

УДК 657.6+658.01:004(036); 002:004.056; 65.012.8

№ держреєстрації 0112U007713

Інв. №

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
65026, м. Одеса, вул. Преображенська, 8, тел. (048) 23-61-58

ЗАТВЕРДЖУЮ

Ректор

Одеського національного
економічного університету
докт. екон. наук, професор

_____ *М.І. Звєряков*

«___» _____ 2013 г.

ЗВІТ

про науково-дослідну роботу

**УДОСКОНАЛЕННЯ ПРИНЦИПІВ ТА МЕТОДІВ
ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ,
ІНФОРМАЦІЙНОЇ ТА ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ
ПІДПРИЄМСТВ ТА ОРГАНІЗАЦІЙ
СФЕРИ ЕКОНОМІКИ, БІЗНЕСУ ТА ФІНАНСІВ**

(проміжний)

Рукопис закінчено 1 грудня 2013 року

Науковий керівник НДР

*завідувач кафедри Інформаційних систем в економіці
докт. техн. наук, доцент*

О.О. Скопа

Одеса – 2013

СПИСОК ВИКОНАВЦІВ

Науковий керівник

докт. техн. наук, доцент
(вступ, підрозділи 1.1-1.5, 3.5, висновки до звіту)

О.О. Скопа

Відповідальний виконавець

канд. техн. наук., доцент
(підрозділи 3.1, 3.3, 3.4, висновки до розділів)

Н.Ф. Казакова

Виконавці

канд. екон. наук, доцент
(підрозділ 2.3)

О.В. Орлик

канд. техн. наук, доцент
(підрозділ 3.1)

Ю.В. Щербина

канд. техн. наук, доцент
(підрозділ 3.2)

А.О. Петров

канд. техн. наук, доцент
(підрозділи 3.5, 3.6)

С.Л. Волков

канд. екон. наук, ст. викладач
(підрозділ 2.5)

О.І. Мацків

ст. викладач
(підрозділи 2.1, 2.2, список першоджерел)

О.Г. Єсіна

ст. викладач
(підрозділ 2.6)

А.Ю. Вакула

ст. викладач
(підрозділи 1.6, 1.7)

О.О. Фразе-Фразенко

ст. викладач
(підрозділ 3.3)

А.В. Мінін

викладач
(підрозділ 2.4)

О.О. Йона

аспірант
(підрозділ 3.6)

Є.В. Вавілов

аспірант
(підрозділ 3.7)

К.Б. Айвазова

У зборі та обробці інформації приймали участь студенти: кредитно-економічного факультету: Д. Осипенко (розрахунки до підрозділу 3.4), В. Педько (пошук літератури до розділу 1), А. Білодон (оформлення списку літературних першоджерел).

ЗМІСТ

Стор.

РЕФЕРАТ	3
ВСТУП	9
<i>Підстави для проведення науково-дослідної роботи</i>	9
<i>Мета НДР</i>	14
<i>Основні завдання для досягнення мети</i>	14
<i>Взаємозв'язок з іншими роботами</i>	15
РОЗДІЛ 1. ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ. УПРАВЛІННЯ ІДЕНТИФІКАЦІЙНОЮ ІНФОРМАЦІЄЮ І ДОСТУПОМ	16
1.1. Сутність та поняття інформаційної безпеки підприємства	16
1.2. Методи забезпечення безпеки інформації підприємства	18
1.3. Основні складові інформаційної безпеки	22
1.4. Організація системи інформаційної безпеки підприємства	24
1.4.1. Правила побудови системи інформаційної безпеки підприємства	24
1.4.2. Принципи захисту інформації	25
1.5. Основні заходи щодо створення і забезпечення функціонування комплексної системи захисту на підприємствах та в організаціях сфери економіки, бізнесу та фінансів	27
1.6. Загрози процесам аутентифікації у інформаційних системах фінансових установ та підприємств.....	31
1.7. Огляд та аналіз поточного стану технологій розпізнавання образів та перспективи їх використання у системах захисту інформації	38
1.7.1. Передумови до використання біометричної аутентифікації у системах захисту інформації. Аналіз поточного стану технологій та перспектив їх розвитку.....	38
1.7.2. Визначення цільових завдань СЗІ, які використовують біометричні дані	43
<i>Узагальнення проблеми обробки візуальної інформації у СЗІ</i>	43
<i>Формальна постановка завдання</i>	48
<i>Розробка загальної схеми дослідження</i>	50

1.7.3. Огляд та вибір інформативних ознак зображень для розв'язку задачі біометричної ідентифікації особи	53
<i>Вибір предмета та технології розпізнавання</i>	53
<i>Аналіз систем контурних ознак</i>	55
<i>Ознаки, засновані на вимірі просторових частот</i>	57
<i>Ознаки, засновані на статистичних характеристиках</i>	59
<i>Ознаки, що засновані на описі структурних елементів</i>	65
<i>Розв'язок проблеми вибору інформативних ознак для систем біометричної ідентифікації</i>	67

Висновки до розділу 1	70
------------------------------------	----

РОЗДІЛ 2. УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА ФІНАНСОВО- ЕКОНОМІЧНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВ.....

2.1. Загальні принципи побудови системи безпеки підприємства	73
2.2. Політика та стратегія безпеки	80
2.2.1. Основи політики безпеки підприємства	80
2.2.2. Суб'єкти безпеки підприємства	81
2.2.3. Засоби та методи забезпечення безпеки	83
2.2.4. Концепція безпеки підприємства	84
2.3. Економічна безпека господарюючих суб'єктів муніципального утворення	87
2.4. Безпека фінансового ринку та фінансової стабільності як суспільне благо	97
2.5. Аналіз аномалій мережевого трафіку інформаційно-обчислювальних систем спеціального використання	105
2.6. Принципи побудови захищених мереж сфери економіки, бізнесу та фінансів	114

Висновки до розділу 2	125
------------------------------------	-----

РОЗДІЛ 3. КОНФІДЕНЦІЙНІСТЬ ТА ЗАХИСТ ДАНИХ

3.1. Елементи практичної реалізації частотного тесту генераторів криптографічних перетворень	127
3.2. Надійність програмного забезпечення інформаційних систем галузі економіки, бізнесу та фінансів	137
3.2.1. Використання стійких до збоїв програм	142
3.2.2. Оцінка надійності програмного забезпечення за результатами налагодження та нормальної експлуатації	146
3.2.3. Експоненціальна модель Шумана	147

3.2.4. Експоненціальна модель Джелінського-Моранди.....	150
3.2.5. Вейбулівська модель	150
3.2.6. Структурна модель Нельсона.....	151
3.3. Теорема до теорії випробовування надійності автоматичних банківських систем однократного використання	152
3.4. Регуляризований розв'язок одномірного інтегрального рівняння Фредгольма I роду в умовах існування некоректних задач.....	167
3.5. Візуалізація структури показників якості функціонування інформаційно-вимірювальних систем галузі економіки, бізнесу та фінансів	182
3.6. Принципові питання вирішення задачі багатокритеріальної оптимізації показників якості інформаційно-вимірювальних систем галузі економіки, бізнесу та фінансів на основі мультихромосомного генетичного алгоритму.....	194
3.7. Проблематика якості Інтернет-послуг, які надаються структурам сфери економіки	207
<i>Висновки до розділу 3</i>	215
ЗАГАЛЬНІ ВИСНОВКИ	217
СПИСОК ЛІТЕРАТУРНИХ ПЕРШОДЖЕРЕЛ	222
ДОДАТОК. Терміни та означення	234

РОЗДІЛ 3

КОНФІДЕНЦІЙНІСТЬ ТА ЗАХИСТ ДАНИХ

3.1. Елементи практичної реалізації частотного тесту генераторів криптографічних перетворень

Побудова криптостійких систем у для галузі економіки, бізнесу та фінансів може бути здійснена шляхом багатократного застосування простих криптографічних перетворень (примітивів). У якості таких примітивів Клод Шеннон запропонував використовувати підстановки (*substitution*) і перестановки (*permutation*). Часто використовуваними криптографічними примітивами є перетворення типу *циклічне зрушення* або *гамування*, тобто метод шифрування, заснований на «накладенні» γ -послідовності на відкритий текст. Як γ -послідовності найчастіше використовують псевдовипадкові послідовності (ПВП), що формуються на основі поліномів.

