

Obsah

Úvod monografie	10
1 Bezpečnost a bezpečnostní prostředí.....	13
1.1 Úvod.....	13
1.2 Základní pojetí bezpečnosti.....	13
1.2.1 Sekuritizace.....	14
1.2.2 Kodaňská škola.....	14
1.2.3 Teorie rizik.....	15
1.2.4 Teorie krizí.....	15
1.2.5 Teorie kauzality.....	16
1.3 Vymezení pojmu bezpečnostní prostředí.....	16
1.4 Typy faktorů bezpečnostního prostředí.....	18
1.5 Způsoby popisu bezpečnostního prostředí.....	19
1.6 Bezpečnostní prostředí České republiky.....	20
1.7 Příklady bezpečnostního prostředí.....	22
1.7.1 Měkké cíle.....	22
1.7.2 Státní správa.....	23
1.7.3 Doprava.....	23
1.7.4 Energetika.....	24
2 Druhy bezpečnosti a jejich konvergence.....	26
2.1 Úvod.....	26
2.2 Vymezení druhu bezpečnosti.....	26
2.3 Konvergence druhů bezpečnosti.....	28
2.4 Členění druhů bezpečnosti podle příbuznosti a společných znaků.....	29
2.5 Státní ochrana.....	29
2.6 Environmentální ochrana.....	33
2.7 Ochrana života a zdraví osob.....	34
2.8 Ochrana majetku.....	37
2.9 Ochrana informací.....	38
2.10 Konvergence druhů bezpečnosti.....	40
2.11 Shrnutí.....	41
3 Konvergovaná bezpečnost a její význam.....	43
3.1 Úvod.....	43
3.2 Základní pojmy z oblasti bezpečnosti.....	43
3.3 Uvažované druhy bezpečnosti.....	44
3.4 Charakteristické vlastnosti základních typů bezpečnosti.....	45
3.4.1 Fyzická bezpečnost (FB).....	45
3.4.2 Informační bezpečnost (IB).....	46
3.4.3 Kybernetická bezpečnost (KB).....	46
3.4.4 Provozní bezpečnost (PB).....	47
3.5 Požadavky na slučování bezpečností.....	48
3.6 Vlastnosti konvergované bezpečnosti KnB.....	49
3.7 Společný přístup ke konvergované bezpečnosti KnB v různých hospodářských segmentech.....	50
3.8 Mezinárodní přístup ke konvergované bezpečnosti KnB.....	51
3.9 Prostředky pro řešení KnB v bezpečnostní praxi.....	52
3.10 Modelový příklad řešení kybernetického incidentu v případě oddělených druhů bezpečnosti a v případě využití vlastností KnB.....	53

3.11	Shrnutí	55
4	Fyzická bezpečnost	57
4.1	Úvod.....	57
4.2	Fyzická bezpečnost, cíl a účel	57
4.3	Hlavní hrozby, újmy, opatření	58
4.4	Základní model bezpečnostního prostředí.....	61
4.5	Způsoby zajištění fyzické bezpečnosti	63
4.6	Systém fyzické bezpečnosti	64
4.7	Shrnutí	68
5	Kybernetická bezpečnost.....	70
5.1	Úvod.....	70
5.2	Specifika kybernetické bezpečnosti.....	70
5.3	Kybernetická bezpečnost v České republice.....	72
5.3.1	CERT a týmy typu CSIRT	72
5.4	Standardy kybernetické bezpečnosti	72
5.4.1	ISO/IEC 27001 a 27002.....	73
5.4.2	Zákon č. 110/2019 Sb., o zpracování osobních údajů	74
5.4.3	GDPR	74
5.5	Hrozby v kybernetickém prostoru	75
5.5.1	Malware	75
5.5.2	Sociální inženýrství.....	77
5.5.3	Denial of Service	78
5.5.4	SQL injection a Cross-site scripting	79
5.6	Opatření proti hrozbám	79
5.6.1	Firewall	80
5.6.2	Antivirus a Anti-Malware software.....	80
5.6.3	Anti-Spam software	80
5.6.4	Technologie pro monitoring, prevenci a detekci	80
5.6.5	Virtual Private Network	81
5.6.6	Penetrační testy	81
5.7	Shrnutí	82
6	Provozní bezpečnost	85
6.1	Vymezení druhu bezpečnosti	85
6.2	Hrozby a újmy na negativní dopady	86
6.3	Základní model bezpečnostního prostředí.....	87
6.3.1	Pravidla provozování přenosové soustavy	87
6.3.2	Provozní bezpečnost rozvodny	88
6.3.3	Rizika vybraného referenčního objektu.....	94
7	Odolnost referenčního objektu.....	98
7.1	Úvod.....	98
7.2	Odolnost' infrastrukturních systémov.....	98
7.3	Obecné východiská hodnotenia odolnosti.....	99
7.4	Oblasti vymedzujúce odolnosť	100
7.4.1	Pripravenosť	100
7.4.2	Absorpčia	101
7.4.3	Redundancia	102
7.4.4	Robustnosť	103
7.4.5	Rezistencia.....	104
7.4.6	Reakcieschopnosť	105

