вагонопотоками у межах МТК за умови інтероперабельності транспортної системи// Збірник наукових праць ДонІЗТ – Донецьк: ДонІЗТ, 2011.4.*Козак В.В., Данько М.І., Альошинський Є.С., Шварьов Д.А*. Практичні рекомендації з оптимізації функціонування транспортного комплексу міжнародних вантажних залізничних перевезень// Вагонный парк. № 2. – Харьков, 2011.– С.4-7.

Поступила в редколлегию 27.06 .2011

УДК 519.876.5.:621.391; 621.391:519.72

О.О. СКОПА, канд.техн.наук, доц.Одеського державного економічного університету

ІНСТРУМЕНТАЛЬНІ ЗАСОБИ СТАТИСТИЧНОГО ТЕСТУВАННЯ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ

Проведений аналіз стану розвитку інструментальних засобів для тестування псевдовипадкових послідовностей, вживаних в криптографії та особливості застосування критерію згоди χ^2.
Ключові слова: псевдовипадкова послідовність, криптографічне перетворення, криптографія, генератор псевдовипадкової послідовності, кофіденційність, цілісність, достовірність, критерій згоди

Проведен анализ состояния развития инструментальных средств для тестирования псевдослучайных последовательностей, применяемых в криптографии и особенности применения критерия согласия χ^2.
Ключевые слова: псевдослучайная последовательность, криптографическое превращение, криптография, генератор псевдослучайной последовательности, конфиденциальность, целостность, достоверность, критерий согласия

The analysis of development of tools status is conducted for testing of pseudocasual sequences, applied in cryptography and feature of application the criterion of consent χ^2.
Keywords: pseudo-random sequence, kriptografiches-something conversion, cryptography, pseudorandom generator of the sequence, confidentiality, integrity, reliability, criterion of consent

Постановка проблеми в загальному вигляді та її зв'язок з науковими і практичними завданнями

В даний час, в області захисту конфіденційності інформації, яка передається в інформаційно-телекомунікаційних системах, спостерігається тенденція заківленості до проблеми розробки потокових шифрів. Такі шифри, на відміну від блокових шифрів, хоча й поступаються в криптографічній стійкості, володіють вищою продуктивністю, що дозволяє використовувати їх в реальному масштабі часу. Саме через ці причини, європейським криптологическим співтовариством ECRYPT був оголошений відкритий конкурс (2004...2008 р.) на розробку нових потокових шифрів – eSTREAM (*ECRYPT STREAM Cipher Project*) [1] з метою виявлення найбільш гідного претендента на використання в якості стандарту для країн європейського співтовариства. Розробка подібних шифрів зводиться до побудови генераторів шифруючих гам, які по своїх статистичних властивостях максимально наближаються до випадкових послідовностей з рівномірним законом розподілу вірогідності формованих символів. Алгоритми формування псевдовипадкових послідовностей (ПВП) з високим ступенем «випадковості»

знаходять широке застосування і при створенні захищених криптографічних протоколів як формувачі ключової інформації. Хоча завдання побудови рівномірно розподілених псевдовипадкових послідовностей в своїй постановці просте, насправді його рішення пов'язане з цілим поряд проблем, які вимагають проведення серйозних наукових досліджень і глибокого володіння математичним апаратом в області статистики. І те й інше не може не викликати серйозних труднощів у інженерів, що займаються практичною реалізацією функцій захисту інформаційних процесів.

Аналіз наукової та технічної літератури (наприклад [2...4]) показує, що до теперішнього часу розроблена достатньо велика кількість інструментальних засобів, що дозволяють здійснювати попередній аналіз придатності криптографічних перетворень, які породжуються генераторами ПВП, для потреб криптографії. Ці пакети прикладних програм реалізують набори тестів, покликані дати відповідь на питання, чи можливо, знаючи деяку ділянку формованої гамми, передбачити подальший (або попередній) її символ з вірогідністю, відмінною від 0,5? При негативній відповіді формована гамма визнається дійсно випадковою. Програмне забезпечення і опис наборів цих тестів є загальнодоступним і може бути отримане через інтернет-сайти їх розробників.

Проблема, проте, полягає в тому, що використання пропонованого програмного забезпечення припускає глибокий комплексний аналіз готового продукту. Описи цих тестів, що додаються, містять комплексні програми випробувань датчиків ПВП і процедури обчислення узагальненого показника якості, які враховують результати від усіх тестів, що входять до складу пакету. Ці тести дозволяють виявляти різні види аномалій в псевдовипадковій послідовності, які, в принципі, можуть бути використані як уразливості криптоалгоритму для організації на їх основі атаки з боку зловмисників.

