

CUPRINS

	Prefața	15
1	Societatea informațională – societatea cunoașterii	17
1.1	Caracteristici definitorii	17
1.2	Strategii și programe europene privind societatea informațională	25
1.3	Directive ale Comisiei Europene privitoare la societatea informațională	31
1.4	Societatea informațională și globalizarea	35
2	Noțiunea de securitate informatică	41
2.1	Noțiuni introductive	41
2.2	Definiții ale noțiunii de securitate informatică	43
3	Vulnerabilități, amenințări și riscuri în securitatea informatică	49
3.1	Noțiuni introductive	49
3.2	Conceptele de vulnerabilitate, amenințare și risc	49
3.3	Clase de vulnerabilități, amenințări și riscuri	50
3.3.1	Clasificarea ca listă de termeni	50
3.3.1.1	Interceptarea radiațiilor	51
3.3.1.2	Interceptarea informațiilor introduse de la tastatură	53
3.3.1.3	Interceptarea pachetelor	54
3.3.1.4	Deturnarea sesiunii	62
3.3.1.5	Falsificarea adresei expeditorului	62
3.3.1.6	Simularea hiperconexiunilor și simularea Web	63
3.3.1.7	Interceptarea parolelor	70
3.3.1.8	Virusii	71
3.3.1.9	Viermi	89
3.3.1.10	Bombele logice	92
3.3.1.11	Caii troieni	92
3.3.1.12	Hărțuirea	93
3.3.1.13	Mascarea	93
3.3.1.14	Degradarea serviciului	95
3.3.1.15	Refuzarea serviciului	95
3.3.1.16	Pirateria software	95

3.3.1.17	Copierea neautorizată de date	96
3.3.1.18	Uși ascunse	96
3.3.1.19	Privilegii excesive	96
3.3.1.20	Distrugerea datelor	96
3.3.1.21	Frauda informatică	97
3.3.1.22	Amenințări în domeniul telecomunicațiilor	100
3.3.2	Clasificarea ca listă de categorii	102
3.3.3	Clasificarea definită pe baza categoriilor de rezultate	103
3.3.4	Clasificarea ca liste empirice	103
3.3.5	Clasificarea conform Legii 161/2003, publicată în Monitorul Oficial al României numărul 27 din 21.04.2003	104
4	Agenți de amenințare în criminalitatea informatică	105
4.1	Categorii de agenți de amenințare	105
4.2	Hackerii	109
4.3	Crima organizată	121
4.4	Teroriștii, sau extremiștii ideologici și politici	122
4.5	State care sponsorizează agresiuni cibernetice	129
5	Tehnici și mijloace fundamentale de protecție împotriva amenințărilor informatice	137
5.1	Defectări, defecte și erori în sistemele de calcul	137
5.1.1	Noțiunile de defectare, defect și eroare	137
5.1.2	Noțiunile de detecție și localizare a defectelor	143
5.2	Sisteme de calcul tolerante la defectări	148
5.2.1	Considerații generale privind toleranța la defectări	148
5.2.1.1	Noțiuni introductive	148
5.2.1.2	Necesitatea toleranței la defectări	149
5.2.1.3	Caracterizare generală a metodelor și tehnicilor utilizate pentru implementarea toleranței la defectări	151
5.2.1.4	Scurt istoric al perfecționării metodelor, tehnicilor, structurilor și arhitecturilor sistemelor de calcul tolerante la defectări	152
5.2.2	Detecția și localizarea defectelor în sistemele de calcul tolerante la defectări	164
5.2.2.1	Noțiuni introductive	164
5.2.2.2	Clase generale de teste utilizate în sistemele tolerante la defectări	165
5.2.2.3	Structuri autotestabile	167
5.2.2.4	Procesoare de testare	170
5.2.2.4.1	Procesorul de testare și reparare al sistemului JPL-STAR	172

