Economie teoretică şi aplicată
Volumul XVII (2010), No. 1(542), pp. 49-68

Costul securităţii informatice în lucrul cu aplicaţii distribuite

Ion IVAN
Academia de Studii Economice, Bucureşti
ionivan@ase.ro
Dragoş PALAGHIŢĂ
Academia de Studii Economice, Bucureşti
mail@dragospalaghita.ro

Rezumat. *Se prezintă obiectivul, necesitatea, mijloacele şi eficienţa estimată a modelării costului securităţii informatice. Sunt descrise caracteristicile structurale ale aplicaţiilor informatice distribuite şi efectele asupra complexităţii. Se stabilesc cerinţele de securitate ale aplicaţiilor informatice distribuite şi se identifică aspecte implicate de planificarea, realizarea şi implementarea securităţii informatice. Se prezintă factori de influenţă pentru securitatea informatică şi se analizează corelaţiile dintre factorii cei mai importanţi. Se analizează costurile asociate proceselor de securitate. Se definesc modele de costuri pentru securitatea informatică. Se calculează complexitatea modelelor. Se identifică criterii de optim în securitatea informatică. Se prezintă modalităţi de optimizare bicriterială. Se analizează costul securităţii informatice şi se prezintă modele de securitate informatică în aplicaţia de validare identificatori organizaţie. Concluziile evidenţiază calitatea rezultatelor cercetării şi oferă deschiderea pentru cercetări viitoare.*

Cuvinte-cheie: securitate; costuri; modele; analiză; previziune; eficienţă.

Cod JEL: C63.
Cod REL: 10J.

1. Introducere

Obiectivul vizat este construirea de modele pentru estimarea costului subsistemeleor de securitate informatică din aplicaţiile informatice distribuite.

Necesitatea este data de:

- creşterea complexităţii aplicaţiilor informatice (Pendharkar et al., 2008, pp. 1181-1188) care determină măsuri în exploatarea bazelor de date, în utilizarea programelor executabile şi în utilizarea site-urilor web;
- creşterea numărului de utilizatori şi a diversităţii acestora conform (Khansa, Liginlal, 2009, pp. 216-235) care generează măsuri în accesarea resurselor aplicaţiei informatice;
- administrarea bazelor de date care generează măsuri de actualizare, realocare, restructurare;
- dezvoltarea E-commerce ce implica un volum foarte mare de informaţii transmise ce impune măsuri(1) în scopul păstrării confidenţialităţii, integrităţii şi disponibilităţii informaţiilor;
- trecerea la noua economie ce generează virtualizarea proceselor de afaceri având ca urmare creşterea fluxurilor de date transferate online şi schimbarea caracterului bunurilor deţinute de organizaţii de la bunuri materiale la bunuri virtuale, determinând măsuri în protejarea bunurilor şi fluxurilor-cheie de informaţii din cadrul organizaţiei (Huang, Hu, 2008, pp. 793-804);
- dezvoltarea accelerată a tehnologiilor folosite pentru elaborarea produselor software ce implică soluţii de securitate mai complexe, ce trebuie să protejeze o gamă largă de bunuri şi tranzacţii.

În acest scop:

- se iau aplicaţii informatice distribuite de comerţ electronic, de plăţi, de management resurse întreprindere, de gestiune stocuri;
- se culeg date legate de comportament, costurile de întreţinere, de depanare, mentenanţă şi de restructurare conţinut (Kumar et al., 2008, pp. 1853-1867);
- se fac serii de date privind comportamentul aplicaţiei, comportamentul utilizatorilor, nivelul de validare existent şi de potenţiale riscuri de securitate (Anwar et al., 2009, pp. 13-25, Lu et al., 2009, pp. 4617-4625, Aroba et al., 2008, pp. 1944-1950);
- se identifică factori direcţi şi indirecţi de influenţă a cheltuielilor;
- se construiesc structuri de modele de costuri bazate pe diferiţi factori de influenţă (Lee, Kim, 2009, pp. 453-475);
- folosind diferite metode se estimează coeficienţii modelelor;
- se validează modelele utilizând metodologii specifice (Jasmine, Vasantha, 2008, pp. 951-954);
- se rafinează modelele folosind metode cantitative şi algoritmi genetici (Ivan et al., 2008, Vişoiu, 2009, pp. 861-866).

Pentru a realiza o abordare graduală se procedează la studierea modelelor de costuri din software existent în literatura de specialitate. Se orientează detalierea spre securitatea informatică şi se analizează implicarea acesteia în creşterea cheltuielilor de dezvoltare software, concomitent cu scăderea cheltuielilor din exploatarea curentă a aplicațiilor.

Se identifică factori de influență în vederea creşterii nivelului de securitate, se analizează vulnerabilitățile şi se construiesc modele liniare şi neliniare, după care se trece la realizarea de construcții orientate pe optimizare şi, în final, se validează toate modelele folosind date obținute din exploatarea aplicației distribuite pentru validarea elementelor de identificare pentru organizații.

Pentru a realiza acest demers se utilizează resurse puse la dispoziție prin contractul nr. 41/ASE în cadrul Şcolii Doctorale din Academia de Studii Economice Bucureşti.

2. Stadiul cercetării în domeniu

În lucrările în domenii (Vacca, 2009 [VACC09], Tipton, Krause [TIKR08], 2008, Stamp, 2005 [STAM05], Pfleeger, Pfleeger, 2006 [PFLE06]) se prezintă concepte de bază ale securității informatice pe baza cărora se prezintă aria de acoperire a subiectelor de securitate informatice conform tabelului următor:

Tabelul 1

Aria de acoperire a literaturii de specialitate

Cuprins	[VACC09]	[TIKR08]	[STAM05]	[PFLE06]
Criptografie	X	X	X	X
Securitatea aplicațiilor		X	X	X
Securitatea rețelelor	X	X	X	X
Securitatea Internet	X	X		
Securitatea bazelor de date				X
Securitatea Sistemelor de operare	X		X	X
Securitatea fizică	X	X		X
Arhitecturi de securitate		X		
Analiza riscului	X	X		X
Managementul riscului	X	X		
Managementul securității	X			X
Controlul accesului	X	X	X	X
Protocoale de securitate	X	X	X	X
Insecuritatea software			X	
Economia securității				X
Confidențialitatea informațiilor	X	X	X	X
Aspecte legale ale securității informatice		X		X

Există reviste de specialitate în domeniul securităţii informatice:

- Computers & Security, ISSN: 0167-4048, publicată de Elsevier Advanced Technology;
- International Journal of Information Security, ISSN: 1615-5270, publicată de Springer New York;
- Journal of Cryptology, ISSN: 1432-1378, publicată de Springer New York;
- IEEE Transactions on Information Forensics and Security ISSN: 1556-6013, publicată de IEEE;
- Cryptologia, ISSN: 1558-1586, publicată de Taylor & Francis;
- IET Information Security, ISSN**:** 1751-8709, publicată de Institution of Engineering and Technology;
- ACM Transactions on Information and System Security, ISSN: 1094-9224, publicată de ACM
- Security and Privacy, ISSN**:** 1540-7993, publicată de IEEE;
- *IEEE Transactions on Dependable and Secure Computing,* ISSN 1545-5971, publicată de IEEE.

