УДК 621.373.5: 621.317.75:519.246

Разумейчик В.С., Буслюк В.В., Дереченник С.С., Поляков В.И., Лапич С.В.

ОЦЕНКА ВЕРОЯТНОСТНЫХ ХАРАКТЕРИСТИК СЛУЧАЙНЫХ СИГНАЛОВ МИКРОЭЛЕКТРОННОГО ШУМОВОГО МОДУЛЯ

Введение. В последние годы стремительно развиваются электронные системы обработки и защиты информации, особенно предназначенные для портативных и специализированных устройств. Эффективность защиты цифровых данных во многом определяется качеством случайных числовых последовательностей, используемых в криптографических протоколах. Генератор случайных чисел, как аппаратно-программное устройство, выдает последовательности, каждый следующий элемент которых статистически и вычислительно трудно предсказать по всем предыдущим элементам.

Согласно современным стандартам криптографии, алгоритмы выработки псевдослучайных чисел не могут быть отнесены к генераторам случайных чисел (хотя ключи таких алгоритмов могут строиться с помощью генераторов). В компьютерных системах могут использоваться различные источники случайности: *физические источники* (например, шум в радиоэлектронных приборах), *системные источники* (использующие состояния и события операционной системы – системное время, сетевую активность, прерывания), *источники, основанные на активности операторов* (движения мышью, нажатия клавиш), при этом физические источники случайности являются предпочтительными [1].

Задача повышения информационной безопасности обусловливает необходимость разработки специализированных малогабаритных устройств, генерирующих электрические сигналы случайного (шумового) характера. Научно-исследовательским унитарным предприятием «СКБ Запад», выпускающим дискретные кремниевые диоды-генераторы шума серий ND101…ND104L и ND201L [2], созданы экспериментальные образцы двухканального микроэлектронного шумового модуля, в каждом из каналов которого формируются сигналы аналогового и дискретного (телеграфного) вида. В данной работе исследовалась неопределенность (случайность) этих сигналов путем определения их вероятностных (статистических) характеристик.

Особенности формирования и алгоритм обработки телеграфного сигнала. Основой для генерации случайных чисел являются случайные битовые последовательности (последовательности из нулей и единиц), которые, в свою очередь, могут формироваться, например, из телеграфного сигнала путем подсчета числа событий типа «перемена состояния сигнала» внутри заданного интервала времени. *Телеграфный сигнал* – это случайный процесс $x(t)$, представляющий собой последовательность прямоугольных положительных и отрицательных импульсов со случайными длительностями и детерминированными значениями уровней c и $-c$ (рисунок 1), причем перемены знака внутри любого интервала $(t, t+\tau)$ происходят с некоторой интенсивностью λ в случайные моменты времени, и не зависят от процессов в смежных интервалах времени [3, 4].

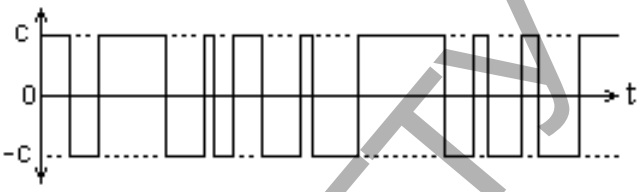

Рис. 1. Пример реализации случайного телеграфного сигнала

Случайной величиной телеграфного сигнала является количество перемен знака внутри заданного интервала, а распределение вероятностей этой случайной величины будет описываться законом Пуассона. Параметр λ полностью определяет корреляционные и спектральные свойства телеграфного сигнала (при $\lambda \to 0$ характеристики сигнала приближаются к характеристикам постоянной составляющей, при $\lambda \to \infty$ – к характеристикам белого шума). Функция автокорреляции и эффективный интервал корреляции:

$$R_x(\tau) = c^2 \cdot \exp\left(-2\lambda|\tau|\right), \qquad (1)$$

$$T_к = 2\int_0^\infty \left[R_x(\tau)/c^2\right] d\tau = 1/\lambda. \qquad (2)$$