В даний час, однією з проблем, пов'язаною з захистом даних, що передаються в інформаційно-телекомунікаційних системах галузі економіки, бізнесу та фінансів, а також з конфіденційністю інформації, є потреба в генераторах криптографічних перетворень, які відповідають високим вимогам до рівномірності розподілу вірогідності формованих ними чисел. Ці вимоги сформовані фахівцями NIST, які в 1999 р. в рамках проекту AES (*Advanced Encryption Standard*) розробили набір статистичних тестів NIST STS (*NIST Statistical Test Suite*) для випробувань ПВП [68].

Також зазначимо, що генератори криптографічних перетворень знаходять застосування в криптографічних протоколах галузі економіки, бізнесу та фінансів для формування ключів, при хешуванні паролів, а також в алгоритмах, закладених в основу поточкових симетричних криптографічних систем, вживаних для захисту конфіденційності передаваної інформації. Побудова таких генераторів – абсолютно нетривіальне завдання і його рішення вимагає копіткої праці математиків та аналітиків. Генератор, слабкий з кри-

птографічної точки зору, може значно ослабити захищеність інформаційної системи і, з цієї причини, для розробників криптографічних систем важливо мати в наявності засіб перевірки їх надійності.

Аналіз наукової і технічної літератури показав, що за останні десятиліття було розроблена і досліджена велика кількість «елементарних» генераторів криптографічних перетворень до яких відносять лінійні конгруентні генератори [71, 72], генератори Фібоначчі з запізнюванням [71], генератори, побудовані на лінійних регістрах зі зворотним зв'язком [72...75] і деякі їх різновиди. Багаторічні дослідження вчених привели до висновку про те, що всі вони не є криптографічно стійкими і можуть входити до складу формувачів криптографічних перетворень тільки як складові елементи.

Як показано в [72], ідея побудови складеного генератора базується на тому факті, що комбінація двох і більше вихідних послідовностей від генераторів різного типу за допомогою таких операцій як «+», «-», «x», « \oplus », дозволяє розробити структуру генератора з «кращими властивостями випадковості». Найбільш вдалі складені генератори (з погляду криптографії) детально розглянуті в роботі Б. Шнаєра [76].

З часом в алгоритмах, що здавалися раніше надійними, знаходять нові «слабкі місця». З цієї причини в процесі розробки криптографічних протоколів стає питання про пошук нових інженерних рішень з метою побудови нових, ефективних з точки зору криптографії стійких генераторів, вільних від виявлених недоліків.

Найбільш вдалим на сьогоднішній день формувачем криптографічних перетворень є алгоритм, реалізований в потоковому шифрі RC4 [76]. Однак, все частіше з'являються повідомлення про те, що і в ньому вже знайдені уразливості. Стверджується, що вдалося встановити статистичну залежність характеру ПВП, що генерувалася в потоковому шифрі RC4, від перших символів ключа.

На відміну від інших інженерних завдань, розробка нового алгоритму формування відрізняється тим, що достовірна відповідь на питання про ефек-

тивність знайденого рішення задачі може з'явитися тільки через деякий час, коли для нього буде розроблений індивідуальний метод криптоаналізу. Розробникові залишається задовольнятися тільки результатами попереднього тестування. Про це прямо сказано в керівництві до пакету тестів, розроблених NIST [68]. Будь-який із запропонованих тестів або навіть цілий пакет тестів не замінює криптоаналізу. При цьому попереднє тестування є обов'язковим. Генератор, що не задовольняє умовам тестування непридатний. Кожен з вхідних в пакет тестів орієнтується на пошук певного виду аномалій в потоці формованих символів.

До тестових пакетів, які найбільш рекомендуються до використання, відноситься вже згадуваний пакет NIST STS. Він включає набір з 16-ти тестів і методику їх використання. Успішний результат випробувань проєктованого генератора із застосуванням всього набору цих тестів дає підстави сподіватися на те, що формована генератором послідовність невідмітна від «справжньої» випадкової послідовності.

Відомі й інші пакети тестів, створені для потреб криптографії. До них відноситься набір статистичних тестів під назвою Diehard [69], призначений для визначення якості послідовності випадкових чисел. Ці тести були розроблені Дж. Марсальей (George Marsaglia). Він включає 12 тестів і доступний в Інтернеті за адресою: <http://stat.fsu.edu/pub/diehard/>.

За адресою <http://www.isi.qut.edu.au/resources/cryptx/> можна зв'язатися з розробниками пакету тестів CRYPT-X [70] і отримати програмне забезпечення та керівництво по їх застосуванню.

Проте використання відмічених пакетів прикладних програм натрапляє на ряд серйозних перешкод. Перша з них полягає в тому, що вони призначені для оцінки вже готових генераторів. У практичній роботі галузі економіки, бізнесу та фінансів такі пристрої розробники конструюють поетапно, поступово доводячи їх до рівня відповідності вимогам, що пред'являються.

Друга проблема полягає в тому, що в основі кожного з вхідних в пропонуваній пакет тестів лежить достатньо складне теоретичне обґрунтування,

що вимагає від розробників серйозної математичної підготовки та знань різних несуміжних розділів математики. На жаль, в керівництві, що додається до тестів, розробники такого обґрунтування, як правило, не приводять.

Нарешті, третя проблема, полягає в тому, що, хоча до програмного забезпечення і наданий вільний безкоштовний доступ, скористатися ним складно. Більшість тестів припускають попереднє створення файлу, в який записується випробовувана псевдовипадкова послідовність у вигляді 32-бітових слів, а потім запускається процедура тестування. Це не завжди зручно і підходить не для всіх тестів, оскільки вимагає значних програмно-апаратних ресурсів. До того ж, пропонувані тести розраховані на певну програмно-апаратну платформу.

Перераховані проблеми вимушують розробників якщо не розробляти власні тести, то, принаймні, створювати власне програмне забезпечення, яке їх реалізує, є зручним в роботі та може ефективно використовуватися в процесі пошуку конструктивного вирішення генератора, що розробляється.

Всякий пакет тестів має свою внутрішню логіку. Передбачається, що випробування нового генератора повинне починатися з частотного тестування. Як вказується в [68], якщо генератор не проходить частотний тест, то проведення всіх інших тестів вже не має сенсу. Тому, враховуючи все вищесказане, метою підрозділу є аналіз виконання частотного тестування і методики її проведення.

Тестування генератора, зокрема частотне, засноване на порівнянні цього генератора з ідеалом. Передбачається, що такий ідеальний генератор формує криптографічну послідовність з рівномірним розподілом вірогідності одиниць і нулів, причому таку, що наступний вихідний біт неможливо передбачити за наслідками спостереження деякого відрізка цієї послідовності з вірогідністю, що відрізняється від 0,5.

