

Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Институт кибернетики

Направление подготовки: Стандартизация и метрология

Кафедра компьютерных измерительных систем и метрологии

БАКАЛАВРСКАЯ РАБОТА

Тема работы	
Аппаратный генератор случайных чисел для математического моделирования	
УДК 004.3	

Студент

Группа	ФИО	Подпись	Дата
8Г21	А.В. Букрина		

Руководитель

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент кафедры КИСМ	В.Ю. Казаков	Кандидат физико- математических наук		

КОНСУЛЬТАНТЫ:

По разделу «Финансовый менеджмент, ресурсоэффективность и ресурсосбережение»

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Старший преподаватель кафедры Менеджмент	А.В. Хаперская			

По разделу «Социальная ответственность»

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Ассистент кафедры ЭБЖ	И.Л. Мезенцева			

ДОПУСТИТЬ К ЗАЩИТЕ:

Зав. кафедрой	ФИО	Ученая степень, звание	Подпись	Дата
КИСМ	О.В. Стукач	Доктор технических наук, профессор		

Томск – 2016 г.

Министерство образования и науки Российской Федерации
 Федеральное государственное автономное образовательное учреждение
 высшего образования
**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
 ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Институт кибернетики
 Направление подготовки (специальность) Стандартизация и метрология
 Кафедра компьютерных измерительных систем и метрологии

УТВЕРЖДАЮ:
 Зав. кафедрой
 _____ О.В. Стукач
 (Подпись) (Дата) (Ф.И.О.)

ЗАДАНИЕ
на выполнение выпускной квалификационной работы

В форме:

бакалаврской работы

(бакалаврской работы, дипломного проекта/работы, магистерской диссертации)

Студенту:

Группа	ФИО
8Г21	А.В. Букриной

Тема работы:

Аппаратный генератор случайных чисел для математического моделирования	
Утверждена приказом директора (дата, номер)	от 11.02.2016 г., № 958/с

Срок сдачи студентом выполненной работы:	17.06.2016 г.
--	---------------

ТЕХНИЧЕСКОЕ ЗАДАНИЕ:

<p>Исходные данные к работе</p> <p><i>(наименование объекта исследования или проектирования; производительность или нагрузка; режим работы (непрерывный, периодический, циклический и т. д.); вид сырья или материал изделия; требования к продукту, изделию или процессу; особые требования к особенностям функционирования (эксплуатации) объекта или изделия в плане безопасности эксплуатации, влияния на окружающую среду, энергозатратам; экономический анализ и т. д.).</i></p>	<p>Техническое описание модуля Arduino; Драйвера к модулю Arduino; Язык программирования LabVIEW; Драйвер VISA программы LabVIEW.</p>
<p>Перечень подлежащих исследованию, проектированию и разработке вопросов</p> <p><i>(аналитический обзор по литературным источникам с целью выяснения достижений мировой науки техники в рассматриваемой области; постановка задачи исследования, проектирования, конструирования; содержание процедуры исследования, проектирования, конструирования; обсуждение результатов выполненной работы; наименование дополнительных разделов, подлежащих разработке; заключение по работе).</i></p>	<p>Выбор схемы аппаратного генератора шума; Выбор платы сбора данных для сопряжения генератора шума с персональным компьютером; Разработка программы для модуля Arduino; Разработка программы для персонального компьютера на LabVIEW с помощью драйвера VISA; Исследование статистических характеристик аппаратного генератора случайных чисел; Финансовый менеджмент, ресурсоэффективность и ресурсосбережение; Социальная ответственность.</p>

<p>Перечень графического материала <i>(с точным указанием обязательных чертежей)</i></p>	<p>Функциональная схема аппаратного генератора случайных чисел; Принципиальная схема генератора шума; Принципиальная схема модуля Arduino; Блок-схема программы для модуля Arduino; Лицевая панель и блок-схема программы на LabVIEW; Мультимедийная презентация в формате .pptx на __ слайдах</p>
---	--

Консультанты по разделам выпускной квалификационной работы
(с указанием разделов)

Раздел	Консультант
Финансовый менеджмент, ресурсоэффективность и ресурсосбережение	А.В. Хаперская
Социальная ответственность	И.Л. Мезенцева

Названия разделов, которые должны быть написаны на русском и иностранном языках:

Дата выдачи задания на выполнение выпускной квалификационной работы по линейному графику

Задание выдал руководитель:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент кафедры КИСМ	В.Ю. Казаков	Кандидат физико-математических наук		

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
8Г21	А.В. Букрина		

Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Институт кибернетики
Направление подготовки (специальность) Стандартизация и метрология
Уровень образования бакалавр
Кафедра компьютерных измерительных систем и метрологии
Период выполнения осенний / весенний семестр 2015/2016 учебного года

Форма представления работы:

бакалаврская работа

(бакалаврская работа, дипломный проект/работа, магистерская диссертация)

КАЛЕНДАРНЫЙ РЕЙТИНГ-ПЛАН
выполнения выпускной квалификационной работы

Срок сдачи студентом выполненной работы:	17.06.2016 г.
--	---------------

Дата контроля	Название раздела (модуля) / вид работы (исследования)	Максимальный балл раздела (модуля)
20.05.2016 г.	<i>Основная часть</i>	60
25.05.2016 г.	<i>Финансовый менеджмент, ресурсоэффективность и ресурсосбережение</i>	20
30.05.2016 г.	<i>Социальная ответственность</i>	20

Составил преподаватель:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент кафедры КИСМ	В.Ю. Казаков	Кандидат физико-математических наук		

СОГЛАСОВАНО:

Зав. кафедрой	ФИО	Ученая степень, звание	Подпись	Дата
КИСМ	О.В. Стукач	Доктор технических наук, профессор		

Реферат

Выпускная квалификационная работа 83 с., 21 рисунок, 20 таблиц, 31 источник, 1 приложение.

Ключевые слова: аппаратный генератор случайных чисел, генератор случайных чисел, шум, метод Монте-Карло.

Объектом исследования является аппаратный генератор случайных чисел.

Цель работы – разработка аппаратного генератора случайных чисел для компьютерного моделирования и анализ статистических характеристик полученных последовательностей чисел.

В процессе работы проводилось создание генератора случайных чисел в виде USB-устройства и анализ характеристик устройства и выходных данных.

В результате исследования был создан аппаратный генератор случайных чисел с программным обеспечением для персональных компьютеров, определены его характеристики.

Достигнутые технико-эксплуатационные показатели: генерация истинно случайных чисел с нормальным законом распределения.

Степень внедрения: данная разработка находится на этапе научно-исследовательских и опытно-конструкторских работ.

Эффективность использования разработанного устройства заключается в уменьшении методической ошибки математического моделирования методом Монте-Карло.

Данное устройство может применяться на персональных компьютерах для математического моделирования методом Монте-Карло.

Выпускная квалификационная работа выполнена в текстовом редакторе Microsoft Office Word 2007 и представлен в распечатанном виде на листах формата А4.

