

ÚVOD .....	6
<b>1 POJEM „BEZPEČNOST“ .....</b>	<b>7</b>
1.1 INFORMAČNÍ BEZPEČNOST .....	9
1.2 ZÁKLADNÍ POJMY A NÁZVOSLOVÍ INFORMAČNÍ BEZPEČNOSTI.....	11
<b>2 KRYPTOGRAFIE V INFORMAČNÍCH SYSTÉMECH.....</b>	<b>20</b>
2.1 VÝZNAM POJMŮ SE KTERÝMI SE SETKÁVÁME V KRYPTOLOGII.....	24
2.1.1 <i>Symetrické šifry a šifrování</i> .....	25
2.1.2 <i>Asymetrické šifry a šifrování</i> .....	27
2.1.3 <i>Eliptické kryptosystémy (ECC)</i> .....	29
2.1.4 <i>Hash algoritmy</i> .....	29
2.1.5 <i>Typy šifrování</i> .....	31
2.2 CERTIFIKAČNÍ AUTORITA .....	32
2.2.1 <i>Třídy certifikátů</i> .....	33
2.2.2 <i>Postup získání certifikátu</i> .....	36
2.2.3 <i>Tvorba certifikátu</i> .....	37
2.3 MOŽNOSTI ZABEZPEČENÍ OSOBNÍCH DAT A KOMUNIKACE.....	38
<b>3 ZÁVISLOST PROSPERITY FIRMY NA BEZPEČNOSTI INFORMACÍ.....</b>	<b>42</b>
3.1 ANALÝZA BEZPEČNOSTI INFORMAČNÍHO SYSTÉMU.....	42
3.1.1 <i>Efekty bezpečnostní analýzy</i> .....	43
3.1.2 <i>Okolnosti za kterých je vhodné provádět bezpečnostní analýzu IS</i> .....	45
3.2 PROCES ŘEŠENÍ INFORMAČNÍ BEZPEČNOSTI .....	45
3.2.1 <i>Doporučené schéma řešení bezpečnosti dle ISO 13335</i> .....	47
3.2.2 <i>Cíle a strategie řešení bezpečnosti informačního systému</i> .....	48
3.2.3 <i>Analýza rizik IS</i> .....	50
3.2.4 <i>Bezpečnostní politika IS</i> .....	50
3.2.5 <i>Bezpečnostní standardy IS</i> .....	51
3.2.6 <i>Implementace bezpečnosti IS</i> .....	51
3.2.7 <i>Příklady bezpečnostních projektů</i> .....	52
3.2.8 <i>Základní přístup</i> .....	56
3.2.9 <i>Neformální přístup</i> .....	57
3.2.10 <i>Podrobná analýza rizik</i> .....	57
3.2.11 <i>Kombinovaný přístup</i> .....	58
3.2.12 <i>Problémy a chyby vyskytující se při analýze rizik</i> .....	59
3.2.13 <i>Nástroje pro provádění analýzy rizik</i> .....	60
3.2.14 <i>Bezpečnostní politika informačních systémů</i> .....	61
3.2.15 <i>Problémy a chyby při tvorbě politiky</i> .....	63