5.2.2.4.2	Procesorul de service al sistemului HP 9000 model T500	173
5.2.3	Sistemelor tolerante la defectări - concepte structurale și arhitecturale fundamentale în domeniul	178
5.2.3.1	Redundanța și comportamentele cu defectări permise	178
5.2.3.2	Tehnicile de bază utilizate pentru mascarea defectelor	180
5.2.3.3	Partiționarea ierarhică a sistemelor tolerante la defectări	185
5.2.3.4	Principii generale de restabilire funcțională a unui sistem tolerant la defectări	189
5.2.3.5	Tehnici și metode hardware de tolerare a defectelor	193
5.2.3.5.1	Noțiunea de unitate hardware înlocuibilă	193
5.2.3.5.2	Tipuri de unități hardware înlocuibile în sisteme de calcul tolerante la defectări	194
5.2.3.5.3	O sinteză a tehnicilor și metodelor hardware de tolerare a defectelor	201
5.2.3.6	Tehnici și metode software de tolerare a defectelor	205
5.2.3.6.1	Rolul unităților software înlocuibile în proiectarea arhitecturii sistemelor de calcul tolerante la defectări	205
5.2.3.6.2	Tehnici și metode software de tolerare a defectelor	207
5.2.3.7	Concluzii privind structurile și arhitecturile sistemelor tolerante la defectări	218
5.3	Criptologia	219
5.3.1	Noțiuni fundamentale	219
5.3.2	Istoric	223
5.3.3	Criptografia modernă	227
5.3.3.1	Criptografia cu chei simetrice	227
5.3.3.2	Criptografia asimetrică	229
5.3.3.3	Managementul cheilor în criptografia modernă	231
5.3.3.3.1	Generarea cheilor	231
5.3.3.3.2	Transferul cheilor	232
5.3.3.3.3	Verificarea cheilor	232
5.3.3.3.4	Utilizarea cheilor	233
5.3.3.3.5	Actualizarea cheilor	233
5.3.3.3.6	Stocarea cheilor	233
5.3.3.3.7	Copii de siguranță (Backup)	234
5.3.3.3.8	Durata de viață a cheilor	234
5.3.3.3.9	Distrugerea cheilor	235
5.3.3.4	Concluzii	235
5.4	Alte mijloace tehnice pentru asigurarea securității informatice	237
5.4.1	Securitatea hardware-ului și firmware-ului	237

5.4.2	Securitatea sistemelor de operare	240
5.4.3	Autentificarea, autorizarea și managementul încrederii	243
5.4.4	Controlul accesului și managementul privilegiilor	245
5.4.5	Protecția, prevenirea și preempțiunea referitoare la un atac	248
5.4.6	Cunoașterea situațională legată de starea cibernetică la nivel extins	250
5.4.7	Detecția, atenționarea și răspunsul automat la atacuri	253
5.4.8	Detecția și diminuarea atacurilor din partea persoanelor din interior	254
5.4.9	Detectarea informațiilor ascunse și a fluxurilor ascunse de informații	257
5.4.10	Restabilirea și reconstituirea	259
6	Mijloace funcționale de protecție împotriva amenințărilor informatice	261
6.1	Noțiuni introductive	261
6.2	Securitatea informatică în sistemele de operare Windows	271
6.2.1	Noțiuni introductive	271
6.2.2	Lucrul cu conturile de utilizator	272
6.2.2.1	Adăugarea, configurarea și ștergerea conturilor de utilizator	272
6.2.2.2	Modificarea unui grup de utilizatori sau a unui tip de cont	275
6.2.2.3	Modificarea ecranului Start Up	276
6.2.2.4	Modificarea unei imagini de cont	276
6.2.2.5	Modificarea și setarea unei parole	277
6.2.3	Gestionarea securității prin Windows Action Center	278
6.2.4	Utilizarea aplicației Windows Firewall	280
6.2.5	Utilizarea aplicației Microsoft Security Essentials	282
6.2.5.1	Scanarea, la cerere, a calculatorului	283
6.2.5.2	Programarea scanărilor	283
6.2.5.3	Scanarea mai mult decât doar a hard diskului	284
6.2.5.4	Nivele de alertă în Microsoft Security Essentials	284
6.2.6	Criptarea fișierelor pentru siguranță	286
6.2.7	Alte metode de evitare a virușilor și a altor atacuri periculoase	286
6.2.7.1	Evitarea atacurilor periculoase	286
6.2.7.2	Evitarea intrușilor	287
6.2.7.3	Securitatea pe Internet	288
6.3	Securitatea informatică asigurată de produse Bitdefender	291
6.3.1	Prezentare generală	291
6.3.2	Software antivirus pentru utilizatori individuali	295
6.3.2.1	Bitdefender Antivirus Plus 2013	295