Определения

В данной работе применены следующие термины с соответствующими определениями:

случайное число: Число, представляющее собой реализацию случайной величины;

псевдослучайное число: Число, полученное в соответствии с заданным алгоритмом, используемое в качестве случайного числа;

физическое случайное число: Случайное число, полученное на основе некоторого физического явления;

аппаратный генератор случайных чисел: Устройство, которое генерирует последовательность случайных чисел на основе измеряемых, хаотически изменяющихся параметров протекающего физического процесса;

шум: Беспорядочные колебания различной физической природы, отличающиеся сложностью временной и спектральной структуры;

радиоэлектронный шум: Случайные колебания токов и напряжений в радиоэлектронных устройствах;

генератор шума: Генератор случайных непериодических сигналов для имитации реальных шумовых процессов;

метод Монте-Карло: Общее название группы численных методов, основанных на получении большого числа реализаций стохастического (случайного) процесса, который формируется таким образом, чтобы его вероятностные характеристики совпадали с аналогичными величинами решаемой задачи.

Обозначения и сокращения

ГСЧ – Генератор случайных чисел;

USB - Universal Serial Bus;

ГШ – генератор шума;

ПК – персональный компьютер;

АЦП – аналого-цифровой преобразователь;

МШУ – малошумящий усилитель.

Оглавление

	С.
Введение	14
1 Случайные числа. Метод Монте-Карло	16
1.1 Описание метода Монте-Карло и роль случайных чисел в данном методе	16
1.2 Примеры использования метода Монте-Карло	18
2 Шумы: классификация и характеристики	26
2.1 Понятие шума и его классификация	26
2.2 Статистические характеристики шумов	27
2.3 Генераторы шума: назначение и применение	30
3 Аппаратный генератор случайных чисел	34
3.1 Источник шума, аналоговая часть аппаратного ГСЧ	35
3.2 «DFRduino» - цифровая часть аппаратного ГСЧ	37
3.3 Программное обеспечение аппаратного ГСЧ	39
3.4 Статистический анализ полученных последовательностей случайных чисел	41
Заключение	79
Список использованных источников	80
Приложение А (справочное) Принципиальная схема устройства DFRduino Uno	83

Введение

В современном мире случайные числа играют важную роль в различных областях деятельности людей, таких как программирование, статистика, метрология, компьютерное моделирование, криптография и т.п. В частности, важной областью основанной на использовании последовательностей случайных чисел является компьютерное моделирование сложных систем.

Целая группа алгоритмов численного моделирования под общим названием «метод Монте-Карло» основана на использовании генераторов случайных чисел. Обычно применяются программные генераторы случайных чисел (ПГСЧ), которые позволяют получить псевдослучайные числа. Так как компьютер детерминированная система, то программно можно генерировать только последовательности чисел статистически «очень похожих» на случайные. Создание и испытание подобных алгоритмов является хорошо развитым разделом компьютерных наук. Тем не менее, общим недостатком подобных алгоритмов является то, что через определенное число шагов последовательность псевдослучайных чисел повторяется. Более сложные алгоритмы выдают более длинные последовательности до момента заикливания [1].

Альтернативой программной генерации случайных чисел является аппаратная генерация случайных чисел на основе различных физических явлений, например, тепловой шум резистора и другие типы шумов радиоэлектронной аппаратуры [2]. Для уменьшения методической ошибки результатов математического моделирования методом Монте-Карло возможно использование физических (аппаратных) генераторов случайных чисел.

Так как генераторы шума плохо сопрягаются с вычислительными системами, то возникает необходимость в создании легко сопрягаемого с компьютером аппаратного генератора случайных чисел. Такой генератор

позволит получить неограниченные последовательности случайных чисел с нужными характеристиками.

Целью данной работы является создание аппаратного генератора случайных чисел в виде USB-устройства, а так же анализ статистических свойств генерируемых последовательностей случайных чисел.

Для достижения поставленной цели были поставлены следующие задачи:

- изучение шумов и их статистических характеристик;
- изучение метода Монте-Карло в математическом моделировании;
- создание аппаратного генератора случайных чисел;
- написание программного обеспечения для данного устройства;
- анализ статистических характеристик полученных данных.

В первом разделе данной работы приведено описание метода Монте-Карло и примеры его использования для различных задач.

Во втором разделе рассматривается понятие шума, его классификация, а так же приведены статистические характеристики, которые применяются для анализа шума.

В третьем разделе приведено описание создания аппаратного генератора случайных чисел, разработка программ для функционирования данного устройства и анализ статистических характеристик полученных последовательностей чисел.

1 Случайные числа. Метод Монте-Карло

1.1 Описание метода Монте-Карло и роль случайных чисел в данном методе

Метод Монте-Карло используется для решения задач в различных областях физики, химии, математики, экономики, оптимизации, теории управления и др.

Изначально данный метод применялся для решения сложных задач нейтронной физики и теории переноса излучения, где обычные численные методы оказались неэффективными. После влияние данного метода распространилось на широкую область задач статистической физики, достаточно различных по своему содержанию. Метод используется для решения задач теории массового обслуживания, теории игр и математической экономики, задач теории передачи сообщений при наличии помех и т.д. [3].

Для решения задачи с помощью метода Монте-Карло необходимо построить вероятностную модель, представить искомую величину, например многомерный интеграл, в виде математического ожидания функционала от случайного процесса, который далее моделируется на компьютере. В результате проведения вычислительного эксперимента получают необходимую выборку, и результаты всех испытаний усредняют [4].

Достоинством методов Монте-Карло является простая схема вычислительного алгоритма. Трудность метода заключается в том, что нужна не любая, а достаточно достоверная оценка искомой величины, т.е. оценка с малой погрешностью. Добиться такого результата довольно трудно. Большую роль играет адекватность построенной вероятностной модели, которые известны во многих задачах.

Следующая важная составляющая – моделирование случайных величин с заданными распределениями. Такое моделирование реализуется путём преобразования одного или нескольких независимых

значений случайного числа a , распределённого равномерно в интервале от нуля до единицы. Последовательности «выборочных» значений a обычно получают на ЭВМ с помощью теоретико-числовых алгоритмов. Такие числа называются «псевдослучайными», они проверяются статистическими тестами и решением типовых задач. При использовании теоретико-числовых алгоритмов может возникнуть проблема заикливания программы ЭВМ, что приведет к повторению последовательностей чисел. Возникновение такой проблемы может привести к неверному результату моделирования. Для усовершенствования таких программ усложняют алгоритмы, увеличивают затраты времени на вычисления случайных чисел, но и это не гарантирует, что последовательности чисел не будут повторяться через некоторый интервал времени. Поэтому для математического моделирования методом Монте-Карло существенную роль играет качество используемых генераторов случайных чисел [5] .

Для наиболее достоверных результатов необходимо получать достаточно длинные последовательности случайных чисел со стабильными статистическими характеристиками и необходимым законом распределения. В таком случае применение аппаратных генераторов случайных чисел будет полностью оправдано.