В исследуемом шумовом модуле телеграфный сигнал формируется с помощью интегрального компаратора напряжения IZ393, включенного по схеме повторителя. На его неинвертирующий вход поступает центрированный случайный аналоговый сигнал $\overset{\circ}{u}(t) = u(t) - \overline{u}$ (напряжение шума $u(t)$ обратносмещенного диода-генератора ND201L с отфильтрованной постоянной составляющей $\overline{u}$), на инвертирующий вход – напряжение смещения u_{I0}. Функция преобразования *идеального* компаратора *при однополярном напряжении питания* U_{CC} соответствует формированию несимметричного (*смещенного*) телеграфного сигнала:

$$x(t) = 0{,}5 \cdot U_{CC}\left[1 + sign\left(\overset{\circ}{u}(t) - u_{I0}\right)\right]. \qquad (3)$$

Степень совершенства *реального* компаратора определяется минимально возможным порогом чувствительности, а также его быстродействием – временем переключения из одного состояния в другое. Граничная частота шума диода-генератора ND201L (ТУ BY 290948129.001-2010) при токе 50 *мкА* составляет 10 *МГц*, а эффективное напряжение шума – величину порядка 10…15 *мВ*. Для компаратора IZ393 (ТУ РБ 14553180.029-98) такой входной сигнал является небольшим, и ему соответствует типовое (для напряжения питания 5 *В*) значение времени переключения 0,7 *мкс*.

Разумейчик Вита Станиславовна, *кандидат технических наук, доцент кафедры «ЭВМ и системы» Брестского государственного технического университета.*

Буслюк Виктор Вячеславович, *доцент кафедры «ЭВМ и системы» Брестского государственного технического университета, главный инженер Научно-исследовательского унитарного предприятия «СКБ Запад».*

Дереченник Станислав Станиславович, *доцент, кандидат технических наук, заведующий кафедрой «ЭВМ и системы» Брестского государственного технического университета*

Поляков Виктор Иванович, *доцент, кандидат технических наук, профессор кафедры «ЭВМ и системы» Брестского государственного технического университета*

Лапич Сергей Вячеславович, *аспирант Брестского государственного технического университета*

Беларусь, БрГТУ, 224017, г. Брест, ул. Московская, 267.

