


Komparácia efektívnosti využitia fyzickej ostrahy a perimetrického detekčného systému pre potreby perimetrickej ochrany

**Efectivnes Comparison of Physical Security and PDS for the Needs of Perimeter
Protection**

Mário Mičo

Bakalárska práca
2013

 Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2012/2013

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Mário MIČO**
Osobní číslo: **A10103**
Studijní program: **B3902 Inženýrská informatika**
Studijní obor: **Bezpečnostní technologie, systémy a management**
Forma studia: **prezenční**

Téma práce: **Komparace efektivity využití fyzické ostrahy a perimetrického detekčního systému pro potřeby perimetrické ochrany**

Zásady pro vypracování:

1. Analyzujte aktuální legislativní prostředí v oblasti ochrany majetku a osob.
 2. Zhodnoťte význam perimetrické ochrany a fyzické ostrahy v oblasti ochrany majetku a osob.
 3. Analyzujte současné trendy perimetrického detekčního systému (dále PDS) a fyzické ostrahy ve vztahu k systémům fyzické ochrany.
 4. Specifikujte požadavky na perimetrickou ochranu realizovanou PDS a fyzickou ostrahou.
 5. Komparujte efektivnost využití fyzické ostrahy a PDS pro potřeby perimetrické ochrany.
-

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. ČERNÝ, Josef, Ivanka, Ján. *Systemizace bezpečnostního průmyslu I.* 2.vyd. Zlín : UTB Zlín,2006. 135 s. ISBN 80-7318-402-8.
2. LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti II.* 2.vyd. Zlín : UTB Zlín, 2007. 123 s. ISBN 978-80-7318-631-9.
3. LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management I.* 1.vyd. Zlín : VeRBuM, 2011. 316 s. ISBN 978-80-87500-05-7.
4. MC9S08QG4CPAE Data Sheet [online]. Freescale Semiconductor,2011 [cit. 2012-01-25].
5. PINKER, Jiří. *Mikroprocesory a Mikropočítače.* Praha : BEN – technická literatura, 2004. 220 s. ISBN 80-7300-110-1.

Vedoucí bakalářské práce:

Ing. Martin Hromada, Ph.D.

Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce:

25. února 2013

Termín odevzdání bakalářské práce:

30. května 2013

Ve Zlíně dne 25. února 2013

prof. Ing. Vladimír Vašek, CSc.
děkan



doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT

Táto bakalárska práca pojednáva o rozčlenení jednotlivých detektorov z rôznych fyzikálnych hľadísk pre potreby perimetrickej ochrany. Taktiež popisuje základné princípy fungovania a hlavných úloh fyzickej ostrahy. V teoretickej časti sú popísané systémy spadajúce do oblasti majetku a osôb vo vzťahu k priemyslu komerčnej bezpečnosti. Cieľom tejto bakalárskej práce je komparácia týchto dvoch odlišných prístupov bezpečnostného priemyslu. V závere práce sú spomenuté jednotlivé vývojové trendy daných bezpečnostných prvkov a popis silných a slabých stránok zvolených oblastí..

Kľúčové slová: perimeter, komparácia, bezpečnosť

ABSTRACT

This bachelor thesis deals with the analysis of individual detectors from different physical points of view for the needs of perimeter protection. It also describes the basic principles of operation and the main tasks of physical security. In the theoretical part had been described the systems belonging to the area of property and persons in relation to the commercial security industry. The main aim of this bachelor thesis is the comparison of these two different approaches security industry. In conclusion are mentioned the individual developmental trends of the security elements and a description of the strengths and weaknesses of selected areas.

Key words: perimeter, comparison, security

Ďakujem svojmu vedúcemu bakalárskej práce Ing. Martinovi Hromadovi, Ph.D. za odborné vedenie, podnetné rady, informácie a pripomienky, ktoré mi poskytoval počas spracovávania mojej bakalárskej práce. Ďalej chcem poďakovať svojim rodičom a blízkym za podporu, ktorej sa mi dostávalo počas môjho štúdia.

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně

.....
podpis diplomanta

Obsah

ÚVOD	9
I. TEORETICKÁ ČASŤ	10
1 PERIMETRICKÁ OCHRANA	11
1.1 LEGISLATÍVNE PROSTREDIE V SBS	11
1.2 NÁVRH ZÁKONA O SÚKROMNEJ BEZPEČNOSTNEJ ČINNOSTI	11
1.2.1 KATEGÓRIE BEZPEČNOSTNÝCH SLUŽIEB	12
1.3 ŽIVNOSTENSKÝ ZÁKON	13
1.3.1 PODMIENKY K PREVÁDZKOVANIU ŽIVNOSTI	13
1.3.2 ROZDELENIE ŽIVNOSTÍ.....	14
1.3.3 KONCESOVANÉ ŽIVNOSTI.....	14
1.4 TRESTNÝ ZÁKONÍK	16
1.4.1 § 2 TRESTNOSŤ ČINU A DOBA JEHO SPÁCHANIA.....	16
1.4.2 §13 TRESTNÝ ČIN	16
1.4.3 §14 PREČINY A ZLOČINY	17
1.4.4 §28 KRAJNÁ NÚDZA	17
1.4.5 §29 NUTNÁ OBRANA	17
1.4.6 §178 PORUŠOVANIE DOMOVEJ SLOBODY	17
1.4.7 § 205 KRÁDEŽ	18
2 VYUŽITIE A VÝZNAM PERIMETRICKEJ OCHRANY	19
2.1 ROZDELENIE DETEKTOROV PERIMETRICKEJ OCHRANY	23
2.1.1 ELEKTROMECHANICKÉ DETEKTORY	23
2.1.2 ELEKTROMAGNETICKÉ DETEKTORY	23
2.1.2.1 Elektromagnetické žiarenie	24
2.1.2.2 Dopplerov jav	24
2.1.3 ELEKTROAKUSTICKÉ DETEKTORY	24
2.1.4 AKTÍVNE DETEKTORY	25
2.1.4.1 Štrbinové káble.....	25
2.1.4.2 Kapacitné detektory.....	26
2.1.4.3 Duálne detektory	27
2.1.4.4 Mikrovlnné detektory a bariéry	28
2.1.4.5 Infračervené závory a bariéry	28
2.1.5 PASÍVNE DETEKTORY	28
2.1.5.1 Mikrofónové káble	29
2.1.5.2 Diferenciálne tlakové detektory	29
2.1.5.3 Pasívne infračervené detektory.....	29
3 FYZICKÁ OCHRANA	31

3.1	EXPANZIA SÚKROMNÝCH BEZPEČNOSTNÝCH SLUŽIEB	31
3.2	STRÁŽNA SLUŽBA	31
3.2.1	ÚVOD	31
3.2.2	FYZICKÁ OSTRAHA OBJEKTU	32
3.2.2.1	Statická ostraha objektu	33
3.2.2.2	Pohyblivá ostraha objektu	33
3.2.2.3	Monitorovacia ostraha objektu.....	34
3.2.2.4	Bezpečnostné doprovody osôb a vozidiel	34
3.2.3	TECHNICKÉ PROSTRIEDKY OCHRANY OBJEKTU	35
3.2.4	REŽIMOVÉ OPATRENIA	35
II.	PRAKTICKÁ ČASŤ	37
4	ÚVOD.....	38
5	SWOT ANALÝZA.....	39
5.1	HISTÓRIA	39
5.2	SWOT MATICA	40
5.2.1	ANALÝZA S-W	40
5.2.2	ANALÝZA O-T.....	41
5.3	TRVALÁ PREVÁDZKA.....	41
5.3.1	PERIMETRICKÉ DETEKČNÉ SYSTÉMY	42
5.3.2	FYZICKÁ OSTRAHA	43
5.3.3	SWOT ANALÝZA TRVALEJ PREVÁDZKY	45
5.3.4	TABUĽA SWOT ANALÝZY	47
6	VÝVOJOVÉ TRENDY	49
6.1	PRINCÍP RFID TAGU	49
	ZÁVER	51
	ZÁVER V ANGLIČTINE.....	52
	ZOZNAM POUŽITE LITERATÚRY	52
	ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK.....	55
	ZOZNAM OBRÁZKOV	56
	ZOZNAM TABULIEK	57

ÚVOD

V posledných 20 rokoch objem hmotného a nehmotného majetku prudko narástol. Na tomto fakte ma určitý podiel aj pád komunizmu. Vznik demokratickej republiky prinieslo do Českej republiky možnosť voľne podnikat' a hlavne vytvárať zahraničný obchod. Tento fakt zapríčinil obrovský rast majetkov u ľudí. Ochranu obyvateľstva ako takého má nastarosti hlavne polícia ČR a armáda ČR. Bohužiaľ štátny rozpočet na tieto zložky ochrany ľudí je výrazne obmedzený a ich sila pokrytia je nedostačujúca. Preto čoraz viacej ľudí hľadá určité alternatívy ako nielen svoj majetok ale aj život ochrániť. Ľudia sa obracajú na súkromné bezpečnostné služby čoraz viacej.

Jednou z oblastí pôsobnosti priemyslu komerčnej bezpečnosti je perimetrická ochrana, ktorá spočíva v zabezpečení objektu na jeho katastrálnych hraniciach. Toto zabezpečenie je realizované najskorej mechanickými zábrannými systémami ako sú ploty a závary. V tesnej blízkosti alebo priamo na mechanických zábranných systémov sa nachádzajú detekčné prvky perimetrickej ochrany. Detekujú strážený priestor a vyhlasujú poplachy pri snahe prekonať mechanické zábranné systémy. Keďže táto ochrana je na začiatku stráženého objektu je veľmi pravdepodobné, že páchatel' bude zneškodnený skorej ako stihne niečo ukradnúť.

Tento druh poplachových zabezpečovacích a tiesňových systémov je veľmi drahý a preto sa často inštaluje len do strážených objektov zo stupňom zabezpečenia tri a štyri. Sem patria atómové elektrárne, muničné sklady, štátne rezervy a objekty národného a vyššieho významu.

Fyzická ostraha je tiež veľmi dôležitou súčasťou ochrany osôb a majetku. Jedná sa hlavne o statickú ostrahu a pohyblivú ostrahu objektu. Ich presná náplň činností je uvedená v zmluve o ochrane objektu, kde zákazník presne definuje miesto, čas, procesy a organizáciu. Taktiež stanovuje rozsah právomocí.