2 Шумы: классификация и характеристики

Использование псевдослучайных чисел наиболее простой вариант, т.к. их можно сгенерировать на любом ПК с помощью специальной программы, но использование генераторов псевдослучайных чисел приводит к проблемам, которые были описаны ранее. Поэтому в качестве ГСЧ лучше использовать генераторы шума на основе физических явлений, что позволит уменьшить погрешность моделирования и получить наиболее достоверные результаты.

2.1 Понятие шума и его классификация

Беспорядочные колебания различной физической природы, отличающиеся сложностью временной и спектральной структуры, называются шумом.

Существуют разные, сложившиеся исторически, виды шумов: естественные и технические; аддитивные и мультипликативные.

Естественные шумы вызваны фундаментальными физическими причинами, например, дискретностью заряда электрона или диссипацией энергии. Технические шумы вызваны несовершенством технологии изготовления прибора. Сейчас термин «технический шум» практически не употребляется.

Аддитивным шумом является шум, обычно в токе, либо напряжении, статистические характеристики которого не зависят от напряжения, приложенного к прибору, либо протекающего через прибор тока. Например, аддитивным является тепловой шум, выделяющийся на резисторе.

Мультипликативный шум вызван флуктуациями параметров элемента и проявляется при приложении напряжения к этому элементу, либо пропускании через него электрического тока. Например, мультипликативную природу имеет шум, описываемый функцией $v(t)$, выделяющийся на резисторе, обладающем флуктуациями сопротивления [7].

Так же шумы имеют классификацию в зависимости от спектра: белый шум, розовый шум, черный шум и т.д.

2.2 Статистические характеристики шумов

Шумы являются случайными сигналами. Для них рассчитывают различные статистические характеристики такие, как: математическое ожидание, дисперсия, функция автокорреляции и спектральная плотность шума.

Представленные вероятностные характеристики являются основными характеристиками шума, которые обычно используют на практике. Они достаточно просто измеряются, и их значений достаточно для решения многих задач, связанных с шумами.

2.3 Генератор шума: назначение и применение

Генератором шума называют генератор случайных непериодических (шумовых) сигналов.

Генераторы шума применяются:

- в радиоэлектронике для определения коэффициента шума и предельной чувствительности радиоприемных устройств, помехоустойчивости систем автоматического регулирования и систем телеуправления и др.;
- в акустике для маскировки звуков при определении артикуляции, измерении времени реверберации помещений, коэффициента звукопоглощения различных материалов;
- в измерительной технике в качестве калиброванных источников мощности при измерении параметров случайных процессов (атмосферные помехи и др.), а так же применяются для проверки и настройки радиоэлектронных устройств, каналов связи, при поверке и калибровке средств измерений и других целей [9].

Генераторы шума (ГШ) являются источниками случайного шумового сигнала с нормированными статистическими характеристиками. В зависимости от значения верхней граничной частоты спектра шума ГШ подразделяются на низкочастотные (от нескольких Гц до нескольких МГц), высокочастотные (от нескольких МГц до сотен МГц) и сверхвысокочастотные (от сотен МГц до десятков ГГц). Основным узлом ГШ является первичный источник шума, в качестве которого в зависимости от диапазона частот используются тепловые шумы в резисторах, дробовый шум в электронных лампах, шумы плазмы в тиратронах, газоразрядных стабилитронах и др. Первичный шум усиливается и преобразуется в выходной сигнал с заданными параметрами. Атенюатор на выходе ГШ позволяет калибровать уровень шумового сигнала.

Работа генераторов шума основана на одном из двух физических принципов: использование естественных источников шумов и случайных импульсов, либо возбуждении стохастических автоколебаний.

На рисунке 6 изображена схема генератора шумовых сигналов.



Рисунок 6 – Схема генератора шумовых сигналов

Рассмотрим элементы данной схемы более подробно.

Задающий генератор, называемый часто первичным источником шума, является основным узлом, определяющим принцип действия прибора. Его сигналы должны иметь достаточно большой уровень напряжения во всей требуемой полосе частот, описываться заданными вероятностными характеристиками:

- законом распределения вероятностей;

- корреляционной функцией;
- дисперсией или среднеквадратическим отклонением.

Часто он вырабатывает сигналы, имитирующие белый шум. Работа задающего генератора шума основана на использовании физических явлений, при которых возникают достаточно интенсивные шумы со статистическими характеристиками, поддающимися расчету [10].

Преобразователями генераторов шумовых сигналов служат усилители, нелинейные преобразователи, фильтры.

Усилителям необходимо, чтобы они имели достаточно широкую полосу пропускания и возможность усиления сигналов со значительным отношением пикового значения напряжения к среднеквадратическому значению, т.е. они должны иметь амплитудную характеристику, которая будет линейна на значительных пределах.

Калиброванный аттенюатор является основным элементом схемы выхода. Он характеризуется определенными коэффициентами передачи, которые постоянны на всей полосе сигнала шума.

Для измерения уровня сигнала служат измерители средней мощности шума и квадратичные вольтметры, которые измеряют среднеквадратическое значение выходного напряжения прибора [12].

Такие генераторы шума достаточно трудно сопрягать с ПК, они, обычно, достаточно больших размеров и их использование не удовлетворяют нашим требованиям в компактности и простого сопряжения с компьютером. Поэтому необходимо иметь аппаратный ГСЧ на базе источника шума, который будет удовлетворять данным условиям.

3 Аппаратный генератор случайных чисел

Для аппаратной генерации случайных чисел с заданным законом распределения и со стабильными статистическими характеристиками необходимо использовать некое физическое явление. В нашем случае это будет шум со стабилитрона. Структурная схема проектируемого USB-устройства, генерирующего случайные числа, приведена на рисунке 7.



Рисунок 7 – Структурная схема аппаратного ГСЧ

Устройство аппаратного генератора случайных чисел в основном состоит из четырех блоков: источник шума, микроконтроллер, USB-интерфейс и ПК.

В роли источника шума используется шум со стабилитрона, который возникает на приближении напряжения к напряжению пробоя стабилитрона. Такой шум необходимо усиливать с помощью операционных усилителей, т.к. значения шума в стабилитроне очень малы. Далее уже усиленный шум поступает на микроконтроллер. С помощью АЦП микроконтроллера осуществляется преобразование аналогового сигнала в цифровой код. В нашем случае шумовые напряжения преобразуются в случайные числа от 0 до 1024. Далее этот цифровой код поступает на ПК с помощью USB-интерфейса и отображается на экране посредством программы для отображения данных.

Рассмотрим каждый блок структурной схемы USB-генератора случайных чисел подробнее.

3.1 Источник шума, аналоговая часть аппаратного ГСЧ

Для разработки аналоговой части аппаратного ГСЧ в качестве генератора шума использовался стабилитрон, т.к. он наиболее устойчив к внешним воздействиям (например, к температуре) и образует стабильный шум на определенном участке вольтамперной характеристики.