В той же час, інженерам-розробникам необхідні інструментальні засоби, що реалізовують прості й надійні процедури тестування на початкових і проміжних етапах створення генераторів, які дозволяють переконається в правильності вибраного шляху. З цієї причини розробники алгоритмів формування ПВП, як правило, часто пропонують власні засоби випробування, що підтверджують якість створеного програмного продукту і далеко не завжди використовують комплекти тестів, рекомендовані NIST [2] або іншими авторитетними організаціями. Частково це пояснюється ще й тим, що розробнику важливий не стільки узагальнений показник «випадковості» сформованої датчиком гамми, скільки вид окремої аномалії в її складі, який приводить до погіршення цієї самої «випадковості». З цієї причини у кожному конкретному випадку доводиться шукати свій відповідний спосіб тестування, і саме ця обставина пояснює підвищену увагу багатьох дослідників у цій області до побудови нових тестів. Підтвердженням цього є той факт, що наприклад, для шифру RC4, створеного в 1987 році, і в якому в подальшому, були виявлені деякі відхилення від випадковості, ніхто не міг запропонувати відповідного тесту, що практично реалізовувався, протягом багатьох років, не дивлячись на велике число робіт, присвячених цьому питанню. Все це говорить про те, пошук нових ефективних тестів, придатних для використання в якості інструментальних засобів в процесі

проектування, залишається поки ***актуальним і не вирішеним до кінця завданням***.

Вперше практичне вирішення проблеми тестування датчиків випадкових чисел було запропоноване Д.Кнутом в його класичній роботі «Мистецтво програмування для ЕОМ» [5]. У ній розглядається декілька тестів, що дозволяють визначити, наскільки відповідає розподіл вірогідності деякої випадкової величини в спостережуваному процесі, очікуваному виду розподілу.

Серед розроблених тестів Д. Кнутом, найбільш відповідним для потреб криптографії представляється тест, заснований на критерії згоди χ^2 Пірсона. В даний час він застосовується для обчислення значення показника якості в переважній більшості тестів, що входять до складу криптографічних пакетів. Цінність цього критерію визначається тим, що з його допомогою можна безпосередньо оцінити ступінь рівномірності розподілу вірогідності чисел, що отримуються на виході генератора ПВП, і це робить його придатним для попередньої оцінки не тільки самого генератора, але й вхідних в його склад окремих компонентів. Згадана робота Д. Кнута була написана за часів становлення обчислювальної техніки і не орієнтована на потреби криптографії. Основний упор автор робив на економії обмежених, на ті часи, обчислювальних ресурсів і не ставилося питання про точність методу, що так важливо в області криптоаналізу.

Метою статті *є* акцентування уваги на особливостях застосування критерію згоди χ^2 для підтвердження відповідності розподілу вірогідності символів сформованої псевдовипадкової послідовності рівномірному закону.

Про застосування χ^2-критерію написано багато і він, без сумніву, є одним з найчастіше вживаних. Проте, в більшості літературних джерел з області статистики, процедура його застосування розглядається в загальній постановці. Тим часом зацікавлениість до нього зростає, і не тільки у зв'язку з вирішенням криптографічних завдань. У Росії, наприклад, навіть був випущений в 2001 році стандарт, що визначає порядок його використання [7].

Розглянемо суть і особливості вирішуваного завдання. Припустимо, деякий генератор породжує букви алфавіту $A=\{a_1,a_2,...,a_S\}$, $S>1$. Причому ці букви представлені в обчислювальній системі двійковими кодовими комбінаціями фіксованої довжини m. Тоді загальне число символів на виході джерела буде рівне 2^m. За умови рівномірності розподілу їх вірогідності виконуватиметься проста гіпотеза H_0, відповідно до якої всі символи рівноімовірні:

$$H_0 : p(a_1) = p(a_2) = ... = p(a_S) = 1/S.$$

Відповідно, передбачається, що альтернативна гіпотеза H_1 полягає в запереченні цього твердження.

Для підтвердження справедливості гіпотези формується вибірка $x_1, x_2, ..., x_n$ по якій визначаються оцінки вірогідності символів на виході генератора. Величина n, як показано в роботі [5], повинна бути такою, щоб кожен символ мав можливість бути сформованим хоча б п'ять разів. Іншими словами, повинна виконуватися умова $np_i \geq 5$. Зазвичай цю величину n_i вибирають рівною 5...10 і

підраховують оцінки вірогідності як $p_i^* = \frac{n_i}{n}$. Звідси величина n повинна задовольняти умові $n \geq 5 \cdot 2^m$. Так, наприклад, якщо генератор формує на виході восьмибітові символи, то їх загальне число буде рівне 256 (від 0 до 255). Підрахувавши величину $n_i i$ для кожного з них, можна визначити показник

$$\chi^2 = \sum_{i=1}^{2^m} \frac{\left(p_i^* - \frac{n}{S} \right)^2}{\frac{n}{S}},$$

який характеризує ступінь наближення реального розподілу чисел на виході генератора до рівномірного закону.

