EVALUAREA ECONOMICĂ A SISTEMELOR DE SECURITATE A INFORMAŢIEI

Rodica BULAI, Daniel MOTREAC

Universitatea Tehnică a Moldovei

Abstract: In this paper is presented the methodology of economical evaluation and its implementation in the software tool, that helps to obtain the reasonable estimates according with the mode of justification the investments for some means of protection and identification the key priorities of budget costs for the information security.

Cuvinte cheie: *sistemelor de securitate a informaţiei (SSI), evaluarea economică, coeficientul ROI, rentabilitatea investiţiilor.*

1. Introducere

Practica funcţionării sistemelor de securitate a informaţiei (SSI) denotă faptul că asigurarea nivelului de ptotecţie până la 100% este o măsură costisitoare şi, în unele cazuri, iraţională:

- chiar cel mai perfect sistem de securitate informaţională existent la moment, nu va putea face faţă ameninţărilor ce pot apărea pe viitor;
- sinecostul protecţiei complexe poate deveni mai mare de cît costul sistemelor informaţionale protejate.

Managementul securităţii informaţiei, necesită adoptarea periodică a diverselor decizii, care se incheie, de regulă, prin selectarea unor opţiuni (una dintre schemele posibile organizaţionale, una dintre opţiunile tehnice disponibile) sau determinarea anumitor parametri individuali organizatorici şi/sau tehnici pentru sistem sau subsisteme. O posibilă abordare pentru selectarea deciziilor de management este "voinţa" de abordare, cînd decizia, din unele sau altele motive, se ia intuitiv şi în mod formal legătura cauza-efect între anumite premise şi decizii specifice nu poate fi stabilită. În mod evident, alternativa la "voinţa" de abordare este luarea de decizii bazate pe proceduri formale şi anumite analize secvenţiale.

Baza acestei analize şi, ulterior, de luare a deciziilor este analiza economică, care implică studiul tuturor factorilor (sau cel puţin a celor de bază): modelele de comportament, dinamica schimbărilor, utilizarea unei valori monetare universale etc., sub influienţa cărora are loc dezvoltarea sistemelor analizate. Anume în baza modelelor economice trebuiesc luate deciziile, care cuprind atît măsurile organizatorice, cât şi cele tehnice privind strategia generală sau individuală de dezvoltare.

Economia în orice activitate are propriile caracteristici, de aceea, economia în domeiul securităţii informaţiei (SI), pe de o parte, se bazează pe anumite legi economice generale şi metode de analiză, iar pe de altă parte - are nevoie de un sens individual, dezvoltarea unor măsuri de analiză specifice acestui domeniu.

O dificultate deosebită a analizei economice în SI, este determinată de factorii specifici, cum ar fi:

a) dezvoltarea rapidă a tehnologiilor informaţionale, în special mijloacele şi metodele de atac, precum şi a celor de protecţie;

b) incapacitatea de a prezice corect toate scenariile posibile de atacuri împotriva sistemelor informaţionale;

c) imposibilitatea de a furniza estimări fiabile, de a da o notă cît mai reală a costului resurselor informaţionale, precum şi de a evalua efectele diferitelor perturbări în termeni monetari, ce ţine de cheltuieli.

Acest lucru necesită eforturi suplimentare pentru a organiza procesul de analiză economică, şi de multe ori poate duce la faptul că multe decizii privind securitatea informaţiei pot fi inadecvate. Situaţii în care lipsa unei metodologii de analiză economică are un efect negativ asupra securităţii, ar putea fi cînd:

a) administraţia companiei poate lua decizii neadecvate cu privire la investiţiile în SI, care, la rândul lor, pot duce la pierderi care ar fi putut fi evitate;

b) administraţia companiei poate lua anumite decizii în ceea ce priveşte organizarea proceselor de afaceri şi prelucrarea informaţiilor în cadrul întreprinderii, cu scopul de a reduce cheltuielile curente şi de a reduce supraîncarcarea personalului, fără a lua în considerare consecinţele economice posibile ale lipsei unui SSI.

2. Metodologia de evaluare economică a securităţii informaţiei

În calitate de indicator principal de măsurare a costurilor (cheltuielilor), în practica economică este coeficientul *ROI (Return on Investment).*

$$ROI = I(R,d) + I(C,d) \quad (1)$$

unde:

R - veniturile suplimentare, generate de schimbări, condiţionate de investiţiile în SI;

C – cheltuielile, condiţionate de investiţiile în SI;

d - rata de actualizare, permite de a lua în considerare cheltuielile pe parcursul modificărilor survenite, atît cumulativ, cît şi pentru fiecare actualizare;

I – funcţia de actualizare, cheltuielile făcute în SI într-o perioada anumită de timp (de obicei perioada de timp se începe la începutul punerii în aplicare a proiectului).

