

OBSAH

PŘEDMLUVA	9
1. ÚVOD	11
1.1 ZÁKLADNÍ NÁZVOSLOVÍ	12
1.2 ZÁKLADNÍ POJMY	12
1.3 DEFINICE ISMS	14
1.4 ZÁKLADNÍ POJMY A NÁZVOSLOVÍ INFORMAČNÍ BEZPEČNOSTI	15
1.4.1 Pojmy	15
1.4.2 Ustavení ISMS	16
1.4.3 Zavádění a provoz ISMS	16
1.4.4 Monitorování a přezkoumání ISMS	16
1.4.5 Údržba a zlepšování ISMS	16
2. HISTORIE	19
3. DEMINGŮV MODEL	23
3.1 PDCA	24
4. DEFINICE POJMŮ	27
4.1 ITIL	28
4.2 COBIT	30
4.3 CRAMM	33
4.4 CC	33
4.5 PŘIMĚŘENÁ BEZPEČNOST	36
5. NORMALIZAČNÍ INSTITUCE	39
5.1 POJMY	40
5.2 NADNÁRODNÍ, CELOSVĚTOVÉ	41
5.3 EVROPSKÉ	42
5.4 NÁRODNÍ	43
5.5 DALŠÍ	44
5.5.1 Další evropské normalizační organizace zabývající se bezpečností IT	44
5.5.2 Americké normalizační organizace zabývající se bezpečností IT	45
6. NORMY	47
6.1 ZÁKLADNÍ NORMY ŘADY 27 K	48
6.2 CHYSTANÉ NORMY ŘADY 27 K	53

6.3	TELEKOMUNIKAČNÍ PROSTŘEDÍ	56
6.4	ZDRAVOTNICKÉ PROSTŘEDÍ	56
6.5	SÍŤOVÁ BEZPEČNOST	57
6.6	SOUVISEJÍCÍ NORMY K 27 K	57
7.	ZAVÁDĚNÍ ISMS	65
7.1	OBSAH ISMS	66
7.2	ETAPY ZAVÁDĚNÍ ISMS	66
7.3	POVINNÁ DOKUMENTACE	67
7.4	ŠKOLENÍ	70
7.5	MĚŘENÍ ÚČINNOSTI	71
7.6	MONITOROVÁNÍ A AUDITY	73
8.	PROJEKTOVÁNÍ ISMS	75
8.1	BEZPEČNOSTNÍ PROJEKT	76
9.	AKTIVA	81
9.1	DEFINICE A KLASIFIKACE AKTIV	82
9.2	HODNOCENÍ AKTIV	82
9.3	VÝPOČET HODNOTY AKTIVA	83
10.	BEZPEČNOSTNÍ HROZBY	85
11.	ANALÝZA RIZIK	89
11.1	METODIKY	91
11.2	ŘÍZENÍ RIZIK	95
12.	OPATŘENÍ	99
12.1	DEFINICE	100
12.2	VÝBĚR OPATŘENÍ	101
A.5	Bezpečnostní politika	105
A.6	Organizace bezpečnosti informací	107
A.7	Řízení aktiv	108
A.8	Bezpečnost lidských zdrojů	109
A.9	Fyzická bezpečnost a bezpečnost prostředí	110
A.10	Řízení komunikací a řízení provozu	111
A.11	Řízení přístupu	116
A.12	Akvizice, vývoj a údržba IS	122
A.13	Zvládání bezpečnostních incidentů	124
A.14	Řízení kontinuity činnosti organizace	125
A.15	Soulad s požadavky	128
13.	AUDIT A CERTIFIKACE	129
13.1	ZÁKLADNÍ POJMY	130

13.2	PRŮBĚHY PROCESŮ	130
14.	ZABEZPEČENÍ A OCHRANA DAT	133
14.1	KRITICKÁ INFRASTRUKTURA	134
14.2	KRYPTOLOGIE	135
14.3	VIRY A ŠKODLIVÉ KÓDY	137
14.4	PENETRAČNÍ TESTY	138
14.5	DLP SYSTÉMY	142
14.6	KYBERTERORISMUS	144
15.	ITSM	151
15.1	POJEM ITSM	152
15.2	NORMA ISO/IEC 20000	153
15.3	NORMA ISO/IEC 27013	160
16.	SÍŤOVÁ BEZPEČNOST	161
16.1	DEFINICE A POJMY	162
16.2	NORMY	163
16.3	VRSTVY ISO/OSI MODELU (L1, L2, L3)	166
16.4	MANAGEMENT BEZPEČNOSTI PASIVNÍ VRSTVY	167
16.5	BUDOVÁNÍ BEZPEČNÉ SÍŤOVÉ INFRASTRUKTURY	170
17.	APLIKAČNÍ BEZPEČNOST	171
17.1	DEFINICE A POJMY	172
17.2	NORMY	173
17.3	BEZPEČNOST APLIKAČNÍ VRSTVY	173
17.4	BEZPEČNOST WEBOVÝCH APLIKACÍ	175
18.	PRŮMYSLOVÁ BEZPEČNOST	179
18.1	VYMEZENÍ POJMŮ	180
18.2	INDUSTRIAL ETHERNET (IE)	182
18.3	PARAMETRY PRŮMYSLOVÉ SÍŤOVÉ INFRASTRUKTURY	184
18.4	TOPOLOGIE	185
18.5	REDUNDANCE	189
18.6	SCADA	194
18.7	SYNCHRONIZACE V DISTRIBUOVANÝCH ŘÍDICÍCH SYSTÉMECH	197
19.	OBOROVÉ ISMS	199
19.1	ISMS VE STÁTNÍ SPRÁVĚ	200
19.1.1	Pojmy a definice	200
19.1.2	Právní prostředí	202
19.1.3	Normy a směrnice	203
19.1.4	Kritická opatření	206
19.2	ISMS VE ZDRAVOTNICTVÍ	207

