

## CUPRINS

Mulțumiri .....	5
Abrevieri .....	7
Considerații introductive .....	9

### PARTEA I

<b>Aspecte generale privind securitatea sistemelor informatice și criminalitatea informatică .....</b>	<b>11</b>
--	-----------

<b>Capitolul I. Amenințări actuale și tendințe viitoare în ce privește securitatea sistemelor informatice și rețelelor de comunicații .....</b>	<b>13</b>
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. Analizoarele 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).....	43
8.1. Descriere.....	43
8.2. Exemple.....	43
8.3. Elemente cu valoare probatorie .....	43
§ 9. Refuzul serviciului (Denial of Service) .....	43
9.1. Descriere.....	44
9.2. Exemple:.....	44
9.3. Elemente cu valoare probatorie .....	45

<b>Capitolul II. Conceptul, principalele caracteristici și evoluția criminalității informatice</b> .....	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 .....	500
Secțiunea a III-a. Principalele caracteristici ale criminalității informatice .....	52
Secțiunea a IV-a. Aspecte privind evoluția criminalității informatice .....	53
§ 1. Etapele evoluției .....	53
§ 2. Amenințări actuale .....	54
§ 3. Principalii factori care influențează dezvoltarea criminalității informatice, provocări ale combaterii fenomenului .....	55
3.1. Dependența de tehnologia informației și comunicațiilor .....	55
3.2. Numărul utilizatorilor .....	56
3.3. Disponibilitatea dispozitivelor și accesului .....	57
3.4. Disponibilitatea informațiilor .....	57
3.5. Lipsa mecanismelor de control .....	58
3.6. Dimensiuni internaționale .....	58
3.7. Independența locației și prezenței la locul infracțiunii .....	59
3.8. Automatizarea .....	660
3.9. Resursele .....	60
3.10. Viteza proceselor de schimb de date .....	61
3.11. Viteza de dezvoltare .....	62
3.12. Comunicațiile anonime .....	62
3.13. Tehnologia de criptare .....	63
 <b>Capitolul III. Explicații criminologice ale subculturilor criminalității informatice</b> .....	64
Secțiunea I. Considerații generale .....	64
Secțiunea a II-a. O scurtă prezentare a Teoriei lui Emile Durkheim .....	64

Secțiunea a III-a. O scurtă prezentare a Teoriei lui Robert Merton .....	66
Secțiunea a IV-a. Explicarea subculturilor criminalității informatice prin prisma tipologiei modurilor individuale de adaptare dezvoltată de Merton .....	68
§ 1. Conformismul navigatorilor pe Internet .....	69
§ 2. Inovația: hacking-ul pentru profit .....	770
§ 3. Ritualismul: hacking-ul ca obișnuință .....	71
§ 4. Retragerea: hacking-ul ca dependență .....	71
§ 5. Rebeliunea: hacking-ul ca nesupunere la regulile societății .....	72
§ 6. Hackingul non-utilitar .....	72

## PARTEA A II-A

<b>Preocupări ale societății internaționale pentru prevenirea și combaterea criminalității informatice .....</b>	<b>73</b>
--	-----------

<b>Capitolul I. Organizații internaționale și regionale cu atribuții și preocupări în prevenirea și combaterea criminalității informatice și principalele realizări .....</b>	<b>75</b>
Secțiunea I. Considerații generale .....	75
Secțiunea a II-a. Organizația Națiunilor Unite (UN) .....	75
Secțiunea a III-a. Grupul celor Opt Națiuni (G8) .....	79
Secțiunea a IV-a. Uniunea Internațională a Telecomunicațiilor (ITU) .....	82
Secțiunea a V-a. Consiliul Europei (CoE) .....	85
Secțiunea a VI-a. Uniunea Europeană (EU) .....	88

<b>Capitolul II. Principalele instrumente juridice și recomandări cu vocație internațională și regională care conțin reglementări privind prevenirea și combaterea criminalității informatice .....</b>	<b>913</b>
Secțiunea I. Considerații generale .....	913
Secțiunea a II-a. Recomandarea nr. R (89) 9 asupra criminalității în relație cu calculatorul .....	94
Secțiunea a III-a. Convenția privind criminalitatea informatică .....	97

Secțiunea a IV-a. Protocolul adițional referitor la incriminarea actelor de natură rasistă și xenofobă săvârșite prin intermediul sistemelor informatice .....	100
--	-----

