

**UNIVERSITATEA BABEȘ BOLYAI CLUJ-NAPOCA
FACULTATEA DE ȘTIINȚE ECONOMICE ȘI GESTIUNEA
AFACERILOR
ȘCOALA DOCTORALĂ ȘTIINȚE ECONOMICE ȘI
GESTIUNEA AFACERILOR**

**CONTRIBUȚII LA SECURITATEA
SISTEMELOR INFORMATICE
ECONOMICE**

- Rezumatul tezei de doctorat -

**Conducător științific
Prof. univ dr. TOMAI Nicolae**

**Doctorand
MIHUȚ Marius**

**Cluj-Napoca
2014**

CUPRINSUL TEZEI DE DOCTORAT

INTRODUCERE	1
Oportunitatea și motivația lucrării	2
Obiectivele lucrării	2
Structura lucrării	3
1. ASPECTE TEORETICE ALE SECURITĂȚII SISTEMELOR INFORMATICE	6
1.1 MODELE DE SECURITATE	6
1.1.1 Modele de securitate multinivel	6
1.1.2 Modelul Bell-LaPadula	7
1.1.3 Modelul de integritate Biba	11
1.1.4 Modelul de integritate Clark-Wilson	12
1.1.5 Compararea modelelor de securitate multinivel	14
1.2 MODELE DE SECURITATE MULTILATERALE	15
1.2.2 Modelul Zidul chinezesc	16
1.2.3 Modelul BMA	17
1.3 MODELE DE SECURITATE SPECIFICE UNUI DOMENIU	18
1.3.1 Modelul Graham-Denning	18
1.3.2 Modelul Take-Grant	18
1.4 ASPECTE ALE SECURITĂȚII SISTEMELOR COLABORATIVE	19
1.5 ASPECTE ALE SECURITĂȚII UBIQUITOUS COMPUTING	21
1.5.1 Caracteristici ale procesării omniprezente	22
1.5.2 Particularități ale securității ubicomp	23
1.6 ASPECTE ALE SECURITĂȚII WEB-SERVICES	26
1.7 CONCLUZII LA ACEST CAPITOL	29
2. MANAGEMENTUL SECURITĂȚII INFORMAȚIEI	31
2.1 SITUAȚIA ACTUALĂ	31
2.2 GUVERNANȚA IT	34
2.3 CADRUL DE LUCRU COBIT	35
2.4 SETUL DE BUNE PRACTICI ITIL	46
2.5 STANDARDELE DE SECURITATE ISO/IEC 27000	47
2.5.1 Măsuri de securitate ISO	48
2.6 SISTEMUL DE STANDARDE NIST	53
2.7 ALINIAREA ȘI INTEGRAREA STANDARDELOR COBIT, ITL, ISO ȘI NIST	54
2.7.1 Integrarea pe verticală	55
2.7.3 Alinierea pe orizontală	56
2.8 CONCLUZII LA ACEST CAPITOL	57
3. MANAGEMENTUL DE RISC	62
3.1 IDENTIFICAREA AMENINȚĂRILOR	63
3.2 IDENTIFICAREA VULNERABILITĂȚILOR	65
3.3 METODE DE EVALUARE A RISCULUI	67
3.3.1 Analiza calitativă	68
3.3.2 Analiza cantitativă	69
3.3.3 Analiza pe post	71
3.3.4 Compararea metodelor de evaluare a riscurilor	72
3.5 REDUCEREA RISCURILOR	73
3.6 CONCLUZII LA ACEST CAPITOL	80
4. CALCULAȚIA COSTURILOR ȘI CHELTUIELILOR DE SECURITATE	82

4.1 METODE DE CALCULAȚIE A COSTURILOR PARȚIALE	82
4.2 METODE DE CALCULAȚIE A COSTURILOR COMPLETE	82
4.3 METODA DE CALCUL A COSTURILOR ABC	83
4.4 MODELUL DE COST HP LABORATORIES	87
4.5 EVALUAREA COSTULUI TOTAL DE DEZVOLTARE	89
4.6 METODA DE CALCUL COMBINATĂ ABC-HP	90
4.7 CONCLUZII LA ACEST CAPITOL	92
5. SECURITATEA SISTEMELOR INFORMATICE ECONOMICE: STUDII DE CAZ	94
5.1 NECESITATEA ABORDĂRII MULTIDISCIPLINARE	94
5.2 STUDIU DE CAZ: METODA DE CALCUL COMBINATĂ ABC-HP	95
5.3 STUDIU DE CAZ: ANALIZA PPP A SECURITĂȚII	100
5.3.1 Introducere	100
5.3.2 Analiza securității bazată pe protecție, preț și performanță	101
5.3.3. Rezultate și discuții	104
5.3.3.1 Situația inițială	104
5.3.3.2 Primul scenariu	106
5.3.3.3 Al doilea scenariu	108
5.3.3.4 Al treilea scenariu	110
5.3.3.5 Centralizarea rezultatelor	112
5.4 CONCLUZII LA ACEST CAPITOL	113
6. ELEMENTE UTILIZATE ÎN MODELUL DE SECURITATE	116
6.1 PRINCIPIUL LUI PARETO	116
6.1.1 Aplicarea principiului lui Pareto în management și informatică	117
6.1.2 Aplicarea principiului lui Pareto în managementul securității	118
6.2 PRIORITIZAREA ACTIVITĂȚILOR SECURITĂȚII	120
6.2.1 Metode de prioritizare	120
6.2.2 Prioritizarea bazată pe Metoda Drumului Critic (CPM)	122
6.3 MĂSURĂTORI ȘI METRICI DE SECURITATE	127
6.4 DOCUMENTAȚII DE SECURITATE	130
6.5 VIZUALIZAREA SECURITĂȚII	133
6.6 MONITORIZAREA SECURITĂȚII	134
6.6.1 Auditul – noțiuni generale	135
6.6.2 Auditul securității	138
6.7 TABELUL DE RESPONSABILITĂȚI RACI	139
6.8 FIȘA CU INDICATORI AGREGAȚI	140
6.9 REGULA 1-10-100	141
6.10 ANALIZA DATELOR DE JURNALIZARE	142
6.11 CONCLUZII LA ACEST CAPITOL	143
7. DESCRIEREA MODELULUI DE SECURITATE PROPRIU	145
7.1 SITUAȚIA ACTUALĂ	145
7.2 CONCEPTE ALE SECURITĂȚII	146
7.3 CADRUL DE LUCRU SERIOS	153
7.4 DESCRIEREA CADRULUI DE LUCRU SERIOS	154
7.5 STUDIU DE CAZ: EVALUAREA UNUI SISTEM DE SECURITATE	185
7.5.1 Introducere	185
7.5.2 Situația inițială	187
7.5.3 Situația 1 – după efectuarea analizei de risc	188
7.5.4 Situația 2 – după implementarea măsurilor de securitate selectate conform Principiului lui Pareto	189

