ÚVOD ..... 6

1 POJEM „BEZPEČNOST“ ..... 7

1.1 INFORMAČNÍ BEZPEČNOST ..... 9

1.2 ZÁKLADNÍ POJMY A NÁZVOSLOVÍ INFORMAČNÍ BEZPEČNOSTI ..... 11

2 KRYPTOGRAFIE V INFORMAČNÍCH SYSTÉMECH ..... 20

2.1 VÝZNAM POJMŮ SE KTERÝMI SE SETKÁVÁME V KRYPTOLOGII ..... 24

*2.1.1 Symetrické šifry a šifrování ..... 25*

*2.1.2 Asymetrické šifry a šifrování ..... 27*

*2.1.3 Eliptické kryptosystémy (ECC) ..... 29*

*2.1.4 Hash algoritmy ..... 29*

*2.1.5 Typy šifrování ..... 31*

2.2 CERTIFIKAČNÍ AUTORITA ..... 32

*2.2.1 Třídy certifikátů ..... 33*

*2.2.2 Postup získání certifikátu ..... 36*

*2.2.3 Tvorba certifikátu ..... 37*

2.3 MOŽNOSTI ZABEZPEČENÍ OSOBNÍCH DAT A KOMUNIKACE ..... 38

3 ZÁVISLOST PROSPERITY FIRMY NA BEZPEČNOSTI INFORMACÍ ..... 42

3.1 ANALÝZA BEZPEČNOSTI INFORMAČNÍHO SYSTÉMU ..... 42

*3.1.1 Efekty bezpečnostní analýzy ..... 43*

*3.1.2 Okolnosti za kterých je vhodné provádět bezpečnostní analýzu IS ..... 45*

3.2 PROCES ŘEŠENÍ INFORMAČNÍ BEZPEČNOSTI ..... 45

*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 ..... 52*

*3.2.8 Základní přístup ..... 56*

*3.2.9 Neformální přístup ..... 57*

*3.2.10 Podrobná analýza rizik ..... 57*

*3.2.11 Kombinovaný přístup ..... 58*

*3.2.12 Problémy a chyby vyskytující se při analýze rizik ..... 59*

*3.2.13 Nástroje pro provádění analýzy rizik ..... 60*

*3.2.14 Bezpečnostní politika informačních systémů ..... 61*

*3.2.15 Problémy a chyby při tvorbě politiky ..... 63*

*3.2.16 Vybraná pravidla a normy z oblasti bezpečnosti IT* ..... *64*
*3.2.17 ISO 17799 – komplexní chápání bezpečnosti informací* ..... *66*
*3.2.18 Bezpečnostní model* ..... *69*
3.3 BEZPEČNOST IS A LEGISLATIVA ..... 81

**4 MODERNÍ ALGORITMICKÁ OCHRANA DAT ..... 85**

**5 MATEMATICKÝ ZÁKLAD KRYPTOGRAFICKÝCH METOD ..... 86**

5.1 TEORIE ČÍSEL ..... 86
5.2 MODULÁRNÍ ARITMETIKA ..... 88
5.3 BITOVÉ OPERACE ..... 91

**6 SYMETRICKÉ ŠIFROVÁNÍ ..... 93**

6.1 PROUDOVÉ ŠIFRY ..... 94
*6.1.1 XOR* ..... *95*
*6.1.2 Vermanova šifra* ..... *96*
6.2 BLOKOVÉ ŠIFRY ..... 98
*6.2.1 DES* ..... *99*
*6.2.2 Blowfish* ..... *101*
*6.2.3 IDEA* ..... *105*
*6.2.4 AES* ..... *109*

**7 ASYMETRICKÉ ŠIFROVÁNÍ ..... 110**

7.1 RSA ..... 111
*7.1.1 Postup šifrování* ..... *111*
*7.1.2 Demonstrační příklad* ..... *112*
*7.1.3 Implementace RSA* ..... *114*
*7.1.4 Generování prvočísel* ..... *114*
*7.1.5 Bezpečnost RSA* ..... *115*
7.2 ELIPTICKÉ KŘIVKY ..... 116
*7.2.1 Teorie eliptických křivek* ..... *116*
*7.2.2 Příklad výpočtu bodů elipsy nad tělesem* ..... *118*
*7.2.3 Digitální podpis podle schématu ECDSA* ..... *119*
*7.2.4 Bezpečnost eliptických křivek* ..... *121*

**8 ANALÝZA SYMETRICKÝCH A ASYMETRICKÝCH ŠIFER ..... 122**

8.1 KOMUNIKACE MEZI VÍCE ÚČASTNÍKY ..... 122
8.2 BEZPEČNOST ..... 122
8.3 RYCHLOST ..... 123
8.4 POUŽITÍ ..... 123

**SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK** ..... **128**

**SEZNAM PŘÍLOH** ..... **129**