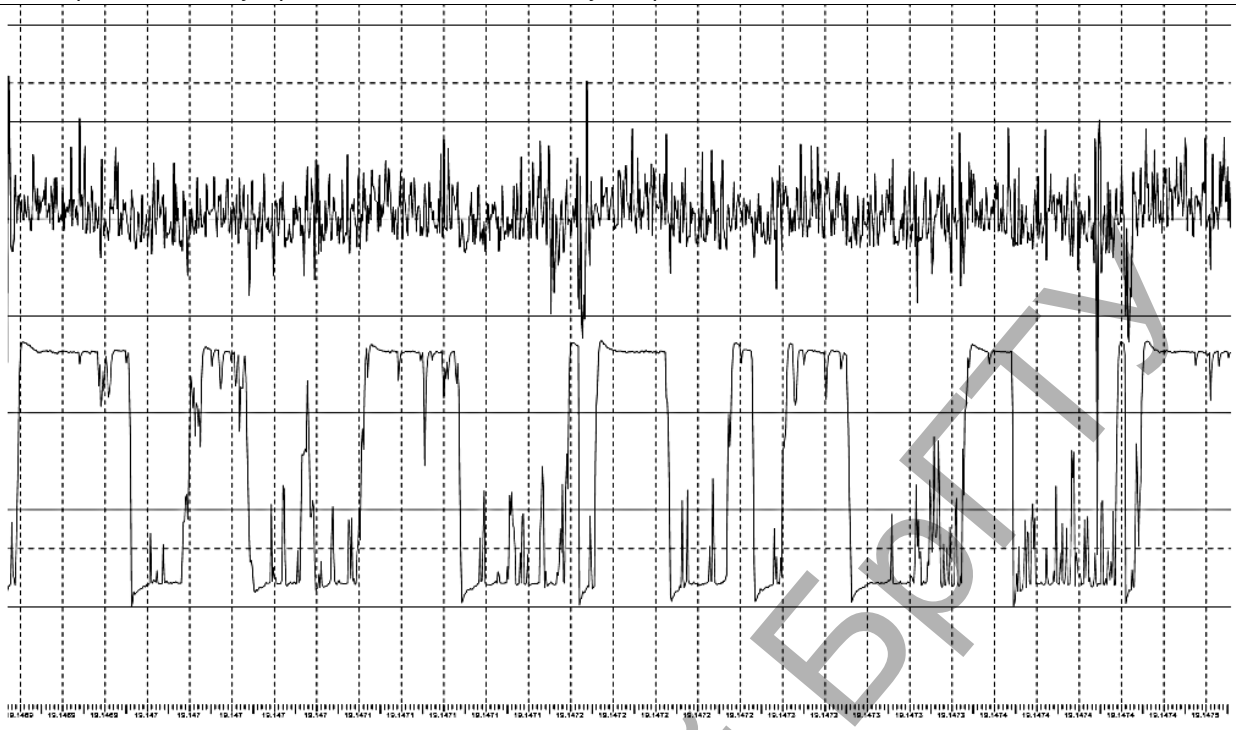

Рис. 2. Осциллограммы аналогового (верхняя кривая, коэффициент отклонения 50 *мВ/дел*) и телеграфного (нижняя кривая, 5 *В/дел*) сигналов: временная развертка 20 *мкс/дел*, напряжение питания $U_{CC} = 12\ B$

