слежения. В качестве ФНЧ используются изодромное звено в основном контуре и пропорционально-интегрирующее звено в контуре управляемого генератора.

Приводятся результаты анализа математической модели по основным показателям качества и результаты моделирования. Определены требования к параметрам контуров слежения с целью обеспечения заданных показателей устойчивости, точности и быстродействия. Обеспечивая более высокие показатели точности по сравнению с системой с астатизмом первого порядка [1], анализируемая система более критична к выбору ФНЧ, удовлетворяющему требованиям устойчивости. В частности, ФНЧ в виде апериодического звена в контуре управляемого генератора не удовлетворяет этим требованиям.

**Литература**

1. Ганкевич С.А. Технические средства защиты информации: Тезисы докладов IX Белорусско-российской научно технической конференции, 28–29 июня 2011 г., Минск. Минск: БГУИР, 2011.С. 26.

## МЕТОДИКА ПОЛУЧЕНИЯ ИСТИННО СЛУЧАЙНЫХ ЧИСЕЛ ДЛЯ ЗАДАЧ ЗАЩИТЫ ИНФОРМАЦИИ

К.В. ГУБЧИК, А.А. ИВАНЮК

Последовательности случайных чисел (СЧ) являются необходимым инструментом решения многих задач защиты информации (протоколы аутентификации, генерация сессионных ключей, защита авторских прав и др.). В работе [1] был предложен метод реализации физически неклонируемой функции (ФНФ) на базе статического ОЗУ (СОЗУ), который основан на анализе начального состояния памяти при включении питающего напряжения. Недостаток разработанного метода: большинство ячеек СОЗУ принимают одно из состояний чаще, чем другое, поэтому нарушается требование непредсказуемости данного физического отпечатка [1]. Чтобы обойти эту проблему, предлагается методика использования сигнатуры памяти вместо физического отпечатка памяти. При этом, зная сигнатуру, практически невозможно предсказать исходный физический отпечаток памяти. Это происходит за счет сжатия с потерями исходной ЧП при помощи алгоритма формирования сигнатур (LFSR-анализатор, CRC-анализатор, адаптивный сигнатурный анализатор [2]). Полученная сигнатура может использоваться в качестве начального состояния генератора СЧ, когда не требуется высокой скорости генерации СЧ. Создание ГИСЧ (генератора истинно случайных чисел) является актуальной проблемой в областях защиты информации, т. к. в них требуются истинно случайные и невоспроизводимые числа, при этом сами генераторы должны обладать свойством неклонируемости как для различных технологий, так и для идентичных устройств, выполненных по единой технологии. В качестве источника случайности предлагается использовать сигнатуру состояния памяти, что позволит обеспечить высокие требования к качеству ЧП, формируемых при помощи ГИСЧ.

**Литература**

1. Holcomb D.E., Burleson W.P., Fu K. IEEE Transactions on Computers, September 2009. P. 1198–1210.

2. Иванюк А.А., Петроненко Д.С. Доклады БГУИР. 2004. № 4. С. 84–92.