тестирования и сделан вывод о том, что все тесты пройдены успешно, т. е. данный генератор псевдослучайных последовательностей может быть успешно использован в криптографировании для симметричной системы с открытым ключом.

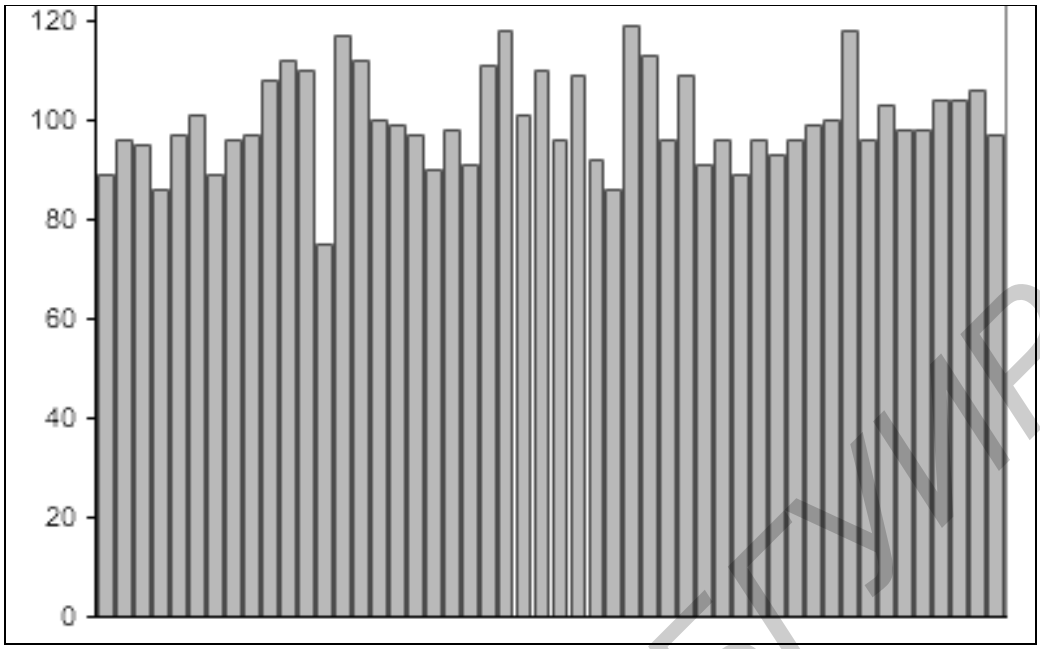

Рисунок 3 - Гистограмма последовательности случайных чисел, выдаваемых системой СФС

Библиографический список

1. Кононов А.Ф. Синтез систем передачи информации с хаотической несущей // Известия Южного федерального университета, 2008, т. 88, №11, с. 103-107.

2. Шилин Л.Ю., Шилин Д.Л. Анализ режимов работы импульсных систем фазовой синхронизации // Доклады БГУИР, 2008, №1, с. 22-28.

3. Кузнецов А.П., Батура М.П., Шилин Л.Ю. Анализ и параметрический синтез систем с фазовым управлением // Мн. Наука и техника, 1993. с. 224.