Даний критерій заснований на тому, що зі зростанням величини n, показник χ^2 сходиться до розподілу χ^2 з $(S-1)$ ступенями свободи. Тут S можна розглядати як число інтервалів на яких спостерігається досліджувана величина, а одиниця визначає число параметрів, які обчислюються на основі спостережуваної статистики [7].

Для ухвалення рішення щодо справедливості нульової гіпотези H_0, слід визначити рівень значущості $(1-\alpha)$. Тут α − вірогідність помилки першого роду, що означає вірогідність відхилення гіпотези H_0, коли вона насправді справедлива.

З урахуванням характеру розподілу величини χ^2, її порогове значення, відповідне прийнятому рівню значущості $\chi^2_{(1-\alpha),(S-1)}$ може бути визначено за допомогою функції **chi2inv**$\left((1-\alpha),(S-1)\right)$ пакету MATLAB. Наприклад, для розглянутого вище випадку, величина $\chi^2_{0.99,255} = 311,5603$. Якщо цей поріг величиною χ^2 перевищений, то нульова гіпотеза відкидається. Наприклад, при рівні $\alpha = 0,01$, у разі тестування ста послідовностей, отриманих від генератора випадкових чисел з різними значеннями ключа, не більше ніж для однієї з них показник χ^2 може перевищити значення $\chi^2_{(1-\alpha),(S-1)}$.

У роботі Дж.Тейлора [7] показано, що якщо розрахункове значення показника усереднювати по великому числу випробовуваних послідовностей, то розрахункова величина $\overline{\chi}^2$, задовольнятиме умові

$$\overline{\chi}^2 \leq (S-1). \qquad (1)$$

Таким чином, якщо частка тестованих послідовностей, які успішно проходять цей тест не менше величини рівня значущості $(1-\alpha)$ і виконується умова (1), можна вважати, що випробовуваний генератор пройшов попередню перевірку і може бути випробуваний за допомогою одного з прикладних тестових пакетів [2…4]. Якщо ж тест на основі критерію не дав позитивних результатів, подальші перевірки безглузді.

Одним з «вузьких» місць цього тесту є вибір кількості символів вихідного алфавіту S або, інакше кажучи, вибір числа інтервалів на яких спостерігаються символи вихідної послідовності тестованого генератора. У роботі [8], стверджується, що число інтервалів повинне вибиратися так, щоб на кожен символ вихідного алфавіту був свій інтервал. Тобто, якщо, наприклад, генератор оперує 32-х бітовими числами, то і число інтервалів повинне бути рівним 2^{32}. Це твердження робиться на тій підставі, що інакше виявляється «лукавість процесу». Сенс цього негативного явища полягає в тому, що якщо тестувати деяку регулярну (або близьку до регулярної) послідовність, то вона ідентифікуватиметься як абсолютно «випадкова» з рівномірним законом розподілу вірогідності і, чим довшим є розмір слова в алфавіті, тим меншою є ступінь небезпеки. Далі автори цієї роботи розумно ставлять питання про те, що при такому розмірі алфавіту буде потрібно неймовірно великий розмір пам'яті і часових ресурсів для реалізації тесту. З метою подолання цієї проблеми пропонується тест на основі так званого алгоритму «Стопка книг». Його суть зводиться до того, що символи алфавіту нумеруються в послідовному порядку і при формуванні датчиком випадкового числа, символ з відповідним номером переміщується на перше місце в алфавіті. При цьому всі символи, що займають попередні позиції (зліва), переміщаються управо на один крок. Це відбувається аналогічно тому, як книга, що витягується навмання з вертикальної стопки, кладеться на верхнє місце, а всі вищестоячі опускаються вниз на одну позицію. Потім весь діапазон чисел розбивається на відносно невелику кількість інтервалів і далі застосовується критерій χ^2. Описаний алгоритм можна проілюструвати рис.1.

