УДК 621.391 **DOI:10.30837/rt.2020.4.203.14**

О.А. ЗАМУЛА, д-р техн. наук, І.Д. ГОРБЕНКО, д-р техн. наук, ХО ЧІ ЛИК

СТАТИСТИЧНІ ВЛАСТИВОСТІ ПОХІДНИХ СИСТЕМ СИГНАЛІВ

Вступ

Завадозахищеність інформаційно-комунікаційних систем (ІКС), і одна з її складових, – структурна скритність системи, у значній мірі визначаються структурними або статистичними властивостями сигналів-переносників даних користувачів системи. Досягнення необхідних значень завадозахищеності, скритності, криптографічної стійкості може бути реалізовано на основі використання в радіоканалах динамічного режиму передачі даних в поєднанні із застосуванням дискретних складних сигналів, що володіють заданою структурною скритністю, необхідними кореляційними і ансамблевими властивостями. У свою чергу відомо [1], що для технології розширеного спектру зазначені властивості сигналів тотожні властивостям дискретних послідовностей (ДП), згідно із законом яких маніпулюють параметрами високочастотної несучої. Динамічний режим передбачає такий спосіб передачі інформації по радіоканалу, при якому здійснюється динамічна зміна за певним (випадковим) законом відповідності: «інформаційний біт – складний сигнал». Момент зміни відповідності повинен визначатися керуючої послідовністю (УП) або гамою.

Проведений аналіз [1 – 3] показав, що у даний час відсутні регулярні методи синтезу ДП оптимальних за мінімаксним критерієм. Завдання синтезу ДП виявляється ще складнішим, якщо висуваються вимоги до розмірності (об'єму) системи сигналів, структурним властивостям і числу елементів ДП. Таким чином, досить актуальною проблемою залишається пошук ефективних методів синтезу дискретних сигналів (послідовностей), що відповідають потенційно можливим граничним характеристикам кореляційних функцій (мінімаксним властивостям або границі «щільної упаковки») і володіють необхідними кореляційними, структурними, статистичними, ансамблевими властивостями.

У [4] авторами запропоновано метод синтезу похідних систем сигналів, для яких у якості вихідних застосовуються ортогональні сигнали, а у якості таких, що продукують, – нелінійні дискретні складні криптографічні сигнали (КС). Синтез останніх засновано на використанні випадкових (псевдовипадкових) процесів, у тому числі алгоритмів криптографічного перетворення інформації. Показано [5], що синтезовані таким чином похідні сигнали володіють покращеними (у порівнянні з лінійними класами сигналів) ансамблевими і кореляційними властивостями, тоді як статистичні властивості таких систем сигналів є не вивченими.

Вимоги до статистичних властивостей сигналів – переносників даних

Очевидно, що вимоги до статистичних властивостей сигналів відповідають вимогам, що пред'являються до генераторів, які формують випадкові (псевдовипадкові) послідовності. Крім того, повинна існувати можливість виконати оцінку відповідності властивостей синтезованих сигналів певним вимогам.

Методи формування послідовностей символів для додатків керуючих сигналів і сигналів-переносників інформації можна розділити на два великі класи – випадкові (фізичні) і псевдовипадкові [6 – 7]. Засоби, що забезпечують генерацію випадкових послідовностей чисел або бітів, будемо називати генераторами випадкових послідовностей (ГВП), а генератори, що забезпечують генерацію псевдовипадкових послідовностей (ПВП), – детермінованими генераторами випадкових послідовностей (ДГВП). ДГВП є одним з базових примітивів для більшості криптографічних додатків. Одним з основних властивостей і переваг ДГВП є забезпечення відновленності послідовності в просторі і часі. У той же час ПВП повинні мати гарантовані властивості щодо періоду повторення, відновлення відрізків ПВП в просторі і часі, можливість проведення попереднього дослідження їх властивостей і інше [6]. При цьому необхідно враховувати, що ніякий детермінований алгоритм не може генерувати повністю випадкові послідовності, він може тільки апроксимувати деякі властивості випад-

кових послідовностей. Більшість ДГВП мають ряд серйозних недоліків, а послідовності, які генеруються такими генераторами, не відповідають вимогам, що пред'являються криптографічними додатками і додатками, пов'язаними з реалізацією динамічного режиму функціонування систем зв'язку зі складними сигналами.

Основними недоліками ДГВП є:

– неприпустимо короткий або недоведений період повторення послідовності;

– недостатня нерозрізненість гами, що також робить її певним чином передбачуваною «вперед і назад»;

– властивості випадковості, рівноймовірності, незалежності та однорідності не відповідають вимогам і інші.

