

OBSAH

Úvod	6
/1. díl - Mgr. Vladimír Čížek/	
1 Úvod do informačních technologií	8
1.1 Vznik internetu	8
1.2 Internet v ČR	8
1.3 Internet	9
1.4 Struktura internetu	10
1.5 Způsoby připojení	11
1.6 Domény	12
1.7 Základní služby	14
1.8 Webová adresa	16
1.9 Internetový prohlížeč	17
1.10. Vyhledávání informací na Internetu	19
1.11. Webová prezentace	20
1.11.1. Webhosting	20
1.11.2. Jazyk HTML - Hypertext Markup Language	21
1.12. Etika a právo na internetu	46
2 Informační zdroje	48
2.1. Výběr definic	48
2.1.1. Data a informace	48
2.1.2 Zpráva	48
2.1.3. Média	48
2.1.4. Masmédia	49
2.1.5. Komunikace	49
2.1.6. Agentura	50
2.2. Zajímavé zdroje na internetu	50
2.2.1. Parlamentní servery, servery veřejné správy,	50
2.2.2. Ekonomické servery a mezinárodní organizace na internetu	50
2.2.3 Tiskové agentury	51
2.2.4. Další zajímavé odkazy	51
3 Zpracování elektronických informací	52
3.1. Zpracování elektronických dokumentů	52
3.2. Zásady pro prezentaci informací	58
3.3. Přijatelný elektronický formát - PDF	58
3.4. Etika nejen internetové žurnalistiky	59
/2. díl - doc. Ing. Oldřich Pekárek/	
4 Boj o infromatický prostor	60
5 Informační systém	63
6 Bezpečnost informací	66
6.1 Bezpečnostní funkce [4,16]	67
6.2 Jak stanovit bezpečnostní požadavky	67
6.3 Kriteria bezpečnosti informačních systémů, hodnocení bezpečnosti [4,11,LA19]	68

7	Bezpečnostní politiky, cíle a strategie	69
	7.1 Bezpečnostní politika organizace	69
	7.2 Bezpečnostní politika informačního systému	70
	7.3 Role a odpovědnosti v bezpečnostní politice	71
8	Bezpečnostní prvky IS	73
	8.1 Aktiva	73
	8.2 Hrozby	74
	8.3 Bezpečnostní protipatření	75
	8.4 Riziko	76
9	Analýza rizik	78
	9.1 Typy analýzy rizik	79
	9.2 Zvládání rizik	80
10	Havarijní plán	86
11	Bezpečnostní audit a monitoring	87
12	Bezpečnostní informovanost a vzdělávání	88
13	Fyzická a administrativní bezpečnost	90
14	Personální bezpečnost	91
15	Škodlivý software	92
	15.1 Typy virů a způsoby virové nákazy [13]	92
	15.2 Možnosti napadení viry	93
	15.3 Aktualizace antivirových programů	94
16	Systém managementu bezpečnosti informací - ISMS	95
17	Možné modely bezpečnosti IS	99
	17.1 Model „Všichni uživatelé mají potřebu znát“	99
	17.2 Model „Ne všichni uživatelé mají potřebu znát“	99
	17.3 Model „Víceúrovňová bezpečnost“	100
	17.4 Modely Bell - La Padula a Biba	100
18	Bezpečnostní protipatření	102
	18.1 Hesla a osobní identifikační čísla	103
	18.2 Magnetické karty	103
	18.3 Čipové karty	104
19	Základy kryptografie	105
	19.1 Základní rozdělení kryptografických algoritmů [5,7,]	107
	19.2 Kryptologická analýza	109
	19.3 Směry dalšího rozvoje	110
20	Elektronický podpis	112
	20.1 Funkce certifikační autority	114
	20.2 Funkce kryptografického kontrolního součtu	115
21	Role státní správy při budování informatické společnosti	116
	21.1 Problém elektronické podatelny	116
	21.2 Stručný výpis ze základních legislativních norem, které se vztahují k problematice elektronické podatelny	118
	Závěr	121
	Slovník některých použitých odborných výrazů	122
	Literatura	124
	Legislativní akty	125
	Normy	126
	Přílohy A, B, C, D	127
	V edici vysokoškolské učebnice a skripta VŠERS již vyšlo	137