I. TEORETICKÁ ČASŤ

1 PERIMETRICKÁ OCHRANA

1.1 Legislatívne prostredie v SBS

Situácia s kriminalitou vo svete je vážna a určite by sme ju nemali podceňovať. Fyzická ochrana je jedna zo základných a dodnes najdôležitejších foriem ochrany. Svedčí o tom aj fakt, že v Európe je približne 10 000 súkromných služieb, ktoré zamestnávajú okolo 600 000 zamestnancov. Žiadne detektory ani prvky bezpečnostných technológií zatiaľ nedokážu plne nahradiť ľudskú myseľ. Fyzická ostraha rieši veľké množstvo udalostí. Tento druh ochrany zabezpečujú vysoko školený a trénovaný ľudia aby dosahovali čo najväčšiu efektívnosť s čo najnižšími škodami. Fyzická ostraha má najväčšiu úlohu v zabezpečení ochrany osôb a majetku. Jedná sa o odhaľovanie narušiteľov a ich následné zadržanie. Pretože neexistuje zákon o civilných bezpečnostných službách musí sa fyzická ochrana odvolávať na alternatívne zákony ako sú živnostenský zákon č.455/1991 Sb. v znení zmien a doplnkov, obchodný zákonník a trestným zákonom č. 40/2009 Sb. v znení zmien a doplnkov.

1.2 Návrh zákona o súkromnej bezpečnostnej činnosti

Zámer podriaďiť súkromné bezpečnostné služby samotnej právnej úprave bol prvý krát verejne deklarovaný v koalíčnej zmluve prijatej koalíčným poslancom ODS. Následne bola táto úloha spracovať priamo paragrafové znenie zákona uložená Ministerstvu vnútra ČR programovým vyhlásením vlády a to sa odrazilo aj v pláne legislatívnych prácach vlády na rok 2011.

Návrh zákona o súkromnej bezpečnostnej činnosti bol v januári 2013 predložený Vláde ČR. V súlade s legislatívnymi pravidlami vlády je návrh zákona najprv prerokovaný Legislatívnou radou vlády. Až potom je zaradený na program rokovania vlády. Legislatívna rada vlády sa delí na niekoľko pracovných komisií so zameraním na rôzne odbory práva. Tieto pracovné komisie sa návrhu zákona venujú najskôr a ich pripomienky a odporúčania sú súčasťou prerokovania Legislatívnej rady vlády (LRV) a tvoria potom aj časť stanoviska LRV. Vláda zvyčajne o návrhu hlasuje a prijíma ho v znení pripomienok uvedených v stanovisku LRV. Stanovisko LRV je teda kľúčové a výrazne ovplyvňuje výslednú podobu návrhu zákona.

Návrh zákona o súkromnej bezpečnostnej činnosti už bol prejednávaný pracovnými komisiami LRV. Rokovania celej LRV by malo prebehnúť v priebehu mesiaca mája (s najvyššou pravdepodobnosťou 30.5.2013). Až potom bude stanovený termín, kedy bude návrh zaradený na rokovanie vlády.

1.2.1 Kategórie bezpečnostných služieb

Toto rozdelenie do kategórií je zatiaľ len pripravované a zapísané v návrhu zákona o súkromnej bezpečnostnej činnosti. Rozdelenie je do piatich kategórií:

- Ostraha majetku a osôb
- Činnosť súkromných detektívov
- Prevoz hotovosti a cenín
- Technická služba k ochrane osôb a majetku
- Bezpečnostné poradenstvo

Ostraha majetku a osôb

- ochrana hnutel'ného a nehnuteľného majetku, osôb a právnych záujmov,
- zabezpečovanie poriadku v miestach verejných podujatí,
- prevádzka a obsluha dohľadových centier, ktoré napríklad prijímajú informácie o narušení konkrétneho stráženého miesta,
- prevoz hotovosti a cenín do hodnoty 5 000 000 Kč (rozdiel od špeciálnej kategórie prevoz hotovosti a cenín, kde sa vyžaduje prekročenie tejto hodnoty).

Činnosť súkromných detektívov

- hľadanie určitej osoby,
- zisťovanie skutočností, ktoré bude možné uplatniť pri orgáne štátu (súd, správny orgán)
- získavanie informácií o konkrétnej osobe (samozrejme za splnenia podmienok zákona č 101/2000Sb., o ochrane osobných údajov a o zmene niektorých zákonov)
- ďalej sa bude jednať o získavanie informácií v súvislosti s vymáhaním pohľadávky a pri vyhľadávaní protiprávneho jednania ohrozujúceho obchodné tajomstvo

Prevoz hotovosti a cenín

- Prevozom hotovosťou a cenín sa rozumie preprava takých hotovostí a cenín, prípadne iného majetku vyžadujúceho ostrahu, ktoré presahujú hodnotu 5 000 000 Kč za súčasného poskytovanie sprievodných služieb (počítanie, overovanie a spracovanie, výmena a smena nominálu, správa depozít).

Technická služba k ochrane osôb a majetku

- Táto služba je úzko spojená so zabezpečovacími systémami a dohľadovými, poplachovými a prijímacími centrami. V podstate sa bude jednať o bezpečnostnú službu, ktorá oprávňuje jej držiteľa na projektovanie, kontrole, montáži, údržbe a opravy zabezpečovacích systémov a montáži, údržbe, servisu a revíziu dohľadového, poplašného a prijímacieho centra.

Bezpečnostné poradenstvo

- Jedná sa o špeciálnu možnosť prevádzkovateľa poskytovať poradenskú, analytickú, projekčnú a podobnú činnosť súvisiacu s jednotlivými bezpečnostnými činnosťami. Samotné bezpečnostné činnosti uvedené v predchádzajúcich bodov však vykonávať nemôžu. [1]

1.3 Živnostenský zákon

Jedným zo zákonov ktorým sa môžu riadiť súkromné bezpečnostné služby je živnostenský zákon č. 455/1991 sb. ktorý určuje spôsob živnosti ktorý je potrebný k danému poskytovaniu služieb občanov. Podľa živnostenského zákona je živnosť sústavná činnosť prevádzkovaná samostatne, vo vlastnom mene, na vlastnú zodpovednosť, za účelom dosiahnutia zisku a za podmienok ustanovených týmto zákonom. [2]

1.3.1 Podmienky k prevádzkovaniu živnosti

Pri zakladaní živnosti, ktorá je potrebná k podnikaniu v oblasti priemyslu komerčnej bezpečnosti je nutné splniť niektoré podmienky k nadobudnutiu živnosti. Živnosť môže prevádzkovať aj fyzická alebo právnická osoba ktorá nemá trvalý pobyt alebo sídlo na území Českej republiky za rovnakých podmienok ako fyzická alebo právnická osoba z trvalým pobytom alebo sídlom na území Českej republiky.

Živnost' může převádzkovat' fyzická alebo právnická osoba ktorá splňa nasledovné všeobecné podmienky:

- Dosiahnutie veku 18 rokov
- Spôsobilosť k právnym úkonom
- bezúhonnosť

Za bezúhonnú sa pre účely tohto zákona nepovažuje osoba, ktorá bola právomocne odsúdená pre trestný čin spáchaný úmyselne, pokiaľ bol tento trestný čin spáchaný v súvislosti s podnikaním, alebo predmetom podnikania, o ktorý žiada alebo ktorý ohlasuje. Bezúhonnosť sa u občanov Českej republiky preukazuje výpisom z registra trestov. U občanov iného členského štátu Európskej únie sa bezúhonnosť preukazuje dokladom podľa § 46 odst. 1 písm. a) a u osôb ktoré nie sú občanmi Českej republiky ani iného členského štátu Európskej únie preukazujú svoju bezúhonnosť dokladom podľa § 46 odst. 1 písm. b).

1.3.2 Rozdelenie živností

Živnosti rozdeľujeme na dva druhy:

- Ohlasovacie - remeselné, viazané, voľné
- Koncesované

1.3.3 Koncesované živnosti

Tento druh živnosti zahrnuje druhy živností, ktoré umožňujú podnikat' v oblasti priemyslu komerčnej bezpečnosti. Podľa §27 majú koncesované živnosti nasledovné podmienky k prevádzkovaní tejto živnosti.

Občan Českej republiky alebo iného členského štátu Európskej únie musí preukázať svoju odbornú spôsobilosť dokladom o uznaní odbornej kvalifikácie vydaním uznávacím orgánom podľa zákona o uznávacej odbornej kvalifikácii. Pre podnikanie v oblasti priemyslu komerčnej bezpečnosti sú predmetom podnikania tri nasledovné živnosti:

- Ostraha majetku a osôb
- Služby súkromných detektívov
- Poskytovanie technických služieb k ochrane majetku a osôb

Ostraha majetku a osôb a služby súkromných detektívov majú dané požadované odborné spôsobilosti ktoré sú potrebné k založeniu týchto koncesovaných živností.

- a) vysokoškolské vzdelanie
- b) vyššie odborné vzdelanie právnického, bezpečnostného alebo podobného zamerania
- c) stredné vzdelanie s maturitou v odbore bezpečnostným alebo právnym a 3 roky praxe v odbore
- d) stredné vzdelanie s maturitnou skúškou, 3 roky praxe v odbore a osvedčení o rekvalifikáciu alebo iný doklad o odbornej kvalifikácii pre príslušnú pracovnú činnosť vydaný zariadením akreditovaným podľa osobitných právnych predpisov, zariadením akreditovaným Ministerstvom školstva, mládeže a telovýchovy, alebo ministerstvom, do ktorého pôsobnosti patrí odvetvie, v ktorom je živnosť prevádzkovaná
- e) stredné vzdelanie s maturitnou skúškou, 3 roky praxe v odbore a odbornú kvalifikáciu pre činnosť strážny podľa osobitného predpisu.

Ďalšie podmienky ktoré sú potrebné k založeniu koncesovanej živnosti sú spoľahlivosť podnikateľa, štatutárneho orgánu alebo členov štatutárneho orgánu a bezúhonnosť všetkých osôb, ktoré pre podnikateľa predmetnú činnosť vykonávajú § 6 odst. 2 zákona č. 455/1991.

Poskytovanie technických služieb k ochrane majetku a osôb majú tiež dané požadované odborné spôsobilosti, ktoré sú potrebné k založeniu týchto koncesovaných živností.

- a) Vysokoškolské vzdelanie som študijnom programe zameranom na študijnom odborov strojárstvo, elektrotechniku, telekomunikácie alebo výpočtovej technikov 1 rok praxe v odbore
- b) vyššie odborné vzdelanie v odborov vzdelania zameranom na strojárstvo, elektrotechniku, telekomunikácie alebo výpočtovej technikov 2 roky praxe v. Odborov
- c) stredné vzdelanie s maturitou v odborov vzdelania zameranom na strojárstvo, elektrotechniku, telekomunikácie alebo výpočtovej technikov 2 roky praxe v odbore
- d) stredné odborné vzdelanie s vyučením v odborov vzdelania zameranom na strojárstvo, elektrotechniku, telekomunikácie alebo výpočtovej technikov 3 roky praxe v odbore

e) osvedčenie o rekvalifikácii alebo iný doklad o odbornej kvalifikácii pre príslušné pracovné činnosti vydaný zariadením akreditovaným podľa osobitných právnych predpisov, zariadením akreditovaným ministerstvom školstva, mládeže a telovýchovy, ministerstvom alebo, vykonajte pôsobnosti ktorého Patri odvetví, v ktorom je živnosť prevádzkovaná, 4 roky praxe v odborov. [2]

1.4 Trestný zákonník

Podľa zákonov Českej republiky je trestný zákonník popísaný v zákone číslo 40/2009, ktorý je platný od 01.01. 2010. Skladá sa z dvoch častí:

- Prvá časť – Obecná časť
- Druhá časť – Zvláštna časť

1.4.1 § 2 Trestnosť činu a doba jeho spáchania

(1) Trestnosť činu sa posudzuje podľa zákona účinného v čase, keď bol čin spáchaný; podľa neskoršieho zákona sa posudzuje len vtedy, ak je to pre páchatel'a priaznivejšie.

