

CUPRINS

Mulțumiri	5
Abrevieri	7
Considerații introductive	9

PARTEA I

Aspecte generale privind securitatea sistemelor informatice și criminalitatea informatică	11
--	-----------

Capitolul I. Amenințări actuale și tendințe viitoare în ce privește securitatea sistemelor informatice și rețelelor de comunicații	13
---	-----------

Secțiunea I. Considerații generale	13
--	----

Secțiunea a II-a. Principalele taxonomii dezvoltate în sfera securității sistemelor informatice și rețelelor de comunicații	14
---	----

§ 1. Palauskas N., Garsva E., Clasificarea atacurilor asupra sistemelor informatice	16
---	----

§ 2. Howard John D., Longstaff Thomas A., Un limbaj comun pentru incidentele privind securitatea calculatoarelor	19
--	----

§ 3. Weber Daniel James, O taxonomie a intruziunilor în calculatoare	25
--	----

§ 4. Lough Daniel Lawry, O taxonomie a atacurilor asupra calculatoarelor cu aplicație pentru rețelele fără fir	28
--	----

§ 5. RAND Europe, O taxonomie a incidentelor de securitate	29
--	----

Secțiunea a III-a. O scurtă analiză a principalelor amenințări la adresa securității sistemelor informatice și rețelelor de comunicații	32
---	----

§ 1. Virușii informatici (computer virus)	32
---	----

1.1. Descriere	32
----------------------	----

1.2. Exemple	34
1.3. Elemente cu valoare probatorie	34
§ 2. Troienii (Trojan Horse).....	34
2.1. Descriere.....	34
2.2. Exemple.....	35
2.3. Elemente cu valoare probatorie	35
§ 3. Jurnalul de taste (Keylogger).....	36
3.1. Descriere.....	36
3.2. Exemple:.....	36
3.3. Elemente cu valoare probatorie	37
§ 4. Analizările de trafic de rețea (Sniffer/Analysers).....	37
4.1. Descriere.....	37
4.2. Exemple	37
4.3. Elemente cu valoare probatorie	37
§ 5. Kitul de rădăcină (Rootkit)	38
5.1. Descriere.....	38
5.2. Exemple	38
5.3. Elemente cu valoare probatorie	38
§ 6. Instrumente de scanare (Scanning Tool).....	39
6.1. Descriere.....	39
6.2. Exemple.....	40
6.3. Elemente cu valoare probatorie	40
§ 7. Instrumente de spargere a parolei (Password Cracker Tool)	41
7.1. Descriere.....	41
7.2. Exemple.....	42
7.3. Elemente cu valoare probatorie	42
§ 8. Rețele (ro)bot (Botnet).....	42
8.1. Descriere.....	42
8.2. Exemple.....	43
8.3. Elemente cu valoare probatorie	43
§ 9. Refuzul serviciului (Denial of Service)	43
9.1. Descriere.....	43
9.2. Exemple:.....	44
9.3. Elemente cu valoare probatorie	45

Capitolul II. Conceptul, principalele caracteristici și evoluția criminalității informatice	46
Secțiunea I. Considerații generale	46
Secțiunea a II-a. Conceptul „criminalitate informatică”	46
§ 1. Noțiunea de criminalitate	46
§ 2. Noțiunea de criminalitate informatică	47
§ 3. Infrațiuni din sfera criminalității informatice	49
Secțiunea a III-a. Principalele caracteristici ale criminalității informatice	51
Secțiunea a IV-a. Aspecte privind evoluția criminalității informatice	52
§ 1. Etapele evoluției	53
§ 2. Amenințări actuale	54
§ 3. Principalii factori care influențează dezvoltarea criminalității informatice, provocări ale combaterii fenomenului	54
3.1. Dependența de tehnologia informației și comunicațiilor	54
3.2. Numărul utilizatorilor	55
3.3. Disponibilitatea dispozitivelor și accesului	56
3.4. Disponibilitatea informațiilor	57
3.5. Lipsa mecanismelor de control	57
3.6. Dimensiuni internaționale	58
3.7. Independența locației și prezenței la locul infracțiunii	58
3.8. Automatizarea	59
3.9. Resursele	60
3.10. Viteza proceselor de schimb de date	60
3.11. Viteza de dezvoltare	61
3.12. Comunicațiile anonime	61
3.13. Tehnologia de criptare	62
Capitolul III. Explicații criminologice ale subculturilor criminalității informatice	63
Secțiunea I. Considerații generale	63
Secțiunea a II-a. O scurtă prezentare a Teoriei lui Emile Durkheim	63

