Bilyy L. A., Tsyhanchuk R. O.

The method of determination of difference equations approximating differential equations. To reduce the amount of difference equations while maintaining the desired accuracy of the approximation is appropriate, taking into account the large number of members of the decomposition of the desired solution in a Taylor series. Factors such approximations are the method of undetermined coefficients.

Key words: *continuous time, discrete time, dynamic model, differential equations, difference equations, approximation.*

Білий Леонід Адамович – професор, доктор технічних наук, професор кафедри економічної кібернетики Львівського інституту банківської справи Університету банківської справи Національного банку України (м. Київ);

Циганчук Роман Олегович – завідувач редакційного сектору видавництва Університету банківської справи Національного банку України (м. Київ).

УДК 004.056.57:656.2

О. А. Нємкова

RS-АНАЛІЗ В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ СИСТЕМ ПОТОКОВОГО ШИФРУВАННЯ

Застосовано RS-аналіз до деяких генераторів псевдовипадкових послідовностей і розраховано значення коефіцієнта Хьорста. Установлена відповідність результатів аналізу до статистичних властивостей генераторів. Запропоновано використовувати RS-аналіз для тестування генераторів псевдовипадкових послідовностей на наявність персистентності, іншими словами – перевіряти генератори на придатність для застосування у криптографії.

Ключові слова: *генератор псевдовипадкової послідовності, коефіцієнт Хьорста, потокове шифрування, лінійний конгруентний генератор, персистентність.*

Постановка проблеми. Відкритість сучасних інформаційних систем, у яких відбувається обробка, збереження та передавання таємної інформації, потребує застосування криптографічних перетворень великих масивів даних. Якість криптографічного перетворення повинна бути дуже високою, тому що переважно це стосується передавання та зберігання банківської інформації, закритих баз даних мобільних операторів, медичних і фармацевтичних компаній, військових розробок та інших даних, що пов'язані з державною

таємницею. Зростаюча кількість кібератак за останні роки підтверджує висновок про необхідність надійного захисту, чого можна досягти лише за допомогою шифрування даних.

Останнім часом можна почути пропозиції шифрувати значну кількість інформації, яка не тільки передається назовні з локальної корпоративної мережі, а й зберігається на жорстких дисках у системі. У деяких випадках потрібне швидке криптографічне закриття інформації. Зазвичай для цього використовують потокове шифрування, яке базується на генерації високоякісних псевдовипадкових послідовностей. Перевагами потокового шифрування є його відносна простота і відсутність розмноження помилок. Процес шифрування полягає в генерації гами і подальшого накладання її на потік даних. Стійкість шифрів, утворених за допомогою гами, суттєво залежать від її стохастичних властивостей, а також від довжини періоду гами.

Важливість тематики обумовила побудову достатньо великої кількості генераторів псевдовипадкових послідовностей. Генерація псевдовипадкових послідовностей відбувається, як правило, алгоритмічно, за певними правилами. Такі послідовності мають більшу чи меншу довжину, або період, після якої вони починають повторюватись. До того ж такі послідовності можуть виявитися криптографічно нестійкими. Тому при створенні чергового псевдовипадкового генератора важливо довести, що він видає послідовність, яка наближається до випадкової.

На нинішній день не існує універсальних і перевірених на практиці критеріїв або методик для визначення якості гами та її придатності до шифрування. Для непередбачуваності гами прийнято вважати, щоб її період був набагато більшим за довжину послідовності даних, що шифруються, а різноманітні комбінації бітів визначеної довжини були рівномірно розповсюджені по всій її довжині.

Спосіб перевірки послідовностей, точніше часових рядів, на випадковість був запропонований достатньо давно, майже сто років тому. Галузь знань, у який він уперше був випробуваний, була далека від криптографії. Спосіб має назву *RS*-аналіз і застосовується в наш час переважно для аналізу фінансових часових рядів [1], хоча об'єктом аналізу може бути будь-яке явище природи та суспільства. Найважливішою особливістю *RS*-аналізу є те, що наперед не ставиться ніяких обмежень стосовно закону розподілу ряду, який досліджується. Власне, у результаті аналізу можна стверджувати, наскільки ряд близький до суто випадкового. Кількісною ознакою цього слугує показник Хьорста. Для суто випадкового процесу показник Хьорста становить 1/2. Цікаво, що переважна більшість природних явищ, а також величин часових процесів фінансової природи характеризуються показником Хьорста, більшим за 1/2. Такі процеси отримали назву процесів із довгою пам'яттю, або

персистентних. Система на наступному ході нібито пам'ятає, що було з нею на попередніх ходах і зберігає таку тенденцію. Іншими словами, якщо відхилення від рівноваги були значними на попередніх ходах, то і на наступному ході варто очікувати значного відхилення. *RS*-аналіз використовують для перевірки наявності в ряду даних довготривалої залежності.