(2) Ak sa zákon zmení počas páchania činu, užije sa zákona, ktorý je účinný pri dokončení rokovaní, ktorým je čin spáchaný.

(3) Pri neskorších zmenách zákona, ktorý je účinný pri dokončení konania, ktorým je čin spáchaný, sa užije zákona najmiernejšieho.

(4) Čin je spáchaný v čase, keď páchatel' alebo účastník konal alebo v prípade opomenutia bol povinný konať. Nie je rozhodujúce, kedy následok nastane alebo kedy mal nastať.

1.4.2 §13 Trestný čin

(1) Trestným činom je protiprávny čin, ktorý trestný zákon označuje za trestný a ktorý vykazuje znaky uvedené v takomto zákone.

(2) K trestnej zodpovednosti za trestný čin je treba úmyselné zavinenie, ak neustanovuje trestný zákon výslovne, že postačí zavinenie z nedbanlivosti.

1.4.3 §14 Prečiny a zločiny

- (1) Trestné činy sa delia na prečiny a zločiny.
- (2) Prečiny sú všetky nedbanlivostné trestné činy a tie úmyselné trestné činy, na ktoré trestný zákon ustanovuje trest odňatia slobody s hornou hranicou trestnej sadzby do piatich rokov.
- (3) Zločiny sú všetky trestné činy, ktoré nie sú podľa trestného zákona prečiny; zvlášť závažnými zločinmi sú tie úmyselné trestné činy, na ktoré trestný zákon ustanovuje trest odňatia slobody s hornou hranicou trestnej sadzby najmenej desať rokov.

1.4.4 §28 Krajná núdza

- (1) Čin inak trestný, ktorým niekto odvracia nebezpečenstvo priamo hroziace záujmu chránenému týmto zákonom, nie je trestným činom.
- (2) Nejde o krajnú núdzu, ak bolo možné toto nebezpečenstvo za daných okolností odvrátiť inak alebo spôsobený následok je zrejme rovnako závažný alebo ešte závažnejší ako ten, ktorý hrozil, alebo bol ten, komu nebezpečenstvo hrozilo, povinný ich znášať.

1.4.5 §29 Nutná obrana

- (1) Čin inak trestný, ktorým niekto odvracia priamo hroziaci alebo trvajúci útok na záujem chránený trestným zákonom, nie je trestným činom.
- (2) Nejde o nutnú obranu, ak obrana bola celkom zjavne neprimeraná útoku.

1.4.6 §178 Porušovanie domovej slobody

- (1) Kto neoprávnene vnikne do obydlia iného alebo tam neoprávnene zotrúva, bude potrestaný odňatím slobody až na dva roky.
- (2) Odňatím slobody na šesť mesiacov až tri roky bude páchatel' potrestaný, ak je pri čine uvedenom v odseku 1 násilie alebo hrozba bezprostredného násilia alebo ak prekoná prekážku, ktorej účelom je zabrániť vniknutiu.
- (3) Odňatím slobody na jeden rok až päť rokov alebo peňažným trestom sa páchatel' potresce, ak použije pri čine uvedenom v odseku 1 násilie alebo hrozbu bezprostredného násilia a taký čin spácha so zbraňou alebo najmenej s dvoma osobami.

1.4.7 § 205 Krádež

(1) Kto si prisvojí cudziu vec tým, že sa jej zmocní, a

- a) spôsobí tak na cudzom majetku škodu nie nepatrnú,
- b) čin spácha vlámaním,
- c) bezprostredne po čine sa pokúsi uchovať si vec násilím alebo hrozbou bezprostredného násilia,
- d) čin spácha na veci, ktorú má iný na sebe alebo pri sebe, alebo
- e) čin spácha na území, na ktorom je vykonávaná alebo bola vykonaná evakuácia osôb,

bude potrestaný odňatím slobody až na dva roky, zákazom činnosti alebo prepadnutím veci alebo inej majetkovej hodnoty.

(2) Kto si prisvojí cudziu vec tým, že sa jej zmocní, a bol za taký čin v posledných troch rokoch odsúdený alebo potrestaný, potrestá sa odňatím slobody na šesť mesiacov až tri roky.

(3) Odňatím slobody na jeden rok až päť rokov alebo peňažným trestom bude páchatel' potrestaný, ak spôsobí činom uvedeným v odseku 1 alebo 2 väčšiu škodu.

(4) Odňatím slobody na dva roky až osem rokov bude páchatel' potrestaný,

- a) ak spácha čin uvedený v odseku 1 alebo 2 ako člen organizovanej skupiny,
- b) ak spácha taký čin za stavu ohrozenia štátu alebo za vojnového stavu, za živelnej pohromy alebo inej udalosti vážne ohrozujúcej život alebo zdravie ľudí, verejný poriadok alebo majetok, alebo
- c) ak spôsobí takým činom značnú škodu.

(5) Odňatím slobody na päť až desať rokov bude páchatel' potrestaný,

- a) ak spôsobí činom uvedeným v odseku 1 alebo 2 škodu veľkého rozsahu, alebo
- b) ak spácha taký čin v úmysle umožniť alebo uľahčiť spáchanie trestného činu vlastizrady (§ 309), teroristického útoku (§ 311) alebo teroru (§ 312).

(6) Príprava je trestná. [14]

2 VYUŽITIE A VÝZNAM PERIMETRICKEJ OCHRANY

Pod pojmom perimetrická ochrana rozumieme zabezpečenie hraníc pozemku, ktoré sú vymedzené katastrálnym úradom a sú zapísané v katastri príslušnej obce.

Je to vonkajšia obvodová ochrana areálu pred vstupom nepovolaných osôb. Je to špeciálna aplikácia technických, elektronických, poprípade elektronicko-mechanických vonkajších zabezpečovacích systémov, ktorých úlohou je zachytiť prípadného páchatel'a ešte predtým ako začne páchať trestnú činnosť v strážených priestoroch. [3]

Prakticky je možné strážiť celú plochu pozemku ale nie je to ekonomicky efektívne preto sa perimetrická ochrana využíva na strázenie určitých koridorov, spravidla lineárnych, na obvode chráneného pozemku. Dôležitou požiadavkou na časti vonkajšej perimetrickej ochrany je nezávislosť funkcie na klimatických podmienkach. V dnešnej dobe sa používa celý rad prvkov pre montáž týchto systémov. Vždy je dôležité dobre zvoliť systém pre konkrétne podmienky. Perimetrická ochrana je dôležitá súčasť zabezpečenia rozsiahlych areálov ako sú napríklad elektrárne, chemické sklady, väznice, letiská. Sú to objekty z vysokým stupňom zabezpečenia. Perimetrické detektory sa inštalujú hlavne do objektov z vysokou dôležitosťou kvôli vysokej poriadovacej cene. Technológia ide stále dopredu tým pádom klesá cena starších modelov jednotlivých detektorov čo v dnešnej dobe má za následok, že sa tieto perimetrické detekčné systémy začínajú montovať aj do menších firiem a dokonca aj do rodinných domov.

Najčastejšie používané systémy pre perimetrickú ochranu sú:

- Stráženia plotov z plotového pletiva

Na pletivo plotu sa pripevní špeciálny detekčný kábel, ktorý prevádza mechanické namáhanie a záchvevy na elektrický signál, spracovávaný vyhodnocovacou jednotkou. Tá odfiltruje bežné rušenia a vyhlási poplach pri podliezaní, preliezaní alebo prestrihávaní plotu. Podmienkou pre použitie tejto signalizácie je dokonale vypnuté plotové pletivo.

Plané poplachy môže u tohto spôsobu zabezpečenia spôsobiť silný dážď, krupobitie, silný vietor a prítomnosť zveri.



Obr. 1 Stráženie plotov

➤ Infračervené závory

Infračervené závory sú umiestnené na pevne zabudovaných stĺpoch a vytvára medzi vysielacou a prijímacou jednotkou neviditeľný lúč alebo rad lúčov nad sebou. Pri prerušení lúča dôjde k poplachu. Vysielač s prijímačom musia byť umiestnené na priamu viditeľnosť, takže pri inštalácii infračervených závor pre stráženie pozemkov je nutné prihliadať k úpravám terénu a výsadbe rastlín.



Obr. 2 Infračervené závory

➤ Mikrovlnné bariéry

Rovnako ako u infračervenej závory tvorí mikrovlnnú bariéru vysielaciu a prijímaciu časť. Na rozdiel od závory však bariéra vytvára ucelené ochranné pole eliptického tvaru, ktorého rozmery a dosah sú dané konfiguráciou bariéry. Ochranné pole zaručuje veľmi kvalitné stráženie záujmového priestoru a u kvalitných mikrovlnných bariér je možné nastaviť veľkosť predmetu, na ktorý systém reaguje vyhlásením poplachu.

Mikrovlnné bariéry nájdu uplatnenie nielen pri ochrane pozemkov, ale môžu strážiť aj vstup na balkóny a terasy, preliezanie stien a vniknutie na ploché strechy objektov.

Aj tu je nutná priama viditeľnosť medzi vysielačom a prijímačom a v zabezpečenom koridore by nemali byť pohybujúce sa predmety, trávy, kríky alebo konáre stromov, ktoré by sa mohli stať zdrojom planých poplachov.



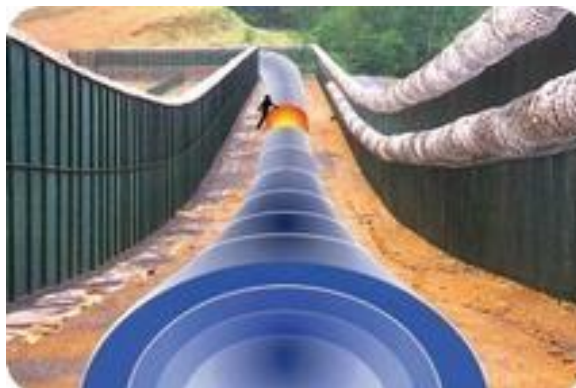
Obr. 3 Mikrovlnné bariéry

➤ Zemné detekčné káble

Zemné detekčné káble sú zrejme najspoľahlivejším ochranným systémom pre vonkajšie použitie. Bohužiaľ aj najdrahším.

