OBSAH

Úvod ... 7

1 Současné problémy bezpečnosti spojené s fenoménem globalizace a rozvojem trestné činnosti v digitálním prostředí ... 9

1.1 Globalizace současného světa ... 9

1.2 Faktory, mající vliv na závažnou kriminalitu v souvislosti s informačními technologiemi ... 11

1.3 Nové technologie se do činnosti bezpečnostních služeb promítají dvojím způsobem ... 13

1.4 Technologicky orientovaná trestná činnost v digitálním prostředí ... 15

2 Trendy rozvoje high-tech orientované trestné činnosti v digitálním prostředí ... 20

2.1 Základní historická období rozvoje trestné činnosti v digitálním prostředí ... 20

2.2 Současné technologické a sociologické hrozby v prostředí informačních a komunikačních technologií ... 27

2.3 Hrozby jako důsledek Internetu a propojování sítí ... 29

2.4 Možné nové směry rozvoje informačně komunikačních technologií a s nimi spojené nové formy práce orgánů činných v trestním řízení ... 30

2.5 Změny v přístupu a práci orgánů činných v trestním řízení ... 33

3 Kybernetická kriminalita ... 34

3.1 Charakteristika kybernetické kriminality a vymezení základních pojmů ... 34

3.2 Formy trestné činnosti páchané v informačních technologiích a jejich objasňování ... 36

4 Telekomunikační kriminalita ... 52

4.1 Faktory ovlivňující high-tech telekomunikační hrozby ... 53

4.2 Současný stav telekomunikační kriminality ... 58

5 Metodika a metody zkoumání telekomunikační kriminality ... 71

5.1 Charakteristika objektu zkoumání ... 71

5.2 Pracovní postupy ... 73

5.3 Způsob získávání údajů a jejich zdroje ... 73

5.4 Použité metody vyhodnocení a interpretace výsledků ... 74

6. Strukturální analýza telekomunikačního útoku ... 76

6.1 Vztahy mezi zúčastněnými subjekty a jejich vztah k telekomunikačním technologiím ... 76

6.2 Analýza a návrh modelu obecného telekomunikačního útoku ... 86

7 Technologické faktory vyhodnocení telekomunikační kriminality ... 114

7.1 Penetrace fixních sítí SR ... 114

7.2 Penetrace mobilních sítí SR ... 115

7.3 Penetrace VoIP SR ... 116

7.4 Poměrné zastoupení inteligentních mob. telefonů – svět celkem ... 118

7.5 Penetrace pobočkových ústředen SR ... 120

7.6 Podíl osobních počítačů infikovaných malware ... 122

7.7 Míra infekce inteligentních mobilních telefonů ... 124

7.8 Malware – míra infekce technolog. počítačů, telekom. operátorů ... 127

8 **Závěrečné vyhodnocení výsledků telekomunikační kriminality** ... 128
8.1 Vyhodnocení vzorců váh technologických variant v závislosti na čase ... 129
8.2 Vyčíslení celkového počtu možných variant útoků popsaných v rámci strukturální analýzy ... 134
8.3 Vyčíslení počtu možných variant útoku podle typu telekomunikační sítě ... 134
8.4 Vyčíslení počtu variant útoku postižitelných jednotlivými paragrafy a hlavami zákona 300/2005 Z.z. TZ pro postih zákonem definovaný na úrovni obecného útoku ... 134
8.5 Vyčíslení počtu variant útoku postižitelných jednotlivými paragrafy a hlavami zákona 300/2005 Z.z. TZ pro postih zákonem definovaný na úrovni technologické varianty útoku ... 135
8.6 Vyčíslení počtu variant útoku postižitelných jednotlivými paragrafy a hlavami zákona 300/2005 Z.z. TZ pro postih zákonem definovaný na úrovni obecného útoku a na úrovni technologické varianty útoku ... 136
8.7 Vyčíslení počtu variant útoku postižitelných jednotlivými paragrafy a hlavami zákona 300/2005 Z.z. TZ a v závislosti na unikátním vzorci pro vyhodnocení váhy techno-logické varianty útoku ... 138
8.8 Vyčíslení výsledných metrik popisujících technologický potenciál možných útoků pro jednotlivé hlavy zákona 300/2005 Z.z. TZ ... 140
8.9 Srovnání se statistikou vývoje kriminality podle jednotlivých hlav TZ získanou ze statistik Generální prokuratury SR ... 141