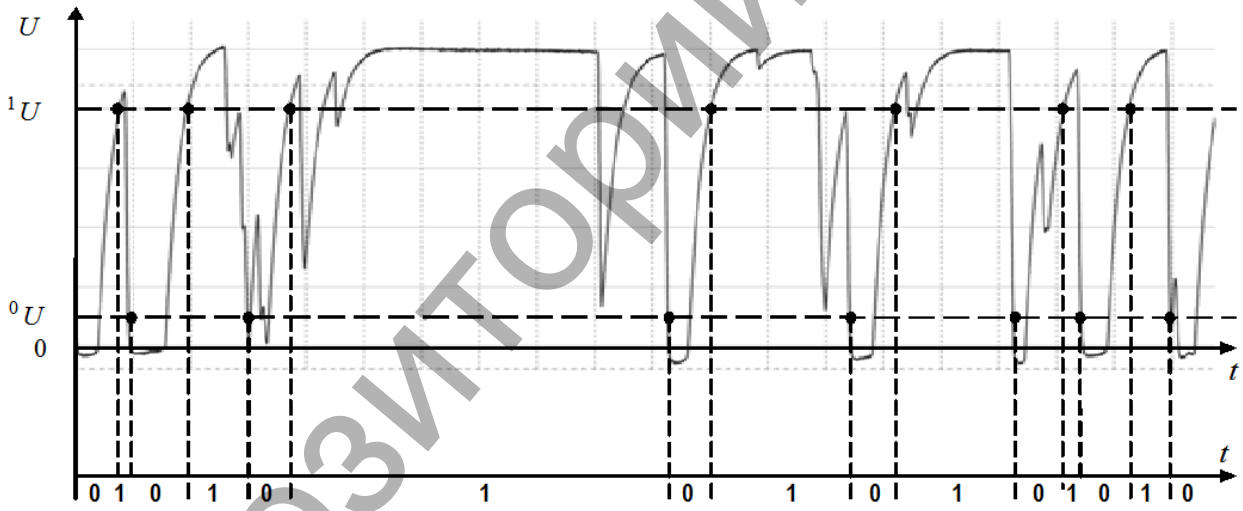

Рис. 3. Принцип восстановления телеграфного сигнала в цифровой код

Экспериментальные измерения сигналов шумового модуля выполнялись при напряжениях питания компаратора 5 *В* и 12 *В* и напряжении смещения в пределах ±20 *мВ* с помощью многофункционального измерительного комплекса «Alma Meter» (производство УП «Унитехпром» БГУ, г. Минск) в режиме дистанционного управления от компьютера через интерфейс Ethernet. Для задания напряжения смещения использовался генератор В-330, для наблюдения сигналов – цифровой осциллограф В-320. После дискретизации сигналов с частотой $F_Д = 1/\Delta t$ выполнялся их экспорт в компьютерный файл в виде N – точечной $\left(N = 10^6 \ldots 10^7\right)$ цифровой реализации: $\left\{x_n = x\left(t_n\right), t_n = n \cdot \Delta t,\ n = \overline{0, N-1}\right\}$.

Наблюдаемые телеграфные сигналы шумовых модулей (пример осциллограммы приведен на рисунке 2) характеризуются наличием существенных искажений в виде выбросов напряжения на обоих (низком и высоком) уровнях сигнала. Эти искажения мало зависят от напряжения питания и обусловлены поступлением высокочастотных составляющих аналогового шумового сигнала на вход компаратора, имеющего ограниченное быстродействие.

Для корректной статистической обработки реального телеграфного сигнала был разработан алгоритм классификации текущего значения конкретной реализации сигнала на уровни логического «нуля» (низкий уровень напряжения) и логической «единицы» (высокий уровень напряжения) с использованием выбираемых пороговых значений напряжения ${}^0U$ и ${}^1U$, соответствующих, например, стандартным значениям конкретной цифровой логики. Алгоритм имитирует работу цифрового элемента (например, триггера Шмитта, применяемого для восстановления цифрового сигнала, искаженного в линиях связи), на вход которого поступает телеграфный сигнал и иллюстрируется рисунком 3. Реализация алгоритма в системе MatLab (фрагмент М-файла приведен на рисунке 4) позволила восстановить телеграфный сигнал, т.е. преобразовать его в цифровой выходной код, удобный для статистической обработки.

```
for i = 1:n
 x1(i) = a(2,i);
 x2(i) = a(3,i); % аналоговый сигнал
 if ((x2(i)>=Uhigh)&(dig_==0))
 dig_=1;
 x2dig_(i)=-0.5; % центрированный цифровой сигнал 0/1 -> -0.5/0.5
i0_=i0_+1;
 x2dig_0_(i0_)=count_;
 ii=ii+1;
 x2dig(ii)=count_;
 dig0_=dig0_+count_;
 count_=1;
 elseif ((x2(i)<=Ulow)&(dig_==1))
 dig_=0;
 i1_=i1_+1;
 x2dig_(i)=0.5; % центрированный цифровой сигнал 0/1 -> -0.5/0.5
 x2dig_1_(i1_)=count_;
 ii=ii+1;
 x2dig(ii)=count_;
 dig1_=dig1_+count_;
 count_=1;
 else
 count_=count_+1;
 x2dig_(i)=x2dig_(i-1);
 end
end
if (dig_==1)
 i1_=i1_+1;
 x2dig_1_(i1_)=count_; % массив длительностей 1 цифрового сигнала
 ii=ii+1;
 x2dig(ii)=count_;
 dig1_=dig1_+count_;
else
 i0_=i0_+1;
 x2dig_0_(i0_)=count_; % массив длительностей 0 цифрового сигнала
 ii=ii+1;
 x2dig(ii)=count_; % общий массив длительностей (0 и 1) цифрового сигнала
 dig0_=dig0_+count_;
end
```

Рис. 4. Фрагмент М-файла для цифровой обработки (восстановления) телеграфного сигнала

Результаты исследования вероятностных характеристик. По экспортированным компьютерным реализациям наблюденных сигналов в программной среде MatLab R2012a 7.14 вычислялись статистические оценки следующих вероятностных характеристик:

- функции распределения вероятностей, математическое ожидание и дисперсия напряжения шума;
- нормированной функции автоковариации (функции корреляционных коэффициентов);
- функции распределения длительностей импульсов цифрового выходного кода.

