Литература

1. Бегма Т. В. Математичні моделі функціонування складних систем / Бегма Т. В., Капустян Н. В., Хорошко В. О. // Вісник СНУ ім. В. Даля, №7(161), 2.1, 2011. – С. 252 –263.
2. Энслоу Ф. Г. Мультипроцессорные системы и параллельные вычисления / Энслоу Ф. Г. – М.:Мир, 1976. – 383с.
3. Скорик В. Н. Мультимикропроцессорные системы / Скорик В. Н., Степанов А. Е., Хорошко В. А. – К.: Техника, 1989. – 192с.
4. Мину М. Математическое моделирование / Мину М. – М.: Наука, 1990. – 488с.
5. Капустян М. В. Оценка эффективности функционирования сложных систем / Капустян М. В., Хорошко В. А. // Інформаційна безпека, №1, 2011. – с. 5-8.

Пархуць Л.Т., Хорошко В.О. Чирков Д.В. Оцінка ефективності використання багатопроцесорних систем управління інформаційною безпекою

Викладено методику оцінки ефективності використання багатопроцесорних ЕОМ різних типів при реалізації комплексних алгоритмів систем управління інформаційною безпекою.

Ключові слова: *окремий алгоритм, комплексний алгоритм, мікропроцесорні ЕОМ.*

Parhutc L.T., Khoroshko V.A., Chirkov D.V. Estimation of efficiency of application of multiprocessor control system by informative safety

The method of estimation of efficiency of the use of multiprocessor COMPUTERS of different types is expounded during realization of kompleksnikh algorithms of control system by informative safety.

Key words: special algorithm, complex algorithm,computer microprocessors.

Стаття надана 20.04.2012

УДК 519.711:004.052.2

Мінін А.В., Скопа О.О., Алєксандер М.

Східноукраїнський національний університет імені Володимира Даля, м. Луганськ
Одеський державний економічний університет, м.Одеса
Державна вища технічна школа у Новому Сончі, Польща

БІНОМІАЛЬНІ МОДЕЛІ ВИПРОБУВАННЯ ЖИВУЧОСТІ ЗАХИЩЕНИХ ІНФОРМАЦІЙНИХ КАНАЛІВ

Аналізується схема біноміальних випробувань із узагальненням нових результатів теоретичного і прикладного характеру щодо випробування живучості захищених інформаційних каналів.

Ключові слова: *біноміальні випробування, живучість інформаційних каналів, β-функція.*

У 1717 році Я.Бернуллі запропонував схему біноміальних випробувань, якій пощастило стати класичною моделлю в теорії ймовірностей. Завдяки простоті і спільності вихідних передумов вона знайшла широке застосування в теорії визначення різноманітних показників технічних систем, а також при оцінці тих параметрів, вимір яких неможливий. До таких параметрів відносяться, наприклад, надійність, працездатність, живучість, стійкість

технічних систем, а також інші властивості, що характеризуються імовірнісними показниками [1, 2].

Зупинимося на класичному прикладі процедури біноміальних випробувань та сформулюємо вихідні передумови для схеми випробувань Бернуллі стосовно дослідження живучості захищених інформаційних каналів [3].

Надалі будемо розглядати довільний інформаційний канал, який випробовується n разів [4-5, 8]. Вважаємо, що обсяг n випробування встановлюється заздалегідь до їхнього початку. У кожнім i-м випробуванні можливе виникнення лише однієї з двох подій – A_i або $\overline{A}_i$, з яких $\overline{A}_i$ – подія, протилежна A_i. Наприклад, A_i може складатися в успішному результаті i-го випробування і тоді $\overline{A}_i$ – подія, що полягає у виникненні відмовлення в цьому випробуванні. Події A_i (при $i=\overline{1,\ n}$) вважаються незалежними. Це означає, що імовірність їхнього спільного виникнення дорівнює добуткові ймовірностей $P(A_i)$. $P(A_i)$ – імовірність виникнення події A_i, що вважається однаковою при кожному з n випробувань, тобто $P(A_1)=P(A_2)=\ =P(A_3)=...=P(A_n)=const$.

Зобразимо кожне i-е випробування на схемі (рис. 1) [1] світлим кружком, якщо в ньому реалізується подія A_i, а темним – протилежний випадок.

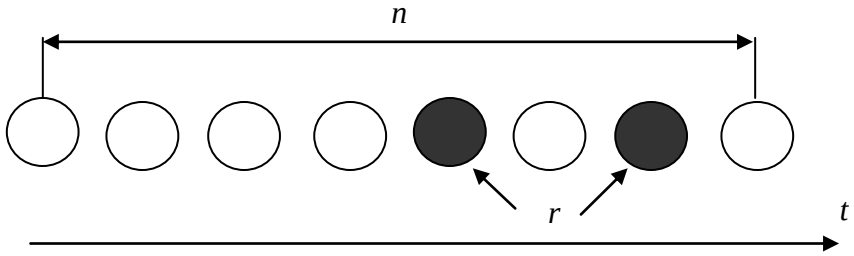

Рис. 1. Система умовних зображень

Розглянемо випадкову величину r, що дорівнює числу подій $\overline{A}_i$ в n випробуваннях. На рис. 1 ілюструється ситуація, що відповідає одному з результатів у схемі з n випробувань, коли величина r набула конкретного значення: $r=2$. У загальному випадку до проведення випробування конкретне значення величини непередбачене і можна лише стверджувати, що ним є одне з чисел $k=0,\ 1,...,n$. Значення випадкової величини r являють собою фіксовані числа. Вони приймаються нею з різними ймовірностями $P_k=P(r=k)$. З припущень, прийнятих у схемі Бернуллі, а також з формул додавання і множення ймовірностей випливає, що

$$P(r=k)=\binom{n}{k}R^{n-k}q^k,$$

де: $q=1-R$, $\binom{n}{k}=\frac{n!}{k!(n-k)!}$, $n!=n\cdot(n-1)\cdot\ ...\ \cdot2\cdot1$,