Există conferinţe de securitate informatică:

- IEEE Intelligence and Security Informatics, ce a conţinut în ediţia 2009 secţiuni ce făceau referire la distribuirea informaţiei şi data mining, protejarea infrastructurii şi răspunsul de urgenţă, informatică în contextul terorismului,
- IEEE Symposium on Security and Privacy a conţinut în ediţia 2009 sesiuni ce făceau referire la metode de atac şi apărare, securitatea informatică, cod rău intenţionat, pierderi informaţionale, confidenţialitate, baze formale, securitatea reţelei, securitate fizică şi securitate web;
- ACM Conference on Computer and Communications Security în cadrul ediţiei din 2009 conţine elemente de securitate informatică bazată pe comportament, tehnici de asigurare a securităţii informatice, proiectarea de sisteme sigure, confidenţialitate, securitatea serviciilor mobile, criptografie aplicată, atacuri informatice şi securitatea sistemelor;
- USENIX Security Symposium include subiecte precum autentificare şi autorizare, metode autonome, grid computing, aspect de securitate asociate email-ului, protecţie împotriva viruşilor, tehnologii şi proceduri de securitate şi răspunsuri la atacuri cibernetice;
- Computer Security Foundations Symposium ce include secţiuni precum proiectarea protocoalelor, securitate web, autorizarea sesiunilor, verificarea sesiunilor şi analiză de securitate a programelor;
- Network and Distributed System Security Symposium ce include discuţii legate de pericolele web, criptografie şi confidenţialitate şi integritate.

Revistele şi conferinţele enumerate acoperă o gamă variată de probleme de actualitate în domeniul securităţii informatice, oferind o imagine de ansamblu a stadiului cercetării în acest domeniu.

3. Securitatea informatică

Informația este definită[2] ca nişte fapte şi idei care sunt reprezentate sau codificate ca diferite forme de date.

Securitatea este reprezentată[2] de măsurile luate pentru a proteja un sistem. Securitatea este considerată, de asemenea, ca o condiție a unui sistem care rezultă din instituirea şi menținerea unor măsuri pentru a proteja bunurile. Securitatea impune ca resursele unui sistem să nu fie supuse accesului neautorizat, schimbărilor neautorizate sau accidentale, distrugerea sau pierderea bunurilor protejate (Vydrin, 2009, pp. 261-275).

Securitatea informațiilor se poate defini[3] ca protecția informațiilor şi a sistemelor informatice de acces neautorizat, utilizarea, divulgarea, tulburarea, modificarea sau de distrugere în scopul de a asigura:

- *integritatea*[3] ca paza împotriva modificărilor de informații incorecte sau distrugere, şi include asigurarea nonrepudiere şi autenticitatea informațiilor.
- *autenticitatea*[3] este necesară pentru a asigura că datele, informațiile sau tranzacțiile sunt originale; nonrepudierea[4] implică faptul că nimeni nu poate nega primirea sau emiterea unei tranzacții; autenticitatea şi nonrepudierea sunt aplicate în domeniul comerțului electronic prin utilizarea de semnături digitale[3].
- *confidențialitatea*[4] înseamnă păstrarea de restricții autorizate privind accesul şi publicarea, inclusiv prin mijloace pentru protejarea vieții private şi de proprietate de informații cu caracter personal
- *disponibilitatea*[3] este reprezentată de asigurarea de acces în timp util şi de încredere la informații.

În lucrările citate (Vacca, 2009, Tipton, 2008) securitatea informatică abordează probleme ce urmăresc:

- riscul de securitate informatică, analizând concepte generale legate de risc, vulnerabilități şi amenințări (Alhazmi, Malaiya, 2008, pp. 14-22);
- controlul accesului expunând diferite modalități de autentificare şi procesele necesare utilizării lor; se analizează vulnerabilitățile sistemelor de control al accesului luând în considerare principalele tipuri de atacuri cărora sunt expuse (Chen, Ji, 2009, pp. 530-541);
- aspecte criptografice ale sistemelor de securitate urmărind managementul cheilor de criptare în rețea; identifică cele mai eficiente metode de criptare şi se descriu algoritmii folosiți; sunt prezentate avantaje şi dezavantaje ale utilizării diferitelor metode de criptare;
- securitatea aplicațiilor prin detalierea celor mai noi metode de securizare şi creştere a calității produselor program;
- securitatea Internet prin descrierea vulnerabilităților implicate de mediul online;
- securitatea în rețea prin identificarea vulnerabilităților protocoalelor de transfer şi analiza amenințărilor prezente în comunicarea în rețea;

- securitatea reţelelor fără fir, prezentând aspecte legate de vulnerabilităţi, ameninţări şi politici de securitate recomandate în acest caz;
- securitatea reţelelor celulare, detaliind aspecte legate de securizarea în contextul transmisiunilor radio, modalităţile de atac al reţelelor radio şi modalităţi de blocare a atacurilor în cadrul reţelelor celulare;
- căi de creştere a nivelului de securitate prin îmbunătăţirea calităţii codului sursă, prin identificarea şi eliminarea vulnerabilităţilor fizice ale sistemului, prin instruirea utilizatorilor, prin creşterea calităţii sistemelor de control al accesului, prin îmbunătăţirea sistemelor de management al parolelor, prin creşterea calităţii politicilor de securitate şi diferenţierea clară a rolurilor utilizatorilor, prin dezvoltarea unui sistem de caracteristici de calitate asociat sistemului de securitate şi procedarea la creşterea nivelului lor individual pentru a obţine o creştere globală a calităţii sistemului de securitate utilizat;
- aspecte de management ale securităţii informatice detaliind concret principalele componente ale unui sistem de management al securităţii informatice; prezentând aspecte legate de sistemele de prevenţie a intruziei şi sunt descrise pe larg tehnici de identificare a vulnerabilităţilor;
- identificarea aspectelor legale ale securităţii informatice prin studierea legilor şi regulilor impuse la nivel global pentru bune practici în acest domeniu.