Altfel coeficientul ROI poate fi determinat în modul următor (2):

$$ROI = \frac{\Delta R - \Delta C}{\Delta I} \quad (2)$$

Coeficientul *ROI*, formula (1), demonstrează sarcinile de bază care urmează să fie rezolvate în analiza oricărui proiect de investiţii din domeniul SI: calcularea cheltuielilor asociate şi veniturile suplimentare.

Una dintre metodele cele mai promiţătoare pentru calculul indicelui *ROI* este tehnica care se bazează pe evaluarea cantitativă a riscurilor informaţionale şi pe evaluarea atenuării acestor riscuri. Algoritmul de analiză a eficienţei investiţiilor asupra sistemelor de securitate a informaţiei este reprezentată în figura 1.

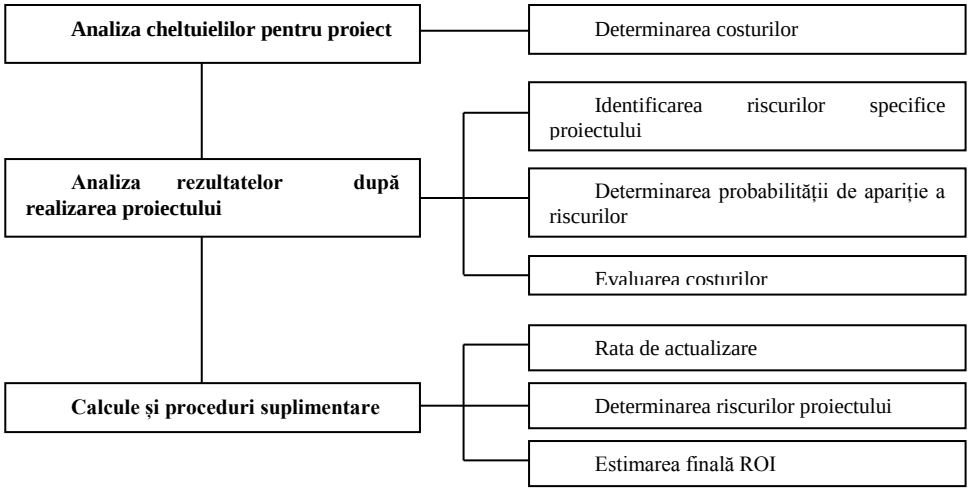


Figura 1. Metodologia de analiză a eficienţei investiţiilor (ROI) în SSI

Analiza costurilor pentru proiecte în domeniul SI poate fi efectuată pe baza metodologiei Total Cost of Ownership - TCO (Costul Total de Proprietate), introdusă de compania Gartner Group în 1987. Această metodă se orientează pe analiza costurilor (atît directe, cît şi indirecte), asociate cu tehnologiile şi sistemele informaţionale, în situaţiile în care este necesar să se evalueze efectele economice ale introducerii şi utilizării unor astfel de sisteme: evaluarea investiţiilor, compararea cu tehnologiile alternative, elaborarea bugetelor totale şi curente, etc.

Valoarea totală a TCO include:

a) cheltuieli de proiectare a unui sistem de informţional;
b) cheltuieli de achiziţie de hardware şi software (inclusiv metodele utilizate de licenţiere), precum şi plăţile de leasing;
c) cheltuieli de dezvoltare software şi documentaţie, de testare şi de identificare a erorilor, de modificare în timpul perioadei de funcţionare;
d) cheltuieli pentru administrarea sistemelor informaţionale;
e) cheltuieli pentru suport tehnic şi alte servicii;
f) cheltuieli materiale;
g) costul serviciilor de telecomunicaţii (acces la Internet, dedicat şi canale dial-up, etc);
h) cheltuieli pentru instruirea utilizatorilor, specialiştilor TI, SI;
i) cheltuieli indirecte - cheltuieli ale întreprinderii, legate de apariţia unor defecţiuni în sistemele informaţionale.

