

OBSAH

Předmluva	3
Úvod	5
1. Rizikové faktory, chybovost systémů, soukromí jednotlivců a obchodní tajemství	11
1.1 Rizikové faktory	11
1.2 Chyby způsobené informační technologií	24
1.3 Právo na soukromí jednotlivců a obchodní tajemství	32
2. Postup návrhu kontrolních opatření	45
2.1 Klasifikace potenciálních narušitelů	48
2.2 Účinnost ochranných opatření	51
2.3 Hodnota chráněných údajů	52
2.4 Cena za ztrátu dat	54
2.5 Zpřesnění rozpočtu	54
3. Kontroly přesnosti (správnosti) při dávkovém zpracování dat	57
3.1 Přezkoušení dat	57
3.2 Ověření správnosti dat	58
3.3 Základní typy kontrol	58
3.4 Kontrola znaků a polí	60
3.5 Kontrola transakcí	62
3.6 Kontroly dávek	63
3.7 Kontrola správnosti zpracování	64
3.8 Organizace zpracování	65
4. Kontroly přesnosti (správnosti) v systémech s prací v reálném čase	69
4.1 Psychologie vzniku chyb	71
4.2 Typy kontrol	72
4.3 Kontroly v rámci jedné transakce	73
4.4 Kontroly skupin transakcí	75
4.5 Dodatečná oprava chyb	76
4.6 Chyby opravované specializovaným operátorem	77
4.7 Chyby opravované pomocí nepřímé zpětné vazby	77
4.8 Kontrolní skupina pro vstup/výstup	78
5. Možné způsoby zabezpečení přenosu proti chybám	81
5.1 Detekce chyb	82
5.2 Reakce systému na zjištěnou chybu	83
5.3 Korekce chyb	85
5.4 Zabezpečení s informační zpětnou vazbou	86
5.5 Způsoby opakování chybných dat	86
5.6 Množství opakovaných dat při zjištění chyby	87
5.7 Řídící znaky pro zabezpečení přenosu	91
5.8 Opatření proti ztrátě záznamu	92
5.9 Minimalizace počtu bitů nutných pro zjišťování chyb	93
5.10 Kritéria pro volbu kódu	93
5.11 Korekční kódy	95
5.12 Paritní zabezpečení	96
5.13 Některá doporučení týkající se sedmiprvkových kódů	98
5.14 Kódy MzN	99
5.15 Polynomické kódy	101
5.16 Pravděpodobnost detekce chyb	104
5.17 Výsledky dosahované v praxi	109
5.18 Enkodéry a dekodéry	109
5.19 Polynomické zabezpečení zpráv s proměnnou délkou	110
5.20 Dosažení mimořádně vysokého stupně zabezpečení	112
5.21 Přehled vlastností různých způsobů zabezpečení proti chybám přenosu	113