În cadrul sistemelor de securitate informatică calitatea are un rol important, fiind un factor de influenţă major în buna funcţionare a aplicaţiei informatice. Caracteristicile de calitate sunt ierarhizate la nivel de:

- text sursă prin:
  - omogenitate, care este reprezentată de natura textului sursă de a avea aceleaşi caracteristici şi proprietăţi în toate modulele sistemului de securitate; se urmăreşte utilizarea de operatori şi operanzi în moduri similare, cât şi utilizarea aceleiaşi formatări în cadrul modulelor sistemului;
  - inteligibilitate, ce se concretizează prin însuşirea textului sursă de a fi perceput cu uşurinţă de dezvoltatorii software chiar dacă nu au avut experienţe anterioare cu sistemul de securitate; inteligibilitatea textelor sursă în cadrul sistemelor de securitate este utilă prin economia de resurse dată de înţelegerea rapidă a logicii implementate în sistem de către dezvoltatori şi realizarea modificărilor necesare utilizând resurse limitate;
  - testabilitate, ce reprezintă capacitatea textului sursă de a fi supus procesului de testare cât mai uşor, cuprinzând toate căile logice posibile; un nivel ridicat al testabilităţii în cadrul sistemelor de securitate informatică asigură minimizare numărului de defecte şi omisiuni ale sistemului îmbunătăţind astfel nivelul global de calitate al sistemului; testabilitatea se asigură prin dezvoltarea omogenă a sistemului de securitate şi prin utilizarea logică a raportării interne pentru toate operaţiile făcute şi toate evenimentele apărute în sistem;

- mentenabilitate printr-un nivel ridicat al căreia se minimizează costurile asociate procesului de depanare şi îmbunătățire al aplicației; această caracteristică este în legătură strânsă cu omogenitatea şi inteligibilitatea textelor sursă;
- veridicitatea tipurilor de date, astfel urmărind eliminarea cazurilor de suprascriere a memoriei ce duce la coruperea sistemului de securitate; se urmăreşte stabilirea de limite inferioare şi superioare pentru tipurile de date utilizate şi impunerea lor ca standarde înainte de prelucrarea lor de către aplicația informatică;
- percepție a erorilor, caracteristică concretizată de nivelul în care sistemul de securitate raportează erorile şi le interpretează corect; un nivel ridicat de percepție a erorilor în cadrul sistemului de securitate reduce costurile legate de restaurarea aplicației informatice, plata de despăgubiri şi costul reingineriei sistemului de securitate informatică;
- secretizarea frazelor de acces este un aspect important în cadrul sistemului de securitate informatică nefiind recomandată utilizarea lor direct în codul sursă sub formă hard-codată;

▪ interacțiune cu aplicația informatică:
- compatibilitate, reprezentând utilizare de protocoale de comunicare comune, menținând astfel comunicarea între cele două entități în cele mai bune condiții;
- coexistență, concretizată în abilitatea sistemului de securitate de a funcționa la parametrii optimi în cadrul aplicației informatice; un grad ridicat al coexistenței ajută la creşterea gradului de fiabilitate al aplicației informatice şi la minimizare costurilor de mentenanță asociate sistemului de securitate;
- acuratețe, ce este reprezentată de exactitatea cu care sunt percepute semnalele emise de către aplicația informatică;
- securizarea informațiilor, care se concretizează prin abilitatea sistemului de securitate de a proteja şi a asigura confidențialitatea datelor utilizate şi procesate în cadrul aplicației informatice.

▪ interacțiune cu utilizatorul urmărind:
- siguranța transferurilor de informații în cadrul aplicației informatice prin implementarea de sisteme de autentificare şi autorizare eficiente asigurând astfel identificarea corectă a utilizatorilor, minimizând cazurile de furt al identității şi costurile cu:
  - repunerea în funcțiune a sistemului de securitate şi al aplicației informatice;
  - evaluarea daunelor provocate de intruziunea neautorizată în aplicația informatică;
  - plata de despăgubiri pentru a compensa compromiterea bunurilor protejate;

- validitatea datelor introduse de către utilizator; asigurând un nivel ridicat al validităţii datelor introduse se minimizează oportunităţile de atac asupra bunurilor protejate şi se îmbunătăţeşte calitatea interacţiunii om – calculator; validitatea datelor se asigură prin implementarea de controale şi proceduri de validare care să prevină cele mai frecvente tipuri de atacuri informatice la care este expusă aplicaţia informatică.

Securitatea informatică este o cerinţă necesară pentru sistemele distribuite de mari dimensiuni conform (Dudin et al., 2009, pp. 234-240). Este imperativă dezvoltarea de sisteme sigure în condiţiile în care numărul ameninţărilor şi al agenţilor ce le provoacă este în continuă creştere.

4. Factori de influenţă a securităţii informatice

Aplicaţiile informatice sunt construcţii complexe utilizate în contexte sociale şi economice definite. Factorii de influenţă sunt numeroşi şi au efecte diferite.

Factorii de influenţă direcţi sunt:

- grupul ţintă, definit ca totalitatea indivizilor ce formează colectivitatea ce foloseşte produsul informatic; grupul ţintă influenţează securitatea informatică în mod direct prin:
  - diversitate structurală, fiind necesară o analiză de structură a colectivităţii pentru a determina tipare comportamentale diferenţiate pe criterii de vârstă, educaţie, sex astfel încât sistemul de securitate să realizeze prin înregistrarea acţiunilor utilizatorilor încadrarea lor într-un tipar comportamental şi prin aplicarea de politicii de securitate desemnate pentru tiparul respectiv să se atingă eficienţa maximă;
  - dimensiune; astfel sistemul de securitate trebuie să fie corelat cu numărul de indivizi ce accesează aplicaţia pentru a funcţiona mereu la parametrii optimi;
  - situaţia socială în cadrul colectivităţii; astfel, dacă se dovedeşte că membri ai colectivităţii sunt împotriva acţiunilor întreprinse de aceasta trebuie luate măsuri în plus pentru mai buna securizare a aplicaţiei, cât şi a securităţii fizice a mediului ambiant în care aplicaţia informatică operează;
- calitatea proceselor de dezvoltare software influenţează direct securitatea informatică deoarece:
  - un nivel de calitate ridicat duce la minimizarea numărului de defecte existent, ducând astfel la scăderea riscului de securitate informatică;
  - un nivel de calitate scăzut creşte numărul de vulnerabilităţi în cadrul aplicaţiei şi astfel riscul de securitate informatică creşte;
    - dacă se urmează în cadrul ciclului de dezvoltare software al aplicaţiei informatice atingerea unor elemente de calitate fixate precum:
      - omogenitatea textelor sursă prin dezvoltarea de module şi proceduri ce se integrează în totalitate în cadrul sistemului de securitate;

