

# **BEZPEČNOSTNÍ TECHNOLOGIE, SYSTÉMY A MANAGEMENT II.**

**Kamerové systémy**

**Řízení rizik v bezpečnostním inženýrství**

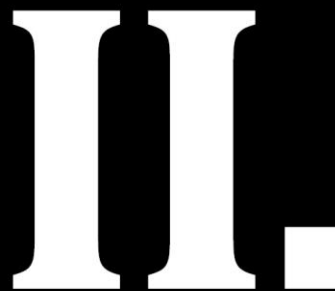
**Technologie profesní obrany**

**Informační podpora**

**Bezpečnostní politika a bezpečnostní systém státu**



**Bezpečnostní  
technologie,  
systémy  
a management**



Luděk Lukáš a kolektiv

Radim Bačuvčík – VeRBuM

Zlín 2012

## **KATALOGIZACE V KNIZE – NÁRODNÍ KNIHOVNA ČR**

Lukáš, Luděk

Bezpečnostní technologie, systémy a management II. / Luděk Lukáš a kolektiv. – 1. vyd.  
– Zlín : VeRBuM, 2012. – 387 s.

ISBN 978-80-87500-19-4

351.759.5 \* 351.78:614.8 \* 62-027.45 \* 614.8 \* 005.934

- ochrana majetku
- osobní bezpečnost
- zabezpečovací technika
- bezpečnostní inženýrství
- bezpečnostní management
- kolektivní monografie

005 - Management. Řízení [4]

### **Recenzovali:**

**prof. Ing. Josef Reitšpís, PhD.**

**doc. Ing. Vladimír Vráb, CSc.**

**Tato kniha vznikla za podpory projektu Evropského Fondu pro  
Regionální Rozvoj CEBIA-Tech č. CZ.1.05/2.1.00/ 03.0089.**

**This book was supported by European Regional Development Fund  
under the project CEBIA-Tech No. CZ.1.05/2.1.00/ 03.0089.**

**Tato monografie byla doporučena k publikaci vědeckou redakcí  
nakladatelství VeRBuM**

**© doc. Ing. Luděk Lukáš, CSc., autoři kapitol, 2012**

**© Radim Bačuvčík - VeRBuM, 2012**

**ISBN 978-80-87500-19-4**

# Obsah

I. ČÁST - Kamerové systémy .....	15
1. Kamerové systémy ako súčasť komplexného bezpečnostného systému .....	17
1.1 Úvod.....	17
1.2 Technické normy kamerových systémov .....	20
1.2.1 Medzinárodné normalizačné orgány.....	21
1.2.2 Regionálne normalizačné orgány .....	22
1.2.3 Národné normalizačné orgány .....	25
1.2.4 Štandardizačné konzorciá spoločností .....	26
1.3 Zhrnutie.....	27
2. Teoretické základy snímání a komprese digitálneho videosignálu .....	29
2.1 Úvod.....	29
2.2 Teoretické základy snímání obrazu .....	29
2.2.1 CCD snímače.....	30
2.2.2 CMOS snímače .....	33
2.2.3 DPS snímače.....	33
2.3 Teorie barev a digitalizace obrazu.....	34
2.3.1 Lidský systém vnímání .....	35
2.3.2 Barevné modely.....	36
2.3.3 Digitalizace obrazu .....	38
2.4 Komprese obrazu a videa.....	40
2.4.1 Neztrátové kompresní algoritmy.....	40
2.4.2 Ztrátový kompresní algoritmus JPEG.....	42
2.4.3 Komprese videosignálu .....	43
2.5 Shrnutí .....	45
3. Kamerové systémy .....	46
3.1 Úvod.....	46
3.2 Základní prvky kamery .....	46
3.2.1 Objektiv.....	46
3.2.2 Technologie optických senzorů.....	51
3.3 Technické parametry kamer .....	54
3.3.1 Rozlišovací schopnost.....	54
3.3.2 Poměr stran obrazu .....	54
3.3.3 Citlivost.....	55
3.3.4 Dynamický rozsah .....	56
3.3.5 Napájení kamer.....	56
3.3.6 Řídící vstupy kamer .....	56
4. IP kamery .....	58
4.1 Úvod.....	58
4.2 Princip a konstrukce IP kamer .....	58
4.2.1 Princip činnosti IP kamer .....	58
4.2.2 Konstrukce IP kamer .....	59
4.2.3 Fixní IP kamery .....	60
4.2.4 IP PTZ kamery .....	60
4.2.5 Současné trendy v oblasti funkcí IP kamer .....	61

