

## Cuprins

<b>Capitolul I. Introducere.....</b>	1
<b>Capitolul II. Sisteme informaticе.....</b>	10
§1. Definiție.....	12
§2. Tipuri de sisteme informaticе.....	16
§3. Componentele sistemelor informaticе.....	17
§4. Date, informații, cunoaștere .....	20
§5. Procesele de folosire.....	22
§6. Caracteristicile sistemelor informaticе.....	22
§7. Resurse informaționale.....	26
§8. Categorii de erori.....	28
<b>Capitolul III. Amenințări și vulnerabilități .....</b>	30
§1. Potențiali atacatori ai sistemelor informaticе .....	31
§2. Amenințări și vulnerabilități.....	33
2.1. Tipuri de amenințări .....	33
2.2. Amenințările fundamentale .....	34
2.2.1. Divulgarea de informații .....	35
2.2.2. Alterarea de informații .....	35
2.2.3. Repudierea .....	35
2.2.4. Refuzul serviciului ( <i>denial of service</i> ) .....	36
2.2.5. Atacuri Denial-of-Service distribuite ( <i>DDoS</i> ) ....	36
2.2.6. Folosirea nelegitimă .....	36
2.3. Amenințările care facilitează .....	37
2.3.1. Mascara...	37
2.3.2. Contaminanți informatici (programe malicioase sau <i>malware</i> ) .....	38
2.3.3. Cai troieni informatici.....	43
2.3.4. Bombe logice informaticе ( <i>Logic Bomb</i> ).....	43
2.3.5. Viruși informatici.....	44
2.3.6. Backdoor.....	46

2.3.7. Vierme informatic.....	46
2.3.8. Spyware .....	47
2.3.9. Eludarea măsurilor de securitate.....	49
2.3.10. Violarea autorizării .....	49
2.4. Amenințările indirekte .....	50
2.4.1. Interceptare .....	50
2.4.2. Scavenging.....	50
2.4.3. Indiscreție .....	50
2.4.4. Eroare administrativă.....	51
§3. Vulnerabilități și expuneri .....	51
§4. Tehnici folosite de atacatori .....	52

<b>Capitolul IV. Cerințele operaționale și legale privind prevenirea criminalității informaticе .....</b>	<b>56</b>
§1. Noțiunea de «securitate» .....	60
§2. Cadrul legislativ românesc privind securitatea sistemelor informaticice .....	64
§3. Managementul strategic al securității sistemelor informaticice .....	67

<b>Capitolul V. Mijloace legale de prevenire a criminalității informaticе .....</b>	<b>70</b>
§1. Explicații prealabile .....	73
1.1. Noțiune .....	73
1.2. Elemente .....	73
1.2.1. Obiectul infracțiunii .....	73
1.2.2. Subiecții infracțiuni .....	74
1.2.3. Latura obiectivă .....	75
1.2.4. Latura subiectivă.....	75
§2. Infracțiuni contra confidențialității datelor și sistemelor informaticice .....	76
2.1. Accesul ilegal la un sistem informatic.....	76
2.1.1. Structura juridică .....	77
2.1.2. Conținutul constitutiv .....	78
2.1.3. Formele infracțiunii .....	82
2.1.4. Sancțiunea .....	82

---

2.2. Interceptia ilegală a unei transmisii de date informatice.....	82
2.2.1. Conținutul legal și caracterizare .....	82
2.2.2. Structura infracțiunii .....	83
2.2.3. Conținutul constitutiv .....	84
2.2.4. Formele infracțiunii .....	87
2.2.5. Sancțiunea .....	87
2.3. Alterarea integrității datelor informative .....	87
2.3.1. Conținutul legal și caracterizare .....	87
2.3.2. Structura juridică .....	88
2.3.3. Conținutul constitutiv .....	88
2.3.4. Formele infracțiunii .....	91
2.3.5. Sancțiunea .....	91
2.4. Perturbarea funcționării sistemelor informative .....	91
2.4.1. Conținutul legal și caracterizare .....	91
2.4.2. Structura juridică .....	92
2.4.3. Conținutul constitutiv .....	93
2.4.4. Formele infracțiunii .....	95
2.4.5. Sancțiunea .....	95
2.5. Operațiuni ilegale cu dispozitive sau programe informative.....	95
2.5.1. Conținutul legal și caracterizare .....	95
2.5.2. Structura infracțiunii .....	96
2.5.3. Conținutul constitutiv .....	97
2.5.4. Formele infracțiunii .....	99
2.5.5. Sancțiunea .....	99
§3. Infracțiuni informative.....	99
3.1. Falsul informatic.....	99
3.1.1. Conținutul legal și caracterizare .....	99
3.1.2. Structura infracțiunii .....	100
3.1.3. Conținutul constitutiv .....	100
3.1.4. Formele infracțiunii .....	103
3.1.5. Sancțiunea .....	103
3.2. Frauda informatică.....	103
3.2.1. Conținutul legal și caracterizare .....	103
3.2.2. Structura juridică .....	105
3.2.3. Conținutul constitutiv .....	107