V určitej hĺbke pod povrchom zeme je uložený špeciálny detekčný kábel, ktorý okolo seba vytvára niekoľko metrov široké detekčné pole a vyhodnocuje jeho zmeny. Rovnako ako u mikrovlnnej bariéry, aj tu sa dá nastaviť minimálna veľkosť objektu, ktorý vyvolá poplach.

Zemné káble majú celý rad výhod. Majú vysokú mieru spoľahlivosti, na rozdiel od ostatných ochranných systémov nie sú vidieť, plynulo kopírujú všetky výškové nerovnosti a strážený koridor sa nemusí skladať z priamok.[3]



Obr. 4 Zemné detekčné káble

➤ Mechanické zábranné systémy

Základom každej perimetrickej ochrany je jej ohraničenie. K tomu sa najčastejšie využívajú rôzne druhy plotov a plotových systémov. Pre vstup do objektov sa využívajú priechody cez ploty. Charakteristické priechody sú bránky, dvere a závory. Tieto mechanické časti taktiež patria k perimetrickej ochrane. Nad plotmi sa môžu nachádzať žiletkové systémy a ostnaté drôty. Naopak pod plotmi sa môžu nachádzať podhradové systémy.



Obr. 5 Žiletkový systém

➤ CCTV – systémy uzavretých televíznych okruhov

Problémom vonkajšieho zabezpečenia je veľké množstvo podnetov, na ktoré by mali senzory perimetrickej ochrany reagovať. Jedná sa hlavne o:

- Vlnenie trávnatého porastu
- Pohyb lístia, stromov a kríkov
- Vibrácie oplotenia vo vetre
- Prúdenie vzduchu
- Vietor
- Sneh a dážď
- Pohyb rôznych druhov zvery
- Dopravný ruch v blízkosti hranice pozemku

Tieto podnety, ktoré svojím charakterom približujú situáciu narušenia sa nedá nikdy úplne eliminovať. Preto sa z tohto dôvodu často kombinuje v perimetrickej ochrane použitie

CCTV. Jedná sa o systém kamerových a záznamových zariadení. CCTV sa môžu využívať vo vnútorných priestoroch aj vo vonkajších priestoroch. Rozdiel je v triedach prostredia.

- ACS – Systémy kontroly a riadenia vstupov

Tieto systémy sa inštalujú na vstupy do objektov, a interiérových priestorov. Tieto systémy nahrádzajú staré manuálne systémy kontroly a riadenia vstupov ako boli dochádzkové knihy, a kľúčové režimy s príslušnou dokumentáciou. ACS sú plne elektronické fungujú na princípe čipových kariet ktoré sa využívajú ako kľúče do miestností alebo ako dochádzkový systém cez terminál. Na každej čipovej karte sú presne špecifikované oprávnenia vstupov. Je to moderný a efektívny systém kontroly a riadenia vstupov.

2.1 Rozdelenie detektorov perimetrickej ochrany

Z hľadiska použitého fyzikálneho princípu činnosti môžeme detektory rozdeliť do troch skupín.

- Elektromechanické detektory
- Elektromagnetické detektory
- Elektroakustické detektory

2.1.1 Elektromechanické detektory

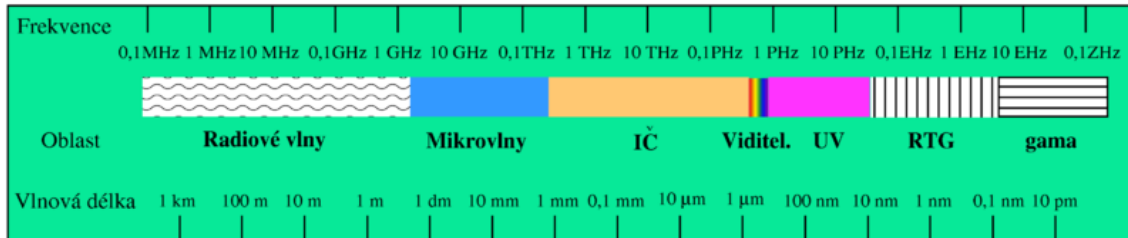
Najstaršie detekčné prvky v systéme technickej ochrany, naďalej však platný v perimetrickej ochrane. Tieto detektory fungujú na princípe vyhodnotenia zmeny mechanickej energie (fyzikálnej zmeny) a následnej premeny na elektrický poplachový signál. Patria sem magnetické kontakty, piezoelektrické detektory, tenzometrické detektory a seizmické detektory.

2.1.2 Elektromagnetické detektory

Tieto typy detektorov využívajú k svojej činnosti elektromagnetické vlny. Fyzikálna zmena spôsobená páchatelom je zosnímaná pomocou týchto vln a priamo v detektore premenená na elektrický poplachový signál.

2.1.2.1 Elektromagnetické žiarenie

Elektromagnetické žiarenie je kombinácia priečneho postupného vlnenia magnetického a elektrického poľa teda elektromagnetického poľa. Elektromagnetické spektrum zahŕňa elektromagnetické vlnenie o rôznych vlnových dĺžkach a rôznych frekvenciách. [4]



Obr. 6 Elektromagnetické spektrum

2.1.2.2 Dopplerov jav

Princíp dopplerovho javu je na základe zmeny vlnovej dĺžky elektromagnetických alebo akustických vln vyvolaná relatívnym pohybom zdroja a pozorovateľa. Ak je v jednom bode zdroj žiarenia s vyžarovanou konštantnou frekvenciou (vysielač) a prijímač, čím bližšie sa pohybuje objekt k zdroju žiarenia, tým vyššiu frekvenciu odrazeného signálu prijíma prijímač. V prípade, že sa objekt od zdroja žiarenia vzdďaľuje, frekvencia prijímaná prijímačom klesá. Intenzita odrazu sa mení v závislosti na veľkosti odrazovej plochy a materiálu, z ktorého je konštruovaná. Tento princíp sa používa v radaroch, prípadne sonaroch. [5]

2.1.3 Elektroakustické detektory

Elektroakustické detektory využívajú akustických vln. Detektory zosnímajú fyzikálnu zmenu spôsobenú páchatelom s pomocou týchto vln a prevedú ju na elektrický poplachový signál. Dá sa sem zaradiť mikrofónne káble alebo plotové systémy s funkciou takzvaného príposluchu. Táto funkcia umožňuje ostrahu počuť zvuky priamo v mieste poplachu. Elektroakustické detektory pre perimetrickú ochranu najčastejšie využívajú počujúce pásmo pre človeka, čo odpovedá 20 Hz až 20 kHz. [4]

Z hľadiska vyžarovania energie jednotlivých detektorov ich delíme na dve základné kategórie:

- Aktívne
- Pasívne

2.1.4 Aktívne detektory

Aktívne detektory zaisťujú charakteristické rysy nebezpečia s využitím určitej vyžarovanej energie (ultrazvuk, elektromagnetické vlny). V dôsledku tohto fyzikálneho javu dochádza k vytvoreniu detekčného priestoru takzvanej bariéry. Pri vstupe narušiteľa do tejto aktívnej detekčnej zóny a jeho pohybu v nej dôjde k špecifickým zmenám v prostredí. To má za následok vyhlásenie poplachu. Nevýhodou je ľahká detekcia stráženého priestoru. Taktiež môžu existovať mŕtve zóny. Je to priestor v ktorom nie je možné odhaliť páchateľa.

Patria sem:

- Štrbinové káble
- Kapacitné detektory
- Duálne detektory
- Mikrovlnné detektory a bariéry
- Infračervené závory a bariéry
- Zemné perimetrické systémy

2.1.4.1 Štrbinové káble

Tieto káble sú uložené v zemi v hĺbke približne 30 cm. Tieto koaxiálne káble sa ukladajú väčšinou v pároch. Káble na svojom tienení majú malé vzduchové štrbiny, ktoré umožňujú vyžarovať vysokofrekvenčný signál. Jeden z páru vysiela tieto vlny a druhý ich následne zachytáva. Vysielací kábel ktorý vytvára tento vysokofrekvenčný signál vyžaruje okolo seba elektromagnetické pole ktoré má eliptický tvar. Prijímací kábel následne tento signál prijíma a vyhodnocuje jeho zmeny. Pokiaľ príde k narušeniu tohto signálu zmení sa jeho charakteristika a prijímací kábel vyhodnotí poplach. Tieto káble sa dajú nastaviť k rozpoznávaniu rôznych veľkostí narušiteľov. Systém efektívne dokáže odfiltrovať falošné popluchy vyvolané zvieratami. Výhodou oproti všetkým bariéram a záclonám je

možnosť zabezpečenia perimetru členitých terénov či už z rôznymi výškami alebo smermi. Ďalšia výhoda je ich neviditeľnosť. Nevýhoda je ich poriadková cena a náklady na inštaláciu. V zimných obdobiach môže prísť k skresleniu elektromagnetického poľa čo ale efektívne vyvažuje prijímacia časť ktorá odfiltrávať určité nastavené odchýlky. Káble môžu mať spoločný obal a tým môžu vytvárať jeden celok. Tieto detektory môžu mať dĺžku jedného úseku až 200 metrov.



Obr. 7 Štrbinový kábel

2.1.4.2 Kapacitné detektory

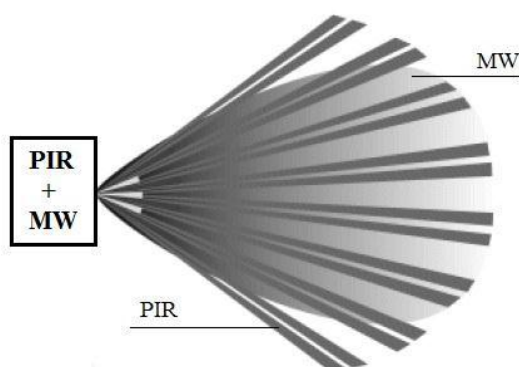
Detektory ktoré pracujú na princípe kondenzátora kde medzi dvoma elektródami vzniká elektrostatické pole. Dielektrikom je vzduch. Vložením akéhokolvek predmetu do elektrostatického poľa dochádza k jeho zmene. Kapacitné detektory sú využívané k ochrane predmetovej a perimetrickej ochrane.

Kapacitné káble detekujú zmeny elektrostatického poľa vytvoreného v okolí kábla. Systém vyhlási poplach, ak narušiteľ zmení kapacitu poľa priblížením sa, alebo dotykom s chráneným predmetom. Plotové detekčné systémy na báze kapacitných káblov sú zložené z troch káblov usporiadaných pod sebou a inštalovaných na plot. Do nich je privádzaný nízkonapäťový signál vytvárajúci elektrostatické pole, ktorého zmeny oproti zemi vyhodnocuje procesorová jednotka pripojená na EZS. Na rovnakom princípe pracujú aj interiérové kapacitné detektory.

