

Obsah

Podíl na zpracování publikace	5
Předmluva.....	6
1. Bezpečnost, základní pojmy	7
1.1 Bezpečnost	7
1.2 Nežádoucí jevy a situace	8
1.3 Hrozba	8
1.4 Ztráta	10
1.5 Riziko	10
1.6 Prevence	12
1.7 Dílčí závěr	15
Literatura	16
2. Vybrané nástroje a metody zjišťování, třídění a hodnocení informací	17
2.1 Základní hlediska pro posuzování informace a její hodnoty	18
2.2 Informace z hlediska uživatelského	19
2.3 Třídění informací podle informačního zdroje	20
2.3.1 Informace z hlediska času a cíle, kterého má být dosaženo	21
2.3.2 Obsah informace, vzájemná vazba mezi informacemi a kompletnost informací	23
2.3.3 Kritéria k zajištění a hodnocení informací pro řízení	25
2.4 Stanovení hodnoty informace	27
2.5 Hodnota informace při aplikaci teorie užitku	28
2.6 Dílčí závěr	29
Literatura	30
3. Systém managementu bezpečnosti informací	32
3.1 Řízení informační bezpečnosti	33
3.2 Standardy	37
3.3 Soudobé informační prostředí	38
3.4 Informační zdroje	40
3.5 Stavový prostor množiny informačních zdrojů	40
3.6 Komunikace mezi subjekty	41
3.6.1 Zašifrování zprávy	41
3.6.2 Elektronický podpis	42
3.6.3 Bezpečnost elektronického podpisu a šifrovaných zpráv	43
3.6.4 Certifikát	44
3.6.5 Certifikační autority	44
3.6.6 CRL (Certificate Revocation List)	44

3.6.7 Použití certifikátu.....	45
3.6.8 Další využití elektronického podpisu.....	46
3.7 Dílčí závěr.....	46
Literatura.....	46
4. Zvýšení bezpečnosti informačních systémů zajištěním vhodné autentizace.....	49
4.1 Problematika autentizace.....	49
4.2 Znalostní autentizace prostřednictvím hesel.....	50
4.3 Bezpečnost znalostní autentizace prostřednictvím hesel.....	51
4.4 Navržená dvoufaktorová autentizace.....	53
4.5 Biometrický prvek navržené dvoufaktorové autentizace.....	54
4.6 Dílčí závěr.....	56
Literatura.....	57
5. Transparentnost informací.....	59
5.1 Transparentnost.....	59
5.2 Transparentnost a její míra.....	60
5.3 Rozhodování a transparentnost.....	62
5.4 Dílčí závěr.....	64
Literatura.....	64
Publikovaná literatura.....	65