РУХАНИ ЖАҢҒЫРУ

20 АСТАНА

ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Студенттер мен жас ғалымдардың
«ҒЫЛЫМ ЖӘНЕ БІЛІМ - 2018»
XIII Халықаралық ғылыми конференциясы

СБОРНИК МАТЕРИАЛОВ

XIII Международная научная конференция
студентов и молодых ученых
«НАУКА И ОБРАЗОВАНИЕ - 2018»

The XIII International Scientific Conference
for Students and Young Scientists
«SCIENCE AND EDUCATION - 2018»

12th April 2018, Astana

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Студенттер мен жас ғалымдардың «Ғылым және білім - 2018» атты XIII Халықаралық ғылыми конференциясының БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ XIII Международной научной конференции студентов и молодых ученых «Наука и образование - 2018»

PROCEEDINGS of the XIII International Scientific Conference for students and young scholars «Science and education - 2018»

2018 жыл 12 сәуір

Астана

УДК 378

ББК 74.58
Ғ 96

Ғ 96
«Ғылым және білім – 2018» атты студенттер мен жас ғалымдардың XIII Халықаралық ғылыми конференциясы = XIII Международная научная конференция студентов и молодых ученых «Наука и образование - 2018» = The XIII International Scientific Conference for students and young scholars «Science and education - 2018». – Астана: http://www.enu.kz/ru/nauka/nauka-i-obrazovanie/, 2018. – 7513 стр. (қазақша, орысша, ағылшынша).

ISBN 978-9965-31-997-6

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 378

ББК 74.58

ISBN 978-9965-31-997-6

Таковы в целом принципы и функции по созданию геоинформационной системы по мониторингу безопасности водных объектов, которые сводятся к созданию геоинформационной системы (ГИС) в составе прикладных программных продуктов MIKE 11 с модулями одномерного моделирования для рек и каналов.

Список использованной литературы

1. Шинибаев Б.Д. Защита гидротехнических сооружений от размывов: Справочн. пособие – Алма-Ата: Кайнар, 1984. – 124. 119 Методика определения критериев безопасности гидротехнических сооружений. РД 153-34.2-21.342-00. М.:, 2000.

2. Методика оценки уровня безопасности гидротехнических сооружений. Стандарт предприятия. СТП НИИЭС. М.: 2004.

3. Сборник законодательных нормативно-технических материалов по безопасности гидротехнических сооружений в Узбекистане. ГОСВОДХОЗ-НАДЗОР. Диагностический центр Экспертного совета. Ташкент. 2008.

4. Методика расчета устойчивости грунтовых плотин / Зотеев В. Г., Костерова Т К., Морозов М. Г. и др.//Водное хозяйство России. 2002.Т.4.Ж 5.

5. Рекомендации по оценке надежности гидротехнических сооружений: П842-86 / Гидропроект. М., 1986.

УДК 519.21

АНАЛИЗ РАСПРЕДЕЛЕНИЯ ГЕНЕРИРУЕМЫХ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ И ШУМА В АНАЛОГОВОМ ВХОДЕ МИКРОКОНТРОЛЛЕРА

Гизатов А.А.

Студент 4 курса Евразийского национального университета им. Л.Н.Гумилева, Астана

Научный руководитель – Атанов С.К.

Введение

Случайные величины являются немаловажным разделом в криптографии, теории вероятности и случайных процессах. Псевдослучайные числа могут быть воспроизведены благодаря программным генераторам псевдослучайных чисел, аппаратным генераторам случайных чисел, физическим шумам (процессам) в устройствах, а также комбинации из выше перечисленных. Генераторы псевдослучайных чисел (ГПСЧ) необходима для создания криптографических ключей, сеансов аутентификации, одноразовых блокнотов (шифр Вернама), схемах цифровой подписи и т.д. Главные критерии ГПСЧ:

- диапазон значений;
- скорость генерации;
- равномерность распределения (энтропия);
- криптографическая стойкость.