De asemenea, estimarea costurilor de îmbunătăţire şi corectare a SSI ar trebui să includă costurile de reorganizare a proceselor de afaceri şi de informare a personalului: plata serviciilor de bussines-consultanţă şi consultanţiile pentru SI, cheltuieli de perfectare a documentelor organizatorice, cheltuieli pentru efectuarea auditului asupra stării SI etc. În plus, analiza cheltuielilor ar trebui să prevadă şi faptul că, punerea în aplicare a metodelor de protecţie implică apariţia responsabilităţilor şi activităţilor suplimentare pentru personalul sistemului informaţional, care, în consecinţă, pot duce la cheltuieli suplimentare.

Valoarea TCO pentru fiecare caz, trebuie să fie determinată individual, luând în considerare particularităţile proiectului: funcţionalităţile necesare, infrastructura existentă, numărul de utilizatori etc. Pentru analiza eficienţei şi opotunităţilor unui SSI, TCO se defineşte ca suma tuturor cheltuielilor, ajustate cu factorului de timp (3):

Error! Objects cannot be created from editing field codes. (3)

unde:

T - ciclul de viaţă al proiectului (SSI); *n* - valoarea chieltuielilor luate în considerare; C_{nt} - cheltuielile *n* suportate în perioada *t*, lei.

Cu toate acestea, cea mai mare dificultate o constituie definirea efectelor pozitive odata cu introducerea unui SSI. Ca regula, avantajele de la introducerea sistemelor informaţionale (ERP-sisteme, sisteme de contabilitate, CAD/CAM sisteme etc.) se determină prin faptul că ele oferă automatizarea şi accelerarea diferitor procese, economisindu-se costul forţei de muncă, timpul şi îmbunătăţindu-se eficienţa generală a afacerii. Punerea în aplicare a unui SSI în sine, ca regulă, nu oferă economii de cost (deşi, în unele cazuri, poate oferi). Atingerea unui rezultat pozitiv depinde de factori greu de controlat, atît din cadrul întreprinderii, cît şi din exteriorul ei. Mai mult decât atât, implementarea soluţiilor de securitate poate provoca stres şi activităţi suplimentare asupra personalului, iar în consecinţă, la o reducere a productivităţii.

În acest sens, una din puţinele metode care ar putea ajuta compania pentru a determina eficienţa unui SSI, este valoarea monetară (cel puţin aproximativă) a daunei care poate surveni asupra resurselor informaţionale şi care pot fi prevenite, ca urmare a soluţiilor identificate. Astfel, prejudiciul ce trebuie neutralizat va constitui o parte din veniturile suplimentare aduse, în urma utilizării SSI.

În mod evident, calculele în această abordare pot fi estimate doar aproximativ. Aceasta se datorează faptului că activitatea intruşilor, este sursa de ameninţări a SI, practic imprevizibile: nefiind posibilitatea de a prezice strategia de atacare, aptitudinea atacului, intenţiile şi resursele concrete (financiare, tehnice, organizatorice), care vor fi utilizate pentru a fi efectuate anumite acţiuni şi intenţiile cu privire la informaţiile furate (dacă ţinta atacului ar fi furtul de informaţii confidenţiale). În consecinţă, pentru punerea în aplicare a tuturor calculelor necesare trebuie de făcut o serie de ipoteze şi evaluari în cadrul unei organizaţii anumite, precum şi după posibilitate de a studia informaţia statistică a atacurilor asupra resurselor informaţionale.

Astfel, evaluarea economică a eficienţei măsurilor de protecţie a informaţiilor include:

a) evaluarea ameninţărilor existente la adresa activelor informaţionale, ceea ce va afecta punerea în aplicare a măsurilor de protecţie;

b) evaluarea probabilităţii realizării fiecărei dintre ameninţările identificate;

c) evaluarea economică a urmărilor atacului informaţional.

Pentru a pune în aplicare o astfel de analiză se folosesc de obicei următoarele concepte de bază:

a) Valoarea estimată a pierderilor concomitente (Single Loss Expectancy, SLE_i) - suma medie estimată a prejudiciului ce rezultă dintr-un atac informaţional de tip *i*. Acesta poate fi definită ca produsul dintre valoarea totală a activelor protejate (*AV*) şi un factor de eşec din cauza unor încălcări ale SI (vulnerabilitatea la atacuri), care se notează cu EF_i (factorul de expunere sau Exposure Factor);

b) Numărul anual de încălcări a securităţii informaţionale (numarul anual de apariţie, Annualized Rate of Occurrence, ARO_i) - frecvenţa estimată a apariţiei în timpul anului a atacurilor informaţionale de tip *i*;

c) Valoarea estimată a pierderilor medii anuale (Annualized Loss Expectancy, ALE_i) - suma totală a pierderilor în urma atacurilor informaţionale (riscuri de implementare) de tip *i* timp de un an (4).