System vyhodnocovania elektrostatického poľa môže byť umiestnený nielen nad, ale aj v okolí plota. Tento systém je charakteristický vysokým počtom falošných poplachov spôsobených pohybom plota pri nápore vetra, alebo pohybom drobných živočíchov v priestore okolo plota. Preto je vhodná kombinácia s kamerovým systémom. System je možné prekonať premostením, alebo podkopením elektrostatického poľa. [4]

2.1.4.3 Duálne detektory

Pri častom vzniku falošných poplachov je nutné zvoliť inú detekčnú technológiu. Inštaláciou duálnych detektorov obmedzíme falošné poplachu, a tým aj znížime náklady na fyzickú ostrahu. Zásahová jednotka nebude vychádzať zbytočne kvôli falošným poplachom. Duálne detektory majú integrované dve detekčné technológie. Najčastejšie sa jedná o kombináciu mikrovlnného detektoru a pasívneho infračerveného detektora. Jedná sa vlastne o zlúčenie aktívneho a pasívneho detektora. Obe detekčné technológie môžu pracovať v dvoch režimoch. Jednou možnosťou je spolupráca oboch technológií a vyhlásenie poplachu v okamžiku, kedy je zaznamenávaný poplach obomi detekčnými technológiami súčasne. V tomto prípade sa jedná o režim AND. V druhom režime pracuje každá detekčná technológia samostatne. V prípade zaznamenania pohybu páchatel'a aspoň jednou z detekčných technológií dôjde k vyhláseniu poplachu. Vtedy sa jedná o režim OR.



Obr. 8 Duálny detektor

2.1.4.4 Mikrovlnné detektory a bariéry

Jedná sa o líniové aktívne detektory. Mikrovlnné detektory k svojej činnosti využívajú mikrovlnné žiarenie a Dopplerovho javu. Zmenou kmitočtu dôjde k vyhláseniu poplachu. Aby sa nepriaznivo neovplyvňovali osoby a prístroje v blízkosti detektora, využívajú sa k detekcii len malé výkony. Aj keď pracujú mikrovlnné detektory s malým výkonom, detekcia je dostatočná. Dosahy týchto detektorov sa pohybujú od desiatok do stovky metrov. V podstate sa dá využiť mikrovlnné žiarenie v dvoch variantách. Ako mikrovlnné bariéry alebo detektore.

2.1.4.5 Infračervené závorý a bariéry

Infračervené bariéry patria k najrozšírenejším druhom vonkajších detektorov narušenia. Vysielač vysiela a prijímač prijíma infračervené lúče, ktorých prerušenie vyvolá poplachový stav. Dosah infračervených bariér a závor môže byť až 250 metrov. Efektívne rozmedzie je 100 až 150 metrov. Pre vyššiu odolnosť sú infračervené bariéry vybavené systémom chrániacich zariadenie pred zarosením optiky a poveternostným vplyvom. Podmienkou správneho fungovania infračervených bariér je odolnosť voči falošným poplachom spôsobených snežením, prebehnutím malých zvierat a podobne. Odolnosť voči falošným poplachom sa zvyšuje priamo úmerne s počtom lúčov vysielaných a prijímaných infračervenou bariérou. Pri poklese viditeľnosti spôsobenej napríklad hmlou by mala byť znížená citlivosť detekcie, aby nevznikali falošné poplchy. Vysielače a prijímače sa montujú na priamu viditeľnosť. Montáž na členitý kopcovitý terén je problematická.

2.1.5 Pasívne detektory

Detektory pasívne reagujú na fyzikálne zmeny v určitom prislúchajúcom prostredí. Na rozdiel od aktívnych detektorov nevyžarujú do priestoru žiadny signál. Obrovská výhoda týchto pasívnych detektorov je, že sú ťažko detekovateľné a majú nízke mesačné náklady.

Patria sem:

- Mikrofónne káble
- Diferenciálne tlakové detektory
- Pasívne infračervené detektory
- Plotové perimetrické systémy

2.1.5.1 Mikrofone káble

Ochrana dôležitých objektov s vysokým rizikom alebo objektov, na ktoré hrozí pri útoku vysoká škoda napríklad objekty osobitnej dôležitosti akými sú napríklad sklady hmotných rezerv štátu, sklady zbraní a streliva, medzinárodné letiská a podobne, je charakteristická použitím perimetrickej ochrany. Mikrofonické káble sa používajú na stráženie plotov takto dôležitých objektov. Výstupný signál z kábla má charakter nízkofrekvenčného signálu v akustickom frekvenčnom pásme, čo umožňuje po zosilnení pripojiť k vyhodnocovacej jednotke reproduktor pre akustický príposluch. Táto funkcia umožňuje obsluhu odhadnúť charakter vplyvov pôsobiacich na plot a tak odlíšiť falošné popluchy od skutočného narušenia v závislosti od akustickej charakteristiky prijatého signálu. Mikrofone káble sú upevnené na pletivo poprípade na steny pevných murovaných plotov. Pretože sú káble citlivé na mechanické deformácie, ľahko dokážu detekovať preliezanie, strihanie, podliezanie, rezanie plota. Vibrácie ktoré spôsobujú tieto techniky prekonávania plotov tvoria na mikrofonom káble deformácie a tým vzniká špecifický elektrický signál. Signál je privádzaný do vyhodnocovacieho procesora kde sa signál spracuje a výhodní ho. Procesor dokáže efektívne odfiltrávať falošné popluchy vzniknuté vplyvom počasia. Podmienkou detekcie sabotáže je ukončovací rezistor takzvaný terminátor.

2.1.5.2 Diferenciálne tlakové detektory

Tieto detektory sú určené pre perimetrickú ochranu stráženého priestoru. Jedná sa o hydraulické podzemné detektory tvorené paralelným uložením dvoch hadíc z pružného materiálu po obvodě chráneného priestoru. Hadice sú zvyčajne uložené v hĺbke 20 cm pod povrchom zemi a ukladajú sa do pieskového podložia. Hadice sú natlakované nemrznúcou kvapalinou a sú snímané a vyhodnocované rozdiely tlakových prejavov na ne pôsobiacich. Rozdiel tlakov je následne porovnávaný vo vyhodnocovacej jednotke takzvaného procesora a prevádzaný na impulz signalizujúci poplach. Výhodou je využívanie tlakových hadíc v členitom teréne.

2.1.5.3 Pasívne infračervené detektory

Pasívne infračervené detektory vyhodnocujú zmeny žiarenia dopadajúceho na detektor. Ak sa v zornom poli detektora pohybuje teleso s teplotou inou, akú má jeho okolie, detektor vyhodnotí zmeny a vyšle signál pre vyhlásenie poplachu. Princíp detektorov pre montáž do

vonkajšieho prostredia je podobný ako princíp detektorov pre použitie v interiéri. Dosah vonkajších PIR detektorov je 150 až 200 metrov. Tieto detektory sa používajú hlavne ako doplnok ku kamerovým systémom pre snímanie poplachového záznamu, monitoringu, alebo zameranie pozornosti operátora na danú oblasť.

3 FYZICKÁ OCHRANA

3.1 Expanzia súkromných bezpečnostných služieb

Kľúčové faktory rastu SBS:

- Vysoký počet oznámených trestných činov
- Verejnosť pociťuje vyššie ohrozenie kriminálnymi živlami
- Vysoké kozmické požiadavky kozmického programu USA
- Zvyšujúca sa hrozba demonštrácií, pumových útokov a únosov
- Rozvoj elektroniky a s tým spojená produkcia detektorov
- Zvyšujúci sa objem súkromného majetku
- Väčší dopyt po ochrane majetku a schopnosť platiť za nadštandard
- Znižujúci sa podiel štátnej polície vo vzťahu k ochrane osôb a majetku [6]

3.2 Strážna služba

3.2.1 Úvod

Hlavnou úlohou strážnych služieb je zabezpečiť pomocou statickej alebo pohybovej ostrahy objektu, respektíve monitorovacou ostrahou objektu, požadovaný stav zaistenia celkovej bezpečnosti objektu a plniť v tejto súvislosti aj ďalšie úlohy stanovené v zmluve zo zákazníkom (tj. Od zaistovania kontrolnej priepustkovej služby a ostatných kontrolných činností na pevných stanoviskách a obchádzkovej službe až po realizáciu najrôznejších bezpečnostných opatrení v chránenom objekte). [6]

Ochrana objektu je v obecnej rovine zabezpečovaná väčšinou kombináciou bezpečnostných opatrení, ktoré sú:

- Fyzická ostraha objektu
- Technické prostriedky ochrany objektu
- Režimové opatrenia

3.2.2 Fyzická ostraha objektu

Pod pojmom fyzická ostraha objektu rozumieme vyškolených pracovníkov súkromnej bezpečnostnej služby, ktorý za vykonávanú prácu dostávajú finančné ohodnotenie. Títo zamestnanci SBS vykonávajú viaceré činnosti stráženia objektov medzi ktoré patria:

- Statická ostraha objektov
- Pohyblivá ostraha objektov
- Monitorovacia ostraha objektov
- Bezpečnostné doprovody osôb a vozidiel
- Osobná ochrana
- Ostatné činnosti (zaist'ovanie bezpečnostných kurzov, bezpečnostné poradenstvo, bezpečnostné analýze, audity)

Rozsah ochrany, ktorú bude mať na starosti fyzická ostraha objektu si určuje zákazník. Tento rozsah musí byť súčasťou obchodnej zmluvy, ktorá je základnou listinou pri vykonávaní činností súkromných bezpečnostných služieb. V zmluve musia byť presne stanovené určité kritéria:

- Systém ochrany objektu
- Hlavné úlohy na jednotlivých stanovištiach
- Prieputkový režim
- Oprávnenia a povinnosti pracovníkov ostrahy
- Kľúčový režim
- Spôsob vyrozumenia zodpovedných pracovníkov vedenia objektu (pracovníkov zákazníka)
- Činnosť v zvláštnych prípadoch – pri vzniku mimoriadnych udalostí a živelných pohromách
- Oprávnenie konkrétne vymedzených pracovníkov zákazníka pri kontrole výkonu strážnych služieb na danom objekte

3.2.2.1 *Statická ostraha objektu*

Táto forma ostrahy vykonáva svoju prácu na presne stanovených pozíciách, ktoré si zadal zákazník vo svojich požiadavkách. Statická ostraha objektu môže pôsobiť na rovnom alebo vyvýšenom stanovišti z ktorého pokryje lepšie strážené územie. Statická ostraha má niekoľko hlavných úloh medzi ktoré patria:

- Kontrola vstupu automobilov a ľudí do stráženého objektu
- Zabezpečovanie kontroly vnášaných, vynášaných vecí a materiálov do stráženého objektu
- Vedenie knihy príchodov a odchodov
- Vedenie kľúčového režimu, vydávanie jednotlivých kľúčov oprávneným osobám a následné vedenie dokumentácie
- Sprevádzanie návštev

Statická ostraha a jej hlavné úlohy slúžia k efektívnemu fungovaniu firmy. Statická ostraha ďalej musí:

