

OBSAH:

0.	Úvod	11
1.	Informace a informační systém v podnikání	12
1.1	Význam informací pro podnikání	12
1.2	Pojem informace	13
1.3	Informační systém	14
1.4	Pracujeme s informacemi (informační proces)	15
1.4.1	Získávání informací pro vlastní podnikání	16
1.4.2	Přenos informace	18
1.4.3	Registrace, ukládání, využívání informací	20
1.4.4	Zpracovávání informací	20
1.4.5	Druhy informací určených ke zpracovávání	22
1.4.6	Požadavky analytického procesu na informace	23
1.4.7	Redukce prvotních informací	23
1.4.8	Postup analytického zpracovávání informací	24
1.4.9	Faktory ovlivňující úroveň analytické práce a její výsledky	25
1.5	Informační systém v podmínkách zpracovávání informací pomocí výpočetní techniky	26
1.5.1	Význam a důvod budování efektivního informačního systému	27
1.5.2	Způsoby vybudování informačního systému s využitím výpočetní techniky	28
1.5.3	Systém pro automatizaci administrativních činností	28
2.	Význam ochrany informací	29
2.1	Komplexnost pojetí ochrany informací	29
2.1.1	Systém vlastnictví z hlediska možného napadání protispolečenskou či trestnou činností	30
2.1.2	Systém činnosti objektu podnikání	31
2.2	Ohrožování a možnosti napadení informačního systému	32
2.3	Ochrana informací a informačního systému	34
2.4	Bezpečnostní management a jeho úloha při ochraně informací	37
3.	Příčiny a důvody úniků, ztrát a zneužívání informací	38
3.1	Informace a zločin – zločin a informace	40
3.2	Některé vybrané příčiny a podmínky zločinnosti v oblasti práce s informacemi	44
3.3	Vliv lidského faktoru z hlediska kriminologie	50
3.4	Kriminologická prevence ohrožení informací	51

3.5	Možná preventivní opatření v jednotlivých fázích práce s informacemi	52
3.5.1	Ve fázi projektování informační činnosti a systémů.	52
3.5.2	Ve fázi zavádění systému a procesů	54
3.5.3	Ve fázi fungování (běžného procesu) systému	56
3.5.4	Ve fázi ukončení (likvidace).....	57
4.	Způsoby získávání informací, pronikání do informačních systémů	58
4.1	Získávání informací obecně	58
4.2	Získávání informací v automatizovaných informačních systémech	59
4.3	Průmyslová špionáž – strašidlo nebo skutečnost?	61
4.4	Kdy a kde důležité informace nejčastěji unikají?	61
4.5	Odkud se informace získávají	63
4.6	Využití technických prostředků k získávání informací	64
4.7	Jak se bránit „tichému“ organizovanému zločinu? Čím hledat štěnice?	66
4.8	Kdy řešit informační bezpečnost systému	67
4.9	Bezpečnostní incident	68
4.10	Informační rizika	69
4.10.1	Únik informace	70
4.10.2	Ztráta dostupnosti informace	70
4.10.3	Ztráta integrity informace	70
4.10.4	Ztráta důvěryhodnosti (důvěrnosti)	70
4.10.5	Cesty k minimalizaci rizika	71
5.	Lidský faktor v ochraně informací	72
5.1	Pojetí informace z hlediska psychologie	72
5.2	Kvalitativní psychologické pojetí informace	73
5.3	Komunikace z pohledu psychologie	74
5.4	Psychologická ochrana informace	75
6.	Ochrana informací z hlediska práva	77
6.1	Úvod do systému právní ochrany informací	77
6.1.1	Proč chránit informace	77
6.1.2	Základní přístup k budování systému právní ochrany informací	78
6.2	Nástroje právní ochrany informací	81
6.2.1	Ochrana státního, hospodářského a služebního tajemství	81
6.2.2	Ochrana osobních údajů v informačních systémech	84

6.2.3	Právní úprava ochrany obchodního tajemství	92
6.2.4	Úloha pracovněprávních předpisů při ochraně informací	100
6.2.4.1	Sankce za porušení povinnosti	102
7.	Budování systému ochrany informací	104
7.1	Úvod do problematiky	104
7.2	Bezpečnost informačního systému	104
7.3	Důvěryhodný systém	106
7.4	Roviny informační bezpečnosti	107
7.5	Návrh optimálních opatření	111
7.6	Oblasti opatření v ochraně dat	113
7.7	Bezpečnostní politika	113
7.8	Bezpečnostní analýza	116
7.8.1	Obsah analyzovatelných prvků ochrany informačního systému.....	117
7.8.2	Metodika CRAMM	120
7.9	Fáze vývoje informačního systému	122
7.10	Bezpečnostní projekt	127
7.10.1	Projektování informačního systému	128
7.11	Problémy při budování bezpečných informačních systémů	130
7.12	Havarijní inženýrství	131
8.	Fyzická (technická) bezpečnost	132
8.1	Výklad základního pojmu	132
8.2	Objekty a prvky jejich ochrany	133
8.3	Strážní služba a střežení objektu	134
8.4	Monitorovací systémy	135
8.4.1	Elektrické zařízení řízeného vstupu a pohybu	135
8.4.2	Systémy průmyslové televize	135
8.5	Mechanické zábranné systémy a jejich rozdělení	136
8.5.1	Mechanické zábranné prostředky obvodové ochrany	137
8.5.2	Bezprostřední vnější ochrana objektu	138
8.6	Vstupní otvorové výplně	140
8.6.1	Základní třídění zámků	140
8.6.2	Bezpečnostní uzamykací systémy	141
8.6.3	Bariérové závory	141
8.6.4	Profilové cylindrické vložky	142
8.6.5	Magnetický kódovací systém	142
8.6.6	Zařízení generálního klíče	142
8.6.7	Uzavírání oken	142