Secțiunea a III-a. O scurtă prezentare a Teoriei lui Robert Merton	65
Secțiunea a IV-a. Explicarea subculturilor criminalității informatice prin prisma tipologiei modurilor individuale de adaptare dezvoltată de Merton	67
§ 1. Conformismul navigatorilor pe Internet	68
§ 2. Inovația: hacking-ul pentru profit	69
§ 3. Ritualismul: hacking-ul ca obișnuință	70
§ 4. Retragerea: hacking-ul ca dependență	70
§ 5. Rebeliunea: hacking-ul ca nesupunere la regulile societății	71
§ 6. Hackingul non-utilitar	71

PARTEA A II-A

Preocupări ale societății internaționale pentru prevenirea și combaterea criminalității informatice	73
--	-----------

Capitolul I. Organizații internaționale și regionale cu atribuții și preocupări în prevenirea și combaterea criminalității informatice și principalele realizări	75
Secțiunea I. Considerații generale	75
Secțiunea a II-a. Organizația Națiunilor Unite (UN)	75
Secțiunea a III-a. Grupul celor Opt Națiuni (G8)	78
Secțiunea a IV-a. Uniunea Internațională a Telecomunicațiilor (ITU)	81
Secțiunea a V-a. Consiliul Europei (CoE)	84
Secțiunea a VI-a. Uniunea Europeană (EU)	86

Capitolul II. Principalele instrumente juridice și recomandări cu vocație internațională și regională care conțin reglementări privind prevenirea și combaterea criminalității informatice	89
Secțiunea I. Considerații generale	89
Secțiunea a II-a. Recomandarea nr. R (89) 9 asupra criminalității în relație cu calculatorul	91
Secțiunea a III-a. Convenția privind criminalitatea informatică	93

Secțiunea a IV-a. Protocolul adițional referitor la incriminarea actelor de natură rasistă și xenofobă săvârșite prin intermediul sistemelor informatice	97
--	----

Capitolul III. Analiză comparativă a modului în care legislațiile altor state au implementat măsurile prevăzute de convenția privind criminalitatea informatică	101
Secțiunea I. Considerații generale	101
Secțiunea a II-a. Analiza comparativă a modului în care au fost definiți termenii utilizați	103
Secțiunea a III-a. Analiza comparativă a modului în care au fost incriminate infracțiunile împotriva confidențialității, integrității și disponibilității datelor	105
§ 1. Accesarea ilegală	106
§ 2. Interceptarea ilegală	110
§ 3. Afectarea integrității datelor	113
§ 4. Afectarea integrității sistemului	115
§ 5. Abuzurile asupra dispozitivelor	117
Secțiunea a IV-a. Analiza comparativă a modului în care au fost incriminate infracțiunile informatice	121
§ 1. Falsificarea informatică	121
§ 2. Frauda informatică	124
Secțiunea a V-a. Analiza comparativă a modului în care au fost incriminate infracțiunile referitoare la conținut	127
§ 1. Infracțiuni referitoare la pornografia infantilă	127
Secțiunea a VI-a. Analiza comparativă a modului în care au fost incriminate infracțiunile referitoare la atingerile aduse proprietății intelectuale și drepturilor conexe	132

Capitolul IV. Puncte de vedere exprimate în literatura și doctrina de specialitate cu privire la metodele, tehnicile și procedurile de cercetare a infracțiunilor din sfera criminalității informatice	139
Secțiunea I. Considerații generale	139
Secțiunea a II-a. Principalele modele de cercetare a infracțiunilor din sfera criminalității informatice prezentate în literatura de specialitate	139