9 **Závěr analýzy telekomunikační kriminality** ... 143

10 **Digitální stopa z pohledu kriminalistické a forenzní praxe** ... 147
10.1 Vymezení základních pojmů ... 148
10.2 Počítačová kriminalita (computer crime) ... 151
10.3 Kriminalita počítačově související (computer related crime) ... 153
10.4 Kybernetická kriminalita (cyber crime) ... 156
10.5 Kriminalita kybernetický související (cyber related crime) ... 157
10.6 Informační a informatická kriminalita ... 157
10.7 Digitální stopa ... 159
10.8 Definice digitální stopy ... 161
10.9 Obecný význam definice digitální stopy ... 165
10.10 Digitální stopa a její místo v klasické teorii stop ... 166
10.11 Kriminalistické, forenzní a jinak využitelné digitální stopy ... 169
10.12 Digitální stopy z pohledu kriminalistické kategorizace stop ... 170
10.13 Paměťové a materiální stopy ... 172
10.14 Stopy obsahující informaci o základní struktuře působících objektů ... 173
10.15 Stopy převažujících charakteristik odráženého objektu nebo subjektu ... 174
10.16 Stopy dle předmětu zkoumání informačního obsahu ... 174
10.17 Stopy dle objemu, hmotnosti, rozměrů nebo viditelnosti ... 175
10.18 Stopy interakce při jejich vzniku ... 175

10.19 Sdružené stopy ... 176
10.20 Kategorizace stopy ... 176
10.21 Zařazení digitální stopy ... 177
10.22 Zdroje digitální stop ... 178
10.23 Digitální stopy a místo trestného činu ... 180
10.24 Charakteristiky a specifika digitálních stop ... 182
10.25 Klíčové oblasti praktického využití digitálních stop ... 192

11 Základní modely forenzního zpracování digitálních stop ... 195
11.1 Digitální stopa jako výsledek určitého procesu ... 195
11.2 Proč potřebujeme metodologické postupy ... 197
11.3 Terminologie ... 197
11.4 Computer Forensic Investigative proces (1984) ... 199
11.5 DFRWS Investigative Model (2001) ... 199
11.6 Abstract Digital Forensic Model (2002) ... 201
11.7 Integrated Digital Investigation Process (2003) ... 201
11.8 Enhanced Digital Investigation Process Model (2004) ... 203
11.9 Computer Forensic Field Triage proces Model (2006) ... 204
11.10 Digital Forensic Model based on Malaysian Investigation Process (2009) ... 206
11.11 Ostatní vyšetřovací procesy a jejich modely ... 207
11.12 Identifikace obecných fází modelů digitálního vyšetřování ... 210
11.13 Závěr ... 212

12 Vybrané aspekty personální bezpečnosti obecně a v digitálním prostředí ... 214
12.1 Pojem osobnost ... 216
12.2 Metody a postupy poznávání osobnosti zájmového jedince ... 219
12.3 Osobnostní faktory ... 220
12.4 Pozorování ... 222
12.5 Biografická metoda ... 223
12.6 Analýza činnosti a jejích výsledků ... 223
12.7 Metodika vedení vyšetřovacího rozhovoru ... 224
12.8 Navazování a posilování kontaktu při rozhovoru ... 226
12.9 Forenzně psychologický audit ... 227
12.10 Osobní rizikové faktory ... 229
12.11 Osobnost rizikového jedince z pohledu forenzní psychologie ... 230

13 Motivace a znalosti pachatelů v kybernetickém prostoru ... 236

Seznam zkratek a značek ... 244

Slovník termínů ... 246

Literatura ... 247