4.3	Komunikační část IP kamer .....	61
4.3.1	Hardwarové komunikační rozhraní IP kamery .....	62
4.3.2	Přenosové technologie síťového videa.....	63
4.3.3	Komunikace IP kamery v síti.....	64
4.4	Software pro správu IP kamerových systémů .....	66
4.5	Shrnutí .....	68
II.	ČÁST - Řízení rizik v bezpečnostním inženýrství .....	71
1.	Úvod do problematiky řízení rizik .....	74
1.1	Úvod.....	74
1.2	Terminologický rámec řízení rizik .....	74
1.3	Proces řízení rizik.....	81
1.3.1	Komunikace a konzultace .....	82
1.3.2	Vymezení souvislostí .....	82
1.3.3	Posuzování rizik .....	84
1.3.4	Zvládání rizik .....	89
1.3.5	Monitorování a přezkoumání procesu .....	93
1.4	Shrnutí .....	93
2.	Řízení rizik v oblasti fyzické ochrany .....	96
2.1	Úvod.....	96
2.2	Materiály a metody.....	96
2.2.1	Charakteristika vybrané problematiky .....	96
2.3	Výsledky .....	98
2.3.1	Postup analýzy rizik aplikovaný na fyzickou ochranu .....	98
2.3.2	Analýzy definování lidské chyby u fyzické ochrany objektu.....	101
2.3.3	Metody stanovení vah při návrhu na minimalizaci rizika objektu .....	102
2.4	Shrnutí .....	103
3.	Řízení rizik v průmyslové bezpečnosti.....	104
3.1	Úvod do problematiky řízení rizik.....	104
3.2	Strategie řízení rizik v průmyslové bezpečnosti .....	104
3.3	Postup analýzy rizik aplikovaný na průmyslové podniky .....	105
3.3.1	Indexové metody (RR) .....	106
3.3.2	Revize bezpečnosti (SR) .....	107
3.3.3	Kontrolní seznam (CL).....	107
3.3.4	Předběžná analýza ohrožení (PHA).....	107
3.3.5	Analýza What if (WI) .....	108
3.3.6	Analýza What if v kombinaci s Kontrolním seznamem (WI-CL) .....	108
3.3.7	Analýza nebezpečnosti a provozovatelnosti (HAZOP).....	108
3.3.8	Analýza příčin a následků poruch (FMEA) .....	108
3.3.9	Analýza stromem poruch (FTA).....	109
3.3.10	Analýza stromem událostí (ETA).....	109
3.3.11	Analýza příčin a následků (CCA).....	109
3.3.12	Analýza lidského faktoru (HRA) .....	109
3.4	Shrnutí .....	110
4.	Využití řízení rizik v požární ochraně.....	112
4.1	Úvod.....	112
4.2	Strategie požární bezpečnosti .....	112