Існує кілька підходів до визначення вимог до рівнів гарантій ДГВП. Перший підхід пов'язаний з тестуванням ПВП на нерозрізненість, для чого, наприклад, застосовуються федеральні стандарти FIPS 140-1, FIPS 140-2, FIPS 140-3. Більш детальні вимоги і механізми реалізації визначені в AIS 20, що дозволяє реалізувати різні рівні гарантій: К1, К2, К3, К4 [8].

Основними загальними вимогами до ДГВП є [6]:

- вимога нерозрізненості вихідних послідовностей ДГВП від істинно випадкових послідовностей;

- вимога непередбачуваності вихідних бітів для порушника з обмеженими обчислювальними ресурсами;

- вимога незворотності генератора в сенсі попередньо заданої малої ймовірності компрометації ключа самого ДГВП.

Таким чином, ПВП повинна мати деякі статистичні властивості [9], які притаманні істинно випадковим послідовностям.

Найбільш прийнятними (з точки зору практичного використання) методиками тестування є: FIPS PUB 140-1, AIS 20 і AIS 31, NIST 800-90b, NIST 800-22. До складу NIST 800-22 [10] входять 16 статистичних тестів, при цьому обчислюються 188 значень ймовірностей. Всі тести спрямовані на виявлення різних дефектів випадковості (невідповідність вимогам випадковості).

Порядок тестування.

1. Висувається нульова гіпотеза H_0 – припущення про те, що двійкова послідовність, яка підлягає тестуванню, є випадковою.

2. Для послідовності, що формується генератором, розраховується статистика тесту.

3. З використанням спеціальної функції і статистики тесту розраховується значення ймовірностей $P \in [0,1]$.

4. Значення ймовірності P порівнюється з рівнем значущості α, $\alpha \in [0,001; 0,01]$. Якщо $P \geq \alpha$, то гіпотеза H_0 приймається. В іншому випадку приймається альтернативна гіпотеза.

В результаті тестування ПВП символів формується вектор значень ймовірності $\mathrm{P} = \{\mathrm{P}_1, \mathrm{P}_2, ..., \mathrm{P}_{188}\}$. У NIST використовуються два пороги для прийняття рішення про результати тестування – це 0.96 і 0.99, тобто для різних рівнів значимості встановлюється, що з 100 блоків може не пройти чотири і один тест відповідно.

Основні результати досліджень

З використанням NIST SP 800-22 було виконано тестування реалізацій похідних криптографічних послідовностей символів (ПКПС). Для тестування із залученням NIST SP 800-22 для точності розрахунків необхідно мати послідовність символів довжиною не менше 100. Для тестування було синтезовано 20 похідних сигналів на основі криптографічних послідовностей з періодом $N = 1024$. Для тестування ПКПС були застосовані наступні тести NIST SP 800-22: частотний побітовий тест (monobit test), частотний блоковий тест (frequency within block test), тест на послідовність однакових біт (runs test), тест на найдовшу послідовність

з одиниць в блоці (the longest run test), спектральний тест (spectral test), тест на підпослідовності (serial test). Результати тестування за зазначеними тестами наведено у табл. 1 – 6.

Таблиця 1

Результати тестування похідних сигналів (ПКПС) з $N = 1024$ (монобітний тест)

Номер похідного сигналу	Кількість «1»	Кількість «0»	$P-value$	$P-value > 0.01$
1	515	509	0.8512686236882057	Так
2	515	509	0.8512686236882057	Так
3	497	527	0.34850142376108484	Так
4	503	521	0.5737754036327304	Так
5	492	532	0.21129954733371054	Так
6	478	546	0.033586612896897634	Так
7	522	502	0.5319710580974011	Так
8	518	506	0.7076604666545525	Так
9	522	502	0.5319710580974011	Так
10	530	494	0.26058903427361774	Так
11	538	486	0.10416255883043911	Так
12	518	506	0.7076604666545525	Так
13	516	508	0.8025873486341526	Так
14	526	498	0.38157390570502125	Так
15	538	486	0.10416255883043911	Так
16	512	512	1.0	Так
17	529	495	0.2880087580039419	Так
18	551	473	0.014789214221761392	Так
19	511	513	0.9501646619415056	Так
20	515	509	0.8512686236882057	Так

Таблиця 2

Результати тестування похідних сигналів (ПКПС) з $N = 1024$ (частотний блоковий тест)