- inteligibilitatea procedurilor implementate pentru a minimiza timpul de testare, optimizare şi mentenanță a sistemului de securitate asociat aplicației informatice;
- flexibilitatea sistemelor de comunicare în rețea şi a sistemelor de raportare pentru a lucra cu un număr extins de raportare astfel încât să se asigure o compatibilitate înaltă cu sistemele de detecție a intruziei;
- scalabilitatea textelor sursă pentru a permite îmbunătățirea facilă a sistemului de securitate;

▪ tehnologiile utilizate la dezvoltare reprezintă un aspect important deoarece influențează nivelul securității informatice prin:
  - transferul de calitate; dacă instrumentele folosite au un nivel de calitate înalt atunci sistemele de securitate ce sunt dezvoltate utilizându-le vor avea, de asemenea, un nivel înalt de calitate;
  - gradul în care tehnologiile de asistare în dezvoltare îl ajută pe dezvoltator să îmbunătățească sistemul de securitate prin observații făcute la momentul dezvoltării;
  - gradul de noutate al instrumentelor utilizate şi nivelul de acoperire a ultimelor tipuri de atacuri informatice, permițând astfel dezvoltatorului software să aducă performanțele sistemului de securitate implementat la cele mai înalte standarde;
  - mediul în care se utilizează produsul informatic şi în care activează sistemul de securitate informatică influențează securitatea informatică prin gradul de securitate fizică;
  - elementele de hardware influențează direct sistemul de securitate informatică prin rezistența la uzură, prin fiabilitate, fiind necesară funcționarea lor continuă, dar şi prin viteza de procesare pentru a asigura un timp de răspuns foarte mic pentru fiecare eveniment realizat ce afectează sistemul de securitate;
  - elementele de dinamică a problemei de rezolvat implică o flexibilitate crescută a sistemului de securitate, fiind necesară reacția la situații noi neprevăzute generate de modificările structurale sau logice apărute în transferurile informaționale generate de rezolvarea problemei.

Factorii indirecți care determină securitatea sunt:

▪ complexitatea, care reprezintă un factor important de influență a securității informatice; conform (Pocatilu, 2004) pe măsură ce complexitatea produselor program creşte, numărul defectelor din cod creşte şi astfel nivelul securității informatice scade. Complexitatea are modele:
  - Halstead (1977), model care este caracterizat de următoarele ecuații:
    - lungimea codului N ce este reprezentată de suma numărului de operatori N_1 şi operanzi N_2:

      $$N = n_1 \times \log_2 n_1 + n_2 \times \log_2 n_2$$

      unde:

      n_1 – numărul de operatori distincți;

      n_2 – numărul de operanzi distincți

- volumul care este concretizat prin produsul lungimii codului cu numărul minim de biţi necesari pentru stocarea operatorilor şi operanzilor:
  $V = N \times \log_2 n$

unde:

$N = N_1 + N_2$

$n = n_1 + n_2$

- dificultatea este definită prin:
  $D = \frac{n_1 \times N_2}{2n_2}$
- efortul de a implementa un program e calculat utilizând:
  $E = D \times V$

- McCabbe este definit prin:
  $C = m - n + 2$

unde:

m este numărul arcelor din graf;
n este numărul nodurilor grafului.

În figura 1 se realizează reprezentarea grafică a influenţei factorilor direcţi şi indirecţi asupra securităţii informatice.

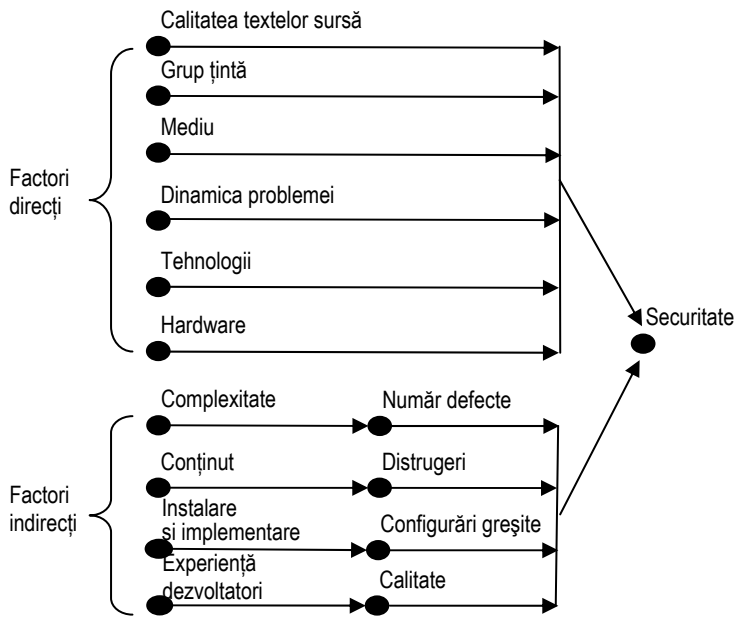

Figura 1. *Reprezentare grafică a factorilor de influenţă*

Factorii de influenţă reprezintă un element important în analiza securităţii informatice şi în stabilirea coeficienţilor modelelor de costuri.

5. Modele de costuri pentru securitatea informatică

Un model este o expresie matematică folosită pentru descrierea unui proces economic utilizând un set de variabile şi de operatori pentru a cuantifica legătura dintre ele[6].

Pentru a construi modele:

- se analizează modul de culegere a datelor;
- se construiesc proceduri de culegere a datelor;
- se construiesc proceduri automate de achiziție a datelor;
- factorii se pun în corespondență cu variabilele;
- se defineşte o tehnologie specifică.

Modele economice conform lucrărilor Ivan şi Vişoiu (2005) sunt formate din:

- variabile exogene, ce sunt asociate factorilor ce influențează un proces sau o altă variabilă rezultativă din model;
- variabile endogene sau rezultative care sunt asociate obiectivului urmărit de realizarea modelului;
- seturile de date culese manual sau automat prin utilizarea de proceduri specifice de achiziție a datelor;
- coeficienții modelului, care sunt rezultați prin aplicarea unor modele de estimare a parametrilor pe baza seturilor de date;
- operatori care sunt folosiți pentru realizarea expresiilor şi marcarea legăturilor dintre factorii componenți ai modelului economic;
- funcții matematice elementare ce intră în alcătuirea modelelor neliniare;
- funcții matematice compuse ce sunt folosite la elaborarea modelelor economice cu un grad ridicat de complexitate.