причому формально припускають, що $0!=1$, називаючи число $\binom{n}{k}$ біноміальним коефіцієнтом. Таким чином, можна знайти імовірність P_k того, що в біноміальних випробуваннях виникне фіксоване число k подій $\overline{A}_i$ і $n-k$ подій A_i. Зокрема $P(r=0)=R^r$ – імовірність того, що в n біноміальних випробуваннях виникне n подій A_i. Якщо припустити, що x є ціле фіксоване число, то з формули додавання ймовірностей і з отриманого вище результату випливає, що $P(r\le x)=\sum_{k=0}^{x}\binom{n}{k}R^{n-k}q^k$. Цей вираз можна записати для будь-якого, не обов'язково цілого числа x: $P(r\le x)=\sum_{k=0}^{[x]}\binom{n}{k}R^{n-k}q^k=B_i(n,\ R,\ x)$, де: $[x]$ – ціла частина числа x, а $B_i(n,\ R,\ x)$ – додаткове позначення зазначеної суми щодо нецілих чисел.

Як наслідок відзначимо, що з цього виразу знаходиться імовірність $P(r\le x)$ того, що число r подій $\overline{A}_i$ у n біноміальних випробуваннях не перевищить фіксоване значення $[x]$.

Приклад 1. Здійснюється $n=12$ включень захищеного каналу з метою перевірки і контролю відповідності його параметрів паспортним вимогам. Відомо, що в кожному із включень канал функціонує незалежно від того, які результати його випробування були в інших циклах. Іншими словами, якщо A_i – випадкова подія, що полягає в успішному функціонуванні каналу в i-му циклі, то, як зазначено в умові, всі події A_i при $i=\overline{1,n}$ є незалежними. Нехай дано, що від циклу до циклу не відбувається нагромадження пошкоджень, в силу чого імовірність $P(A_i)$ успішного функціонування каналу в i-му циклі залишається однаковою і дорівнює $P(A_i)=R=0,97$ при $i=\overline{1,n}$. Потрібно знайти імовірність того, що:

– у n циклах не виникне жодного відмовлення каналу, тобто $r=0$;

– у n циклах виникне не більше трьох відмов, тобто $r\le 3$. При $r\ge 3$ канал вважається таким, що вийшов з ладу і система має задіяти резервний канал.

Розв'язання. Оскільки вихідні передумови схеми Бернуллі в даному випадку виконуються, то шукані імовірності можна знайти за вищеприведеними формулами:

$$P_0=P(r=0)=R^n=(0,97)^{12}=0,694;$$

$$P(r\le 3)=P(r=0)+P(r=1)+P(r=2)+P(r=3)=0,694+0,257+0,044+0,004=0,999$$

.

Приклад 2. Є $n=12$ захищених каналів. Особливості їхнього включення такі, що випадкові події A_i (кожна з яких полягає в успішному функціонуванні i-го каналу) при $i=\overline{1,n}$, незалежні. В силу ідентичності можна також допустити, що імовірність $P(A_i)$ успішного функціонування i-го каналу однакова для кожного з них, причому $P(A_i)=R=0,97$ при $i=\overline{1,n}$. Потрібно знайти імовірність того, що в $n=12$ випробуваннях виникне не більше трьох відмов (тобто $r>3$).

Розв'язання. Використовуючи результати розрахунків з прикладу 1 та раніше наведені формули, отримуємо:

$$P(r>3)=1-P(r\le 3)=1-\sum_{k=0}^{3}\binom{n}{k}R^{n-k}(1-R)^k=1-\left(R^n+\binom{n}{1}R^{n-1}q+\binom{n}{2}R^{n-2}q^2+\binom{n}{3}R^{n-3}q^3\right)=0,001$$

.

Відзначимо, що в прикладах 1 і 2, незважаючи на подібність поставлених задач і використовуваних технічних засобів, розглядаються дві принципово відмінні схеми випробування, хоча обидві вони укладаються в біноміальну модель Бернуллі. У прикладі 1 розглядається ситуація, в якій випробуванням піддається один канал циклічного або багаторазового використання. Приклад 2 ілюструє випадок випробування n ідентичних каналів, час використання $t_{âèê}$ яких набагато перевищує час чекання включення $t_{ï\div}$. У літературі такі технічні системи умовно називають системами одноразового використання. Зрозуміло, що захищені інформаційні канали відносяться саме до таких технічних систем у зв'язку з тим, що їх найчастіше використовують лише для передавання спеціальних даних, наприклад, ключів, паролів, кодових слів та інших параметрів різноманітних криптографічних перетворень.

Відмінності в зазначених двох схемах випробувань найбільше чітко виявляються, наприклад, коли при виконанні допущень прикладу 2 у процесі циклічних випробувань відбувається нагромадження пошкоджень, урахування яких в межах моделі біноміальних випробування Бернуллі виявляється неможливим через залежність подій A_i і зміни імовірності $P(A_i)$ від циклу до циклу.

Приклад 3. Розглянемо систему передавання спеціальних відомостей (рис. 2), що складається з n ідентичних каналів. Вважатимемо, що зазначена система відповідає визначенню про систему одноразового використання, тобто кожен з каналів для передавання ключів використовується надзвичайно рідко – $t_{âèê}>>t_{ï\div}$.

Система функціонує успішно, якщо число r її каналів, що виходять з ладу, не перевищує фіксоване ціле число $x\le(n-1)$. Відомо, що події A_i при $i=\overline{1,n}$, кожна з яких полягає в успішному функціонуванні i-го каналу системи, незалежні і мають рівні імовірності $P(A_i)=R$. Потрібно знайти імовірність $\hat{P}$ успішного функціонування системи в цілому, тобто встановити факт гарантованого передавання відомостей.