7.5.5 Situația 3 – după efectuarea unui audit de securitate	190
7.5.6 Situația 4 – după efectuarea unei scanări a sistemului informatic	191
7.5.7 Situația 5 – după testarea sistemului de securitate	192
7.5.8 Situația 6 – la apariția unui eveniment de securitate	193
7.6 VERIFICAREA ȘI VALIDAREA MODELULUI DE SECURITATE	194
7.6.1 Verificarea modelului de securitate	194
7.6.2 Validarea modelului de securitate	195
7.7 CONCLUZII LA ACEST CAPITOL	197
CONCLUZII ȘI CONTRIBUȚII PERSONALE	199
Contribuții personale	199
Diseminarea rezultatelor	201
Perspective	202
BIBLIOGRAFIE	204

LISTA ABREVIERILOR

ALE – Annual loss expectancy

BCS – Balanced Scorecard

CMM – Capability Maturity Model

CNSS – Committee on National Security Systems

COBIT – Control Objectives for Information and related Technology

CRAMM – CCTA Risk Analysis and Management Method

ISACA – Information Systems Audit and Control Association

ISO/IEC – International Organization for Standardization/International Electrotechnical Commission

IT – Information Technology

ITIL – Information Technology Infrastructure Library

NIST – National Institute of Standards and Technology

PDCA – Plan Do Check Act

RACI – Responsible, Accountable, Consulted, Informed

SDLC – System Development Life Cycle

LISTA FIGURILOR

Figura 1. Organizarea informației în modelele de securitate multi-nivel	6
Figura 2. Structura obiectelor	8
Figura 3. Organizarea informației în modelele de securitate multilaterale	16
Figura 4. Ciclul de viață al unei organizații virtuale	20
Figura 5. Arhitectura de securitate web-services (WS)	28
Figura 6. Abordarea actuală a managementului securității	31
Figura 7. Metodologia CRAMM	32
Figura 8. Organigrama managementului de risc	33
Figura 9. Diagrama de conținut COBIT	37
Figura 10. Descrierea unui proces, împreună cu obiectivele și indicatorii cheie	42
Figura 11. Compararea abordărilor NIST (SDLC) și ISO (PDCA)	57
Figura 12. Etapele managementului de risc	62
Figura 13. Premisele metodelor de calcul a costurilor	86
Figura 14. Modelul inițial al sistemului informatic creat cu OPNET	105
Figura 15. Configurarea funcționării modelului	106
Figura 16. Încărcarea rețelei în scenariul 1 (protocolul Ethernet)	107
Figura 17. Încărcarea rețelei în scenariul 1 (protocolul TCP/IP)	107
Figura 18. Întârzierea rețelei în scenariul 1 (protocolul Ethernet)	107
Figura 19. Întârzierea rețelei în scenariul 1 (protocolul TCP/IP)	107
Figura 20. Încărcarea rețelei în scenariul 2 (protocolul Ethernet)	109
Figura 21. Încărcarea rețelei în scenariul 2 (protocolul TCP/IP)	109
Figura 22. Întârzierea rețelei în scenariul 2 (protocolul Ethernet)	109
Figura 23. Întârzierea rețelei în scenariul 2 (protocolul TCP/IP)	109
Figura 24. Încărcarea rețelei în scenariul 3 (protocolul Ethernet)	111
Figura 25. Încărcarea rețelei în scenariul 3 (protocolul TCP/IP)	111
Figura 26. Întârzierea rețelei în scenariul 3 (protocolul Ethernet)	111
Figura 27. Întârzierea rețelei în scenariul 3 (protocolul TCP/IP)	111
Figura 28. Aplicarea principiului lui Pareto în managementul securității	119
Figura 29. Diagrama de rețea (de interdependențe între activități)	126
Figura 30. Rezultatul rulării Pathfinder	127
Figura 31. Graficul de vizualizare a stării securității	133
Figura 32. Costurile de eliminare a unui defect în diverse etape	141
Figura 33. Modelul de securitate al cadrului de lucru SERIOS	146
Figura 34. Schema funcțională a managementului de risc	171
Figura 35. Modul de calcul a indicatorilor agregați	176
Figura 36. Instrumentul de vizualizare a stării securității	178
Figura 37. Indicatorii agregați de securitate în situația inițială	188
Figura 38. Indicatorii agregați de securitate după analiza de risc	189
Figura 39. Indicatorii agregați de securitate după implementarea măsurilor de securitate, selectate conform Principiului lui Pareto	190
Figura 40. Indicatorii agregați de securitate după efectuarea auditului	191
Figura 41. Indicatorii agregați de securitate după scanarea sistemului informatic	191
Figura 42. Indicatorii agregați de securitate după testarea măsurilor de securitate	192
Figura 43. Indicatorii agregați de securitate după un eveniment de securitate	193
Figura 44. Evoluția indicatorilor de agregare	196

LISTA TABELELOR

Tabelul 1. O comparație a modelelor de securitate multinivel	15
Tabelul 2. Gruparea activităților domeniului și procese	40
Tabelul 3. Familia de standarde ISO/IEC 27000	47
Tabelul 4. Catalogul generic de amenințări	63
Tabelul 5. Catalogul generic de vulnerabilități	66
Tabelul 6. Matricea de risc utilizată la analiza pe post	71
Tabelul 7. Exemplu de ierarhizare a evenimentelor pe baza gradului de expunere	72
Tabelul 8. Compararea metodelor de evaluare a riscului	72
Tabelul 9. Catalogul generic al măsurilor de securitate	74
Tabelul 10. Diferențele între metoda ABC și metodele tradiționale	84
Tabelul 11. Costul total al serviciului Programarea unui modul software	91
Tabelul 12. Costul total de dezvoltare al proiectului	91
Tabelul 13. Interesele diferite referitoare la securitate într-o organizație	94
Tabelul 14. Bugetul departamentului IT	95
Tabelul 15. Costul spațiului ocupat de server	96
Tabelul 16. Costul alimentării cu energie a serverului	96
Tabelul 17. Costul răcirii serverului	96
Tabelul 18. Identificarea inductorilor de cost	98
Tabelul 19. Centrele de cheltuieli asociate activităților	98
Tabelul 20. Costurile asociate fiecărui centru de cheltuieli	99
Tabelul 21. Calcularea costului serviciului <i>Administrarea serverului IT</i>	99
Tabelul 22. Calcularea costului total pentru ieșirea / obiectul de calculație <i>Administrarea serverului IT</i>	100
Tabelul 23. Matricea de risc	103
Tabelul 24. Compararea rezultatelor obținute în fiecare scenariu	112
Tabelul 25. Metode de prioritizare	120
Tabelul 26. Nivelurile de risc asociate unor dispozitive conectate	122
Tabelul 27. Identificarea activităților și sarcinilor de securitate	123
Tabelul 28. Atribuirea unui nivel de criticalitate activităților și sarcinilor	124
Tabelul 29. Evaluarea duratei de efectuare a activităților și sarcinilor	124
Tabelul 30. Atribuirea de priorități activităților și sarcinilor	125
Tabelul 31. Procesul de management al securității - cadrul de lucru SERIOS	147
Tabelul 32. Structura unui capitol al cadrului de lucru SERIOS	151
Tabelul 33. Structura formală a controalelor de securitate	152
Tabelul 34. Structura formală a metricilor de securitate	153
Tabelul 35. Evidența elementelor documentației de securitate	165
Tabelul 36. Matricea de risc	171
Tabelul 37. Tabelul de evaluare a nivelului de risc	172
Tabelul 38. Fișa de evaluare a securității	178
Tabelul 39. Definirea nivelurilor de maturitate	179
Tabelul 40. Modelul modificat al fișei de evaluare a securității	187