Există mai multe tipuri de modele asociate costurilor:

- modele liniare, unde se definesc expresii matematice între variabilele exogene şi variabilele endogene de forma:

$$Ct = \sum_{i=1}^{NF} Ch_i$$

unde:

Ct – cost total al implementării sistemului de securitate;
Ch_i – cheltuiala i;
NF – număr variabile endogene;

- modele neliniare, ce conțin înmulțiri, împărțiri, expresii logaritmice, integrale, radicali şi expresii matematice complexe; forma analitică a modelului de cost neliniar este:

Ct = f(CM,CDS)

unde:

Ct – costul total al implementării sistemului de securitate;
CM – complexitatea modulelor;
CDS – costul dezvoltării sistemului de securitate.

Se defineşte următorul model neliniar de analiză al costului[7]:

$$Ct = a_i \times KLoC^{b_i} \times EAF$$

unde:

a_i, b_i – coeficienţi tabelari atribuiţi în funcţie de tipul proiectului;

KloC – numărul de linii sursă la livrare;

EAF – coeficientul de efort estimat pe baza datelor culese printr-o metodologie specifică.

Pentru dezvoltarea modelelor de cost trebuie identificate variabilele ce influenţează costurile şi separarea lor în variabile dependente şi independente. Astfel, în tabelul 2 se reprezintă corelarea între momentele de timp şi valorile factorilor identificaţi.

Tabelul 2

Corelarea momente timp - factori

T	Ch_{Tsec}	Ch_P	Ch_{RBD}	Ch_D	Ch_{PSS}	Ch_T	Ch_{DESP}	Ch_{OPT}	Ch_{VUL}
t_1	$Ch_{Tsec\ 1}$	Ch_{P1}	Ch_{RBD1}	Ch_{D1}	Ch_{PSS1}	Ch_{T1}	Ch_{DESP1}	Ch_{OPT1}	Ch_{VUL1}
t_2	$Ch_{Tsec\ 2}$	Ch_{P2}	Ch_{RBD2}	Ch_{D2}	Ch_{PSS2}	Ch_{T2}	Ch_{DESP2}	Ch_{OPT2}	Ch_{VUL2}
...	...	...	...	...	...	...	...	...	...
t_i	$Ch_{Tsec\ i}$	Ch_{Pi}	Ch_{RBDi}	Ch_{Di}	Ch_{PSSi}	Ch_{Ti}	Ch_{DESPi}	Ch_{OPTi}	Ch_{VULi}
...	...	...	....	....	...	...	...	...	...
t_n	$Ch_{Tsec\ n}$	Ch_{Pn}	Ch_{RBDn}	Ch_{Dn}	Ch_{PSSn}	Ch_{Tn}	Ch_{DESPn}	Ch_{OPTn}	Ch_{VULn}

unde:

Ch_{Tsec} – cheltuielile totale cu sistemul de securitate;

Ch_P – cheltuielile cu munca de programare;

Ch_{RBD} – cheltuielile cu recuperarea bazei de date;

Ch_D – cheltuielile cu proiectarea sistemului de mentenanţă;

Ch_{PSS} – cheltuielile cu proiectarea sistemului de securitate;

Ch_T – cheltuielile cu testarea;

Ch_{DESP} – cheltuielile cu despăgubirile plătite;

Ch_{OPT} – cheltuielile cu optimizarea sistemului de securitate;

Ch_{VUL} – cheltuieli asociate eliminării vulnerabilităţilor.

Costurile de securitate sunt reprezentate de aceste cheltuieli conducând la modelul:

$$Ch_{T\sec} = Ch_P + Ch_{RBD} + Ch_D + CH_{PSS} + Ch_T + Ch_{DESP} + Ch_{OPT} + Ch_{VUL}$$

Conform Andersen şi Choobineh (2008), costurile de securitate informatică au un impact important în alegerea strategiilor de securizare a bunurilor întreprinderii, astfel determinarea costurilor devine o analiză esenţială în selectarea celui mai bun sistem de securitate considerând condiţiile de mediu şi sociale ale companiei.

6. Optimizarea securității informatice

Optimizarea ca proces de selecție dintr-o mulțime are rolul de a îmbunătăți. Considerând mulțimea de momente M_1, M_2, ..., M_k şi mulțimea de variante V_1, V_2, ..., V_k se determină varianta optimă ca:

$$V(M_h) = \min_{1 \le i \le k} \{V_i\}$$

unde:

$V(M_h)$ – varianta optimă dintre M_1, M_2, ..., M_k.

Pentru a realiza optimizarea în cele mai bune condiții este necesară (Ivan et al., 2008, pp. 39-56) definirea unor criterii de optim prin intermediul cărora să se urmărească îmbunătățirea numai a anumitor caracteristici ale sistemului de securitate asociat aplicației informatice. Astfel, pentru securitatea informatică se definesc următoarele criterii de optim:

- minimizarea timpilor de execuție a procedurilor ce compun sistemul de securitate informatică prin optimizarea algoritmilor de prelucrare a datelor, prin eliminarea textelor sursă nenecesare, prin analiza firelor de execuție şi direcționarea lor pe calea cea mai scurtă;
- maximizarea eficienței aplicației prin definirea de praguri de eficiență în cadrul tuturor operațiunilor realizate, identificându-se astfel zonele critice în cadrul sistemului de securitate;
- maximizarea corectitudinii sistemului de securitate informatică pentru a identifica cât mai exact amenințările şi tentativele de atac asupra bunurilor protejate;
- minimizarea timpilor de depanarea a sistemului de securitate prin reutilizarea codului sursă.