6.3.2.2	Bitdefender Internet Security 2013	295
6.3.2.3	Bitdefender Total Security 2013	295
6.3.3	Software de securitate pentru companii	300
6.3.3.1	Descriere generală	300
6.3.3.2	Soluții Business	301
6.3.3.3	Generația de produse Bitdefender 2013 în România	303
6.3.4	Bitdefender Quickscan – scanare gratuită în rețea	304
6.3.5	Ghiduri electronice Bitdefender	305
6.3.5.1	Ghid privind un blog sigur	306
6.3.5.2	Ghid de securizare a rețelelor wireless	306
6.3.5.3	Ghid de protejare a copiilor online	306
6.3.5.4	Ghid de securitate on-line pentru utilizatorii de Internet în vârstă	307
6.3.5.5	Ghid de prevenire a dezvăluirii datelor confidențiale	307
6.4	Securitatea informatică asigurată de produse ale companiei Kaspersky Lab	308
6.4.1	Prezentare generală	308
6.4.2	Oferte de produse și servicii Kaspersky Lab	309
6.4.2.1	Kaspersky Pure 2.0	311
6.4.2.2	Kaspersky Pure Total Security	312
6.4.2.3	Kaspersky Antivirus 2012	313
6.4.2.4	Kaspersky Internet Security 2012	315
6.4.2.5	Comparație privind funcționalități cheie între produse Kaspersky	317
6.4.2.6	Kaspersky Small Office Security	318
6.4.2.7	Kaspersky Open Space Security	321
6.4.2.8	Kaspersky Mobile Security Enterprise Edition	323
6.4.2.9	Kaspersky One Universal Security	325
6.4.2.10	Kaspersky Password Manager	325
6.5	Securitatea informatică asigurată de produse ale companiei Symantec	327
6.5.1	Prezentare generală	327
6.5.2	Software de securitate pentru utilizatori individuali	328
6.5.2.1	Norton Antivirus 2012	328
6.5.2.2	Norton Internet Security 2012	329
6.5.2.3	Norton 360 6.0	330
6.5.3	Software de securitate pentru companii	332
6.5.3.1	Symantec Endpoint Protection Small Business Edition 12.0	332
6.5.3.2	Symantec Protection Suite Small Business Edition	333
6.5.3.3	Symantec Endpoint Protection 12.0	334
6.6	Securitatea informatică asigurată de produse ale companiei	335

	Panda Security	
6.6.1	Prezentare generală	335
6.6.2	Software de securitate pentru utilizatori individuali	335
6.6.2.1	Panda Antivirus Pro 2012 1 PC	335
6.6.2.2	Panda Internet Security 2012 1 PC	336
6.6.2.3	Panda Global Protection 2012 1 PC	337
6.6.2.4	Panda Antivirus Pro 2012 3 PC	338
6.6.2.5	Panda Internet Security 2012 3 PC	339
6.6.3	Software de securitate pentru companii	340
6.6.3.1	Panda Security for Business Soho	340
6.6.3.2	Panda Security for Business Soho + protecție pentru Exchange	340
6.6.3.3	Panda Cloud Office Protection	340
6.6.3.4	Panda Cloud Email Protection	341
6.6.3.5	Panda Security for Business SMB	341
6.7	Securitatea informatică asigurată de produse ale companiei McAfee Security	342
6.7.1	Prezentare generală	342
6.7.2	Software de securitate pentru utilizatori individuali	343
6.7.2.1	McAfee All Access	343
6.7.2.2	McAfee Total Protection	343
6.7.2.3	McAfee Internet Security	344
6.7.2.4	McAfee Antivirus Plus 2012	344
6.7.3	Software de securitate pentru companii	344
6.8	Institutul independent de securitate IT AV-TEST	345
7	Auditul și managementul securității sistemelor informatice	353
7.1	Securitatea sistemelor informatice – concepte și caracteristici	354
7.2	Sisteme de management al securității informației	358
7.2.1	Stabilirea sistemului de management al securității informației (SMSI)	360
7.2.2	Implementarea și funcționarea sistemului de management al securității informației	360
7.2.3	Monitorizarea și revizuirea sistemului de management al securității informației	361
7.2.4	Mentținerea și îmbunătățirea sistemului de management a securității informației	362
7.3	Controalele fizice și de mediu	364
7.4	Securitatea informației și a sistemelor	365
7.4.1	Controlul accesului logic	366
7.4.2	Cadrul de securitate a accesului	367

7.4.3	Controale privind accesul la aplicații și la sistemul de operare	368
7.5	Controale de rețea și controale Internet	369
8	Politici și strategii referitoare la securitatea informațională	373
8.1	Politica europeană în domeniul securității informaționale	373
8.1.1	Necesitatea unei politici publice	375
8.1.2	Conștientizarea pericolelor	378
8.1.3	Dezvoltarea suportului tehnologic	379
8.1.4	Standardizarea și certificarea	380
8.1.5	Securitatea în aplicațiile guvernamentale	381
8.1.6	Cooperarea internațională	382
8.1.7	Securitatea informatică în planul E-Europe 2005	382
8.1.8	Rezoluția Parlamentului European din 12 iunie 2012 referitoare la protecția infrastructurilor critice de informație - realizări și etape următoare: către un context global de securitate cibernetică	384
8.1.9	Organisme europene implicate în asigurarea securității informatice	393
8.1.9.1	Un sistem european de avertizare și informare în domeniul securității informatice	393
8.1.9.2	Agencia pentru rețeaua europeană și securitatea informațională	394
8.1.9.3	Un centru al UE de combatere a criminalității informatice menit să lupte împotriva infractorilor și să îi protejeze pe consumatorii online	396
8.1.9.3.1	Introducere: răspunsul european la criminalitatea fără frontiere	397
8.1.9.3.2	Propunere de instituire a unui centru european de combatere a criminalității informatice	400
8.1.9.3.2.1	Funcțiile de bază și misiunile pe care ar trebui să le îndeplinească centrul european de combatere a criminalității informatice	401
8.1.9.3.2.2	Amplasarea	403
8.1.9.3.2.3	Implicațiile pe care le presupune EC3 în termeni de resurse	404
8.1.9.3.2.4	Guvernanța	404
8.1.9.3.2.5	Cooperarea cu actorii-cheie	405
8.1.9.3.3	O foaie de parcurs pentru instituirea centrului european de combatere a criminalității informatice	406
8.1.9.3.4	Concluzii	407
8.2	Elemente de strategie a NATO în domeniul securității	407

