

Obsah

I. ČÁST - Modelování a prognostika v oblasti bezpečnosti a fyzické ostrahy	17
1 Základy bezpečnostní futurologie	20
1.1 Úvod.....	20
1.1.1 Terminologie v oblasti bezpečnostní futurologie.....	20
1.2 Futurologie.....	23
1.2.1 Význam futurologie.....	25
1.2.2 Historie futurologie.....	26
1.3 Bezpečnostní futurologie	28
1.3.1 Oblasti zájmu bezpečnostní futurologie	29
1.4 Shrnutí	32
2 Prognostická metodologie.....	34
2.1 Úvod.....	34
2.2 Prognostika.....	35
2.3 Prognózy – funkce a klasifikace	37
2.3.1 Funkce prognóz	37
2.3.2 Klasifikace prognóz	39
2.4 Principy a metodologie tvorby prognóz.....	41
2.5 Prognostické metody	43
2.5.1 Subjektivní a objektivní metody	44
2.5.2 Univerzální, strukturální a procesuální metody	45
2.6 Shrnutí	49
3 Modelování v oblasti krizového řízení	51
3.1 Úvod.....	51
3.2 Vybrané nástroje pro modelování v rámci krizového řízení.....	52
3.2.1 RISKAN.....	52
3.2.2 TEREX.....	54
3.2.3 EMERGENCY OFFICE	55
3.2.4 POSIM	57
3.2.5 PRACTIS.....	58
3.2.6 SITUNET	58
3.2.7 OBNOVA.....	59
3.2.8 ANALYZÁTOR.....	61
3.3 Závěr.....	63
4 Efektivnost' systémů ochrany objektů	64
4.1 Požadavky na ochranu objektů	64
4.2 Stanovení úrovně ochrany objektu – případová štúdia Bankový subjekt	68
4.2.1 Úroveň ochrany aktivních prvků systému ochrany	70
4.2.2 Úroveň ochrany pasivních prvků systému ochrany	72
4.2.3 Dislokace aktivních a pasivních prvků ochrany.....	73
4.3 Softvérové nástroje na podporu projektování systémů ochrany objektů.....	73
4.3.1 Program AutoCAD.....	74
4.3.2 Program SketchUP.....	75
4.3.3 Program VideoCAD a IP Video Design Tool.....	76
4.4 Zhrnutí.....	78

5	Simulační technologie v průmyslu komerční bezpečnosti	80
5.1	Úvod.....	80
5.2	Vymezení výukové simulace	80
5.2.1	Kategorie simulací	80
5.2.2	Typy výukových simulátorů	81
5.3	Teorie procesu simulace.....	83
5.3.1	Přípravná fáze	83
5.3.2	Fáze vlastní simulace.....	86
5.3.3	Závěrečná fáze.....	87
5.4	Využití simulačních technologií v průmyslu komerční bezpečnosti.....	88
5.4.1	Vhodnost simulačních technologií pro činnosti PKB	88
5.4.2	Využití simulačních technologií na UTB a proces implementace	89
5.5	Shrnutí	90
II.	ČÁST - Informační bezpečnost	93
1	Dopad bezpečnosti informací na prosperitu firmy	95
1.1	Úvod.....	95
1.2	Analýza bezpečnosti informačního systému	95
1.2.1	Efekty bezpečnostní analýzy	96
1.2.2	Situace vhodné pro provádění bezpečnostní analýzy IS	96
1.3	Proces řešení informační bezpečnosti	97
1.3.1	Doporučené schéma dle ISO 13335.....	97
1.3.2	Strategie řešení bezpečnosti informačního systému	98
1.3.3	Analýza rizik IS	99
1.3.4	Bezpečnostní politika IS.....	100
1.3.5	Bezpečnostní standardy IS.....	100
1.3.6	Implementace bezpečnosti IS	100
1.3.7	Příklady bezpečnostních projektů	100
1.3.8	Základní přístup	104
1.3.9	Neformální přístup.....	104
1.3.10	Podrobná analýza rizik.....	105
1.3.11	Kombinovaný přístup.....	105
1.3.12	Problémy a chyby vyskytující se při analýze rizik	105
1.3.13	Bezpečnostní politika informačních systémů.....	106
1.3.14	Problémy a chyby při tvorbě politiky	108
2	Úvod do penetračních testů a bezpečnostních auditů.....	110
2.1	Úvod.....	110
2.2	Penetrační testy	110
2.2.1	Cíle penetračních testů	110
2.2.2	Základní typy penetračních testů	111
2.2.3	Fáze penetračního testu	112
2.2.4	Metody používané v penetračních testech.....	114
2.2.5	Normy pro penetrační testování.....	116
2.3	Bezpečnostní audit	117
2.3.1	Audit bezpečnosti v organizaci.....	117
2.3.2	Audit bezpečnosti informačních systémů	117
2.3.3	Rámcový audit informační bezpečnosti se zaměřuje na oblasti:	117
2.3.4	Audit probíhá v prostorech organizace v následujících krocích:	117
2.3.5	Přínosy auditu bezpečnosti organizace a informační bezpečnosti:	118