Насправді, реальний генератор криптографічних перетворень видає «несправжню» випадкову послідовність, а повністю визначувану значенням секретного ключа. Ступінь його схожості з реальним формувачем випадкової гами може бути встановлена на підставі вибраного еталону та критерію, який

дозволяє визначити ступінь відмінності отриманого результату від очікуваного рівномірного розподілу вірогідності.

Формальне визначення критерію припускає завдання нульової гіпотези H_0 , відповідно до якої тестована послідовність є випадковою. З нею безпосередньо пов'язана альтернативна гіпотеза H_A відповідно до якої ця послідовність не може бути визнана випадковою. Приймаючи нульову гіпотезу, експериментатор з вірогідністю α , ризикує помилитися – зробити так звану «помилку першого роду». Відповідно, з вірогідністю $1 - \alpha$, він буде правим. Зазвичай, величину α вибирають в межах $0,01 < \alpha < 0,001$.

При частотному тестуванні передбачається, що поява символів на виході генератора повністю підкоряється розподілу Бернуллі. При якому вірогідність одиничного символу p рівна вірогідності появи нульового символу – $q = 1 - p$. В цьому випадку різниця між числом одиниць n_1 і числом нулів n_0 , $S_n = n_1 - p$ в n -розрядній послідовності складає $\varepsilon = \varepsilon_1, \varepsilon_2, \dots, \varepsilon_n$, де ε_i – двійковий символ, що приймає значення $\{0,1\}$. Різниця буде підпорядкована біноміальному закону розподілу вірогідності, який відповідно до теореми Муавра-Лапласа, при достатньо великому значенні n , добре апроксимується стандартним нормальним законом $N_{0,1}$ з нульовим математичним очікуванням і одиничною дисперсією. Як показано в [68, 77], ця різниця, відповідно до центральної граничної теореми, задовольняє умові:

$$\lim_{n \rightarrow \infty} P \left(\frac{S_n}{\sqrt{n}} < z \right) = \Phi(z) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^z e^{-\frac{u^2}{2}} du,$$

де $\Phi(z)$ – функція Лапласа, яка є чисельно рівною площі фігури, обмеженої зверху кривою Гауса, знизу віссю абсцис, а справа – прямою $y = z$.

У [68] показано, що для позитивних значень z , буде справедливий вираз:

$$P \left(\frac{S_n}{\sqrt{n}} \leq z \right) = 2\Phi(z) - 1.$$

За даними випробування n -розрядної двійкової послідовності необхідно обчислити статистику:

$$s_{obs} = \frac{|n_1 - n_0|}{\sqrt{n}} = \frac{|S_n|}{\sqrt{n}}.$$

Значення статистики дозволяє розрахувати вірогідність того, що параметр z не вийде за межі допустимого значення α , визначуваного вибраним критерієм. Ця вірогідність може бути представлена у вигляді:

$$2 \left[1 - \Phi \left(\frac{|s_{obs}|}{\sqrt{n}} \right) \right] = \operatorname{erfc} \left(\frac{|s_{obs}|}{\sqrt{n}} \right). \quad (3.1)$$

Враховуючи, що додаткова функція помилки визначається як

$$\operatorname{erfc}(z) = \frac{2}{\sqrt{\pi}} \int_z^{\infty} e^{-u^2} du, \quad (3.2)$$

то, з урахуванням меж інтеграції, вираз (3.1) можна переписати у вигляді:

$$2 \left[1 - \Phi \left(\frac{|s_{obs}|}{\sqrt{2n}} \right) \right] = \operatorname{erfc} \left(\frac{|s_{obs}|}{\sqrt{2n}} \right).$$

Якщо, в результаті випробувань обчислена величина $P = \operatorname{erfc} \left(\frac{|s_{obs}|}{\sqrt{2n}} \right) \geq \alpha$,

то тестована послідовність визнається випадковою.

Якщо величина α вибрана рівною 0,01, то це означає, що зі ста тестованих послідовностей не більше ніж одна з них може бути забракована як «невипадкова».

Програмна реалізація такого тесту має дві складності. Перша з них полягає в тому, що достатньо складно реалізувати ефективний підрахунок числа одиничних n_1 і, відповідно, нульових n_0 символів в тестованій послідовності. Це пояснюється тим, що в більшості сучасних обчислювальних архітектур команд для роботи з окремими бітами немає.

Друга складність полягає в необхідності обчислення в кожному тесті значення додаткової функції помилки erfc . В принципі, її значення можна обчислити і за допомогою прикладного програмного пакету MatLab, але в

процесі тестування великого числа послідовностей звертатися до окремого програмного пакету не зручно.

Оскільки розмір тестованої послідовності n невеликий (у [68] рекомендується вибирати n не більше, ніж 100 символів), їх кількість в кожному байті може бути підрахована так, як це описано далі.

Зважаючи, що при двійковому численні вага кожного двійкового розряду машинного слова більше суми вагів всіх розрядів, які стоять зліва від нього (молодших по відношенню до цього розряду), значення двійкових символів, що входять до складу цього слова і їх кількість визначається по наступній методиці.

Вважатимемо, що символи a_i , k -розрядного слова $a = \{a_k, a_{k-1}, \dots, a_1\}$, що виражає число b , пронумеровані справа наліво (від молодшого розряду до старшого). Тоді значення кожного з них можна розрахувати за правилом:

$$a_i = \begin{cases} 1, & \text{при } b - 2^{k-1} \geq 0, \\ 0, & \text{при } b - 2^{k-1} < 0. \end{cases}$$

Обчислення цієї процедури безпосередньо недоцільно, оскільки піднесення до ступеня – операція, трудомістка для обчислювальної системи. Якщо, наприклад, прочитування тестованої послідовності здійснюється побайтно, процедура підрахунку кількості одиничних n_1 і нульових n_0 бітів, написана на мові Delphi, може мати наступний вигляд:

```

b:=a-128;
if b>=0 then Begin
    a:=a-128; n1:=n1+1 End
else n0:=n0+1;
b:=a-64;
if b>=0 then Begin
    a:=a-64; n1:=n1+1 End
else n0:=n0+1;
b:=a-32;
if b>=0 then Begin
    a:=a-32; n1:=n1+1 End

```

```

    else n0:=n0+1;
b:=a-16;
if b>=0 then Begin
    a:=a-16; n1:=n1+1 End
    else n0:=n0+1;
b:=a-8;
if b>=0 then Begin
    a:=a-8; n1:=n1+1 End
    else n0:=n0+1;
b:=a-4;
if b>=0 then Begin
    a:=a-4; n1:=n1+1 End
    else n0:=n0+1;
b:=a-2;
if b>=0 then Begin
    a:=a-2; n1:=n1+1 End
    else n0:=n0+1;
b:=a-1;
if b>=0 then Begin
    a:=a-1; n1:=n1+1 End
    else n0:=n0+1;

```

Тут лічильники **n1** і **n0** обнуляються на початку тестування і потім накопичують інформацію про кількість відповідних символів до закінчення тестування всієї послідовності. Така процедура виглядає декілька громіздко, проте працює швидко. Вона легко може бути розширена і на випадок блоку більшого розміру.

Алгоритм розглянутої процедури приведено на рис. 3.1.

