

Cuprins

Mulțumiri.....	5
Abrevieri.....	7
Considerații introductive.....	9
PARTEA I. ASPECTE GENERALE PRIVIND SECURITATEA SISTEMELOR INFORMATICE ȘI CRIMINALITATEA INFORMATICĂ.....	11
Capitolul I. Amenințări și tendințe în ce privește securitatea sistemelor informatice și rețelelor de comunicații.....	13
<i>Secțiunea I. Considerații generale</i>	<i>13</i>
<i>Secțiunea a II-a. Principalele taxonomii dezvoltate în sfera securității sistemelor informatice și rețelelor de comunicații.....</i>	<i>13</i>
§ 1. Palauskas N., Garsva E., Clasificarea atacurilor asupra sistemelor informatice	15
§ 2. Howard John D., Longstaff Thomas A., Un limbaj comun pentru incidentele privind securitatea calculatoarelor	18
§ 3. Weber Daniel James, O taxonomie a intruziunilor în calculatoare	22
§ 4. Lough Daniel Lawry, O taxonomie a atacurilor asupra calculatoarelor cu aplicație pentru rețelele fără fir	25
§ 5. RAND Europe, O taxonomie a incidentelor de securitate	26
Capitolul II. Conceptul, principalele caracteristici și evoluția criminalității informatice	29
<i>Secțiunea I. Considerații generale</i>	<i>29</i>
<i>Secțiunea a II-a. Conceptul „criminalitate informatică”</i>	<i>29</i>
§ 1. Noțiunea de criminalitate.....	29
§ 2. Noțiunea de criminalitate informatică	30
§ 3. Infrațiuni din sfera criminalității informatice/la regimul tehnologiei informației și comunicațiilor (TIC)	32
<i>Secțiunea a III-a. Principalele caracteristici ale criminalității informatice</i>	<i>34</i>
<i>Secțiunea a IV-a. Aspecte privind evoluția criminalității informatice</i>	<i>35</i>
§ 1. Etapele evoluției	35
§ 2. Amenințări actuale	36
§ 3. Principalii factori care influențează dezvoltarea criminalității informatice, provocări ale combaterii fenomenului.....	37

3.1. Dependența de tehnologia informației și comunicațiilor	37
3.2. Numărul utilizatorilor	37
3.3. Disponibilitatea dispozitivelor și accesului	38
3.4. Disponibilitatea informațiilor	39
3.5. Lipsa mecanismelor de control	39
3.6. Dimensiunile internaționale	39
3.7. Independența locației și prezenței la locul infracțiunii	40
3.8. Automatizarea	40
3.9. Resursele	41
3.10. Viteza proceselor de schimb de date	42
3.11. Viteza de dezvoltare	42
3.12. Comunicațiile anonime	42
3.13. Tehnologia de criptare	43
§ 4. Particularități ale evoluției fenomenului criminalității informatic în România	44
4.1. Repere temporale	44
4.2. Particularități	45
Capitolul III. Explicații criminologice ale subculturilor criminalității informatice	51
<i>Secțiunea I. Considerații generale</i>	<i>51</i>
<i>Secțiunea a II-a. O scurtă prezentare a Teoriei lui Emile Durkheim</i>	<i>51</i>
<i>Secțiunea a III-a. O scurtă prezentare a Teoriei lui Robert Merton</i>	<i>52</i>
<i>Secțiunea a IV-a. Explicarea subculturilor criminalității informatice prin prisma tipologiei modurilor individuale de adaptare dezvoltată de Merton</i>	<i>54</i>
§ 1. Conformismul navigatorilor pe Internet	56
§ 2. Inovația: hacking-ul pentru profit	56
§ 3. Ritualismul: hacking-ul ca obișnuință	57
§ 4. Retragerea: hacking-ul ca dependență	57
§ 5. Rebeliunea: hacking-ul ca nesupunere la regulile societății	57
§ 6. Hackingul non-utilitar	58
PARTEA A II-A. PREOCUPĂRI ALE SOCIETĂȚII INTERNAȚIONALE PENTRU PREVENIREA ȘI COMBATerea CRIMINALITĂȚII INFORMATICE	59
Capitolul I. Organizații internaționale și regionale cu atribuții și preocupări în prevenirea și combaterea criminalității informatice și principalele realizări	61
<i>Secțiunea I. Considerații generale</i>	<i>61</i>