Программный генератор псевдослучайных чисел и аппаратный генератор случайных чисел

Программный ГПСЧ образовывает числа по определенному заданному алгоритму, т.е. воспроизведение псевдослучайных чисел в той или иной мере зависит от метода программной реализации. Заметное различие результата программной генерации псевдослучайных чисел можно увидеть при сравнении работ [1] и [2], в каждой из которых разработан собственный алгоритм. Программные генераторы при определенных условиях, как сказано в исследовательской работе [1], способны не только вырабатывать десятичные числа в случайном порядке с высокой энтропией, но и бинарные числа, последовательности которых обладают криптографической стойкостью.

ГПСЧ японских ученых, который носит название Вихрь Мерсенна (Mersenne Twister), алгоритм и работа которого описаны в работе [3], имеет такие преимущества, как большой диапазон (2^{19937}–1), высокая скорость и энтропия, однако не является криптографически

стойким в связи с тем, что наблюдение за достаточным количеством итерации позволяло предугадать следующие числа. Поэтому на базе Вихря Мерсенна с комбинацией регистра сдвига с линейной обратной связью (LFSR), который используется для генерации псевдослучайной последовательности битов, был разработан CryptoMT, криптостойкость которого показано в работе [4]. Все вышесказанное доказывает, что программная реализация показывает себя с очень хорошей стороны, особенно с комбинированием разных алгоритмов.

Аппаратный генератор случайных чисел (ГСЧ) в своей основе для воспроизводства случайных чисел использует шумы физических процессов, принимая их сигналы во вход и преобразовывая в цифровой сигнал. Можно предположить, что такие шумы в силу того, что они происходят в беспорядочно происходящих физических явлениях, абсолютно непредсказуемы. Русские ученые в своей работе [5], применяя статистические тесты, показали, что аппаратный генератор при определенных условиях может оказаться хуже, чем программный ГПСЧ.

Аппаратно-программный ГСЧ являет собой заманчивым способом устранить недостатки и программного ГПСЧ, и аппаратного ГСЧ, как показано в работе [6]. Тем не менее, эффективность такого ГСЧ зависит от объема, вида и значения параметров закона распределения.

Программный ГПСЧ в микроконтроллере и шум с аналогового входа

Микроконтроллер – это интегральные схемы, соединяющие на одном полупроводниковом кристалле все основные функциональные блоки вычислителя: центральный процессор, запоминающее устройство, устройства для ввода и вывода информации и межмодульные магистрали. Микроконтроллеры не имеют собственных ГСЧ, но в них могут быть загружены программа с алгоритмом для воспроизведения псевдослучайных чисел.

В данной работе мы проведем анализ энтропии случайных чисел программного ГПСЧ и шума с аналогового входа микроконтроллера Arduino Uno. Для проверки программного генератора был загружен простой алгоритм программы, которая была написана в среде Arduino IDE, и вырабатывает псевдослучайные числа в диапазоне 1–99999 включительно. Сгенерировав примерно 10 МБ чисел, мы получили результат, показанный на рисунке 1.

