

Obsah

Obsah	5
Slovo autora.....	7
Úvod	9
1. Informační bezpečnost	10
1.1 Co znamená pojem informační bezpečnost.....	10
1.2 Co ohrožuje informační systémy	15
1.3 Požadavky na důvěryhodné informační systémy	23
1.4 Základní způsoby ochrany IS.....	30
1.5 Správa informační bezpečnosti.....	47
2. Bezpečnostní politika	52
2.1 Dělení bezpečnostní politiky	53
2.2 Obsah bezpečnostní politiky	54
2.3 Bezpečnostní politika v životním cyklu informačního systému.....	58
2.4 Bezpečnostní analýza	65
3. Bezpečnostní dekompozice informačního systému.....	78
3.1 Bezpečnostní hlediska	78
3.2 Fyzická bezpečnost.....	82
3.3 Personální bezpečnost.....	97
3.4 Režimová bezpečnost.....	102
3.5 Technická bezpečnost	103
3.6 Programová bezpečnost	116
3.7 Datová bezpečnost	127
3.8 Komunikační bezpečnost.....	133
4. Legislativa a kritéria hodnocení bezpečnosti.....	156
4.1 Bezpečnostní zákonodárství v USA.....	156
4.2 Evropská legislativa	157
4.3 Právní ochrana informací v České republice	158
4.4 Kritéria hodnocení bezpečnosti informačních systémů	162
5. Kryptografie v informačních systémech.....	195
5.1 Základní pojmy	195
5.2 Historie kryptografie	197
5.3 Komerční šifry	199
5.4 Základní šifrovací systémy.....	203
5.5 Symetrický šifrovací systém.....	207
5.6 Asymetrický šifrovací systém	212

5.7 Distribuce klíčů	222
5.8 Kryptografické prostředky	224
5.9 Základní typy kryptografických útoků	225
5.10 Hodnocení bezpečnosti šifer	225
6. Bezpečnost a Internet	228
6.1 Co je to Internet ?	229
6.2 Co Internet nabízí ?	230
6.3 Internet očima právníka	231
6.4 Vývoj Internetu	233
6.5 Komunikační protokoly Internetu	235
6.6 Nové hrozby přicházející z Internetu	247
6.7 Základní způsoby zabezpečení	252
7. Bankovníctví a elektronický obchod	273
7.1 Elektronická banka	273
7.2 Elektronický obchod a Internet	276
Závěr	281
Rejstřík	282