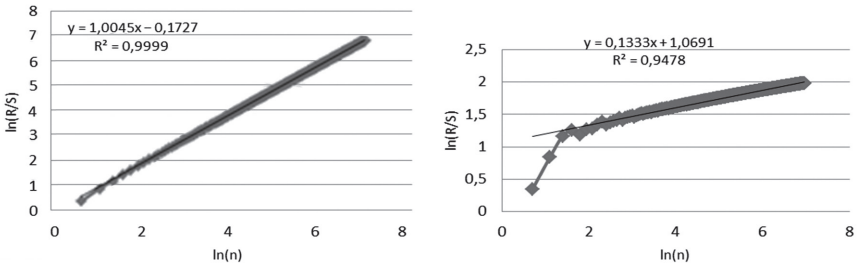
У нашій роботі *RS*-аналіз застосовується для дослідження якості генераторів псевдовипадкових послідовностей.

Методологія *RS*-аналізу. Нехай є послідовність a_n. Утворюється послідовність часткових сум A_n. Вираховуються такі числові характеристики: сер. зн. A_n – середнє арифметичне елементів A_n, послідовність R_n – розмах накопичених сум (різниця максимального і мінімального значень часткових сум відхилення елементів a_n від середнього арифметичного A_n), послідовність S_n – середнє квадратичне відхилення a_n від сер. зн. A_n, послідовність $RS_n = R_n/S_n$. На площині будується множина точок $(x_n; y_n) = [ln(n); ln(RS_n)]$. Надалі застосовується метод найменших квадратів для визначення кутового коефіцієнта тренду. Цей кутовий коефіцієнт називається коефіцієнтом Хьорста і позначається літерою *H*. Знання коефіцієнта Хьорста дозволяє отримати значення розмірності Мінковського $d = 2 - H$ [2].

Перед перевіркою гами, отриманої шляхом генерації, за методом *RS*-аналізу слід переконатись, що у граничних випадках, таких як лінійна або квадратична залежність, а також періодична залежність із коротким періодом виходить достовірний результат.

У результаті виконання чисельного експерименту для послідовності, значення елементів якої утворюють лінійну залежність від номера, отримане значення коефіцієнта Хьорста дорівнює одиниці, як і очікувалося (*рис. 1*а). Такий самий результат отримано для квадратичної залежності. Виходячи з основних положень цієї теорії, слід очікувати такий же результат у разі монотонної визначеної залежності.

При дослідженні короткоперіодичної послідовності значення коефіцієнта Хьорста повинно становити малу величину, значно меншу за одиницю. Якщо скористатись аналогією з відхиленням рухомої частинки від початкової точки, то випадок лінійної залежності від номера відповідає прямолінійному рівномірному руху, тому віддаль частинки прямо пропорційна часу. Ейнштейн послуговувався цією методикою для виведення формули для розрахунку віддалення броунівської частинки від початку руху, його частинка рухалася хаотично – кожний рух після наступного удару не був пов'язаний із попереднім. Якщо ж частинка коливається з малою амплітудою навколо початкової точки, то її віддаль від місця початку руху не перевищує амплітуди коливань і фактично не росте з часом. Розрахунки підтверджують цей висновок (*рис. 1б*).



а) б)

Рис. 1: **а) значення *H* дорівнює 1,00 для лінійної залежності, б) значення *H* дорівнює 0,13 для короткоперіодичної послідовності**

Таким чином, отримані результати для лінійної та короткоперіодичної залежності вкладаються в теорію.