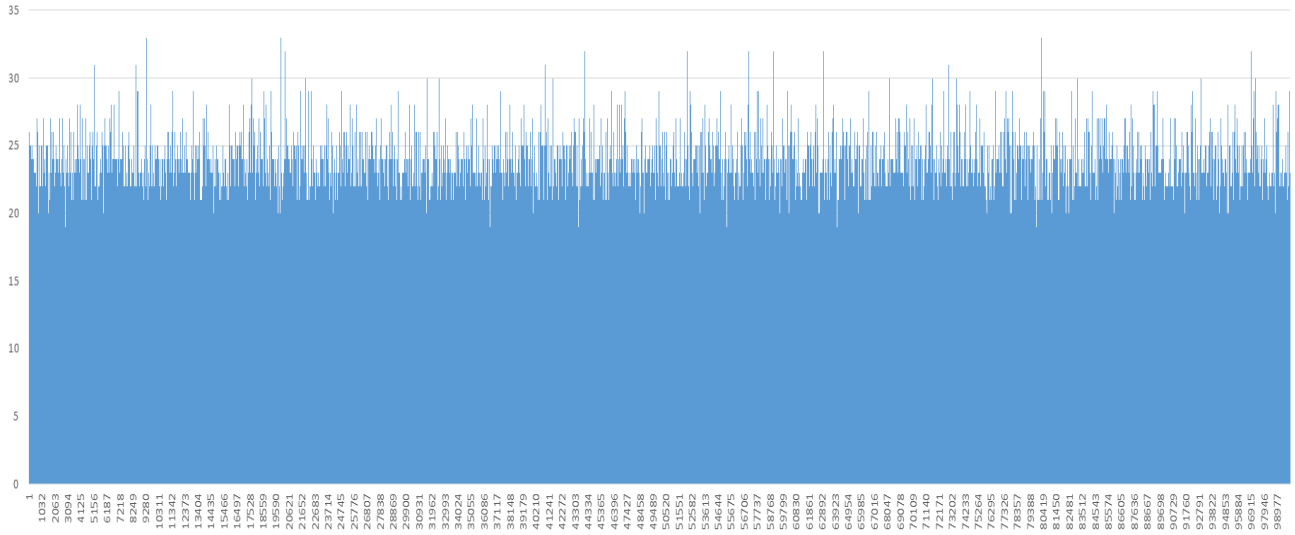

Рисунок 2. Гистограмма сгенерированных чисел программного ГПСЧ микроконтроллера с диапазоном 1–99999

На гистограмме мы явно наблюдаем так называемые «колокола». Они показывают, что числа распределены неравномерно с некой закономерностью, которая не была нами задана. Посмотрим, что получится при диапазоне чисел 1–1024, сгенерировав те же 10 МБ. На рисунке 2, видны почти те же колокола. Таким образом, какой бы мы не выбрали

диапазон, равномерность распределения будет иметь такую же закономерность, т.е. числа псевдослучайны.

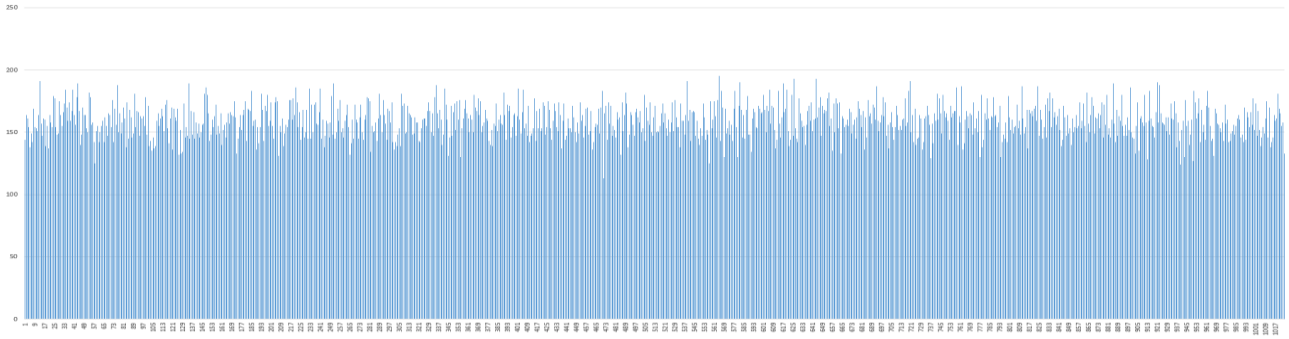

Рисунок 3. Гистограмма сгенерированных чисел программного ГПСЧ микроконтроллера с диапазоном 1–1024

Arduino Uno имеет пять аналоговых входных портов с АЦП разрядностью 10 бит. Выбрав два аналоговых входа A0 и A5, мы решили проверить, какой шум наблюдается в них, если оставить их неподключенными к чему-либо, как показано на рисунке 3.