LISTA ANEXELOR

Anexa 1. Structura standardului de securitate ISO/IEC 17799:2005	211
Anexa 2. Structura controalelor de securitate NIST	216
Anexa 3. Fișa de evaluare a securității și indicatorii agregați pentru măsurile inițiale	227
Anexa 4. Rezultatele analizei de risc	230
Anexa 5. Fișa de evaluare și indicatorii agregați pentru cele 120 măsuri de securitate care ar trebui implementate	237
Anexa 6. Fișa de evaluare și indicatorii agregați pentru măsurile de securitate care vor fi implementate (selectate conform Principiului lui Pareto)	245
Anexa 7. Fișa de evaluare a securității și indicatorii agregați după implementarea celor 23 măsuri de securitate	247
Anexa 8. Fișa de evaluare a securității și indicatorii agregați după efectuarea auditului de securitate	255
Anexa 9. Fișa de evaluare a securității și indicatorii agregați în urma scanării sistemului informatic	265
Anexa 10. Fișa de evaluare a securității și indicatorii agregați în urma testării sistemului de securitate	275
Anexa 11. Fișa de evaluare a securității și indicatorii agregați în urma unui eveniment de securitate	285

CUVINTE CHEIE: amenințare, analiza protecție-preț-performanță, bun informațional, cadru de lucru SERIOS, contramăsură de securitate, evaluarea securității, fișa cu indicatori agregați, metode de calcul a costurilor și cheltuielilor de securitate, model de securitate, nivel de maturitate, prioritizarea securității, program de securitate, sistem de metrici de securitate, sistem de securitate a informației, vulnerabilitate

INTRODUCERE

Orice organizație este interesată de protejarea bunurilor informaționale deținute (informațiile și infrastructura asociată). În multe organizații, acestea sunt considerate resurse critice, întrucât existența organizației depinde de modul în care ele sunt protejate. Din acest motiv sunt alocate și cheltuite sume mari de bani pentru îmbunătățirea securității lor, însă rezultatele nu sunt întotdeauna cele așteptate.

În orice organizație, categorii diferite de persoane au interese, motive și percepții diferite despre ceea ce înseamnă securitatea informației, iar securitatea *are un înțeles diferit pentru aceste persoane* (Brotby, 2009: XVIII). *Un element cheie care afectează difuzarea unei inovații sau tehnologii noi la nivelul unei organizații este modul în care ea este acceptată la nivel individual* (Mihuț și Tomai, 2009: 43).

În aceste condiții, problematica securității informației trebuie abordată dintr-o perspectivă multidisciplinară și trebuie creat un limbaj comun al securității. Măsurile tehnice nu sunt suficiente pentru asigurarea securității informației, *multe din probleme putând fi explicate mai clar și convingător prin utilizarea limbajului microeconomiei* (Anderson, 2001: 1). Această idee este întărită și de alți autori care precizează că *scopul este de a transforma securitatea informației într-un domeniu multidisciplinar în care specialiștii în tehnologie vor lucra împreună cu experții în „probleme sensibile“ cum ar fi politici publice, economie și sociologie* (Shostack și Stewart, 2008: 103). Știința care va cerceta acest domeniu de studiu multidisciplinar se va numi *Economia Securității Informației*, iar o metodă principală de lucru va fi *aplicarea ideilor din alte domenii* (Shostack și Stewart, 2008: 103).

Lucrarea de față își propune abordarea multidisciplinară a securității atât din perspectivă economică și managerială, cât și din perspectivă tehnică (informatică), precum și stabilirea modalităților prin care metode și instrumente din alte domenii, pot fi utilizate în domeniul securității.

Obiectivul principal al lucrării este conceperea unui model de securitate, precum și proiectarea cadrului de lucru (*framework*), care să implementeze sistemul de securitate bazat pe modelul conceput.

Oportunitatea și motivația lucrării

Lucrarea își propune extinderea ariei de cercetare în domeniul securității informației, prin explorarea unor zone comune cu alte domenii, cum ar fi: managementul, informatica sau contabilitate (costuri și cheltuieli). Abordarea multidisciplinară este necesară datorită faptului că securitatea informației nu poate fi asigurată numai cu mijloace tehnice, precum și datorită faptului că în orice organizație trebuie creat un “limbaj comun al securității” și trebuie puse de acord interesele unor categorii diverse de personal.

Oportunitatea lucrării este dată de necesitatea creării unor sisteme de securitate mai eficiente (din perspectiva costurilor și cheltuielilor), mai eficace (din perspectiva protecției asigurate), care să asigure suport pentru luarea deciziilor (din perspectiva managerială) și care să nu afecteze performanțele sistemelor informatice (din perspectiva tehnică).

Punctul de plecare al lucrării l-au constituit cercetările științifice făcute de către autor, cu ocazia studiilor de masterat. Alegerea temei de cercetare s-a făcut ca urmare a unor preocupări profesionale ale autorului în domeniul administrării sistemelor informatice, din ultimii 18 ani.

Obiectivele lucrării

În cadrul lucrării am urmărit unele concepte, probleme și elemente din domeniul securității informației. Obiectivele urmărite sunt:

- Conceperea unui model de securitate adaptat situației actuale și dimensiunilor organizațiilor din țara noastră, care să poată fi folosit pentru crearea unui sistem de securitate propriu organizației sau pentru pregătirea organizației în vederea obținerii unei certificări în domeniul securității;
- Proiectarea unui cadru de lucru care să poată fi utilizat pentru implementarea unui sistem de securitate bazat pe modelul propus și care să asigure securitatea informației într-un timp cât mai scurt și cu un consum cât mai redus de resurse;

- Aplicarea sau adaptarea unor idei și elemente din alte domenii, crearea unor instrumente de lucru noi și includerea acestora în cadrul de lucru;
- Studierea domeniului securității printr-o analiză multidisciplinară, pentru a identifica zonele care pot fi îmbunătățite sau modificate în acest domeniu.

