

В настоящий момент программный комплекс ВЛР включает следующие лабораторные работы:

1. Изучение полупроводникового триода.
2. Определение ширины запирающего слоя р-п-перехода и концентрации примеси в области лавинного пробоя.
3. Определение ширины запрещённой зоны полупроводника и температурного коэффициента сопротивления металла.
4. Снятие характеристик и определение параметров фотоэлемента.

Заключение. Виртуальные лабораторные работы имеют некоторые преимущества, такие как: безопасность работы, исключение поломок оборудования, наличие видеоматериалов для наглядности выполнения опытов, автоматизированный сбор и анализ данных, проверка знаний в интерактивном режиме и автоматизированная система оценки выполнения работы.

Для повышения качества подготовки студентов необходимо комбинировать работу с виртуальным и реальным оборудованием.

Виртуальные работы внедрены в учебный процесс на кафедре физики в Тульском государственном университете.

Список цитируемых источников

1. Ваннах, М. Виртуальные лабораторные работы / М. Ваннах // Компьютерра. — Б. м. : [б. и.], 2004. — № 3.
2. Зарецкая, С. Дистанционное обучение в современном мире / С. Зарецкая. — Б. м. : ИНИОН РАН, 2002.
3. Троицкий, Д. И. Виртуальные лабораторные работы в инженерном образовании / Д. И. Троицкий // Преподавание информационных технологий в Российской Федерации : сб. докл. — М. : АПКИТ, 2007. — С. 51—55.

Материал поступил в редакцию 25.02.2015 г.

УДК 517.05.512

Е. В. Ставер

Учреждение образования «Белорусского государственного университета информатики и радиоэлектроники», Минск

СТАТИСТИЧЕСКАЯ ПРОВЕРКА СЛУЧАЙНОСТИ ДВОИЧНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Введение. Сталкиваясь и работая с криптографией без генераторов случайных чисел в этом деле не обойтись. Одно из возможных применений таких генераторов — генерация ключей. Если последовательность случайных чисел предсказуема, то даже самый стойкий алгоритм шифрования, в котором данная последовательность будет использоваться, оказывается, уязвим — например, резко уменьшается пространство возможных ключей, которые необходимо «перебрать» злоумышленнику для получения некоторой информации, с помощью которой он сможет «взломать» всю систему.

Американский институт по стандартам NIST разработал набор тестов для оценки случайности последовательности чисел. О них и пойдёт речь в данной статье. Будут рассмотрены частотный блочный и частотный побитовый тесты.

Основная часть. Пакет статистических тестов, который был разработанной Лабораторией информационных технологий (англ. *Information Technology Laboratory*) [1]. В его состав входят статистические тесты, цель которых - определение меры случайности двоичных последовательностей генераторов случайных чисел. Тесты основаны на различных статистических свойствах случайных последовательностей.

Цель исследования. Целью является исследование математических методов для тестирования последовательностей с применением частотного блочного и частотного побитового теста.

Объект исследования. Объект исследования – случайные последовательности и математические методы для их тестирования.

Методы исследования. Под генерацией случайных чисел подразумевается получение последовательности из двоичных знаков 0 и 1. Генераторы случайных чисел бывают случайные — физические генераторы/датчики случайных чисел (ДСЧ/ФДСЧ) и псевдослучайные — программные датчики/генераторы случайных чисел (ПДСЧ).

Первые принимают на вход некий случайный бесконечный процесс, а на выходе дают бесконечную последовательность 0 и 1. Вторые представляют собой заданную программистом детерминированную функцию, которая инициализируется и на выходе выдаёт последовательность 0 и 1.

Частотный блочный тест. Суть теста — определение доли единиц внутри блока длиной m бит. Цель — определить, что частота повторения единиц в блоке длиной m бит приблизительно равна $m/2$ [1]. Вычисленное в ходе теста значение вероятности p должно быть не меньше 0,01. Если $p < 0,01$, последовательность не носит случайный характер (рисунок 1).