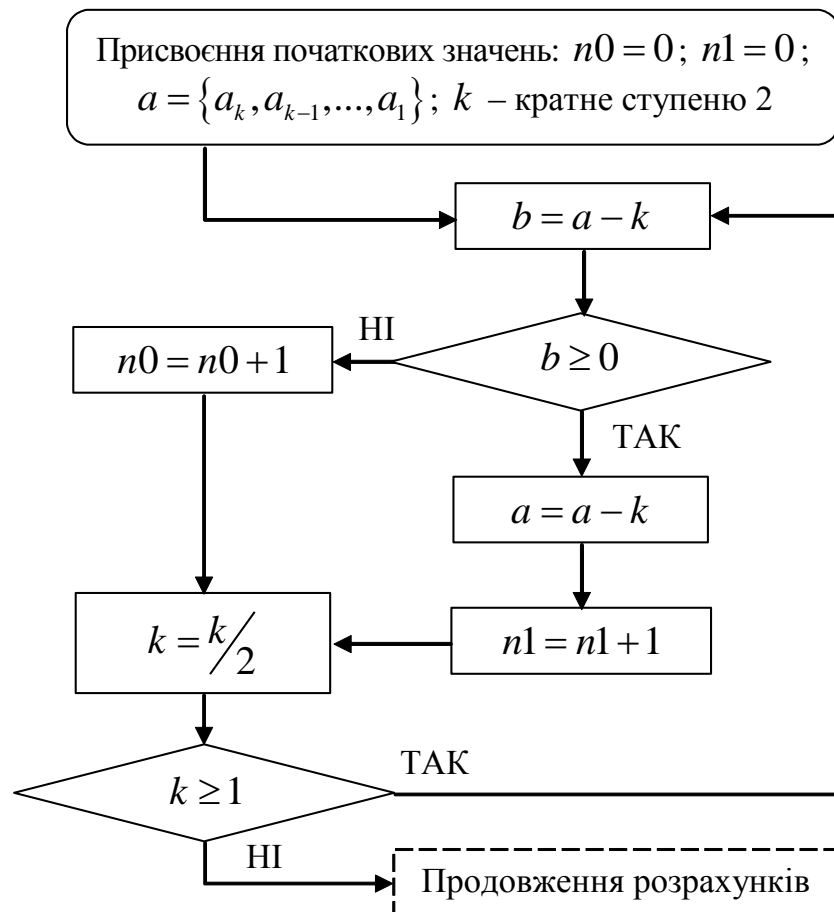


Рис. 3.1 – Алгоритм підрахунку кількості одиничних і нульових бітів

Що стосується обчислення показника P , що є додатковою функцією помилки $erfc(x)$ вигляду (3.2), то її можна представити так:

$$erfc(x) = 1 - erf(x) = \frac{2}{\sqrt{\pi}} \int_x^{\infty} e^{-t^2} dt.$$

Брати такий інтеграл у вказаних межах незручно, тому краще обчислити функцію $erf(x) = \frac{2}{\sqrt{\pi}} \int_0^x e^{-t^2} dt$, а потім перейти до функції $erfc(x)$.

Функція $erf(x)$ не може бути представлена через елементарні функції.

Проте її можна представити у вигляді ряду:

$$erf(x) = \frac{2}{\sqrt{\pi}} \sum_{n=0}^{\infty} \frac{(-1)^n x^{2n+1}}{n!(2n+1)} = \frac{2}{\sqrt{\pi}} \left(x - \frac{x^3}{3} + \frac{x^5}{10} - \frac{x^7}{42} + \frac{x^9}{216} - \dots \right).$$

Цим розкладанням можна користуватися, якщо значення аргументу функції $erf(x)$ не перевищує значення $x = 3$. При більшому значенні аргументу можна скористатися асимптотичним розкладанням вигляду

$$erfc(x) = \frac{e^{-x^2}}{x\sqrt{\pi}} \left[1 + \sum_{n=1}^{\infty} (-1)^n \frac{1 \times 3 \times 5 \times \dots \times (2n-1)}{(2x^2)^n} \right] = \frac{e^{-x^2}}{x\sqrt{\pi}} \sum_{n=0}^{\infty} (-1)^n \frac{(2n)!}{n!(2x)^{2n}}$$

і обчислити значення функції $erfc(x)$ безпосередньо. Якщо ряд для визначення значення функції $erf(x)$ вимагає обчислення до 30-ти членів, то останній ряд, для обчислення функції $erfc(x)$, дає хороше наближення вже при обчисленні чотирьох членів.

Представлені розкладання для функцій $erf(x)$ і $erfc(x)$ можна знайти за адресою [http:// functions.wolfram.com/GammaBetaErf/](http://functions.wolfram.com/GammaBetaErf/).

Т.ч., як слідує з викладеного, для тестування послідовності, що формується проєктованим генератором, необхідний програмний продукт, в який цей генератор входить як складова частина, і який дозволить формувати m n -розрядних послідовностей. Тут m – задане число тестів. При чому цей продукт повинен мати окремий вбудований генератор ключів, з тим, щоб забезпечити їх незалежність. У цьому ж продукті можна розмістити і програму для тестування, яка, з використанням викладених прийомів, дозволить визначати частку послідовностей, що не пройшли тест.

На закінчення відзначимо, що саме такий підхід поетапного тестування і підбору складових елементів генератора дозволяє зробити попередні висновки про прийнятність передбачуваної архітектури проєктованого генератора або шифру. На практиці реалізований описуваний підхід до тестування у вигляді двох окремих складових – модуля генератора і модуля тесту. Це дозволяє застосовувати модуль тестування для інших типів генераторів тієї ж розрядності.

СПИСОК ЛІТЕРАТУРНИХ ПЕРШОДЖЕРЕЛ

1. Горбатюк, О. М. Сучасний стан та проблеми інформаційної безпеки України на рубежі століть [Текст] / О. М. Горбатюк // Вісник Київського університету імені Т. Шевченка. – 1999. – № 14 : Міжнародні відносини. – С. 46-48.
2. Баринов, А. Информационный суверенитет или информационная безопасность? [Текст] / А. Барсуков // Національна безпека і оборона. – 2001. – № 1. – С. 70-76.
3. Бучило, И. Л. Информационное право: основы практической информации [Текст] : монографія / И. Л. Бучило. – М., 2001. – 253 с.
4. Борсуковский, Ю. Подходы и решения : Информационная безопасность [Текст] / Ю. Борсуковский // Мир денег. – 2001. – № 5. – С. 41-42.
5. Щербина, В. М. Інформаційне забезпечення економічної безпеки підприємств та установ [Текст] / В. М. Щербина // Актуальні проблеми економіки. – 2006. – № 10. – С. 220-225.
6. Березюк, Л. П. Организационное обеспечение информационной безопасности [Текст] : навч. посібник / Л. П. Березюк. – Хабаровськ : ДВГУПС, 2008. – 188 с.
7. Игнатъев, В. А. Информационная безопасность современного коммерческого предприятия [Текст] : монографія / В. А. Игнатъев. – Старий Оскол : ООО «ТНТ», 2005. – 448 с.
8. Маракова, І. Захист інформації [Текст] : підручник / Маракова І., Рибак А., Ямпольський Ю. – Одеса : ОдНПУ, 2001. – 164 с.
9. Захаров, Е. Информационная безопасность или опасность отставания? [Текст] / Е. Захаров // Права людини. – 2000. – № 1. – С. 3-5.
10. Про інформацію : закон України [Текст] : [закон України : офіц. текст: за станом на 02 жовтня 1992 року]. – К.. : Парламентське вид-во, 1996. – Т.4.
11. Про захист інформації в автоматизованих системах : закон України [Текст] : [закон України : офіц. текст: за станом на 05 липня 1994 року]. – К.. : Парламентське вид-во, 1996. – Т.7.
12. Литвиненко, О. Інформація і безпека [Текст] / О. Литвиненко // Нова політика. – 1998. – № 1. – С. 47-49.
13. Горбатюк, О. М. Сучасний стан та проблеми інформаційної безпеки України на рубежі століть [Текст] / О. М. Горбатюк // Вісник Київського університету імені Т. Шевченка. – 2009. – № 14 : Міжнародні відносини. – С. 46-48