На рисунке 5 представлены гистограмма и функция корреляционных коэффициентов аналогового шумового сигнала. Размах сигнала в данной реализации из 10^6 отсчетов составил от минус 44,0 *мВ* до 43,6 *мВ* со средним значением минус 21,7 *мВ* и среднеквадратическим отклонением 9,9 *мВ*. Гистограмма распределения напряжения шума имеет несимметричную форму, ее соответствие нормальному закону распределения вероятности недостаточно. Корреляционная длина (величина временного параметра, при которой автокорреляционная функция уменьшается в e раз, т.е. до значения 0,368) составила величину 50 *нс*, а двусторонний (эффективный) интервал корреляции – величину 100 *нс*, что соответствует эффективной ширине спектра аналогового шумового сигнала 10 *МГц*.

В таблице 1 и на рисунках 6, 7 приведены результаты статистической обработки цифровой реализации из 10^7 отсчетов телеграфного сигнала шумового модуля с размахом 5 *В*, подвергнутого цифровой обработке (восстановлению) в соответствии с указанным выше алгоритмом для различных вариантов значений пороговых напряжений.

Аппроксимация функции корреляционных коэффициентов (функции автокорреляции) выражением (1) позволяет найти параметр интенсивности телеграфного сигнала: $\lambda \approx 0{,}184 \cdot 10^6 c^{-1}$ и, согласно (2), корреляционную длину: $T_{\text{К}} = 1/\lambda \approx 5{,}43 \cdot 10^{-6} c$. Достоверность данного результата подтверждается практическим совпадением корреляционной длины со средней длительностью (5,44 *мкс*) импульсов сигнала для данных значений пороговых напряжений. Распределение длительностей импульсов соответствует экспоненциальному закону, что свидетельствует о пуассоновском характере процесса перемены состояний телеграфного сигнала.