Structura lucrării

Conținutul lucrării este dezvoltat pe parcursul a șapte capitole.

În primele două capitole am examinat aria de cercetare (domeniul securității informației), cu scopul de a identifica principalele elemente conceptuale și structurale din domeniu și de a dimensiona și poziționa modelul de securitate care face obiectul tezei. Am analizat modelele și sistemele de securitate existente, precum și particularitățile securității informației în câteva domenii noi ale informaticii. La sfârșitul celor două capitole am prezentat concluziile generale și direcțiile de cercetare pe care le-am urmat pe parcursul celorlalte capitole.

În capitolul trei am analizat managementul de risc, deoarece este principalul proces în managementul securității. Am elaborat *Cataloagele generice* de amenințări și vulnerabilități, pentru utilizarea lor în cadrul modelului de securitate. Am studiat comparativ metodele de evaluare a riscului, pentru a stabili modul în care ele pot fi utilizate într-un studiu de caz prezentat în lucrare. Pentru etapa de tratare a riscului din cadrul managementului de risc, am întocmit un *Catalog generic de măsuri de securitate*, care a fost folosit în cadrul de lucru descris în capitolul șapte.

În capitolul patru am analizat două modele de calcul a costurilor și cheltuielilor indirecte, precum și motivele pentru care fiecare dintre aceste modele nu este suficient pentru calcularea costurilor și cheltuielilor de securitate. Pe baza analizei, am propus o metodă de calcul combinată. Verificarea metodei de calcul am făcut-o prin intermediul unui studiu de caz.

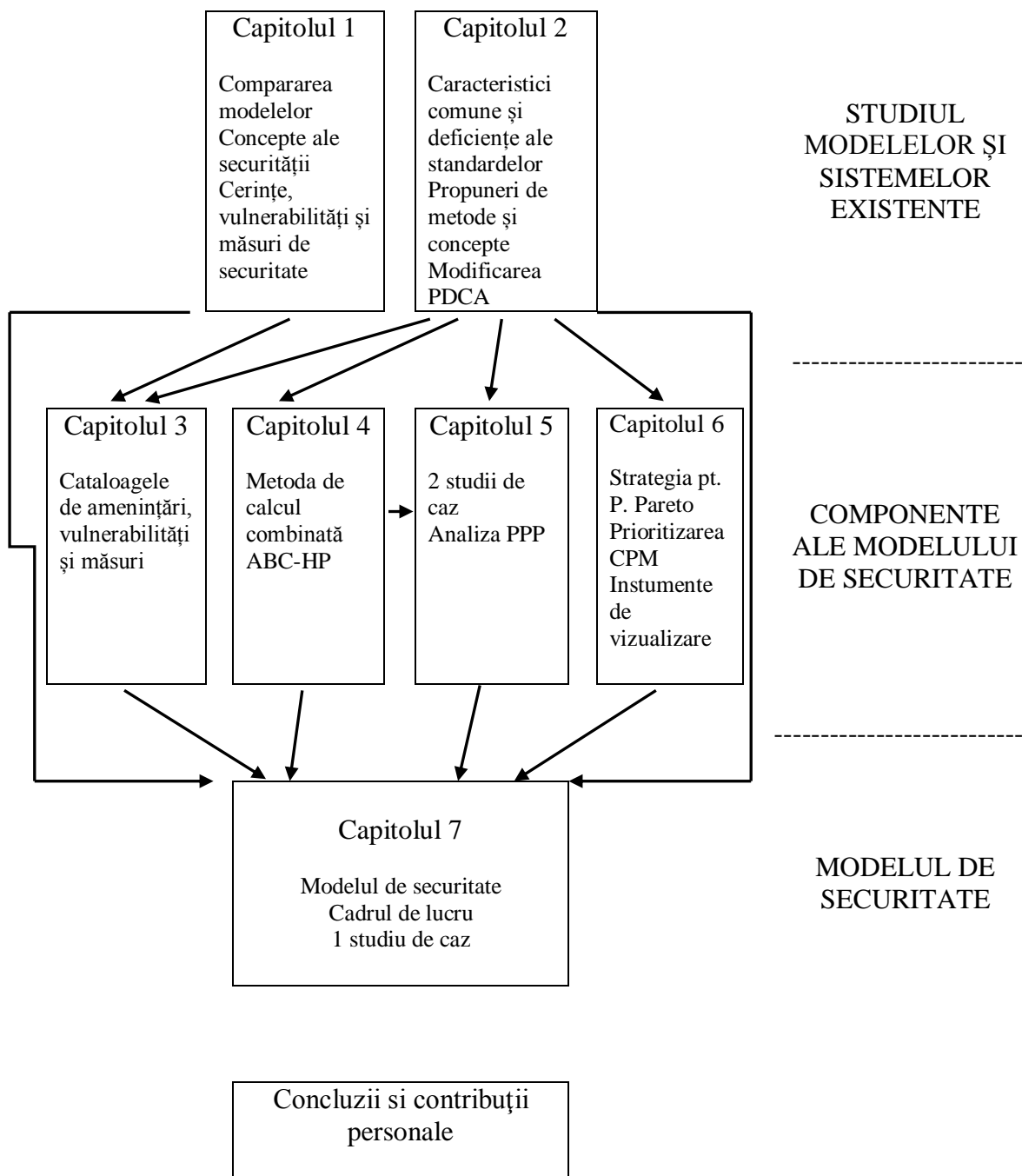
În capitolul cinci, prin intermediul unui studiu de caz, am prezentat pașii necesari pentru utilizarea metodei de calcul combinată propusă în capitolul patru. De asemenea, am propus extinderea metodei de analiză cost-beneficiu (utilizată în deciziile privind implementarea unor măsuri de securitate) cu o metodă de analiză în

care se ia în calcul și factorul tehnic (performanța). Prezentarea acestei metode s-a făcut în cadrul unui studiu de caz. Metodele prezentate în cele două studii de caz vor putea fi utilizate ca și instrumente de lucru ale cadrului de lucru prezentat în capitolul șapte.

În capitolul șase am prezentat modul în care concepte, metode și principii din alte domenii pot fi aplicate în domeniul securității. De asemenea, am prezentat instrumentele de lucru specifice securității (metrici de securitate, instrumente vizuale) și elementele specifice unui sistem de management (documentațiile de securitate), care vor fi utilizate în cadrul de lucru SERIOS.