3	Kryptografie v informačních systémech.....	119
3.1	Úvod.....	119
3.2	Využití šifrování.....	119
3.3	Nasazení šifer.....	120
3.4	Pojmy kryptografie.....	122
3.5	Symetrické šifry.....	123
3.5.1	DES (Data Encryption Standard).....	123
3.5.2	3DES (Triple – DES).....	123
3.5.3	IDEA.....	124
3.5.4	BlowFish.....	125
3.5.5	CAST.....	125
3.6	Asymetrické šifry.....	125
3.6.1	RSA.....	126
3.7	Eliptické kryptosystémy (ECC).....	126
3.8	HASH algoritmy.....	126
3.9	Typy šifrování.....	128
4	Bezpečnost symetrických a asymetrických šifer.....	130
4.1	Úvod.....	130
4.2	Symetrické šifrování.....	130
4.2.1	Proudové šifry.....	131
4.2.2	Blokové šifry.....	134
4.3	Asymetrické šifrování.....	144
4.3.1	RSA.....	145
4.3.2	Eliptické křivky.....	148
4.3.3	Digitální podpis podle schématu ECDSA.....	151
5	Digitální forenzní technologie.....	153
5.1	Úvod.....	153
5.2	Digitální stopa.....	153
5.2.1	Autentizace digitální stopy.....	154
5.2.2	Právní aspekty zajištění digitálních stop.....	154
5.2.3	Lokalizace digitální stopy.....	154
5.2.4	Práce s digitální stopou.....	154
5.3	Bitová kopie.....	155
5.3.1	Vytvoření bitové kopie.....	155
5.4	Analýza digitálních dat.....	156
5.4.1	Příprava před forenzní analýzou.....	157
5.4.2	Obnovení dat z bitové kopie.....	157
5.4.3	Obnovení smazaných dat.....	157
5.4.4	Extrakce a třídění dat.....	158
5.4.5	Vyhledání řetězců.....	158
5.4.6	Typy prováděných analýz.....	158
III.	ČÁST - Fyzická ostraha.....	163
1	Fyzická ostraha.....	166
1.1	Úvod.....	166
1.2	Právní rámec fyzické ostrahy.....	166
1.2.1	Trestní zákoník.....	166
1.2.2	Trestní řád.....	167
1.2.3	Občanský zákoník.....	168
1.3	Dělení fyzické ostrahy.....	169

1.4	Metody fyzické ostrahy	173
1.5	Požadavky na fyzickou ostrahu	174
1.6	Výzbroj a výstroj	175
1.7	Využití pracovního psa	177
1.7.1	Strážní psi	178
1.7.2	Hlídací psi	178
1.8	Shrnutí	179
2	Fyzická ostraha v praxi	180
2.1	Úvod	180
2.2	Malá versus velká firma	180
2.3	Kvalita versus cena služeb bezpečnostních agentur	182
2.4	Konkurenceschopnost a boj o zákazníka v tržním prostředí bezpečnostních agentur	183
2.5	Nejčastěji poskytované služby realizovány bezpečnostními službami v rámci České republiky	184
2.6	Právní předpisy a interní nařízení	185
2.7	Pozice pracovníků PKB	186
2.8	Pohled do běžného dne pracovníka ostrahy	187
2.9	Shrnutí	190
3	Výcvik profesní obrany a obranná střelba	192
3.1	Úvod	192
3.2	Výcvik profesní obrany v průmyslu komerční bezpečnosti	193
3.2.1	Prostředí komerční bezpečnosti a profesní obrana	193
3.2.2	Problematika výcviku profesní obrany se zbraněmi	196
3.3	Problematika obranné střelby	197
3.3.1	Obecná pravidla obranné střelby	198
3.3.2	Základní vybavení pro obrannou střelbu, rozsah znalostí a dovednosti	199
3.3.3	Výcvik v obranné střelbě	200
3.4	Shrnutí	201
4	Odhalení potenciálně rizikových jedinců a skupin pomocí techniky profilování	204
4.1	Úvod	204
4.2	Aplikace metody profilování	204
4.2.1	Príklady negatívnych indikácií	205
4.3	Prípady z minulosti s efektívnou možnosťou využitia profilovania na základe negatívnych indikácií jedincov	207
4.3.1	Osamelí vlci	207
4.3.2	Útok na izraelských turistov v Burgase	207
4.3.3	Richard Reid – terorista s bombou v topánkach a Umar Farouk Abdulmutallab – terorista s bombou na tele	208
4.3.4	Pohroma letu Germanwings	209
4.4	Ilustratívne príklady využitia profilovania v rôznych oblastiach	210
4.4.1	Príklad – hotel	210
4.4.2	Príklad – firma	210
4.4.3	Príklad – Cestovné prostriedky (Cestujúci pod falošnou identitou)	211
4.5	Metodológia správnej profilácie	211
4.6	Zhrnutie	212
5	Činnost zásahových jednotek v rámci dohledových a popl. přijímacích center	213
5.1	Úvod	213