19.2.1	Definice	207
19.2.2	Provozní a právní prostředí	208
19.2.3	Normy	209
19.3	ISMS A POSKYTOVATELÉ ICT SLUŽEB	215
19.3.1	Pojmy	215
19.3.2	Bezpečnostní stavební bloky ITU-T	217
19.3.3	Normy	218
19.3.4	Konvergence k NGN	220
19.4	AKADEMICKÉ A ŠKOLSKÉ PROSTŘEDÍ	224
20.	SPECIFICKÉ ŘEŠENÍ ISMS	229
20.1	NAC (BYOD)	230
20.1.1	Definice a pojmy	230
20.2	VIRTUALIZACE	238
20.2.1	Definice	238
20.2.2	Problémy virtualizace	240
20.2.3	Doporučení	241
20.3	CLOUD COMPUTING	242
20.3.1	Bezpečnostní hrozby v cloudu	244
20.3.2	Vývoj v oblasti regulace cloudu	247
20.3.3	Odpovědnost za ztrátu dat v cloudu	248
20.4	MCN	252
20.4.1	Výpočet dostupnosti	254
20.4.2	Model hrozeb	256
21.	LEGISLATIVA A PRÁVNÍ PROSTŘEDÍ	263
22.	PŘÍPADOVÉ STUDIE	265
22.1	METODIKA PRAKTICKÉHO ZAVEDENÍ ISMS	266
22.2	ANALÝZA RIZIK	267
22.2.1	Identifikace a hodnocení aktiv	267
22.2.2	Identifikace hrozeb a zranitelností	267
22.2.3	Maticová metoda analýzy rizik	268
22.2.4	Analýza rizik pomocí pravděpodobnosti incidentu a jeho dopadu	270
22.2.5	Srovnávací (GAP) analýza rizik	271
22.3	VÝBĚR OPATŘENÍ A JEJICH MĚŘENÍ	272
22.4	UŽIVATEL JAKO ZDROJ RIZIK	276
22.5	METODIKA A NÁVRH BEZPEČNÉ INFRASTRUKTURY IT	279
22.6	SÍŤOVÁ BEZPEČNOST DLE ISO/IEC 27033	281
22.7	ZABEZPEČENÍ SÍŤOVÉ INFRASTRUKTURY	288
22.7.1	Metodika zabezpečení síťové infrastruktury	288
22.7.2	Aplikace síťových opatření	292
22.8	UTM – KOMPLEXNÍ OCHRANA	296
22.9	KLASIFIKACE FIREWALLŮ	297

22.10 FUNKČNÍ MODEL NAC	303
22.11 TOPOLOGICKÁ STUDIE SÍTĚ V PRŮMYSLOVÉM PROSTŘEDÍ	315
22.11.1 Popis	315
22.11.2 Topologie hvězda	315
22.11.3 Topologie kruh	317
22.11.4 Vyhodnocení	318
22.12 BEZPEČNOST BEZDRÁTOVÉHO ŘEŠENÍ	319
22.12.1 Historie bezpečnosti WiFi	319
22.12.2 Kategorie útoků na bezdrátové sítě a možnosti obrany	319
22.12.3 Autentizační metody ve WiFi sítích	321
22.13 METODIKA ZÁLOHOVÁNÍ DAT	325
22.13.1 Statistické údaje	326
22.13.2 Záloha a archiv	327
22.13.3 Privátní zálohování třetí stranou	334
22.14 BEZPEČNOSTNÍ SMĚRNICE PRO UŽIVATELE LAN A IS	335
22.14.1 Forma dokumentu „Minimální bezpečnostní pravidla pro uživatele“	337
22.14.2 Příklad provozního řádu počítačové sítě (školy)	340
22.14.3 Bezpečnostní školení	343
 23. REJSTŘÍK OBECNĚ POUŽÍVANÝCH POJMŮ	 345
24. PŘEHLED BEZPEČNOSTNÍCH NOREM	355
25. SEZNAM ZKRATEK	361
26. SEZNAM OBRÁZKŮ	367
27. SEZNAM TABULEK	371
28. POUŽITÁ LITERATURA	373