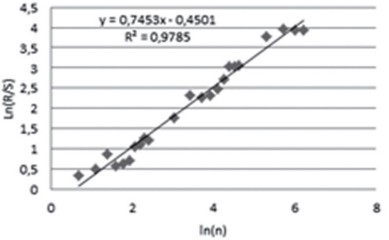
Дослідження деяких псевдовипадкових послідовностей. У наш час існує достатня кількість генераторів псевдовипадкових послідовностей. Тим не менш, отримати псевдовипадкову послідовність можна трьома шляхами: скористатися готовими таблицями, скористатися вбудованими у програми генераторами або використати заданий алгоритм. У цій роботі перевірялися псевдовипадкові послідовності, узяті з трьох типів джерел.

На *рис. 2а*) представлені результати розрахунку коефіцієнта Хьорста для п'ятизначних випадкових чисел, узятих із таблиці 26.11 [3]. Хоча числа позиціонувались як випадкові, результати проведеного аналізу дають підставу стверджувати, що вони не є суто випадковими, послідовність персистентна.

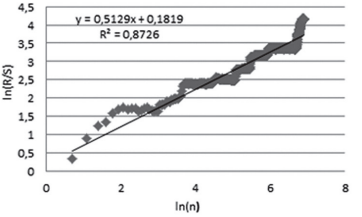
Як другу послідовність було досліджено результат роботи генератора rnd(1). Цей генератор визначений у програмі MathCAD як такий, що генерує білий шум – випадкову послідовність із рівномірним розподілом на відрізку [0; 1]. Результати перевірки представлено на *рис. 2б*). Можна стверджувати, що даний генератор (із критерієм *H*) наближається до ідеального (кожне наступне число дуже слабо пов'язане з попереднім, дуже слабо – за критерієм Хьорста). Його варто використовувати для генерації псевдовипадкової послідовності в модельних експериментах. Такий процес для руху броунівських частинок говорить про те, що відстань, на яку віддаляється частинка з часом від початку руху, пропорційна квадратному кореню з часу (формула Ейнштейна).

Третім досліджуваним генератором був лінійний конгруентний генератор. Як відомо, такі генератори не можуть бути використані у криптографії. Уперше лінійні конгруентні генератори зламав Дж. Рідс, а потім Дж. Бояр. Послідовність чисел може бути прорахована, для цього достатньо знання трьох сусідніх значень. З часом Дж. Бояр вдалося зламати квадратичні та кубічні гене-

ратори. Надалі за її ідеями були зламані будь-які поліноміальні генератори, тим самим доведена неможливість їх використання у криптографії. Тим не менш, для задач математичного моделювання ці генератори широко використовуються.



а)



б)

Рис. 2: **а) значення *H* дорівнює 0,745 для послідовності, узятої з таблиць; б) значення *H* дорівнює 0,513 для генератора rnd(1)**

У свій час Національне бюро стандартів Сполучених Штатів рекомендувало таблицю констант, при використанні яких конгруентні генератори мають задовільні статистичні властивості та достатню довжину [4]. Для перевірки поведінки лінійного конгруентного генератора було згенеровано кілька послідовностей для рекомендованих значень констант *a*, *b*, *m* і розраховано коефіцієнти Хьорста для кожної з них. Результати розрахунків представлено в *табл.*

Таблиця

Коефіцієнт Хьорста для лінійного конгруентного генератора залежно від довжини послідовності та констант *a*, *b*, *m*

a	*b*	*m*	Переповнення при	*H*
106	1 283	6 067	2^{20}	0,612
211	1 663	7 875	2^{21}	0,653
421	1 663	7 875	2^{22}	0,617
939	1 399	6 655	2^{23}	0,679
859	2 531	11 979	2^{24}	0,760
141	28 411	134 456	2^{25}	0,648
1 255	6 173	29 282	2^{26}	0,537
1 021	24 631	116 640	2^{27}	0,649
1 277	24 749	117 128	2^{28}	0,684
2 311	25 367	120 050	2^{29}	0,545
3 613	45 289	214 326	2^{30}	0,563
8 121	28 411	134 456	2^{31}	0,546
9 301	49 297	233 280	2^{32}	0,626
2 416	374 441	1 771 875	2^{33}	0,578
17 221	107 839	510 300	2^{34}	0,786
84 589	45 989	217 728	2^{35}	0,577

Значення коефіцієнта Хьорста із *табл.* підтверджують висновок про наявність залежності в досліджуваних послідовностях. Відхилення від величини 1/2 не можна списати за рахунок точності розрахунку. Слід відмітити, що за деяких значень векторів ініціалізації спостерігалися значення коефіцієнта Хьорста менші за 1/2 (ці результати не показано в *табл.*). Це означає, що в послідовностях були короткоперіодичні фрагменти, подібні один до одного, і на довжині обчислень таких короткоперіодичних фрагментів було багато.