5.2 Terminologie.....	213
5.3 Zásahová jednotka	214
5.4 Předpoklady pro výkon činnosti ZJ	215
5.5 Minimální požadavky na pracovníky ZJ.....	215
5.6 Příklady působení ZJ	216
5.6.1 Působení ZJ ve spolupráci s Poplachovým přijímacím centrem (PPC)	217
5.6.2 Působení ZJ ve spolupráci s Dohledovým centrem (DC)	218
5.6.3 Lokální působení ZJ na objektu	219
5.7 Vybavení ZJ	220
5.8 Shrnutí.....	221
IV. ČÁST - Poplachové zabezpečovací a tísňové systémy	223
1 Zřizování poplachových zabezpečovacích a tísňových systémů	228
1.1 Úvod.....	228
1.1.1 Terminologie	228
1.2 Postup zřizování PZTS.....	229
1.3 Návrh systému.....	231
1.3.1 Bezpečnostní posouzení.....	232
1.3.2 Návrh skladby systému	234
1.4 Příprava realizace	239
1.4.1 Technické posouzení	240
1.4.2 Projektová dokumentace	241
1.5 Montáž PZTS.....	243
1.6 Trvalý provoz.....	246
1.7 Shrnutí.....	248
2 Elektrické zabezpečovací a tísňové poplachové systémy	250
2.1 Úvod.....	250
2.2 Komponenty EZS/TPS	251
2.3 Prístupové úrovne.....	253
2.4 Ústredne EZS.....	253
2.5 Vstupná funkcia EZS.....	255
2.6 Výstupná funkcia EZS	255
2.7 Systémové a technické požiadavky na EZS/TPS a ich komponenty.....	256
2.8 Rozdelenie ústrední EZS/TPS.....	257
2.9 Zhrnutie.....	259
3 Integrace poplachových systémů	261
3.1 Integrované poplachové systémy	261
3.1.1 Požadavky na integraci PZTS	262
3.2 Technické způsoby integrace PZTS.....	263
3.2.1 Integrace IN/OUT.....	264
3.2.2 Poplachový zabezpečovací a tísňový systém jako integrační prvek.....	267
3.2.3 Automatizační systém jako integrační prvek.....	271
3.2.4 Integrace s využitím prvků poplachových aplikací	274
V. ČÁST - Trendy fyzické bezpečnosti a krizového řízení	279
1 Bezpečnostní management v organizaci, teorie a praxe	281
1.1 Úvod.....	281
1.2 Bezpečnost, cíl a předmět	281
1.3 Bezpečnostní incident	283