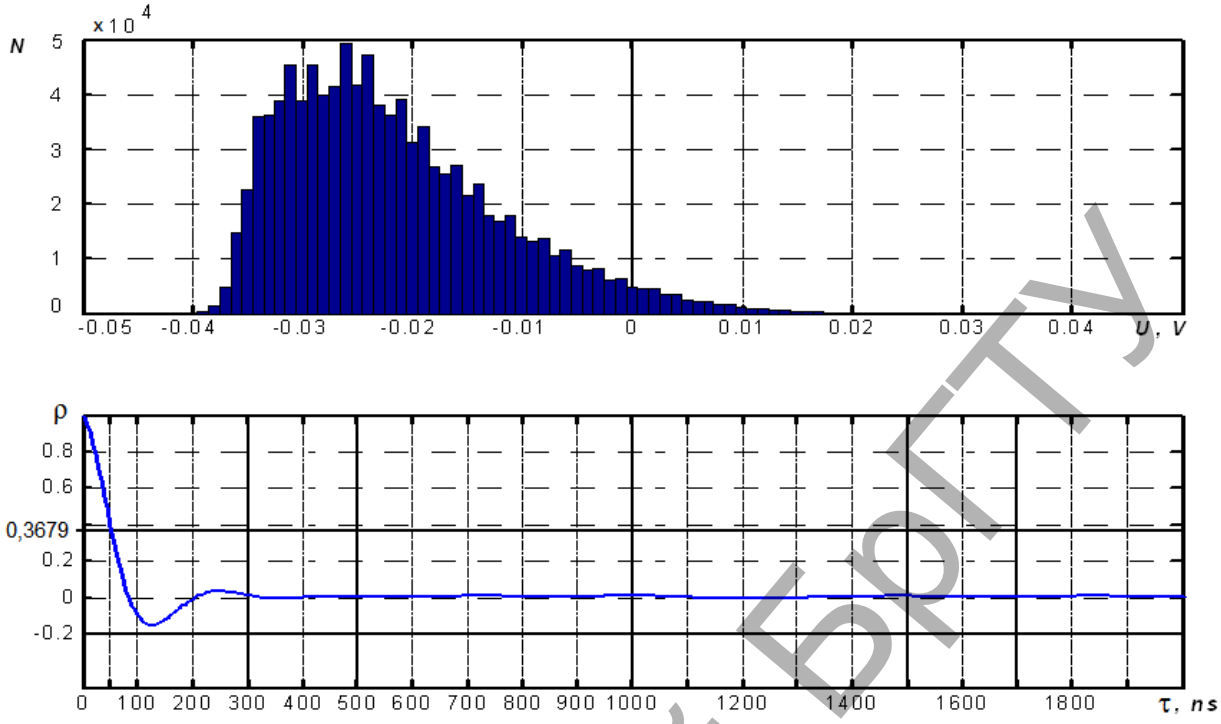

Рис. 5. Гистограмма (вверху) и функция корреляционных коэффициентов (внизу) центрированного аналогового шумового сигнала

Таблица 1. Статистические характеристики восстановленного телеграфного сигнала (минимальная длительность импульсов во всех случаях составляет 0,10 *мкс*)

Значения пороговых напряжений	Вид импульсов	Длительность импульсов, *мкс*			
		суммарная	максимальная	средняя	с.к.о.
${}^0U = 1{,}0B$, ${}^1U = 4{,}0B$	«0»	280 572	44,70	6,10	5,17
	«1»	219 428	46,05	4,77	5,65
	«0» и «1»	500 000	46,05	5,44	5,46
${}^0U = 0{,}5B$, ${}^1U = 2{,}7B$	«0»	234 429	27,15	2,96	2,70
	«1»	265 571	46,65	3,35	5,11
	«0» и «1»	500 000	46,65	3,16	4,09

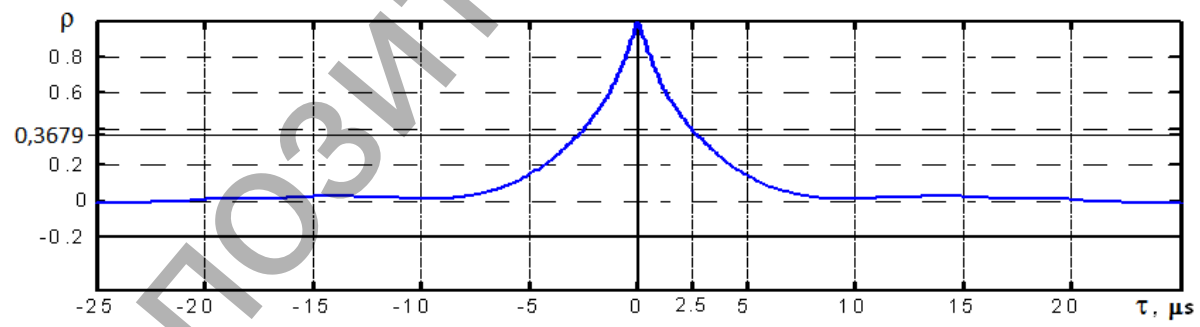

Рис. 6. Функция корреляционных коэффициентов телеграфного сигнала, преобразованного в цифровой код с порогами ${}^0U = 1{,}0B$, ${}^1U = 4{,}0B$ и центрированного на величину минус 1/2

Установлено, что статистические, а, следовательно, корреляционные и спектральные свойства телеграфного сигнала существенно зависят от выбора пороговых значений напряжения для его цифрового восстановления. Так, если сигнал, преобразованный с порогами ${}^0U = 1{,}0B$, ${}^1U = 4{,}0B$, имеет эффективную ширину спектра 0,57 *МГц*, то при назначении порогов ${}^0U = 0{,}5B$, ${}^1U = 2{,}7B$ (уровни сигналов транзисторно-транзисторной логики с диодом Шоттки) этот параметр увеличивается практически до 1 *МГц* (корреляционная длина снижается до 3,16 *мкс*). Дальнейшее увеличение эффективной ширины спектра телеграфного сигнала ограничивается конечным быстродействием (значением времени переключения до 0,7 *мкс*) компаратора IZ393 шумового модуля.

