помещениях: методика расчета: РД5.0173-87. – М.: РТП НПО "Ритм", 1988. – 160 с. 4. Халяпин Д.Б. Защита информации. Вас подслушивают? Защищайтесь! / Д.Б.Халяпин. – М.: НОУ ШО "Баярд", 2004. – 432 с. 5. Кузавков В.В. Модель розповсюдження мовного сигналу і його ізоляція вікном / В.В. Кузавков, М.В. Логінов // Зб. наук. праць ВІТІ НТУУ „КПІ" – 2010. – № 2. – С. 53–58. 6. Методика контролю захищеності мовної інформації від витоку акустичним та віброакустичним каналами: НД ТЗІ 2.3-017-08. – К.: ДССЗЗІ України, 2008. – 18 с. 7. Блінцов В.С. Головні завдання забезпечення інформаційної безпеки на водному транспорті та об'єктах морської інфраструктури / В.С. Блінцов // Сучасні проблеми інформаційної безпеки на транспорті: матеріали всеукраїнської науково-технічної конференції з міжнародною участю. – Миколаїв: НУК, 2011. – С. 24 – 27. 8. Клюкин И.И. Судовая акустика: учебное пособие / И.И. Клюкин, А.А. Клещёв. – Л.: Судостроение, 1981. – 144 с.

УДК 621.317.083

Ю. Костів, В. Максимович, М. Мандрона, Ю. Рибак
Національний університет "Львівська політехніка",
кафедра безпеки інформаційних технологій

ВИКОРИСТАННЯ СТАТИСТИЧНИХ ТЕСТІВ НІСТ США ДЛЯ ДОСЛІДЖЕННЯ ГЕНЕРАТОРІВ М –ПОСЛІДОВНОСТЕЙ

Сформульовано вимоги до генераторів псевдовипадкових імпульсних послідовностей при їх використанні в криптографії та для імітації вихідних сигналів дозиметричних детекторів. Наведено результати тестування п'яти генераторів М-послідовності і на їх основі зроблено висновки щодо випадковості їх вихідних сигналів.

Ключові слова: генератори псевдовипадкових чисел, захист інформації, псевдовипадкові числа, статистичні характеристики.

The paper presents the requirements for pseudorandom pulse sequence generators for their use in simulation of the dosimeter detectors output signals, as well as for their use in cryptography. The paper presents the results of testing of five M – sequences generators and conclusions about their randomness.

Key words: pseudorandom generator, protection of information, pseudorandom numbers, statistic characteristics.

Вступ

Генератори псевдовипадкових чисел (ГПЧ) і псевдовипадкових імпульсних послідовностей (ГПІП) широко використовуються в багатьох сферах вимірювальної техніки, зокрема, для проектування і налагодження дозиметричних пристроїв, та інформаційних технологій. При цьому вимоги до їх технічних характеристик відрізняються залежно від мети їхнього застосування.

Генерування псевдовипадкових послідовностей і перевірка випадковості згенерованої послідовності є одними з найважливіших проблем сучасної криптології. Генератори псевдовипадкових послідовностей використовуються в сучасних криптосистемах для створення ключової інформації і забезпечення параметрів цих систем.

Відомо, що для реалізації криптографічних перетворень використовують різні псевдовипадкові послідовності. Звідси випливає, що стійкість криптоперетворень безпосередньо залежить від алгоритму формування псевдовипадкових чисел та послідовностей.

Метою роботи є використання статистичних тестів Національного інституту стандартів і технологій (НІСТ) США для тестування генераторів М-послідовностей.

Вимоги до генераторів псевдовипадкових чисел і генераторів псевдовипадкових імпульсних послідовностей

У разі використання ГППП для імітації вихідних сигналів дозиметричних детекторів ставляться такі вимоги [1]:

– статистичні характеристики вихідних сигналів ГППП повинні забезпечувати можливість перевірки метрологічних характеристик дозиметрів з урахуванням установлених вимог до останніх;

– період повторення псевдовипадкової імпульсної послідовності має перевершувати час вимірювання параметрів іонізуючих випромінювань;

– швидкодія ГППП має забезпечувати формування вихідних імпульсів у заданому частотному діапазоні;

– ГППП повинні забезпечувати можливість оперативної зміни середньої частоти вихідних імпульсів, що дає змогу досліджувати динамічні властивості вимірювальних пристроїв.