4.3	Základní analýza průmyslových zón vs. požární jednotky.....	113
4.4	Statistika při návrhu požární bezpečnosti.....	114
4.5	Stanovení účinného zásahu jednotek PO .....	116
4.5.1	Rozdělení doby potřebné pro zásah jednotek PO .....	116
4.5.2	Doba jízdy (teoretický model) .....	118
4.5.3	Četnost zablokování v řízení záchranného systému .....	119
4.5.4	Úspěšnost požárního zásahu jednotek PO .....	120
4.5.5	Analýzy stromů události a poruch.....	121
4.5.6	Shrnutí účinného zásahu jednotek PO .....	121
4.6	Model RHAVE.....	123
4.7	Využití GISu při rozmístování jednotek PO .....	123
4.7.1	Analýza mimořádné události.....	124
4.7.2	Modelování doby jízdy jednotek PO .....	124
4.7.3	Rozmístění požárních stanic.....	124
4.7.4	Shrnutí využití GIS pro rozmístění požárních stanic .....	125
4.8	Shrnutí .....	125
5.	Vybrané techniky posuzování rizik .....	127
5.1	Úvod do problematiky analýzy rizik.....	127
5.2	Vhodnost výběru metody.....	127
5.3	Stručná charakteristika metod.....	129
5.3.1	Analýza stromu poruchových stavů ( <i>FTA – Fault tree analysis</i> ).....	130
5.3.2	Analýza stromu událostí ( <i>ETA – Event tree analysis</i> ) .....	131
5.3.3	Analýza typu motýlek ( <i>Bow tie analysis</i> ) .....	132
5.3.4	Křivky FN ( <i>FN curves</i> ) .....	133
5.3.5	Analýza nákladů a přínosů ( <i>CBA – Cost/benefit analysis</i> ).....	135
5.3.6	Indexy rizika ( <i>Risk indices</i> ).....	136
5.4	Shrnutí .....	137
III.	ČÁST - Technologie profesní obrany.....	139
1.	Rozdělení zbraní a osobních prostředků.....	142
1.1	Úvod.....	142
1.2	Zákonitosti rozdělení zbraní a prostředků.....	142
1.2.1	Důvody rozdělení zbraní a osobních prostředků v průmyslu komerční bezpečnosti.....	143
1.2.2	Pravidla rozdělení zbraní a osobních prostředků v průmyslu komerční bezpečnosti.....	143
1.3	Definice a terminologie .....	144
1.4	Schematická diferenciac zbraní a osobních prostředků .....	145
1.4.1	Diferenciac z hlediska ohrožených zájmů.....	145
1.4.2	Diferenciac z hlediska aspektů řešení situace profesní obrany .....	146
1.5	Shrnutí .....	155
2.	Právní hodnocení zbraní a obranných prostředků.....	156
2.1	Úvod.....	156
2.2	Zbraně a psychika pracovníka PKB .....	156
2.2.1	Extrémní názory .....	156
2.2.2	Použití zbraně.....	157
2.3	Právní hodnocení zbraní .....	157
2.3.1	Zbraně regulované zákonem .....	157

2.3.2	Chladné zbraně – nože .....	160
2.3.3	Ostatní zbraně .....	161
2.4	Právní hodnocení obranných prostředků.....	161
2.4.1	Služební ( <i>pracovní</i> ) pes .....	162
2.4.2	Pouta.....	162
2.5	Právní hodnocení ochranných prostředků.....	163
2.5.1	Balistická ochrana.....	163
2.5.2	Audiovizuální technika .....	163
2.6	Shrnutí .....	164
3.	Zbraně v profesní obraně .....	166
3.1	Úvod do problematiky palných zbraní v profesní obraně.....	166
3.2	Zákonné podmínky pro držení a nošení střelných palných zbraní.....	166
3.2.1	Zákonné a podzákonné normy pro držení střelných palných zbraní.....	166
3.2.2	Okolnosti získání zbrojní licence a zbrojního průkazu .....	167
3.2.3	Nošení střelných palných zbraní.....	169
3.2.4	Použití zbraně kategorie D při výkonu činností PKB.....	170
3.3	Manipulace se zbraněmi a jejich používání.....	171
3.3.1	Mýty a fakta o zbraních.....	171
3.3.2	Bezpečná manipulace se zbraněmi .....	173
3.3.3	Vhodné zbraně pro průmysl komerční bezpečnosti .....	176
3.3.4	Základy výcviku se zbraněmi .....	177
3.4	Shrnutí .....	178
4.	Obranné prostředky v profesní obraně.....	180
4.1	Úvod.....	180
4.2	Úderné zbraně .....	180
4.2.1	Obušek.....	181
4.2.2	Teleskopický obušek .....	181
4.2.3	Tonfa .....	182
4.2.4	Kubotan.....	183
4.2.5	Srovnání úderných obranných prostředků .....	184
4.3	Poutací obranné prostředky .....	184
4.3.1	Kovová pouta .....	184
4.3.2	Jednorázová pouta.....	185
4.3.3	Srovnání poutacích obranných prostředků.....	186
4.4	Chemické obranné prostředky.....	186
4.4.1	Náplně .....	187
4.4.2	Obranný sprej – typ: Mlha .....	187
4.4.3	Obranný sprej – typ: Tekutá střela.....	188
4.4.4	Kombinované obranné spreje.....	188
4.4.5	Pepper gel .....	189
4.4.6	Srovnání obranných sprejů.....	189
4.5	Elektrické obranné prostředky.....	190
4.5.1	Soudobé elektrické paralyzéry – kontaktní.....	190
4.5.2	Soudobé elektrické paralyzéry – distanční.....	191
4.5.3	Kombinované elektrické paralyzéry .....	191
4.5.4	Taser .....	192
4.5.5	Citlivá místa.....	193
4.5.6	Doba výboje.....	194
4.6	Pracovní pes .....	194