- Zabraňovať, rozkrádaniu, poškodzovaniu firmy a jej majetku
- Vyhodnocovať signalizáciu na pultoch centralizovanej ochrany a prostriedkov PZTS
- Robiť následné výjazdy na miesta signalizácie
- Rozpoznávať a odhadovať nebezpečia pri haváriách a iných mimoriadnych udalostiach

3.2.2.2 *Pohyblivá ostraha objektu*

Táto forma ostrahy objektu pôsobí v celom areály podniku alebo v jeho určitej časti. Pohyblivá ostraha objektu sa presúva medzi jednotlivými pevnými stanovišťami a tým dopĺňajú funkciu statickej ostrahy. Pohyblivá ostraha objektu je realizovaná hlavne v miestach z veľkou členitosťou podniku ako sú budovy a stroje. Táto fyzická ostraha má rovnaké povinnosti ako statická ostraha objektu. Mimo tieto povinnosti majú za úlohu:

- Znemožňovať vstupu osôb a vozidiel mimo miesta určené pre vjazd a výjazd
- Realizovať dohodnuté bezpečnostné opatrenia na určitých miestach objektu

- Ako prvý reagovať na príčiny signalizácie PPC a PZTS
- Informovať pomocou vysielacky o nežiaducom stave v objekte PPC

3.2.2.3 Monitorovacia ostraha objektu

Pracovníci monitorovacej ostrahy tvoria ochranu veľkého množstva objektov bez toho aby v nich trvalo hliadkovali. Nie vo všetkých strážených objektoch sa nachádza stanovisko ostrahy. Chránený objekt pracovníci monitorovacej služby navštevujú iba ako mobilné hliadky ale pešie hliadky, a to v časoch určených alebo dohodnutých so zákazníkom alebo v prípade vzniku poplachového stavu vyvolaného prostriedkami PZTS alebo inými kontrolnými prostriedkami inštalovanými v chránenom objekte. Signalizácia týchto prostriedkov je vyvedená na trvalom obsadenom mieste – monitorovacie centrum napríklad poplachové prijímacie centrá, z ktorého je objekt trvalo monitorovaný a odkiaľ je zaisťovaný výjazd pracovníkov hliadkovacej služby do ohrozeného objektu.

Vybudovaný monitorovací systém teda umožňuje systematicky sledovať aktuálny stav všetkých poplachových či iných technologických systémov, ktoré sú v chránenom objekte inštalované. Monitorovacia ostraha objektov je priebežne spojená s výjazdom zásahového vozidla, ktorého posádka zaisťuje včasnú reakciu na prípadné poplachy či iné signály a prevádza zásah na mieste.

3.2.2.4 Bezpečnostné doprovody osôb a vozidiel

Pracovníci hliadkovacích služieb sprevádzajú taktiež bezpečnostné doprovody súvisiace prevažne s prevozmi finančných hotovostí či iných cenností, ktoré sú prepravované pracovníkmi zákazníka. Hliadkovacia služba v tejto súvislosti poskytuje asistenciu a zaisťuje bezpečnosť prevádzanej akcie. Bezpečnostné doprovody tak predstavujú jednu z foriem súkromnej bezpečnostnej činnosti, v jej rámci zaisťovaná ochrana majetku a osôb pri ich presunoch či prevozoch. Jedná sa vlastne o špecifickú formu kontrolnej činnosti, ktorá má zaisťovať bezpečnosť dopresádzaného majetku a osôb a ich cieľom je zabezpečiť, aby nenastal niektorý z nežiaducich stavov. To znamená aby nedošlo pri preprave k ohrozeniu či porušeniu bezpečnosti prepravovaného majetku či osôb.

Bezpečnostný doprovod je zaisťovaný buď ako osobná ochrana jednotlivcov alebo skupiny, a to pešo, vozidlom alebo iným dopravným prostriedkom.

Pred vlastnou realizáciou bezpečnostného doprovodu je veľmi dôležité, aby hliadkovacou službou boli ocenené všetky bezpečnostné rizika spojené s týmto bezpečnostným doprovodom, vzhľadom k cieľom prepravy, dôvodov doprovodu, celkovej trase a ostatným aspektom. Musí byť vyhodnotená celá trasa, po ktorej bude bezpečnostný doprovod prevádzaný, charakter a počet odprevádzaných osôb a ďalšie bezpečnostné hľadiska činností, ktoré by mali byť v priebehu bezpečnostného doprovodu prevádzané. Na základe vyhodnotenia všetkých uvedených skutočností je následne určené akým spôsobom bude bezpečnostný doprovod prevedený, aký počet osôb ju bude zaisťovať, aké prostriedky budú k jeho zabezpečeniu použité. Hlavnou úlohou pracovníkov odprevádzanej služby je aby odprevádzaná osoba alebo zásielka bola na mieste doručenia včas a bezpečne. [6]

3.2.3 Technické prostriedky ochrany objektu

Technické prostriedky ochrany objektu sú rozoberané v prvej kapitole teoretickej časti. Do technických prostriedkov ochrany objektu patrí viac ako len perimetrická ochrana. Patria sem:

- PZTS – Poplachové zabezpečovacie a tiesňové systémy
- CCTV – Uzatvorené kamerové okruhy
- MZS – Mechanické zábranné systémy
- EPS – Elektronická požiarna signalizácia
- PPC – Poplachové a prijímacie centra
- ACCESS – Systémy kontroly a riadenia vstupov

3.2.4 Režimové opatrenia

Režimové opatrenia predstavujú stanovený súbor procedúr, ktoré zahŕňujú režim vstupu a výstupu osôb, vjazdu a výjazdu dopravných prostriedkov, režim pohybu osôb, dopravných prostriedkov a chránených informácií v objekte a jeho jednotlivých častiach v pracovnej a mimopracovnej dobe, režim manipulácie s kľúčmi, identifikačnými prostriedkami a médiami, ktoré sa používajú pre systémy zabezpečenia vstupov, režim manipulácie s technickými prostriedkami a jej ich využívaním. Režimové opatrenia sú pravidla popísané v prevádzkovom nariadení objektu, zaväzujúcim všetky osoby, ktoré sú oprávnené vstupovať do objektu.

Vedľa iných náležitostí obsahujúcich režimové opatrenia aj zoznamy osôb oprávnených vstupovať do ochránených priestorov objektu, zoznam dopravných prostriedkov oprávnených vchádzať do objektu, spôsob kontroly preukazovania oprávnenosti k vstupu alebo vjazdu do objektu. V súvislosti so zaisťovaním režimových opatrení sú riešené aj otázky, ktoré sa týkajú všetkých procedúr kľúčového režimu.

V teoretickej časti tejto práce boli popísané a rozčlenené základné princípy perimetrických detekčných systémov a fyzickej ochrany. Tieto informácie o jednotlivých druhov zabezpečenia perimetru predchádzali praktickej časti, kde budú následne komparované a vyhodnocované SWOT analýzou ich výhody a nevýhody.

II. PRAKTICKÁ ČASŤ

4 ÚVOD

Zabezpečenie perimetrie v objekte sa dá rôznymi spôsobmi, preto v praktickej časti tejto práce budú jednotlivé spôsoby zabezpečenia komparované. Pomocou SWOT analýzy sa budú hľadať ich hlavné výhody a nevýhody. Ďalej budú spracovávané ich možné hrozby a príležitosti. Výsledkom praktickej časti bude zhrnutie všetkých predností a nedostatkov jednotlivých druhov perimetrickej ochrany v praktickej tabuľke, ktorá môže slúžiť ako nástroj pri výbere zabezpečenia perimetru.

5 SWOT ANALÝZA

Pre komparáciu efektívnosti využitia fyzickej ostrahy a perimetrických detekčných systémov pre potreby perimetrickej ochrany je možné využiť SWOT analýzu. Jedná sa o základnú metódu marketingového plánovania. Táto analýza poukazuje na štyri dôležité aspekty, ktoré sú potrebné k najefektívnejšiemu definovaniu potrieb zákazníka. Aspekty vyplývajú už z názvu analýzy, avšak sú to začiatkové písmena anglických slov.

S – strength (silné stránky)

W – weaknesses (slabé stránky)

O – opportunities (príležitosti)

T – threats (hrozby)

Úspešná aplikácia vhodného zabezpečenia objektu vychádza hlavne z kvalitne vypracovaného bezpečnostného posúdenia objektu. Pri porovnávaní fyzickej ostrahy a perimetrických detekčných systémov treba zhodnotiť silné a slabé stránky jednotlivých druhov perimetrickej ochrany (S-W). Taktiež treba identifikovať vhodné príležitosti a hrozby (O-T).

Cieľom úspešného zabezpečenia objektu by malo byť obmedzenie slabých stránok jednotlivých druhov zabezpečenia a naopak tieto nedostatky doplniť kombináciou ich silných stránok. Využívanie príležitostí okolí a snažiť sa predvídať hrozby sú záležitosti veľa krát vyplývajúce z bezpečnostného posúdenia.

5.1 História

SWOT analýza vznikla v Stanforde, vo výskumnom ústave v rámci výskumu v rokoch 1960-1970. Cieľom výskumu bolo zistiť príčinu neúspešného firemného plánovania. Samotnú SWOT analýzu vymyslel Albert Humphrey (1926-2005), ktorý projekt a päťčlenný tím výskumníkov viedol. Behom výskumného projektu boli aplikované dáta od 500 najvýznamnejších amerických spoločností (podľa „Fortune 500“, klasifikácia 500 najlepších spoločností v USA podľa hrubého príjmu). Neskorej Humphrey pôsobil ako konzultant v viacej než 100 spoločnostiach, napríklad v USA, Veľkej Británii, Nemecku, Dánsku, Nórsku alebo Mexiku. Albert Humphrey zomrel 31. 10. 2005.

5.2 SWOT MATICA

Pri SWOT analýze sa analyzujú faktore interné, teda silné a slabé stránky, a faktory externé teda príležitosti a ohrozenie. Jednotlivé faktory sa dajú usporiadať do takzvanej SWOT matice. Tato matica predstavuje koncepčný rámec pre systematickú analýzu a uľahčuje chápanie a porovnávanie informácií. Výstupom matice sú 4 typy stratégie.

SWOT-analýza		Interní analýza	
		Silné stránky	Slabé stránky
E x t e r n í a n a l ý z a	Príležitosti	<i>S-O-Strategie:</i> Vývoj nových metod, které jsou vhodné pro rozvoj silných stránek společnosti (projektu).	<i>W-O-Strategie:</i> Odstranění slabín pro vznik nových příležitostí.
	Hrozby	<i>S-T-Strategie:</i> Použití silných stránek pro zamezení hrozeb.	<i>W-T-Strategie:</i> Vývoj strategií, díky nimž je možné omezit hrozby, ohrožující naše slabé stránky.

