

Obsah

Místo úvodu trocha beletrie...	1
<i>Kniha první:</i>	
Počítačové viry z pohledu laika a mírně pokročilého uživatele	3
1. Definice a základní vlastnosti počítačového viru	3
<i>Co je to počítačový virus?</i>	3
2. Počítačový virus a operační systém	5
2.1. <i>Virus a MS-DOS</i>	6
2.2. <i>Virus a Windows</i>	7
2.3. <i>Virus a Unix/Linux</i>	12
2.4. <i>Virus a jiné operační systémy</i>	15
2.5. <i>Virus a Java</i>	16
2.6. <i>Problémy (ne)destruktivity virů</i>	17
3. Dělení počítačových virů	19
3.1. <i>Viry podle umístění v paměti</i>	19
3.2. <i>Viry podle cíle infekce</i>	22
3.3. <i>Viry podle koncepce návrhu a projevů chování</i>	32
4. Virům podobné počítačové hrozby	40
4.1. <i>Trojské koně</i>	40
4.2. <i>Makroviry</i>	41
4.3. <i>Červi</i>	47
4.4. <i>Bomby</i>	49
4.5. <i>Virové hrozby a WAP</i>	50
4.6. <i>Kryptoviry jako budoucí směr vývoje?</i>	51

5. Virová etika a pohnutky tvůrců virů	53
6. Základní antivirové prostředky a mechanismy	57
6.1. <i>Softwarové prostředky</i>	57
6.2. <i>Prostředky s podporou hardwaru</i>	70
6.3. <i>Neuronové sítě a viry</i>	71
7. Metodické uživatelské postupy antivirové kontroly a ochrany	
7.1. <i>Příznaky přítomnosti viru na počítači</i>	72
7.2. <i>Základní odvirovací praktiky</i>	78
7.3. <i>Základní bezpečnostní praktiky</i>	81
8. Počítačové viry a Internet	85
8.1. <i>Potenciální možnosti virového útoku</i>	86
8.2. <i>Informační zdroje a (anti)virově zaměřené servery</i>	87

Kniha druhá:

Počítačové viry z pohledu programátora – virologa	99
1. Programová podpora pro práci s viry	99
2. Nejfrekventovanější virová přerušení	107
2.1. <i>Volání BIOSu a dokumentovaných služeb Dosu</i>	108
2.2. <i>Použití nedokumentovaného Dosu</i>	115
3. Obecné virové mechanismy	117
3.1. <i>Zjištění přítomnosti viru v paměti</i>	117
3.2. <i>Zjištění přítomnosti viru v souboru</i>	119
3.3. <i>Zjištění adresy viru v paměti</i>	121
3.4. <i>Přesměrování vektorů přerušení na tělo viru</i>	121
3.5. <i>Rezidentní instalace</i>	123
3.6. <i>Obsluha kritické chyby Dosu</i>	129
3.7. <i>Charakteristické okamžiky infekce virem</i>	129
3.8. <i>Typický mechanismus infekce souborových virů</i>	131
3.9. <i>Simulace zavedení operačního systému</i>	132
4. Základní virové konstrukce	135
4.1. <i>Konstrukce bootovacího viru</i>	135
4.2. <i>Konstrukce souborového viru COM</i>	144
4.3. <i>Konstrukce souborového viru EXE</i>	148

4.4. Konstrukce souborového SYS-viru	155
4.5. Konstrukce souborového duplicitního viru	166
4.6. Konstrukce polymorfních virů	168
4.7. Konstrukce virů stealth	176
4.8. Konstrukce tunelujících virů	179
4.9. Konstrukce Windows virů	183
4.10. Konstrukce generátorů virů	195
4.11. Konstrukce makroviru	197
4.12. Konstrukce javového viru	204
4.13. Konstrukce skriptovacího červa	206
5. Obranné virové mechanismy	208
5.1. Pasivní obrana	208
5.2. Aktivní obrana	209
5.2.1. Přesměrování ladících přerušeni	209
Slovníček použitých pojmů a zkratek	218
Rejstřík	221