În capitolul șapte am prezentat modelul de securitate propus în lucrare și cadrul de lucru prin intermediul căruia se poate implementa un sistem de securitate bazat pe acest model. Validarea cadrului de lucru s-a făcut prin intermediul unui studiu de caz, care este prezentat în cuprinsul capitolului.

Structura lucrării și contribuțiile personale sunt prezentate în figura următoare:



CONCLUZII ȘI CONTRIBUȚII PERSONALE

Abordarea problematicii securității trebuie făcută dintr-o perspectivă multidisciplinară, întrucât securitatea nu poate fi rezolvată numai prin tehnologie.

Modelul de securitate este adaptat situației actuale, întrucât se poate implementa pe un sistem informatic operațional, utilizând resursele proprii ale organizației

Cadrul de lucru care implementează acest model de securitate nu se focalizează pe obținerea unei certificări, ci urmărește dezvoltarea unui sistem și a unor procese de securitate care să fie integrate în procesele organizației.

Sistemul de metrice de securitate și instrumentele manageriale care fac parte din cadrul de lucru oferă suport în luarea deciziilor, permițând eficientizarea activităților de securitate.

Sistemul de metrice propus permite trecerea de la o abordare a securității bazată pe măsuri reactive la o securitate bazată pe măsuri preventive.

Contribuții personale

În primul capitol am prezentat aspectele teoretice ale modelelor de securitate. Contribuția noastră la acest capitol a fost o analiză a acestor modele și exprimarea opiniilor proprii în legătură cu acestea. De asemenea, am identificat particularități referitoare la cerințele de securitate, vulnerabilități și metodele de securizare din următoarele domenii: sisteme colaborative, ubiquitous computing și web-services.

În al doilea capitol am analizat sistemele de management utilizate pentru administrarea (gubernanța IT) și sistemele de management a securității ISO și NIST. Contribuția noastră la acest capitol a fost o analiză **multidisciplinară** a elementelor structurale și conceptuale ale sistemelor de securitate a informației, precum și exprimarea unor opinii proprii.

În capitolul trei am analizat principalele elemente și etape ale procesului de management a riscului. Contribuția noastră la acest capitol a fost stabilirea condițiilor în care pot fi utilizate metodele de evaluare a riscului, precum și elaborarea unor *Cataloge generice* de amenințări, vulnerabilități și măsuri de securitate.

În capitolul patru am analizat două metode de calcul a costurilor care pot fi aplicate pentru calcularea costurilor și cheltuielilor de securitate și anume: modelul de cost propus de HP Laboratories și metoda ABC. Contribuția noastră la acest capitol a fost stabilirea condițiilor în care pot fi aplicate aceste metode, precum și identificarea unei *Metode combinate de calcul ABC-HP*, pentru calcularea precisă a unor costuri și cheltuieli de securitate. Verificarea preciziei metodei s-a făcut prin aplicarea ei pentru calcularea costului unui serviciu informatic și compararea rezultatului cu rezultatul obținut prin estimarea aceluiași cost cu ajutorul modelului Krasner, descris la subcapitolul 4.5. Diferența mai mică de 10% dintre cele două rezultate ne-a permis să concluzionăm faptul că metoda combinată este precisă, putând fi utilizată pentru calcularea unor costuri și cheltuieli de securitate.

În capitolul cinci am prezentat două studii de caz proprii care abordează problematica securității organizației dintr-o perspectivă multidisciplinară. Contribuția noastră la acest capitol a fost argumentarea necesității abordării multidisciplinare a securității, prezentarea pașilor *Metodei combinate de calcul ABC-HP*, precum și conceperea unei *Metode de analiză tridimensională a impactului măsurilor de securitate asupra sistemului informatic al unei organizații*.

În capitolul șase am prezentat elementele, metodele și principiile preluate din alte domenii, pe care le-am utilizat în modelul de securitate și în cadrul de lucru din lucrare. Contribuția noastră la acest capitol a fost stabilirea modului de aplicare a Principiului lui Pareto și a Metodei Drumului Critic în domeniul securității. De asemenea, am propus modalitatea de utilizare a Reguli 1-10-100 în domeniul securității și am creat un instrument vizual - *graful stării de securitate*, ce a fost inclus ca instrument al cadrului de lucru.

În capitolul șapte am descris modelul de securitate care a făcut obiectul acestei lucrări, precum și cadrul de lucru SERIOS, care este instrumentul de implementare a sistemului de securitate bazat pe acest model. La subcapitolul 7.6 am prezentat un studiu de caz prin intermediul căruia am utilizat cadrul de lucru în cadrul unei companii. Contribuția noastră la acest capitol a fost *descrierea modelului și cadrului de lucru*, prezentarea elementelor conceptuale și structurale ale acestora, descrierea modelului de organizare a proceselor PIV, descrierea și *formalizarea sistemului de metrice de securitate*, introducerea conceptului de *bun informațional* și interpretarea

rezultatelor studiului de caz.

Diseminarea rezultatelor

Ideile prezentate în capitolele 1 și 6, precum și studiile de caz din capitolele 4, 5 și 7 au fost diseminate în lucrări științifice publicate în reviste din București și Suceava, precum și în volumele unor conferințe internaționale și din țară.

Articole științifice publicate în volumele unor conferințe internaționale

1. MiHuț, M., și Tomai, N. (2009) *Analysis of Collaborative Systems Security Using a Three-criteria Approach: Protection, Price and Performance*, International Technology, Education and Development Conference (INTED2009), published by International Association of Technology, Education and Development (IATED), pp. 3400-3409.
2. MiHuț, M., Arba, R. și Tomai, N. (2009) *Using Data-Mining Solution for Diagnosing Systems*, Conferența Engenharia2009, Corvilha, Portugalia.
3. MiHuț, M., Arba, R., Vereș, O și Tomai, N. (2009) *Centre-based Cost Analyze for Virtual IT Companies*, Conferența Engenharia2009, Corvilha, Portugalia.