<i>Secțiunea a II-a. Organizația Națiunilor Unite (UN)</i>	61
<i>Secțiunea a III-a. Grupul celor Șapte Națiuni (G7)</i>	66
<i>Secțiunea a IV-a. Uniunea Internațională a Telecomunicațiilor (ITU)</i>	70
<i>Secțiunea a V-a. Consiliul Europei (CoE)</i>	73
<i>Secțiunea a VI-a. Uniunea Europeană (EU)</i>	76

Capitolul II. Principalele instrumente juridice și recomandări cu vocație internațională și regională care conțin reglementări privind prevenirea și combaterea criminalității informatice

<i>Secțiunea I. Considerații generale</i>	79
<i>Secțiunea a II-a. Recomandarea nr. R (89) 9 asupra criminalității în relație cu calculatorul</i>	81
<i>Secțiunea a III-a. Convenția privind criminalitatea informatică</i>	83
<i>Secțiunea a IV-a. Protocolul adițional referitor la incriminarea actelor de natură rasistă și xenofobă săvârșite prin intermediul sistemelor informatice</i>	86

Capitolul III. Analiză comparativă a modului în care legislatorii naționali au implementat măsurile prevăzute de Convenția privind criminalitatea informatică

<i>Secțiunea I. Considerații generale</i>	89
<i>Secțiunea a II-a. Analiza comparativă a modului în care au fost definiți termenii utilizați</i>	90
<i>Secțiunea a III-a. Analiza comparativă a modului în care au fost incriminate infracțiunile împotriva confidențialității, integrității și disponibilității datelor</i>	92
§ 1. Accesarea ilegală	93
§ 2. Interceptarea ilegală	96
§ 3. Afectarea integrității datelor	99
§ 4. Afectarea integrității sistemului	101
§ 5. Abuzurile asupra dispozitivelor	102
<i>Secțiunea a IV-a. Analiza comparativă a modului în care au fost incriminate infracțiunile informatice</i>	105
§ 1. Falsificarea informatică	105
§ 2. Frauda informatică	108
<i>Secțiunea a V-a. Analiza comparativă a modului în care au fost incriminate infracțiunile referitoare la conținut</i>	110
§ 1. Infracțiuni referitoare la pornografia infantilă	110

<i>Secțiunea a VI-a. Analiza comparativă a modului în care au fost incriminate infracțiunile referitoare la atingerile aduse proprietății intelectuale și drepturilor conexe</i>	114
--	-----

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/la regimul tehnologiei informației și comunicațiilor (TIC)	120
<i>Secțiunea I. Considerații generale</i>	120
<i>Secțiunea a II-a. Principalele modele de cercetare a infracțiunilor din sfera criminalității informatice/la regimul tehnologiei informației și comunicațiilor (TIC) prezentate în literatura de specialitate</i>	120
§ 1. Pollit M. Mark, Paradigma digitală.....	121
§ 2. Farmer Dan, Venema Wietse, Analiza criminalistică a computerelor UNIX.....	122
§ 3. Primul Atelier de lucru de cercetare criminalistică digitală (DFRWS), Procesul de investigație în raport cu știința criminalistică digitală.....	122
§ 4. Reith Mark, Carr Clint, Gunsch Gregg, Un model criminalistic digital abstract.....	125
§ 5. Gordon R. Gary, Hosmer D. Chet, Siedma Christine, Rebovich Dan, Metodologia investigării criminalistice digitale.....	126
§ 6. Carrier Brian, Spafford H. Eugene, Un proces integrat de investigație digitală.....	128
§ 7. Baryamureeba Venansuis, Tushabe Florence, Un model avansat/îmbunătățit al procesului integrat de investigare digitală.....	129
§ 8. Ciardhuain O' Séamus, Un model extins de investigații a criminalității informatice.....	130
§ 9. Kohn Michael, Elloff JHP, Oliver MS, Model cadru pentru investigarea criminalistică digitală.....	131
§ 10. Freiling C. Felix, Schwittay Bastian, Un model comun procesului pentru răspuns la incident și investigare criminalistică digitală.....	132
<i>Secțiunea a III-a. Principalele proceduri, ghiduri, practici dezvoltate în domeniul prevenirii și combaterii criminalității informatice</i>	134
§ 1. Organizația Națiunilor Unite, Manual pentru prevenirea și controlul infracțiunilor în legătură cu calculatorul.....	135
§ 2. INTERPOL, Manualul de Investigare a Infracțiunilor privind Tehnologia Informațiilor (ITCIM).....	137

