УДК 621.383.92

Горбадей О. Ю., Зеневич А. О. *Белорусская государственная академия связи, Минск*

ИСПОЛЬЗОВАНИЕ ДИОДОВ-ГЕНЕРАТОРОВ ШУМА ДЛЯ СОЗДАНИЯ ДВУХУРОВНЕВОЙ СЛУЧАЙНОЙ ЧИСЛОВОЙ ПОСЛЕДОВАТЕЛЬНОСТИ

Показана возможность применения диодов-генераторов шума для создания двухуровневой случайной числовой последовательности. Выполнена оценка равномерности и случайности двухуровневой случайной числовой последовательности, формируемой диодами-генераторами шума. Показано соответствие статистического распределения случайной числовой последовательности распределениям Пуассона и Гаусса. Выполнена статистическая проверка полученных двухуровневых последовательностей на случайность по тестам стандарта NIST.

Ключевые слова: *последовательность случайная числовая, энтропия, диод-генератор.*

Gorbadey O. Yu., Zenevich A. O. *Belarusian State Academy of Communication", Minsk*

USE OF THE DIODES-NOISE GENERATORS TO CREATE A TWO-LEVEL RANDOM NUMERICAL SEQUENCE

The possibility of using diodes noise generators to create a two-level random number sequence is shown. There are founded for some types of diodes-generators the operating conditions (such as overvoltage), which the maximal values of entropy and evenness of the statistical distributing of output impulses are arrived. For the realization of researches the experimental setting is developed. The estimation of the uniformity and randomness of two level random number sequence, formed by diodes noise generators. Accordance of the statistical distribution of random numerical sequence to Poisson and Gauss distribution is shown. There is made the statistical checking of the received two-level sequences for random order using NIST standard. The test results confirmed that the got binary sequences were random.

Key words: random numerical sequence, entropy, diode generator.

Горбадей О. Ю., Зеневич А. О. *Білоруська державна академія зв'язку, Мінськ*

ВИКОРИСТАННЯ ДІОДІВ-ГЕНЕРАТОРІВ ШУМУ ДЛЯ СТВОРЕННЯ ДВОРІВНЕВОЇ ВИПАДКОВОЇ ЧИСЛОВОЇ ПОСЛІДОВНОСТІ

Показана можливість застосування діодів-генераторів шуму для створення дворівневої випадкової числової послідовності. Виконана оцінка рівномірності і випадковості дворівневої випадкової числової послідовності, що формується діодами-генераторами шуму. Показана відповідність статистичного розподілу випадковій числовій послідовності розподілам Пуассона і Гауса. Виконана статистична перевірка отриманих дворівневих послідовностей на випадковість по тестах стандарту NIST

Ключові слова: *послідовність випадкова числова, ентропія, діод-генератор.*

Введение. В настоящее время создание генераторов случайных числовых последовательностей (ГСПЧ), основанных на физических источниках случайности, является важной и актуальной задачей для таких областей науки и техники как криптография, численное моделирование случайных процессов в критически важных отраслях деятельности государства [1-3]. Для обеспечения быстродействия применяют алгоритмы генерации псевдослучайных числовых последовательностей. Однако такие алгоритмы не позволяют получит истинно случайную кодовую последовательность, поскольку они реализуются на основе компьютера. Компьютер является детерминированной системой и поэтому через некоторый период времени кодовая последовательность повторяется.

В связи с этим стандарты криптографических алгоритмов требуют применять физические источники шума при разработке ГСЧП гарантированного качества. Наиболее часто для этих целей применяются ГСЧП, основанных на способе счета случайных событий за фиксированный интервал времени [4, 5]. В таких ГСЧП используются диоды-генераторы шума, в основу работы, которых положен случайный характер возникновения микроплазменного пробоя их *p-n*-перехода [6].

Ранее в работах приводились результаты исследования диодов КГ401 на предмет исследования кратковременного и долговременного дрейфа шумовых характеристик, выбора токового и температурного режимов работы, минимального интервала счета шумовых импульсов для необходимого значения энтропии [7-9].

Однако в настоящее время неопределенны статистические модели описания выходного потока импульсов диодов – генераторов шумов, а также способов формирования из этих потоков случайных числовых последовательностей. Поэтому это и явилось целью данной работы.

Описание экспериментальной установки и методики измерения

Для проведения исследований использовалась экспериментальная установка, блок-схема которой представлена на рис.1.

