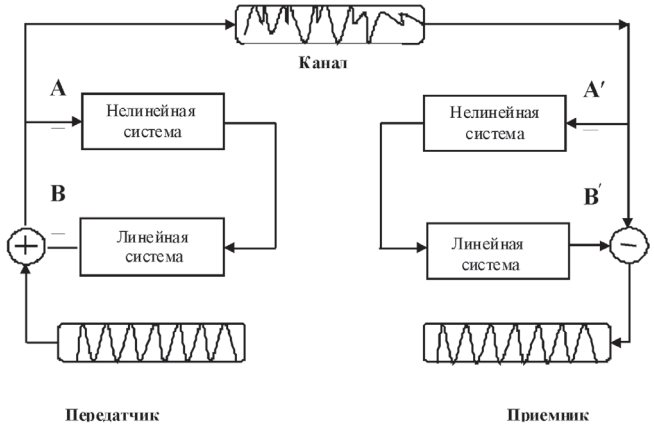

Пример схемы связи с использованием хаоса

Вывод

Идея большинства предложенных решений базируется на синхронизации приемником исходного невозмущенного хаотического сигнала, генерируемого передатчиком. С помощью таких схем связи может передаваться как аналоговая, так и цифровая информация с различными скоростями информационных потоков и разной степенью конфиденциальности. Еще одним потенциальным достоинством схем связи с использованием хаоса является возможность реализации новых методов разделения каналов, что особенно важно в многопользовательских коммуникационных системах [7- 8].

Шумоподобность и самосинхронизируемость систем, основанных на хаосе, дают им потенциальные преимущества над традиционными системами с расширением спектра, базирующимися на псевдослучайных последовательностях. Кроме того, они допускают возможность более простой аппаратной реализации с большей энергетической эффективностью и более высокой скоростью операций.

Список литературы

1. Тайлак Б.Е. Модель псевдослучайного генератора, построенного на базе хаотической системы: // Труды международной научной конференции «Наука и образование – ведущий фактор стратегии «Казахстан – 2030». – Караганда:

2. Изд-во КарГТУ, 2009. – С. 353-355.

3. Тайлак Б.Е. Генератор псевдослучайных последовательностей на базе хаотической системы // Материалы международной научно-практической конференции. – Омск – 2009.

4. Д. Кнут. Искусство программирования.– СПб.: Питер, 2000. – Т.2.

5. Marsaglia G. DIEHARD Statistical Tests.

6. Menezes A., van Oorshot P., Vanstone S. Handbook of Applied Cryptography / CSR Press. 1997.

7. Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. – М.: КУДИЦ-ОБРАЗ, 2003. – 240 с.

8. Когай Г.Д., Тайлак Б.Е., Томилова Н.И., Спанова Б.Ж. Методические основы применения хаотической динамики к криптографическому преобразованию информации. «Наука и образование – ведущий фактор стратегии «Казахстан – 2030». – Караганда: КарГТУ, – Сагиновские чтения № 5. – 2013. – Часть III.

9. Бейсенби М.А., Тен Т.Л., Когай Г.Д., Тайлак Б.Е. Управление детерминированным хаосом в распределенных сетях. Учебное пособие – Караганда: КарГТУ, 2012.

АНАЛИЗ ГЕНЕРАТОРА ПСП НА ОСНОВЕ СВОЙСТВ ХАОТИЧЕСКИХ СИСТЕМ

Когай Г.Д., Тен Т.Л.

Карагандинский государственный технический университет», Караганда, e-mail: tentl@mail.ru

Существует множество алгоритмов, обеспечивающих различные уровни криптографической защищенности, основанные на различных принципах защиты, от применения секретных алгоритмов, до использования математических методов, основанных на вычислительной сложности. Одно из современных перспективных направлений криптографической защиты информации в распределенных компьютерных сетях есть применение алгоритмов, основанных на поведенческих свойствах нелинейных динамических систем, так называемых «детерминированном хаосе».

Цель – разработать метод генерации псевдослучайных чисел на основе свойств хаотических систем. Провести анализ статистической безопасности работы генератора, используя различные методики оценки качества работы генератора. От качества работы ГСЧ зависит качество работы всей системы и точность результатов. Поэтому случайная последовательность, порождаемая ГСЧ, должна удовлетворять целому ряду критериев.

Описание алгоритма

Для исследования ПСП применяются две группы тестов [1]:

Графические тесты – статистические свойства последовательностей отображаются в виде графических зависимостей, по виду которых делают выводы о свойствах исследуемой последовательности.

Оценочные тесты – статистические свойства последовательностей определяются число-

выми характеристиками. Результаты оценочных тестов показывают степень близости свойств исследуемой и истинно случайной последовательностей.

