

OBSAH

Předmluva	7
1. Pojem informace, data a informační bezpečnost	9
1.1 Obecné poznámky	9
1.2 Pojem informace a data	10
1.3 Systém a informační systém	14
1.4 Vymezení pojmu informační bezpečnost	16
1.5 Základní pojmy a názvosloví informační bezpečnosti	17
1.6 Formulace disciplíny teorie informační bezpečnosti	20
2. Bezpečnostní hrozby a rizika	23
2.1 Druhy hrozeb v informační bezpečnosti	23
2.2 Hrozby v informačních systémech	25
2.3 Hrozby databázové bezpečnosti	26
2.4 Pojem a podstata rizika v informační bezpečnosti	27
2.5 Bezpečnostní incidenty a jejich minimalizace	29
2.5.1 Charakteristika bezpečnostních incidentů	29
2.5.2 Minimalizace incidentů	31
2.6 Prevence bezpečnostních incidentů	32
2.7 Normy informační bezpečnosti	33
3. Útoky a útočníci na data a informace	37
3.1 Úvodní poznámky	37
3.2 Způsoby úniku informací	38
3.3 Klasifikace útočníků na informační systém organizace	39
3.4 Charakteristika útoků na data a informace	41
3.5 Útoky proti integritě a utajení dat	44
3.6 Útoky na počítačové sítě	48
3.7 Útoky na kryptografické algoritmy	51
4. Bezpečnostní politika organizace	55
4.1 Pojem bezpečnostní politika organizace	55
4.2 Obsah a druhy bezpečnostní politiky	56
4.3 Výhody a přínosy bezpečnostní politiky organizace	59
4.4 Typy bezpečnostních politik organizace	60
4.5 Základní principy bezpečnostní politiky organizace	61
4.6 Problematika a nedostatky při realizaci bezpečnostní politiky organizace	62

5. Proces řešení informační bezpečnosti	65
5.1 Úvodní poznámky	65
5.2 Postup řešení informační bezpečnosti	66
5.3 Etapy řešení informační bezpečnosti	67
5.4 Možný postup řešení informační bezpečnosti	76
5.5 Řízení informační bezpečnosti	77
5.6 Problémy v procesu řešení informační bezpečnosti	80
6. Kryptologie v informačních systémech	83
6.1 Základní pojmy kryptologie	83
6.2 Kryptologické principy a šifrovací systémy	85
6.3 Proudové a blokové šifry	87
6.4 Symetrické šifry	88
6.5 Asymetrické šifry	90
6.6 Hodnocení bezpečnosti kryptografických modulů	91
6.7 Podstata a význam elektronického podpisu při komunikaci	93
7. Počítačové viry a škodlivé kódy	101
7.1 Mechanismus nákazy	102
7.2 Druhy počítačových virů	102
7.3 Možnosti ochrany proti počítačovým virům	106
7.4 Škodlivé kódy	111
7.5 Hacking	112
7.6 Cracking	117
7.7 Spamming	119
7.8 Spyware, problém s únikem dat z počítače	124
8. Počítačová a informační kriminalita	127
8.1 Úvodní poznámky	127
8.2 Charakteristika počítačové kriminality	129
8.3 Různá pojetí počítačové kriminality	130
8.4 Základní skupiny počítačové kriminality	132
8.5 Pachatelé počítačové kriminality	136
8.6 Odhalování počítačové a informační kriminality	137
8.7 Trendy počítačové kriminality	140
8.8 Doporučení pro omezení počítačové kriminality	142
9. Informační válka a kyberterorismus	145
9.1 Pojem informační válka	145
9.2 Druhy informační války	147
9.3 Informační operace a průběh informační války	150

9.4	Pojem a podstata kyberterorismu	152
9.5	Trendy kyberterorismu	154
10.	Právo na svobodný přístup k informacím	157
10.1	Právo na informace ve veřejné správě ČR	158
10.2	Obecná právní úprava a zákon č. 106/1999 Sb., o svobodném přístupu k informacím	159
10.3	Speciální právní úprava a zákon č. 123/1998 Sb., o právu na informace o životním prostředí	167
10.4	Právo na informace v Evropské unii	170
11.	Současná právní úprava ochrany informací	173
11.1	Ochrana utajovaných informací	174
11.2	Ochrana osobních údajů	188
11.3	Ochrana ostatních informací	195
12.	Právní následky za porušení zákonné ochrany informací	199
12.1	Postih pracovněprávní ve vztahu k porušení povinnosti mlčenlivosti a konkurence	199
12.2	Postih občanskoprávní	204
12.3	Správní postih	205
12.4	Trestní postih	209
Závěr		213
Literatura		215