Obr. 9 SWOT matica

5.2.1 Analýza S-W

Táto analýza skúma interné vplyvy teda silné a slabé stránky komparujúcich druhov ochrany. Definuje taktiež vnútorné predpoklady pre zhodnotenie príležitostí a odvrátenie hrozieb vonkajšieho prostredia. Tento rozbor by mal byť tvorený pred samotnou realizáciou zabezpečenia ale aj v určitých intervaloch podľa nej. Intervale nových rozborov by sa mohli dať definovať podľa stupňa zabezpečenia objektu. To znamená, že pokiaľ sa jedná o stupne zabezpečenia jedna a dva čo sú stupne s nízkym a nízkym až stredným rizikom bude interval nových rozborov a analýz v dlhšom časovom intervale. SWOT analýza je časovo a finančne náročná a pri týchto stupňoch zabezpečenia by náklady na túto analýzu boli nepriamo úmerné z celkovým zabezpečením objektu. Pri stupňoch zabezpečenia tri a štyri čo sú stupne zo stredným až vysokým a vysokým rizikom je táto analýza veľmi efektívna a mala by sa vykonávať v určitých časových intervaloch. Pri týchto stupňoch zabezpečenia je efektivita z finančného a časového hľadiska priamo

úmerná celkovému zabezpečeniu. Medzi vnútorné vplyvy, ktoré sú treba analyzovať napríklad patrí:

- Vybavenosť, opotrebovanie prístrojov, druh materiálov
- Ľudské zdroje, motivácia zamestnancov
- Finančné zdroje, image podniku
- Dobrá organizácia práce
- Prepojenosť systémov
- Záložné zdroje

5.2.2 Analýza O-T

Cieľom je maximálne využiť príležitostí a eliminovať hrozby. Jedná sa o externé vplyvy ktoré často krát nemožno ovplyvniť. Treba ich však predvídať. Treba sledovať štatistiky kriminality na danom území ktoré pravidelne vypisuje ministerstvo vnútra v spolupráci z policajnými zložkami štátu. Taktiež treba sledovať nové trendy vývoj a inovácie ktoré prinášajú jednotliví výrobcovia perimetrických detekčných systémov. U fyzickej ostrahy sa jedná skorej o sledovanie nových donucovacích prostriedkov, rôznych druhov školení, celková výstroj a výzbroj. Medzi vonkajšie vplyvy môžeme taktiež zahrnúť konkurenciu a dodávateľov. Každý objekt ktorý sa pripravuje na zabezpečenie perimetrie by mal najskorej eliminovať svoje vnútorné hrozby, nedostatky ako sú napríklad diery v plotoch, slabo upevnené pevné časti plotov stojky a podobne.

5.3 Trvalá prevádzka

Pod pojmom trvalá prevádzka sa označuje doba, ktorá začína plynúť okamžikom uvedenia poplachového a zabezpečovacieho systému do prevádzky. Pretože tento stav je už reálne a funkčné zabezpečenie objektu preto je vhodné ako kritérium pri vytvorení SWOT analýze. Trvalá prevádzka patrí k poslednej časti pri realizácii projektu na poplachové zabezpečovacie a tiesňové systémy. Hlavnou náplňou tejto etapy je realizácia:

- Pravidelná údržba
- Pravidelná kontrola
- Servisné zásahy podľa potreby

- Funkčné skúšky
- Pravidelné revízie

Pravidelná kontrola prevádza ju väčšinou servisná organizácia ale po dodatočnom zazmluvnení ju môže realizovať aj fyzická ostraha. Táto kontrola je len vizuálna preto ju môže realizovať fyzická ostraha pri svojich pravidelných obchádzkach stráženého objektu.

Pravidelná údržba obsahuje prehliadku a zároveň aj funkčnú skúšku. Túto údržbu realizuje spravidla firma ktorá systém do objektu inštalovala. Časové intervaly údržby sa odvíjajú od stupňa zabezpečenia stráženého objektu. Pri každej funkčnej skúške sa musí previesť záznam do prevádzkovej knihy. [7]

5.3.1 Perimetrické detekčné systémy

Všetky systémy PZTS ako aj perimetrické detekčné systémy potrebujú určitý servis a pravidelnú kontrolu. Podľa stupňa zabezpečenia sú doporučené nasledovné intervaly funkčných skúšok.

p.č.	Činnosť	interval / stupeň zabezpečení		
		3 měsíce	6 měsíců	12 měsíců
1.	Řídící vstupy od ostatních aplikací/ výstupy využívané ostatními aplikacemi.	4	3	1,2
2.	Jeden detektor zapojený do smyčky, popř. jedna adresa detektoru.		3	1,2
3.	Výstražná zařízení (vnější i vnitřní).	4	3	1,2
4.	Funkční zkouška ústředny (podle návodu výrobce).		3	1,2
5.	Zkouška funkce náhradního napájecího zdroje (v klidovém stavu a při signalizaci poplachu).	4	3	1,2
6.	Přenos stavů na PPC nebo do nadstavbového systému	4	3	1,2

Obr. 10 Doporučené lehoty funkčných skúšok [14] (upravil Valouch, 2012)

Ďalej perimetrické detekčné systémy potrebujú byť nejakým spôsobom napájané. Sú tri možnosti ako PZTS napájať.

Typ A: Energia je dodávaná z vonkajšieho zdroja a v prípade jeho výpadku je energia dodávaná z dobíjacieho náhradného zdroja (akumulátor), ktorý je automaticky dobíjaný z vonkajšieho zdroja energie.

Typ B: Energia je dodávaná z vonkajšieho zdroja a v prípade výpadku je energia dodávaná z dobíjacieho zdroja (lithiová batéria) ktorý nie je automaticky dobíjaný z vonkajšieho zdroja.

Typ C: Energia je dodávaná iba z náhradného zdroja, ktorý je v tomto prípade základným zdrojom energie (batéria).

Záložný zdroj je zdrojom elektrickej energie. Tento zdroj v prípade výpadku elektrickej siete dokáže nahradiť túto sieť a zabezpečiť nepretržitý prívod elektrickej energie do napájania perimetrického detekčného systému.

Pokiaľ niektorý z typov napájania zlyhá systém sa stáva nefunkčný a celý priestor je nestrážený. Náhradné zdroje a ich výkonnosť musí byť pravidelne kontrolovaná. Doba napájania pomocou náhradného napájacieho zdroja je stanovená podľa stupňa zabezpečenia.

	Stupeň 1	Stupeň 2	Stupeň 3	Stupeň 4
Typ A	12	12	60	60
Typ B	24	24	120	120

Obr. 11 Minimálna doba napájania náhradným napájacím zdrojom

Pokiaľ všetky vyššie uvedené veci fungujú správne perimetrické detekčné systémy sú veľmi spoľahlivé. Dokážu presne reagovať pri napadnutí objektu. Tieto systémy môžu pracovať 24 hodín v kuse. Jedná sa len o dodatočného nastavenia podľa potrieb zákazníka a následné zastrešovanie a odstrešovanie systému.

5.3.2 Fyzická ostraha

Hlavnou úlohou strážnych služieb je zabezpečiť pomocou statickej alebo pohybovej ostrahy objektu, respektíve monitorovacou ostrahou objektu, požadovaný stav zaistenia celkovej bezpečnosti objektu a plniť v tejto súvislosti aj ďalšie úlohy stanovené v zmluve zo zákazníkom (tj. Od zaist'ovania kontrolnej priepustkovej služby a ostatných kontrolných činností na pevných stanoviskách a obchádzkovej službe až po realizáciu najrôznejších bezpečnostných opatrení v chránenom objekte). [6]

Fyzická ostraha je jednou z častí SWOT analýze. Treba pripomenúť jej hlavné úlohy a rozčlenenie ktoré sú charakteristické pre fyzickú ostrahu. Ich hlavnou úlohou je ochrana

osôb a majetku podľa pokynov zákazníka. Zákazník si pokyny a priority určuje sám. Avšak firma ktorá bude fyzickú ostrahu vykonávať môže zákazníkovi ponúknuť poradenstvo, na základne ich doterajších skúseností.

Statická ostraha objektu

Táto forma ostrahy vykonáva svoju prácu na presne stanovených pozíciách, ktoré si zadal zákazník vo svojich požiadavkách. Statická ostraha objektu môže pôsobiť na rovnom alebo vyvýšenom stanovišti z ktorého pokryje lepšie strážené územie. Statická ostraha má niekoľko hlavných úloh medzi ktoré patria:

- Kontrola vstupu automobilov a ľudí do stráženého objektu
- Zabezpečovanie kontroly vnášaných, vynášaných vecí a materiálov do stráženého objektu
- Vedenie knihy príchodov a odchodov
- Vedenie kľúčového režimu, vydávanie jednotlivých kľúčov oprávneným osobám a následné vedenie dokumentácie
- Sprevádzanie návštev

Statická ostraha a jej hlavné úlohy slúžia k efektívnemu fungovaniu firmy. Statická ostraha ďalej musí:

- Zabraňovať, rozkrádaniu, poškodzovaniu firmy a jej majetku
- Vyhodnocovať signalizáciu na pultoch centralizovanej ochrany a prostriedkov PZTS
- Robiť následné výjazdy na miesta signalizácie
- Rozpoznávať a odhadovať nebezpečia pri haváriách a iných mimoriadnych udalostiach

Pohyblivá ostraha objektu

Táto forma ostrahy objektu pôsobí v celom areály podniku alebo v jeho určitej časti. Pohyblivá ostraha objektu sa presúva medzi jednotlivými pevnými stanovišťami a tým dopĺňajú funkciu statickej ostrahy. Pohyblivá ostraha objektu je realizovaná hlavne v miestach z veľkou členitosťou podniku ako sú budovy a stroje. Táto fyzická ostraha má rovnaké povinnosti ako statická ostraha objektu. Mimo tieto povinnosti majú za úlohu:

- Znemožňovať vstupu osôb a vozidiel mimo miesta určené pre vjazd a výjazd
- Realizovať dohodnuté bezpečnostné opatrenia na určitých miestach objektu
- Ako prvý reagovať na príčiny signalizácie PPC a PZTS
- Informovať pomocou vysielacky o nežiaducom stave v objekte PPC

Tieto úlohy fyzickej ostrahy sú väčšinou možné realizovať len za pomoci vytvorenia tímu fyzickej ostrahy aby dochádzalo k efektívnemu pokrytiu celého objektu. Keďže fyzickú ostrahu robia ľudia nie je možné aby jedna a tá istá osoba vykonávala službu 24 hodín denne. Musia sa v pravidelných intervaloch meniť smeny. Fyzická ostraha nevyžaduje pravidelný servis ako PDS. Fyzická ostraha musí v pravidelných intervaloch absolvovať preškolenia ich spôsobilosti.

5.3.3 SWOT analýza trvalej prevádzky

Silné stránky perimetrických detekčných systémov

Sú hlavne ich rovnakej výkonnosti počas celej doby zastreženia objektu niekoľko rokov pri pravidelnom servisovaní, kontrolovaní a prevádzaním funkčných skúšok. PDS nepotrebujú žiadne menenie smien, teda nedochádza k výpadkom stráženia objektu. PDS okrem spotrebovanej energie nevyžadujú žiadne iné mesačné náklady. PDS pri sabotáži systému páchatelom väčšinou vyšlú signál do ústredne, ktorá následne vyhlási poplach.