Розв'язок. Оскільки у прикладі $\hat{P}=P(r\le x)$ та умови схеми біноміальних випробування виконуються, то знаходимо:

$$\widehat{P} = P\left(r \le x\right) = B_i\left(n, R, x\right).$$

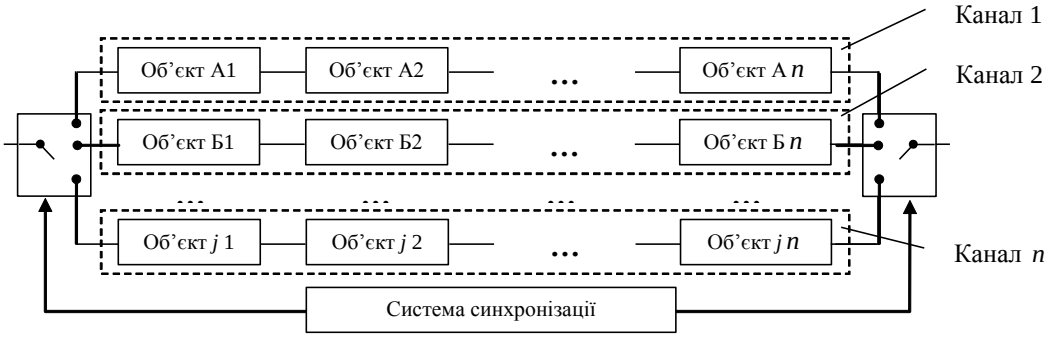

Рис. 2. Система передавання спеціальних відомостей

Зокрема при $x = \left(n-1\right)$, використовуючи відому формулу бінома Ньютона, дістаємо:

$$\widehat{P} = P\left(r \le \left(n-1\right)\right) = \sum_{k=0}^{n-1}\binom{n}{k}R^{n-k}q^k = \sum_{k=0}^{n}\binom{n}{k}R^k q^k - \binom{n}{n}R^{n-n}q^n = 1-q^n.$$

Надалі для викладу теоретичних досліджень будуть потрібні деякі властивості функції біноміального розподілу, багато з яких формулюються у вигляді нерівностей. Для повноти подання матеріалу узагальнимо теоретичну сторону схеми випробування Бернуллі стосовно випадків, які розглядаються. Зазначимо, що чудовою особливістю функції $B_i\left(n, R, x\right)$ є її зв'язок з неповною β-функцією, а саме:

$$B_i\left(n, R, l\right) = \sum_{k=0}^{[l]}\binom{n}{k}R^{n-k}\left(1-R\right)^k = I_R\left(n-\left[l\right],\ \left[l\right]+1\right). \quad (1)$$

У довідниковій літературі наводиться стандартне позначення неповної β-функції – $I_x\left(a,b\right)$. В зв'язку з цим у даному позначенні покладемо $a = n-\left[l\right]$, $b = \left[l\right]+1$ і $x = R$, щоб отримати (1). З метою збереження стандартного позначення використаємо в (1) символ l замість x. Відзначимо, що, як це відзначається в науковій літературі,

$$I_x\left(a,b\right) = \frac{1}{B\left(a,b\right)}\int_0^x t^{a-1}\left(1-t\right)^{b-1}dt, \quad (2)$$

$$B\left(a,b\right) = \int_0^1 t^{a-1}\left(1-t\right)^{b-1}dt = \frac{\tilde{A}\left(a\right)\tilde{A}\left(b\right)}{\tilde{A}\left(a+b\right)}$$

де $x \in \left[0,1\right]$; t – змінна інтегрування; – коефіцієнт, де $\tilde{A}\left(a\right)$, $\tilde{A}\left(b\right)$ і $\tilde{A}\left(a+b\right)$ – значення γ-функції $\tilde{A}\left(y\right) = \int_0^\infty t^{y-1}e^{-t}dt$,

причому $\tilde{A}(y+1)=y\tilde{A}(y)$. Для цілих $y=n+1$ γ-функція набуває значення $\tilde{A}(n+1)=n!$. Коефіцієнт $B(a,b)$ називають β-функцією аргументів a і b.

Формула (1) встановлює той факт, що при цілих $a=n-[l]$ і $b=[l]+1$ неповна β-функція збігається з $B_i(n,R,l)$, якщо в (2) додатково покласти верхню межу $x=R$.

Згідно з [6, 7] мають місце співвідношення:

$$\left.\begin{aligned} I_x(a,b)&=1-I_{1-x}(b,a)\\ I_x(a,b)&=xI_x(a-1,b)+(1-x)I_x(a,b-1)\\ I_x(a,b)&=\frac{1}{x}\left(I_x(a+1,\ b)-(1-x)I_x(a+1,b-1)\right);\quad x>0;\\ I_x(a,b)&=x^a\varphi(x),\quad \varphi(x)=\frac{1}{a\cdot B(a,b)}F(a,\,1-b,\,a+1,\,x), \end{aligned}\right\} \tag{3}$$

де $F(a,\,1-b,\,a+1,\,x)=\dfrac{\tilde{A}(a+1)}{\tilde{A}(a)\tilde{A}(1-b)}\sum\limits_{k=0}^{\infty}\dfrac{\tilde{A}(a+k)\tilde{A}(1-b+k)}{\tilde{A}(a+1+k)}\cdot\dfrac{x^k}{k!}$, – гіпергеометрична функція Гауса.

Для дослідження властивостей функції $I_x(a,b)$ сформулюємо необхідні умови та приведемо у вигляді лем результати досліджень та узагальнень. Відзначимо, що в загальному випадку деякі з властивостей функції $I_x(a,b)$ показані в [8].

Лема 1. Нехай дано невід'ємні функції $f_1(y)$ і $f_2(y)$, причому:

– $f_1(y)$ обмежена на інтервалі $(0,x)$, безперервна на $(0,x)$ і не має нулів усередині $[0,x]$;

– $f_2(y)$ обмежена на інтервалі $(0,1)$, безперервна на $(0,1)$ і не має нулів усередині $[0,1]$.