14. Остроухов, В. В. До проблеми забезпечення інформаційної безпеки України [Текст] / В. В. Остроухов // Політичний менеджмент. – 2008. – № 4. – С. 135–141.
15. Павлидис, Т. Алгоритмы машинной графики и обработки изображений [Текст] / Т. Павлидис. – М. : Радио и связь, 1986. – 394 с. – ISBN відсутній : [Електронний ресурс] // Портал : eknigu.com. – Режим доступу \www/ URL: [http://www.eknigu.com/info/Cs_Computer_20_science/CsIp_Image_20processing/Pavlidis_20T._20_Algoritmy_20mashinn_oj_20grafiki_20i_20obrabotki_20izobrazhenij_20\(RiS,_201986\)\(ru\)\(K\)\(T\)\(394s\)_CsIp_.djvu#a](http://www.eknigu.com/info/Cs_Computer_20_science/CsIp_Image_20processing/Pavlidis_20T._20_Algoritmy_20mashinn_oj_20grafiki_20i_20obrabotki_20izobrazhenij_20(RiS,_201986)(ru)(K)(T)(394s)_CsIp_.djvu#a). – Заголовок з документа, доступ вільний, 14.01.2013.
16. Искусственный интеллект. Книга 1. Системы общения и экспертные системы : довідник / коллект. авторов ; под. ред. Э. Попова. – М. : Радио и связь, 1990. – 464 с. – ISBN 5-256-00365-8 (кн. 1) : [Електронний ресурс] // Портал : без назви. – Режим доступу \www/ URL: <http://www.twirpx.com/file/218565>. – Заголовок з документа, доступ вільний, 14.01.2013.
17. Александров, В. В. Алгоритмы и программы структурного метода обработки данных : монография / В. В. Александров, Н. Д. Горский. – Л. : Наука, 1983. – 208 с. – ISBN відсутній.
18. Александров, В. В. Базы видеоданных: проблемы и перспективы : монография / В. В. Александров, Н. Д. Горский. – Л. : ЛНИВЦ, 1985. – 72 с. – ISBN відсутній.
19. Александров, В. В. Представление и обработка изображений. Рекурсивный подход : монография / В. В. Александров, Н. Д. Горский. – Л. : Наука, 1985. – 192 с. – ISBN відсутній.
20. Common Criteria [Електронний ресурс] / Портал : Вільна енциклопедія. – Режим доступу \www/ URL: http://uk.wikipedia.org/wiki/Common_Criteria#.D0.A1.D0.BF.D0.BE.D1.81.D1.82.D0.B5.D1.80.D0.B5.D0.B6.D0.B5.D0.BD.D1.96.D1.81.D1.82.D1.8C. – Заголовок з екрану, доступ вільний, 14.01.2013.
21. Bonsor, K. How Facial Recognition Systems Work [Електронний ресурс] / K. Bonsor, R. Johnson // Портал : Howstuffworks – Режим доступу \www/ URL: <http://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition.htm>. – Заголовок з екрану, доступ вільний, 15.01.2013.
22. Цифровая обработка сигналов в оптике и голографии : Введение в цифровую оптику [Текст] / Л. П. Ярославский. – М. : Радио и связь, 1987. – 296 с. : ил., табл. – Библиогр. : с. 291–294. – ISBN відсутній.

23. Александров, В. В. ЭВМ видит мир : монография / В. В. Александров, Н. Д. Горский. – Л. : Машиностроение, Ленингр. отд-ние, 1990. – 136 с. – ISBN відсутній.
24. Распознавание лиц [Электронный ресурс] / Портал : Википедия. – Режим доступа \www/ URL: http://ru.wikipedia.org/wiki/Распознавание_лиц. – Заголовок з екрану, доступ вільний, 16.10.2012.
25. Колодникова, Н. В. Обзор текстурных признаков для задач распознавания образов [Текст] / Н. В. Колодникова // Доклады ТУСУР : Автоматизированные системы обработки информации, управления и проектирования. – 2004. – БН. – С. 113-124. – ISSN відсутній. – [Электронный ресурс] / Портал : tusur.ru. – Режим доступа \www/ URL: www.tusur.ru/filearchive/reports-magazine/2004-9-1/113.pdf. – Заголовок з контейнера, доступ вільний, 23.04.2013.
26. Спектральный анализ меридиональной системы [Электронный ресурс] / Портал : tusur.ru. – Режим доступа \www/ URL: http://skfb.ru/pr110_aa1.html. – Заголовок з екрану, доступ вільний, 23.04.2013.
27. Традиционные методы биометрической аутентификации и идентификации : навчальний електронний посібник / Колешко В. М., Воробей Е. А., Азизов П. М. [та ін.]. – Минск : БНТУ, 2009. – 107 с. – ISBN відсутній. – [Электронный ресурс] / Портал : BNTU. – Режим доступа \www/ URL: rep.bntu.by/bitstream/data/780/7/Основной%20текст.pdf. – Заголовок з контейнера, доступ вільний, 24.04.2013.
28. Протасов, К. Т. Непараметрический алгоритм распознавания объектов подстилающей поверхности Земли по данным аэрокосмической съемки [Текст] / К. Т. Протасов, А. И. Рюмкин // Вестник Томского государственного университета. – 2002. – №275. – С. 41-46. – ISSN відсутній.
29. Андреев, Г. А. Анализ и синтез случайных пространственных текстур [Текст] / Г. А. Андреев, О. В. Базарский, А. С. Глауберман та ін. // Зарубежная радиоэлектроника. – 1984. – №2. – С. 3-33. – ISSN відсутній.
30. Харалик, Р. М. Статистический и структурный подходы к описанию текстур [Текст] / Р. М. Харалик // ТИИЭР. – 1979. – Т.67. – №5. – ISSN відсутній.
31. Потапов, А. А. Новые информационные технологии на основе вероятностных текстурных и фрактальных признаков в радиолокационном обнаружении малоконтрастных целей [Текст] / А. А. Потапов // Радиотехника и электроника. – 2003. – Т.48. – №9. – С. 1101-1119. – ISSN відсутній.

32. Сергеев, В. В. Параллельно-рекурсивные КИХ-фильтры для обработки изображений [Текст] / В. В. Сергеев // Компьютерная оптика. – 1992. – №10-11. – С.186-201. – ISSN відсутній.
33. Напрюшкин, А. А. Алгоритмическое и программное обеспечение системы интерпретации аэрокосмических изображений для решения задач картирования ландшафтных объектов : Дис.... канд. техн. наук. – Томск, 2002. – 183 с.
34. Цифровая обработка изображений : в 2 кн., пер. с англ. / У. Претт. – М. : Мир, 1982. – 790 с. – ISBN 978-5-94836-122-2.
35. Обиралов, А. И. Дешифрирование снимков для целей сельского хозяйства : навчальний посібник / А. И. Обиралов. – М. : Недра, 1982. – 144 с. – ISBN відсутній.
36. Вишневский, В. В. Структурный анализ цифровых контуров изображений как последовательностей отрезков прямых и дуг кривых [Текст] / В. В. Вишневский, В. Г. Калмыков // Штучний інтелект. – 2004. – №3. – С. 479-488. – ISSN відсутній.
37. Калмыков, В. Г. Структурный метод описания и распознавания отрезков цифровых прямых в контурах бинарных изображений / В. Г. Калмыков // Штучний інтелект. – 2002. – №4. – С. 450-457. – ISSN відсутній.
38. Загоруйко, Н. Г. Методы распознавания и их применение : монографія / Н. Г. Загоруйко. – М. : Советское радио, 1972. – 208 с. – ISBN відсутній.
39. Pushkareva, T.G. Detection of fires from satellite images using a nonparametric algorithm of pattern recognition in space of the informative parameters [Текст] / Т. G. Pushkareva, К. Т. Protasov // Proceedings of SPIE. – 2000. – V. 4341. – С. 283-285. – ISSN відсутній.
40. Кормилицына И. Г. Финансовая стабильность: сущность, факторы, индикаторы [Электронный ресурс] / Портал : Финансы и кредит. – Режим доступа \www/ URL: <http://www.fin-izdat.ru/journal/fc/detail.php?ID=43883>. – Финансы и кредит, 2011. – №35(467). – С. 44-54. – Заглавие из текста, доступ свободный, 10.10.2012.
41. Арсентьев М. Финансовая безопасность России [Электронный ресурс] / Портал : Проблемы безопасности России. – Режим доступа \www/ URL: http://www.rau.su/observer/N08_00/08_21.htm. – Заглавие с экрана, доступ свободный, 12.10.2012.
42. Овчинникова А. В. Экономический рост в рамках устойчивого развития социально-эколого-экономической системы [Электронный ресурс] / Портал : Экономика и право. – Режим доступа \www/ URL: http://www.vestnik.udsu.ru/2012/2012-022/vuu_12_022_08.pdf. – Заглавие из текста, доступ свободный, 10.10.2012.