§ 3. Rețeaua Europeană a Institutelor de Criminalistică (ENFSI) Orientări pentru bune practici în examinarea criminalistică a tehnologiilor digitale.....	138
§ 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	140
§ 5. Institutul Național de Justiție din cadrul Ministerului de Justiție al SUA, Investigarea scenei „electronice” a infracțiunii: Un ghid pentru primul respondent.....	142
§ 6. Serviciul Secret al SUA, Bune practici pentru confiscarea dovezilor electronice: Un ghid de buzunar pentru prim-respondent	144
§ 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	147
§ 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.....	148
§ 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.....	150
§ 10. Institutul Național pentru Standarde și tehnologie din cadrul Ministerului Comerțului al SUA, Ghid pentru gestionarea incidentelor de securitate a calculatoarelor.....	151

**PARTEA A III-A. COORDONATELE ACTIVITĂȚII ORGANELOR
LEGISLATIVE ȘI EXECUTIVE DIN ROMÂNIA PENTRU DEZVOLTAREA
CONCEPTULUI DE PREVENIRE ȘI COMBATERE A CRIMINALITĂȚII
INFORMATICE**

Capitolul I. Prevenirea criminalității informatice	159
<i>Secțiunea I. Considerații generale privind prevenirea criminalității</i>	159
<i>Secțiunea a II-a. Măsuri specifice de prevenire a criminalității informatice.....</i>	160

Capitolul II. Incriminarea faptelor din sfera criminalității informatice/la regimul tehnologiei informației și comunicațiilor (TIC).....	162
<i>Secțiunea I. Considerații generale</i>	162

<i>Secțiunea a II-a. Analiza conținutului normelor de incriminare a faptelor din sfera criminalității informatice/la regimul tehnologiei informației și comunicațiilor (TIC)</i>	162
§ 1. Accesul ilegal la un sistem informatic.....	163
§ 2. Interceptarea ilegală a unei transmisii de date informatice.....	166
§ 3. Alterarea integrității datelor informatice	169
§ 4. Perturbarea funcționării sistemelor informatice	172
§ 5. Transferul neautorizat de date informatice.....	175
§ 6. Operațiuni ilegale cu dispozitive sau programe informatice	178
§ 7. Falsul informatic	182
§ 8. Frauda informatică.....	184
Capitolul III. Particularități ale percheziției informatice	188
§ 1. Considerații generale	188
§ 2. Reglementarea percheziției informatice.....	189
2.1. Percheziția informatică în reglementarea anterior în vigoare.....	189
2.2. Percheziția informatică în reglementarea în vigoare	189
§ 3. Încuviințarea percheziției informatice.....	190
3.1. Organele judiciare competente să dispună percheziția informatică	190
3.2. Persoanele care pot solicita încuviințarea percheziției informatice	190
3.3. Motive pentru a solicita încuviințarea percheziției informatice	191
3.4. Condiții pentru a solicita încuviințarea percheziției informatice	191
3.5. Elaborarea și înaintarea cererii de încuviințare a percheziției informatice	192
3.6. Soluționarea cererii de încuviințare a percheziției informatice	193
3.7. Emiterea mandatului de percheziție informatică	194
§ 4. Efectuarea percheziției informatice	195
4.1. Persoanele abilitate să efectueze percheziția informatică	195
4.2. Alte persoane în prezența cărora se efectuează percheziția informatică	195
4.3. Perioada în care poate fi efectuată percheziția informatică.....	196
4.4. Mijloace tehnice și proceduri folosite pentru efectuarea percheziției informatice	197
4.5. Activități prealabile efectuării percheziției informatice	197

4.6. Colectarea datelor informatice, cu ocazia percheziției informatice.....	198
4.7. Examinarea datelor informatice colectate, cu ocazia efectuării percheziției informatice	202
4.8. Întocmirea procesului-verbal de percheziție informatică.....	203
4.9. Asigurarea confidențialității datelor/informațiilor cunoscute cu ocazia percheziției informatice	204