К графическим тестам относят:

• гистограмма распределения элементов последовательности;

• распределение на плоскости;

• проверка серий;

• проверка на монотонность;

• автокорреляционная функция;

• профиль линейной сложности;

• графический спектральный тест.

Осуществляемые проверки бывают двух типов:

• проверки на равномерность распределения;

• проверки на статистическую независимость.

Анализ статистической безопасности генератора ПСП

1) Проверка на частоту появления цифры в последовательности

Рассмотрим пример. Случайное число 0.2463389991 состоит из цифр 2463389991, а число 0.5467766618 состоит из цифр 5467766618. Соединяя последовательности цифр, имеем: 24633899915467766618.

Понятно, что теоретическая вероятность pi выпадения i-ой цифры (от 0 до 9) равна 0.1.

Далее следует вычислить частоту появления каждой цифры в выпавшей экспериментальной последовательности. Например, цифра 1 выпала 2 раза из 20, а цифра 6 выпала 5 раз из 20.

Далее считают оценку и принимают решение по критерию «хи-квадрат».

2) Проверка появления серий из одинаковых цифр

Обозначим через nL число серий одинаковых подряд цифр длины L. Проверять надо все L от 1 до m, где m – это заданное пользователем число: максимально встречающееся число одинаковых цифр в серии.

В примере «24633899915467766618» обнаружены 2 серии длиной в 2 (33 и 77), т.е. n2 = 2 и 2 серии длиной в 3 (999 и 666), т.е. n3 = 2.

Вероятность появления серии длиной в L равна: pL = 9 · 10–L (теоретическая). Т.е. вероятность появления серии длиной в один символ равна: p1 = 0.9 (теоретическая). Вероятность появления серии длиной в два символа равна: p2 = 0.09 (теоретическая). Вероятность появления серии длиной в три символа равна: p3 = 0.009 (теоретическая).

Например, вероятность появления серии длиной в один символ равна pL = 0.9, т.к. всего может встретиться один символ из 10, а всего символов 9 (ноль не считается). А вероятность того, что подряд встретится два одинаковых символа «XX» равна 0.1 · 0.1 · 9, т.е. вероятность 0.1 того, что в первой позиции появится символ «X», умножается на вероятность 0.1 того, что во второй позиции появится такой же символ «X» и умножается на количество таких комбинаций 9.

Частость появления серий подсчитывается по формуле «хи-квадрат» с использованием значений pL.

Исследования на статистическую безопасность разработанного генератора были проведены по двум графическим тестам: «Гистограмма распределения элементов», «Распределение на плоскости».

Тест «Гистограмма распределения элементов» позволяет оценить равномерность распределения символов в исследуемой последовательности и определить частоту появления конкретного символа. Для построения гистограммы в сгенерированной последовательности подсчитывается, сколько раз встречается каждый элемент, после чего строится график зависимости числа появлений элементов от их численного представления (ASCII-значение для байтов). Считается, что последовательность удовлетворяет свойствам случайности, если в ней присутствуют все возможные элементы рассматриваемой разрядности, при этом разброс частот появления символов стремится к нулю. В противном случае последовательность не является случайной [1].

Тест «Распределение на плоскости» предназначен для определения зависимостей между элементами исследуемой последовательности. Для этого на поле размером (2R-1) ´ (2R-1), где R – разрядность чисел исследуемой последовательности, наносятся точки с координатами (xi; xi+1), где xi – элементы исследуемой последовательности X, $i = \overline{1,(n-1)}$, n – длина последовательности. Далее анализируется вид полученной картинки – если точки на поле расположены хаотично, то считается, что между элементами последовательности отсутствуют зависимости. Если же на поле присутствуют зависимости, т.е. получены какие-то узоры, то последовательность не является случайной. Для последовательностей большой длины хорошим результатом является абсолютно черное поле.

Для моделирования работы генератора псевдослучайных чисел на основе свойств хаотических систем была разработана компьютерная программа в среде Delphi 7.0. На рис. 1 показано рабочее окно программы «Шифратор-дешифратор», вкладка «Analysis». Входные значения чисел A, D, M и длины гаммы задаются в соответствующих полях ввода программы. В поле «Число гамм» указывается количество элементов в генерируемой последовательности. Для активизации процесса генерации ПСП служит кнопка «Генерация». В полях «Двоичный код» и «Десятичный код» выводятся сгенерированные элементы гаммы соответственно в двоичной и десятичной системе счисления [2-3].

На рис. 2 приведены результаты выполнения программы для генерации последовательности заданной длины – 100000 элементов при следующих входных данных A=1277, D=24749, M=117128.