ГПЧ і ГППП є одними з найважливіших структурних елементів сучасних криптосистем. Генератори псевдовипадкових послідовностей, які використовуються в криптографії, повинні [2]:

– проходити статистичні тести на випадковість;

– проходити «тест на наступний біт». Суть тесту така: не повинно існувати поліноміального алгоритму, який, знаючи перші k біт випадкової послідовності, зможе передбачити k +1 біт з імовірністю понад 50 %;

– залишатися надійними навіть у випадку, коли частина або всі його стани стали відомі (або були коректно обчислені). Це означає, що не повинно бути можливості отримати випадкову послідовність, знаючи параметри генератора;

– мати хороші статистичні властивості, тобто псевдовипадкова послідовність за статистичними властивостями не повинна відрізнятися від істинно випадкової послідовності;

– мати великий період формованої послідовності;

– мати ефективну апаратну і програмну реалізацію.

Одним із типів ГПЧ, що широко використовуються у вимірювальній техніці, є генератори М-послідовностей. Основними їх перевагами є висока швидкодія і простота побудови. Вони не належать до криптостійких, однак можуть бути використані як складові криптографічних систем.

Генератори М-послідовностей

М-послідовність, або послідовність максимальної довжини, – псевдовипадкова двійкова послідовність, породжена регістром зсуву з лінійними зворотними зв'язками і максимальним періодом.

Варіанти побудови ГПЧ на основі генератора М-послідовностей необхідно розглядати, враховуючи рівняння його функціонування

$$Q(t+1) = T^r Q(t), \qquad (1)$$

де Q(t) і Q(t+1) – стани регістра генератора двійкової послідовності в моменти часу t і t+1 (до і після синхроімпульсу), T – квадратна матриця порядку N вигляду

$$T_1 = \begin{vmatrix} a_1 & a_2 & \dots & a_{N-1} & a_N \\ 1 & 0 & & 0 & 0 \\ 0 & 1 & & 0 & 0 \\ & & & & \\ 0 & 0 & \dots & 1 & 0 \end{vmatrix} \text{ або } T_2 = \begin{vmatrix} 0 & \dots & 0 & 0 & a_N \\ 1 & \dots & 0 & 0 & a_{N-1} \\ & & & & \\ 0 & \dots & 1 & 0 & a_2 \\ 0 & \dots & 0 & 1 & a_1 \end{vmatrix}$$

N – степінь многочлена

$$\Phi(x) = \sum_{i=0}^{N} a_i x^i, \quad a_N = a_0 = 1, \quad a_j \in \{0,1\}, \quad j = \overline{1,(N-1)}, \qquad (2)$$

r – натуральне число.

Якщо k=1 і $T=T_1$, генератор має вигляд, поданий на рис. 1, а при k=1 і $T=T_2$ – на рис. 2.