Номер похідного сигналу	Кількість блоків	Довжина блоків	$P-value$	$P-value > 0.01$
1	51	20	0.33940489399393925	Так
2	51	20	0.5534531438608977	Так
3	51	20	0.8813982930103362	Так
4	51	20	0.6488836444446106	Так
5	51	20	0.40437005733917836	Так
6	51	20	0.3748688142935794	Так
7	51	20	0.5293703452563876	Так
8	51	20	0.7456190658758038	Так
9	51	20	0.5293703452563878	Так
10	51	20	0.6872742496942255	Так
11	51	20	0.2927697888058552	Так
12	51	20	0.2678516820668022	Так
13	51	20	0.9033253460171587	Так
14	51	20	0.9188302753065043	Так
15	51	20	0.1469610705317797	Так
16	51	20	0.7456190658758047	Так
17	51	20	0.4736606532819697	Так
18	51	20	0.35338907550154847	Так
19	51	20	0.9073701122564067	Так
20	51	20	0.2500343356092065	Так

Таблиця 3

Результати тестування похідних сигналів (ПКПС) з $N = 1024$ (тест на послідовність однакових біт)

Номер похідного сигналу	π	$2/\sqrt{n}$	$V(obs)$	$P-value$	$P-value > 0.01$
1	0.5029296875	0.0625	509	0.8521250020025395	Так
2	0.5029296875	0.0625	503	0.5745108154065952	Так
3	0.4853515625	0.0625	522	0.5137393123371727	Так
4	0.4912109375	0.0625	499	0.4220554377618176	Так
5	0.48046875	0.0625	507	0.7917222651893452	Так
6	0.466796875	0.0625	499	0.5000821445021373	Так
7	0.509765625	0.0625	526	0.3747852254608464	Так
8	0.505859375	0.0625	517	0.7512906048863373	Так
9	0.509765625	0.0625	529	0.2823222794660727	Так
10	0.517578125	0.0625	537	0.10870671148349663	Так
11	0.525390625	0.0625	488	0.15527454436985028	Так
12	0.505859375	0.0625	525	0.4139245820069865	Так
13	0.50390625	0.0625	513	0.9486062978096323	Так
14	0.513671875	0.0625	521	0.5572946676001701	Так
15	0.525390625	0.0625	504	0.6755378568281317	Так
16	0.5	0.0625	519	0.6617487760817584	Так
17	0.5166015625	0.0625	513	0.9220226305700431	Так
18	0.5380859375	0.0625	487	0.16609336473330275	Так
19	0.4990234375	0.0625	538	0.10413523041859732	Так
20	0.5029296875	0.0625	489	0.1508741397898685	Так

Таблиця 4

Результати тестування похідних сигналів (ПКПС) з $N = 1024$
(тест на найдовшу послідовність з одиниць в блоці)

Номер похідного сигналу	M	K	N	χ^2	$P-value$	$P-value > 0.01$
1	8	3	16	2.5848131767158087	0.4601582158650065	Так
2	8	3	16	4.910991740701903	0.17843200168629486	Так
3	8	3	16	2.840887683858429	0.4168132306658415	Так
4	8	3	16	2.299431426250259	0.5126298393652022	Так
5	8	3	16	1.4862582449817263	0.6854455326497724	Так
6	8	3	16	2.3224200745898065	0.508239427919698	Так
7	8	3	16	3.1691947567842096	0.3662670999085182	Так
8	8	3	16	10.258130285753692	0.01649468713031408	Так
9	8	3	16	0.2232915342847958	0.9736854118111586	Так
10	8	3	16	1.966671701487854	0.5793528537379324	Так
11	8	3	16	10.946509638593566	0.012018662584735648	Так
12	8	3	16	1.0802337929911223	0.7818477379705312	Так
13	8	3	16	4.754440741329501	0.19068693056675992	Так
14	8	3	16	0.519846469107887	0.9145094314246653	Так
15	8	3	16	3.0901474502960573	0.37793397002883145	Так
16	8	3	16	0.5456175029974611	0.9087605671831471	Так
17	8	3	16	0.5456175029974611	0.9087605671831471	Так
18	8	3	16	5.474477981185082	0.14017311067991284	Так
19	8	3	16	0.9697299296305197	0.8085758557302485	Так
20	8	3	16	0.3992037675828323	0.9404034454800299	Так

Таблиця 5

Результати тестування похідних сигналів (ПКПС) з $N = 1024$ (спектральний тест)