Якщо дано функцію $\varphi(y)$, що строго убуває на інтервалі $(0,1)$, то за умови, що $f_1(y)>f_2(y),\ \ (y\in[0,x]\subset[0,1])$ і $\int\limits_0^x f_1(y)dy=\int\limits_0^1 f_2(y)dy=1$, виконується нерівність:

$$\int\limits_0^x f_1(y)\varphi(y)dy>\int\limits_0^1 f_2(y)\varphi(y)dy. \tag{4}$$

Якщо за тих самих умов φ (y) строго зростає на інтервалі $[0,\ 1]$, то:

$$\int_0^x f_1(y)\varphi(y)dy < \int_0^1 f_2(y)\varphi(y)dy \quad . \tag{5}$$

Доведення. Перепишемо (4) у вигляді співвідношення:

$$\int_0^x \big(f_1(y) - f_2(y)\big)\varphi(y)dy > \int_x^1 f_2(y)\varphi(y)dy \quad . \tag{6}$$

Покажемо, що (6) виконується. З цією метою використовуємо відому теорему про середнє, відповідно до якої в умовах розглянутого твердження існує точка $\xi \in (x,1)$, для якої $\int_x^1 f_2(y)\varphi(y)dy = \varphi(\xi)\int_x^1 f_2(y)dy$, і, аналогічно, існує точка $\xi' \in (0,x)$, для якої

$$\int_0^x \big(f_1(y) - f_2(y)\big)\varphi(y)dy = \varphi(\xi')\int_0^x \big(f_1(y) - f_2(y)\big)dy \quad ,$$

де $\xi' < \xi$.

Тоді, з врахуванням того, що за умовою леми $\varphi(\xi') > \varphi(\xi)$ співвідношення (6) запишемо як $\varphi(\xi')\int_0^x \big(f_1(y) - f_2(y)\big)dy > \varphi(\xi)\int_x^1 f_2(y)dy$ або

$\varphi(\xi')\left(1 - \int_0^x f_2(y)dy\right) = \varphi(\xi')\int_x^1 f_2(y)dy > \; > \varphi(\xi)\int_x^1 f_2(y)dy$. Але це відповідає $\varphi(\xi') > \varphi(\xi)$ й еквівалентно (4) і (5), що, як показано вище, виконується.

Аналогічно можна довести співвідношення (6) для випадку, коли φ строго зростає на інтервалі $[0,1]$.

Лема 2. Функція $I_x(a,b)$ строго зростає за $b > 0$ при $a > 0$ і $x \in (0,1)$.

Доведення. Тому що $I_x(a,b) = \frac{B_x}{B}$, $B_x = \int_0^x y^{a-1}(1-y)^{b-1}dy$, $B = \int_0^1 y^{a-1}(1-y)^{b-1}dy$, то $\frac{\partial I_x}{\partial b} = \frac{B_x' B - B' B_x}{B^2}$, $B_x' = \frac{\partial}{\partial b}B_x$, $B' = \frac{\partial}{\partial b}b$ і, таким чином, варто встановити, що $B_x' B - B' B_x > 0$ або

$$\frac{B'_x}{B_x}=\int_0^x f_1(y)\varphi(y)dy>\frac{B'_1}{B}=\int_0^x f_2(y)\varphi(y)dy, \tag{7}$$

$$f_1(y)=\frac{y^{a-1}(1-y)^{b-1}}{\int_0^x y^{a-1}(1-y)^{b-1}dy}>f_2(y)=\frac{y^{a-1}(1-y)^{b-1}}{\int_0^1 y^{a-1}(1-y)^{b-1}dy}$$

де , причому функція $\varphi(y)=\ln(1-y)$ строго убуває за $y\in(0,1)$ і тепер зрозуміло, що (7) безпосередньо випливає з (4).

Лема 3. Функція $I_x(a,b)$ строго убуває за $a>0$ при $b>0$ і $x\in(0,1)$. Функція $I_x(a(1-t),at+1)$ строго зростає за $t\in(0,1)$ при $a>0$ і $x\in(0,1)$.

Доведення. Використовуючи нерівність (4), знаходимо, що похідна

$$\frac{\partial I_x(a(1-t),at+1)}{\partial t}=\frac{B'_xB-B'B_x}{B^2}>0 \tag{8}$$

при всіх $x\in(0,1)$, $t\in(0,1)$ і $a>0$ або $\frac{B'_x}{B_x}>\frac{B'}{B}$, $B'_x=\frac{\partial}{\partial t}B_x$,

$B_x=\int_0^x y^{a(1-t)-1}(1-y)^{at}dy$ $B_1=\int_0^1 y^{a(1-t)-1}(1-y)^{at}dy$

де , .

Дійсно, $\frac{B'_x}{B_x}=\frac{\frac{\partial B_x}{\partial t}}{B_x}=\int_0^x f_1(y)\varphi(y)dy$ $\frac{B'_1}{B_1}=\int_0^1 f_2(y)\varphi(y)dy$, , де

$f_1(y)=\frac{y^{a(1-t)-1}(1-y)^{at}}{\int_0^x y^{a(1-t)-1}(1-y)^{at}dy}$ $f_2(y)=\frac{y^{a(1-t)-1}(1-y)^{at}}{\int_0^1 y^{a(1-t)-1}(1-y)^{at}dy}$,

і $a\ln\left(\frac{1}{y}-1\right)=\psi(y)$.

Легко переконатися, що добутки $f_1(y)\psi(y)$ і $f_2(y)\psi(y)$ інтегруються на $[0,1]$. При цьому $\int_0^x f_1(y)dy=\int_0^1 f_2(y)=1$, $f_1(y)>f_2(y)$, $y\in(0,1)$, а $\psi(y)$ безперервна на $(0,y)$ та убуває за $y\in(0,1)$. У такий спосіб (8) випливає з нерівності (4).

