Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.056.5

Кухаренко
Алексей Игоревич

Формирование случайных последовательностей для систем защиты информации

АВТОРЕФЕРАТ

на соискание степени магистра технических наук
по специальности 1-98 80 01 – Методы и системы защиты информации, информационная безопасность

_____

Научный руководитель
Давыдов Геннадий Владимирович
кандидат технических наук, доцент

_____

Минск 2015

КРАТКОЕ ВВЕДЕНИЕ

Современные информационные технологии широко используют последовательности случайных чисел в самых разных приложениях — от метода Монте-Карло и имитационного моделирования до криптографии и систем защиты информации. При этом от качества, недетерминированности, непредсказуемости случайных чисел напрямую зависит качество получаемых результатов. Поэтому качество является важнейшей и основной характеристикой случайных чисел.

Проблема создания генератора, формирующего последовательность абсолютно случайных чисел является весьма актуальной. Для ее решения применяются устройства, использующие источники энтропии на основе измеряемых параметров протекающего физического процесса, чаще всего шума.

В общем случае под шумовым сигналом понимается переменное напряжение или мощность, частотные и амплитудные параметры которых носят случайный характер. Первичными источниками шума (источниками энтропии) могут служить вакуумные и полупроводниковые шумовые диоды, фотоэлектронные умножители, газоразрядные приборы, а также лавинно-пролетные диоды, стабилитроны, туннельные диоды и ряд других.

Данная работа ставит целью изучить результаты имеющихся исследований, посвященных методам формирования и исследования последовательностей случайных чисел. Будут рассмотрены, основные этапы на пути к созданию генератора истинно случайных чисел, такие как генерация шумового сигнала, его усиление, избежание влияния внешних помех, оцифровка полученного сигнала, последующая обработка специальными алгоритмами и, наконец, контроль последовательности с помощью статистических тестов. Будет разработан и исследован модуль формирования случайных последовательностей на диоде и операционном усилителе, представляющий собой электронное устройство, которое применяется для генерации истинно случайных чисел с равномерным распределением, и передачи полученных чисел на персональный компьютер.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цели и задачи проводимых исследований. В системах защиты информации используются случайные последовательности для формирования ключей в различных алгоритмах шифрования. Основные требования к случайным последовательностям — это недетерминированность, непредсказуемость. Тема данной магистерской диссертации посвящается исследованию методов формирования истинно случайной последовательности чисел, а также способам проверки получаемых данных статистическими тестами. В работе рассматриваются шаги, необходимые для превращения шумового сигнала в поток случайных чисел, применимых для систем защиты информации. Поэтому целью настоящей работы стало создание методики формирования случайных последовательностей с использованием источника энтропии.

Для достижения поставленной цели в этой диссертации решены следующие задачи:

- разработан алгоритм и методика формирования случайных последовательностей на базе физического источника энтропии;
- разработан модуль формирования случайных последовательностей, представляющий собой электронное устройство, которое применяется для генерации истинно случайных чисел с равномерным распределением, и передачи полученных чисел на персональный компьютер посредством USB интерфейса;
- исследован модуль на качество формируемой случайной последовательности с помощью статистических тестов.

Личный вклад магистранта в выполненную работу. Работа полностью выполнена магистрантом на базе его исследований, начатых им будучи студентом БГУИР, в работе использовались электронные устройства, такие как тестовая плата или модуль формирования случайных последовательностей, созданные автором.

Результаты работы опубликованы в:

- тезисах докладов X Белорусско-российской научно-технической конференции, Минск 29-30 мая 2012 г;
- докладах XVIII Международной научно-технической конференции «Современные средства связи», Минск 15-16 октября 2013 г.;
- тезисах международной научно-техническая конференция, приуроченой к 50-летию МРТИ-БГУИР, Минск 18-19 марта 2014 г.

КРАТКОЕ СОДЕРЖАНИЕ

Работа состоит из введения, общей характеристики работы, трёх глав, заключения и приложения.

В первой главе «Обзор методов формирования и исследования случайных последовательностей чисел» рассмотрены публикации, посвященные методам формирования и исследования последовательностей случайных чисел. В разделе «Источники шумового сигнала для ГСЧ» рассматриваются методы и схемы создания источников энтропии, и в разделе «Обзор методик построения ГСЧ» описываются способы применения этих источников для формирования случайных чисел. Статистические тесты, помогающие удостовериться в случайности полученных чисел описаны в разделе «Методы исследования статистических характеристик случайных последовательностей».

Во второй главе «Разработка средств формирования случайных последовательностей» рассмотрены методы формирования шумового сигнала. В разделе «Методы получения источника энтропии» исследованы два варианта источника энтропии: на шумовом диоде и на операционном усилителе. Раздел «Разработка модуля формирования случайных последовательностей» описывает создание модуля, представляющего собой электронное устройство, которое применяется для генерации истинно случайных чисел с равномерным распределением, и передачи полученных чисел на персональный компьютер.

В третей главе «Исследование статистических характеристик модуля формирования случайных последовательностей» происходит исследование и проверка разработанного модуля. В первом разделе проверяется простой алгоритм генерирования случайной последовательности, на основе полученных результатов в разделе «Алгоритм обработки данных для формирования случайной последовательности» создается рабочий вариант алгоритма. В разделе «Исследование случайной последовательности полученной в результате обработки данных с источника энтропии» статистическим тестами NIST подверглась данные, полученные с модуля формирования случайных последовательностей.

ЗАКЛЮЧЕНИЕ

Результатами данной работы являются:

- проведённый обзор методов формирования и исследования последовательностей случайных чисел;
- разработана методика формирования случайных последовательностей на базе физического источника энтропии;
- разработан модуль формирования случайных последовательностей, представляющий собой электронное устройство, которое применяется для генерации истинно случайных чисел с равномерным распределением, и передачи полученных чисел на персональный компьютер посредством USB интерфейса;
- для модуля формирования случайных последовательностей был разработан алгоритм обработки данных, была разработана его блок-схема, реализован в программном коде и проверен результат работы алгоритма различными тестами;
- исследован модуль на качество формируемой случайной последовательности с помощью статистических тестов, в итоге проведённого исследования подтверждена случайность сгенерированной последовательности чисел.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

[1–А] Давыдов Г. В., Кухаренко А. И., Попов В. А., Тереня А. А. Аппаратный генератор случайных чисел // Тезисы докладов X Белорусско-российской научно-технической конференции, Минск 29-30 мая 2012 г.

[2–А] Давыдов Г. В., Кухаренко А. И., Сейткулов Е.Н. Оценка качества случайных последовательностей для формирования маскирующих речеподобных сигналов // Доклады XVIII Международной научно-технической конференции «Современные средства связи», Минск 15-16 октября 2013 г.

[3–А] Давыдов Г. В., Кухаренко А. И. Оценка качества случайных последовательностей статистическими тестами // Международная научно-техническая конференция, приуроченная к 50-летию МРТИ-БГУИР, Минск 18-19 марта 2014 г.