8.7	Úschovná místa	143
8.7.1	Rozdělení úschovných objektů	143
8.7.2	Směry vývoje úschovných objektů	146
8.8	Programovatelné zámky pro prostředky výpočetní techniky	146
8.9	Technické elektrické zabezpečení	147
8.9.1	Elektrická požární signalizace (EPS)	147
8.9.2	Elektrická zabezpečovací signalizace (EVS)	148
8.10	Klimatizační zařízení	149
9.	Režimová ochrana	150
9.1	Systém režimové ochrany	150
9.2	Základní dokumenty režimové ochrany	151
9.3	Ochrana spisové agendy	151
9.4	Dokumentace pro jiné způsoby ochrany	152
9.5	Režimová ochrana informačních středisek	153
9.6	Režimová ochrana a její vztah k procesu řízení organizace	154
10.	Hardwarová ochrana	155
10.1	Ochrana hardware	155
10.2	Ochrana nosičů informací	156
10.3.	Hardwarová ochrana osobních počítačů	157
10.3.1	Ochrana disku počítače	157
10.3.2.	Bezpečnostní karty	157
10.3.3	Čipové karty	158
10.3.4	Identifikační karty	159
10.3.5	Optické paměťové karty	161
10.3.6	Ostatní prostředky ochrany osobních počítačů	162
11.	Softwarová ochrana	163
11.1	Ochrana dat v osobních počítačích	163
11.1.1	Ochrana programového vybavení	163
11.1.2	Poplachové a dohlížecí procedury	164
11.1.3	Bezpečnost systémových programů	165
11.1.4	Bezpečnost a ochrana informací. Duhová série	167
11.2	Programovatelné zámky	168
11.3	Identifikace uživatelů terminálu	170
11.4	Autorizační schemata	171
11.5	Ochrana závislá na obsahu zabezpečované informace	174
11.6	Ochrana informací na magnetických médiích	174
11.7	Počítačové viry	175
11.7.1	Charakteristika počítačových virů	175

11.7.2	Mechanismus nákazy	176
11.7.3	Druhy počítačových virů	176
11.7.4	Možnosti ochrany proti počítačovým virům	178
11.7.4.1	Preventivní opatření	178
11.7.4.2	Antivirová ochrana	180
11.7.4.3	Postup při odstraňování virů	181
12.	Personální ochrana	183
12.1	Metody a postupy získávání firemních informací	183
12.2	Potřeba výběru vhodných pracovníků organizace	184
12.3	Získávání nových spolupracovníků	185
12.4	Výběr pracovníků	190
12.5	Nejčastější chyby při výběru uchazečů o zaměstnání	193
12.6	Uvolňování pracovníků z organizace	195
13.	Ochrana informací v sítích	197
13.1	Obecně o šifrování	197
13.2	Základní kryptografické principy	198
13.3	Kódovací postupy	198
13.4	Hodnocení bezpečnosti kryptografických modulů	201
13.5	Ochrana dat v sítích	201
13.5.1	Bezpečnost v sítích LAN	203
13.5.2	Bezpečnost v sítích WAN	204
13.5.3	Bezpečnost v síti INTERNET	205
13.6	Bezpečnost EDI systémů	207
13.7	Bezpečnostní řešení v UN/EDIFACT	211
13.8	Význam a funkce certifikační autority	212
13.9	Další bezpečnostní opatření	213
13.10	Řešení na straně uživatelů	213
14.	Správa ochrany informací	216
14.1	Správa informační bezpečnosti	216
14.2	Bezpečnostní management – postavení	217
14.2.1	Kompetence (práva)	218
14.2.2	Odpovědnost (povinnosti)	218
14.2.3	Působnost	218
14.2.4	Vztahy bezpečnostního manažera v rámci organizace	219
14.2.5	Materiální vybavení	219
14.2.6	Personální zajištění	219
14.2.7	Činnost bezpečnostního managementu	220
14.3	Charakteristické výkonné funkce v informačním systému	221

14.3.1	Správce bezpečnosti informační soustavy	221
14.3.2	Správce WAN	222
14.3.3	Správce DEC	222
14.3.4	Správce LAN	222
14.3.5	Aplikační programátor	223
14.3.6	Správce aplikační úlohy	223
14.3.7	Správce technických prostředků	223
14.3.8	Uživatel osobního počítače	223
14.4	Vedení záznamů o aktivitách systému	223
14.5	Príznaková analýza a možnosti jejího užití	224
14.5.1	Klasifikace jevů a informací o jevech	225
14.5.2	Podmínky užití příznakové analýzy	225
14.5.3	Proces analýzy v příznacích	227
14.6	Jak dál v budoucnosti- strategické řízení podniku v souladu s ochranou informací	228
15.	Počítačová kriminalita	230
15.1	Vymezení pojmu počítačová kriminalita	230
15.2	Situace v zahraničí	232
15.3	Mezinárodní konvence a počítačová kriminalita	233
Závěr		235
Použitá a doporučená literatura		236