Capitolul IV. Instituții cu atribuții în prevenirea și combaterea criminalității informatice și principalele realizări	205
<i>Secțiunea I. Considerații generale</i>	<i>205</i>
<i>Secțiunea a II-a. Structura specializată în cadrul Parchetului de pe lângă Înalta Curte de Casație și Justiție</i>	<i>205</i>
§ 1. Structura Direcției de Investigare a Infrațiunilor de Criminalitate Organizată și Terorism.....	205
§ 2. Structura Secției de combatere a infracțiunilor de terorism și a criminalității informatice.....	206
§ 3. Rolul Serviciului de combatere a criminalității informatice și atribuțiile procurorilor din cadrul acestuia.....	207
3.1. Rolul Serviciului de combatere a criminalității informatice.....	207
3.2. Atribuțiile procurorilor din cadrul Serviciului de combatere a criminalității informatice	207
<i>Secțiunea a III-a. Structura specializată în cadrul Inspectoratului General al Poliției Române</i>	<i>208</i>
§ 1. Structura Direcției de Combatere a Criminalității Organizate.....	209
§ 2. Structura Serviciului de combatere a criminalității informatice și atribuțiile polițiștilor din cadrul acestuia.....	209
2.1. Structura Serviciului de combatere a criminalității informatice	209
2.2. Atribuțiile polițiștilor din cadrul Serviciului de combatere a criminalității informatice	210
<i>Secțiunea a IV-a. Principalele realizări pe linia combaterii criminalității informatice.....</i>	<i>210</i>
§ 1. Repere statistice	210
§ 2. Cauze instrumentate.....	213
 Capitolul V. Cooperarea internațională pentru prevenirea și combaterea criminalității informatice.....	 219

**PARTEA A IV-A. PUNCTE DE VEDERE CU PRIVIRE LA
METODOLOGIA CERCETĂRII INFRAȚIUNILOR DIN SFERA
CRIMINALITĂȚII INFORMATICE/LA REGIMUL TEHNOLOGIEI
INFORMAȚIEI ȘI COMUNICAȚIILOR (TIC).....223**

Capitolul I. Conceptul investigare criminalistică digitală, status-ul și conținutul acestui proces	225
<i>Secțiunea I. Conceptul investigare criminalistică digitală</i>	<i>225</i>
<i>Secțiunea a II-a. Status-ul și conținutul procesului de investigare criminalistică digitală</i>	<i>226</i>

Capitolul II. Considerații generale cu privire la metodologia cercetării infracțiunilor din sfera criminalității informatice/la regimul tehnologiei informației și comunicațiilor (TIC).....229

<i>Secțiunea I. Clasic și nou în cercetarea infracțiunilor din sfera criminalității informatice/la regimul tehnologiei informației și comunicațiilor (TIC)</i>	<i>229</i>
<i>Secțiunea a II-a. Principiile, scopul și definiția metodologiei de cercetare a infracțiunilor din sfera criminalității informatice/la regimul tehnologiei informației și comunicațiilor (TIC)</i>	<i>230</i>
§ 1. Precizări terminologice cu privire la cercetarea penală a infracțiunilor din sfera criminalității informatice/la regimul tehnologiei informației și comunicațiilor (TIC) și investigarea criminalistică a locului faptei și a sistemelor informatice	230
§ 2. Principiile cercetării infracțiunilor din sfera criminalității informatice/la regimul tehnologiei informației și comunicațiilor (TIC) și investigării criminalistice a locului faptei și a sistemelor informatice.....	231
2.1. Principiile cercetării infracțiunilor din sfera criminalității informatice/la regimul tehnologiei informației și comunicațiilor (TIC)	231
2.2. Principiile investigării criminalistice a locului faptei și a sistemelor informatice.....	232
§ 3. Obiectivele cercetării infracțiunilor din sfera criminalității informatice/la regimul tehnologiei informației și comunicațiilor (TIC)	232
3.1. Obiectivul cercetării penale a infracțiunilor din sfera criminalității informatice/la regimul tehnologiei informației și comunicațiilor (TIC).....	232

3.2. Obiectivul investigării criminalistice a locului faptei și a sistemelor informatice	233
3.3. Obiectivele concrete ale cercetării infrațiunilor din sfera criminalității informatice	233
§ 4. Definiția metodologiei cercetării infrațiunilor din sfera criminalității informatice/la regimul tehnologiei informației și comunicațiilor (TIC).....	234