3.2.16	<i>Vybraná pravidla a normy z oblasti bezpečnosti IT</i> .....	64
3.2.17	<i>ISO 17799 – komplexní chápání bezpečnosti informací</i> .....	66
3.2.18	<i>Bezpečnostní model</i> .....	69
3.3	BEZPEČNOST IS A LEGISLATIVA.....	81
<b>4</b>	<b>MODERNÍ ALGORITMICKÁ OCHRANA DAT</b> .....	<b>85</b>
<b>5</b>	<b>MATEMATICKÝ ZÁKLAD KRYPTOGRAFICKÝCH METOD</b> .....	<b>86</b>
5.1	TEORIE ČÍSEL.....	86
5.2	MODULÁRNÍ ARITMETIKA.....	88
5.3	BITOVÉ OPERACE.....	91
<b>6</b>	<b>SYMETRICKÉ ŠIFROVÁNÍ</b> .....	<b>93</b>
6.1	PROUDOVÉ ŠIFRY.....	94
6.1.1	<i>XOR</i> .....	95
6.1.2	<i>Vernanova šifra</i> .....	96
6.2	BLOKOVÉ ŠIFRY.....	98
6.2.1	<i>DES</i> .....	99
6.2.2	<i>Blowfish</i> .....	101
6.2.3	<i>IDEA</i> .....	105
6.2.4	<i>AES</i> .....	109
<b>7</b>	<b>ASYMETRICKÉ ŠIFROVÁNÍ</b> .....	<b>110</b>
7.1	RSA.....	111
7.1.1	<i>Postup šifrování</i> .....	111
7.1.2	<i>Demonstrační příklad</i> .....	112
7.1.3	<i>Implementace RSA</i> .....	114
7.1.4	<i>Generování prvočísel</i> .....	114
7.1.5	<i>Bezpečnost RSA</i> .....	115
7.2	ELIPTICKÉ KŘIVKY.....	116
7.2.1	<i>Teorie eliptických křivek</i> .....	116
7.2.2	<i>Příklad výpočtu bodů elipsy nad tělesem</i> .....	118
7.2.3	<i>Digitální podpis podle schématu ECDSA</i> .....	119
7.2.4	<i>Bezpečnost eliptických křivek</i> .....	121
<b>8</b>	<b>ANALÝZA SYMETRICKÝCH A ASYMETRICKÝCH ŠIFER</b> .....	<b>122</b>
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
--------------------	-----