$$ALE_i = SLE_i \times ARO_i = (AV \times EF_i) \times ARO_i \quad (4)$$

Efectul imediat al punerii în aplicare a măsurilor de îmbunătăţire a nivelului de securitate va fi manifestat prin:

a) Impactul negativ al fiecărei încălcări (fiecare din ameninţările realizate) după finalizarea activităţilor (EF_i) va fi mai mic decât a fost înainte de punerea lor în aplicare: $EF_i \rangle EF_i^{/}$;

b) Frecvenţa de încălcare a SI se va reduce după punerea în aplicare a mijloacelor de securitate **Error! Objects cannot be created from editing field codes.**.

În rezultat, micşorarea valorii $ALE^{/}_i$ va fi (5):

$$ALE_i^{/} = SLE_i \times ARO_i = (AV_i \times EF_i^{/}) \times ARO_i^{/} \quad (5)$$

Astfel, suma anuală a veniturilor suplimentare, condiţionate de investiţiile în SI va constitui (6):

$$R = \Delta ALE_i = ALE_i - ALE_i^{/} \quad (6)$$

Reieşind din formulele de mai sus, rezultă că venitul obţinut din urma neutralizării atacului se va calcula după formula (7):

$$I(R,d) = \sum_{t=0}^{T} \frac{\sum_{i=1}^{I} ALE_{it} - ALE_{it}^{/}}{(1+d)^t} \quad (7)$$

3. Sistemul de evaluare economică a securităţii informaţiei

Pe baza metodologiei descrise, s-a proiectat un instrument software (figura 2) care ne ajută să obţinem estimări rezonabile cu privire la modul în care investiţiile sunt justificate pentru anumite mijloace de protecţie, şi de a identifica priorităţile-cheie ale cheltuielilor din buget pentru SI (în cazul în care organizaţia deţine sume fixe pentru aceste scopuri).