4.6.1	Strážní psi .....	195
4.6.2	Hlídací psi.....	196
4.7	Shrnutí .....	196
5.	Ochranné prostředky .....	199
5.1	Úvod.....	199
5.2	Protiúderové ochranné prostředky .....	200
5.2.1	Prostředky na ochranu očí .....	200
5.2.2	Prostředky na ochranu sluchu .....	201
5.2.3	Prostředky na ochranu čichu, dýchání .....	201
5.2.4	Prostředky na ochranu hlavy, krku a ramen .....	202
5.2.5	Prostředky na ochranu rukou, paží, nohou a chodidel.....	203
5.2.6	Prostředky na ochranu vitálních orgánů .....	204
5.3	Balistické ochranné prostředky.....	204
5.3.1	Balistické materiály.....	204
5.3.2	Typy balistické ochrany .....	205
5.3.3	Balistické vesty .....	206
5.3.4	Předpoklad dalšího vývoje balistických ochran.....	207
5.4	Ochranná vozidla, kontejnery a zavazadla .....	208
5.4.1	Ochranná vozidla .....	208
5.4.2	Kontejnery pro přepravu cenin.....	210
5.4.3	Zavazadla pro přepravu cenin .....	210
5.5	Komunikační a záznamové ochranné prostředky .....	211
5.5.1	Emisní bezpečnost.....	212
5.5.2	Detektory odposlechů a skrytých kamer .....	212
5.5.3	Zařízení na ochranu před odposlechem.....	213
5.5.4	Rušičky signálů a mikrofonů .....	214
5.5.5	Zabezpečení počítačů a sítí proti sledování a krádeži dat .....	214
5.5.6	Šifrování.....	215
5.5.7	Shrnutí.....	215
5.6	Spektrální, akustické a jiné ochranné prostředky .....	216
5.6.1	Spektrální ochranné prostředky .....	216
5.6.2	Akustické a kombinované ochranné prostředky.....	217
5.7	Shrnutí .....	217
IV.	ČÁST - Informační podpora .....	221
1.	Informační podpora, pojetí, vymezení a vliv na kvalitu činností .....	224
1.1	Úvod.....	224
1.2	Informatika a bezpečnostní složky .....	225
1.3	Vztah proces – informační potřeby – informace .....	226
1.4	Informace a její vlastnosti .....	229
1.5	Informační podpora řídicích, rozhodovacích a poznávacích procesů .....	231
2.	Informačné systémy v bezpečnostných službách .....	241
2.1	Úvodom .....	241
2.2	Informácie vo firemnom prostredí.....	241
2.3	Architektúra a súčasti informačného systému .....	244
2.4	Hierarchia informačných systémov .....	247
2.5	Špecifiká informačných systémov v bezpečnostných službách .....	251
2.6	Zhrnutie.....	256

3. Informační management.....	258
3.1 Úvod.....	258
3.2 Informační management .....	258
3.3 Obsah informačního managementu.....	259
3.4 Zásady, metody a nástroje informačního managementu.....	260
3.4.1 Zásady informačního managementu.....	260
3.4.2 Metody informačního managementu.....	261
3.4.3 Nástroje informačního managementu.....	261
3.5 Role a povinnosti informačního manažera .....	262
3.6 Základní dokumenty informačního managementu.....	265
3.7 Informační strategie.....	266
3.8 Bezpečnostní a informační politika.....	269
3.9 Monitoring a audit informačního systému.....	270
3.10 Provozní řád informačního systému.....	272
3.11 Systém řízení bezpečnosti informací.....	274
3.12 Shrnutí .....	276
4. Informační zdroje v oblasti průmyslu komerční bezpečnosti.....	279
4.1 Úvod.....	279
4.2 Informační zdroje.....	279
4.3 Primární informační zdroje.....	280
4.3.1 Vědecké, technické a odborné časopisy .....	280
4.3.2 Dokumenty ochrany duševního vlastnictví .....	282
4.3.3 Normy.....	283
4.3.4 Zákony a legislativní dokumenty.....	284
4.3.5 Zprávy a informace z vědeckých a odborných setkání.....	285
4.3.6 Vědecko-kvalifikační práce .....	286
4.3.7 Výzkumné a technické zprávy .....	286
4.3.8 Interní firemní informace .....	287
4.3.9 Tajné informace.....	287
4.4 Sekundární informační zdroje.....	288
4.5 Terciární informační zdroje .....	289
4.6 Strategie vyhledávání informací.....	290
4.7 Závěr.....	291
5. Konkurenční zpravodajství jako specifická forma informační podpory.....	293
5.1 Úvod.....	293
5.2 Vymezení konkurenčního zpravodajství.....	294
5.3 Technologie zpravodajství – zpravodajský cyklus.....	296
5.3.1 Zpravodajský cyklus .....	297
5.3.2 Zpravodajský produkt.....	299
5.3.3 Zpravodajská sociotechnika .....	299
5.3.4 Technologie primárních zdrojů.....	300
5.3.5 Technologie sekundárních zdrojů informací – otevřené zdroje.....	301
5.3.6 Technologie zpravodajské (investigativní) analýzy.....	301
5.4 Roviny zpravodajské činnosti.....	303
5.4.1 Obranné zpravodajství.....	304
5.4.2 Ofenzivní zpravodajství.....	305
5.4.3 Vlivové zpravodajství (lobbying).....	305
5.5 Shrnutí .....	306