Optimizarea textului sursă are rolul de a îmbunătăți calitatea procedurilor şi a timpilor de execuție. Prin optimizarea textului sursă se urmăreşte şi minimizarea numărului de defecte, îmbunătățind astfel performanța generală a sistemului de securitate informatică prin creşterea caracteristicilor de calitate ale produsului informatic. Optimizarea prin creşterea nivelului de calitate a sistemului de securitate are la bază:

- testarea, prin care se observă probleme în calitatea sistemului prin reluarea segmentelor cilului de dezvoltare în care au fost generate se vor implementa soluții pentru rezolvarea lor;
- raportarea internă a sistemului de securitate, prin care se determină pe baza simulărilor cu date de test ce caracteristici de calitate au un nivel mai scăzut decât cel aşteptat;
- rularea de rapoarte periodice pentru a monitoriza evoluția aplicației în condiții de utilizare curentă, astfel dorindu-se scoaterea în evidență a problemelor celor mai frecvente datorate securității informatice;
- apariția de tehnologii noi, prin utilizarea cărora se realizează un transfer de calitate asupra sistemului de securitate, el devenind mai performant;

- dezvoltarea de tehnologii noi de securizare a informaţiei, prin implementarea cărora sistemul de securitate este mai eficient;
- certificarea dezvoltatorilor pentru a permite aflarea de noi tehnici de lucru mai bune decât cele vechi; acest lucru conduce la scrierea mai eficientă a codului şi cu mai puţine erori;
- certificarea companiei dezvoltatoare de software în sisteme de calitate pentru a instaura politici de dezvoltare software ce urmează criterii bine definite pentru optimizarea calităţii proceselor din ciclul de dezvoltare software.

Creşterea calităţii sistemului de securitate conduce la obţinerea unei variante îmbunătăţite a sistemului ce corespunde creşterii nivelurilor caracteristicilor de calitate specificate. Această variantă este net superioară celei vechi prin prisma caracteristicilor de calitate optimizate.

Optimizarea costurilor(5) reprezintă practicile, abilităţile şi comportamentul adoptat de o organizaţie pentru reducerea cheltuielilor, minimizarea costurilor cu păstrarea calităţii sistemelor software dezvoltate şi menţinerea constantă a potenţialului de creştere a organizaţiei. Se urmăreşte optimizarea costurilor la nivel de organizaţie, la nivel de echipă de dezvoltatori software şi la nivel de texte sursă. Procesul de optimizare a costurilor la nivel de organizaţie trebuie să identifice zonele administrative şi de producţie ale organizaţiei în care se înregistrează cele mai mari cheltuieli şi să intervină prin minimizarea sau eliminarea următoarelor costuri:

- auxiliare, ce nu suportă operaţiuni generatoare de profit;
- cu personalul auxiliar, ce nu influenţează activităţile ce aduc profit;
- cu procurarea de materiale şi echipamente care nu sunt necesare bunei derulări a proceselor de afaceri şi dezvoltare software;
- cu transportul angajaţilor, în acest scop identificându-se căi de micşorare a numărului de călătorii de afaceri dacă este posibilă rezolvarea situaţiilor prin intermediul video-conferinţelor sau prin intermediul reţelei de calculatoare interne;
- cu terţii, realizând licitaţii pentru obţinerea celui mai bun preţ pentru materialele şi echipamentele necesare.

7. Costul securităţii informatice pentru aplicaţia de validare identificatori organizaţie

Aplicaţia pentru analiza identificatori organizaţie realizează analiza ortogonalităţii denumirilor de companie în vederea eliminării situaţiilor în care există două companii cu denumiri foarte apropiate.

În cadrul aplicaţiei de analiză a ortogonalităţii denumirilor de organizaţie se construieşte un vocabular VOCDEN = $\{D_1, D_2, \ldots, D_k\}$ ce conţine toate denumirile de organizaţie introduse în baza de date.

Se identifică următoarele situaţii:

a) Entitatea are denumirea formată dintr-un singur cuvânt, analiza este realizată prin compararea denumirii cu toate celelalte denumiri stocate deja care au un singur

cuvânt, ortogonalitatea este studiată la nivel de cuvânt şi calculată pentru cuvintele CI şi CB utilizând:

$$ORTOC(CI,CB) = 1 - \frac{Len(SMC)}{\max\{Len(CI), Len(CB)\}}$$

unde:

Len(SMC) – lungimea subşirului maxim comun;
Len(CI) – lungimea cuvântului CI;
Len(CB) – lungimea cuvântului CB.

Pentru obținerea şirului SMC se procedează la definirea indicatorului de extragere a subşirului maxim comun ⊗ din două cuvinte CI şi CB.

SMC = CI ⊗ CB

unde:

Len(SMC) ≤ max{Len(CI), Len(CB)}

Astfel $ORTOC(CI,CB) \in [0,1]$.

Se consideră cuvintele „test” şi „rest”:

SMC = „test” ⊗ „rest”

SMC = „est”.

Pentru cuvintele definite şi SMC calculat se calculează ortogonalitatea astfel:

ORTOC(„test”, „rest”) = $1 - \frac{3}{4} = 0{,}25$

Ortogonalitatea în cadrul aplicației de validare identificatori organizație se calculează prin formarea unui vocabular extras din VOCDEN, VOC = $\{C_1, C_2, ..., C_n\}$ ce conține denumiri de companie ce au un singur cuvânt. Se defineşte următoarea formulă pentru a analiza ortogonalitatea:

$$ORTOTOT(CI,VOC) = \min_{i=1,n}\{ORTOC(CI,VOC_i)\}$$

Dacă ORTOTOT(CI,V) este mai mică de 0,75, atunci se procedează la reformularea denumirii.

b) Entitatea are denumirea formată din mai multe cuvinte; astfel ortogonalitatea este stabilită prin analiza la nivel de vocabular şi la nivel de cuvânt.

Analiza la nivel de vocabular se realizează prima pentru a determina corespondența între texte şi necesitățile de validare ale aplicației pentru calcul ortogonalității.

Pentru a analiza ortogonalitatea a două texte T_1 şi T_2 se construiesc două vocabulare V_1 şi V_2 ce sunt definite de sortarea alfabetica a cuvintelor care compun texte T_1, respectiv T_2. Vocabularele se definesc ca seturile de cuvinte sortate $V_1 = \{C_{11}, C_{12},..., C_{1n}\}$ şi $V_2 = \{C_{21}, C_{22}, ..., C_{2n}\}$, unde C_{1i} corespunde cuvântului de pe poziția i a vocabularului V_1, iar C_{2j} corespunde cuvântului de pe poziția j a vocabularului V_2. Pentru calculele făcute se utilizează operatorul \ din teoria mulțimilor fiind definit considerând două mulțimi A ş si B:

$B \setminus A = \{x \in B \mid x \notin A\}$

Dacă în urma calculării ortogonalității textelor una din următoarele ecuații este adevărată:

$V_1 \backslash CC = \{\varnothing\}$

$V_2 \backslash CC = \{\varnothing\}$

unde:

CC – setul cuvintelor comune,

atunci ortogonalitatea este reprezentată de formula

$$ORTOT(V_1, V_2) = 1 - \frac{NCC}{\max(NrCV_1, NrCV_2)}$$

unde:

NCC – număr cuvinte comune;

$NrCV_1$ – număr cuvinte cuprinse în vocabularul V_1;

$NrCV_2$ – număr cuvinte cuprinse în vocabularul V_2.