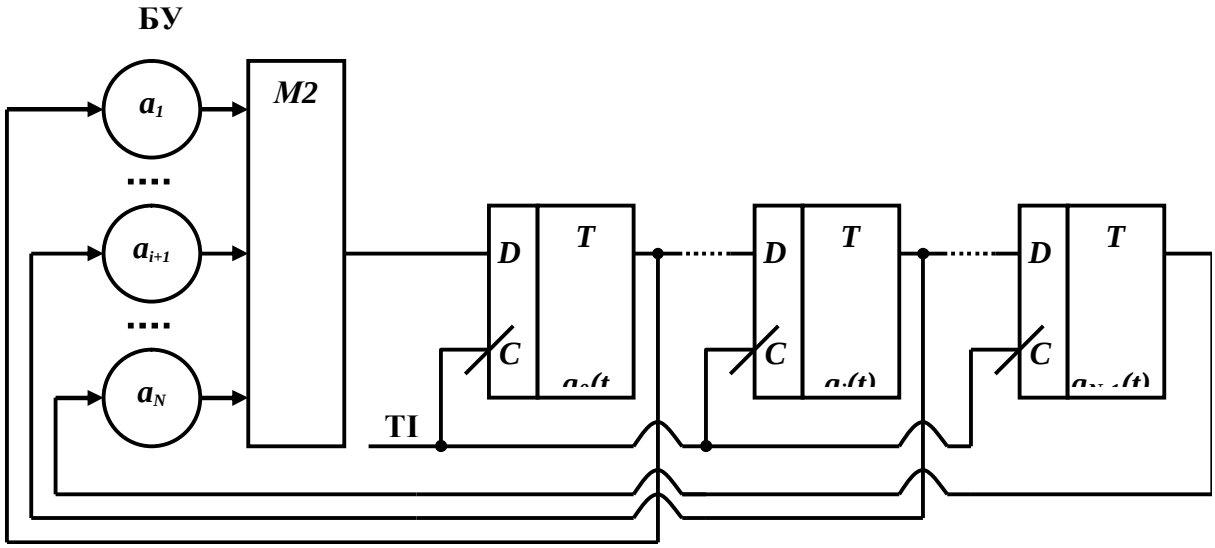

Рис. 1. Схема генератора, якщо k = 1 і T = T_1

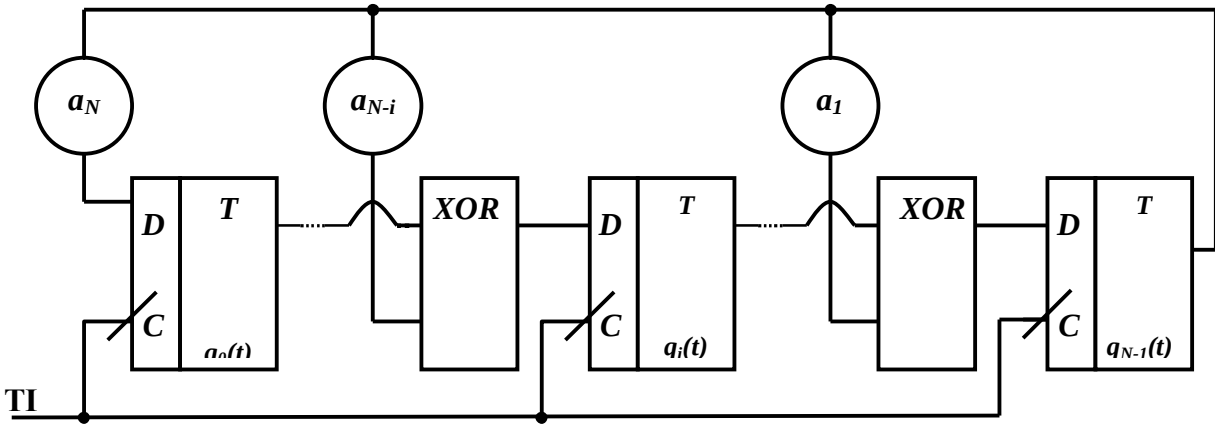

Рис. 2. Схема генератора, якщо k=1 і T= T_2

Отже, генератори М-послідовностей відрізняються:

– степенем і видом твірного полінома, що задають кількість розрядів регістра зсуву і впливають на форму зворотних зв'язків;

– виглядом (T_1 чи T_2) і степенем r матриці, що задають спосіб формування зворотних зв'язків і формують їх остаточну конфігурацію.

Пакет статистичних тестів Національного інституту стандартів і технологій

Національний інститут стандартів і технологій (США) (The National Institute of Standards and Technology) – підрозділ управління з питань технологій США, одного з агентств міністерства торгівлі США. Місія Інституту – "просувати" інноваційну та індустріальну конкурентоспроможність США шляхом розвитку наук про виміри, стандартизації та технології з метою підвищення економічної безпеки та покращення якості життя.

Статистичні тести НІСТ [3] – пакет статистичних тестів, розроблений головною організацією НІСТ, яка є лабораторією інформаційних технологій (Information Technology Laboratory). До складу пакета входять 15 статистичних тестів, метою яких є визначення міри випадковості двійкових послідовностей, згенерованих апаратними чи програмними засобами. Ці тести основані на різних статистичних властивостях, притаманних тільки випадковим послідовностям.

Ці статистичні тести застосовуються для порівняння псевдовипадкових послідовностей з істинно випадковою послідовністю.

Результати статистичного тесту повинні інтерпретуватися з певною обережністю і застереженнями, щоб уникнути неправильних висновків про досліджуваний генератор.

Статистичні тести НІСТ призначені для перевірки певної нульової гіпотези H_0 про те, що послідовність, яка перевіряється, є випадковою. З цією нульовою гіпотезою пов'язана альтернативна гіпотеза H_a про невипадковість послідовності. Для кожного тесту отримують висновок, що дає змогу відхилити нульову гіпотезу, ґрунтуючись на сформованій досліджуваним генератором послідовності.

Кожен тест оснований на обчисленні значення тестової статистики, яка є функцією даних.