Articole științifice publicate în volumele unor conferințe din țară

1. MiHuț, M. (2006) *TrustCoM – a Security Model for Collaboration Systems*, Annals of the “Tiberiu Popoviciu” Seminar, Supplement: International Workshop in Collaborative Systems, vol. 4, 2006, pp. 195-202.
2. MiHuț, M. (2007) *Integrating Knowledge Management and e-Learning*, Proceedings of the International Conference on Knowledge Engineering, Principles and Techniques, KEPT2007, Cluj-Napoca (Romania), vol. II, pp. 73–77
3. MiHuț, M. (2007) *TENCompetence – an Infrastructure for Knowledge Management*, Proceedings of the International Conference Competitiveness and European Integration, vol. Business Information Systems & Collaborative Support Systems in Business, pp. 227-229.
4. MiHuț, M. (2008) *Aspects of Ubiquitous Computing Security*, Annals of the “Tiberiu Popoviciu” Seminar, Supplement: Romanian Workshop on Mobile Business, vol. 6, 2008, pp. 71-77.
5. MiHuț, M. (2009) *Prioritization of IT Security Activities*, 16th International Economics Conference “Industrial Revolutions, From the Globalization and Post-

- Globalization Perspective ”– IECS 2009, Sibiu, vol. 5, pp. 138-143.
6. Mihaș, M., și Tomai, N. (2009) *Theoretical Aspects of Diffusion in IT Domain*, Studia Universitas “Babeș-Bolyai” Informatica series, Proceedings of the International Conference on Knowledge Engineering, Principles and Techniques - KEPT 2009, Cluj-Napoca, vol. III – Special Issue 2009, pp. 43-46.
 7. Mihaș, M. (2014) *Security Measurement and Visualization: a New Approach*, Proceedings of the 13th International Conference on Informatics in Economy IE2014, pp. 490-495.

Articole științifice publicate în reviste din țară

8. Mihaș, M. (2008) *Analyzing Log Files Using Data-Mining*, Journal of Applied Computer Science, issue 4 / 2008, pp. 32-34.
9. Mihaș, M., Todor, L.S. (2009) *Aspecte ale Securității Web-services*, Calitatea – Acces la Succes magazine, Proceedings of the International Conference “Sustainable Development in Conditions of Economic Instability”, vol. 10, nr. 101 special / 2009, partea a II-a, Editura Cibernetica MC, București, pp. 122-124.
10. Mihaș, M., Todor, L.S. (2010) *Strategia de Aplicare a Principiului lui Pareto în Managementul Securității*, Quality – Access to Success magazine, Proceedings of the International Conference “Sustainable Development in Conditions of Economic Instability”, vol. 11, nr. 113 special / 2010, Editura Cibernetica MC, București, pp. 546-560
11. Mihaș, M., și Tomai, N. (2010) *A Cost Model for the IT Department* Journal of Applied Quantitative Methods, vol. 5, nr. 2 / 2010, pp. 358-366.

Perspective

Cadrul de lucru poate fi implementat de organizațiile care nu își permit costurile implementării unor sisteme de management a securității certificate. El poate fi utilizat atât pentru implementarea unui sistem de securitate propriu, cât și pentru pregătirea organizației în vederea implementării unor standarde de securitate.

Unele elemente ale cadrului de lucru (matricea de risc, nivelurile de maturitate, nivelurile de categorisire) utilizează o scală de evaluare cu trei trepte. Pentru creșterea performanței sistemului de securitate pot fi utilizate scale cu mai multe trepte.

Cadrul de lucru poate fi extins astfel încât să fie utilizat în domenii cum ar fi: managementul cunoștințelor, sisteme colaborative și organizații virtuale.

În analiza multidimensională a securității mai poate fi adăugată o dimensiune legată de modul în care este percepută securitatea la nivel individual, în cadrul unei organizații.

BIBLIOGRAFIE

1. Anderson, R. (2001) *Why Information Security is Hard - An Economic Perspective*, University of Cambridge Computer Laboratory, disponibil la <http://www.acsac.org/2001/papers/110.pdf>, accesat la 20/10/2011.
2. Arens, A.A., Loebbecke, J.K. (2003), *Audit. O abordare integrată*, Editura ARC, Chişinău, Moldova.
3. Arnason, S.T., Willett, K.D. (2008) *How to achieve 27001 certification: an example of applied compliance management*, Auerbach Publications, Boca Raton FL, USA.
4. Bell, D.E., LaPadula, L.J. (1973) *Secure Computer Systems, Mathematical Foundation*, The Mitre Corporation, Bedford MA, USA.
5. Bell, D.E., LaPadula, L.J. (1976) *Secure computer system: unified exposition and Multics interpretation*, The Mitre Corporation, Bedford MA, USA.
6. Biba, K.J. (1977) *Integrity Considerations for Secure Computer Systems*, Technical Report MTR-3153 rev. 1, The Mitre Corporation, Bedford, MA., USA
7. Boehm, B. (1987) *Industrial Metrics Top 10 List*, *IEEE Software*, sept. 1987, pp. 84-85.
8. Boehm, B. and Basili, V.R. (2001) *Software Defect Reduction Top 10 List*, *IEEE Computer*, vol. 34, nr. 1, ianuarie 2001, pp. 135-137.
9. Brewer, D.F.C., Nash, M.J. (1989) *The Chinese wall security policy*, The IEEE Symposium on research in security and privacy, pp. 206-214, Oakland CA, USA.
10. Brody, W.K. (2009) *Information security management metrics: a definitive guide to effective security monitoring and measurement*, Taylor & Francis Group, Boca Raton FL, USA.
11. Chakrabarti, A. (2007) *Grid computing security*, Springer-Verlag Berlin Heidelberg, Germania.
12. Clark, D.D., Wilson, D.R. (1987) *A Comparison of Commercial and Military Computer Security Policies*, Proceedings of the 1987 IEEE Symposium on Research in Security and Privacy (SP'87), IEEE Press, pp. 184–193, Oakland CA, USA
13. CMMI (2010) *CMMI for Development, version 1.3*, Software Engineering Institute, disponibil la <http://www.sei.cmu.edu/reports/10tr033.pdf>, accesat la 30/08/2013.