7.4.7	Obnovitelnost'	106
7.4.8	Adaptabilita	107
7.5	Vazby oblastí vymezujících odolnost'	109
7.6	Záver	110
8	Algoritmus pro výpočet odolnosti systému ochrany z pohledu konvergované bezpečnosti	113
8.1	Úvod	113
8.2	Konvergovaná bezpečnost, principy a východiska řešení	113
8.3	Podstata hodnocení odolnosti z pohledu konvergované bezpečnosti	115
8.4	Specifikace a podrobný popis algoritmu hodnocení odolnosti při on-line hodnocení	118
8.5	Postup výpočtu indexu odolnosti referenčního objektu s využitím obecných katalogů penalizačních faktorů	123
8.5.1	Specifikace referenčního objektu	124
8.5.2	Specifikace aktiv	124
8.5.3	Vytvoření výchozího katalogu penalizačních faktorů	124
8.5.4	Zpřesnění katalogu penalizačních faktorů	125
8.5.5	Výpočet indexu odolnosti aktiva pro jednotlivé druhy bezpečnosti	125
8.5.6	Výpočet indexu odolnosti pro druh bezpečnosti	126
8.5.7	Výpočet indexu odolnosti referenčního objektu	126
8.6	Shrnutí	126
9	Nástroje kybernetické bezpečnosti	127
9.1	Úvod	127
9.2	Zjištění stavu infrastruktury	127
9.3	Základní bezpečnostní nástroje pro ochranu endpointů	129
9.3.1	Antivirus	130
9.3.2	Firewall	131
9.4	Nástroje pro dohled nad sítí	134
9.4.1	Omezení možnosti auditu	136
9.4.2	Monitoring sítě na úrovni HW prvků	138
9.4.3	DPI	139
9.4.4	Korelace informací	141
9.5	SIEM (Security Information and Event Management)	141
9.6	Shrnutí	143
10	Penalizace a katalog penalizačních faktorů	145
10.1	Úvod	145
10.2	Podstata penalizace	146
10.3	Katalog penalizačních faktorů	147
10.3.1	Tvorba obecného katalogu penalizačních faktorů	147
10.3.2	Aktualizace penalizačních údajů	151
10.4	Postup použití katalogu penalizačních faktorů	152
10.5	Shrnutí	152
11	Způsoby a metody kvantifikace penalizace	155
11.1	Úvod	155
11.2	Vybrané metody pro kvantifikaci penalizačních faktorů	155
11.2.1	Checklist v kombinaci s bodovou metodou	155
11.2.2	Multikriteriální hodnocení velikosti penalizace	156
11.2.3	Metoda založená na expertním odhadu	156
11.2.4	Fullerova metoda	157

11.2.5	Modifikovaná Saatyho metoda	157
11.2.6	Párové srovnání rozšířené o ELO rating.....	158
11.2.7	Metfesselova alokace.....	159
11.2.8	Stupnice hodnocení.....	159
11.3	Popis modelového příkladu.....	160
11.4	Postup výběru optimální metody.....	161
11.5	Kvantifikované penalizační faktory pro modelový příklad	161
11.6	Metodika pro určení optimální metody pro kvantifikaci penalizačních faktorů	164
11.6.1	Fyzická bezpečnost	165
11.6.2	Kybernetická bezpečnost.....	165
11.6.3	Provozní bezpečnost.....	166
11.6.4	Souhrnné výsledky	167
11.7	Shrnutí	167
12	Systémy kategorie PSIM/SIEM jako zdroj dat pro hodnocení odolnosti	169
12.1	Úvod.....	169
12.2	Využití technologických prostředků pro hodnocení odolnosti	169
12.3	PSIM systémy	170
12.4	Systémy integrovatelné pod PSIM	173
12.5	Příklad využití PSIM v dopravě.....	176
12.6	SIEM systémy	177
12.7	Systém pro konvergovanou bezpečnost – CSIM.....	178
12.8	Příklady využití dat z podsystémů CSIM pro hodnocení odolnosti	180
12.9	Shrnutí	182
13	On-line security manager – nástroj pro hodnocení odolnosti z pohledu konvergované bezpečnosti	184
13.1	Úvod.....	184
13.2	Modul OSM	184
13.3	Princip modulu OSM a jeho funkcionality	185
13.4	Obecný princip fungování modulu OSM	187
13.5	Funkční bloky modulu OSM	187
13.5.1	Blok: Databáze a katalogy.....	188
13.5.2	Blok: Nastavení modulu	190
13.5.3	Blok: Výpočet odolnosti.....	191
13.5.4	Blok: Konfigurační rozhraní	191
13.5.5	Blok: Zobrazení dat	191
13.5.6	Blok: Historie	192
13.5.7	Blok: Vstupní data a konverze dat.....	192
13.5.8	Blok: Výstupní data a konverze dat	193
13.6	Metodický postup stanovení odolnosti v modulu OSM	193
13.7	Shrnutí	198
	Resumé – summary	200
	Představení autorů kapitol	201