Заключение. В работе получены оценки одномерных и двумерных вероятностных характеристик аналогового и телеграфного сигналов микроэлектронного шумового модуля. В качестве одномерных характеристик определены: среднее, размах, среднеквадратическое отклонение и распределение напряжения шума (для аналогового сигнала); интенсивность и распределение длительностей импульсов (для телеграфного сигнала). Для обоих видов сигнала найдены функция корреляционных коэффициентов и корреляционная длина (двумерные характеристики).

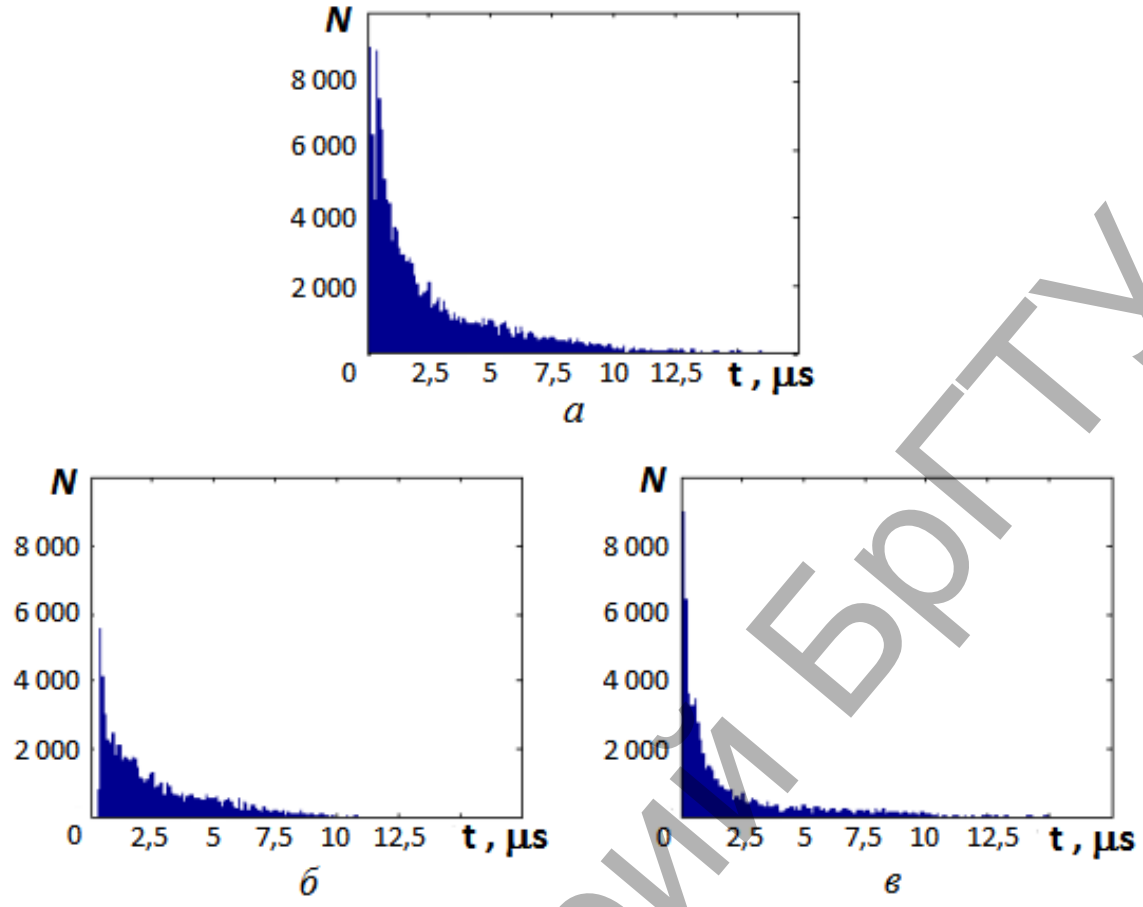

Рис. 7. Гистограммы длительностей импульсов (а), длительностей импульсов «0» (б) и длительностей импульсов «1» (в) телеграфного сигнала, преобразованного в цифровой код с порогами ${}^{0}U = 0{,}5B$, ${}^{1}U = 2{,}7B$

Аналоговый сигнал характеризуется интервалом корреляции, соответствующим нормированной граничной частоте диода-генератора шума ND201L. Распределение напряжения этого сигнала отличается от нормального закона, что обусловлено нелинейностью вольт-амперной характеристики полупроводникового прибора. При дальнейшем преобразовании сигнала интегральным компаратором напряжения IZ393, включенным по схеме повторителя, формируется сигнал телеграфного вида, который подвергается затем пороговому преобразованию (восстановлению). Перемены логических состояний преобразованного телеграфного сигнала образуют пуассоновский поток событий. Интенсивность (и корреляционная длина) такого сигнала может регулироваться выбором пороговых уровней напряжения, но ограничивается быстродействием компаратора напряжения.

Таким образом, телеграфный сигнал микроэлектронного шумового модуля, построенного на базе диода-генератора шума и интегрального компаратора напряжения, подвергнутый пороговому преобразованию, обладает вероятностными характеристиками, необходимыми для формирования случайных битовых последовательностей. Основным нормируемым параметром такого сигнала является его интенсивность (для заданных пороговых уровней напряжения), которая, для заданного алгоритма получения случайных бит, определяет скорость формирования битовой последовательности.