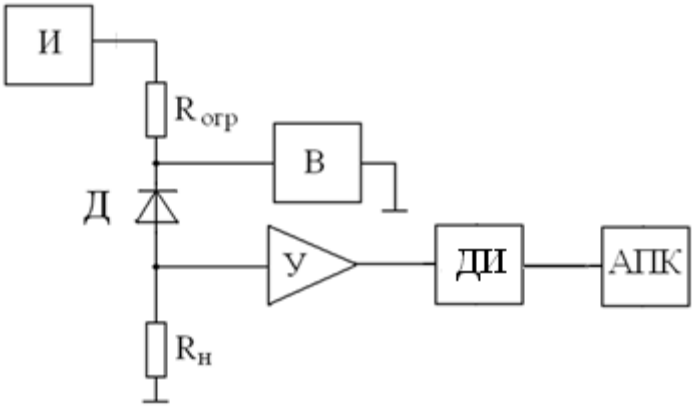

Рис. 1. Блок-схема экспериментальной установки.
И – источник напряжения, Д – диод-генератор, В – вольтметр, У – усилитель,
ДИ – амплитудный дискриминатор импульсов, АПК – аппаратно-программный комплекс,
$R_{огр}$ – ограничительный резистор, $R_н$ – нагрузочный резистор

Для реализации режима микроплазменного пробоя шумовой диод ШД включался по схеме, показанной на рис. 1. При этом последовательно с диодом ШД подключался нагрузочный резистор $R_н$, а для ограничения тока, протекающего через него, применялся ограничительный резистор $R_{огр}$. Источник постоянного напряжения И использовался для питания шумового диода. Напряжения $U_{см}$, подаваемые на диод, были близкими или превышали напряжение его лавинного пробоя. Именно при этих напряжениях наблюдается микроплазменный пробой шумового диода. Таким образом, реализовывался микроплазменный режим работы шумового диода. Контроль напряжения питания диода осуществлялся при помощи вольтметра В. Импульсы напряжения, сформированные на резисторе $R_н$ в результате микроплазменного пробоя диода, поступали на вход усилителя У. После усиления в усилителе эти импульсы подавались на вход амплитудного дискриминатора Д. На выходе дискриминатора формировались импульсы, стандартизированные по амплитуде и длительности. Сформированные импульсы поступали на вход аппаратно-программного комплекса АПК. Последний выполнял: вычисление числа импульсов, поступающих на вход АПК за некоторый промежуток времени и интенсивность потока импульсов λ (количество импульсов за единицу времени); определение

статистического распределения числа импульсов; формирование из потока импульсов двухуровневой последовательности состояний логического нуля и логической единицы.

Формирование последовательности осуществлялось следующим образом. Уровень логического нуля соответствовал случаям, когда за фиксированный интервал времени измерения регистрировалось четное число импульсов. В случае регистрации в течение интервала времени нечетного числа импульсов устанавливался уровень логической единицы. Из двухуровневой последовательности формировалась случайная бинарная последовательность, содержащая нули и единицы.

На основании полученных статистических распределений импульсов выполнялась оценка возможности получить из этого распределения равномерной двухуровневой последовательности состояний логического нуля и логической единицы. В качестве оценочного параметра использовалась следующая величина равномерности:

$$\varepsilon = \sum_{i=0}^{\infty} (-1)^i P(i),$$

где i – число импульсов, $P(i)$ – вероятность появления i-го числа импульсов за некоторый временной интервал T.

Определение энтропии статистического распределения числа импульсов H, поступающих на вход аппаратно-программного комплекса, осуществлялась при помощи следующего выражения:

$$H = -(0.5 + \varepsilon/2)\log_2(0.5 + \varepsilon/2) - (0.5 - \varepsilon/2)\log_2(0.5 - \varepsilon/2).$$

В процессе экспериментальных исследований выполнялась оценка соответствия статистического распределения числа импульсов распределениям Пуассона и Гаусса, как это описано в работах [10, 11]. В качестве критерия соответствия использовался χ^2 для уровня значимости 0,05. Измерения выполнялись при постоянной температуре 293 *K*. Поскольку диоды различаются напряжением пробоя U_n, то для определения зависимостей использовалась величина перенапряжения $\Delta U = U_{см} - U_n$.

Результаты эксперимента

В качестве объектов исследования использовались диоды-генераторы КГ401 (производство Российской Федерации) [7] и ND102L, ND103L (производство Республики Беларусь). Результаты исследований, связанных с оценкой соответствия статистического распределения числа импульсов распределениям Пуассона и Гаусса, представлены в табл. 1. Максимальное значение перенапряжения выбиралось равным ΔU = 0,15 *B*, поскольку для всех типов исследуемых диодов – генераторов наблюдалось резкое увеличение электрического тока, что могло привести их тепловому пробою.