Примітка 1. Відмітимо, що зазвичай використовується такий варіант теореми про середнє:

Нехай функції $f(x)$ та $g(x)$ обмежені на інтервалі $[a,b]$ і безперервні на (a,b); нехай $g(x)$ не має нулів у проміжку (a,b). Тоді існує така точка $\xi \in (a,b)$, для якої $\int_a^b f(x)g(x)dx = f(\xi)\int_a^b g(x)dx$. Це співвідношення зберігається при таких умов (використаних вище):

1. Функція $g(x)$ обмежена на інтервалі $[a,b]$, безперервна на (a,b) і не має нулів у цьому проміжку (тобто та ж умова, що наведена вище для $g(x)$);

2. Функція $f(x)$ безперервна на (a,b). При цьому знімається вимога до обмеженості $f(x)$ на інтервалі $[a,b]$;

3. Добуток $\varphi(x) = g(x)f(x)$ інтегрується (у змісті Римана) на інтервалі $[a,b]$.

Доведемо приведене співвідношення за наведених умов. Для цього введемо позначення: $\Phi(x) = \int_a^x \varphi(t)dt$ і $F(x) = \int_a^x g(t)dt$ при $x \in [a,b]$. Тоді відповідно до відомої теореми інтегрального обчислення $\Phi(x)$ і $F(x)$ – безперервні функції на інтервалі $[a,b]$. При цьому $F'(x) = g(x) \neq 0$ при усіх $x \in (a,b)$ (за умовою 1).

Викладене дозволяє використовувати теорему Коші, за допомогою якої знаходимо:

$$\frac{\int_a^b f(t)g(t)dt}{\int_a^b g(t)dt} = \frac{\Phi(b)-\Phi(a)}{F(b)-F(a)} = \frac{\Phi'(\xi)}{F'(\xi)} = \frac{f(\xi)g(\xi)}{g(\xi)} = f(\xi),$$

де ξ - деяке число з проміжку (a,b), що і доводить твердження.

Лема 4. Функція $I_x(a(1-t), at+1)$ убуває за a при $x \leq 1-t$ або зростає за a при $x > 1-t$ для кожного $t \in (0,1)$.

Доведення. Позначимо $B_x' = \frac{\partial}{\partial a}B_x$ і $B_1' = \frac{\partial}{\partial a}B_1$, де функції B_x і B_1 ті ж, що в лемі 2. Покажемо, що

$$\frac{B_x'}{B_x} < \frac{B'}{B} \text{ при } x \leq 1-t. \quad (9)$$

Оскільки $\frac{B'_x}{B_x}=\int\limits_0^x f_1(y)\psi_1(y)\,dy$, $\frac{B'_1}{B_1}=\int\limits_0^x f_2(y)\psi_1(y)\,dy$, $\psi_1(y)=(1-t)\ln y+t\ln(1-y)=\ln y^{1-t}(1-y)^t$, а функція $y^{1-t}(1-y)^t$ строго зростає при $y<1-t$, то, відповідно, до нерівності (5) співвідношення (9) виконується. Це означає, що перша частина леми встановлена. Аналогічно з огляду на факт строгого убування функції $\psi_1(y)$ при $y>1-t$ за допомогою (4) можна переконатися у справедливості другої частини леми.

Лема 5. Функція $\varphi(x)=\frac{I_x(a,b)}{x^a}$ при $a>0$ й $b>1$ убуває по $x\in(0,1)$.

Доведення. Оскільки $x^a=a\int\limits_0^x t^{a-1}dt$, то

$$\varphi(x)=\frac{1}{B(a,b)}\cdot\frac{1}{x^a}\int\limits_0^x t^{a-1}(1-t)^{b-1}\,dt=\frac{1}{B(a,b)a}\times\frac{\int\limits_0^x t^{a-1}(1-t)^{b-1}\,dt}{\int\limits_0^x t^{a-1}dt}$$

або ж

$$\varphi(x)=\frac{1}{B(a,b)a}\int\limits_0^x f_1(t)\psi(t)\,dt,$$

де $f_1(t)=\frac{t^{a-1}}{\int\limits_0^x \tau^{a-1}d\tau}$, $\int\limits_0^x f_1(t)\,dt=1$ і $f_2(t)=\frac{t^{a-1}}{\int\limits_0^{x_1}\tau^{a-1}d\tau}<f_1(t)$

$\psi(t)=(1-t)^{b-1}$. Нехай $x<x_1$, і $t\in[0,x]\subset[0,x]$, причому $\int\limits_0^{x_1} f_2(t)\,dt=1$, $\psi'(t)=-(b-1)(1-t)^{b-2}<0$. Звідси, згідно із лемою 1, $x<x_1\Rightarrow\int\limits_0^x f_1(t)\psi(t)\,dt>\int\limits_0^{x_1} f_2(t)\psi(t)\,dt$ або ж $x<x_1\Rightarrow\varphi(x)>\varphi(x_1)$. У такий спосіб лема доведена. Вона встановлює, що неповна β-функція $I_x(a,b)$ зростає за $x\in[0,1]$ повільніше, ніж показникова функція x^a при $a>0$.

Властивість убування функції $\varphi(x)$ по $x\in[0,1]$ має найважливіше значення для виведення таких нерівностей з неповною β-функцією.

Наслідок 1. Справедливе співвідношення:

$$\frac{d}{dx}\ln I_x(a,b)<\frac{a}{x}$$ при $x\in(0,1)$, $a>0$, $b>0$.

Доведення. Оскільки $\frac{d}{dx}\varphi(x)=\frac{d}{dx}\cdot\frac{I_x(a,b)}{x^a}<0$, то $x^aI'_x-ax^{a-1}I_x<0\Leftrightarrow\frac{I'_x}{I_x}=\frac{d}{dx}\ln I_x<\frac{a}{x}$.

Лема 6. Для неповної β-функції $I_x=I_x(a,b)$ виконуються нерівності:

$$I_x(a,b)\geq x^a, \tag{10}$$

$$I^{\frac{1}{t}}_{x^t}(a,b)\leq I_x(a,b)\leq I^t_{\frac{1}{x^t}}(a,b) \text{ при } t\geq 1,\ b\geq 1. \tag{11}$$

Доведення. При $b=1$ функція $I_x(a,1)=x^a$. Оскільки за лемою 2 для неповної β-функції $I_x(a,1)\leq I_x(a,b)$ при $b\geq 1$, то $I_x(a,1)=x^a\Rightarrow I_x(a,b)\geq x^a$.