Dacă amândouă ecuațiile sunt adevărate rezultă că vocabularele sunt identice, iar ortogonalitatea este 0.

Dacă amândouă ecuațiile de mai jos sunt adevărate:

$V_1 \backslash CC \neq \{\varnothing\}$

$V_2 \backslash CC \neq \{\varnothing\}$

unde:

$CC = \{CC_1, CC_2, ..., CC_k\}$ submulțimea cuvintelor comune.

Se calculează ortogonalitatea individuală a cuvintelor conținute în vocabularele:

$V'_1 = V_1 \backslash CC$

$V'_2 = V_2 \backslash CC$

Fiecare cuvânt C_{1i} conținut în vocabularul V'_1 se compară cu fiecare cuvânt C_{2j} conținut în vocabularul V'_2 pentru a determina subșirul maxim comun SMC. Ortogonalitatea se calculează folosind următoarea formulă:

$$ORTOC(C_{1i}, C_{2j}) = 1 - \frac{Len(SMC_{ij})}{\max\{Len(C_{1i}), Len(C_{2j})\}}$$

unde:

Len(SMC) – lungimea subșirului maxim comun;

$Len(C_{1i})$ – lungimea cuvântului i din vocabularul V'_1;

$Len(C_{2j})$ – lungimea cuvântului j din vocabularul V'_2.

Astfel valorile prezentate în tabelul 3 reprezintă ortogonalitatea individuală a cuvintelor.

Tabelul 3

Ortogonalitatea ORTO (V'_1,V'_2)

	C_{11}	C_{12}	…	C_{1n}
C_{21}	x_{11}	x_{12}	…	x_{1n}
C_{22}	x_{21}	x_{22}	…	x_{2n}
....	…	...	…	…
C_{2n}	x_{n1}	x_{n2}	…	x_{nn}

unde:

$$ORTOC(V'_i, V'_j) = x_{ij}$$

Pentru a păstra reprezentativitatea în cadrul mulțimii de cuvinte se definesc:

$$Max = \max_{\substack{Len(V'_j) \\ 1 \le i \le nrCV'_i \\ j=1,2}} \{V'_j[i]\}$$

şi setul

$$Min = \min_{\substack{Len(V'j) \\ 1 \le i \le nrCV'_i \\ j=1,2}} \{V'_j[i]\}$$

unde:

Max – vocabularul cu numărul cel mai mare de caractere;
Min – vocabularul cu numărul cel mai mic de caractere;
Max_i – cuvântul de pe poziția i a denumirii de lungime maximă;
Min_j – cuvântul de pe poziția j a denumirii de lungime minimă;
$Len(V'_j)$ – numărul de cuvinte al vocabularului V'_j;
$nrCV'_i$ – numărul de cuvinte din vocabularul V';
V'[i] – cuvântul de pe poziția i a vocabularului V'.
În tabelul 4 se prezintă matricea de ortogonalitate Max–Min

Tabelul 4

Matricea de ortogonalitate Max – Min

	Min_1	Min_2	…	Min_n
Max_1	x'_{11}	x'_{12}	…	x'_{1n}
Max_2	x'_{21}	x_{22}	…	x'_{2n}
....	…	...	…	…
Max_n	x'_{n1}	x'_{n2}	…	x'_{nn}

Formula pentru calculul ortogonalității devine:

$$ORTOC(Max_i, Min_j) =$$

$$= 1 - \frac{Len(SMC_{ij})}{\max\{Len(Max_i), Len(Min_j)\}} * \frac{\max\{Len(Max_i), Len(Min_j)\}}{Len(Max)} =$$

$$= 1 - \frac{Len(SMC_{ij})}{Len(Max)}$$

unde:

len(Max) – numărul de caractere din setul de cuvinte Max.

$$ORTOC(V'_1, V'_2) = \sum_{i=1}^{n} \min_{j=1,n} \{ORTO(Max_i, Min_j)\}$$

Pentru definirea ortogonalității întregului text incluzând ortogonalitatea la nivel de text şi ortogonalitatea calculată pentru cuvintele asociate vocabularului V''_1, respectiv V'_2 se defineşte următoarea formulă:

$$ORTO(V_1,V_2) = ORTOT(V_1,V_2) \times ORTOC(V'_1,V'_2)$$

Prin înmulţirea celor două ortogonalităţi se obţine gradul de reprezentativitate la nivel de frază al ortogonalităţii la nivel de cuvânt obţinând astfel o analiză completă a nivelului de ortogonalitate între cele două texte.

Pentru calculul ortogonalităţii pentru toate denumirile ce au acelaşi număr de cuvinte ca denumirea introdusă de utilizator se extrag din vocabularul VOCDEN în vocabularul VOC = {C_1, C_2, …, C_l} şi se foloseşte următoarea formulă:

$$ORTOTOT(V_1,VOC) = \min_{i=1,n}\{ORTO(V_1,VOC_i)\}$$

Dacă ORTOTOT(V_1, VOC) este mai mică de 0,75 se procedează la reintroducerea denumirii de companie.

Pentru estimarea costului implementării sistemului de securitate informatică în cadrul aplicaţiei de validare identificatori firma se consideră principalii factori ce compun modelul liniar de cost:

- forma modelului de cost Ct:

$$Ct = \sum_{i=1}^{NF} Ch_i$$

- echipamentele necesare securizării produsului informatic;
- echivalentul valoric al timpului exprimat în ore om asociat dezvoltării sistemului de securitate;
- cheltuielile cu documentarea pentru identificarea celor mai noi ameninţări prezente în mediul online.

În tabelul 5 se consideră parametrii asociaţi costurilor auxiliare şi valorile lor estimative.

Tabelul 5

Costuri auxiliare

Denumire	Cost Efectiv	Durata utilizare
Laptop	4000	28
Router wireless	400	28
Instrumente asistare dezvoltare	300	28
Instrumente dezvoltare	1500	28
Chirie locaţie	600	28

În tabelul 6 se prezintă cheltuielile legate de activitatea de programare şi testare a aplicaţiei de validare identificatori organizaţie.

Tabelul 6

Costul activităţilor de programare şi testare a aplicaţiei

Activitate	Durata (zile)	Cost zi	Cost total
Documentare	4	200	800
Dezvoltare software securitate	15	200	3000
Testare software securitate	3	150	450
Depanare software securitate	2	200	400
Implementare şi instalare software securitate	4	150	600

Modelul liniar de cost este:

$$Ct=CA+Cd+Cds+Cts+Cdes+Ciis=6800+800+600+450+400+600=9650$$

unde:

CA- totalul costurilor auxiliare;
Cd- costuri de documentare;
Cds – costuri dezvoltare software securitate;
Cts – costuri testare software securitate;
Cdes – costuri depanare software securitate;
Ciis – costuri implementare şi instalare software securitate.