V. ČÁST - Bezpečnostní politika a bezpečnostní systém státu.....	309
1. Systém mezinárodní bezpečnosti.....	311
1.1 Úvod.....	311
1.2 Základní pojetí mezinárodního bezpečnostního systému.....	311
1.3 Státy.....	313
1.4 Mezivládní bezpečnostní organizace a aliance.....	314
1.5 Nestátní bezpečnostní aktéři v mezinárodním prostoru.....	316
1.6 Mezinárodní právo veřejné v bezpečnostní oblasti.....	319
1.7 Soudobé bezpečnostní hrozby.....	322
1.8 Shrnutí.....	324
2. Bezpečnostní politika a bezpečnostní strategie státu.....	327
2.1 Úvod.....	327
2.2 Bezpečnost.....	327
2.3 Referenční objekt bezpečnostní politiky.....	328
2.4 Obsah a trendy bezpečnostní politiky státu.....	329
2.5 Východiska bezpečnostní politiky státu.....	331
2.5.1 Bezpečnostní zájmy státu (národní zájmy).....	331
2.5.2 Analýza a predikce bezpečnostních hrozeb a rizik.....	332
2.5.3 Disponibilní zdroje pro bezpečnostní politiku státu.....	333
2.5.4 Limity bezpečnostní politiky státu.....	334
2.6 Bezpečnostní strategie státu.....	335
2.6.1 Bezpečnostní strategie České republiky.....	336
2.6.2 Bezpečnostní strategie České republiky 2011 a její charakteristika.....	337
2.7 Shrnutí.....	338
3. Bezpečnostná a obranná politika Slovenskej republiky.....	341
3.1 Úvod.....	341
3.2 Bezpečnostná stratégia Slovenskej republiky.....	342
3.3 Obranná stratégia Slovenskej republiky.....	347
3.4 Zhrnutie.....	350
4. Bezpečnostný systém a obrana Slovenskej republiky.....	352
4.1 Úvod.....	352
4.2 Bezpečnostný systém Slovenskej republiky.....	353
4.3 Obrana a systém obrany Slovenskej republiky.....	360
4.4 Zhrnutie.....	366
5. Strategický rámec plánovania ozbrojených síl ako kľúčová platforma obranného plánovania štátu.....	368
5.1 Úvod.....	368
5.2 Strategické prostredie štátu pre plánovanie ozbrojených síl.....	368
5.3 Analýza trendov výdavkov na obranu.....	374
5.4 Zhrnutie.....	376
Resumé – summary.....	378
Představení autorů kapitol.....	379

## ÚVOD MONOGRAFIE

Oblast bezpečnosti patří trvale mezi priority lidské společnosti. Ve své podstatě se dotýká všech jejích oborů i úrovní. Fungují-li systémy bezchybně, potřeba bezpečnosti není prioritou. Jiná situace nastane, dojde-li k degradaci nebo úplnému přerušení funkce. Ihned se volá po její obnově a hledají se způsoby, jak toho dosáhnout. Otázka bezpečnosti se tak stává prioritou. Díky dlouhodobému společenskému vývoji se člověk i společnost stali v této oblasti proaktivní a snaží se na kritické situace dopředu připravit. Na základě analýzy hrozeb a rizik stanovují priority v ochranných a nápravných opatřeních. Právě znalost situace, její analýza a opatření k eliminaci hrozeb jsou základem zajištění bezpečnosti.