Тестова статистика використовує обчислення значення P-value, за допомогою якого і визначається, чи певна послідовність є випадковою. Якщо значення P-value дорівнює 1, то послідовність абсолютно випадкова; P-value, яке дорівнює 0, вказує, що послідовність абсолютно невипадкова. Для тесту необхідно вибрати рівень значущості α. Якщо значення P-value більше або дорівнює α, то приймається нульова гіпотеза, тобто послідовність є випадковою. Якщо значення P-value менше за α, то нульова гіпотеза відхиляється, тобто послідовність не є випадковою. Як правило, значення α вибирається в інтервалі [0.001, 0.01].

Якщо значення α дорівнює 0.001, це говорить про те, що з 1000 випадкових послідовностей тест не пройде лише одна. Якщо P-value>0.001, послідовність розглядається як випадкова із імовірністю 99.9 %. При P-value<0.001 послідовність розглядається як невипадкова з імовірністю 99.9 %. Якщо значення α дорівнює 0.01, це свідчить про те, що з 100 випадкових послідовностей тест не пройде лише одна. При P-value>0.01 послідовність розглядається як випадкова із імовірністю 99 %. Якщо P-value<0.01, послідовність розглядається як невипадкова з імовірністю 99 % [1].

Методика тестування генераторів псевдовипадкових чисел на випадковість

Процес дослідження генераторів псевдовипадкових чисел на випадковість складається з таких кроків:

1. Генерація псевдовипадкової послідовності для тестування.
2. Виконання набору статистичних тестів.
3. Аналіз проходження статистичних тестів.
4. Прийняття рішення щодо випадковості досліджуваної послідовності.

У цій роботі для генерації псевдовипадкових послідовностей використовуються п’ять генераторів М-послідовностей, побудованих на основі многочленів $\Phi(x)=1+x^{19}+x^{24}$, $\Phi(x)=1+x^{9}+x^{14}+x^{29}$, $\Phi(x)=1+x^{11}+x^{19}+x^{25}+x^{31}$, $\Phi(x)=1+x^{18}+x^{31}$, $\Phi(x)=1+x^{10}+x^{12}+x^{19}+x^{24}+x^{30}$.

Для тестування генераторів використовуються сім тестів з пакета НІСТ:

1. Частотний побітовий тест.
2. Частотний блоковий тест.
3. Тест на послідовність однакових бітів.
4. Тест на найдовшу послідовність одиниць в блоці.
5. Спектральний тест.
6. Тест перевірки серій.
7. Тест приблизної ентропії.

На основі цих тестів написано програми мовою C#.

Тестами № 1, 2, 3, 4, 6, 7 досліджуються послідовності довжиною 1048576 біт, а тестом № 5 – послідовність довжиною 262144 біти.

Результати проходження статистичних тестів оцінюють в процесі аналізу тестової статистики. Існує три варіанти оцінки тестової статистики:

1. Аналіз на основі порогового значення. Якщо тестова статистика менша або більша від порогового значення, тоді послідовність не є випадковою.

2. Аналіз на основі фіксованих інтервалів. Якщо тестова статистика виходить за межі встановленого інтервалу, послідовність не є випадковою.

3. Аналіз на основі імовірнісних значень. Для тестової статистики обчислюється значення P-value.

Оскільки для перших двох варіантів необхідно наперед розрахувати порогові значення і фіксовані інтервали, третій варіант оцінки тестової статистики є найефективнішим.

Для того, щоб генератор пройшов тест, значення змінної P-value повинно бути більшим за рівень значущості α, тобто за 0,01, в іншому випадку тест не пройдений. Коли тест пройдений, послідовність вважається випадковою з імовірністю 99 %. Якщо значення P-value дорівнює 1, то послідовність абсолютно випадкова; те, що P-value дорівнює 0, вказує, що послідовність абсолютно невипадкова, отже, чим більше значення змінної P-value, отриманої під час тестування, тим ближчі властивості досліджуваної послідовності до властивостей абсолютно випадкової послідовності.

Параметри досліджуваних генераторів

У цій роботі тестуються п’ять генераторів М-послідовностей, які побудовані на основі таких многочленів:

$\Phi(x)=1+x^{19}+x^{24}$ – генератор М-послідовності варіант А;

$\Phi(x)=1+x^{9}+x^{14}+x^{29}$ – генератор М-послідовності варіант Б;

$\Phi(x)=1+x^{11}+x^{19}+x^{25}+x^{31}$ – генератор М-послідовності варіант В;

$\Phi(x)=1+x^{18}+x^{31}$ – генератор М-послідовності варіант Г;

$\Phi(x)=1+x^{10}+x^{12}+x^{19}+x^{24}+x^{30}$ – генератор М-послідовності варіант Д.