14. CNSS Instruction no. 4009 (2010) *National Information Assurance (IA) Glossary*, Committee on National Security Systems, disponibil la http://www.ncix.gov/publications/policy/docs/CNSSI_4009.pdf, accesat la 22/11/2011.
15. COBIT 4.1 (2007) *Framework, Control Objectives, Management Guidelines, Maturity Models*, IT Governance Institute, disponibil la <http://www.isaca.org/Knowledge-Center/cobit/Pages/Downloads.aspx>, accesat la 13/10/2011.
16. COBIT (2008) *Aligning CobiT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit*, IT Governance Institute, disponibil la <http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Aligning-COBIT-4-1-ITIL-V3-and-ISO-IEC-27002-for-BusinessBenefit.aspx>, accesat la 20/10/2011.
17. CRAMM (2005) *The Logic behind CRAMM's Assessment of Measures of Risk and Determination of Appropriate Countermeasures*, Insight Consulting, disponibil la [http://www.cramm.com/files/techpapers/CRAMM%20 Countermeasure%20Determination%20and%20Calculation.pdf](http://www.cramm.com/files/techpapers/CRAMM%20Countermeasure%20Determination%20and%20Calculation.pdf), accesat la 15/01.2010.
18. Dorfman, M.S. (1997) *Introduction to Risk Management. and Insurance* (6th ed.). Prentice Hall Inc., Upper Saddle River NJ, USA.
19. Fătăcean, Gh. (2006) *Contabilitatea managerială și Controlul de gestiune*, Editura Alma Mater, Cluj-Napoca, România.
20. Granof, M. H., Platt D. E. și Vaysman, I. (2000) *Using Activity-Based Costing to Manage More Effectively*, University of Texas at Austin, disponibil la <http://www.businessofgovernment.org/sites/default/files/ABC.pdf>, accesat la 11/12/2007.
21. Hayat, M. Z., Reeve, J. S. și Boutle, C. J. (2006) *Prioritisation of Network Security Services*, IEE Journal of Information Security, 153 issue 2, pp. 43-50.
22. Hayat, M. Z., Reeve, J. S. și Boutle, C. (2006) *Dynamic Threat Assessment for Prioritising Computer Network Security*, 5th European Conference on Information Warfare and Security, Helsinki, Finland.
23. IBM Corporation și Microsoft Corporation (2001), *Security in a Web Services World: A Proposed Architecture and Roadmap*, disponibil la adresa: www.ibm.com/developerworks/library, accesat la 10/06//2009.
24. ISO/IEC 17799 (2005) *Tehnologia informației – Tehnici de securitate – Cod de practică pentru managementul securității informațiilor*, International Organization

- for Standardization.
25. ISO/IEC 27001 (2005), *Tehnologia informației – Tehnici de securitate – Sisteme de management a securității informației – Cerințe*, International Organization for Standardization.
 26. ISO 31000 (2009) *Risk management – Principles and guidelines*, International Organization for Standardization.
 27. Ivan, I. și Toma, C. (2006) *Information Security Handbook*, Academy of Economic Studies Publishing House, București, România.
 28. Jaquith, A. (2007) *Security Metrics: replacing fear, uncertainty and doubt*, Pearson Education Inc., Upper Saddle River NJ, USA.
 29. Jones, A.K. (1978) *Protection Mechanism Models: Their Usefulness*, Foundations of Secure Computing, Academic Press, New York NY, USA, pp. 237-254.
 30. Juran, J.M. (1973) *Calitatea produselor*, Editura Tehnică, București, România.
 31. Kagal, L., Finn, T. și Joshi, A. (2001) *Moving from Security to Distributed Trust in Ubiquitous Computing Environments*, University of Maryland, IEEE Computer, vol. 34, no. 12 December, pp. 154-157.
 32. Kaplan, R. S. și Bruns, W. (1987) *Accounting and Management: A Field Study Perspective*, Harvard Business School Press.
 33. Kaplan, R.S. și Norton, D.P. (1992) *The Balanced Scorecard: Measures That Drive Performance*, Harvard Business Review, ianuarie-februarie 1992, pp. 71-79.
 34. Karapetrovic, S. (2008) *Integrative Augmentation of Standardized Management Systems*, International Journal for Quality research, volumul 2, numărul 1, 2008, disponibil la <http://www.ijqr.net/journal/v2-n1/2.pdf>, accesat la 29/04/2014.
 35. Krasner, J. (2003) *Total Cost of Development: A comprehensive cost estimation framework for evaluation embedded development platform*, Embedded Market Forecasters, disponibil la <http://www.embeddedforecast.com/EMFTCD2003v3.pdf>, accesat la 24/09/2009.
 36. Landoll, J. L. (2006) *The Security Risk Assessment Handbook: a Complete Guide for Performing Security Risk Assessments*, Auerbach Publications, Boca Raton FL, USA.
 37. Landoll, J. L. (2006) *The Security Risk Assessment Handbook: a Complete Guide for Performing Security Risk Assessments*, Auerbach Publications, Boca Raton FL, USA.
 38. Langheinrich, M. (2001) *Privacy By Design - Principles of Privacy-Aware*

- Ubiquitous Systems*, UbiComp'01 Proceedings of 3rd International Conference on Ubiquitous Computing, Springer-Verlag, London, UK, pp. 273-291.
39. Lipton, R.J. și Snyder, L. (1977) *A Linear Time Algorithm for Deciding Subject Security*, Journal of the Association for Computing Machinery (Addison-Wesley) volume 24 no. 3, pp. 455–464.
 40. Magiera, J. și Pawlak, A. (2005) *Security frameworks for virtual organizations (capitol în cartea Virtual Organizations: Systems and Practices, pp. 133 – 148)*, Springer US, Boston MA, USA.
 41. Marty, R (2009) *Applied Security Visualization*, Pearson Education Inc., Boston MA, USA.
 42. Mihuț, M. (2006) *TrustCoM – a Security Model for Collaboration Systems*, Annals of the “Tiberiu Popoviciu” Seminar, Supplement: International Workshop in Collaborative Systems, vol. 4, 2006, pp. 195-202.
 43. Mihuț, M. (2007) *Integrating Knowledge Management and e-Learning*, Proceedings of the International Conference on Knowledge Engineering, Principles and Techniques, KEPT2007, Cluj-Napoca (Romania), vol. II, pp. 73–77
 44. Mihuț, M. (2007) *TENCompetence – an Infrastructure for Knowledge Management*, Proceedings of the International Conference Competitiveness and European Integration, vol. Business Information Systems & Collaborative Support Systems in Business, pp. 227-229.
 45. Mihuț, M. (2008) *Aspects of Ubiquitous Computing Security*, Annals of the “Tiberiu Popoviciu” Seminar, Supplement: Romanian Workshop on Mobile Business, vol. 6, 2008, pp. 71-77.
 46. Mihuț, M. (2008) *Analyzing Log Files Using Data-Mining*, Journal of Applied Computer Science, issue 4 / 2008, pp. 32-34.
 47. Mihuț, M., și Tomai, N. (2009) *Analysis of Collaborative Systems Security Using a Three-criteria Approach: Protection, Price and Performance*, International Technology, Education and Development Conference (INTED2009), published by International Association of Technology, Education and Development (IATED), pp. 3400-3409.
 48. Mihuț, M. (2009) *Prioritization of IT Security Activities*, 16th International Economics Conference “Industrial Revolutions, From the Globalization and Post-Globalization Perspective” – IECS 2009, Sibiu, vol. 5, pp. 138-143
 49. Mihuț, M., Todor, L.S. (2009) *Aspecte ale Securității Web-services*, Calitatea –