43. Ткаченко В. Г. Об особенностях финансовой безопасности Украины в условиях рыночных трансформационных процессов [Электронный ресурс] / Режим доступа \www/ URL: http://www.nbuv.gov.ua/portal/soc_gum/e_apk/2009_6/09_06_01.pdf. – Заглавие из текста, доступ свободный, 12.10.2012.
44. Ивашина, С. Ю. Инфраструктура социализации экономики [Текст] / С. Ю. Ивашина // Бизнес-информ. – Х. : ХНЭУ. – 2012. – № 6. – С. 13-17.
45. Коваленко Е. В. Экономическая безопасность регионов в социально-экономическом контексте [Электронный ресурс] / В.Г. Ткаченко, Е.В Коваленко // Режим доступа \www/ URL: http://www.nbuv.gov.ua/portal/soc_gum/vchu/N151/N151p129-135.pdf. – Заглавие из текста, доступ свободный, 12.10.2012.
46. Столбов, М. И. Финансовый рынок и экономический рост: контуры проблемы [Текст] : монография / М.И. Столбов // М. : Научная книга, 2008. – 201 с. – (Россия в мировой экономике). – ISBN 978-5-91393-007-1.
47. Доклад о человеческом развитии 2011. Устойчивое развитие и равенство возможностей: лучшее будущее для всех [Электронный ресурс] / Режим доступа \www/ URL: http://www.hdr.undp.org/en/media/HDR_2011_RU_Complete.pdf. – Заглавие из текста, доступ свободный, 12.10.2012. – Опубликовано для Программы развития Организации Объединенных Наций (ПРООН).
48. Терентьев А.М., Ляпичева Н.Г., Кочетова Н.А. Мониторинг корпоративной сети ЦЭМИ РАН в условиях использования коммутатора Cisco Catalyst-2924 / Развитие и использование средств сетевого мониторинга и аудита. – Вып. 1. – Сборн. статей под ред. А.М. Терентьева – М. : ЦЭМИ РАН, 2004. – С. 75-87.
49. Жуков А.В., Аминова И.В. Исследование сетевого трафика web-ресурса «Петрозаводский государственный университет» / [Электронный ресурс] : www.energy-links.com (Режим доступа – свободный).
50. Кочетова Н.А., Ляпичева Н.Г. Методы и средства защиты магистральных маршрутизаторов и серверов удаленного доступа производства Cisco Systems / Вопросы информационной безопасности узла Интернет в научных организациях : Сборник статей под ред. М.Д. Ильменского. – М. : ЦЭМИ РАН, 2001. – С.10-42.
51. Хорошко В.А., Шелест М.Е., Маракова И.И., Сыропятов А.А. Защита информации в беспроводных системах связи // Захист інформації. – К.: ДУІКТ. – 2005. – №3 (25) – С. 83- 91.

52. Потапов М.В., Сиропятов А.О., Оценка эффективности информационной защиты комплексных систем связи // Управління проектами та розвиток виробництва: Вісник СНУ ім. В. Даля. – Луганськ : СНУ ім. В. Даля. – 2006. – 7 стор.
53. Маракова И.И., Скопа А.А., Сыропятов А.А. Комплексная защита информации в беспроводных системах связи // Матер. IV наук.-конф. Департамента спец. телеком. систем та захисту інформ. та Служби безпеки «Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні». – К. : НДЦ «Тезис» НТУУ «КПІ». – 2007. – С.73-75.
54. Казакова Н.Ф. Априорна суперечність раціональної концепції інтелектуальної мережі / Управління проектами: стан та перспективи: Матер. міжнар. наук.-техн. конф. – Миколаїв : НУК ім. адмірала Макарова, 2008. – С.65-67.
55. Казакова Н.Ф., Годулян И.О., Чуприна А.А. Анализ эффективности информационных систем путем синтеза критериев оптимизации алгоритмов их функционирования / Матер. II наук.-практ. семін. молодих науковців та студентства «Сучасні телекомунікаційні та інформаційні технології», 12-14 грудня 2007 р., К. : УНДІЗ.
56. Казакова Н.Ф., Согіна Н.М. Скорочення обсягів контрольних випробувань в інформаційних системах за рахунок їх функціональної надмірності / Моделювання та інформаційні технології. Зб. наук. праць ІМЕ НАН України. – Вип. 49. – К. : 2008.
57. Казакова Н.Ф., Годулян И.О., Чуприна О.О. Установление критериев оптимизации алгоритмов при определении эффективности информационных систем / Наукові записки УНДІЗ. – №1. – К. : УНДІЗ, 2007. – С.62-71.
58. Казакова Н.Ф. Методика организации идеального профилактического обслуживания // Под ред. В.В. Шахгильдяна / Матер. науч.-техн. семін. «Системы синхронизации, формирования и обработки сигналов для связи и вещания», 1-4 июня 2007 г., Москва-Одесса : ІЕЕЕ-РНТОРЭС им.А.С.Попова. – С.167-172.
59. Казакова Н.Ф. Управління послугами телекомунікацій // Матер. II звітної наук.-практ. конф. проф.-викл. складу та студентства Міжнар. гуманіт. ун-ту, 12 квітня 2007 р., Одеса : Міжнар. гуманіт. ун-т, 2007. – С.18-21.
60. Казакова Н.Ф. Задачі захисту інформаційних ресурсів від впливу зовнішніх загроз // Матер. II молод. наук. конф. «Сучасні інформаційні технології в повсякденній діяльності та підготовці фахівців», 31 березня 2006 р., Одеса : ОНЮА, 2006.

