Obsah

Recenzoval: Prof. Ing. Jiří Dvořák, DrSc. 3
ISBN 978 - 80 - 7454 - 312 - 8 3
Úvod 9
1. Pojem „Bezpečnost“ 10
1.1. Informační bezpečnost 11
1.2. Základní pojmy a názvosloví informační bezpečnosti 13
2. Kryptografie v informačních systémech 20
2.1. Využití šifrování 20
2.2. Možnosti nasazení šifrování a jeho omezení 21
2.3. Nejčastější pojmy v kryptologii 24
2.4. Symetrické šifry a šifrování 26
2.5. Nejznámější symetrické šifry 27
2.6. Asymetrické šifry a šifrování 29
2.7. Eliptické kryptosystémy (ECC) 30
2.8. Hash algoritmy 30
2.9. Typy šifrování 32
2.10. Certifikační autorita 34
2.10.1. Třídy certifikátů 35
2.10.2. Postup získání certifikátu 38
***2.10.3.* Tvorba certifikátu** 39
2.11. Možnosti zabezpečení osobních dat a komunikace 40
3. Závislost prosperity firmy na bezpečnosti informací 43
3.1. Analýza bezpečnosti informačního systému 43
3.1.1. Efekty bezpečnostní analýzy 44
3.1.2. Okolnosti, za kterých je vhodné provádět bezpečnostní analýzu IS 45
3.2. Proces řešení informační bezpečnosti 46
3.2.1. Doporučené schéma řešení bezpečnosti dle ISO 13335 47
3.2.2. Cíle a strategie řešení bezpečnosti informačního systému 48
3.2.3. Analýza rizik IS 50
3.2.4. Bezpečnostní politika IS 50
3.2.5. Bezpečnostní standardy IS 51
3.2.6. Implementace bezpečnosti IS 51
3.2.7. Příklady bezpečnostních projektů 51
3.2.8. Základní přístup 55
3.2.9. Neformální přístup 56

3.2.10. Podrobná analýza rizik ... 56
3.2.11. Kombinovaný přístup ... 57
3.2.12. Problémy a chyby vyskytující se při analýze rizik ... 57
3.2.13. Nástroje pro provádění analýzy rizik ... 58
3.2.14. Bezpečnostní politika informačních systémů ... 59
3.2.15. Problémy a chyby při tvorbě politiky ... 61
3.2.16. Vybraná pravidla a normy z oblasti bezpečnosti IT ... 62
3.2.17. ISO 17799 – komplexní chápání bezpečnosti informací ... 63
3.2.18. Bezpečnostní model ... 66
3.3. Bezpečnost IS a legislativa ... 75
4. Moderní algoritmická ochrana dat ... 78
5. Matematický základ kryptografických metod ... 79
5.1. Teorie čísel ... 79
5.2. Modulární aritmetika ... 80
5.3. Bitové operace ... 84
6. Symetrické šifrování ... 87
6.1. Proudové šifry ... 88
6.1.1. XOR ... 89
6.1.2. Vernamova šifra ... 90
6.2. Blokové šifry ... 91
6.2.1. DES ... 92
6.2.2. TripleDES ... 95
6.2.3. Blowfish ... 95
6.2.4. IDEA ... 100
6.2.5. AES ... 103
7. Asymetrické šifrování ... 104
7.1. RSA ... 105
7.1.1. Postup šifrování ... 105
7.1.2. Demonstrační příklad ... 106
7.1.3. Implementace RSA ... 107
7.1.4. Generování prvočísel ... 108
7.1.5. Bezpečnost RSA ... 108
7.2. Eliptické křivky ... 109
7.2.1. Teorie eliptických křivek ... 109
7.2.2. Příklad výpočtu bodů elipsy nad tělesem ... 111
7.2.3. Digitální podpis podle schématu ECDSA ... 112

7.2.4. Bezpečnost eliptických křivek 113
8. Analýza symetrických a asymetrických šifer 114
8.1. Komunikace mezi více účastníky 114
8.2. Bezpečnost 114
8.3. Rychlost 114
8.4. Použití 115
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK 120
SEZNAM PŘÍLOH 121