8. Concluzii

Pentru dezvoltarea sistemelor de securitate în condiții de costuri optime este necesară analiza factorilor ce influențează securitatea informatică. Este necesară dezvoltarea unui sistem de caracteristici de calitate şi realizarea corelării sale cu factorii de influență ai securității informatice.

Rezultatele cercetării sunt reprezentate de modele de cost eficiente ce sunt testate în practică. Sunt prezentate modele de cost ce țin cont de necesitățile actuale ale dezvoltării de software performant pentru securitatea informatică. Este prezentat un model de risc ce ajută la estimarea parametrilor din modelele de cost pentru securitatea informatică.

Produsul software pentru validarea identificatorilor organizației este destinat alegerii unei denumiri de organizație cât mai clare şi cât mai diferite față de cele existente în bazele de date. Sunt implementate modele de ortogonalitate testate şi se realizează o analiză completă a denumirilor de organizație.

Note

(1) Vezi http://www.sans.org/reading_room/whitepapers/awareness/ the_need_for_information_security_in_todays_economy_916
(2) Vezi http://www.ietf.org/rfc/rfc2828.txt
(3) Vezi http://csrc.nist.gov/publications/nistir/NISTIR-7298_Glossary_Key _Infor_Security_Terms.pdf
(4) Vezi http://en.wikipedia.org/wiki/Information_security
(5) Vezi http://www.gartner.com/DisplayDocument?doc_cd=166713
(6) Vezi http://en.wikipedia.org/wiki/Economic_model
(7) Vezi http://en.wikipedia.org/wiki/COCOMO

Bibliografie

Alhazmi, O.H., Malaiya, Y.K., „Application of vulnerability discovery models to major operating systems", IEEE Transactions on Reliability, vol. 57, issue 1, 2008, ISSN: 0018-9529

Anderson, E.E., Choobineh, J., „Enterprise information security strategies", *Computers & Security*, vol. 27, issue 1, 2008, ISSN: 0167-4048

Anwar, Z., Montanari, M., Gutierrez, A., Campbell, R.H., „Budget constrained optimal security hardening of control networks for critical cyber-infrastructures", *International Journal of Critical Infrastructure Protection,* vol. 2, issue 1, 2009, ISSN 1874-5482

Aroba, J., Cuadrado-Gallego, J.J., Sicilia, M.-A., Ramos, Isabel, Garcia-Barriocanal, Elena, „Segmented software cost estimation models based on fuzzy clustering", *Journal of Systems and Software*, vol. 81, issue 11, 2008, ISSN: 0164-1212

Chen, Z., Ji, C., „An Information-Theoretic View of Network-Aware Malware Attacks", IEEE *Transactions on Information Forensics and Security*, vol. 4, issue 3, 2009, ISSN: 1556-6013

Dudin, E.B., Zhlyabinkova, I.A., Zakharova, E.G., Smetanin, Yu.G., „Information security in distributed computing systems. A review", *Automatic Documentation and Mathematical Linguistics*, vol. 43, no. 4, 2009, ISSN: 1934-8371

Halstead, M. (1977). *Elements of Software Science, Operating, and Programming Systems Series*, Volume 7, New York, NY, Elsevier, Bucureşti

Huang, D.C., Hu, Q., „An economic analysis of the optimal information security investment in the case of a risk-averse firm", *International Journal of Production Economics*, vol. 114, issue 2, 2008, ISSN: 0925-5273

Ivan, I. Vişoiu, A. (2005). *Baza de modele economice*, Editura ASE, ISBN: 973-594-570-4, Bucureşti

Ivan, I., Doinea, M., Palaghiţă, D., „Optimization of authentication processes in distributed applications", *Theoretical and Applied Economics*, 2008, nr. 6, ISSN 1841 – 8678, Bucureşti

Ivan, I., Vişoiu, A., Ciurea, C., Palaghiţă, D., „Model bases and software quality metrics refinement", The 4th International Conference *Economy and Transformation Management*, Timişoara, 2008

Jasmine, K.S., Vasantha, R., „Cost estimation model for reuse based software products", *IMECS 2008: International Multiconference of Engineers And Computer Scientists*, 2008, ISBN: 978-988-98671-8-8

Khansa, L., Liginlal, D., „Valuing the flexibility of investing in security process innovations", *European Journal of Operational Research*, vol. 192, issue 1, 2009, ISSN: 0377-2217

Kumar, V.K., Carr, M., Kiran, R.N., „Software development cost estimation using wavelet neural networks", *Journal of Systems and Software*, vol. 81, issue 11, 2008, ISSN: 0164-1212

Lee, J., Kim, C.-Ki, „Software architecture evaluation methods based on cost benefit analysis and quantitative decision making", *Empirical Software Engineering,* vol. 14, issue 4, 2009, ISSN: 1382-3256

Lu, J., Bai, C., Zhang, G., „Cost-benefit factor analysis in e-services using bayesian networks", *Expert Systems with Applications*, vol. 36, issue 3, 2009, ISSN 0957-4174

Pendharkar, P.C., Rodger, J.A., Subramanian, G.H., „An empirical study of the Cobb-Douglas production function properties of software development effort", *Information and Software Technology*, vol. 50, Issue 12, 2008, ISSN 0950-5849

Pfleeger, Ch.P., Pfleeger, S.L. (2006). *Security in Computing, 4th Edition*, ISBN: 978-0132390774, Prentice Hall

Pocatilu, P. (2004). *Costurile testării software*, ASE Publishing House, ISBN: 973-594-549-5

Stamp, M. (2005). *Information Security: Principles and Practice*, ISBN: 978-0-471-73848-0, Wiley-Interscience

Tipton, H.F., Krause, M. (2008). *Information Security Management Handbook, Sixth Edition*, 456 pages, ISBN: 978-1420067088, Auerbach Publications

Vacca, J.R. (2009). *Computer and Information Security Handbook*, ISBN: 978-0123743541, Morgan Kaufmann

Vişoiu, A., „Refinement methods for security metrics", *Economic Informatics Conference 2009*, ISBN: 978-606-505-172-2

Vydrin, Al.S., „Theoretical aspects of information security", *Journal of Mathematical Sciences*, vol. 156, no. 2, 2009, ISSN: 1573-8795