Характеристика статистического распределения числа импульсов Табл. 1

Тип диода-генератора	Диапазон перенапряжений, *B*	Интенсивность импульсов, $с^{-1}$	Статистическое распределение
ND 102L	0.00 ÷ 0,05	$\geq 2{,}1\cdot10^4$	Пуассона
	0.05 ÷ 0,15	$< 2{,}1\cdot10^4$	Гаусса
ND 103L	– 0.04 ÷ 0,00	$\geq 8{,}0\cdot10^4$	Пуассона
	0.04 ÷ 0,15	$< 8{,}0\cdot10^4$	Гаусса
КГ 401В	0.00 ÷ 0,03	$\geq 3{,}2\cdot10^4$	Пуассона
	0,03÷ 0,15	$< 3{,}2\cdot10^4$	Гаусса

Как видно из полученных данных (табл. 1), для всех исследуемых диодов-генераторов шума существуют диапазоны перенапряжений, для которых статистическое распределение импульсов соответствует распределению Пуассона. Наибольшее значение интенсивности импульсов при этом соответствовала диодам ND 103L. Также необходимо отметить, что

наименьший диапазон перенапряжений, при котором статистическое распределение импульсов соответствовала распределению Пуассона наблюдался для диодов КГ 401В.

В работе [11], авторами была выполнена оценка соответствия статистических распределений импульсов исследуемых диодов-генераторов распределению Пуассона. Поэтому в данной статье приведены статистических распределения импульсов и их соответствие распределению Гаусса (рис. 2). На рис. 2 представлены данные для диода-генератора шума ND 102L при значении перенапряжения ΔU = 0,10 B. Отметим, что с ростом перенапряжения уменьшалось отношение дисперсии к математическому ожиданию, что наблюдалось для всех типов исследуемых диодов. Для других типов исследуемых диодов-генераторов шума были получены аналогичные результаты.

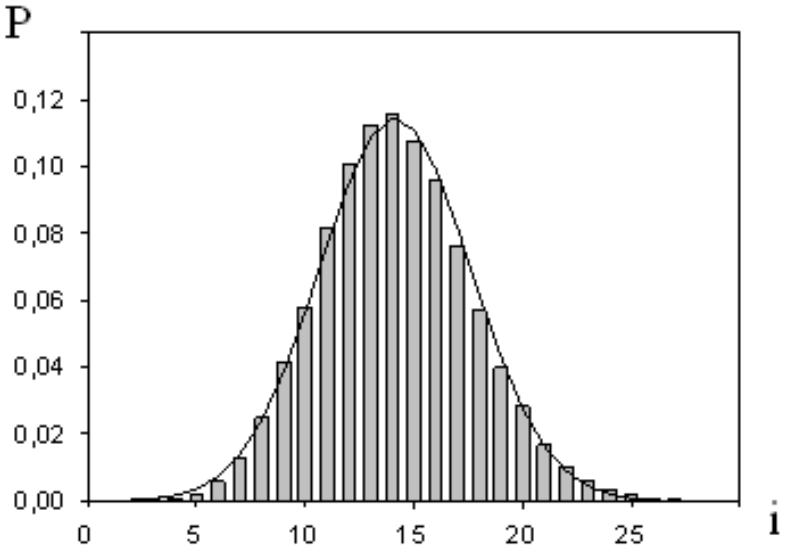

Рис. 2. Аппроксимация экспериментальных данных распределением Гаусса
(сплошной линией обозначена рассчитанная зависимость;
столбцами представлены экспериментальные данные).

Полученные результаты исследования зависимости величины равномерности ε от перенапряжения показаны на рис. 3. На рисунке представлены результаты для диода-генератора ND 102L.