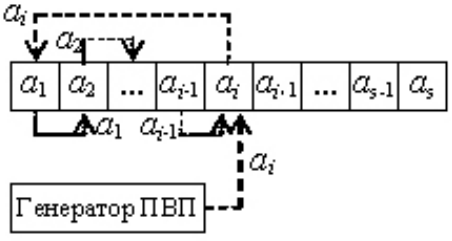

Рис. 1. Принцип перестановки символів алфавіту по методу «Стопка книг»

Справедливо робиться твердження, що при рівноімовірних символах вірогідності попадання сформованого датчиком числа в будь-який з інтервалів будуть рівні, а інакше символи, що частіше зустрічаються, частіше опинятимуться у верхній частині «стопки». На цій підставі робиться висновок про більшу чутливість тесту до нерівномірності тестованої послідовності, що доводиться на високому математичному рівні в цілому ряду опублікованих авторами цього тесту статей.

Не оспорюючи в принципі тверджень, зроблених авторами цієї роботи, слід відмітити, що кількість інтервалів розбиття (або розмір символу m в алфавіті) можна вибрати невеликим також у розглянутому вище χ^2-тесті. При цьому можлива недостатня «випадковість» послідовності буде виявлена при кінцевих випробуваннях генератора іншими додатковими тестами, що не вимагають значних обчислювальних ресурсів.

Друге зауваження є серйознішим і неприємнішим. Програмна реалізація тесту «Стопка книг» зажадає моделювання процедури переміщення чисел в алфавіті («у стопці»), а це, у свою чергу, вимагає великих обчислювальних ресурсів, зводячи декларовані переваги методу до мінімуму.

З врахуванням зазначеного зауваження, для обох методів були проведені порівняльні випробування звичайного методу χ^2 і методу «Стопка книг» при рівній кількості інтервалів. Як генератор ПВП використовувався алгоритм RC4 з довжиною блоку в один байт $(m=8)$. На рис. 2 представлений графік, який відображає результати тестування 100 послідовностей, довжина кожної з яких складала 8192 байт. На рисунку крива 1 відображає величину показника для звичайного χ^2-тесту, а крива 2 відображає усереднювання цієї величини зі зміною числа тестів від 1 до 100. Відповідно, крива 3 відображає величину показника для тесту «Стопка книг», а крива 4 відображає усереднювання цієї величини зі зростанням числа тестів від 1 до 100.

Порівняння характеристик показує близькість результатів, які дають обидва тести за рівних умов для випробовуваних послідовностей і придатних для попереднього аналізу генераторів, що розробляються для криптографічних потреб.