Стабилитрон – обратнo-смещённый диод с р–n переходом. Если к нему приложить обратное напряжение U_{th} , то в р–n переходе возникает лавинный пробой. Протекающий ток через стабилитрон контролируется только внешней цепью, а напряжение U на нем остаётся почти неизменным, т.е. $U \approx U_{th}$. С помощью этого явления создают стабилизаторы напряжения [7].

Генератор шума на стабилитроне основан на явлении лавинного пробоя стабилитрона. Шум создается, когда PN-переход работает в режиме обратного пробоя. В первоначальной стадии пробоя процесс ударной ионизации является недостаточно устойчивым: ударная ионизация возникает, затем она срывается, после чего возникает вновь в тех местах перехода, где обнаруживается в данный момент времени достаточная напряженность электрического поля. Таким образом, шумы являются результатом случайной неравномерности генерации новых носителей заряда при ударной ионизации, которые характерны для определенного диапазона токов.

Таким образом, в качестве генераторов шума можно использовать обратнo-смещенные диоды в диапазоне обратных токов (от минимального до максимального пробивного тока). В таких диапазонах наблюдается наибольшая интенсивность электрических колебаний [13].

Шум от лавинного пробоя очень похож на дробовой шум, но гораздо более интенсивный и имеет широкий частотный спектр (белый). Величину шума трудно предсказать из-за своей зависимости от материалов.

Как уже было сказано ранее, в качестве источника шума был использован шум со стабилитрона. Данный блок будем называть аналоговой частью устройства. Принципиальная схема источника шума приведена на рисунке 8.

Рассмотрим данную схему подробнее. Два малошумящих усилителя (МШУ) в каскаде усиления шума, производимого в обратном смещении стабилитрона, работающего в режиме пробоя перехода, производя белый шум с полосой пропускания несколько сотен мегагерц. Результаты показывают, что довольно широкополосный белый шум может быть сгенерирован с помощью нескольких недорогих компонентов.

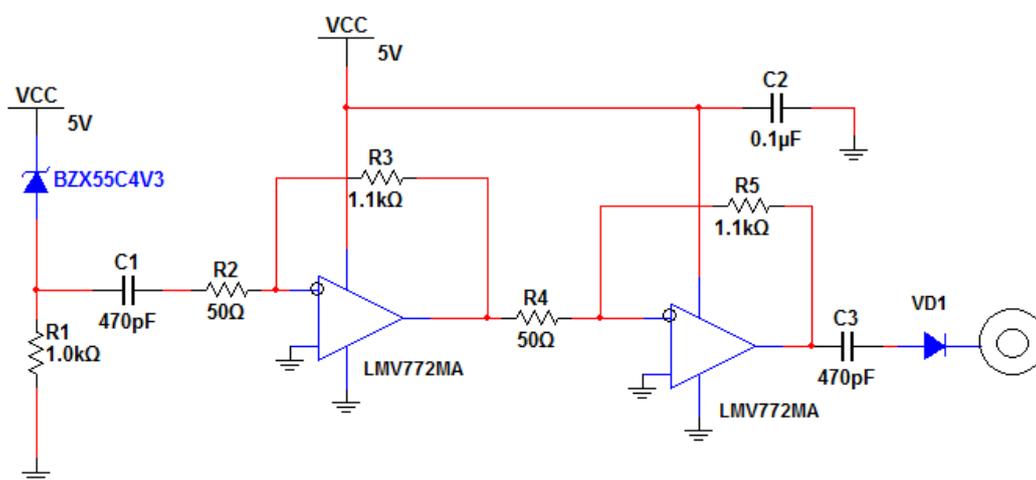


Рисунок 8 – Принципиальная схема источника шума

В основном схема состоит из двух частей: стабилитрон и малошумящие усилители (МШУ). Стабилитрон смещен в обратном направлении, и выходной шум берется из анода [14].

На входе операционного усилителя сигнал имеет очень маленькое значение. Максимальное значение напряжения шума около 10 мВ. Чтобы на выходе получить значения в диапазоне от нуля до пяти вольт необходимо усилить сигнал в 500 раз и оставить только положительную составляющую сигнала. Коэффициент усиления каждого операционного усилителя составляет примерно 22, а общий коэффициент усиления получаем близкий к

500. В конце схемы поставили диод для того, чтобы получить на выходе только положительную часть сигнала в диапазоне от нуля до пяти вольт.

Для данной схемы был взят стабилитрон BZX55C4V3. Данный стабилитрон имеет следующие характеристики: мощность рассеяния 0,5 Вт, минимальное напряжение стабилизации 4 В, номинальное – 4,3 В, а максимальное – 4,6 В. Статическое сопротивление 75 Ом при токе 5 мА, рабочая температура от минус 55 до 200 °С [15].

Так же был использован сдвоенный операционный усилитель LMV772MA со следующими характеристиками: максимальное напряжение питания 5,5 В, минимальное – 2,7 В. Произведение коэффициента усиления на ширину полосы пропускания (fT) равное 3,5 МГц, скорость нарастания выходного напряжения 1,4 В/мкс, входное напряжение смещения нуля 1 мВ, рабочий ток источника питания 1,9 мА, рабочая температура от минус 40 до 125 °С [16].

Данная схема была собрана на обычной макетной плате. Фотография аналоговой части аппаратного ГСЧ представлена на рисунке 9.



Рисунок 9 – Аналоговая часть аппаратного ГСЧ

3.2 «DFRduino» - цифровая часть аппаратного ГСЧ

Аналоговая часть аппаратного ГСЧ подключается к универсальной платформе DFRduino для преобразования и передачи информации на ПК.

Для блоков структурной схемы «микроконтроллер» и «USB-интерфейс» использовалась универсальная платформа DFRduino Uno 3.0, внешний вид которой показан на рисунке 10.

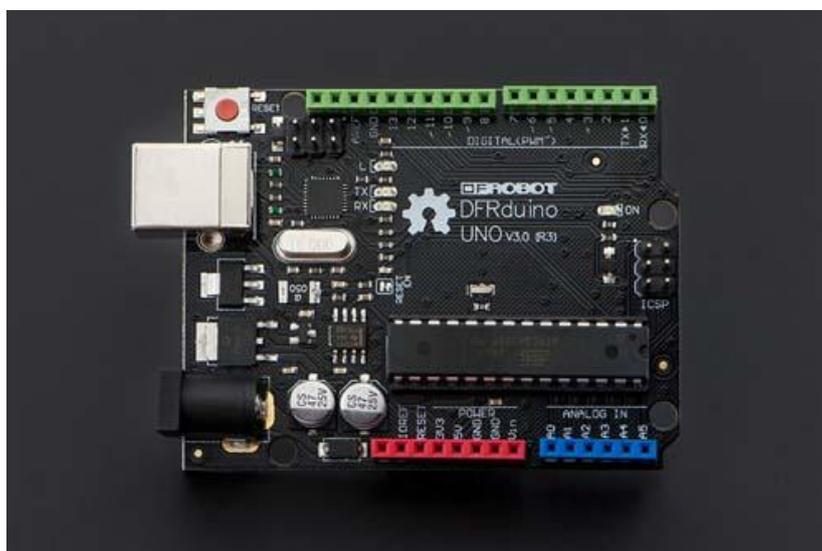


Рисунок 10 – Внешний вид платы DFRduino Uno 3.0

Данная платформа построена на микроконтроллере ATmega328. Эта платформа имеет кнопку перезагрузки, 14 цифровых входов и выходов, 6 аналоговых входов, кварцевый генератор с частотой 16 МГц, силовой разъем, USB разъем, разъем программатора (ICSP). Для работы платформы необходимо подключить ее к компьютеру через USB-порт, либо подключить альтернативный источник питания, например, при помощи адаптера AC/DC или батареи.