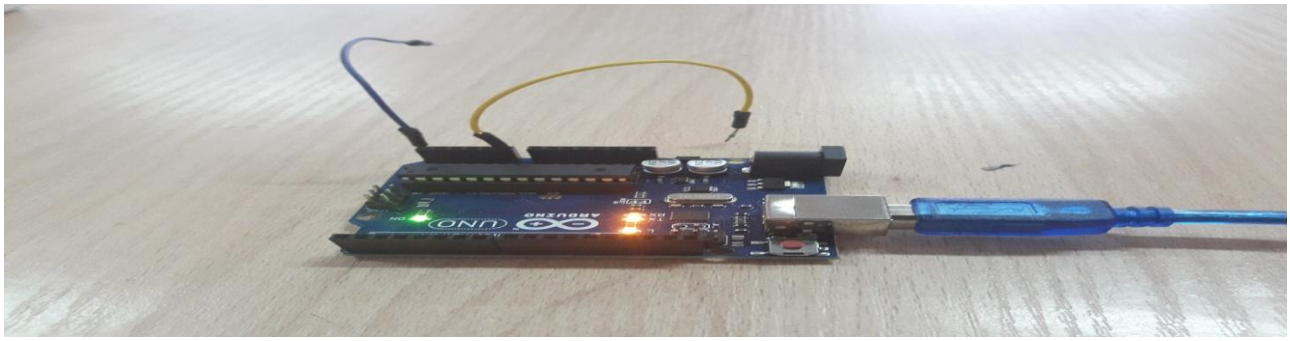

Рисунок 4. Arduino Uno

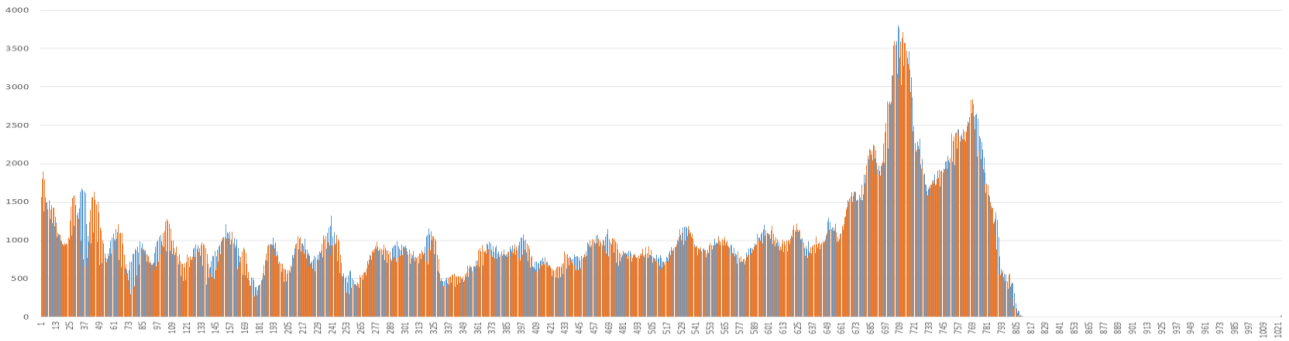

Рисунок 5. Гистограмма шума с аналоговых входов A0 и A5

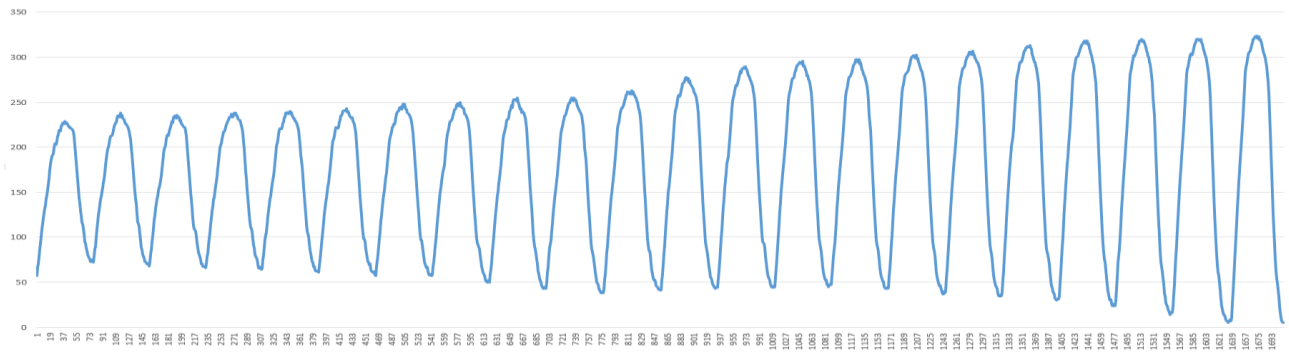

Рисунок 6. Статистический анализ шума

На рисунке 4 мы можем видеть, что с двух аналоговых входов идет одинаковый шум. К тому же заметен большой колокол в диапазоне 670–800 с двух аналоговых входов. Однако явную закономерность показывает нам рисунок 5. График показывает нам, что аналоговые входы ловят посторонний сигнал. Если поставить под Arduino Uno отражающий экран, то они никакие сигналы не будут ловить, и график покажет прямую линию.

В программном ГПСЧ можно инициализировать начальный входной параметр, т.е. точку, с которой начинается генерация псевдослучайных чисел. Для этого существует функция *randomSeed()*. Мы можем задать случайный входной параметр с помощью шума с аналогового входа *randomSeed(analogRead(0))*. Однако это не изменит закономерную последовательность псевдослучайных чисел, как можно это увидеть на рисунке 6.