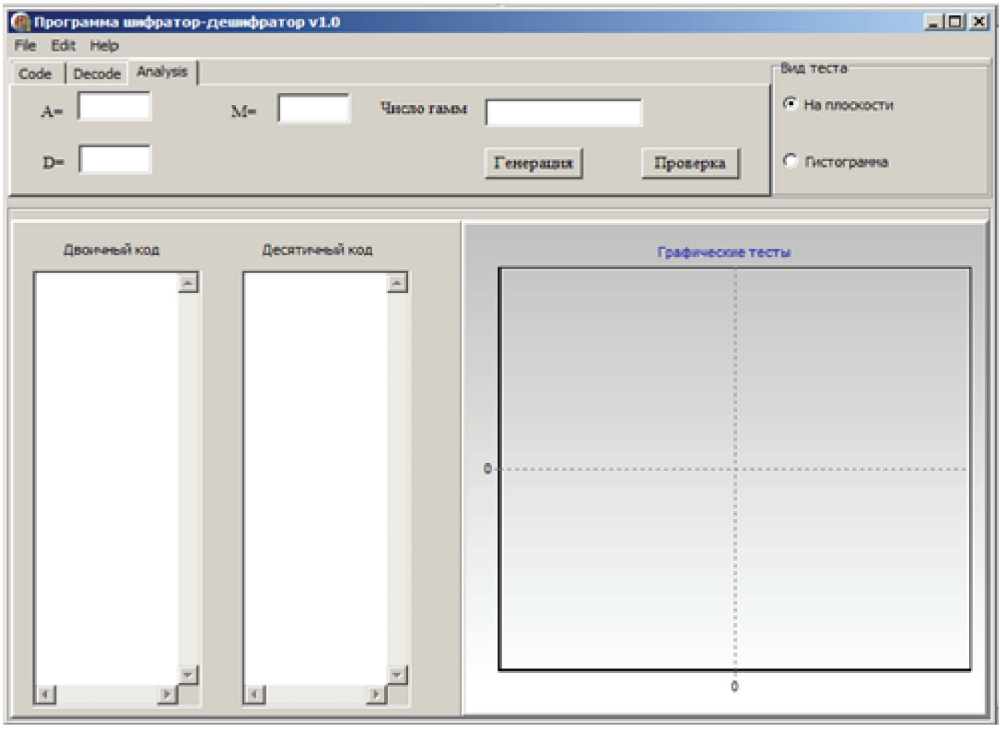

Рис. 1. Общий вид вкладки «Analysis»

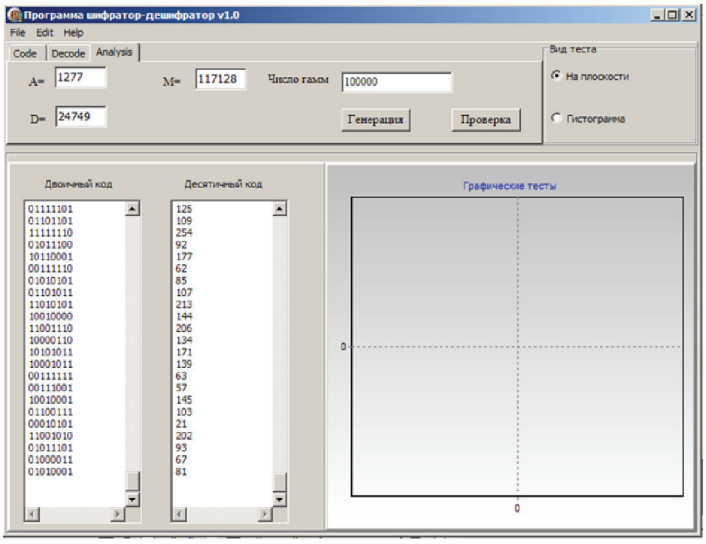

Рис. 2. Пример работы генератора с заданными параметрами

Оценка качества генераторов ПСП основана, прежде всего, на анализе статистических свойств сгенерированных последовательностей. Считается, что детерминированная последовательность конечной длины обладает хорошими псевдослучайными свойствами, если некоторая совокупность статистических критериев не позволяет отличить ее от реализации последовательности случайных чисел. Это определение не является математически строгим, поэтому

были предложены другие подходы к формализованному определения термина «случайность» [4]. Определим суть каждого подхода.