Розглядаючи функцію $\psi(t)=I^{\frac{1}{t}}(a,b)=I^{\frac{1}{t}}_u$, де $u=x^t$, і використовуючи лему 5, а також наслідок 1, знаходимо:

$$\frac{d}{dt}\ln\psi=\frac{\psi'}{\psi}=\left(\frac{1}{t}\ln I_u\right)'=-\frac{1}{t^2}\ln I_u+\frac{1}{t}\left(\frac{d}{du}\ln I_u\right)u'_t<-\frac{1}{t^2\ln I_u}+\frac{1}{t}\cdot\frac{a}{u}u\ln x=\frac{1}{t^2}\left(-\ln I_u+\ln u^a\right)=-\frac{1}{t^2}\ln\frac{I_u}{u^a}<0$$

,

а звідси – $\psi'=\frac{d}{dt}I^{\frac{1}{t}}_{x^t}<0\Rightarrow I^{\frac{1}{t}}_{x^t}(a,b)\leq I_x(a,b)$, якщо $t\geq 1$. Друга частина нерівності (11) тепер стає очевидною.

$$B(a,b)=\int_0^1 u^{a-1}(1-u)^{b-1}du$$

Лема 7. β-функція при $a>0$ і $b>0$ задовольняє нерівностям:

$$B(a,b)\geq\frac{1}{a(1+a)^{b-1}} \text{ при } b\geq 2 \text{ і } \frac{1}{a^b b}\leq B(a,b)\leq\frac{1}{ab} \text{ при } b>1.$$

Доведення. Після заміни $u=\frac{y}{x}$ при $x\in(0,1)$ отримуємо:

$$B(a,b)=\frac{1}{x^a}\int_0^x y^{a-1}\left(1-\frac{y}{x}\right)^{b-1}dy=\frac{1}{a}\int_0^x f(y)\varphi(y)dy=\frac{1}{a}M\varphi(y)$$

,

де: $f(y)=\frac{ay^{a-1}}{x^a}$, $\int_0^x f(y)dy=1$, $\varphi(y)=\left(1-\frac{y}{x}\right)^{b-1}$ і $M\varphi(y)$ – середнє значення функції $\varphi(y)$.

Для подальшого доведення сформулюємо у виді визначення 1 умови виконання нерівності Ієнсена [9] і наведемо саму нерівність.

Визначення 1. Якщо функція $f(t)$ є безперервною ненегативною функцією на інтервалі $[a,b]$ і для неї $\int_a^b f(t)dt=1$, а функція $g(t)$ опукла на цьому ж інтервалі (і, зокрема, якщо існує $g''(t)\geq 0$ на (a,b)), то справедливою є нерівність Ієнсена:

$$\int_a^b f(t)g(t)dt \geq g(\mu),$$

де $\mu=\int_a^b yf(y)dy$,

Оскільки за умовою леми $b\geq 2$, то $\varphi''(y)\geq 0$ при $y\in[0,x]$, отже виходить, що відповідно до приведеної нерівності Ієнсена середнє значення становитиме:

$$M\varphi(y)\geq\varphi(\mu)=\left(1-\frac{\mu}{x}\right)^{b-1},$$

де $\mu=\int_0^x yf(y)dy=\frac{a}{x^a}\int_0^x y^a dy=\frac{a}{a+1}\cdot\frac{x^{a+1}}{x^a}=\frac{ax}{a+1}$.

Звідси дістаємо першу з нерівностей, які ми доводили:

$$B(a,b)\geq\frac{1}{a}\left(1-\frac{a}{a+1}\right)^{b-1}=\frac{1}{a(1+a)^{b-1}}.$$

Оскільки $B(a,b)=\int_0^1 y^{a-1}(1-y)^{b-1}dy=\int_0^1 g(y)\psi(y)dy$, де $g(y)=y^{a-1}$ при $0\leq g(y)\leq 1$ і $0\leq y\leq 1$, а $\psi(y)=(1-y)^{b-1}$ – ненегативна монотонно убутна функція на інтервалі $[0,1]$ при $b>1$, то у такому випадку можна використовувати нерівність Стефенсена [10]. Сформулюємо у вигляді визначення 2 умови, за яких виконується зазначена нерівність, і приведемо саму нерівність щодо розглядуваних питань.

Визначення 2. Нехай функція $f(t)$ безперервна, ненегативна і монотонно убуває на інтервалі $[a,b]$. Нехай функція $g(t)$ безперервна і задовольняє умовам $0 \le g(t) \le 1$ і $a \le t \le b$. Тоді виконується нерівність Стефенсена:

$$\int_{b-c}^{b} f(t)dt \le \int_{a}^{b} f(t)g(t)dt \le \int_{a}^{a+c} f(t)dt,$$

де $c = \int_{a}^{b} g(t)dt$.

Відповідно до приведеної нерівності Стефенсена у зазначених умовах $\int_{0}^{1} g(y)\psi(y)dy \ge \int_{1-c}^{1} \psi(y)dy = \frac{1}{b}(1-y)^{b}\Big|_{1}^{1-c} = \frac{c^{b}}{b}$, де $c = \int_{0}^{1} g(y)dy = \frac{1}{a}$. Звідси дістаємо, що $B(a,b) \ge \frac{1}{b} \cdot \frac{1}{a^{b}}$.

Для подальшого доведення використовуємо нерівність Чебишева [7], сформульовану у вигляді визначення 3, де також наведемо умови її виконання.