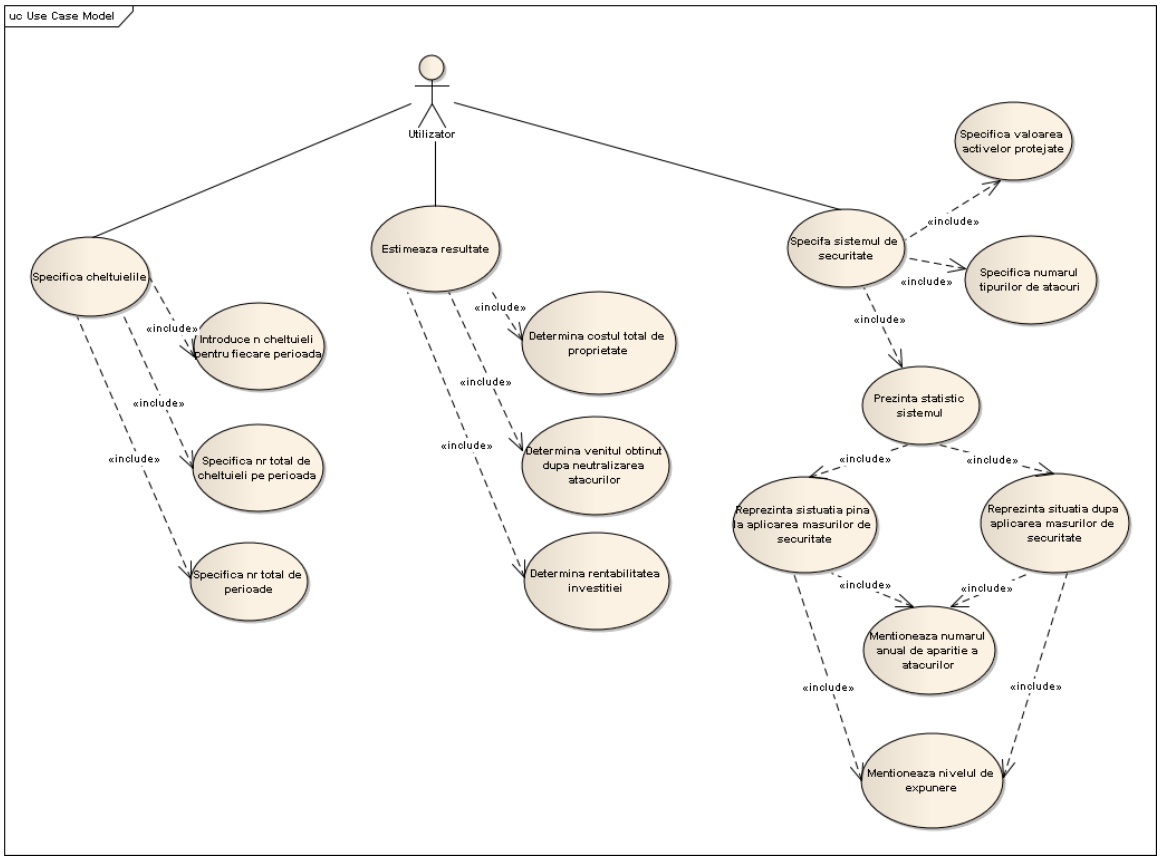
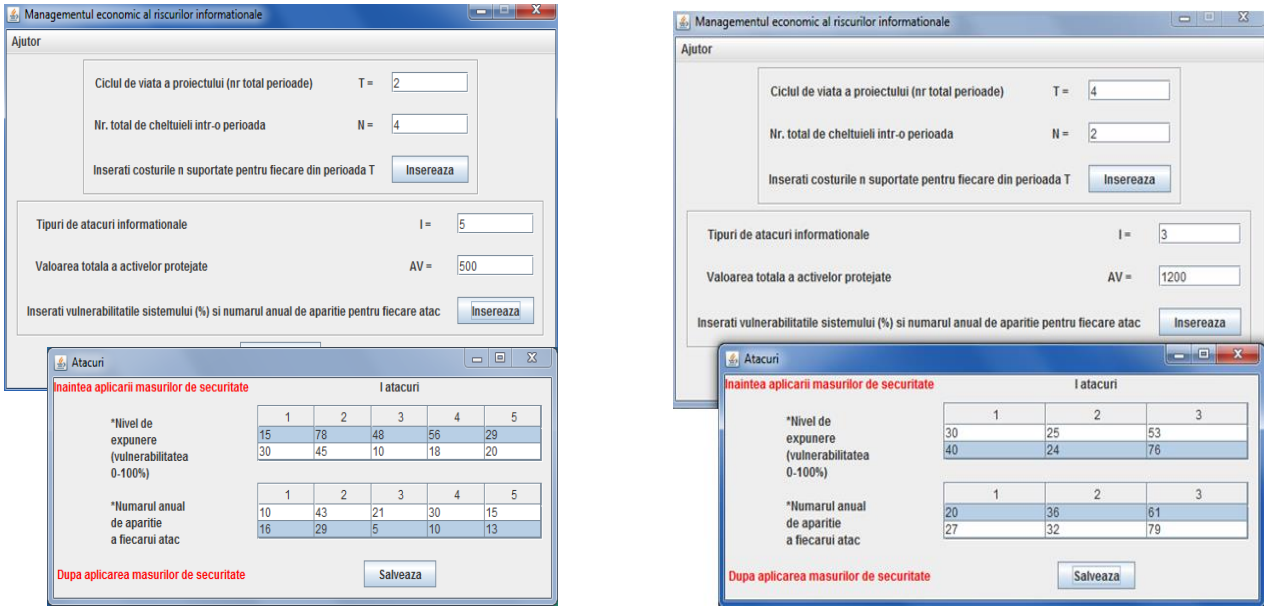


Figura 2. Rentabilitatea investiţiei în Sistemul de securitate a informaţiei

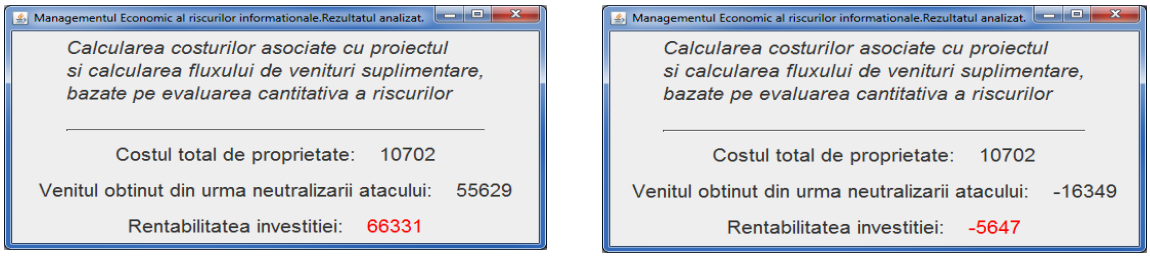
Pentru a demonstra corectitudinea algoritmului implementat, vom considera experimental, două situaţii, una în care SSI asigura o mai mare protecţie după aplicarea noilor măsuri de securitate, figura 3.a), şi a doua, în care SSI asigura o mai mare protectie pina la aplicarea noilor masuri de securitate, figura 3.b).