§ 1. Pollit M. Mark, Paradigma digitală.....	140
§ 2. Farmer Dan, Venema Wietse, Analiza criminalistică a computerelor UNIX	141
§ 3. Primul Atelier de lucru de cercetare criminalistică digitală (DFRWS), Procesul de investigație în raport cu știința criminalistică digitală.....	142
§ 4. Reith Mark, Carr Clint, Gunsch Gregg, Un model criminalistic digital abstract.....	145
§ 5. Gordon R. Gary, Hosmer D. Chet, Siedma Christine, Rebovich Dan, Metodologia investigării criminalistice digitale	146
§ 6. Carrier Brian, Spafford H. Eugene, Un proces integrat de investigație digitală	148
§ 7. Baryamureeba Venansuis, Tushabe Florence, Un model avansat/îmbunătățit al procesului integrat de investigare digitală.....	150
§ 8. Ciardhuain O' Séamus, Un model extins de investigații a criminalității informatice	151
§ 9. Kohn Michael, Elloff JHP, Oliver MS, Model cadru pentru investigarea criminalistică digitală	153
§ 10. Freiling C. Felix, Schwittay Bastian, Un model comun procesului pentru răspuns la incident și investigare criminalistică digitală.....	154
Secțiunea a III-a. Principalele proceduri, ghiduri, practici dezvoltate în domeniul prevenirii și combaterii criminalității informatice	156
§ 1. Organizația Națiunilor Unite, Manual pentru prevenirea și controlul infracțiunilor în legătură cu calculatorul	157
§ 2. INTERPOL, Manualul de Investigare a Infracțiunilor privind Tehnologia Informațiilor (ITCIM)	160
§ 3. Rețeaua Europeană a Institutelor de Criminalistică (ENFSI) Orientări pentru bune practici în examinarea criminalistică a tehnologiilor digitale	161
§ 4. Compartimentul pentru Criminalitate Informatică și Proprietate Intelectuală din cadrul Direcției Penale a Ministerului de Justiție al SUA, Punerea sub acuzare a infracțiunilor din sfera criminalității informatice	163

§ 5. Institutul Național de Justiție din cadrul Ministerului de Justiție al SUA, Investigarea scenei „electronice” a infracțiunii: Un ghid pentru primul respondent	165
§ 6. United States Secret Service, Bune practici pentru confiscarea dovezilor electronice: Un ghid de buzunar pentru prim-respondent.....	169
§ 7. Asociația Ofițerilor Șefi ai poliției din Anglia, Țara Galilor și Irlanda de Nord, Ghid de bune practici pentru dovezi electronice din (bazate pe) calculator	171
§ 8. Institutul Național de Justiție din cadrul Ministerului de Justiție al SUA, Examinarea criminalistică a dovezilor digitale: un ghid pentru autoritățile de aplicare a legii.....	173
§ 9. Compartimentul pentru Criminalitate, Informatică și Proprietate Intelectuale din cadrul Direcției penale a Ministerului de Justiție al SUA, Căutarea și confiscarea calculatoarelor și obținerea dovezilor electronice în investigațiile penale	175
§ 10. Institutul Național pentru Standarde și tehnologie din cadrul Ministerului Comerțului al SUA, Ghid pentru gestionarea incidentelor de securitate a calculatoarelor.....	177

PARTEA A III-A

Coordonatele activității organelor legislative și executive din România pentru dezvoltarea conceptului de prevenire și combatere a criminalității informatice	183
--	------------

Capitolul I. Dezvoltarea conceptului național de prevenire a criminalității informatice, politicile și măsurile întreprinse de factorii responsabili în acest domeniu	185
Secțiunea I. Considerații generale privind prevenirea criminalității	185
Secțiunea a II-a. Măsuri specifice de prevenire a criminalității informatice.....	186

Capitolul II. Modul în care legislația românească incriminează infracțiunile din sfera criminalității informatice	189
Secțiunea I. Considerații generale.....	189