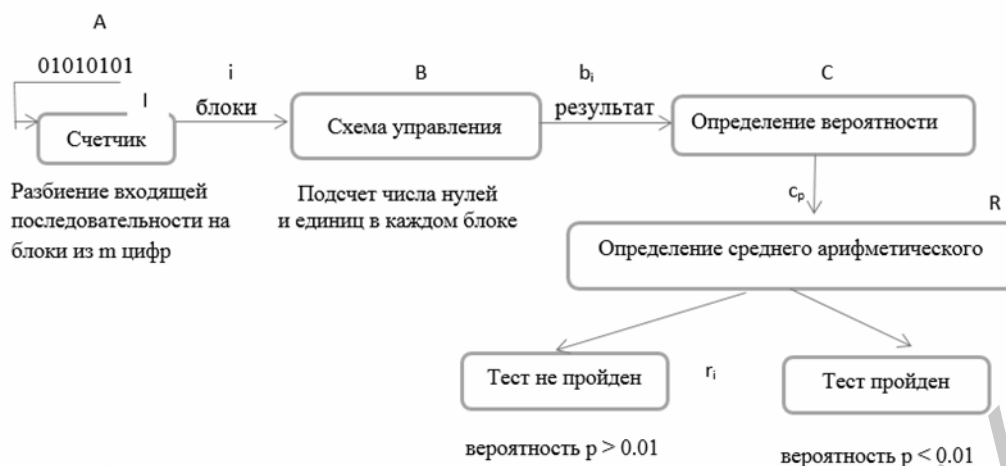


Рисунок 1 — Абстрактный автомат частотного блочного теста

Если принять $m = 1$, данный тест переходит в частотный побитовый. Рекомендуемой длиной тестируемых последовательностей согласно NIST является битовые строки по 1000 000 бит. Всего тестируется для принятия одной из гипотез 100 последовательностей.

В нашем случае, абстрактный автомат получим, если укажем алфавит A, B, C, I, R и программу P, как совокупность команд вида: $i_x, a_j \rightarrow i_y, b_y$.

В нашем случае:

$$A = \{a_1, a_2\}, B = \{b_1, b_2\}, C = \{c_1, c_2\}, I = \{i_1, i_2, \dots, i_n\}, R = \{r_1, r_2\},$$

где a_1 — пришёл 0;

a_2 — пришла 1;

b_1 — инкрементировать счетчик нулей;

b_2 — инкрементировать счетчик единиц;

c_1 — $|\text{количество нулей}/\text{количество единиц} - 1| > 0.01$;

c_2 — $|\text{количество нулей}/\text{количество единиц} - 1| < 0.01$;

i_1 — поместить число a в очередь n_1 ;

i_2 — поместить число a в очередь n_2 ;

i_n — поместить число a в очередь n_m .

$$r_1 - |\sum c_i / i| > 0.01$$

$$r_2 - |\sum c_i / i| < 0.01$$

$\delta: A \times I \rightarrow C \times B \rightarrow C \times R = \{a_1 i_1 \rightarrow b_1 c_1, a_1 i_2 \rightarrow b_1 c_1, a_1 i_n \rightarrow b_1 c_1, a_2 i_1 \rightarrow b_2 c_2, a_2 i_2 \rightarrow b_2 c_2, a_2 i_n \rightarrow b_2 c_2, b_2 c_2 \rightarrow c_2 r_2, b_2 c_2 \rightarrow c_2 r_1, b_1 c_1 \rightarrow c_1 r_1, b_1 c_1 \rightarrow c_1 r_2\}$

Частотный побитовый тест. Данный тест оценивает, насколько это соотношение близко к 1. Принимаем каждую «1» за +1, а каждый «0» за -1 и считаем сумму по всей последовательности. Кстати, говорят, что распределение количества «успехов» в серии экспериментов, где в каждом эксперименте возможен успех или неуспех с заданной вероятностью, имеет биномиальное распределение.

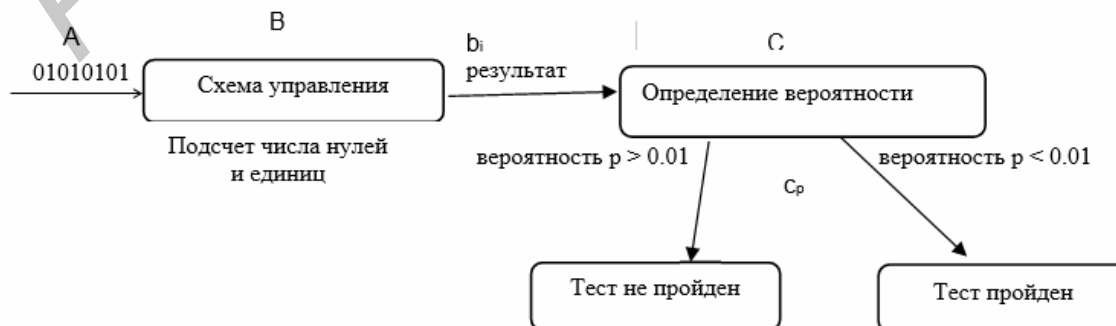


Рисунок 2 — Абстрактный автомат частотного побитового теста

Абстрактный автомат получим, если укажем алфавит A , B и C и программу P , как совокупность команд вида: $b_i a_j \rightarrow b_e c_p$.