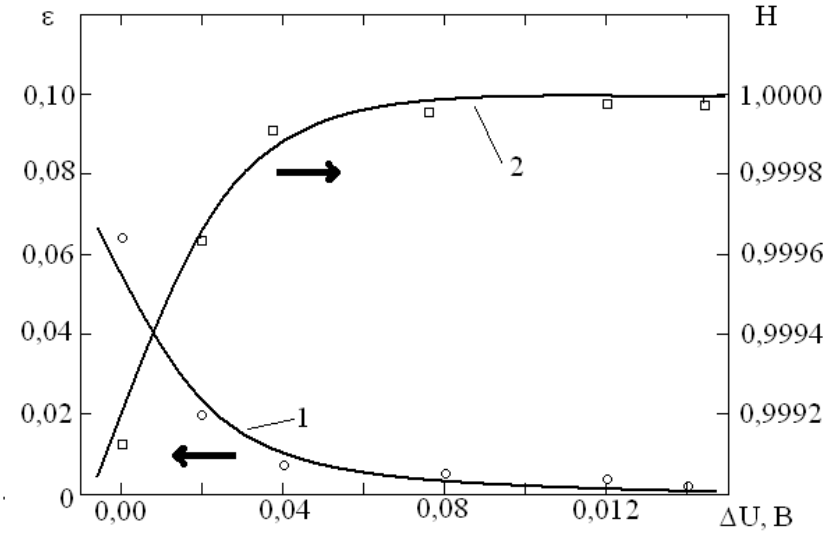

Рис. 3. Зависимости величины равномерности и энтропии от перенапряжения.
1 – величина равномерности; 2 – энтропия

При проведении измерений длительность интервала выборки импульсов была постоянной и составляла 12 мкс. Отметим, что для других типов исследуемых диодов поведение этой зависимости было идентичным. Как видно из полученных результатов с увеличением перенапряжения значение ε уменьшается и приближается к нулю. Рассчитанная зависимость энтропии от перенапряжения, представленная на этом же рисунке (кривая 2), показывает, что уменьшения ε приводит к увеличению H. При значениях $\varepsilon \le 5 \cdot 10^{-3}$ значение энтропии $H > 0{,}9999$. Максимальные значения полученной энтропии для исследуемых диодов-генераторов представлены в табл. 2.

Максимальные значения энтропии для исследуемых диодов-генераторов Табл. 2

Тип диода-генератора	Перенапряжение, B	Интенсивность импульсов, $с^{-1}$	Величина равномерности	Энтропия
ND 102L	0,15	$3{,}0 \cdot 10^{6}$	$2{,}0 \cdot 10^{-3}$	0,999998
ND 103L		$3{,}5 \cdot 10^{6}$	$1{,}4 \cdot 10^{-3}$	0,999999
КГ 401В		$2{,}6 \cdot 10^{6}$	$5{,}1 \cdot 10^{-3}$	0,999985

Как следует из данных, приведенных в табл. 2, наибольшее значение энтропии удается получить для диодов-генераторов шума ND 103L. Также для этого типа диодов наблюдалась наибольшая скорость генерации одного бита двухуровневой кодовой последовательности.

Осуществлялась статистическая проверка полученных двухуровневых последовательностей на случайность по тестам стандарта NIST. Результаты тестов подтвердили, что полученные бинарные последовательности являются случайными.

Заключение. Показано, что диоды-генераторы могут быть использованы для создания двухуровневых случайных кодовых последовательностей. Для диодов-генераторов ND102L, ND103L и КГ401В определены рабочие режимы, такие как перенапряжения, при которых достигаются максимальные значения энтропии и равномерности статистического распределения выходных импульсов.

Работа выполнена при поддержке Белорусского республиканского фонда фундаментальных исследований (договор № Т16К-006).

Список использованной литературы

1. Рентюк В. Высокоэффективный генератор шума на базе стабилизатора напряжения / В. Рентюк // Компоненты и технологии. – 2014. – №1 – С.136-137.

2. Султанов Р. О. Аппаратные генераторы случайных чисел / Р. О. Султанов, Д. В. Лопатин // Психолого-педагогический журнал Гаудеамус. – 2013. – №2 (22). – С.156-158.

3. Колесова Н. А. Оценка качества генераторов случайных чисел / Н. А. Колесова // Вестник АГТУ. Серия: Управление, вычислительная техника и информатика. – 2011. – №1. – С. 119-123.

4. Vincent C. The generation of truly random binary numbers / C. Vincent // Journal of Physics E. – 1970. – V. 3, № 8. – P. 594-598.

5. Бобнев М. П. Генерирование случайных сигналов / М. П. Бобнев. – Москва : Энергия, 1971.– 240 с.

6. Грехов И. В. Лавинный пробой *p-n*-перехода в полупроводниках / Грехов И. В., Сережкин Ю.Н. – Ленинград : Энергия, 1980. – 152 с.

7. Барановский О. К. Об использовании диодов-генераторов шума КГ401 при разработке генераторов случайных числовых последовательностей / О. К. Барановский, П. В. Кучинский // Проблемы защиты информации: сб. научн. ст. – Минск.: БГУ, ГЦБИ. – 2004.– Вып. 5. – С. 147-150.