a) b)

Figura 3. a) SSI asigura o mai mare protecţie după aplicarea noilor măsuri de securitate,
b) SSI asigura o mai mare protectie pina la aplicarea noilor masuri de securitate

Consideraţia experimentală demonstează faptul că, în cazul al doilea, au fost introduse unele masuri de securitate ineficiente, ce au dus la cresterea vulnerabilităţii, şi respectiv, au determinat un venit negativ.



a) b)

Figura 4 a) SSI eficient b) SSI ineficient

4. Concluzii

Managerii responsabili pentru securitatea informaţiei trebuie să analizeze în mod constant schimbările survenite şi să adapteze activitatea lor la situaţia de continuă schimbare. Modalităţile specifice în care se manifestă reacţia liderilor pot fi diferite. Acest lucru poate fi o schimbare a strategiei de marketing, reorganizarea procesului de afaceri, schimbarea tehnologiilor, modificarea produsului fabricat etc. Însă în pofida mediului schimbător, aproape pe toţi îi uneşte un element metodologic comun: reacţia bussines-ului la noile ameninţări şi oportunităţi, care necesită, pe de o parte, noi investiţii - cheltuieli, iar pe de altă parte, oferă posibilitatea de a obţine noi avantaje, prin prevenirea pierderilor, creşterea veniturilor sau reducerea anumitor costuri curente de exploatare.

Complexitatea problemelor de analiză economică, în aproape toate domeniile, este cauzată de faptul că mulţi dintre parametrii cheie a modelelor economice nu pot fi estimaţi exact, având un caracter probabilistic. Astfel, pentru a asigura fiabilitatea maximă a estimărilor în analiza economică şi de luare a deciziilor este necesar să se organizeze colectarea informaţiilor de bază, valorilor predictive, prelucrarea tuturor datelor. În procesul de analiză a acestor decizii de asemenea ar trebui de luat în considerare deciziile intermediare referitoare la estimările diferitor parametri ai modelului. Trebuie de luat în considerare şi faptul că o astfel de analiză poate fi o procedură costisitoare şi necesită o expertiză suplimentară, consultanţi externi, precum şi eforturi depuse de diverşi specialişti (experţi), care lucrează la însuşi întreprindere - toate aceste costuri, într-un final, trebuind să fie justificate.

Deşi din punct de vedere matematic, toate calculele conform coeficientului *ROI* par extrem de simple, definirea parametrilor individuali (prezicerea frecvenţei de încălcări şi dimensiunea pierderilor, precum şi ciclul de viaţa a software-lui, hardware-lui şi modelele organizaţionale) poate cauza dificultăţi semnificative în practică.

Bibliografie

1. CERT podcast: Security for business leader, *The ROI of security*: http://www.cert.org/podcast/notes/2roi.html

2. ISACA - IS Auditing Guideline: G41 *Return on Security Investment (ROSI)* , 2010: http://www.isaca.org/Knowledge-Center/Standards/Documents/G41-ROSI-5Feb10.pdf

3. Christian Locher, *Methodologies for evaluating information security investments*, 2005: http://csrc.lse.ac.uk/asp/aspecis/20050136.pdf

4. *Return on Security Investment (ROSI): A Practical Quantitative Model:* http://www.ra.cs.uni-tuebingen.de/lehre/uebungen/ss09/introsec/ROSIPractical_Model.pdf

5. Маслова, Н., *Методы оценки эффективности систем.* г. Донецк, Украина: Донецкий национальный технический университет, 2008.

6. Анисимов, А., *Методические основы экономики информационной безопасности*, Университет Информационных Технологий, 2006: http://www.intuit.ru/department/itmngt/manofis/14/

7. Домарев В.В., *Моделирование процессов создания и оценки эффективности систем защиты информации,* 2004: http://citforum.ru/security/articles/model_proc/