Любой цифровой вывод данной платформы может быть настроен как вход или выход. Для этого необходимо использовать специальные функции программирования `pinMode()`, `digitalWrite()` и `digitalRead()`. Для питания выводов необходимо напряжение 5 В. На каждом выводе имеется нагрузочный резистор, который по умолчанию отключен. Номинал таких резисторов 20-50 кОм и они могут пропускать ток до 40 мА.

Аналоговые входы платформы имеют разрешение 10 бит, т.е. они могут принимать 1024 различных значения. Выводы платформы имеют диапазон измерения до 5 В относительно земли, но данный диапазон можно

изменить с помощью вывода AREF и функции программирования analogReference() [17].

Принципиальная схема данной платформы приведена в приложении А.

Данная часть устройства – цифровая часть. На нее поступает аналоговый сигнал, с помощью специальной программы для микроконтроллера преобразуется в цифровой код и далее передается на ПК, где посредством программы для данного устройства можно будет увидеть сгенерированные случайные числа.

3.3 Программное обеспечение аппаратного ГСЧ

Для отображения на ПК информации с аппаратного ГСЧ необходимо разработать специальную программу. В ходе работы были разработаны две программы: одна программа для программирования микроконтроллера на выполнение преобразования и вторая – для отображения информации на ПК.

Программа для микроконтроллера написана на упрощенном языке Си в среде разработки Arduino. Суть программы заключается в пропорциональном преобразовании аналогового сигнала в цифровой код, т.е. значения напряжения, поступающие на вход АЦП, пропорционально соотносятся значениям от 0 до 1023. Данный диапазон можно изменять в самой программе. После этого цифровой код поступает на ПК, где он отображается с помощью второй программы.

Рассмотрим листинг программы для микроконтроллера с соответствующими пояснениями.

```
int outputVariable = 0;    // значение переменной выхода 0
int inputVariable = 0;    // значение переменной входа 0
void setup() {
  Serial.begin(9600);     // задаем скорость передачи на ПК
}
void loop()
{
  inputVariable = analogRead(2); // считываем аналоговый сигнал с
  порта 2
```

```

outputVariable = map(inputVariable, 0, 1023, 0, 255); // пропорционально переносим
значение аналогового сигнала из текущего диапазона в заданный
Serial.println(outputVariable); // вывод значений на ПК
delay(1000); // повторение через 1 сек.
}

```

Алгоритм данной программы следующий: инициализируем две целочисленные переменные для входного и выходного значения. Затем задаем скорость передачи данных на ПК с помощью команды `Serial.begin()`. После этого с аналогового входа считывается сигнал, пропорционально преобразуется в значения заданного диапазона и полученные значения передаются на ПК с задержкой равной одной секунде. Далее с помощью USB данные передаются в компьютер и обрабатываются следующей программой.

Программа для отображения информации с аппаратного ГСЧ написана в среде разработки LabVIEW. Суть программы заключается в том, что она регистрирует данные, которые поступают в USB-порт ПК и отображает их в специальном окне. Так же в этой программе ведется динамическое построение гистограммы для входных данных. Это необходимо для определения закона распределения случайной последовательности, что позволит оценивать ее статистические характеристики. Лицевая панель данной программы представлена на рисунке 11.

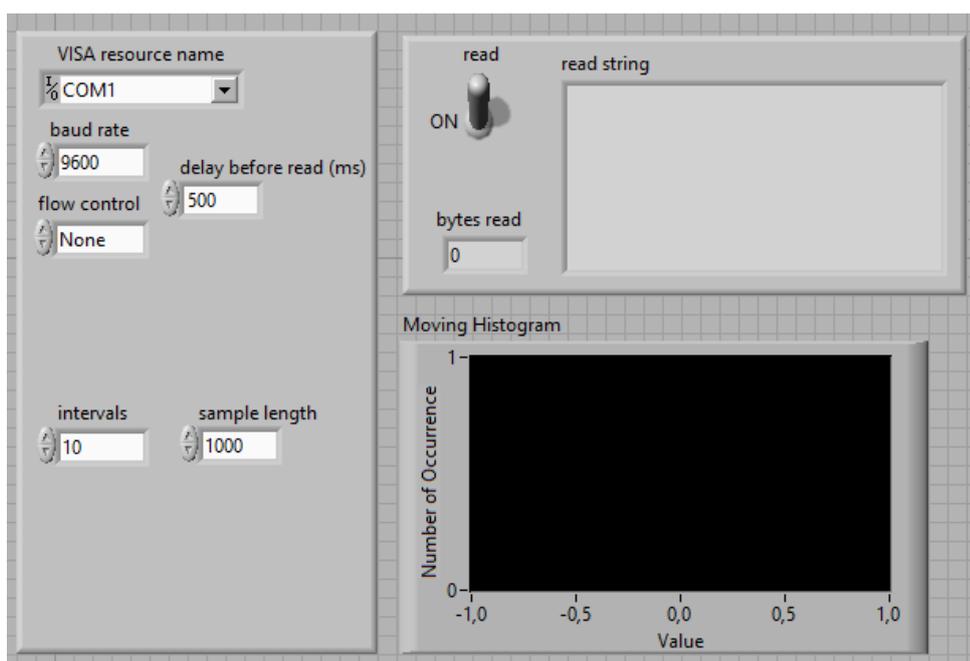


Рисунок 11 – Лицевая панель программы для отображения данных

На данной панели представлены следующие элементы: верхнее окно, работа которого начинается после нажатия рычага «read», отображает полученные данные в виде последовательностей чисел и показывает количество считанных бит информации. В нижнем окне отображается гистограмма, которая строится по полученным значениям в динамическом режиме. На левой панели можно выбирать, с какого COM-порта считывать информацию, а так же выбирать скорость считывания и задержку. Для гистограммы выбираются такие параметры, как количество интервалов группирования и количество значений, по которым строится гистограмма.

Блок-схема данной программы приведена на рисунке 12.