Napomoci zajištění bezpečnosti a ochraně majetku na všech úrovních je cílem monografické řady Bezpečnostní technologie, systémy a management. Multidimenzionalita oboru předznamenává i obsah jednotlivých dílů. První díl, vydaný v roce 2011, byl zaměřen na problematiku detektorů narušení, elektronických bezpečnostních systémů, projektování zabezpečovacích systémů, právní aspekty zajištění ochrany majetku a profesní obranu. Ohlasy na publikaci i její koncept byly v převážné míře pozitivní. Určité výtky se objevily ohledně dodržování pojmového aparátu v jednotlivých monotematických částech. Zkušenější autoři ví, že nejsnadnější cestou k dosažení jazykové čistoty je zpracovat si celý text vlastními silami. Kolektivní publikace jsou poznamenány různými autorskými styly, názory autorů a jsou plné kompromisů. Koncept naší publikace tento problém akceptuje a je na vedoucímu příslušné části, aby se s ním vypořádal.

Druhý díl, který právě držíte ve svých rukou, respektuje původní schéma. Je složen z pěti částí a v každé části je pět kapitol. Jednotlivé kapitoly by na sebe měly navazovat, a tím odborně pokrýt celou problémovou oblast. Technická témata jsou zaměřena na problematiku kamerových systémů, technické prostředky profesní ochrany a informační podporu. Systémová a politologická témata zahrnují problematiku řízení rizik v bezpečnostních aplikacích a systém mezinárodní bezpečnosti a krizové řízení. Autoři kapitol se zaměřili na zveřejnění jak nejnovějších poznatků v prezentovaném oboru, tak i výsledků své výzkumné a tvůrčí činnosti. Podařilo se tak vytvořit publikaci, která rozšiřuje poznatkovou bázi v oblasti bezpečnosti s orientací na problematiku ochrany majetku, fyzické bezpečnosti a soukromých bezpečnostních služeb. Publikované poznatky mohou být využity i v jiných oblastech zajištění bezpečnosti.

Již nyní je zřejmé, že na doposud vydané díly naváží minimálně dva další, které by měly pokrýt další základní témata oboru. Z technických oblastí se jedná především o elektrickou požární signalizaci, systémy kontroly vstupu a poplachové zabezpečovací systémy. Přínosná bude zcela jistě i oblast technologií komerční bezpečnosti, jako jsou fyzická ostraha, převoz peněz či detektivní činnosti. Samostatnou oblastí pak bude i kriminalistika, kriminologie a bezpečnostní futurologie. Vzhledem k blízké vazbě mezi komerční bezpečností a bezpečností zajišťovanou státem autoři zvažují o zařazení takových témat jako ochrana kritické infrastruktury, ochrana obyvatelstva, havarijní plánování atd. Konkrétní struktura dílů bude samozřejmě záviset i na výsledcích výzkumných a tvůrčích činností vysokoškolských pracovišť, které se na publikaci podílí.

Publikace vychází zejména z dlouhé tradice vědecké a pedagogické práce v oblasti bezpečnostních technologií na Fakultě aplikované informatiky Univerzity Tomáše Bati ve Zlíně, Fakultě speciálního inženýrstva Žilinské univerzity v Žilině a Fakultě

bezpečnostního inženýrství Vysoké školy báňské – Technické univerzity v Ostravě. Autorský kolektiv se postupně rozrůstá o zástupce dalších vysokých škol, Vysoké školy bezpečnostního manažerstva v Košiciach, Masarykovy univerzity a Univerzity obrany. Autoři vyšli při zpracování jednotlivých kapitol z aktuálních výzkumů, prováděných v rámci grantových projektů a ze zkušeností, které získali při uplatňování nabytých vědeckých poznatků v praxi.

Jednotlivé kapitoly respektují jak metodologickou, tak poznatkovou stránku. Mezi základní metody, které autoři jednotlivých částí publikace při jejím zpracování použili, patří základní metody tvůrčí práce, především analýza a syntéza. Analýza byla využita při objasňování podstaty i jednotlivých stránek a aspektů prezentované problematiky. Syntéza představovala metodický základ k integraci výkladu jednotlivých poznatků a jejich propojení v logický celek. Významně byla při tvorbě publikace použita metoda systémového přístupu. S jejím využitím byla vytvořena obsahová konstrukce kapitol tak, aby tvořily logicky provázaný celek a současně na sebe navazovaly. Právě ucelenost a komplexnost představuje významný rys přidané hodnoty kolektivní monografie. Autoři především technicky orientovaných kapitol využili při tvorbě poznatků metod modelování, simulace a experimentu.