8. Барановский О. К. Стационарность и долговременный дрейф интенсивности потоков импульсов диодов-генераторов шума / О. К. Барановский, П. В. Кучинский // Проблемы защиты информации: сб. научн. ст. – Минск.: БГУ, ГЦБИ. – 2005. – Вып. 6. – С. 76-81.

9. Барановский О. К. Оптимизация времени пересчета шумовых импульсов диодов-генераторов при формировании случайных числовых последовательностей

/ О. К. Барановский, П. В. Кучинский // Проблемы защиты информации: сб. научн. ст. / Минск.: БГУ, ГЦБИ. – 2006.– Вып. 7. – С. 71-77.

10. Барановский О. К. Оценка энтропии случайных числовых последовательностей формируемых с использованием физического источника шума / О. К. Барановский, П. В. Кучинский, А. Ф.Чернявский // Вести НАН Беларуси. Сер. физ.-мат. наук. – 2004. – № 4. – С. 105-110.

11. Барановский О. К. Исследование возможности использования шумовых диодов для генерации пуассоновского потока импульсов / О. К. Барановский, О. Ю. Горбадей, А. О. Зеневич, О.М. Сильченко // «Проблемы инфокоммуникаций». – 2017. – № 1 (5). – С. 13-18.

References

1. Rentyuk V. "High-efficiency noise generator on the base of voltage stabilizator." *Komponenty i tehnologii* 1 (2014): 136-137.

2. Sultanov R. O. "Hardware generators of random numbers." *Psychological pedagogical journal of Gaudeamus* 2(22) (2013): 156-158.

3. Kolesova N. A. "Quality estimation of random numbers generators." *Vestnik AGTU. Series: management, computing engineering and informatics* 1. (2011): 119-123.

4. Vincent C. "The generation of truly random binary numbers."*Journal of Physics E* 3(8) (1970): 594-598.

5. Bobnev M. P. "Generation of random signals." *Moskva : Energiya* (1971): 240.

6. Grehov I. V. "Avalanche breakdown of *p-n*-transitors in semiconductors." *Leningrad : Energiya* (1980): 152.

7. Baranovskij O. K., Kuchinskij P. V. "About using of noise diodes-generators of noise КГ401 for working of random numerical sequences generators." *Problems of information security: Collection of scientific articles. Minsk BGU GCBI* 5 (2004): 147-150.

8. Baranovskij O. K., Kuchinskij P. V. "Stationarity and of long duration drift of impulses streams intensity of noise diodes-generators." *Problems of information security: Collection of scientific articles. Minsk BGU GCBI* 6 (2005): 76-81.

9. Baranovskij O. K., Kuchinskij P. V. "Optimization of translation time of diodes-generators noise impulses at forming of random numerical sequences." *Problems of information security: Collection of scientific articles. Minsk BGU GCBI* 7 (2006): 71-77.

10. Baranovskij O. K., Kuchinsrij P. V., Chernyavskij A. F. "The entropy estimation of of random numerical sequences that formed with the use of physical noise source." *Vesti NAN Belarusi. Series of physics and of mathematical sciences* 4 (2004): 105-110.

11. Baranovskij O. K., Gorbadej O. Yu., Zenevich A. O., Sil`chenko O. M. "Research of possibility to use the noise diodes for the generation of Poisson impulse streams." *Problemy infokommunikacij* 1(5) (2017): 13-18.

Авторы статьи

Горбадей Ольга Юрьевна – преподаватель кафедры программного обеспечения сетей телекоммуникации, Учреждение образования «Белорусская государственная академия связи», Минск, Беларусь. Тел.: +375 (17) 322 91 02. E-mail: o-st1@yandex.ru

Зеневич Андрей Олегович – доктор технічних наук., профессор, ректор учреждения образования «Белорусская государственная академия связи», Минск, Беларусь. E-mail: A.Zenevich@bsac.by

Authors of the article

Gorbadey Olga Yur`yevna – a teacher of department of telecommunication networks software, Educational Establishment "Belarusian State Academy of Communication", Minsk, Byelorussia. Tel.: +375 (17) 322 91 02. E-mail: o-st1@yandex.ru

Zenevich Andrey Olegovich – doctor of sciences (technic), professor, rector of Educational Establishment "Belarusian State Academy of Communication", Minsk, Byelorussia. E-mail: A.Zenevich@bsac.by

Дата поступления
в редакцию: 17.08.2017 г.

Рецензент:
доктор технических наук Е. В. Гаврилко
Государственный университет телекоммуникаций, Киев