Номер похідного сигналу	H_0	N_1	$P-value$	$P-value > 0.01$
1	486.4	483	0.32955189239856303	Так
2	486.4	480	0.06645742001693215	Так
3	486.4	480	0.06645742001693215	Так
4	486.4	478	0.016002207003436186	Так
5	486.4	486	0.9086766781799538	Так
6	486.4	480	0.06645742001693215	Так
7	486.4	481	0.12148844104797517	Так
8	486.4	486	0.9086766781799538	Так
9	486.4	490	0.30189844442852465	Так
10	486.4	486	0.9086766781799538	Так
11	486.4	486	0.9086766781799538	Так
12	486.4	491	0.1871221556836583	Так
13	486.4	488	0.6463551955394854	Так
14	486.4	492	0.10829365589900763	Так
15	486.4	492	0.10829365589900763	Так
16	486.4	490	0.30189844442852465	Так
17	486.4	485	0.6880685751927309	Так
18	486.4	485	0.6880685751927309	Так
19	486.4	486	0.9086766781799538	Так
20	486.4	485	0.6880685751927309	Так

Крім того, було проведено тестування ПКПС з використанням стандарту FIPS-140. Для того щоб виконати тести FIPS-140, необхідно мати 20000 символів. В цьому випадку було вирішено «склеїти» 20 ПКПС з періодом $N = 1024$, які використовувались при тестуванні за тестами NIST SP 800-22 SP. Були використані наступні статистичні тести FIPS-140: частотний побітовий тест (monobit test), тест покеру (poker test), тест на послідовність однакових біт (runs test), тест на найдовшу послідовність з одиниць/нулів (the longest run test). Результати тестування ПКПС за зазначеними тестами наведено в табл. 7 – 8.

Таблиця 6

Результати тестування похідних сигналів (ПКПС) з $N = 1024$ (тест на підпослідовності)

Номер	ψ_m^2	ψ_{m-1}^2	ψ_{m-2}^2	$\nabla\psi_m^2$	$\nabla^2\psi_m^2$	$P-value1$	$P-value2$	$P > 0.01$
1	5.28125	2.015625	0.1328125	3.265625	1.3828125	0.91659944429465	0.847176717754098	Так
2	14.3125	3.015625	0.4609375	11.296875	8.7421875	0.18543852707816513	0.06787671836894967	Так
3	9.0	3.578125	2.1484375	5.421875	3.9921875	0.71167936424658895	0.40706418913507897	Так
4	9.125	4.28125	1.3984375	4.84375	1.9609375	0.77413839112877647	0.7429435663716482	Так
5	12.40625	6.625	3.265625	5.78125	2.421875	0.67171988224295573	0.6586777475527147	Так
6	31.65625	18.59375	9.796875	13.0625	4.265625	0.10971720056655933	0.37124935114918887	Так
7	11.90625	4.21875	1.546875	7.6875	5.015625	0.46457579096932533	0.28569802683920476	Так
8	5.40625	0.5625	0.34375	4.84375	4.625	0.77413839112877647	0.32798191520517467	Так
9	18.5	9.0625	1.78125	9.4375	2.15625	0.30674264714918487	0.7070464216929457	Так
10	22.625	12.6875	4.78125	9.9375	2.03125	0.26944004415793343	0.73001099814728893	Так

11	34.25	19.0625	7.53125	15.1875	3.65625	0.055600554198860314	0.4545210498689997	Так
12	9.8125	2.5	0.84375	7.3125	5.65625	0.5033219991047654	0.22633255639493863	Так
13	9.8125	4.8125	0.125	5.0	0.3125	0.7575761331330662	0.9889930346992064	Так
14	12.75	6.625	1.78125	6.125	1.28125	0.6332322827218166	0.8645486214149056	Так
15	50.1875	19.75	5.53125	30.4375	16.21875	0.00017685119110517008	0.0027392506072084983	Ні
16	4.03125	1.28125	0.140625	2.75	1.609375	0.9490538343829868	0.8071061737365048	Так
17	8.78125	3.875	2.2578125	4.90625	3.2890625	0.767547686281258	0.5106670730463856	Так
18	36.21875	23.4375	14.5234375	12.78125	3.8671875	0.11960103247709221	0.42427835448812967	Так
19	8.46875	5.3125	2.6484375	3.15625	0.4921875	0.9241725499586169	0.9742570565851398	Так
20	12.6875	6.828125	2.3203125	5.859375	1.3515625	0.662980451379133	0.852568453615844	Так