Идея частотного подхода состоит в том, что в случайной последовательности должна наблюдаться устойчивость частот встречаемости ее элементов. Например, в случайной двоичной последовательности биты 0, 1 должны встречаться независимо и с равными вероятностями не только в самой последовательности, но и в любой ее подпоследовательности, выделенной в соответствии с правилом, не коррелированным с исходными данными. Сложностной подход основан на том, что описание реализации случайной последовательности не может быть существенно короче самой этой реализации (при любом заранее фиксированном способе ее описания), т.е. если в последовательности мало размерностей, с ростом длины последовательности ее алгоритмическая сложность ненамного превышает ее длину. Количественный подход основан на том, что случайных последовательностей много, а неслучайных – мало. Неслучайными называются те последовательности, в которых наблюдаются закономерности. Последовательность случайна, если она проходит тесты, выявляющие такие закономерности. Однако если потребовать, чтобы последовательность проходила любой статистический тест, окажется, что случайных последовательностей вообще не существует. Поэтому принято ограничиваться теми тестами, для которых доля последовательностей, им не удовлетворяющих, стремится к нулю при неограниченном увеличении длины последовательности. В соответствии со статистическим подходом последовательность считается случайной, если она удовлетворяет всем таким статистическим критериям случайности, для которых сложность вычисления используемых в них статистик не выше заданной.

Экспериментальные исследования качества генератора проведены для следующих трех входных параметров A, D и M:

Пример 1. A=106, D=1283, M=6075.

Пример 2. A=421, D=17117, M=81000.

Пример 3. A=1277, D=24749, M=117128.

Вывод

Таким образом, на основе вышесказанного можно сделать вывод, что отсутствует единый подход к определению понятия «случайность», что является одной из причин существования различных наборов при исследовании ПСП на статистическую безопасность.

Список литературы

1. Дмитриев А.С. Запись и распознавание информации в одномерных динамических системах. – Радиотехника и электроника, 1991, т.5. – С.101-108.

2. Loskutov A.Yu., Tereshko V.M., Vasiliev K.A. Stabilization of chaotic dynamics of one-dimensional maps by cyclic parametric transformation. – Int. J. Bi./ and Chaos, 1996, v.6, No4. – P. 725-735.

3. Loskutov A.Yu., Shishmarev A.I. Control of dynamical systems behavior by parametric perturbations an analytic approach. – Chaos, 1994, v.4, No2, p. 351-355.

4. Архангельская А.В. Анализ подходов к определению термина «случайность». ttp://www.contrerror.tsure.ru/site/magazine4/Pdf/Journal4full.pdf

5. Тен Т.Л., Бейсенби М.А., Когай Г.Д. Разработка системы защиты информации в распределенных сетях: Монография. – Караганда, КарГТУ, 2012., с.193-197.

АНАЛИЗ СОВРЕМЕННЫХ МЕТОДОВ НАНЕСЕНИЯ ЗАЩИТНЫХ ПОКРЫТИЙ

Трефилова Н.В.

Самарский государственный технический университет, Самара, e-mail: n-dvorova@ya.ru

Развитие современной техники характеризуется повышенными требованиями, поэтому возникает необходимость повышения физико-механических и эксплуатационных свойств материалов. С увеличением содержания легирующих элементов физико-механические характеристики: прочность, твердость, износостойкость возрастают, но вероятность хрупкого разрушения повышается, также увеличивается и стоимость легированного металла. В настоящее время, это объясняет все возрастающий интерес к покрытиям. Необходимость применения покрытия, прежде всего обусловлена необходимыми эксплуатационными свойствами. Совокупность условий эксплуатации и определяет назначение покрытия, по которым они делятся на: термостойкие, жаростойкие, эрозионностойкие, износостойкие, антифрикционные, коррозионностойкие, отражающие или поглощающие различные излучения.

Все методы модификации поверхностей можно разделить на 2 большие группы:

– процессы формирования защитных покрытий, к которым можно отнести: нанесение электролитических покрытий, гальванизация, осаждение покрытий из газовой фазы методами PVD и CVD, лазерное наслаивание и т.д.

– процессы, связанные с модификацией материала уже существующих поверхностей. Наиболее продвинутые методики в этой области включают упрочнение поверхности с помощью лазерной техники, электронных пучков, имплантации ионов и т.д., а также классические методы химико-термической обработки поверхности (азотирование, борирование).

Способы получения защитных покрытий на металлические изделия различаются технологией нанесения покрытия, и основной целью создания является хорошая адгезия с подложкой, а также получение сплошного, беспористого и стойкого в данной среде защитного слоя.

В настоящее время основными способами нанесения защитного покрытия являются: гальваническое высаживание при электролизе, газотермическое напыление или металлизация, термодиффузионное насыщение в порошке, погружение в расплавленный металл, плакирование. По типу соединения защитного слоя с подложкой различают адгезионные и диффузионные металлические покрытия.