Tato publikace je určena všem zájemcům, kteří chtějí porozumět způsobům a metodám zajištění bezpečnosti, ochrany majetku a fyzické bezpečnosti. Je určena jak pracovníkům bezpečnostního managementu organizací, tak samotným poskytovatelům služeb fyzické bezpečnosti a ochrany majetku. Zejména pro ně jsou cenné kapitoly, zaměřené na podstatu technického fungování kamerových systémů, technických prostředků profesní ochrany a informační podpory. V neposlední řadě je tato publikace určena studentům všech studijních oborů, zaměřených na bezpečnostní technologie, ochranu majetku, fyzickou bezpečnost a bezpečnostní management. Knihu mohou využít všichni odborníci a zájemci, pro které je zajištění bezpečnosti prioritou.

Ve Zlíně 17. června 2012

doc. Ing. Luděk Lukáš, CSc.



## **I. ČÁST - KAMEROVÉ SYSTÉMY**

## Úvod

Část je věnována kamerovým systémům (CCTV – Closed Circuit Television), které představují vhodný prostředek používaný pro ochranu objektů, majetku a osob. Umožňují sledování hlídaného prostoru v reálném čase, nepřetržitý záznam obrazu, verifikaci příčiny poplachu, prohlížení záznamu a archivaci pro následnou rekonstrukci situace. Správně navržený a odborně nainstalovaný kamerový systém může být přínosem nejen z hlediska bezpečnosti, lze ho využít i pro sledování a vyhodnocování technologických postupů při výrobě, kontrole dodržování bezpečnostních předpisů, kontrole pohybu vozidel s možností detekce SPZ a následného porovnání údajů s databází.

Kamerové systémy jsou tvořeny kamerami, hardwarovou částí (přenosové prvky, záznamový prostor, zobrazovací prvky) a softwarem pro činnost systému. Navíc mohou být doplněny mikrofony a reproduktory. Přenos obrazu a ovládání kamer lze realizovat po veřejné telefonní síti (PSTN), ISDN), přes internet TCP/IP (IP kamery), prostřednictvím bezdrátového rádiového přenosu, po sítích LAN nebo WAN nebo pomocí kabelů (včetně optických). Návrh vhodného řešení kamerového systému je nutné vždy posoudit přímo na místě plánované instalace s ohledem na požadavky zákazníka a místní specifické podmínky.

Kamerové systémy lze využít k monitorování venkovních prostranství i míst uvnitř budov. Mohou obsahovat statické i otočné kamery a mohou pracovat ve zcela automatickém režimu nebo být ovládány např. ostrahou objektu. Moderní IP kamery a kamerové systémy umožňují připojení do sítí LAN/WAN. Uživatel s dostatečnými přístupovými právy se může vzdáleně nejen do systému připojit a sledovat obrazy z živých kamer, ale i sledovat záznam, případně celé zařízení vzdáleně ovládat.

Při současném rozvoji výpočetní techniky je trendem všech technických odvětví dosažení digitalizace. U kamer je situace obdobná. Většina kamer využívaných v CCTV systémech je plně digitalizována. Digitální kamery na rozdíl od analogových umožňují větší variabilitu, kompatibilitu s digitálními systémy, jednodušší práci s pořízenými záznamy a v neposlední řadě snadnější archivaci záznamů. Analogové kamery však stále nacházejí uplatnění především pro stále nepřekonanou vysokou kvalitu analogového záznamu. Pomyslný přechod mezi analogovými a digitálními kamerami tvoří digitální, tzv. hybridní kamery umožňující jak digitální, tak analogový záznam.

Kamerové systémy lze navázat na ostatní zabezpečovací systémy v budově. Mezi nejčastější součinnosti patří koordinace s PZS - v případě narušení střeženého objektu lze nastavit záznam údajů z kamery. Se systémem EPS probíhá koordinace například tak, že se aktivuje kamera v prostoru, odkud přišlo hlášení o požáru. Výstup z kamery je vidět na monitorech a lze jej nahrávat na záznamové zařízení. Je-li budova vybavena také systémem místního rozhlasu, je možné do ohroženého prostoru vysílat evakuační hlášení. Kamerové systémy velmi účinným způsobem chrání životy, zdraví a majetek. V neposlední řadě mají kamerové systémy též významnou funkci prevence.