СПИСОК ЦИТИРОВАННЫХ ИСТОЧНИКОВ

1. Информационные технологии и безопасность. Требования безопасности к программным средствам криптографической защиты информации: СТБ 34.101.27-2011.– Введ. 2012-03-01. – Мн.: Госстандарт, 2011. – 33 с.
2. Буслюк, В.В. Кремниевые диоды-генераторы шума серии ND100 для криптографических систем / В.В. Буслюк, С.И. Ворончук, И.В. Лешкевич, С.С. Дереченник // Комплексная защита информации: материалы XIV Междунар. конф., Могилев, 19-22 мая 2009 г. – Минск, 2009. – С. 61–63.
3. Рытов, С.М. Введение в статистическую радиофизику / С.М.Рытов. – Часть 1. Случайные процессы. – М.: Наука, 1976. – 484 с.
4. Фалькович, С.Е. Основы статистической теории радиотехнических систем./ С.Е.Фалькович, П.Ю.Костенко // Харьков: Нац. аэрокосмич. ун-т «Харьк. авиац. ин-т», – 2005. –390 с.

Материал поступил в редакцию 12.01.15

RAZUMEICHYK V.S., BUSLIUK V.V., DERECHENNIK S.S., POLYAKOV V.I., LAPICH S.V. **Estimating the probability characteristics of microelectronic noise module random signals**

Random signals of microelectronic noise module where explored, which are: analogous signal of ND201L reverse-biased generator diode with filtered constant component, and telegraph signal, created with IZ393 integral voltage comparator, connected along with the repeater scheme. An algorithm for classification of actual voltage values into logical levels is developed and implemented for statistical processing of the telegraph signal, with possibility to choose threshold values.

Estimates of one- and two-dimensional probability characteristics have been calculated for both analogous and telegraph signals of the module. Telegraph signal after threshold transformation is applicable to create random bit sequences. Its characteristics (intensity and correlation length) can be regulated by threshold voltage values.