6. Opatření realizovaná v systémech při vzniku chyb	115
6.1 Náhradní opatření	116
6.2 Potvrzení zpráv	117
6.3 Doplnování sériových čísel operátorem	118
6.4 Doplnování sériových čísel počítačem	119
6.5 Kontrola práce operátorů	121
6.6 Automatická evidence a restart systému	122
6.7 Přerušování terminálového dialogu	125
7. Programovatelné zámky, identifikace uživatelů a zajištění oprávněnosti přístupu k datům podle jejich obsahu	127
7.1 Programovatelné zámky	127
7.2 Identifikace uživatelů terminálu	130
7.3 Autorizační schémata	134
7.4 Ochrana závislá na obsahu zabezpečované informace	143
8. Poplachové procedury, dohlížecí procedury a bezpečnost systémových programů	
8.1 Poplachové a dohlížecí procedury	147
8.2 Bezpečnost systémových programů	153
9. Vedení záznamů o aktivitách systému	159
9.1 Dva druhy zaznamenávaných údajů	160
9.2 Prohledávání souborů	162
9.3 Postup při nesouhlasu bilančních kontrol	165
9.4 Systémy s rozsáhlými soubory	166
10. Kryptologie	168
10.1 Základní kryptografické principy	168
10.2 Kódovací postupy	170
10.3 Programy pro šifrování dat	176
10.4 Steganografie	183
10.5 Rozdělení systému distribuovaného zpracování dat na chráněné a nechráněné části	186
11. Obnovovací techniky	187
11.1 Možné příčiny poškození souborů	188
11.2 Pásková záznamová média první, druhé a třetí generace	190
11.3 Individuální opravy	190
11.4 Kontrolní body	192
11.5 Přímá aktualizace souborů	192
11.6 Zpracování ve spráženém režimu (In-Line Processing)	193
11.7 Výpisy souborů	193
11.8 RT-systémy	195
11.9 Kopie souborů	195
11.10 Velké databáze	197
11.11 Poškození jednotlivých záznamů	198
11.12 Obnova záznamů v RT systémech	199
11.13 Dohled na procedury opravy souboru	201
12. Ochrana systémů před sabotáží a monitorováním dat	202
12.1 Metody ochrany před sabotáží	203
12.2 Odposlech datových spojů	204
12.3 Další metody nežádoucího získávání informací	206
13. Elektrické jištění zařízení a systémů	209
13.1 Požadavky požární ochrany na řešení stavebních objektů	209
13.2 Elektrická požární signalizace	214
13.3 Zajišťování požární prevence	222
13.4 Volba vhodných hasebních prostředků	223
13.5 Ochrana před vloupáním a sabotáží	226
13.6 Dodržování bezpečnostních opatření	229
14. Odpovědnost za zabezpečení	231
14.1 Odpovědnost za návrh systému zabezpečení	231
14.2 Ochrana systému	233
14.3 Odpovědnost za zabezpečení zpracování	234

15. Správa dat	236
15.1 Klasifikace dat	236
15.2 Pokyny pro práci s dokumenty různých kategorií	237
16. Klíčové informace a obnova chodu systému	239
16.1 Cíle	239
16.2 Posouzení klíčové důležitosti	240
16.3 Třídy záznamů dle důležitosti	240
16.4 Programy	242
16.5 Způsoby ochrany záznamů	243
16.6 Správa archivovaných záznamů	243
16.7 Testování	244
17. Ohrožení systému zevnitř	245
17.1 Potenciální narušitelé	245
17.2 Využívání složitosti k ochraně systému	247
18. Ochrana systému proti programátorům	249
18.1 Testování programů	251
18.2 Rezidence programů	252
18.3 <i>Souhrn vhodných opatření</i>	254
19. <i>Psychologická ochrana zpracování</i>	256
20. Metodika revize způsobů administrativní ochrany	259
20.1 Způsoby kontroly	259
20.2 Kontrola při přípravě systému	260
20.3 Kontrola před přechodem na nový systém	261
20.4 Kontrola systému po jeho zavedení	261
20.5 Vnitřní kontrolní činnost	262
20.6 Technika vlastní kontrolní činnosti	262
Přílohy	266
A. Chybovost datových přenosů a její statistiky	267
A.1 Chyby a chybové posloupnosti	267
A.2 Metodika měření a zaznamenávání výsledků měření chybovosti	270
A.3 Statistika chyb	273
A.4 Chybovost některých typických telekomunikačních spojů používaných pro přenos dat	283
A.5 Využití statistiky chyb	285
A.6 Teoretické modely chyb	287
B. Využití lineárních sekvenčních automatů k transformacím číslicových posloupností v systémech ochrany dat	289
B.1 Představa lineárního sekvenčního automatu	289
B.2 Inertní lineární automaty	292
B.3 Inertní lineární automaty a racionální přenosové funkce	300
B.4 Obecný model	307
B.5 Redukce lineárních automatů	312
B.6 Identifikace lineárních automatů	323
B.7 Využití lineárních automatů k opravě chyb	331
Literatura	334
Literatura k příloze A	341