У генераторах використовується матриця вигляду T_1, степінь матриці r = 1.

Результати тестування генераторів М-послідовностей

У таблиці наведено результати тестування п’яти генераторів М-послідовностей статистичними тестами НІСТ.

Результати тестування ГПІП

	Генератор М-послідовності варіант А	Генератор М-послідовності варіант Б	Генератор М-послідовності варіант В	Генератор М-послідовності варіант Г	Генератор М-послідовності варіант Д
Частотний побітовий тест	+	+	+	+	+
Значення P-value	0,490	0,817	0,453	0,964	0,828
Частотний блоковий тест	+	+	+	+	+
Значення P-value	0,824	0,905	0,919	0,866	0,783
Тест на послідовність однакових бітів	+	+	+	+	+
Значення P-value	0,857	0,521	0,752	0,565	0,256
Тест на найдовшу послідовність одиниць в блоці	+	+	+	+	+
Значення P-value	0,624	0,230	0,492	0,277	0,778
Спектральний тест	-	+	+	+	+
Значення P-value	0,00021	0,445	0,752	0,143	0,035
Тест перевірки серій	+	+	+	+	+
Значення P-value1 і P-value2	0,087 0,022	0,890 0,718	0,331 0,140	0,585 0,285	0,815 0,893
Тест приблизної ентропії	+	+	+	+	+
Значення P-value	0,114	0,850	0,535	0,507	0,972

Висновки

Як видно з результатів тестування, генератор М-послідовності (варіант А) з семи тестів не пройшов лише один тест – спектральний тест. Це означає, що в послідовності є близько розташовані один до одного повторювані ділянки, що, своєю чергою, демонструє відхилення від випадкового характеру досліджуваної послідовності. Отже, цей генератор не можна використовувати у криптографії, проте його можна використати як елемент складнішої криптографічної системи. Всі інші генератори пройшли всі сім тестів, що свідчить про перспективи їхнього використання в криптографії за умови додаткового дослідження їх на криптостійкість.

1. Методи і засоби опрацювання вихідних сигналів дозиметричних детекторів / Ю.Я. Бобало, В.Б. Дудикевич, В.М. Максимович, В.О. Хорошко та ін. – Львів : Видавництво Нац. ун-ту "Львівська політехніка", 2009. – 200 с. 2. Горбенко І.Д. Прикладна криптологія / І.Д. Горбенко, Ю.І. Горбенко. – Харків: Форт, 2012. – 870 с. 3. NIST SP 800-22. A Statistic Test Suite for Random and Pseudorandom Number Generators for Cryptographic Application: [Електронний ресурс]. April 2000. – Режим доступу: http://csrc.nist.gov./publications/niatpubs//SP800-22rev1a.pdf.

УДК 681.322.067

О.А. Нємкова[1], В.М. Чаплига[1], З.А. Шандра[2]
[1]Львівський інститут банківської справи,
[2]Національний університет "Львівська політехніка"

СТІЙКИЙ МОБІЛЬНИЙ ЗВ'ЯЗОК В УМОВАХ ШТУЧНИХ ЗАВАД

Розглянуто можливість стійкого передавання сигналу мобільного зв'язку за рахунок спеціальної модуляції. Доведено існування критерію, залежно від якого передача є задовільною. В результаті комп'ютерного моделювання в MathCAD надано рекомендації стосовно параметрів модуляції залежно від параметрів шумів.

Ключові слова: мобільний зв'язок, глушники мобільних телефонів, завадостійкість, швидке перетворення Фур'є.

This work deals with the possibility of the steady signal transmission at the expense of its special modulation. It is shown, that there is a criterion, at implementation of which, the reproduction of the signal is satisfactory. By means of computer modeling by MathCAD recommendations about definition of parameters of modulation, proceeding from character of noise are given.

Key words: mobile communications, cell phone silencers, noise immunity, Fast Fourier transform.

Вступ

Розвиток науки і техніки характеризується тим, що часто співіснують винаходи та розробки пристроїв, основна мета функціонування яких зовсім протилежна. Пристрої, створені для однієї задачі, іноді також використовуються для зовсім протилежної. Не оминула ця доля і мобільний зв'язок. Після широкого впровадження серед населення мобілок, систем дистанційного керування у гігагерцевому діапазоні, навігаторів тощо почався процес впровадження пристроїв, які блокують можливість встановлення мобільного зв'язку, для яких би цілей він не був застосований. Цікаво, що на будь-яке застосування того чи іншого пристрою знаходять обґрунтування, хоча не виключена