Průběh vývoje informačního managementu a ekonomiky ..... 130	
Pod pojmem informační management ..... 131	
„Informační management“ ..... 132	
„Informační management“ ..... 133	
„Informační management“ ..... 134	
„Informační management“ ..... 135	
„Informační management“ ..... 136	
„Informační management“ ..... 137	
„Informační management“ ..... 138	
„Informační management“ ..... 139	
„Informační management“ ..... 140	
„Informační management“ ..... 141	
„Informační management“ ..... 142	
„Informační management“ ..... 143	
„Informační management“ ..... 144	
„Informační management“ ..... 145	
„Informační management“ ..... 146	
„Informační management“ ..... 147	
„Informační management“ ..... 148	
„Informační management“ ..... 149	
„Informační management“ ..... 150	
„Informační management“ ..... 151	
„Informační management“ ..... 152	
„Informační management“ ..... 153	
„Informační management“ ..... 154	
„Informační management“ ..... 155	
„Informační management“ ..... 156	
„Informační management“ ..... 157	
„Informační management“ ..... 158	
„Informační management“ ..... 159	
„Informační management“ ..... 160	
„Informační management“ ..... 161	
„Informační management“ ..... 162	
„Informační management“ ..... 163	
„Informační management“ ..... 164	
„Informační management“ ..... 165	
„Informační management“ ..... 166	
„Informační management“ ..... 167	
„Informační management“ ..... 168	
„Informační management“ ..... 169	
„Informační management“ ..... 170	
„Informační management“ ..... 171	
„Informační management“ ..... 172	
„Informační management“ ..... 173	
„Informační management“ ..... 174	
„Informační management“ ..... 175	
„Informační management“ ..... 176	
„Informační management“ ..... 177	
„Informační management“ ..... 178	
„Informační management“ ..... 179	
„Informační management“ ..... 180	
„Informační management“ ..... 181	
„Informační management“ ..... 182	
„Informační management“ ..... 183	
„Informační management“ ..... 184	
„Informační management“ ..... 185	
„Informační management“ ..... 186	
„Informační management“ ..... 187	
„Informační management“ ..... 188	
„Informační management“ ..... 189	
„Informační management“ ..... 190	
„Informační management“ ..... 191	
„Informační management“ ..... 192	
„Informační management“ ..... 193	
„Informační management“ ..... 194	
„Informační management“ ..... 195	
„Informační management“ ..... 196	
„Informační management“ ..... 197	
„Informační management“ ..... 198	
„Informační management“ ..... 199	
„Informační management“ ..... 200	
„Informační management“ ..... 201	
„Informační management“ ..... 202	
„Informační management“ ..... 203	
„Informační management“ ..... 204	
„Informační management“ ..... 205	
„Informační management“ ..... 206	
„Informační management“ ..... 207	
„Informační management“ ..... 208	
„Informační management“ ..... 209	
„Informační management“ ..... 210	
„Informační management“ ..... 211	
„Informační management“ ..... 212	
„Informační management“ ..... 213	
„Informační management“ ..... 214	
„Informační management“ ..... 215	
„Informační management“ ..... 216	
„Informační management“ ..... 217	
„Informační management“ ..... 218	
„Informační management“ ..... 219	
„Informační management“ ..... 220	
„Informační management“ ..... 221	
„Informační management“ ..... 222	
„Informační management“ ..... 223	
„Informační management“ ..... 224	
„Informační management“ ..... 225	
„Informační management“ ..... 226	
„Informační management“ ..... 227	
„Informační management“ ..... 228	
„Informační management“ ..... 229	
„Informační management“ ..... 230	
„Informační management“ ..... 231	
„Informační management“ ..... 232	
„Informační management“ ..... 233	
„Informační management“ ..... 234	
„Informační management“ ..... 235	
„Informační management“ ..... 236	
„Informační management“ ..... 237	
„Informační management“ ..... 238	
„Informační management“ ..... 239	
„Informační management“ ..... 240	
„Informační management“ ..... 241	
„Informační management“ ..... 242	
„Informační management“ ..... 243	
„Informační management“ ..... 244	
„Informační management“ ..... 245	
„Informační management“ ..... 246	
„Informační management“ ..... 247	
„Informační management“ ..... 248	
„Informační management“ ..... 249	
„Informační management“ ..... 250	
„Informační management“ ..... 251	
„Informační management“ ..... 252	
„Informační management“ ..... 253	
„Informační management“ ..... 254	
„Informační management“ ..... 255	
„Informační management“ ..... 256	
„Informační management“ ..... 257	
„Informační management“ ..... 258	
„Informační management“ ..... 259	
„Informační management“ ..... 260	
„Informační management“ ..... 261	
„Informační management“ ..... 262	
„Informační management“ ..... 263	
„Informační management“ ..... 264	
„Informační management“ ..... 265	
„Informační management“ ..... 266	
„Informační management“ ..... 267	
„Informační management“ ..... 268	
„Informační management“ ..... 269	
„Informační management“ ..... 270	
„Informační management“ ..... 271	
„Informační management“ ..... 272	
„Informační management“ ..... 273	
„Informační management“ ..... 274	
„Informační management“ ..... 275	
„Informační management“ ..... 276	
„Informační management“ ..... 277	
„Informační management“ ..... 278	
„Informační management“ ..... 279	
„Informační management“ ..... 280	
„Informační management“ ..... 281	
„Informační management“ ..... 282	
„Informační management“ ..... 283	
„Informační management“ ..... 284	
„Informační management“ ..... 285	
„Informační management“ ..... 286	
„Informační management“ ..... 287	
„Informační management“ ..... 288	
„Informační management“ ..... 289	
„Informační management“ ..... 290	
„Informační management“ ..... 291	
„Informační management“ ..... 292	
„Informační management“ ..... 293	
„Informační management“ ..... 294	
„Informační management“ ..... 295	
„Informační management“ ..... 296	
„Informační management“ ..... 297	
„Informační management“ ..... 298	
„Informační management“ ..... 299	
„Informační management“ ..... 300	

V řadě případů tyto skupiny také sdílejí informace (např. poradenství, bezpečnostní informace a její zvládnutí může vést ke ztrátě na majetku ...) a často se i prolínají, zejména v případě ochrany nehmotných statků a informací a znalostí na informacích založených.

Zvláštní skupinou jsou poznatky a znalosti získané na základě informací. Jde o takové znalosti a informace, které nejsou běžně dostupné, nebo jejichž zpracování je náročné a méně dostupné většině okolních subjektů. Nejedná se tedy o všechny informace, ale jen takové, které mají určitou (často velmi významnou) hodnotu pro jejich nositele a pro určitý okruh subjektů v případě, že by tato informace (znalost) získaly. Současné jde o informace s omezenou dostupností. Jsou to tedy informace a znalosti, které jejich nositeli umožňují získat určitou výhodu vůči ostatním subjektům a jejichž ztráta (prozrazení atp.) by mu mohla způsobit újmu. Tato výhoda nemusí být pouze výhoda v konkurenčním hospodářském prostředí, ale může být výhodou také například v oblasti politiky jakékoliv úrovně a jakékoliv duha.