

1. Co jsou informační systémy.....	8
1.1 Co jsou to informace a data .....	8
1.1.1 Pojem informace.....	8
1.1.2 Informace a data .....	8
1.1.3 Měření množství informace.....	9
1.1.4 Měření objemu dat.....	11
1.1.5 Ekonomická hodnota informace.....	12
1.2 Co je to informační systém .....	14
1.2.1 Informační systém .....	14
1.2.2 Informační systémy a informační technologie .....	16
1.3 Jakou architekturu má IS/IT.....	18
1.3.1 Klasifikace systémů.....	18
1.3.2 Schéma architektury IS/IT.....	20
1.4 Role uživatele v IS/IT .....	21
1.4.1 Přístup uživatelů k IS/IT.....	21
1.4.2 Typy uživatelů IS/IT.....	22
1.4.3 Požadavky na uživatele IS/IT .....	23
2. Informační systémy ve veřejné správě.....	24
2.1 Základní organizace veřejné správy.....	26
2.1.1 Klasifikace obcí .....	28
2.1.2 Územní klasifikace .....	29
2.2 Model metasystému veřejné správy.....	33
2.3 Poslání a pojetí informačních (sub)systémů ve veřejné správě? .....	36
2.4 Registr informačních subsystémů veřejné správy.....	39
2.5 Novodobý informační (sub)systém veřejné správy .....	40
2.5.1 Jednotně věrohodný a kompetentní úřední výkon.....	40
2.5.2 Příklad informačních (sub)systémů VS .....	41
2.5.3 Principiální model občanské obsluhy ve VPI - základ zvyšování efektivity....	41
2.5.4 Důsledky principiálního modelu.....	44
2.6 Vymezení pojmu Státní informační systém .....	46
2.7 Co je obsahem pojmu Regionální informační systém?.....	49
2.8 Co se rozumí pod pojmem městské řízení .....	53

3.	Specializovaný software počítačově orientovaných IS VS a jeho architektura.....	67
3.1	Princip integrace počítačově orientovaných IS ve VS.....	67
3.2	Obvyklá globální architektura VIS VPI.....	69
3.3	Obvyklá globální architektura FIS VPI .....	72
3.4	Obvyklá technologicko-logická integrace GIS a VIS VPI .....	74
3.5	Obvyklá komerční integrace architektur GIS a VIS na produktech Microsoft.....	77
3.6	Detailní architektura produktu Urban (GIS) .....	78
3.6.1	Shrnutí .....	79
4.	Trendy v oblasti informačních systémů VS PRO příští tisíciletí.....	80
4.1	Princip modernizace administrativy VPI/VS.....	84
4.2	Modernizace výkonu VS.....	85
4.3	Princip přívětivé veřejné správy v informační společnosti.....	87
4.4	Místní infokiosky - základ otevřeného městského řízení.....	90
4.4.1	Shrnutí .....	93
5.	Úvod do základů bezpečnostní politiky ISVS .....	95
5.1	Legislativní základ bezpečnostní politiky ISVS .....	95
5.1.1	Bezpečnost ISVS a kompetence ÚVIS.....	96
5.1.2	Vzájemný vztah bezpečnosti soustavy ISVS.....	97
5.2	Standardy ISVS.....	97
5.3	Předpoklady pro řešení informační bezpečnosti ISVS .....	99
6.	Systém řízení bezpečnostní politiky ISVS, atestace a audit bezpečnosti .....	101
6.1	Pravomoci a odpovědnosti v organizaci .....	101
6.1.1	Vedení organizace .....	101
6.1.2	Útvary působící ve funkci správců a provozovatelů IS .....	103
6.1.3	Útvary působící ve funkci poskytovatelů služeb v oblasti IS.....	103
6.1.4	Povinnosti a odpovědnosti útvaru bezpečnosti IS .....	103
6.1.5	Vztah k externím subjektům.....	103
6.1.6	Povinnosti a odpovědnosti zaměstnanců a dalších subjektů .....	104
6.1.7	Zásady bezpečnosti .....	104
6.2	Organizace a řízení bezpečnosti v organizaci .....	106
6.2.1	Základní požadavky.....	106
6.2.2	Předpisy a normy bezpečnostního systému organizace.....	107
6.2.3	Role v rámci řízení bezpečnosti ISVS .....	108
6.2.4	Organizace a řízení bezpečnosti v oblasti ISVS.....	110