<b>Capitolul III. Analiză comparativă a modului în care legislațiile altor state au implementat măsurile prevăzute de convenția privind criminalitatea informatică .....</b>	<b>105</b>
Secțiunea I. Considerații generale .....	105
Secțiunea a II-a. Analiza comparativă a modului în care au fost definiți termenii utilizați .....	107
Secțiunea a III-a. Analiza comparativă a modului în care au fost incriminate infracțiunile împotriva confidențialității, integrității și disponibilității datelor .....	109
§ 1. Accesarea ilegală .....	110
§ 2. Interceptarea ilegală .....	114
§ 3. Afectarea integrității datelor .....	117
§ 4. Afectarea integrității sistemului .....	120
§ 5. Abuzurile asupra dispozitivelor .....	122
Secțiunea a IV-a. Analiza comparativă a modului în care au fost incriminate infracțiunile informatice .....	125
§ 1. Falsificarea informatică .....	126
§ 2. Frauda informatică .....	129
Secțiunea a V-a. Analiza comparativă a modului în care au fost incriminate infracțiunile referitoare la conținut .....	131
§ 1. Infracțiuni referitoare la pornografia infantilă .....	131
Secțiunea a VI-a. Analiza comparativă a modului în care au fost incriminate infracțiunile referitoare la atingerile aduse proprietății intelectuale și drepturilor conexe .....	136

<b>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 .....</b>	<b>143</b>
Secțiunea I. Considerații generale .....	143
Secțiunea a II-a. Principalele modele de cercetare a infracțiunilor din sfera criminalității informatice prezentate în literatura de specialitate .....	143

§ 1. Pollit M. Mark, Paradigma digitală.....	144
§ 2. Farmer Dan, Venema Wietse, Analiza criminalistică a computerelor UNIX .....	145
§ 3. Primul Atelier de lucru de cercetare criminalistică digitală (DFRWS), Procesul de investigație în raport cu știința criminalistică digitală.....	146
§ 4. Reith Mark, Carr Clint, Gunsch Gregg, Un model criminalistic digital abstract.....	149
§ 5. Gordon R. Gary, Hosmer D. Chet, Siedma Christine, Rebovich Dan, Metodologia investigării criminalistice digitale .....	150
§ 6. Carrier Brian, Spafford H. Eugene, Un proces integrat de investigație digitală .....	152
§ 7. Baryamureeba Venansuis, Tushabe Florence, Un model avansat/îmbunătățit al procesului integrat de investigare digitală.....	154
§ 8. Ciardhuain O' Séamus, Un model extins de investigații a criminalității informatice .....	155
§ 9. Kohn Michael, Elloff JHP, Oliver MS, Model cadru pentru investigarea criminalistică digitală .....	157
§ 10. Freiling C. Felix, Schwittay Bastian, Un model comun procesului pentru răspuns la incident și investigare criminalistică digitală.....	158
Secțiunea a III-a. Principalele proceduri, ghiduri, practici dezvoltate în domeniul prevenirii și combaterii criminalității informatice .....	160
§ 1. Organizația Națiunilor Unite, Manual pentru prevenirea și controlul infracțiunilor în legătură cu calculatorul .....	161
§ 2. INTERPOL, Manualul de Investigare a Infracțiunilor privind Tehnologia Informațiilor (ITCIM) .....	164
§ 3. Rețeaua Europeană a Institutelor de Criminalistică (ENFSI) Orientări pentru bune practici în examinarea criminalistică a tehnologiilor digitale .....	165
§ 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 .....	167

§ 5. Institutul Național de Justiție din cadrul Ministerului de Justiție al SUA, Investigarea scenei „electronice” a infracțiunii: Un ghid pentru primul respondent .....	169
§ 6. United States Secret Service, Bune practici pentru confiscarea dovezilor electronice: Un ghid de buzunar pentru prim-respondent.....	173
§ 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.....	176
§ 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.....	178
§ 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 .....	179
§ 10. Institutul Național pentru Standarde și tehnologie din cadrul Ministerului Comerțului al SUA, Ghid pentru gestionarea incidentelor de securitate a calculatoarelor.....	181

**PARTEA A III-A**

<b>Coordonatele activității organelor legislative și executive din România pentru dezvoltarea conceptului de prevenire și combatere a criminalității informatice .....</b>	<b>189</b>
--	------------