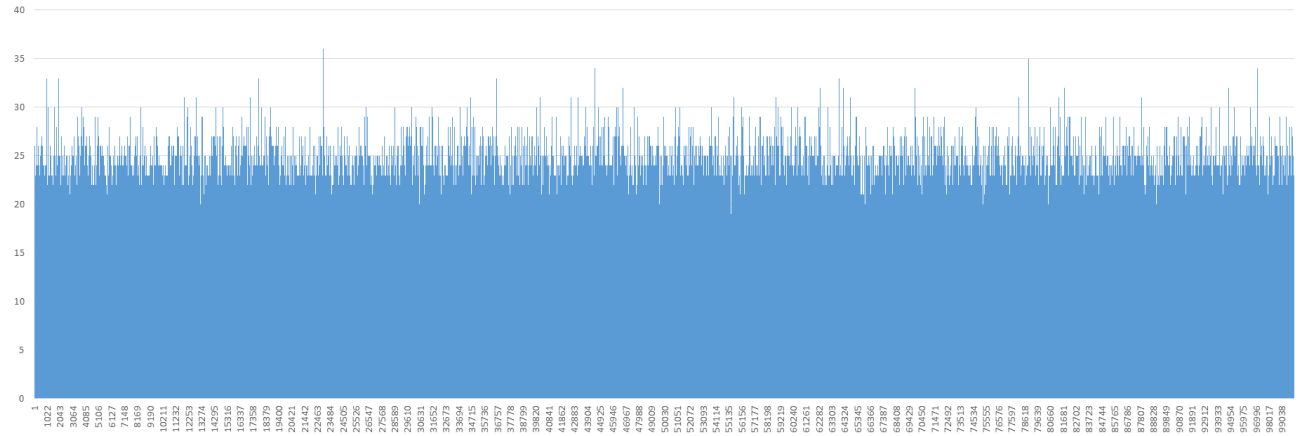

Рисунок 7. Гистограмма сгенерированных чисел программного ГПСЧ микроконтроллера с диапазоном 1–99999 с случайным входным параметром от аналогового шума

Заключение

В данной работе мы провели сравнение различных генераторов псевдослучайных и случайных чисел и сделали анализ простого программного ГПСЧ и шума с аналогового входа. Генерация случайных в микроконтроллере, благодаря загрузке программы и подключения к нему разного рода датчиков шумов, является оптимальным выбором во многих областях, где требуется микроконтроллер. Например, можно загрузить алгоритм Вихря Мерсенна для 32-битного микроконтроллера и применить датчики. Проведенный анализ показал нам, что ГПСЧ и ГСЧ, введенные в микроконтроллер, ведет себя так, как и ожидается в ГПСЧ и ГСЧ других работ.