Таблиця 7

Результати тестування похідних сигналів (ПКПС) з $N = 1024$
(монобітний тест, тест покеру, тест на максимальну довжину серії FIPS-140)

Назва тесту	X	Умова успішного тесту	X задовольняє умові
Монобітний тест	10104	$9654 < X < 10346$	Так
Тест покеру	16.806400000000394	$1.03 < X < 57.4$	Так
Тест на максимальну довжину серії	12	$X < 34$	Так

Таблиця 8

Результати тестування похідних сигналів (ПКПС) з $N = 1024$ (тест серій FIPS-140)

Символ	Довжина серії						Тест пройдено
	1	2	3	4	5	6+	
«1»	2504	1245	605	298	159	187	Так
«0»	2540	1248	605	303	141	162	Так

Висновки

Численні дослідження статистичних властивостей похідних нелінійних криптографічних послідовностей символів із застосуванням NIST SP 800-22, FIPS-140 показали, що параметри, які оцінюються при реалізації відповідних тестів, знаходяться в межах допустимих значень. А це, в свою чергу, означає, що похідні системи сигналів, для яких у якості сигналів, що продукують, застосовуються нелінійні дискретні складні криптографічні сигнали, задовольняють вимогам, що пред'являються до псевдовипадкових послідовностей: непередбачуваність, незворотність, випадковість, незалежність символів і ін. По суті такі сигнали не відрізняються від випадкових послідовностей. Таким чином, використання саме таких похідних сигналів як фізичного переносника даних дозволить поліпшити показники завадозахищеності і інформаційної безпеки сучасних ІКС.

Список літератури:

1. Sarvate D.V. Crosleration Properties of Pseudorandom and Related Sequences / D.V. Sarvate, M.V. Parsley // IEEE Trans. Commun. 1980. Vol. Com 68. P. 59–90.

2. Варакин Л. Е. Системы связи с шумоподобными сигналами. Москва : Сов. радио. 1985. 384 с.

3. Ipatov Valery P. Spread Spectrum and CDMA. Principles and Applications / University of Turku, Finland and St. Petersburg Electrotechnical University ‘LETI’. Russia. John Wiley & Sons Ltd. The Atrium, Southern Gate, Chichester, West Sussex PO19 8SQ, England. 2005. 385 p.
4. Gorbenko I. D., Zamula A. A., Ho Tri Luk Synthesis of derivatives of complex signals based on nonlinear discrete sequences with improved correlation properties // Радіотехніка. 2019. Вип. 199. С. 110-120.
5. Gorbenko I. D., Zamula A. A., Tri Luc Ho Derived signals systems for information communication systems applications: synthesis, formation, processing and properties // International Conference problems of info communications science and technology PIC S&T′2020. 6-9. October 2020. Kharkov, Ukraine. P. 3-10.
6. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Теорія. Практика. Застосування. Харків : Форт, 2012. 880 с.
7. Горбенко Ю.І. Побудова, аналіз, стандартизація та застосування криптографічних систем ; за ред. І.Д. Горбенко. Харків : Форт, 2015. 959 с.
8. Application Notes and Interpretation of the Scheme (AIS) 20. Functionality classes and evaluation methodology for physical random number generators. Certification body of the BSI in context of certification scheme. BSI, 1999.
9. Andrea Rock. Pseudorandom Number Generators for Cryptographic Applications // Diplomarbeit zur Erlangung des Magistergrades an der Naturwissenschaftlichen Fakultat der Paris-London-Universitat Salzburg. Salzburg, 2005.
10. NIST 800-22 A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, 2000.

Надійшла до редколегії 17.10.2020

Відомості про авторів:

Замула Олександр Андрійович – д-р техн. наук, професор, професор кафедри безпеки інформаційних систем і технологій, факультет комп’ютерних наук, Харківський національний університет імені В.Н. Каразіна, Україна; email: zamylaaa@gmail.com, ORCID: http://orcid.org/0000-0002-8973-6190

Горбенко Іван Дмитрович – д-р техн. наук, професор, професор кафедри безпеки інформаційних систем і технологій, факультет комп’ютерних наук, Харківський національний університет імені В.Н. Каразіна, головний конструктор АТ «Інститут інформаційних технологій», Україна; e-mail: GorbenkoI@iit.kharkov.ua, ORCID: https://orcid.org/0000-0003-4616-3449

Хо Чі Лик – магістрант кафедри безпеки інформаційних систем і технологій, факультет комп’ютерних наук, Харківський національний університет імені В.Н. Каразіна, Україна.