6.3	Rozvoj a změny bezpečnostního systému.....	112
6.3.1	Změny bezpečnostního systému.....	112
6.3.2	Schvalovací proces pro zařízení zpracovávající informace.....	112
6.3.3	Nezávislá revize bezpečnosti informací.....	113
7.	Systémová bezpečnostní politika ISVS.....	114
7.1	Fyzická bezpečnost a bezpečnost prostředí (technická a objektová bezpečnost)....	114
7.1.1	Fyzický bezpečnostní perimetr.....	114
7.1.2	Koncepce ochrany objektů, využívání prvků ochrany.....	115
7.1.3	Systémy pro detekci a poplchy.....	116
7.1.4	Provádění ostrahy.....	117
7.2	Administrativní bezpečnost a organizační opatření.....	118
7.2.1	Kontroly vstupu osob.....	118
7.2.2	Zabezpečení kanceláří, místností a zařízení.....	120
7.2.3	Práce v bezpečných zónách.....	122
7.2.4	Samostatné prostory pro dodávku a nakládání.....	122
7.3	Bezpečnost zařízení.....	123
7.3.1	Umístění zařízení IT a jeho ochrana.....	123
7.3.2	Dodávky energie.....	124
7.3.3	Bezpečnost kabeláže.....	125
7.3.4	Údržba zařízení.....	125
7.3.5	Bezpečnost zařízení mimo objekt.....	126
7.3.6	Bezpečná likvidace nebo opakované použití zařízení.....	127
7.3.7	Zásady informační bezpečnosti.....	127
7.3.8	Základní pravidla pro fyzickou a organizační bezpečnost ISVS.....	128
7.4	Personální bezpečnostní politika.....	129
7.4.1	Personální politika a bezpečnostní kultura.....	129
7.4.2	Bezpečnost v popisu práce a při zajišťování lidských zdrojů.....	130
7.4.3	Zahrnutí bezpečnosti do pracovních povinností.....	130
7.4.4	Taktika prověřování uchazečů.....	130
7.4.5	Smlouva o zachování důvěrnosti.....	131
7.4.6	Podmínky výkonu pracovní činnosti.....	131
7.4.7	Školení uživatelů.....	132
7.4.8	Reakce na bezpečnostní incidenty a chyby.....	132
7.4.9	Personální bezpečnostní opatření.....	134

7.4.10	Pravidla pro provádění personální politiky.....	136
7.5	Bezpečnost komunikací a provozu .....	137
7.5.1	Zvláštní aspekty informační bezpečnosti ISVS.....	137
7.5.2	Provozní postupy a odpovědnosti.....	140
7.5.3	Plánování a akceptace systému.....	144
7.5.4	Ochrana proti škodlivým programům (antivirová ochrana) .....	146
7.5.5	Správa systému .....	147
7.5.6	Správa sítě.....	149
7.5.7	Bezpečnost při zacházení s médii .....	149
7.5.8	Výměna informací a programů.....	152
7.6	Řízení přístupu k informačním systémům .....	156
7.6.1	Požadavky na řízení přístupu.....	157
7.6.2	Řízení přístupu uživatelů .....	158
7.6.3	Odpovědnosti uživatele .....	160
7.6.4	Řízení přístupu k síti.....	162
7.6.5	Řízení přístupu k operačnímu systému.....	167
7.6.6	Řízení přístupu k aplikacím .....	171
7.6.7	Monitorování přístupu k systému a jeho použití .....	172
7.6.8	Mobilní výpočetní prostředky a práce na dálku .....	175
7.7	Sdílení dat prostřednictvím referenčního, sdíleného a bezpečného rozhraní.....	177
7.7.1	Vzájemná komunikace mezi ISVS prostřednictvím referenčního, sdíleného a bezpečného rozhraní s využitím systémů dálkového přístupu.....	178
7.7.2	Bezpečnost přístupu třetích stran.....	180
7.7.3	Outsourcing.....	183
7.8	Způsob vytváření ISVS a zavádění nových softwarových produktů.....	188
7.8.1	Bezpečnostní požadavky systémů .....	188
7.8.2	Bezpečnost v aplikačních systémech.....	189
7.8.3	Začlenění šifrové ochrany.....	191
7.8.4	Bezpečnost systémových souborů .....	196
7.8.5	Bezpečnost procesů vývoje a podpory .....	198
7.8.6	Posouzení bezpečnostní politiky a technické shody .....	201
7.8.7	Audit systému .....	202
7.9	Postupy při řešení výjimečných situací při provozu ISVS .....	203
7.9.1	Cíle řízení kontinuity činností .....	203

7.9.2	Proces řízení kontinuity činností .....	203
7.9.3	Analýza dopadů .....	204
7.9.4	Vytváření a implementace plánů kontinuity činností .....	204
7.9.5	System plánování kontinuity činností.....	205
7.9.6	Testování plánů kontinuity činností.....	206
7.9.7	Údržba a přehodnocování plánů kontinuity.....	206
7.9.8	Zásady plánování kontinuity (rizikového plánování) ISVS .....	207
7.9.9	Model krizového plánování .....	208
8.	Přílohy .....	209
8.1	Seznam důležitých zkratk a pojmů.....	209
8.2	Vybrané WWW stránky státní správy a samosprávy.....	212
9.	Použitá a doporučená literatura k dalšímu studiu .....	215