1.4	Teorie bezpečnosti a její vliv na bezpečnostní management.....	284
1.5	Vymezení managementu a jeho diskuse	285
1.6	Funkce managementu	287
1.6.1	Plánování.....	287
1.6.2	Organizování.....	288
1.6.3	Personalistika.....	288
1.6.4	Vedení lidí	289
1.6.5	Kontrola.....	290
1.7	Manažer jako nositel funkcí managementu	291
1.8	Bezpečnostní management v organizaci	292
1.9	Bezpečnostní metody.....	294
1.10	Bezpečnostní politika a bezpečnostní strategie organizace	295
1.11	Shrnutí	297
2	Současný stav a vývojové trendy v oboru dekontaminace.....	298
2.1	Úvod.....	298
2.2	Dekontaminační procesy a technologie.....	298
2.2.1	Rozdělení a hlavní zásady dekontaminace	298
2.2.2	Požadavky na realizaci dekontaminace	299
2.3	Dekontaminační látky, směsi a roztoky	304
2.3.1	Dekontaminační látky, směsi a roztoky používané v AČR	304
2.3.2	Dekontaminační látky, směsi a roztoky používané u HZS ČR.....	306
2.4	Technické prostředky dekontaminace.....	307
2.4.1	Technické prostředky pro dekontaminaci používané v AČR.....	308
2.4.2	Tech. prostředky pro dekontaminaci mob. techniky používané u HZS ČR ..	308
2.5	Trendy rozvoje oboru dekontaminace.....	311
2.6	Shrnutí	311
3	Systémy pro správu informací fyzického zabezpečení	313
3.1	Úvod.....	313
3.2	Vývoj bezpečnostních nadstavbových systémů (BNS)	313
3.3	Vlastnosti a struktura systémů PSIM.....	314
3.3.1	Základní vlastnosti systémů PSIM.....	314
3.3.2	Architektura systémů PSIM	315
3.3.3	Klíčové přínosy nadstavbových systémů.....	316
3.4	Možnosti využití systémů PSIM	318
3.5	Příklady typického nasazení systémů PSIM.....	319
3.5.1	Příklady nasazení PSIM v dopravě	319
3.5.2	Příklady nasazení PSIM v energetice.....	319
3.5.3	Příklady nasazení PSIM pro realizaci projektů „chytrých“ měst.....	320
3.6	Shrnutí	320
4	Roboty jako technické prostředky bezpečnostních systémů	322
4.1	Úvod.....	322
4.1.1	Účel a motivace	322
4.1.2	Definice robotického systému.....	322
4.2	Historie robotických systémů.....	323
4.3	Rozdělení robotických systémů.....	325
4.3.1	Systémové uspořádání obecného robotického systému	325
4.3.2	Průmyslové roboty	327
4.3.3	Servisní roboty	328
4.4	Struktura kinematického řetězce robotického systému.....	329

4.4.1	Rameno, kloub, kinematická dvojice, stupeň volnosti.....	329
4.4.2	Interakce mezi jednotlivými rameny	331
4.4.3	Interakce mezi robotem a okolím – mobilní podsystém	331
4.5	Rozdělení robotů podle typu mobilního systému	331
4.5.1	Rozdělení robotů podle vzoru.....	332
4.5.2	Rozdělení robotů podle pracovního prostředí	332
4.6	Kolové mobilní systémy.....	332
4.6.1	Kolo s přenosem síly a ideálně se odvalující kolo	332
4.6.2	Rozdělení kolových robotů podle počtu kol.....	334
4.6.3	Všesměrová kola	334
4.7	Kráčející roboty	335
4.7.1	Dvounohé kráčející roboty	336
4.7.2	Čtyřnohé kráčející roboty	336
4.8	Mobilní roboty na pásovém podvozku.....	337
4.9	Létající a plavající robotické systémy.....	337
4.10	Použití rob. systémů jako tech. prostředků bezpečnostních systémů.....	339
4.10.1	Použití robotických systémů jako inteligentních zbraňových systémů	339
4.10.2	Monitorovací a pozorovací systémy.....	341
4.10.3	Pomocné systémy (manipulační, zásobovací...)	341
4.11	Závěr.....	341
5	Integrované systémy řízení v budovách	343
5.1	Integrované systémy v budovách – „inteligentní“ budovy	343
5.2	Uživatelské požadavky na integrované systémy v budovách	344
5.3	Technické požadavky na inteligentní budovy.....	345
5.3.1	Společná správa zařízení na jednom operačním pracovišti.....	345
5.3.2	Využívání dat získaných v jednom ze systémů pro činnost ost. systémů	346
5.3.3	Nezávislost na konkrétním dodavateli	346
5.3.4	Energetický management budovy.....	346
5.3.5	Využití informační sítě pro správu budovy	347
5.4	Řídicí systémy v budovách	348
5.4.1	Systémy s řídicí centrálou.....	348
5.4.2	Decentralizované systémy.....	349
5.4.3	Požadavky na otevřené systémy.....	349
5.4.4	Principy komunikace.....	350
5.5	Základní sběrníkové systémy vhodné pro integrované systémy v budovách	352
5.5.1	Sběrníkový systém KNX.....	353
5.5.2	Sběrníkový systém LonWorks.....	353
5.5.3	Protokol BACnet.....	354
5.5.4	Sběrnice Digital Addressable Lighting Interface	355
5.6	Postup při stanovení požadavků a priorit jednotlivých monitorovaných a řízených prvků systémů	356
5.7	Shrnutí	356
	Resumé – summary	359
	Představení autorů kapitol	361