61. Казакова Н.Ф. Аналіз внутрішніх та зовнішніх загроз корпоративних мереж // Матер. міжвідомч. міжрегіон. семінару Наук. Ради НАН України «Технічні засоби захисту інформації», 15 лютого 2006 р., Київ-Одеса : НАН України, 2006. – С.11.
62. Щербина Ю.В., Казакова Н.Ф. Проблемы объективной оценки параметров защищенных автоматизированных систем // Матер. IV наук.-техн. конф. «Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні», 1-3 березня 2006 р., К. : НТУУ «КПІ», 2006. – С.60-61.
63. Казакова Н.Ф. Принципи створення систем мережного управління // Матер. наук.-практ. конф. проф.-викл. складу «Актуальні проблеми та досвід використання сучасних інформаційно-комунікаційних технологій», 10-12 травня 2005 р., Одеса : ОНЮА, 2005. – С.133-138.
64. Казакова Н.Ф. Особенности расчета показателей надежности компьютерных устройств управления резервным оборудованием // Матер. VI Міжнар. наук.-практ. конф. студентів, аспірантів та молодих вчених ІПСА-2004 «Системний аналіз та інформаційні технології», 1-3 липня 2004 р., К. : НТУУ «КПІ», 2004. – С.209-210.
65. Kazakova N. Mobil radio-service management system construction principles // Proceeding of the International Conference TCSET'2002 «Modern Problems of Radio Engineering, Telecommunications and Computer Science»: February 18-23, 2002. – Lviv-Slavsk, Ukraine : Lviv Polytechnic National University – IEEE Networking the World. – 2002. – P.284.
66. Казакова Н.Ф. Аналіз моделей побудови мереж зв'язку з радіодоступом // Тр. II междунар. научно-практ. конф. «Современные информационные и электронные технологии СИЭТ-2001» : 28-31 мая 2001 г. – Одесса : ОдГПУ. – 2001. – С.66-67.
67. Казакова Н.Ф. Інформаційне забезпечення системи управління якістю продукції в сфері телекомунікацій // Тр. IV Междунар. научно-практ. конф. «Системы и средства передачи и обработки информации»: ОАО «Нептун», УГАС им.А.С.Попова, Одесса, 6-14 сент. 2000 г. – Одесса, 2000. – С.59-61.
68. 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.
69. The Marsaglia Random Number CDROM including the Diehard Battery of Tests of Randomness // <http://www.stat.fsu.edu/pub/diehard/> Statistical test suite Crypt-X //<http://www.isi.qut.edu.au/resources/cryptx>.
70. eSTREAM, the ECRYPT Stream Cipher Project [Електронний ресурс] // Портал : без назви. – Режим доступу \www/ URL : <http://>

www.ecrypt.eu.org/stream/index.html. – Заголовок з екрану, доступ вільний, 18.05.2013.

71. Кнут, Д. Искусство программирования для ЭВМ [Текст] : монография / Д. Кнут. – М. : Мир, 1977. – 727 с.
72. Харин, Ю. С. Математические и компьютерные основы криптологии [Текст] : учебное пособие / Ю. С. Харин, В. И. Берник, Г. В. Матвеев, С. В. Агиевич. – М. : Новое издание, 2003. – 272 с.
73. Земор, Ж. Курс криптографии [Текст] : монография / Ж. Земор. – Ижевск : НИЦ «Регулярная и хаотическая динамика»; Институт компьютерных исследований, 2006. – 256 с.
74. Рябко, Б.Я. Криптографические методы защиты информации [Текст] : учебное пособие / Б. Я. Рябко, А. Н. Фионов. – М. : МГУ, 2005. – 115 с.
75. Фомичев, В. М. Дискретная математика и криптология [Текст] : курс лекций / В. М. Фомичев // под общ. ред. Н. Д. Подуфалова. – М. : ДИАЛОГ-МИФИ, 2003. – 400 с.
76. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си [Текст] : монография / Б. Шнайер. – М. : Триумф, 2002. – 816 с.
77. Кац, М. Статистическая независимость в теории вероятностей, анализе и теории чисел [Текст] : монография / М. Кац. – М.: Издательство иностранной литературы, 1963. – 156 с.
78. Скопа О.О. Інтервальне оцінювання надійності Т-систем з паралельним з'єднанням елементів за результатами їх біноміальних іспитів // Наукові праці ОНАЗ: Період. наук. збір. з радіотехніки і телекомунікацій, електроніки та економіки в галузі зв'язку. – Одеса, 2002. – №1. – С.65–71.
79. Казакова Н.Ф., Мухін О.М., Скопа О.О. Скорочення обсягу випробувань систем телекомунікацій на надійність за рахунок їх структурної надмірності // 1-й Міжнарод. радіоелектрон. форум «Прикладная радиоэлектроника. Состояние и перспективы развития»: 8–10 октября 2002 г.: Сб. научн. трудов. – Харьков: ХНУРЕ. – 2002. – С.358–360.
80. Панфилов И.П., Скопа А.А. Надежность работы линии связи, состоящей из основного и резервного каналов // Радиотехника: Всеукр. межведомств. научн.-техн. сб. – Харьков. – 2002. – Вып. 128. – С.91-96.
81. Скопа О.О., Казакова Н.Ф., Мурін О.С. Вплив функціональної надмірності резервованих систем телекомунікацій на скорочення обсягів їх випробувань на надійність // Наук. праці ДонНТУ. Серія:

- Обчислювальна техніка та автоматизація. Випуск 58. – Донецьк: РВА ДонНТУ, 2003. – С.115-121.
82. Скопа О.О. Обслуговування резервних систем зв'язку // Наук. праці ДонДТУ. Серія: Обчислювальна техніка та автоматизація. Випуск 38. – Донецьк: РВА ДонДТУ, 2002. – С.89-91.
 83. Скопа О.О. Оптимізація експлуатації резервних систем телекомунікацій // Праці УНДІРТ. – Одеса, 2002. – №1(29). – С.91–93.
 84. Скопа О.О. Інтервальне оцінювання надійності Т-систем з паралельним з'єднанням елементів за результатами їх біноміальних іспитів // Наукові праці ОНАЗ: Період. наук. збір. з радіотехніки і телекомунікацій, електроніки та економіки в галузі зв'язку. – Одеса, 2002. – №1. – С.65–71.
 85. Скопа А.А., Казакова Н.Ф. Применение теории псевдополубратных матриц к решению задач по оценке надежности систем телекоммуникаций. Часть 1. Общие положения // Праці УНДІРТ. – Одеса, 2002. – №4(32). – С.88-91.
 86. Казакова Н.Ф. Технічне рішення задачі Клопера-Пірсона / Наук. записки Міжнар. гуманіт ун-ту. Випуск 3. – Одеса: МГУ, 2005. – С.89-94.
 87. Казакова Н.Ф. Аналітичне розв'язання одновимірної задачі Клопера-Пірсона // Радиотехника: Всеукр. межведомств. научн.-техн. сб. – Харьков: ХНУРЭ. – 2002. – Вып. 128. – С.97-98.
 88. Бурбаки Н. Теория множеств. – М.: Мир, 1965. – 465 с.
 89. Судаков Р.С. Интервальная оценка монотонных функций по результатам испытаний // Техническая кибернетика. Изв. АН СССР. – 1986. – №1. – С. 82-91.
 90. Судаков Р.С., Северцев Н.А. и др. Статистические задачи отработки систем и таблицы для числовых расчетов показателей надежности. – М.: Высшая школа, 1975. – 607 с.
 91. Харди Г., Литтлвуд Д., Поля Г. Неравенства. – [Электронный ресурс]: http://e-books.enigma.uran.ru/book_djvu/hardi/hardi.djvu: Доступ свободный.
 92. Обратные и некорректные задачи // Наука в Сибири: Еженедельная газета Сибирского отделения РАН. – №40(2725), 08.10.2009. – [Электронный ресурс]: <http://www-sbras.nsc.ru/HBC/article.phtml?nid=519&id=10>. – Режим доступа: вільний.
 93. Кабанихин С. И. Обратные и некорректные задачи. – Учебник: СНИ, 2008. – [Электронный ресурс]: <http://www.twirpx.com/file/238358/> – Режим доступа: вільний.