	informatică	
8.2.1	Noțiuni introductive	407
8.2.2	Necesitatea unei strategii limpezi referitoare la securitatea informatică	408
8.2.3	Pași spre conturarea unei strategii limpezi referitoare la securitatea informatică	413
8.2.4	Elemente ale concepției strategice a NATO în domeniul securității informatică	416
8.2.5	Programe și organisme NATO	424
8.2.6	Concluzii	426
9	Aspectele juridice, identificarea urmelor lăsate și atribuirea responsabilităților pentru atacurile informatice	427
9.1	Noțiuni introductive	427
9.2	Elemente de reglementare legislativă internațională în domeniul securității informatică	430
9.3	Elemente de reglementare legislativă în România în domeniul securității informatică	439
A	Anexe	445
A1	Elemente de arhitectura și structura calculatoarelor	445
A1.1	Noțiuni fundamentale în domeniul calculatoarelor	445
A1.2	Mașini virtuale multi-nivel	447
A1.3	Noțiunile de structură, arhitectură și organizare a calculatoarelor	451
A1.4	Scurt istoric al calculatoarelor	453
A1.4.1	Introducere	453
A1.4.2	Primii pași în domeniul sistemelor de calcul	454
A1.4.3	Generații de calculatoare electronice	457
A1.4.3.1	Prima generație de calculatoare	458
A1.4.3.2	A doua generație de calculatoare	460
A1.4.3.3	A treia generație de calculatoare	462
A1.4.3.4	A patra generație de calculatoare	463
A1.4.3.5	Preocupări relative la generațiile viitoare de calculatoare	466
A1.5	Tipuri de calculatoare	466
A1.5.1	Calculatoarele încorporate	467
A1.5.2	Calculatoarele personale și stații de lucru	468
A1.5.3	Minisupercalculatoarele	469
A1.5.4	Mainframe-urile	470
A1.5.5	Supercalculatoarele	470

A1.6	Hardware-ul calculatoarelor	470
A1.6.1	Noțiuni introductive în domeniul hardware-ului calculatoarelor	470
A1.6.2	Unitatea centrală de prelucrare	472
A1.6.3	Memoria calculatoarelor	474
A1.6.3.1	Memoria intermediară	477
A1.6.3.2	Memoria principală	478
A1.6.3.3	Discurile magnetice	479
A1.6.3.4	Discurile optice și benzile magnetice	481
A1.6.3.5	Alte dispozitive de memorare	483
A1.7	Intrările/ieșirile calculatoarelor	484
A1.7.1	Echipamente periferice de intrare	485
A1.7.1.1	Tastatura	485
A1.7.1.2	Echipamente de poziționare și activare comenzi	486
A1.7.1.3	Echipamente de preluarea imaginilor	489
A1.7.1.4	Microfonul	490
A1.7.2	Echipamente periferice de ieșire	491
A1.7.2.1	Monitorul	491
A1.7.2.2	Boxele	493
A1.7.2.3	Echipamente de imprimare	493
A1.8	Noțiuni introductive în domeniul rețelelor de calculatoare	497
A1.8.1	Definiții și utilizări	497
A1.8.2	Protocoale pentru comunicația prin rețele	498
A1.8.3	Tipuri de rețele și topologii de rețele și dispozitive pentru acestea	500
A1.8.4	Medii de transmisie și dispozitive de transmisie	503
A1.8.5	Ethernet și Internet	505
A1.8.6	Utilizarea resurselor Internetului	507
A1.8.6.1	Noțiuni introductive	507
A1.8.6.2	Protecția prin firewall	508
A1.8.6.3	Browsere Web	508
A1.8.6.4	Pagina de bază	509
A2	Elemente de software de sistem și software de aplicații	511
A2.1	Sisteme de operare	511
A2.1.1	Evoluția sistemelor de operare	511
A2.1.2	Funcțiile și structura sistemelor de operare	519
A2.2	Limbaje de programare și translație	521
A2.2.1	Limbaje și comunicare	521
A2.2.2	Limbaje de programare	523
A2.2.3	Traducerea limbajelor de programare	527

A2.3	Clase de aplicații software	528
	Bibliografie	533