<b>Capitolul I. Dezvoltarea conceptului național de prevenire a criminalității informatice, politicile și măsurile întreprinse de factorii responsabili în acest domeniu .....</b>	<b>191</b>
Secțiunea I. Considerații generale privind prevenirea criminalității .....	191
Secțiunea a II-a. Măsuri specifice de prevenire a criminalității informatice.....	192

<b>Capitolul II. Modul în care legislația românească incriminează infracțiunile din sfera criminalității informatice .....</b>	<b>195</b>
Secțiunea I. Considerații generale.....	195

Secțiunea a II-a. Infracțiuni incriminate în titlul III al Legii nr. 161/2003 și în noul Cod penal al României.....	199
§ 1. Infracțiunile contra confidențialității și integrității datelor și sistemelor informatice.....	200
1.1. Accesul ilegal la un sistem informatic.....	200
1.2. Interceptarea ilegală a unei transmisii de date informatice.....	20203
1.3. Alterarea integrității datelor informatice .....	205
1.4. Perturbarea funcționării sistemelor informatice .....	208
1.5. Operațiuni ilegale cu dispozitive sau programe informatice.....	210
§ 2. Infracțiunile informatice .....	214
2.1. Falsul informatic.....	214
2.2. Frauda informatică.....	216
§ 3. Pornografia infantilă prin sisteme informatice .....	219
Secțiunea a III-a. Aspecte procesuale aplicabile infracțiunilor din sfera criminalității informatice.....	222
§ 1. Sfera de aplicare.....	222
§ 2. Conservarea datelor informatice ori a datelor referitoare la traficul informațional.....	223
§ 3. Ridicarea obiectelor care conțin date informatice, date referitoare la traficul informațional sau date referitoare la utilizatori.....	224
§ 4. Percheziția sistemelor informatice.....	225
§ 5. Accesul în sistemele informatice și interceptarea și înregistrarea comunicărilor desfășurate prin intermediul acestora .....	225
Secțiunea a IV-a. Măsuri privind cooperarea internațională.....	226

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

realizări .....	230
Secțiunea I. Considerații generale.....	230
Secțiunea a II-a. Structuri specializate în cadrul Parchetului de pe lângă Înalta Curte de Casație și Justiție .....	230



§ 1. Direcția de Investigare a Infrațciunilor de Criminalitate Organizată și Terorism din cadrul Parchetului de pe lângă Înalta Curte de Casație și Justiție .....	230
§ 2. Serviciul de prevenire și combatere a criminalității informatice.....	231
2.1. Conducerea, structura și atribuțiile Serviciului de prevenire și combatere a criminalității informatice .....	231
2.2. Atribuțiile Biroului de combatere a criminalității informatice.....	233
2.3. Atribuțiile Biroului de combatere a infrațciunilor cu cărți de credit și alte mijloace de plată electronică .....	234
2.4. Atribuțiile Biroului de combatere a infrațciunilor din domeniul proprietății intelectuale și industriale .....	234
Secțiunea a III-a. Structuri specializate în cadrul Inspectoratului General al Poliției Române .....	235
§ 1. Direcția de Combatere a Criminalității Organizate din cadrul Inspectoratului General al Poliției Române .....	235
§ 2. Serviciul de combatere a criminalității informatice.....	236
Secțiunea a IV-a. Principalele realizări pe linia combaterii criminalității informatice.....	236
§ 1. Principalele rezultate obținute în anul 2011.....	237
1.1. Analiza generală a fenomenului .....	237
1.2. Principalele cauze instrumentate .....	239
1.3. Concluzii .....	242
§ 2. Principalele rezultate obținute în anul 2008.....	2430
2.1. Analiza generală a fenomenului .....	243
2.2. Principalele cauze instrumentate	<b>Error! Bookmark not defined.</b>
2.3. Concluzii .....	246

### **PARTEA A IV-A**

<b>Puncte de vedere cu privire la metodologia cercetării infrațciunilor din sfera criminalității informatice .....</b>	<b>247</b>
--	------------

<b>Capitolul I. Conceptul investigare criminalistică digitală, status-ul și conținutul acestui proces .....</b>	<b>249</b>
---	------------

Secțiunea I. Conceptul investigare criminalistică digitală .....	249
Secțiunea a II-a. Status-ul și conținutul procesului de investigare criminalistică digitală .....	250