Список использованных источников

1. *Герасимов Л.Ю.* О Построении Программных Генераторов Псевдослучайных Чисел На Основе Динамических Систем В Режиме Детерминированного Хаоса // Вестник СамГУ – Естественнонаучная серия. Самарский университет, 2013. С. 11–17.
2. *Григорьева М.В.* Программный Генератор Псевдослучайных Чисел Для Программных Средств Защиты Информации // Научно-Технический Вестник Информационных Технологий, Механики И Оптики. ФГБОУ ВПО «СПбНИУ ИТМО», 2008. С. 271–276
3. *Makoto Matsumoto, Takuji Nishimura.* Mersenne Twister: A 623-dimensional equidistributed uniform pseudorandom number generator // ACM Transactions on Modeling and Computer Simulation (TOMACS) - Special issue on uniform random number generation. Volume 8 Issue 1, Jan. 1998, P. 3-30
4. *Makoto Matsumoto, Mutsuo Saito, Takuji Nishimura, Mariko Hagita.* CryptMT stream cipher version 3 // eSTREAM, ECRYPT Stream Cipher Project. Report 28, 2007, P. 1–16.
5. *Потий А.В., Орлова С.Ю., Гриненко Т.А.* Статистическое тестирование генераторов случайных и псевдослучайных чисел с использованием набора статистических

тестов NIST STS // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Вип. 2, 2001, С. 206-214.

6. *Димаки А. В., Светлаков А. А.* Аппаратно-программный генератор случайных чисел, сопрягаемый с компьютером типа IBM PC // Известия томского политехнического университета. Т. 307, 2004, С. 144-148

УДК 62-1

ПРИБОРЫ УЧЕТА С ДИСТАНЦИОННЫМ КОНТРОЛЕМ ПОКАЗАНИЙ

Екрамова Назгуль Рауиятовна
Магистрантка кафедры вычислительной техники и программного обеспечения
ЕНУ им. Л.Н. Гумилева, Астана, Казахстан
Научный руководитель – к. ф-м н. Н.Н. Ташатов

Электроэнергия является одним из самых дорогих видов ресурсов, а ее правильный и точный учет — важной задачей для поставщиков энергии.

С XIX века люди пользуются электрической энергией, платят за нее деньги. За это время опробовано много методов расчета между электроснабжающими организациями и потребителями, но со временем, стало ясно, что лучшим вариантом является автоматический учет приборами совершенной работы с последующей ее оплатой по состоявшемуся факту.

С этой целью производители электротехнического оборудования выпускают электрические счетчики, учитывающие разными методами затраченную потребителем энергию.

В данный момент распространено два их вида:

1. индукционные приборы старых моделей, которые работают на основе электромеханической конструкции;
2. статические изделия, использующие электронные компоненты и микропроцессорную технику.

Оба вида этих приборов работают по одному общему принципу: они все время во включенном состоянии считают проходящие через них мощности и показывают эту информацию на счетном механизме или табло индикации. По времени их показания постоянно обновляются, увеличиваются.

Это позволяет фиксировать отсчеты в разное время и, вычитая предпоследнее показание из последнего, определять совершенную электрическими приборами работу за конкретный расчетный период.

С введением закона о самостоятельной передаче данных по потребленным ресурсам управляющей компании жильцы столкнулись с необходимостью ежемесячно переписывать показания электросчетчиков, звонить или лично посещать офисы обслуживающих организаций. Но бывает, что на это нет времени или человек забыл передать данные. Использование приборов учета с дистанционной передачей данных позволяют регистрировать показания счетчика в реальном времени, что значительно повышает оперативность и точность биллинга — в любой момент компания знает, на какую сумму необходимо выставить счет.

Приборы учета с дистанционной передачей данных практически исключают манипуляцию с их показаниями. Установка таких приборов учета способствует снижению числа разногласий между сбытовыми компаниями и потребителями.

Использование счетчиков с дистанционной передачей данных удобно как для потребителей, так и для предприятий.

Отправка использованных киловатт не отнимает много времени, а сам процесс комфортен и удобен. Энергоснабжающие предприятия, с помощью этих приборов могут отслеживать уровень потребления энергии населением.