94. Арсенин В.Я., Тихонов А.Н. Некорректные задачи / Математическая энциклопедия. – Сов. энциклопедия, 1982. – Т.3. – С.930-935. – [Электронный ресурс]: http://dic.academic.ru/dic.nsf/enc_mathematics/3375/Некорректные. – Режим доступа: вільний.
95. Відновлення та оптимізація інформації в системах прийняття рішень / Баранов В.Л., Браїловський М.М., Засядько А.А., Казакова Н.Ф., Хорошко В.О. // Підручник. – К.: Видн. ДУІКТ, 2009. – 134 с.
96. Верлань А.Ф., Сизиков В.С. Интегральные уравнения: методы, алгоритмы, программы. Справочное пособие. – К.: Наукова думка, 1986. – 544 с. – [Электронный ресурс]: <http://www.twirpx.com/file/273092/> – Режим доступа: вільний.
97. Морозов В.А. Регулярные методы решения некорректно поставленных задач. – М.: Наука, 1987. – 240 с. – [Электронный ресурс]: <http://www.srcc.msu.ru/nivc/sci/books/morozov6.html> – Режим доступа: вільний.
98. Морозов В.А. Об устойчивых методах решения систем линейных алгебраических уравнений // Вычислительные методы линейной алгебры. – Новосибирск: СО АН СССР, 1974.
99. Тихонов А.Н. О регуляризации некорректно поставленных задач // Доклады АН СССР. – №3, 1963. – С. 501-504. – [Электронный ресурс]: http://www.mathnet.ru/php/getFT.phtml?jrnid=zvmmf&paperid=7494&what=fullt&option_lang=rus – Режим доступа: вільний.
100. Бакут, П. А. Вопросы статистической теории радиолокации : монография / П. А. Бакут, И. А. Большаков [и др.]. – М. : Сов. радио, 1964. – 426 с.
101. Трис, В. Теория обнаружения оценок и модуляции : монография / Ван Трис Г. – М. : Сов. радио, 1972. – 744 с.
102. Гуткин, Л. С. Проблемы оптимизации радиосистем [Текст] / Л. С. Гуткин // Радиотехника. – М. : Радиотехника. – 1971. – №5. – С. 21-29.
103. Гуткин, Л. С. Оптимизация радиоэлектронных устройств по совокупности показателей качества : монография / Л. С. Гуткин. – М. : Сов. радио, 1974. – 368 с.
104. Скопа, А. А. Анализ влияния точности измерения параметров радиоканала на помехоустойчивость приема [Текст] / А. А. Скопа, Н. М. Билык // Наукові записки УНДІЗ. – К. : УНДІЗ. – 2007. – №1. – С. 79-85.
105. Скопа, О. О. Проектний аналіз оцінювання ступеня ризику при скороченні обсягу профілактичних вимірювань об'єктів інфомереж / О. О. Скопа, Н. Ф. Казакова // Вісник Львівського національного

- аграрного університету: Агроінженерні дослідження. – Львів : ЛНАУ. – 2008. – №12. – Т.1. – С. 66-71.
106. Грабовський, О. В. Аналіз показників якості інформаційно-вимірювальних систем [Текст] / О. В. Грабовський // Вісник національного університету «ХП». – Харків : НТУ ХП. – 2013. – С. 59-66.
107. Грабовський, О. В. Організація вимірювання на мережах рухомого зв'язку [Текст] / О. В. Грабовський // Вимірювальна та обчислювальна техніка в технологічних процесах : міжнар. наук. техн. конф., 2007 р. : тези допов. – Хмельницький, 2007. – С. 33.
108. Колесникова, Е. В. Методы оценки качества технических систем [Текст] / Е. В. Колесникова, Г. В. Кострова, И. В. Прокопович // Труды Одесского политехнического университета. – О. : ОНПУ. – 2007. – №1(27). – С. 128-130 : [Електронний ресурс] / Портал : ОНПУ. – Режим доступу \www/ URL: <http://pratsi.opu.ua/app/webroot/articles/1312992391.pdf>. – Заголовок з контейнера, доступ вільний, 30.10.2012.
109. Кириллов, В. И. Квалиметрия и системный анализ : навч. посібник / В. И. Кириллов. – Минск : Новое знание ; М. : ИНФРА-М, 2011. – 440 с. : ил. – (Высшее образование). – ISBN 978-985-475-353-9 (Новое знание) ; ISBN 978-5-16-004689-1 (ИНФРА-М).
110. Пегат, А. Нечеткое моделирование и управление / А. Пегат ; пер. с англ. – М. : БИНОМ. Лаборатория знаний, 2009. – 798 с. : ил. – (Адаптивные и интеллектуальные системы). – ISBN 978-5-94774-353-1 (русск.), ISBN 3-7908-1385-0 (англ.).
111. Адлер, Ю. П. Планирование эксперимента при поиске оптимальных условий : монографія / Ю. П. Адлер, Е. В. Маркова, Ю. В. Грановский. – М : Наука, 1976. – 269 с. – ISBN відсутній.
112. Федорченко, С. Г. Обобщенная функция полезности и ее приложения : монографія / С. Г. Федорченко, Ю. А. Долгов, А. В. Кирсанова [та ін.] / Під ред. С. Г. Федорченко. – Тирасполь : Приднестровский ун-т, 2011. – 196 с. – ISBN978-9975-4062-3-9.
113. Ногин, В. Д. Принятие решений в многокритериальной среде: количественный подход : монографія. – М. : ФИЗМАТЛИТ, 2002. – 144 с. – ISBN 5-9221-0274-5.
114. Батищев, Д. И. Оптимизация многоэкстремальных функций с помощью генетических алгоритмов / Д. И. Батищев, С. А. Исаев // Межвуз. сборник : Воронеж, ВГТУ. – 1997. – №3. – с. 4-17.
115. Кучерявый, А.Е. Качество обслуживания и качество восприятия. Рекомендации МСЭ-Т [Электронный ресурс] / Портал : ITU. – Режим доступа \www/ URL: : <http://www.itu.int/en/ITU-D/Regulatory->

- Market/.../Session3_Kucheryaviy.pdf. – Заголовок с контейнера, доступ свободный, 30.07.2013.
116. Y.1541 : Network performance objectives for IP-based services [Электронный ресурс] / Портал : ITU. – Режим доступа \www/ URL: <http://www.itu.int/rec/T-REC-Y.1541/en>. – Заголовок с экрана, доступ свободный, 29.07.2013.
117. СОУ 64.2-00017584-008 : 2010 «Телекомунікаційні мережі передачі даних загального користування. Система показників якості услуг з передачі даних та доступу до Інтернет. Загальні положення» [Електронний ресурс] / Портал : document.ua. – Режим доступу \www/ URL: <http://document.ua/sou-64.2-00017584-008-2010-srdsdoc-srh3000531215.html>. – Заголовок з екрану, доступ вільний, 29.07.2013.
118. СОУ 64.2-00017584-009:2010 «Телекомунікаційні мережі передачі даних загального користування. Телекомунікаційні послуги. Показники якості. Методи випробувань та оцінки» [Електронний ресурс] / Портал : document.ua. – Режим доступу \www/ URL: <http://document.ua/sou-64.2-00017584-009-2010-srdsdoc-srh2000534389.html>. – Заголовок з екрану, доступ вільний, 29.07.2013.
119. Y.1291 : An architectural framework for support of Quality of Service in packet networks [Электронный ресурс] / Портал : ITU. – Режим доступа \www/ URL: <http://www.itu.int/rec/T-REC-Y.1291/en>. – Заголовок с контейнера, доступ свободный, 30.07.2013.