Secțiunea a II-a. Infracțiuni incriminate în titlul III al Legii nr. 161/2003 și în noul Cod penal al României.....	193
§ 1. Infracțiunile contra confidențialității și integrității datelor și sistemelor informatice.....	194
1.1. Accesul ilegal la un sistem informatic.....	194
1.2. Interceptarea ilegală a unei transmisii de date informatice.....	197
1.3. Alterarea integrității datelor informatice	199
1.4. Perturbarea funcționării sistemelor informatice	202
1.5. Operațiuni ilegale cu dispozitive sau programe informatice.....	204
§ 2. Infracțiunile informatice	207
2.1. Falsul informatic.....	207
2.2. Frauda informatică.....	210
§ 3. Pornografia infantilă prin sisteme informatice	212
Secțiunea a III-a. Aspecte procesuale aplicabile infracțiunilor din sfera criminalității informatice.....	215
§ 1. Sfera de aplicare.....	215
§ 2. Conservarea datelor informatice ori a datelor referitoare la traficul informațional.....	216
§ 3. Ridicarea obiectelor care conțin date informatice, date referitoare la traficul informațional sau date referitoare la utilizatori.....	217
§ 4. Percheziția sistemelor informatice	218
§ 5. Accesul în sistemele informatice și interceptarea și înregistrarea comunicărilor desfășurate prin intermediul acestora	219
Secțiunea a IV-a. Măsuri privind cooperarea internațională.....	220

Capitolul III. Instituții cu atribuții în prevenirea și combaterea criminalității informatice și principalele realizări

realizări	223
Secțiunea I. Considerații generale.....	223
Secțiunea a II-a. Structuri specializate în cadrul Parchetului de pe lângă Înalta Curte de Casație și Justiție	223

§ 1. Direcția de Investigare a Infrațiunilor de Criminalitate Organizată și Terorism din cadrul Parchetului de pe lângă Înalta Curte de Casație și Justiție	223
§ 2. Serviciul de prevenire și combatere a criminalității informatice.....	224
2.1. Conducerea, structura și atribuțiile Serviciului de prevenire și combatere a criminalității informatice	224
2.2. Atribuțiile Biroului de combatere a criminalității informatice.....	226
2.3. Atribuțiile Biroului de combatere a infrațiunilor cu cărți de credit și alte mijloace de plată electronică	227
2.4. Atribuțiile Biroului de combatere a infrațiunilor din domeniul proprietății intelectuale și industriale	227
Secțiunea a III-a. Structuri specializate în cadrul Inspectoratului General al Poliției Române	228
§ 1. Direcția de Combatere a Criminalității Organizate din cadrul Inspectoratului General al Poliției Române	228
§ 2. Serviciul de combatere a criminalității informatice.....	229
Secțiunea a IV-a. Principalele realizări pe linia combaterii criminalității informatice.....	229
§ 1. Principalele rezultate obținute în anul 2007.....	230
1.1. Analiza generală a fenomenului	230
1.2. Principalele cauze instrumentate	231
1.3. Concluzii	233
§ 2. Principalele rezultate obținute în anul 2008.....	234
2.1. Analiza generală a fenomenului	234
2.2. Cazul „Vladuz”.....	235
2.3. Concluzii	236
§ 3. Principalele rezultate obținute în anul 2009.....	237
3.1. Analiza generală a fenomenului	237
3.2. Principalele cauze instrumentate	238
3.3. Concluzii	242
§ 4. Principalele rezultate obținute în anul 2010.....	242
4.1. Analiza generală a fenomenului	242
4.2. Principalele cauze instrumentate	244
4.3. Concluzii	247

PARTEA A IV-A

Puncte de vedere cu privire la metodologia cercetării infrafracțiunilor din sfera criminalității informatice	249
---	------------

Capitolul I. Conceptul investigare criminalistică digitală, status-ul și conținutul acestui proces	251
Secțiunea I. Conceptul investigare criminalistică digitală	251
Secțiunea a II-a. Status-ul și conținutul procesului de investigare criminalistică digitală	252