Визначення 3. Якщо функція $f(t)$ безперервна і монотонно зростає на інтервалі $[a,b]$, а функція $g(t)$ безперервна і монотонно убуває на цьому ж інтервалі при $b > a$, то виконується нерівність Чебишева:

$$\int_{a}^{b} f(t)g(t)dt \le \frac{1}{b-a}\int_{a}^{b} f(t)dt \int_{a}^{b} g(t)dt.$$

Тепер, використовуючи визначення 3 і той факт, що функція $f_1(u) = u^{a-1}$ зростає, а функція $f_2(u) = (1-u)^{b-1}$ убуває на інтервалі $[0,1]$, дістаємо:

$$B(a,b) = \int_{0}^{1} f_1(y)\, f_2(y)dy \le \int_{0}^{1} f_1(y)dy \int_{0}^{1} f_2(y)dy$$

або ж $B(a,b) \le \frac{1}{ab}$.

Наслідок 1. Якщо $a = n - r$ і $b = r + 1$, де n і r – цілі ненегативні числа, то $B(a,b) = \frac{\tilde{A}(a)\tilde{A}(b)}{\tilde{A}(a+b)} = \frac{\tilde{A}(n-r)\tilde{A}(r+1)}{\tilde{A}(n+1)} = \frac{(n-r)!r!}{(n-r)n!}$ або $B(a,b) = \frac{1}{\binom{n}{r}(n-r)}$ і, отже, $\binom{n}{r} \le (1+n-r)^{2}$ і $(n-r)(r+1) \le \binom{n}{r} \le \frac{r+1}{n-r}(n-r)^{r+1}$.

Лема 8. Неповна β-функція задовольняє нерівностям:

1). $I_x(a,b) \le (1+a)^{b-1} x^a$, $b \ge 2$;

2). $x^a \le I_x(a,b) \le a^{b-1} b x^a$, $b > 1$;

3). $I_x(a,b) \le \dfrac{(1+a)^{b-1}}{b} x^{a-1}$, $b \ge 2$.

Доведенння. Оскільки $\int_0^x y^{a-1}(1-y)^{b-1} dy \le \int_0^x y^{a-1} dy = \dfrac{1}{a} x^a$, а за лемою 7 виконуються нерівності $\dfrac{1}{B(a,b)} \le a(1+a)^{b-1}$ і $\dfrac{1}{B(a,b)} \le a^b b$, то $I_x(a,b) = \dfrac{1}{B(a,b)} \int_0^x y^{a-1}(1-y)^{b-1} dy \le (1-a)^{b-1} x^a$, $I_x(a,b) \le a^{b-1} b x^a$.

Нерівність $I_x(a,b) \ge x^a$ отримана в лемі 6.

Останнє співвідношення дістаємо з леми 7 і нерівності Чебишева, відповідно до якої

$$I_x(a,b) \le \frac{1}{B(a,b)} \cdot \frac{1}{x} \int_0^x y^{a-1} dy \int_0^x (1-y)^{b-1} dy = \frac{1}{ab \cdot B(a,b)} x^{a-1} \left(1-(1-x)^b\right) \le \frac{(1+a)^{b-1}}{b} x^{a-1}$$

.

Сформулюємо у вигляді леми уже виявлені й отримані нові властивості функції $\varphi(x)$.

Лема 9. Функція $\varphi(x) = \dfrac{I_x(a,b)}{x^a}$ за $x \in (0,1]$, $a > 0$ і $b > 0$ має такі властивості:

1) $x < x_1 \Rightarrow \varphi(x) > \varphi(x_2)$;

2) $1 \le \varphi(x) \le (1+a)^{b-1}$, $b \ge 2$; (12)

3) $1 \le \varphi(x) \le a^{b-1} b$, $b > 1$. (13)

При цілих $a = n - l$ і $b = l + 1$ функція $\varphi(x) = \sum_{k=0}^{l} \binom{n}{k}$, причому

$$1 \le \varphi(x) \le \binom{n}{l} \le \frac{1}{\hat{R}^{n-l} \hat{q}^l}, \quad (14)$$

де $\hat{R} = 1 - \hat{q} = 1 - \dfrac{l}{n}$.

Наведені властивості випливають з лем 4…8. У (14) використана нерівність $\binom{n}{l} \le \frac{n^n}{(n-l)^{n-l} l^l} = \frac{1}{\hat{R}^{n-l}\hat{q}^l}$, відома з [7], а також враховано, що $\sum_{k=0}^{l}\binom{n}{k}x^{l-k}(1-x)^k = \sum_{k=0}^{l} y_k P_k$, $\sum_{k=0}^{l} P_k = 1$, $l > 0$, де $y_k = \frac{\binom{n}{l}}{\binom{l}{k}} \le \binom{n}{l}$, $P_k = \binom{l}{k}x^{l-k}(1-x)^k$.

Таблиця

Властивості неповної β-функції

№	Найменування	Вираз	Вимоги або характеристика
1	Загальний вираз	$I_x(a,b) = \frac{1}{B(a,b)}\int_0^x y^{a-1}(1-y)^{b-1}dy$	$a>0$, $b>0$; Функція $I_x(a,b)$ зростає по $x \in [0,1]$ при $b>0$ й убуває при $a>0$;
2	β-функція	$B(a,b) = \int_0^1 y^{a-1}(1-y)^{b-1}dy$	–
2	Функція біноміального розподілу	$I_x(n-l,l+1) = \sum_{k=0}^{l}\binom{n}{k}x^{n-k}(1-x)^k = B_l(n,x,l)$	$a=n-l$ і $b=l+1$ - цілі числа; x і n - параметри функції біноміального розподілу
3		$I_x(a,b) = 1 - I_{1-x}(b-a) = x^a\varphi(x)$	$1 \le \varphi(x) \le (1+a)^{b-1}$, $b \ge 2$; $1 \le \varphi(x) \le a^{b-1}b$, $b>1$; $x < x_1 \Rightarrow \varphi(x) > \varphi(x_1)$; Якщо $a=n-l$ і $b=l+1$ - цілі числа, то: $1 \le \varphi(x) = \sum_{k=0}^{l}\binom{n}{k}x^{l-k}(1-x)^k \le \frac{1}{\hat{R}^{n-l}\hat{q}^l}$, де $\hat{R} = 1-\hat{q} = 1-\frac{l}{n}$
4		$x \ge y \Rightarrow I_x(a,b) \le \left(\frac{x}{y}\right)^a I_y(a,b)$	
5		$I^{\frac{1}{t}}_{x^t}(a,b) \le I_x(a,b) \le I^t_{\frac{1}{x^t}}(a,b)$	$t \ge 1$
6		$I_x(a,b) \le \frac{(1+a)^{b-1}}{b}x^{a-1}$	$b \ge 2$