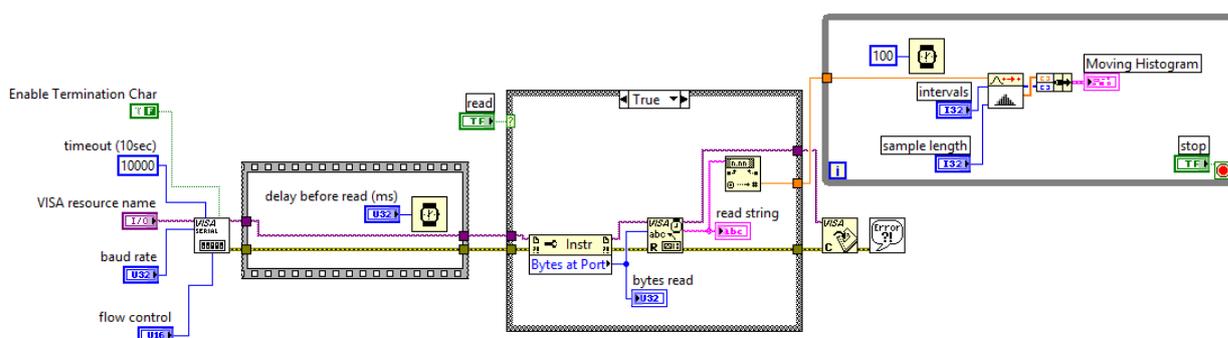


Рисунок 12 – Блок-схема программы для отображения данных

Для данной программы использовались следующие блоки: блок работы с COM-портами VISA Configure Serial Port, блоки задержки Wait, блок считывания VISA Read, блок закрытия VISA Close, блок мониторинга ошибок Simple Error Handler, блок построения гистограммы Histogram, а так же кнопки запуска и остановки программы. Так же использовались структура Case, цикл для построения динамической гистограммы While и Stacked Sequence Structure для управления порядком выполнения узлов данных, независимых друг от друга.

3.4 Статистический анализ полученных последовательностей случайных чисел

Как уже было сказано ранее, аппаратный ГСЧ основан на обработке шума со стабилитрона. Изображение осциллограммы полученного шума со стабилитрона приведено на рисунке 13.

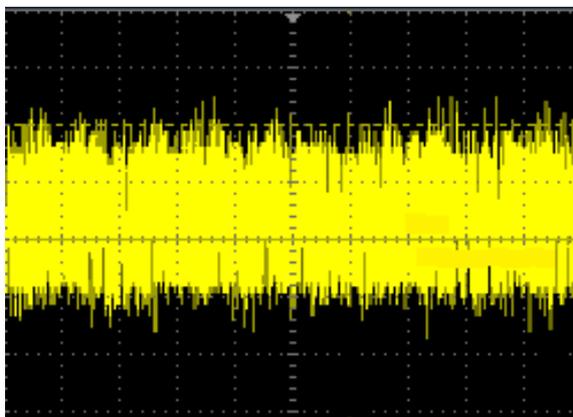


Рисунок 13 – Осциллограмма шума

Данный сигнал содержит 4000 выборок с периодом дискретизации $\Delta t = 2,5$ мкс. Для построения гистограмм было использовано 13 интервалов группирования. Данное значение было получено путем расчета по формуле Стёрджеса для оптимального количества интервалов.

$$k = 1 + 3,32 \lg N = 1 + 3,32 \lg 4000 = 13. \quad (23)$$

На рисунке 14 представлена гистограмма шума со стабилитрона. Из гистограммы можно предположить, что данный шум не является равномерным. Можно заметить, что гистограмма имеет три пика в разных областях.

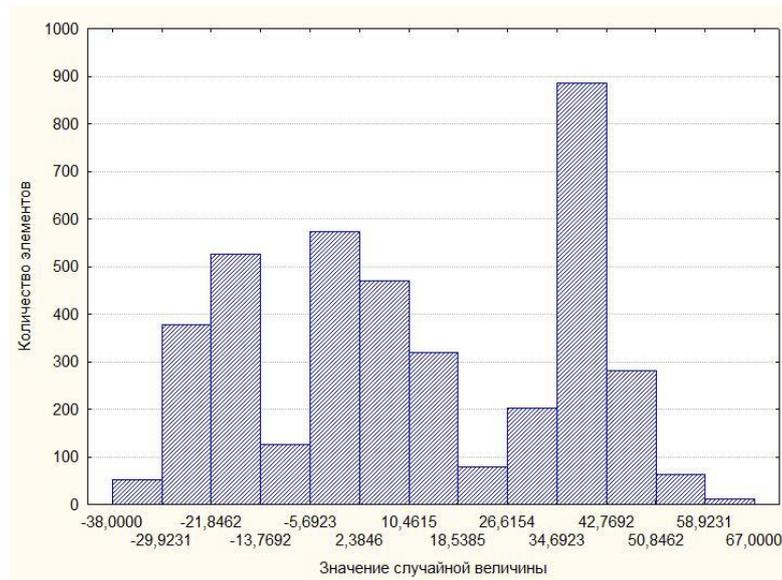


Рисунок 14 – Гистограмма для $\Delta t = 2,5 \mu\text{s}$

Далее рассмотрим, как будет изменяться закон распределения шума при изменении периода дискретизации, т.е. будем производить фильтрацию сигнала (рассмотрим быстроизменяющийся сигнал, медленно изменяющийся сигнал).

Построим гистограмму по полученным значениям с периодом дискретизации $\Delta t = 62,5 \mu\text{s}$, т.е. будем получать числа с медленно изменяющегося сигнала. Полученная гистограмма представлена на рисунке 15.

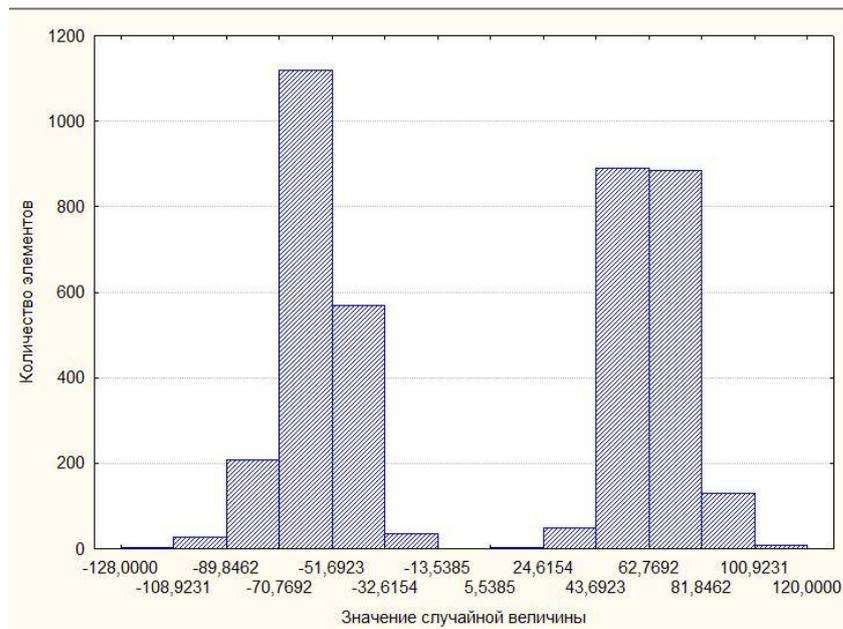


Рисунок 15 – Гистограмма полученных значений для $\Delta t = 62,5 \mu\text{s}$

На данной гистограмме можно увидеть, что случайные числа сосредоточены в верхней и нижней области осциллограммы. Таким образом, изменения значений напряжения происходят в верхней и нижней части осциллограммы, а в центре изменений не наблюдается. Это говорит о том, что при данных условиях происходит некий периодический процесс.

