МЕТОДИКИ ТЕСТУВАННЯ КВАНТОВИХ ГЕНЕРАТОРІВ ВИПАДКОВИХ ЧИСЕЛ

Коптєва М.В., Гріненко Т.О.
Харківський національний університет радіоелектроніки, Харків, Україна
Нарєжній О.П.
Харківський національний університет імені В.Н. Каразіна, Харків, Україна

Квантові генератори випадкових чисел (КГВЧ) найбільш широке застосування знайшли в криптографії. Генератори, які використовуються в криптографічних додатках, повинні задовольняти жорстким вимогам. Бажано, щоб вони видавали дійсно випадкову послідовність чисел. КГВЧ генерують числа, випадковість яких гарантується законами фізики, тому їх можна назвати істино випадковими числами. Для перевірки статистичних властивостей випадкових послідовностей існує досить велика кількість методик тестування, але далеко не всі вони забезпечують стовідсотковий результат [1].

Отже виникає необхідність у детальному аналізі та зрівнянні найбільш відомих методик тестування КГВЧ.

Метою доповіді є проведення порівняльного аналізу сучасних методик тестування квантових генераторів випадкових чисел з використанням пакетів статистичних тестів NIST STS [2], Diehard [3], а також серії тестів FIPS 140-3 [4].

В доповіді надані результати тестування випадкової послідовності, що була отримана з використанням КГВЧ, методиками NIST STS, FIPS 140-3 та Diehard.

Отримані результати дозволили зробити висновок, що методики NIST STS та Diehard дозволяють провести більш детальне дослідження згенерованої послідовності випадкових чисел, так як вони дають найбільш повний статистичний портрет генератора. Ці методики рекомендовано використовувати для комплексного або поточного контролю генератора. Методика FIPS 140-3 надає менш розгорнутий результат тестування і може використовуватися для оперативного контролю генератора [5].

Список літератури

1. Задков В.Н., Владимирова Ю.В. Класичні та квантові генератори випадкових чисел. *Суперкомп'ютери*. 2013. № 2. С. 12-20

2. Ruhkin A.A. Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. *NIST Special Publication 800-22*, 2010.

3. Marsaglia G. Some Difficult-to-Pass Tests of Randomness. *Journal of Statistical Software 07*. 2002. DOI: 10.18637/jss.v007.i03

4. Security requirements for Cryptographic Modules. FIPS 140-3. – U.S. Department of Commerce. 2019. DOI: 10.6028/NIST.FIPS.140-3

5. Сєвєрінов О.В. Аналіз методів побудови генераторів псевдовипадкових послідовностей. *Системи обробки інформації,* 8 (2013): 198-201.