Відмітимо, що за допомогою застосованого аналізу можна підібрати значення констант, що дають значення коефіцієнта Хьорста, більш близьким до 1/2, дозволяючи будувати послідовності з непоганими властивостями для інших прикладних задач, окрім криптографічного захисту.

Таким чином, результати аналізу підтверджують висновок про наявність залежності між елементами послідовності для лінійних конгруентних генераторів. Це дає підстави зробити такий висновок: *RS*-аналіз дає змогу виявити нестохастичність генератора псевдовипадкових послідовностей.

Висновки. *RS*-аналіз застосовано до деяких генераторів псевдовипадкових послідовностей – більш детально досліджено лінійні конгруентні генератори. Для досліджуваних генераторів розраховано значення коефіцієнта Хьорста. Установлено відповідність результатів аналізу до статистичних властивостей генераторів. Запропоновано використовувати *RS*-аналіз для тестування генераторів псевдовипадкових послідовностей на стохастичність (відсутність персистентності).

Список використаних джерел

1. Петерс Э. Фрактальний анализ финансовых рынков. Применение теории хаоса в инвестициях и экономике. – М.: Интернет-трейдинг, 2004. – 304 с.
2. Ширяев А. Н. Основы стохастической финансовой математики. – М.: Фазис, 1998. – Т. 1. – 512 с.
3. Справочник по специальным функциям с формулами, графиками и математическими таблицами / Под ред. М. Абрамовица и И. Стиган. – М.: Наука, главная редакция физико-математической литературы, 1979. – 832 с.
4. Есин В. И., Кузнецов А. А., Сорока Л. С. Безопасность информационных систем и технологий. – Х.: ООО «ЭДЭНА», 2010. – 656 с.

Немкова Е. А.

RS-анализ в информационной безопасности систем поточного шифрования

Проанализированы некоторые генераторы псевдослучайных чисел и рассчитаны значения коэффициента Хёрста с использованием RS-анализа. Установлено соответствие результатов анализа статистическим свойствам генераторов. Предложено использовать RS-анализ для тестирования генераторов псевдослучайных чисел на наличие персистентности, другими словами, проверять генераторы на возможность использования в криптографии.

Ключевые слова: *генератор псевдослучайной последовательности, коэффициент Хёрста, поточное шифрование, линейный конгруэнтный генератор, персистентность.*

Nyemkova E. A.

RS-analysis in information security of streaming encryption's systems

The article deals with the RS-analysis is used for some generators of pseudorandom sequences and values of the Hirst coefficient are calculated. The correspondence is established of analysis results to the statistical properties of generators. It is proposed to use the RS-analysis for testing of generators of pseudorandom sequences for the presence of persistent, in other words, to check the suitability of generators for use in cryptography.
Key words: *pseudorandom sequence generator, coefficient Hirst, streaming encryption, linear congruent generator, persistence.*

Нємкова Олена Анатоліївна – кандидат фізико-математичних наук, доцент кафедри економічної кібернетики Львівського інституту банківської справи Університету банківської справи Національного банку України (м. Київ).

УДК 330.4:378

О. В. Горбачевська, І. Я. Горбачевський

ПРО ВИКОРИСТАННЯ МАТЕМАТИЧНОГО АПАРАТУ ПРИ РОЗВ'ЯЗУВАННІ ЕКОНОМІЧНИХ ЗАДАЧ

Досліджуються підходи до математизації курсу економічної теорії шляхом використання в задачах матметодів. Розглядаються основні типи економічних задач і матметоди їх розв'язання.

Ключові слова: *економічні задачі, математизація економіки, математичний апарат, економічна теорія.*

Постановка проблеми. Викладання марксистсько-ленінської політекономії в основному зводилося до заучування термінів і законів. Сучасна економіка перестала бути гуманітарною наукою і потребує певного рівня математичної підготовки. Для того, щоб привити практичну доцільність, варто в підготовці студентів вивчати економічні задачі. Розв'язання більшості з них передбачає використання математичного апарату і, відповідно, вимагає достатніх знань із різних розділів математики. При цьому хороша економічна задача має бути складена так, щоб для її розв'язання студент мусив упевнено