На рисунке 16 изображена гистограмма, построенная с помощью значений, полученных с периодом дискретизации $\Delta t = 2,5$ мкс.

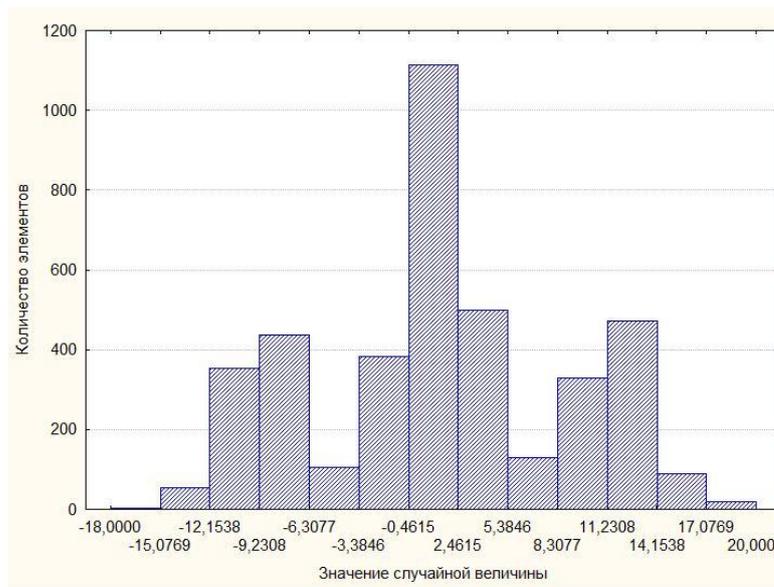


Рисунок 16 – Гистограмма полученных значений для $\Delta t = 2,5$ мкс

Из данной гистограммы можно увидеть, что с периодом дискретизации $\Delta t = 2,5$ мкс не имеем никакого определенного распределения в общем, но, как и на предыдущей гистограмме, видим области с пиками.

Уменьшим период дискретизации получения случайных чисел до 12,5 нс. Получим следующую гистограмму, представленную на рисунке 17.

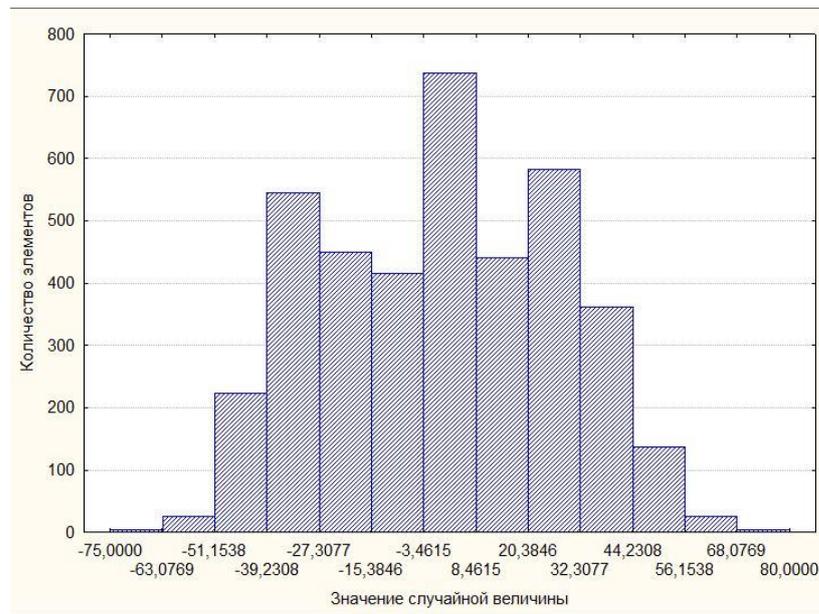


Рисунок 17 – Гистограмма полученных значений для $\Delta t = 12,5$ нс

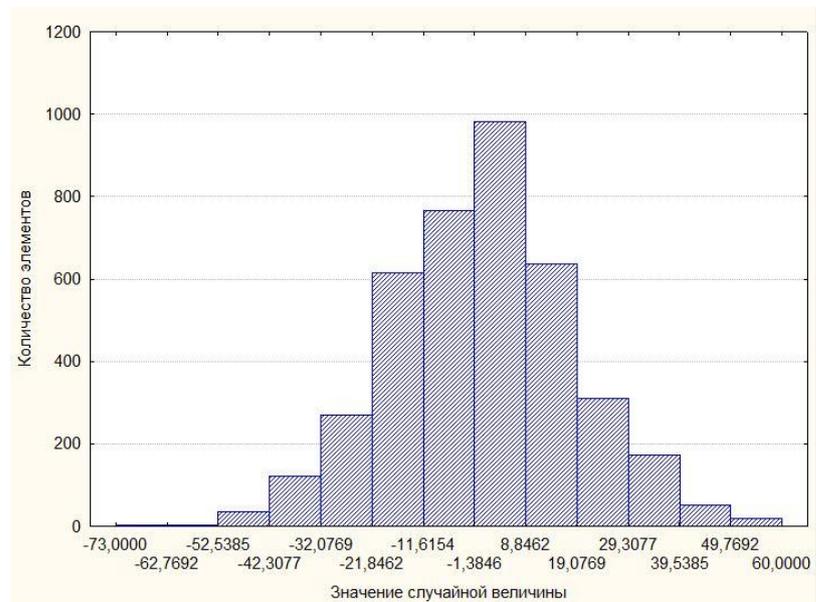


Рисунок 18 – Гистограмма полученный значений для $\Delta t = 6,25$ нс

При периоде дискретизации получения случайных чисел равным 6,25 нс видим, что числа распределены по закону близкому к нормальному закону.

Далее построим гистограмму значений полученных с периодом дискретизации равным 12,5 пс. Полученная гистограмма представлена на рисунке 19.