Capitolul III. Formalizarea și standardizarea activității de cercetare a infrațiunilor din sfera criminalității informatice/la regimul tehnologiei informației și comunicațiilor (TIC)	235
<i>Secțiunea I. Considerații generale</i>	<i>235</i>
<i>Secțiunea a II-a. Necesitatea standardizării activității de cercetare a infrațiunilor din sfera criminalității informatice/la regimul tehnologiei informației și comunicațiilor (TIC), de acreditare a laboratoarelor criminalistice și de certificare a specialiștilor și a mijloacelor de investigare.....</i>	<i>235</i>
<i>Secțiunea a III-a. Perspective actuale privind standardizarea activității de cercetare a infrațiunilor din sfera criminalității informatice/la regimul tehnologiei informației și comunicațiilor (TIC) și acreditarea laboratoarelor criminalistice</i>	<i>236</i>
§ 1. Situația la nivel internațional	236
1.1. În domeniul standardizării	236
1.2. În domeniul acreditării.....	237
§ 2. Situația la nivel european.....	238
2.1. În domeniul standardizării	238
2.2. În domeniul acreditării.....	238
2.3. În domeniul evaluării conformității.....	238
În domeniul evaluării conformității, la nivel european, organismul competent este Sistemul European de Testare, Inspecție și Certificare (ETICS), o asociație non-profit, care are ca scop administrarea sistemului ENEC și a altor sisteme de evaluare a conformității, cum ar fi CCA, HAR și LOVAG, evaluând conformitatea produselor cu terți, în principal în sectorul electrotehnic (dar și în alte domenii care pot fi asociate cu testarea, inspecția și certificarea produselor, proceselor și personalului)	238
§ 3. Situația în SUA	239

3.1. În domeniul standardizării.....	239
3.2. În domeniul acreditării	239
3.3. În domeniul evaluării conformității	239
§ 4. Situația în România	240
4.1. În domeniul standardizării.....	240
4.2. În domeniul acreditării	241

Capitolul IV. Procedura cercetării infracțiunilor din sfera criminalității informatice/la regimul tehnologiei informației și comunicațiilor (TIC) propusă	243
<i>Secțiunea 1. Necesitatea modificării/completării procedurilor de cercetare a infracțiunilor din sfera criminalității informatice/la regimul tehnologiei informației și comunicațiilor (TIC)</i>	<i>243</i>
<i>Secțiunea a II-a. Etapele/fazele cercetării infracțiunilor din sfera criminalității informatice/la regimul tehnologiei informației și comunicațiilor (TIC) propuse.....</i>	<i>244</i>
§ 1. Activitățile premergătoare cercetării propriu-zise	245
§ 2. Cercetarea la fața locului	245
§ 3. Efectuarea perchezițiilor (informatice, domiciliară, altele)	246
§ 4. Ascultarea persoanelor (suspecți, martori, persoane vătămate)	246
§ 5. Examinarea dovezilor	247
§ 6. Finalizarea cercetărilor	247
<i>Secțiunea a III-a. Aspecte privind conținutul și forma de redactare a procedurii/procedurilor.....</i>	<i>249</i>
<i>Secțiunea a IV-a. Particularitățile unor activități de cercetare a infracțiunilor din sfera criminalității informatice/la regimul tehnologiei informației și comunicațiilor (TIC) și de investigare criminalistică a locului faptei și a sistemelor informatice.....</i>	<i>250</i>
§ 1. Particularități ale pregătirii cercetării/investigației	250
§ 2. Particularități ale căutării/conservării dovezilor materiale/digitale	251
§ 3. Particularități privind informațiile care trebuie furnizate de/obținute de la suspecți/inculpați, martori, persoane vătămate	253
3.1. Posibile întrebări cu caracter general	253
3.2. Posibile întrebări cu caracter particular	254
§ 4. Particularități ale dovezilor digitale.....	257
§ 5. Particularități ale colectării dovezilor digitale	258
§ 6. Particularități ale examinării dovezilor digitale	258

§ 7. Particularități ale documentării cercetării și întocmirii rapoartelor (de constatare tehnico-științifică/expertiză)	259
§ 8. Particularități ale echipamentelor (hardware) și programelor (software) specializate folosite în investigarea criminalistică digitală.....	260
Scurte concluzii și propuneri	262
Bibliografie selectivă.....	267