3.2.4. Formele infracțiunii .....	108
3.2.5. Sanctiunea .....	109
3.3. Pornografia infantilă prin sisteme informaticе .....	109
3.3.1. Conținutul legal și caracterizare .....	109
3.3.2. Structura juridică .....	110
3.3.3. Conținutul constitutiv .....	111
3.3.4. Formele infracțiunii .....	114
3.3.5. Sanctiunea .....	114
§4. Reproducerea neautorizată a programelor informaticе protejate.....	114
4.1. Conținutul legal și caracterizare .....	114
4.2. Structura juridică .....	117
4.3. Conținutul constitutiv .....	118
4.4. Formele infracțiunii .....	121
4.5. Sanctiunea .....	121
<b>Capitolul VI. Politici și proceduri.....</b>	<b>122</b>
§1. Politici .....	122
§2. Proceduri .....	1277
§3. Responsabilități .....	128
3.1. Definirea responsabilităților funcționale .....	128
3.2. Managerii.....	1299
3.3. Angajați și utilizatori .....	129
3.4. Deținătorii datelor informaticе .....	130
3.5. Deținătorii procedurilor .....	131
3.6. Custodienii sistemelor informaticе.....	131
3.7. Infrastructura .....	131
3.8. Excepții de la procedurile de securitate .....	132
§4. Clasificarea și controlul informațiilor .....	132
4.1. Contabilitate .....	132
4.2. Inventarul informațiilor și sistemelor .....	132
4.3. Clasificarea datelor informaticе.....	133
4.4. Planuri pentru situații de urgență.....	134
4.5. Procesul de planificare a continuității operaționale .....	134
4.6. Securizarea fizică.....	136
4.6.1. Zone securizate .....	136
4.6.2. Perimetruл fizic de securitate .....	137

---

4.6.3. Controlele pentru intrarea fizică .....	137
4.6.4. Securitatea centrelor de date .....	137
4.6.5. Suport fizic .....	138
4.6.6. Deplasarea echipamentului .....	138
4.6.7. Securitatea echipamentelor .....	139
4.6.8. Așezarea și protejarea echipamentului .....	139
4.6.9. Electricitate .....	139
4.6.10. Securitatea cablajelor .....	140
4.6.11. Întreținerea echipamentelor .....	140
4.6.12. Echipamentul aflat la alte locații .....	140
4.6.13. Eliminarea echipamentului .....	141
§5. Managementul calculatoarelor și rețelelor informaticе .....	141
5.1. Documentarea procedurilor de operare .....	141
5.2. Separarea sarcinilor .....	142
5.3. Proceduri pentru managementul incidentelor informaticе .....	142
5.4. Separarea facilităților .....	143
5.5. Managementul facilităților externe .....	143
5.6. Acceptarea sistemelor informaticе .....	144
5.7. Planuri de rezervă .....	144
5.8. Schimbarea controlului .....	145
§6. Protejarea împotriva contaminanților informatici .....	145
6.1. Controlul virușilor informatici .....	146
6.2. Back-up .....	146
6.3. Înregistrarea operațiunilor informaticе .....	146
6.4. Monitorizarea mediului .....	147
§7. Managementul rețelelor informaticе .....	147
7.1. Controlele pentru securitatea rețelelor informaticе .....	147
§8. Protecția datelor personale și a aplicațiilor .....	148
§9. Manipularea suporturilor fizice .....	148
9.1. Proceduri de manipulare a datelor .....	149
9.2. Securitatea documentației sistemelor .....	149
9.3. Eliminarea suporturilor fizice .....	150
§10. Schimbul de date și programe informaticе .....	150
10.1. Securitatea suporturilor fizice în tranzit .....	150
10.2. Transferul de date între sisteme .....	151

10.3. Date informative partajate .....	151
10.4. Sisteme disponibile public.....	151
§11. Controale pentru acces la sisteme.....	152
11.1. Cerințe pentru acces.....	152
11.2. Documentarea controlului accesului.....	152
§12. Managementul accesului .....	152
12.1. Identificatori login.....	152
12.2. Securitatea parolelor .....	153
12.3. Standarde pentru alocarea parolelor .....	154
12.4. Echipamente nesupravegheate.....	155
§13. Controlul accesului la rețelele informative .....	155
13.1. Acces dial-up .....	156
13.2. Acces la sisteme externe.....	156
13.3. Autentificarea utilizatorilor .....	157
§14. Controlul accesului la aplicații .....	157
14.1. Restricționarea accesului la date informative .....	157
14.2. Folosirea utilitarelor informative .....	158
14.3. Controlul accesului la cod sursă .....	158
§15. Securitatea terțelor părți .....	159
15.1 Condiții pentru încheierea de contracte cu terțe părți .....	159
§16. Monitorizarea accesului și folosirii sistemelor informaticice .....	160
16.1. Înregistrarea evenimentelor ( <i>log-area</i> ) .....	160
16.2. Monitorizarea folosirii sistemului.....	161
16.3. Calculatoare portabile .....	161
§17. Cerințe legale.....	162
17.1. Controlul folosirii programelor informative .....	162
17.2. Protecția programelor informative .....	162
§18. Protecția datelor personale .....	162
§19. Verificarea conformității cu politicile de securitate .....	163
19.1. Conformarea cu politicile de securitate .....	163
19.2. Verificarea conformării tehnice.....	163
§20. Auditul sistemelor informative .....	164
20.1. Controale de audit.....	164
20.2. Protejarea utilitarelor de audit .....	165

§21. Mijloace tehnice de prevenire a criminalității informaticе .....	165
21.1. Analiza de risc .....	166
21.2. Atenuarea riscurilor .....	172
21.3. Etapele atenuării riscului .....	176
21.4. Controale tehnice .....	182
21.5. Sisteme de control biometric .....	186
21.6. Parole .....	186
21.7. Carduri cu cip .....	187
21.8. Sisteme de detectare a intruziunilor .....	188
21.9. Programe anti-virus .....	189
21.10. Criptografie .....	189
21.11. Firewall .....	190
21.12. Routere packet-filtering .....	190
21.13. Filtrare în funcție de serviciu .....	191
21.14. Filtrare independentă de serviciu .....	191
21.15. Standarde, factori critici și principii manageriale .....	193
<b>Index alfabetic .....</b>	<b>199</b>