# 1. KAMEROVÉ SYSTÉMY AKO SÚČASŤ KOMPLEXNÉHO BEZPEČNOSTNÉHO SYSTÉMU

*Tomáš LOVEČEK*

## 1.1 Úvod

Systém, ktorý v sebe zahŕňa jednotlivé subsystémy ochrany hmotného, resp. nehmotného majetku v správe alebo vlastníctve daného subjektu, a ktorý je vytvorený účelným usporiadaním a používaním ochranných opatrení, sa v praxi označuje rôznymi prívlastkami. Najčastejšie sa používajú termíny ako bezpečnostný systém, systém ochrany majetku/objektov, systém fyzickej ochrany, zabezpečovací systém alebo integrovaný bezpečnostný systém. Vo všeobecnosti systémom možno chápať účelovo definovanú množinu prvkov (istých vlastností) a množinu väzieb medzi nimi, ktoré spolu určujú vlastnosti, správanie a funkcie systému ako celku. Na základe tejto definície systém na ochranu hmotného, resp. nehmotného majetku daného subjektu, je možné chápať ako účelové usporiadanie množiny ochranných opatrení a ich vlastností, ktoré majú vytvoriť stav bezpečia. Ak ochrana majetku je proces navodenia stavu bezpečia s využitím ochranných opatrení, ktoré smerujú k prekazeniu, alebo zastaveniu akýchkoľvek činností (napr. vlámanie spojené s vandalizmom) alebo udalostí (napr. elektrický skrat a následný požiar), ktoré sú v rozpore so záujmami vlastníka tohto majetku, tak potom ochranný systém je nástrojom využívaným na dosiahnutie tohto stavu. V kapitole budeme takýto systém označovať ako bezpečnostný systém.

Preto pod pojmom bezpečnostný systém budeme chápať systém realizovaný mechanicko-technickými, personálnymi a režimovými ochrannými opatreniami, resp. prvkami. Ochranné opatrenia možno rozdeliť na:

- pasívne prvky ochrany:
  - pasívne prvky predmetovej ochrany,
  - pasívne prvky plášťovej ochrany,
  - pasívne prvky obvodovej ochrany,
- aktívne prvky ochrany,
- prvky fyzickej ochrany,
- režimovo-organizačné opatrenia.

Pasívne prvky ochrany patriace do skupiny klasickej ochrany, reprezentujú mechanické zábranné prostriedky, ako napríklad stavebné konštrukcie, otvorové výplne, bezpečnostné úschovné objekty, uzamykacie systémy, bezpečnostné sklá, resp. fólie a iné bariéry (napr. retardéry, ploty). Aktívne prvky ochrany, patriace do skupiny technickej ochrany, reprezentujú poplachové systémy, medzi ktoré patrí elektrický zabezpečovací systém, kamerový dohliadací systém, systém kontroly a riadenia vstupu a elektrická požiarňa signalizácia. Fyzickú ochranu môžeme rozdeliť na vlastnú ochranu (napr. Neighbourhood watch) a ochranu zabezpečovanú bezpečnostnými službami.

## **Bezpečnostní technologie, systémy a management II.**

**Editor: doc. Ing. Luděk Lukáš, CSc.**

**Kamerové systémy - garant: doc. Mgr. Milan Adámek, Ph.D.**

**Řízení rizik v bezp. inženýrství - garant: Doc. Mgr. Ing. Radomír Ščurek, Ph.D.**

**Technologie profesní obrany - garant: Ing. Zdeněk Maláník**

**Informační podpora - garant: doc. Ing. Luděk Lukáš, CSc.**

**Bezpečnostní politika a bezpečnostní systém státu - garant: brig. gen. doc. Ing. Miroslav KELEMEN, Ph.D.**

**Jazyková korektura: Ing. Arch. Jaroslav Svozil (česká část)**

**Mgr. Eva Lukášová (slovenská část)**

**Grafická a formální úprava: MgA. Žaneta Drgová, DiS.**

**Ing. Luboš Nečesal**

**Vydavatel: Radim Bačuvčík - VeRBuM**

**(Přehradní 292, 763 14 Zlín 12, Česká republika)**

**Zlín, 2012**

**1. vydání. 387 stran. Náklad 1000 ks.**

**Tisk: Nosova tiskárna, Brno**

**www.verbum.name**

**ISBN 978-80-87500-19-4**