В нашем случае:

$$A = \{a_1, a_2\}, B = \{b_1, b_2\}, C = \{c_1, c_2\}$$

где a_1 — пришёл 0;

a_2 — пришла 1;

b_1 — инкрементировать счётчик нулей;

b_2 — инкрементировать счётчик единиц;

c_1 — |количество нулей/количество единиц – 1| > 0.01;

c_2 — |количество нулей/количество единиц – 1| < 0.01.

$$\delta: Vx A \rightarrow Vx C = \{ b_1 a_1 \rightarrow b_1 c_1, b_2 a_2 \rightarrow b_2 c_2, b_1 a_1 \rightarrow b_1 c_2, b_2 a_2 \rightarrow b_2 c_1 \}.$$

Заключение. Побитный частотный тест гарантирует, что существует примерно одинаковое количество нулей и единиц. Этот тест применяется в виде одностороннего критерия хи-квадрат. Рекомендуемой длиной тестируемых последовательностей согласно NIST STS является битовые строки по 1000 000 бит. Всего тестируется для принятия одной из гипотез 100 последовательностей. Побитный частотный тест гарантирует, что существует примерно одинаковое количество нулей и единиц. Этот тест применяется в виде одностороннего критерия хи-квадрат.

Список цитируемых источников

1. Recommendation for Random Number Generation Using Deterministic Random Bit Generators (англ.) NIST SP 800-90.
2. Statistical Testing of Random Number Generators (англ.) Proceedings of the 22nd National Information Systems Security Conference, 10/99.
3. Information Systems Security Conference, 10/99.

Материал поступил в редакцию 25.02.2015 г.

УДК 681.5:621.777.4:[621.642.17:621.798-986]

А. И. Титоров

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Тульский государственный университет», Тула, Российская Федерация

АВТОМАТИЗАЦИЯ ОПРЕДЕЛЕНИЯ ПРОГНОЗНОЙ ВЕЛИЧИНЫ УДАРНОГО ВЫДАВЛИВАНИЯ ПРИ ИЗГОТОВЛЕНИИ МОНОБЛОЧНЫХ АЭРОЗОЛЬНЫХ БАЛЛОНОВ

Введение. В настоящее время аэрозольные баллоны широко применяются в нашей повседневной жизни. В Российской Федерации наблюдается огромный интерес к производству различных средств косметики и бытовой химии в аэрозольной упаковке. Наиболее распространённым материалом для их изготовления является металл: белая жёсть, чёрная жёсть, алюминий. Металлические баллоны могут состоять из трёх, двух и одной детали (моноблок). Самым популярным является трёхдетальный баллон, изготовленный из белой жести. Подобный баллон изготавливается по следующей схеме. После нанесения лакокрасочного покрытия, лист металла на специальном станке скручивается в цилиндр необходимого диаметра и сваривается по шву. Дно и крышка изготавливаются отдельно и привальцовываются к корпусу, образуя двойной шов, состоящий из пяти слоёв жести, что делает баллон более уязвимым к разрывам.

На современном этапе производства и уровне развития научно-технического прогресса, ужесточившимися требованиями к качеству отдельных элементов и изделию в целом, наибольший интерес представляют моноблочные аэрозольные баллоны из алюминия, предназначенные для упаковки товаров косметической, фармацевтической отраслей промышленности, товаров бытовой химии, автокосметики, товаров кожгалантереи и пищевой промышленности. Благодаря отсутствию швов, они отличаются высокой надёжностью в отношении прочности и герметичности.

Основная часть. Массовому производству и распространению моноблочных аэрозольных баллонов способствовали несколько важных факторов: возможность придания любой формы и любого наружного оформления, в том числе анодирования, простая технология производства. Цилиндрические корпуса таких баллонов изготавливаются из плоской заготовки (рондели) при помощи мощных пресов ударного выдавливания (рисунок 1).