

## OBSAH

Úvod .....	9
<b>1 Historie a současnost informatiky.....</b>	<b>11</b>
1.1 Z historie přenosu a zpracování dat.....	11
1.2 Kybernetický útok .....	13
1.3 Nové hrozby současného světa.....	15
1.4 Společenskopolitické souvislosti rozvoje a postavení informatiky.....	15
1.5 Pojem „masová komunikace“ .....	16
1.6 Jak se informatika stává rozhodujícím faktorem moderní společnosti? .....	18
1.7 Informatika a informační věda .....	19
1.8 Hrozba a riziko .....	22
1.9 Rozpor mezi mírou osobních svobod a nutností obrany společnosti .....	23
1.10 Problém přístupu k soukromí občana.....	23
1.11 Významné etapy rozvoje moderní informatiky .....	24
1.12 Výběr významných událostí v historii internetu .....	25
1.13 Informační systémy .....	26
1.14 Základní východiska bezpečnosti informačních systémů .....	27
1.15 Možné scénáře útoku.....	28
1.16 Problém ochrany informací jako základní projev uvědomělého vlastnictví.....	30
1.17 Bezpečnostní protipatření v informatice z hlediska aktuálních hrozeb.....	31
1.18 Česká legislativa řešící informační bezpečnost.....	33
<b>2 Technika počítačů a komunikačních systémů .....</b>	<b>34</b>
2.1 Úvod do tématu .....	34
2.2 Číselné soustavy .....	34
2.3 Booleova algebra.....	38
2.4 Transformace mezi spojitém a digitálním obrazem informace.....	39
2.5 Sjednocená interpretace alfanumerických znaků .....	40
2.6 Informační systémy .....	42
2.7 Přenos dat vysokými rychlostmi .....	43
2.8 Vzájemné propojování počítačových sítí .....	46
2.9 Nejpoužívanější přenosové prostředky .....	52
2.10 Principy počítače .....	53

2.11	Popis základních bloků počítače dle architektury von Neumanna.....	54
2.12	Programování .....	57
<b>3</b>	<b>Analýza rizik a bezpečnostní politiky informačních systémů .....</b>	<b>60</b>
3.1	Obsah analýzy .....	60
3.2	Analýza rizik - aktiva .....	61
3.3	Analýza rizik - hrozby .....	63
3.4	Vlastní analytické činnosti .....	65
3.5	Bezpečnostní protopatření.....	68
3.6	Několik příkladů současných problémů informační bezpečnosti.....	71
3.7	Míra rizika.....	72
3.8	Metody analýzy rizik.....	74
3.9	Metodika analýzy rizik dle ISO-IEC TR 13335-3 (vybrané kroky) .....	76
3.10	Příklad použití metody DELPHI .....	79
3.11	Cíl bezpečnosti .....	80
3.12	Problém bezpečnostní politiky .....	80
3.13	Bezpečnostní politika informačního systému.....	83
3.14	Nástroje hodnocení bezpečnosti informačních systémů .....	85
3.15	Problém škodlivého software (malware).....	86
3.16	Interní bezpečnostní audit .....	87
3.17	Legislativní opora činnosti .....	89
3.18	Příloha 1 ke kapitole (citace některých částí vyhlášky č.523/2005 Sb.).....	90
<b>4</b>	<b>Kryptografie.....</b>	<b>93</b>
4.1	Kryptografie nejúčinnější nástroj bezpečnosti informací.....	93
4.2	Vysvětlení pojmů kryptologie a kryptografie, historické souvislosti .....	94
4.3	Cíl kryptografie .....	97
4.4	Základní rozdělení kryptografických algoritmů.....	98
4.5	Symetrické šifry .....	99
4.6	Asymetrické šifry .....	99
4.7	Perfektní šifra .....	102
4.8	Kryptologická analýza.....	102
4.9	Příklady jednotlivých typů šifer .....	103
4.10	Autentizace.....	106
4.11	Problém národního kryptografického prostředí (NKP).....	107

4.12	Elektronický podpis.....	108
<b>5</b>	<b>Počítačová kriminalita .....</b>	<b>110</b>
5.1	Popis významu jednotlivých pojmů .....	110
5.2	Potenciální hrozby páčání trestné činnosti v kyberprostoru.....	111
5.3	Legislativa, podle které lze počítačovou kriminalitu postihovat.....	113
5.3.1	Úloha policie a justice při postihování počítačové kriminality. ....	114
5.3.2	Počítačová kriminalita a společnost .....	114
5.3.3	Chápání bezpečnosti při používání počítačů .....	115
5.3.4	Kybernetická kriminalita .....	115
5.3.5	Klasifikace podle mezinárodní dohody o kyberzločinu .....	115
5.3.6	Klasifikace podle dopadu konkrétního skutku .....	116
5.4	Nové typy protiprávního jednání.....	117
5.5	Metody pachatelů kybernetičtí .....	120
5.6	Terorismus a jeho projekce do kyberprostoru.....	121
5.7	Kriminalita spojená s používáním elektronických prostředků .....	122
<b>6</b>	<b>eGovernment.....</b>	<b>123</b>
6.1	Základní registry .....	123
6.2	Informační systémy veřejné správy (ISVS) .....	125
6.3	Příklady ISVS.....	126
6.4	Informační systém datových schránek (ISDS).....	127
6.5	Způsob určení okamžiku doručení dokumentu. ....	128
6.6	Portál veřejné správy (PVS).....	129
6.7	Czech POINT .....	131
<b>7</b>	<b>Spisová služba .....</b>	<b>132</b>
7.1	Vymezení pojmů .....	132
7.2	Spisová služba.....	133
7.3	Povinnosti původců.....	134
7.4	Spisový řád .....	135
7.5	Práce s dokumenty .....	136
7.6	Spisovna .....	137
7.7	Skartační řízení.....	137
7.8	Soustava archivů v České republice.....	138

7.8.1	Národní archiv .....	138
7.8.2	Archiv bezpečnostních složek .....	138
7.8.3	Specializované archivy .....	139
7.8.4	Státní oblastní archivy .....	139
7.8.5	Archivy územních samosprávných celků .....	140
7.8.6	Názvy archivů a jejich zkratky .....	140
<b>Seznam literatury .....</b>		<b>147</b>