<b>Capitolul II. Considerații generale cu privire la metodologia cercetării infracțiunilor din sfera criminalității informatică .....</b>	<b>253</b>
Secțiunea I. Clasic și nou în cercetarea infracțiunilor din sfera criminalității informatică .....	253
Secțiunea a II-a. Principiile, scopul și definiția metodologiei de cercetare infracțiunilor din sfera criminalității informatică...	254
§ 1. Precizări terminologice cu privire la cercetarea penală a infracțiunilor din sfera criminalității informatică și investigarea criminalistică a locului faptei și a sistemelor informatică .....	254
§ 2. Principiile cercetării infracțiunilor din sfera criminalității informatică și investigării criminalistice a locului faptei și a sistemelor informatică .....	257
2.1. Principiile cercetării infracțiunilor din sfera criminalității informatică .....	257
2.2. Principiile investigării criminalistice a locului faptei și a sistemelor informatică .....	258
§ 3. Obiectivele cercetării infracțiunilor din sfera criminalității informatică .....	258
3.1. Obiectivul cercetării penale a infracțiunilor din sfera criminalității informatică .....	258
3.2. Obiectivul investigării criminalistice a locului faptei și a sistemelor informatică .....	259
3.3. Obiectivele concrete ale cercetării infracțiunilor din sfera criminalității informatică .....	260
§ 4. Definiția metodologiei cercetării infracțiunilor din sfera criminalității informatică .....	260

<b>Capitolul III. Formalizarea și standardizarea activității de cercetare a infracțiunilor din sfera criminalității informatică ..</b>	<b>261</b>
Secțiunea I. Considerații generale .....	261

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.....	262
Secțiunea a III-a. Perspective actuale privind standardizarea activității de cercetare a infracțiunilor din sfera criminalității informatice și acreditarea laboratoarelor criminalistice .....	263
§ 1. Situația la nivel internațional .....	263
1.1. În domeniul standardizării .....	263
1.2. În domeniul acreditării .....	264
1.3. În domeniul evaluării conformității.....	264
§ 2. Situația la nivel european.....	265
2.1. În domeniul standardizării .....	265
2.2. În domeniul autorizării .....	265
2.3. În domeniul evaluării conformității .....	266
§ 3. Situația în SUA .....	266
3.1. În domeniul standardizării .....	266
3.2. În domeniul acreditării .....	267
3.3. În domeniul evaluării conformității.....	267
§ 4. Situația în România.....	268
4.1. În domeniul standardizării .....	268
4.2. În domeniul acreditării .....	269

**Capitolul IV. Procedura cercetării infracțiunilor din sfera criminalității informatice propusă .....** 272

Secțiunea 1. Necesitatea modificării/completării procedurilor de cercetare a infracțiunilor din sfera criminalității informatice .....	272
Secțiunea a II-a. Etapele/fazele cercetării infracțiunilor din sfera criminalității informatice propuse .....	274
§ 1. Activitățile premergătoare cercetării propriu-zise .....	274
§ 2. Cercetarea la fața locului .....	274
§ 3. Efectuarea perchezițiilor (sistemelor informatice, domiciliară, în alte locații).....	275
§ 4. Ascultarea persoanelor (învinuiți, martori, părți vătămate).....	276
§ 5. Examinarea dovezilor .....	277

§ 6. Finalizarea cercetărilor .....	277
Secțiunea a III-a. Aspecte privind conținutul și forma de redactare a procedurii/procedurilor .....	279
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 .....	280
§ 1. Particularități ale pregătirii cercetării/investigației .....	281
§ 2. Particularități ale căutării/conservării dovezilor materiale/digitale .....	282
§ 3. Particularități privind informațiile care trebuie furnizate de/obținute de la suspecti/învinuiți, martori, părți vătămate .....	284
3.1. Posibile întrebări cu caracter general.....	284
3.2. Posibile întrebări cu caracter particular .....	286
§ 4. Particularitățile dovezilor digitale.....	289
§ 5. Particularități ale colectării dovezilor digitale .....	290
§ 6. Particularități ale examinării dovezilor digitale .....	293
§ 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.....	296
<b>Scurte concluzii și propuneri .....</b>	<b>300</b>
<b>Bibliografie selectivă .....</b>	<b>308</b>