РАЗРАБОТКА ПРОГРАММНЫХ СРЕДСТВ СТАТИСТИЧЕСКОГО ТЕСТИРОВАНИЯ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Ярук А.М., Киевец Н.Г.

Корзун А.И. - кандидат технических наук, доцент

Представлены результаты тестирования случайных последовательностей по тестам FIPS-140-2 при различных программных реализациях.

Одним из основных элементов систем криптографической защиты информации является криптографический ключ. Ключи, как правило, формируются с помощью генераторов случайных последовательностей (ГСП). Ключи, отвечающие высоким требованиям к равномерности распределения вероятностей случайных чисел, должны быть получены от качественных генераторов. Качество генератора определяется путем его тестирования. Вследствие этого представляет интерес разработка инструментальных средств тестирования ГСП.

Существуют инструментальные средства тестирования ГСП. Недостатки их следующие: 1- необходимость получения результатов тестирования на промежуточных этапах, 2 – сложное теоретическое обоснование, 3 – ограниченность интервалов и промежутков тестирования. [1]

В докладе приводятся результаты тестирования, полученные с помощью программ, написанных на языках программирования вычислительной системы Matlab и JavaScript.

В качестве системы тестирования выбраны тесты стандарта FIPS-140-2, который имеет подробное теоретическое описание алгоритмов тестирования. Стандарт FIPS 140-2 является единственным стандартом, включающим статистические тесты. Стандартом рекомендованы следующие статистические тесты:

– монобитный тест (The Monobit Test);
– тест покера (The Poker Test);
– тест на подпоследовательности одинаковых бит (The RunsTest);
– тест на длинные подпоследовательности одинаковых бит (The LongRunTest). [2]

В качестве инструментальных сред выбраны два языка программирования: язык вычислительной системы Matlab и язык JavaScript. В каждой из сред на основе теоретического описания созданы алгоритмы тестирования с использованием выбранных языков программирования.

Программа Matlab [3] использована потому, что она представляет собой удобную интерактивную среду для разработки алгоритмов, визуализации и анализа данных, числовых расчетов с возможностью вывода промежуточных результатов для проверки вычислений на каждом из этапов тестирования.

JavaScript - прототипно-ориентированный сценарный язык программирования высокого уровня, позволяющий получить собственный программный продукт тестирования и разместить программу в интернете, например в «облаке» для терминального доступа.

Для каждого из означенных выше языков были составлены алгоритмы, написаны программы тестирования и выполнено тестирование в соответствии с методологией FIPS 140-2.

В качестве объекта сравнения результатов тестирования выступало время тестирования при условии задания одинаковой точности вычислений.

Результаты тестирования представлены в таблице

Таблица – Сравнение результатов тестирования

№	Тест	Время тестирования (Matlab),с	Время тестирования (JavaScript),с
1	Монобитный тест (The Monobit Test)	0,29	0,004
2	Тест покера (The Poker Test)	0,28	0,005
3	Тест на подпоследовательности одинаковых бит (The RunsTest)	0,35	0,006
4	Тест на длинные подпоследовательности одинаковых бит (The LongRunTest)	0,30	0,005
Суммарное время расчетов		1,22	0,02

Таким образом, созданы программы тестирования по FIPS 140-2 в системе Matlab и с помощью JavaScript. Суммарное время, затраченное на тестирование в программе, написанной на JavaScript примерно в 60 раз меньше, чем в Matlab. Также целесообразно использовать программу, написанную на JavaScript, при необходимости организации удаленного тестирования.

Список использованных источников:
1. FIPS 140-2 (Change Notice 1) Random Number Tests//FDK Corporstion [Electronic resource]. – 2003. – Mode of access: http://www.fdk.com/cyber-e/pdf/HM-RAE103.pdf – Date of access: 30.06.2014.
2. Н.Ф. Казакова. «Поэтапное тестирование и подбор составных элементов генераторов псевдослучайных последовательностей» - Украина: 2010 г. Журнал «Восточно-Европейский журнал передовых технологий».
3. Бондаренко, В. Ф. MatLab. Основы работы и программирования, компьютерная математика / В. Ф. Бондаренко, В. Д. Дубовец – Минск: Харвест, 2010. – 256 с.