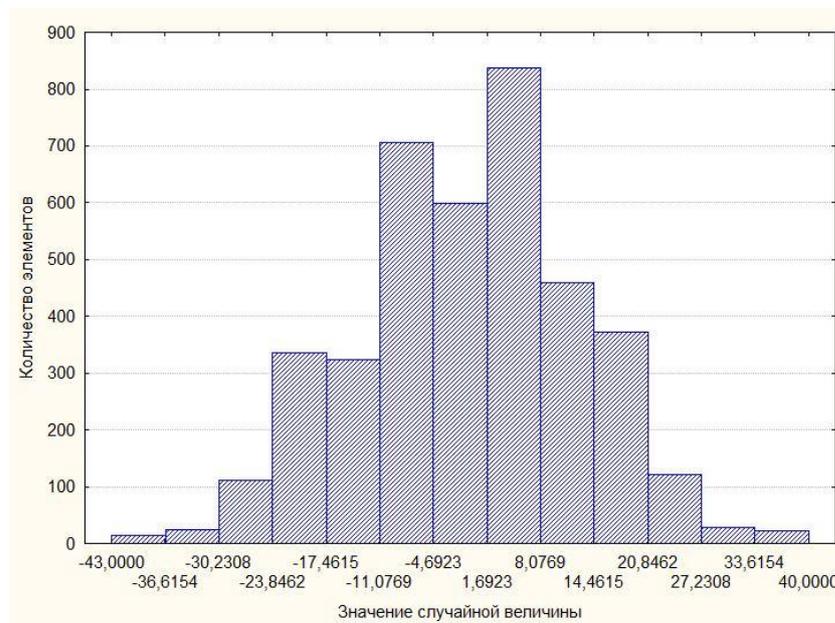


Рисунок 19 – Гистограмма полученных значений для $\Delta t = 12,5$ пс

На данной гистограмме видим, что закон распределения случайных чисел так же близок к нормальному закону.

Из всего вышесказанного можно говорить о том, что при изменении времени получения случайных чисел, меняется и их закон распределения. При получении случайных чисел с быстроизменяющегося сигнала они распределены по закону близкому к нормальному, а при медленно изменяющемся сигнале – закон распределения близок к синусоидальному закону распределения.

Для генерации действительно случайных чисел необходимо, чтобы они были распределены по равномерному закону, но в нашем случае получилось, что они распределены по нормальному закону. Основным условием является то, чтобы закон распределения случайных чисел был стабильный. При необходимости случайные числа с нормальным законом распределения можно преобразовать в числа с равномерным законом.

После получения последовательностей сгенерированных случайных чисел наряду с построением гистограмм необходимо провести и другие статистические тесты, которые позволят нам оценить качество полученных случайных чисел. Например, для таких целей существуют тесты diehard.

Тесты diehard – это набор статистических тестов для измерения качества набора случайных чисел. Они были разработаны Джорджем Марсальей. Вместе они рассматриваются как один из наиболее строгих существующих наборов тестов.

Данные тесты уже написаны на различных языках программирования, и их использование позволит определить качество полученных последовательностей случайных чисел с помощью аппаратного ГСЧ. Проверка по данным тестам будет проводиться на следующем этапе данной работы.

Заключение

В ходе выполнения выпускной квалификационной работы было собрано USB-устройство для генерации последовательностей физических случайных чисел, которые можно использовать для качественного и наиболее точного математического моделирования методом Монте-Карло. Данное устройство основано на преобразовании радиоэлектронного шума стабилитрона в цифровой код, а точнее, в последовательность чисел в диапазоне от нуля до 1024. Данный интервал изменяется посредством программы, которая загружается в микроконтроллер.

Для достижения поставленной цели в полной мере были решены следующие задачи:

- изучение шумов и их статистических характеристик;
- изучение использования метода Монте-Карло в математическом моделировании;
- создание аппаратного генератора случайных чисел;
- написание программного обеспечения для полученного устройства;
- анализ статистических характеристик данных с аппаратного ГСЧ.

Данное устройство можно использовать на любом ПК для генерации последовательностей случайных чисел, которые можно использовать в необходимых целях пользователя. Случайные числа, полученные с помощью аппаратного ГСЧ, позволят получать достаточно близкие к реальности результаты математического моделирования различных стохастических процессов. Так же он достаточно удобен и прост в использовании.

В дальнейшем планируется провести проверку полученных случайных чисел с помощью тестов diehard и на основе этих тестов определить качество и статистические характеристики полученных последовательностей чисел.

Список использованных источников

- 1 Жалуд В., Кулешов В.Н Шумы в полупроводниковых устройствах. – М.: Сов.радио, 1977. – 416 с.
- 2 Димаки А.В., Светлаков А.А. Аппаратно-программный генератор случайных чисел, сопрягаемый с компьютером типа IBM PC. – Томск, Известия Томского политехнического университета №1, 2004. – 144-148 с.
- 3 Большая Советская Энциклопедия. [Электронный ресурс]. – URL: <http://bse.sci-lib.com/> – Загл. с экрана (дата обращения 22.02.2016 г.)
- 4 Соболев И. М. Численные методы Монте-Карло – Москва, 1973. – 305 с.
- 5 Мееров И.Б. Введение в методы Монте-Карло: лекционные материалы. – Нижний Новгород: Нижегородский государственный университет им. Н.И. Лобачевского, 2005 – 24 с.
- 6 Склярова Е.А. Общий физический практикум: лекционные материалы. [Электронный ресурс]. – URL: <http://portal.tpu.ru/SHARED/s/SKEA/studentu> – Загл. с экрана (дата обращения 18.04.2016 г.)
- 7 Якимов А.В. Физика шумов и флуктуаций параметров: Электронное учебное пособие. – Нижний Новгород: Нижегородский госуниверситет, 2013. – 85 с.
- 8 Степанов А.В. Электрические шумы – Москва: Московский государственный университет им. М.В. Ломоносова, 2003. – 29 с.
- 9 Большой энциклопедический политехнический словарь, 2004. – 656 с.
- 10 Дьяконов В. П. Генерация и генераторы сигналов — Москва: ДМК Пресс, 2009. – 384 с.
- 11 Аналоговые измерительные устройства. [Электронный ресурс]. – URL: <http://analogiu.ru/9/9-6.html> – Загл. с экрана (дата обращения 20.02.2016 г.)
- 12 Генераторы шумовых сигналов. [Электронный ресурс]. – URL: <http://radioelpribori.ru/generatoryi-shumovyyih-signalov.html> – Загл. с экрана (дата обращения 21.02.2016 г.)
- 13 Букингем М. Шумы в электронных приборах. М.: Изд. ин. лит., 1986.

14 Building a Low-Cost White-Noise Generator. [Электронный ресурс]. – URL: <https://www.maximintegrated.com/en/app-notes/index.mvp/id/3469> – Загл. с экрана (дата обращения 20.02.2016 г.)

15 BZX55C4V3 datasheet. [Электронный ресурс]. – URL: <https://www.fairchildsemi.com/datasheets/BZ/BZX55C3V6.pdf> – Загл. с экрана (дата обращения 20.04.2016 г.)

16 LMV772MA datasheet. [Электронный ресурс]. – URL: <http://www.alldatasheet.com/datasheet-pdf/pdf/87458/NSC/LMV772MA.html> – Загл. с экрана (дата обращения 4.04.2016 г.)

17 Arduino Uno datasheet. [Электронный ресурс]. – URL: <http://arduino.ru/Hardware/ArduinoBoardUno> – Загл. с экрана (дата обращения 13.03.2016 г.)

18 Тесты diehard. [Электронный ресурс]. – URL: http://moscow.pink/testi-diehard_1259542.html – Загл. с экрана (дата обращения 30.05.2016 г.)

Приложение А (справочное)

Принципиальная схема устройства DFRduino Uno