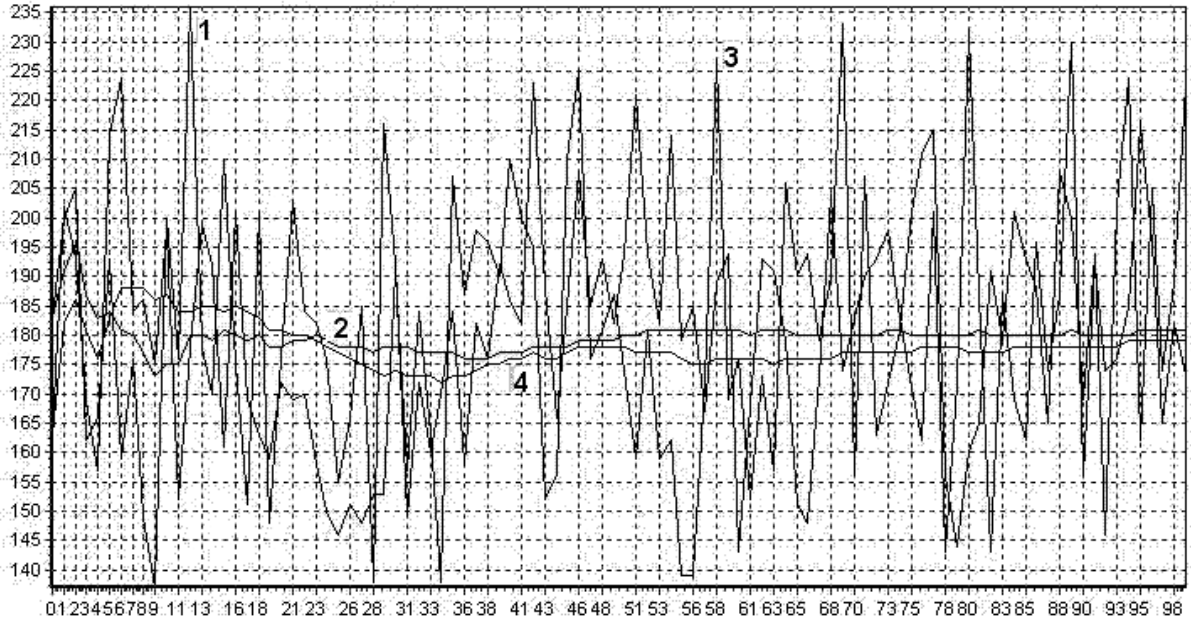

Рис. 2. Зміна показників результатів тестування

На закінчення слід відзначити, що, як вказано в керівництві до пакету тестів, розроблених NIST [2], тестування, не залежно від того, чи проводиться воно окремими тестами, чи пакетами тестів, не є частиною криптоаналізу. По його результатах робиться попередній аналіз стійкості криптографічного перетворення. Інша справа, що загальновідомі пакети, які пройшли випробування часом, дозволяють провести комплексну перевірку генератора для виявлення тих аномальних місць в рівномірно розподіленій послідовності, яку не виявляють традиційні статистичні методи.

Враховуючи, що нові шифри розробляються з урахуванням уразливостей, які стали причинною вдалих криптографічних атак на вже відомі алгоритми, є підстави вважати, що пошук нових методів тестування буде продовжений.

Список літератури: 1.eSTREAM, the ECRYPT Stream Cipher Project // [Электронный ресурс]: http://www.ecrypt. eu.org/stream/index.html. 2. A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications. NIST Special Publication 800-22. May 15, 2001.3.The Marsaglia Random Number CDROM including the

Diehard Battery of Tests of Randomness // [Электронный ресурс]: http://www.stat.fsu.edu/ pub/diehard 4.Statistical test suite Crypt-X // [Электронный ресурс]: http://www.isi. qut.edu. au/resources/cryptx/ 5.*Кнут Д.* Искусство программирования для ЭВМ. Т.2. – М.: Мир, 1977. – 727 с. 6.Правила проверки согласия опытного распределения с теоретическим. Часть I. Критерии типа хи-квадрат 14.12.2001 // [Электронный ресурс]: http:// www.tcnti.ru/shop/catalog/index. php?docum=25096/ **7.***Тейлор Дж.* Введение в теорию ошибок. Пер. с англ. – М.: Мир, 1985. – 272 с. 8. *Дорошенко С.А., Лубкин А.М., Рябко Б.Я., Фионов А.Н.* Экспериментальный анализ шифра RC4 и потоковых шифров, выдвинутых на конкурс ESTREAM. – Новосибирск: Сибирский гос. ун-т телекоммуникаций и информатики // [Электронный ресурс]: http://www.contrterror.tsure.ru/site/ magazine8/ 05-14-Doroshenko.htm

Поступила в редколлегию 31.07.2011

УДК 681.3:378.146

Н.О.РИЗУН, канд. техн. наук, доц., Днепропетровский университет экономики и права им. А. Нобеля

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПОСТРОЕНИЯ НАУЧНО-ИННОВАЦИОННОГО МНОГОУРОВНЕВОГО КОМПЛЕКСА ИНТЕНСИФИКАЦИИ УЧЕБНОГО ПРОЦЕССА В ВУЗЕ (АСПЕКТ ФОРМАЛИЗАЦИИ ПОДСИСТЕМ)

Розроблено теоретичні основи математичної формалізації та синтезу часткових критеріїв підсистем науково-інноваційного багаторівневого комплексу інтенсифікації навчального процесу з використанням інформаційних технологій.
Ключові слова: інтенсифікація, навчальний процес, інформаційні технологій.

Разработаны теоретические основы применения кибернетического подхода к математической формализации и синтеза частных критериев подсистем научно-инновационного многоуровневого комплекса интенсификации учебного процесса с использованием информационных технологий.
Ключевые слова: интенсификация, учебный процесс, информационные технологии.

Theoretical bases of the mathematical formalization and of synthesis of particular criteria subsystems of scientific and innovative multilevel complex of study process intensification with the use of information techniques are developed.
Key words: intensification, study process, information technique.

Введение

Всеобщая технологизация производства, бурный рост информационных и коммуникационных технологий, автоматизация интеллектуальных процедур – с одной стороны; динамичное развитие экономики и рост конкуренции, определяющие постоянную потребность в повышении профессиональной квалификации и переподготовке работников, росте их профессиональной мобильности – с другой, предъявляют новые требования к системе образования.

В этой связи одной из ключевых проблем совершенствования системы образования высшей школы в Украине продолжает оставаться интенсификация учебного процесса с использованием кибернетического подхода, позволяющего обобщить опыт автоматизации отдельных элементов учебного процесса с использованием средств моделирования, обратной связи, формализации и фиксации сигналов учебной информации, интегрируя их в разработку и