
Obsah

Použité zkratky v textu	vi
1. Úvod do problematiky	1
2. Informace obchodní společnosti a bezpečnost	4
2.1. Pojem zabezpečení informací	5
2.2. Informační systém	6
3. Systémové řešení bezpečnosti obchodní společnosti	9
4. Postup realizace zabezpečení elektronických informací	13
5. Analýza rizik IS	17
5.1. Stanovení hranice analýzy rizik IS	19
5.2. Identifikace aktiv	19

5.3. Ohodnocení aktiv	20
5.4. Seskupování aktiv	26
5.5. Identifikace hrozeb	26
5.6. Analýza hrozeb a zranitelností, stanovení míry rizik	27
5.7. Metody analýzy rizik	28
5.8. Závěrečná zpráva o provedení analýzy rizik	30
5.9. Metodika FRAP	31
6. Bezpečnostní politika IS	36
7. Organizace bezpečnosti IS	39
7.1. Bezpečnostní funkce a orgány	39
7.2. Procesní řízení bezpečnosti IS	44
7.3. Outsourcing	46
7.4. Nejčastější nedostatky v organizaci a řízení bezpečnosti	48
8. Klasifikace informací a vlastníci informací	50
8.1. Zavedení modelu klasifikace informací	51
8.2. Identifikace informací	56
8.3. Vlastníci informací	56
8.4. Význam zavedení klasifikace informací	58
8.5. Příklad stanovení pravidel užití informací	59
9. Bezpečnostní opatření	60
9.1. Řízení a zabezpečení provozu IS	62
9.2. Řízení přístupu k informacím	64
9.3. Vývoj částí IS	65
9.4. Fyzická bezpečnost	66
9.5. Personální bezpečnost	66
9.6. Kontinuita podnikání	69
9.7. Soulad s právem a legislativou	71
9.8. Monitorování a audit IS	71
9.9. Penetrační testy	74

OBSAH

10. Kryptografické nástroje	75
10.1. Z historie kryptografie	77
10.2. Současné užívané kryptografické nástroje	80
10.3. Digitální podpis	94
10.4. Správa veřejných klíčů asymetrických šifer	96
11. Bezpečností předpisy IS	105
11.1. Obsah a struktura bezpečnostní politiky IS	107
11.2. Příklady systémových bezpečnostních politik	111
12. Elektronické obchodování	115
12.1. Obchod na internetu	116
13. Zabezpečení elektronických informací a legislativa	123
13.1. Obchodní zákoník	124
13.2. Zákon o ochraně osobních údajů	124
13.3. Zákon o elektronickém podpisu	126
13.4. Zákon o ochraně utajovaných skutečností	129
13.5. Doporučení Evropské unie	130
14. Závěr	131
Příloha 1 Přehled nejrozšířenějších norem pro řízení bezpečnosti elektronických informací	134
Příloha 2 Slovníček odborných termínů z oblasti zabezpečení elektronických informací	137
Literatura	153