- Acces la Succes magazine, Proceedings of the International Conference “Sustainable Development in Conditions of Economic Instability”, vol. 10, nr. 101 special / 2009, partea a II-a, Editura Cibernetica MC, București, pp. 122-124.
50. Mihaș, M., și Tomai, N. (2009) *Theoretical Aspects of Diffusion in IT Domain*, Studia Universitas “Babeș-Bolyai” Informatica series, Proceedings of the International Conference on Knowledge Engineering, Principles and Techniques - KEPT 2009, Cluj-Napoca, vol. III – Special Issue 2009, pp. 43-46
 51. Mihaș, M, Arba, R. și Tomai, N. (2009) *Using Data-Mining Solution for Diagnosing Systems*, Conferența Ingineria 2009, Corvilha, Portugalia
 52. Mihaș, M, Arba, R., Vereș, O și Tomai, N. (2009) *Centre-based Cost Analyze for Virtual IT Companies*, Conferența Ingineria 2009, Corvilha, Portugalia
 53. Mihaș, M., Todor, L.S. (2010) *Strategia de Aplicare a Principiului lui Pareto în Managementul Securității*, Quality – Access to Success magazine, Proceedings of the International Conference “Sustainable Development in Conditions of Economic Instability”, vol. 11, nr. 113 special / 2010, Editura Cibernetica MC, București, pp. 546-560
 54. Mihaș, M., și Tomai, N. (2010) *A Cost Model for the IT Department* Journal of Applied Quantitative Methods, vol. 5, nr. 2 / 2010, pp. 358-366.
 55. Mihaș, M. (2014) *Security Measurement and Visualization: a New Approach*, Proceedings of the 13th International Conference on Informatics in Economy IE2014, pp. 490-495.
 56. Mirams, M., McElheron, P. (1999) *Certificarea ISO 9000*, Editura Teora, București, România.
 57. Mușiu, A.I. (2007) *Control de gestiune: suport de curs*, Editura Risoprint, Cluj-Napoca, România.
 58. NIST Interagency Report (IR) 7298 Revision 2 (2013) *Glossary of Key Information Security Terms*, US Department of Commerce, disponibil la <http://csrc.nist.gov/publications/PubsNISTIRs.html>, accesat la 27/06/2013.
 59. NIST Special Publication 800-30 Revision 1 (2002), *Risk Management Guide for Information Technology Systems*, US Department of Commerce, disponibil la <http://csrc.nist.gov/publications/PubsSPs.html>, accesat la 27/01/2009.
 60. NIST Special Publication 800-53 Revision 3 (2009) *Recommended Security Controls for Federal Information Systems and Organizations*, US Department of Commerce, disponibil la <http://csrc.nist.gov/publications/PubsSPs.html>, accesat la

04/07/2010.

61. NIST Special Publication 800-37 Revision 1 (2010) *Guide for Applying the Risk Management Framework to Federal Information Systems*, US Department of Commerce , disponibil la <http://csrc.nist.gov/publications/PubsSPs.html>, accesat la 12/04/2011.
62. Olaru, M., Isaic-Maniu, A., Lefter, V., Pop, N.A., Popescu, S., Drăgulănescu, N., Roncea, L., Roncea, C. (2000) *Tehnici și instrumente utilizate în managementul calității*, Editura Economică, București, România.
63. Oprea, D. (2007) *Protecția și securitatea informațiilor*, Editura Polirom, Iași, România.
64. Patel, C.D. și Shah, A.J. (2005) *Cost Model for Planning, Development and Operation of a Data Center*, HP Laboratories Palo Alto, Technical Report HPL-2005-107(R.1), disponibil la http://www.hpl.hp.com/techreports/2005/HPL-2005-107R1.html?jumpid=reg_R1002_USEN, accesat la 10/12/2006.
65. PITAC President's Information Technology Advisory Committee (2005) *Cyber Security: A Crisis of Prioritization*, disponibil la http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf, accesat la 03/01/2012.
66. Pattinson, F. (2011) *Security assurance: contrasting FISMA and ISO/IEC 27001*, disponibil la http://www.atsec.com/downloads/documents/FISMA_27001.pdf, accesat la 10/04/2012.
67. Pfleeger, C.P., Pfleeger, S.L. (2003) *Security in Computing*, Prentice Hall, Upper Saddle River NJ, USA.
68. Ritter, T. (2007) *Reaching Out to Protect Within: Comparing and Contrasting ISO 27002/27002 and NIST Special Publication 800-Series information security standard*, IT Compliance Journal, volumul 2, numărul 2, 2007, disponibil la http://download.101com.com/pub/itci/Files/ITCi_Journal_V2N2_07Q3_Web_Final_a.pdf, accesat la 10/04/2012.
69. Rooney, P. (2002) *Microsoft's CEO: 80-20 Rule Applies to Bugs, Not Just Features*, disponibil la <http://www.crn.com/news/security/18821726/microsofts-ceo-80-20-rule-applies-to-bugs-not-just-features.htm>, accesat la 14/06/2010.
70. Schneier, B. (2008) *Security ROI*, disponibil la http://www.schneier.com/blog/archives/2008/09/security_roi_1.html, accesat la 01/02/2009.

71. Seigneur, J.M., Farrell, S. și Damsgaard J.C. (2003) *Distributed Systems Group*, Department of Computer Science, Trinity College, Dublin 2, Ireland.
72. Shostack, A. și Stewart, A. (2008) *The New School of Information Security*, Pearson Education Inc., Boston MA, USA.
73. Smith, M. L., Erwin, J, (2005) *Role & Responsibility Charting (RACI)*, disponibil la http://myclass.peelschools.org/sec/12/4268/Resources/RACI_R_Web3_1.pdf, accesat la 10/06/2012.
74. Stajano, F. (2002) *Security for Ubiquitous Computing*, John Wiley & Sons Ltd., West Sussex, England.
75. Vișan, A., Ionescu, N., (2009) *Managementul Calității – Pentru uzul studenților*, partea a doua, capitolul 8, Universitatea Politehnica din București, Catedra TCM, București, România, disponibil la http://www.aurelvisan.ro/attachments/098_MC_Rez_Cap.%2008_Guru%20Calit.pdf, accesat la 12/06/2010.
76. Wagealla, W., English, C., Terzis, S., Nixon Paddy, L.H. și McGettrick, A. (2004) *A Trust-based Collaboration Model for Ubiquitous Computing*, Department of Computer and Information Sciences University of Strathclyde, Glasgow, Scotland, 2004.
77. Weiser, M. (1991) *The Computer for the 21st Century*, Scientific American Magazine, September 1991, pp. 94-104.
78. http://www.opnet.com/university_program/itguru_academic_edition/
79. <http://hadm.sph.sc.edu/Courses/J716/CPM/CPM.html>
80. <http://hspm.sph.sc.edu/Courses/J716/CPM/Pathfind.html>