Capitolul II. Considerații generale cu privire la metodologia cercetării infrafracțiunilor din sfera criminalității informatice	255
Secțiunea I. Clasic și nou în cercetarea infrafracțiunilor din sfera criminalității informatice	255
Secțiunea a II-a. Principiile, scopul și definiția metodologiei de cercetare infrafracțiunilor din sfera criminalității informatice...	256
§ 1. Precizări terminologice cu privire la cercetarea penală a infrafracțiunilor din sfera criminalității informatice și investigarea criminalistică a locului faptei și a sistemelor informatice	256
§ 2. Principiile cercetării infrafracțiunilor din sfera criminalității informatice și investigării criminalistice a locului faptei și a sistemelor informatice	259
2.1. Principiile cercetării infrafracțiunilor din sfera criminalității informatice	259
2.2. Principiile investigării criminalistice a locului faptei și a sistemelor informatice.....	260
§ 3. Obiectivele cercetării infrafracțiunilor din sfera criminalității informatice	260
3.1. Obiectivul cercetării penale a infrafracțiunilor din sfera criminalității informatice	260
3.2. Obiectivul investigării criminalistice a locului faptei și a sistemelor informatice.....	261
3.3. Obiectivele concrete ale cercetării infrafracțiunilor din sfera criminalității informatice	262
§ 4. Definiția metodologiei cercetării infrafracțiunilor din sfera criminalității informatice.....	262

Capitolul III. Formalizarea și standardizarea activității de cercetare a infracțiunilor din sfera criminalității informatice . 263

Secțiunea I. Considerații generale	263
Secțiunea a II-a. Necesitatea standardizării activității de cercetare a infracțiunilor din sfera criminalității informatice, de acreditare a laboratoarelor criminalistice și de certificare a specialiștilor și a mijloacelor de investigare	264
Secțiunea a III-a. Perspective actuale privind standardizarea activității de cercetare a infracțiunilor din sfera criminalității informatice și acreditarea laboratoarelor criminalistice	265
§ 1. Situația la nivel internațional	265
1.1. În domeniul standardizării	265
1.2. În domeniul acreditării	266
1.3. În domeniul evaluării conformității	266
§ 2. Situația la nivel european	267
2.1. În domeniul standardizării	267
2.2. În domeniul autorizării	267
2.3. În domeniul evaluării conformității	268
§ 3. Situația în SUA	268
3.1. În domeniul standardizării	268
3.2. În domeniul acreditării	269
3.3. În domeniul evaluării conformității	269
§ 4. Situația în România	270
4.1. În domeniul standardizării	270
4.2. În domeniul acreditării	271

Capitolul IV. Procedura cercetării infracțiunilor din sfera criminalității informatice propusă 273

Secțiunea 1. Necesitatea modificării/completării procedurilor de cercetare a infracțiunilor din sfera criminalității informatice	273
Secțiunea a II-a. Etapele/fazele cercetării infracțiunilor din sfera criminalității informatice propuse	275
§ 1. Activitățile premergătoare cercetării propriu-zise	275
§ 2. Cercetarea la fața locului	275
§ 3. Efectuarea perchezițiilor (sistemelor informatice, domiciliară, în alte locații)	276

§ 4. Ascultarea persoanelor (învinuiți, martori, părți vătămate).....	277
§ 5. Examinarea dovezilor	278
§ 6. Finalizarea cercetărilor	278
Secțiunea a III-a. Aspecte privind conținutul și forma de redactare a procedurii/procedurilor	280
Secțiunea a IV-a. Particularitățile unor activități de cercetare a infracțiunilor din sfera criminalității informatice și de investigare criminalistică a locului faptei și a sistemelor informatice	281
§ 1. Particularități ale pregătirii cercetării/investigației	282
§ 2. Particularități ale căutării/conservării dovezilor materiale/digitale	283
§ 3. Particularități privind informațiile care trebuie furnizate de/obținute de la suspecti/învinuiți, martori, părți vătămate	285
3.1. Posibile întrebări cu caracter general.....	285
3.2. Posibile întrebări cu caracter particular	287
§ 4. Particularitățile dovezilor digitale.....	290
§ 5. Particularități ale colectării dovezilor digitale	291
§ 6. Particularități ale examinării dovezilor digitale	294
§ 7. Particularități ale documentării cercetării și întocmirii rapoartelor (de constatare tehnico-științifică/ expertiză)	295
§ 8. Particularități ale echipamentelor (hardware) și programelor (software) specializate folosite în investigarea criminalistică digitală.....	297
Scurte concluzii și propuneri	299
Bibliografie selectivă	307