

# CUPRINS

<b>Introducere</b> .....	9
<b>Capitolul 1 Managementul securității sistemelor informatice</b> .....	11
1.1 Politica de securitate .....	13
1.2 Clasificarea informațiilor în funcție de importanța lor .....	15
1.3 Riscuri asociate sistemelor informatice .....	17
1.4 Auditul sistemelor informatice .....	21
1.4.1 Planificarea .....	26
1.4.2 Derularea misiunii .....	30
1.4.3 Redactarea și prezentarea raportului .....	31
1.4.4 Urmărirea implementării recomandărilor .....	32
<b>Capitolul 2 Necesitatea managementului riscurilor sistemelor informatice</b> .....	33
2.1 Guvernanța corporativă și guvernanța IT .....	33
2.1.1 Guvernanță IT .....	35
2.1.2 Măsurarea performanței .....	40
2.2 Incidente informatice cu consecințe majore .....	43
2.2.1 Cazul UBS (2002) .....	43
2.2.2 Cazul Moody's (2008) .....	43
2.2.3 Cazul băncii Société Générale (2008) .....	44
2.3 Metode-cadru de evaluare și management al riscului informatic .....	45
2.3.1 OCTAVE .....	46
2.3.2 CobiT .....	48
2.3.3 ITIL (Information Technology Infrastructure Library- Biblioteca Infrastructurii IT) .....	54
2.3.4 COSO .....	58
2.3.5 ISO/IEC 27001 .....	61

<b>Capitolul 3 Rețele de calculatoare, Internet</b> .....	63
3.1 Scurt istoric al rețelelor de comunicații .....	63
3.2 Ce este Internetul – modelul rețelei pe 4 niveluri .....	65
3.3 Comunicarea între cele 4 niveluri .....	67
3.4 Încapsularea pachetelor .....	68
3.5 Multiplexare .....	69
3.6 Exemple de protocoale .....	71
3.7 Protocolul IP – Nivelul Rețea .....	75
3.8 Protocolul TCP .....	82
3.9 Analiza unei conexiuni TCP .....	86
3.10 Traducerea Adreselor de Rețea (NAT) – Network Address Translation .....	92
3.11 Traducerea Adreselor de Rețea (NAT) – Exemplu .....	96
<b>Capitolul 4 Soft malițios și atacuri informatice</b> .....	103
4.1 Cine (și de ce) creează malware? .....	104
4.2 Tipuri de activități malițioase și atacuri .....	105
4.3 Metode de infiltrare a programelor malware .....	116
4.4 Metode de apărare .....	128
4.5 Instrumente folosite în securitatea SI .....	132
4.5.1 Firewall .....	135
4.5.2 Reverse Proxy Server .....	154
4.5.3 Bastion host .....	155
4.5.4 VPN (Virtual Private Network) .....	156
4.5.5 Scanere de vulnerabilități .....	159
4.5.6 Instrumente de analiză a traficului de date .....	165
4.5.7 Programe de exploatare a vulnerabilităților .....	164
<b>Capitolul 5 Managementul securității informaționale și protecția sistemelor IT</b> .....	167
5.1 Premise și modele de abordare a implementării monitorizării securității .....	167
5.1.1 Descrierea soluției tehnice .....	171
5.2 Protecția activelor informaționale – baze de date și software .....	177

5.3 Arhitectura serviciilor IT și managementul portofoliului de aplicații și hardware.....	179
5.3.1 Securitatea rețelelor informatice – riscuri .....	185
5.3.2 Riscuri datorate conectării la Internet .....	186
5.4 Criptografie .....	188
5.4.1 Ce este criptografia? .....	188
5.4.2 Cum funcționează comunicarea criptată? .....	190
5.4.3 Evoluția metodelor criptografice .....	192
5.4.4 Aplicații ale sistemelor criptografice – semnături digitale.....	215
<b>Bibliografie</b> .....	<b>219</b>
<b>Abstract</b> .....	<b>227</b>
<b>Contents</b> .....	<b>229</b>