Лема 10. Неповна β-функція задовольняє співвідношенню

$$x \ge y \Rightarrow I_x(a,b) \le \left(\frac{x}{y}\right)^a I_y(a,b).$$

Доведення. Відповідно до наслідку 1 леми 5 виконується нерівність $I'_x(a,b) < I_x(a,b)\frac{a}{x}$ при $x \in (0,1)$, $a>0$, $b>0$. Звідси за $0 \le y \le x$, знаходимо, що $\int_y^x I'_t dt \le \int_y^x I_t \frac{a}{t} dt$ або ж $I_x \le I_y + \int_y^x I_t \frac{a}{t} dt$. Далі для доведення використовуємо нерівність Белмана [7, примітка 1]. Сформулюємо у вигляді визначення 4 зазначену нерівність, а також вимоги, за яких вона виконується

Визначення 4. Якщо функції $f(t)$ і $g(t)$ ненегативні при $t \ge t_0$, то для $c \ge 0$ з нерівності $g(t) \le c + \int_{t_0}^t f(\tau) g(\tau) d\tau$ випливає нерівність Белмана:

$$g(t) \le c e^{\int_{t_0}^t g(\tau) d\tau}, \quad t \ge t_0.$$

Тепер, використовуючи визначення 4, дістаємо, що $I_x \le I_y e^{\int_y^x \frac{a}{t} dt} = I_y e^{\ln\left(\frac{x}{y}\right)^a} = I_y \left(\frac{x}{a}\right)^a$, що і доводить лему.

Отримані результати представимо у вигляді таблиці.

Висновок. Отримані результати, наведені у вигляді лем, є математично строгими співвідношеннями і одночасно мають явний аналітичний вигляд. Вони дозволяють дати обґрунтування числа необхідного обсягу випробувань стосовно дослідження живучості захищених інформаційних каналів, а також відкривають шляхи пошуку його скорочення. Це має досить важливе практичне значення, оскільки більша частина коштів при проведенні, наприклад, проектних робіт, витрачається на проведення випробувань.

Наведені теоретичні результати є частиною загальної теорії випробувань, яка включає в себе також теорію планування експерименту та теорію прискорених випробувань. З урахуванням результатів, що є в [1-5], вони можуть бути розширені на багатомірний випадок. У відповідності з отриманими співвідношенями для подальших досліджень встановлено декілька напрямків скорочення числа випробувань. До них в першу чергу відносяться:

– напрямок, що враховує структурну надмірність систем телекомунікацій;

– напрямок, що враховує їхню функціональну надмірність;

– напрямок з врахуванням запасу за ресурсом.

Література

1. 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.

2. Скопа О.О. Біноміальна схема контрольних випробувань резервних систем зв'язку // Зб. науков. праць УДМТУ. – Миколаїв: УДМТУ, 2002. – №7 (385). – С.116-124.

3. Скопа О.О., Головань В.Г. Оцінка надійності систем телекомунікацій з послідовним з'єднанням об'єктів за результатами їх біноміальних іспитів з зупинкою / Наукові записки УНДІЗ. – 2008. – №4(6). – С.75-79.

4. Согіна Н.М., Скопа О.О., Мірошников В.В., Торошанко Я.І. Методика біноміальних випробувань об'єктів одноразового використання // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К: ВІКНУ, 2009. – Вип. №21. – 120-128.

5. Скопа О.О., Волков С.Л., Мінін А.В. Концепція контрольних випробувань резервних систем на основі біноміальної схеми / Інформаційна безпека. – №2(6), 2011. – Луганськ: СНУ ім. В.Даля. – С.69-76.

6. Bateman H. Higher transcendental functions / [Електронний ресурс]: http://ega-math. narod.ru/Books/Bateman1.djv

7. Беккенбах Э., Беллман Р. Неравенства / [Електронний ресурс]: http://reslib.com/card/ Neravenstva__Bekkenbah_E___Bellman_R__Beckenbach_Bellman__

8. Судаков Р.В. К вопросу об интервальном оценивании показателей надежности последовательной системы // Известия АН СССР: Техническая кибернетика. – 1974. – №3.

9. Иенсена неравенство / [Електронний ресурс]: http://dic.academic.ru/dic.nsf/enc_mathematics/1799/%D0%98%D0%95%D0%9D%D0%A1%D0%95%D0%9D%D0%90#sel=1:1,1:2

10. Беккенбах Э., Беллман Р. Неравенства / [Електронний ресурс]: http://www.ega-math. narod.ru/Books/IneqsB.djv

А.В.Минин, А.А.Скопа, Александер М. Биномиальные модели испытания живучести защищенных информационных каналов

Анализируется схема биномиальных испытаний с обобщением новых результатов теоретического и прикладного характера по испытанию живучести защищенных информационных каналов.

Ключевые слова: *биномиальные испытания, живучесть информационных каналов, β-функция.*

A.V.Minin, O.O.Skopa, Aleksander M. Binomial model TEST survivability protected information channels

Analyzed scheme of binomial test of generalization of the results of new theoretical and applied for testing survivability of protected information channels.

Key words: *binomial test, survivability of information channels, β-function.*

Стаття надана16.06.2012

УДК 004.81

Петров А. С., Украинский А.П.

Восточноукраинский национальный университет имени Владимира Даля, г. Луганск

ФОРМАЛИЗАЦИЯ СТРУКТУРЫ СИСТЕМЫ ПРЕДУПРЕЖДЕНИЯ УТЕЧКИ ИНФОРМАЦИИ

В работе предлагается формализация структуры системы предупреждения утечки информации и методика оценки существующих информационных систем на наличие рисков нарушения информационной безопасности.