Slabé stránky perimetrických detekčných systémov

Sú ich neustále napájanie elektrickou energiou. Náklady, ktoré musia byť vynaložené na ich servis, kontrolu a prevádzanie funkčných skúšok sú vysoké. PDS dokážu strážiť len oblasť na ktorú sú nasmerované preto ich umiestenie je veľmi dôležité zvážiť. Tieto systémy dokážu len detekovať napadnutie avšak nedokážu páchatel'a zastaviť a zneškodniť.

Silné stránky fyzickej ostrahy.

Fyzická ostraha dokáže vizuálne detekovať strážený objekt a intuitívne vyhodnocovať napadnutie. Pokiaľ má fyzická ostraha vybavenie na ochranu objektu lepšiu ako páchatel' dokáže nie len spustiť poplach ale aj páchatel'a v jeho činnosti zastaviť a tým eliminovať vzniknuté škody. Zastavenie páchatel'a v protiprávnej činnosti spôsobí prerušenie jeho vandalizmu poškodovania cudzej veci a následnej krádeže.

Slabé stránky fyzickej ostrahy

Fyzickú ostrahu zabezpečujú ľudia, ktorý túto prácu vykonávajú za účelom zisku. Keďže fyzickú ostrahu väčšinou vykonáva tím a musia sa striedať behom dňa na smeny ich finančné náklady sú vysoké. Fyzická ostraha sa môže dať uplatiť čo u PDS nie je možné.

Hrozby perimetrických detekčných systémov

Najväčšou hrozbou u perimetrických detekčných systémov je dlhodobé vypadnutie energie, ztráta signálu pri bezdrôtových systémov. Málo ale predsa predvídateľná hrozba je sabotáž systému pri jeho samotnej inštalácii. Firma, ktorá systém inštaluje do objektu si môže do objektu nechať nejakú nestráženu cestičku. Môže to byť priamo v teréne alebo v nastaveniach ústredne.

Hrozby fyzickej ostrahy

Najväčšia hrozba pre fyzickú ostrahu spočíva v jej sabotáži. Vysoké finančné ohodnotenie za sprístupnenie objektu páchatel'ovi je veľmi časté. Taktiež je možnosť fyzickú ostrahu citovo vydierať. Citové vydieranie spočíva v tom, že páchatel' drží jeho najbližšiu rodinu ako rukojemníkov a pod podmienkou ublíženia na zdravý donúti fyzickú ostrahu k sprístupnení do objektu.

Príležitosti perimetrických detekčných systémov

Príležitosti pre PDS je sledovanie vývojových trendov a ich následná aktualizácia zabezpečenia. Zastarané systémy sú často krát prekonané preto je potrebné ich pravidelné obnovenie. U PDS sa dlhodobé výpadky energií dajú zabezpečiť naftovými generátormi. Tieto generátore fungujú ako záložné zdroje. Tento druh napájania je nutné využívať hlavne u PDS ktoré spolupracujú z CCTV, nakoľko odber týchto zariadení je veľmi vysoký.

Príležitosti fyzickej ostrahy

Taktiež u fyzickej ostrahy treba sledovať vývojové trendy. Jedná sa hlavne o výstroj a výzbroj. Fyzická ostraha musí byť v neustálej výbornej fyzickej kondícii preto im treba zabezpečiť možnosť trénovať a následne vykonávať fyzické a psychické previerky.

5.3.4 Tabuľka SWOT analýzy

Tieto dve tabuľky SWOT analýzy sú výsledkom predchádzajúcej podkapitoly z názvom SWOT analýza trvalej prevádzky. V tabuľke sú popísané stručné charakteristiky jednotlivých systémov.

SWOT analýza PDS	
Silné stránky	Slabé stránky
stála výkonnosť nízke mesačné náklady Detekovateľnosť pri sabotáži	napájanie elektrickou en. jednorazové náklady na servis smerovanosť detektorov nemožnosť zneškodniť páchatel'a
Príležitosti	Hrozby
Nové trendy Spolupráca zo CCTV a následná vizuálna detekcia záložné generátore	výpadky elektrickej en. Strata signálu Sabotáž systému pri inštalácii

Tabuľka 1. Analýza PDS

SWOT analýza Fyzickej ostrahy	
Silné stránky	Slabé stránky
intuitívne vyhodnocovanie vizuálna detekcia zneškodenie páchatel'a	mesačné mzdy uplatenie
Príležitosti	Hrozby
nové trendy vo výzbroji a výstroji	citové vydieranie slabá vybavenosť vo výzbroji a výstroji fyzická zdatnosť nad páchatel'om

Tabuľka 2. Analýza fyzickej ostrahy

Z tejto analýzy jasne vyplýva, že najvhodnejšie zabezpečenie celého perimetru objektu je kombinácia týchto dvoch systémov. Tam kde zlyhávajú perimetrické detekčné systémy tam napreduje fyzická ostraha. Pokiaľ je objekt strážený len PDS je nutné pri každom vyhlásení poplachu vyslať pomocou poplachového prijímacieho centra zásahovú skupinu, ktorá musí preveriť každý poplach či už sa jedná o reálne vniknutie alebo len o falošný poplach. Naopak pokiaľ sa bude v objekte nachádzať len fyzická ostraha či už statická alebo

pohyblivá nie je možné u veľkých objektov sledovať ich perimenter po celej dĺžke. Tým fyzickej ostrahy by musel byť rádovo v stovkách zamestnancov. Preto je najefektívnejšia kombinácia týchto systémov. Perimetrické detekčné systémy dokážu sledovať celú dĺžku perimetru permanentne. Dokážu taktiež hlásiť približné miesto napadnutia záleží od použitého typu detektora. Fyzická ostraha môže preto okamžite prísť presne na miesto páchania trestnej činnosti nemusí prehľadávať celú oblasť.

6 VÝVOJOVÉ TRENDY

Ako v každej oblasti PZTS aj u perimetrických detekčných systémov nastávajú pokroky a vývoj týchto zariadení ide stále dopredu. PDS sa inštalujú do vonkajšieho prostredia kde sa nachádzajú veľké vplyvy rušenia ako sú poveternostné podmienky ktoré sa neustále menia, slnečné žiarenie, dážď, sneh, teplotné rozdiely, odolná doprava, zver toto všetko musia perimetrické detekčné systémy efektívne odfiltrávať. Vývojári týchto systémov neustále zdokonaľujú a vymýšľajú nové algoritmy aby následne odfiltrávali tieto falošné poplachy. Okrem nových zdokonalených algoritmov sa objavujú na trhu aj nové typy detektorov medzi ktoré patrí PerimetrLocator.

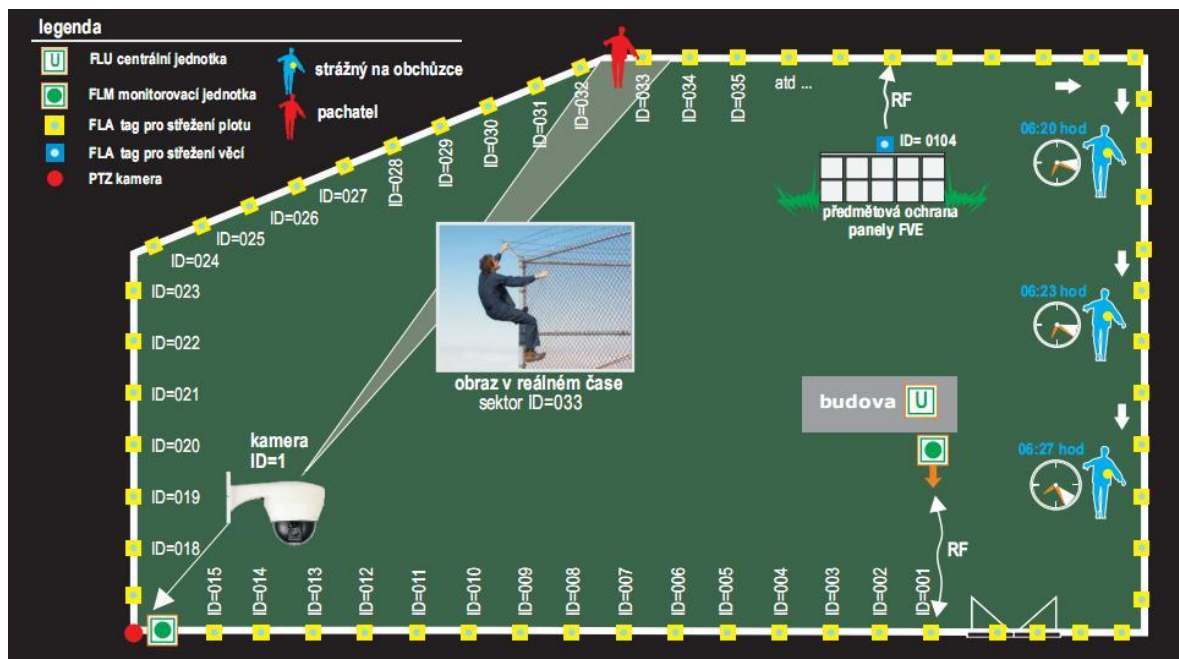
Tento bezdrôtový perimetrický systém je najvhodnejším systémom, ktorý vyplýva z realizovanej SWOT analýzy z kapitoly 5.3 Trvalá prevádzka.

Je to bezdrôtový perimetrický systém zaisťujúci stráženie plotu pomocou špeciálnych akceleračných RFID (Radio Frequency Identification) tagov, ktoré sú upevnené na pletive a dverách. Akceleračné RFID tagy nepotrebujú k svojej činnosti napájanie a ich životnosť sa pohybuje okolo 10-15 rokov. Tento systém nevyžaduje vôbec žiadnu kabeláž, inštalácia je ľahká, rýchla, a hlavne nenákladná. Systém je vhodný pre všetky typy plotov a dverí, má vysokú odolnosť proti rušeniu a nemá žiadnu z nevýhod konvenčných (káblových) perimetrických systémov. Systém sa dá taktiež realizovať ako predmetová ochrana objektov vo vnútri perimetru s využitím akceleračných RFID tagov FLB. PerimetrLocator komunikuje zo všetkými typmi ústredien a umožňuje úplne presné smerovanie kamier na miesto incidentu s presnosťou +/- 2 m a taktiež bezkontaktnú kontrolu obchádzkovej činnosti strážnych po celom perimetre. [9]

6.1 Princíp RFID tagu

RFID tagy perimetrickej ochrany snímajú časové a dynamicke zmeny svojej polohy, teda polohy pletiva, na ktorom sú upevnené, a ktoré sú typické pre preliezanie plotov narušiteľom. Vďaka tomu, že sa signály zo všetkých RFID tagov spracovávajú paralelne, perimetrický systém eliminuje plané poplachy, vzniknuté pôsobením vetra, dažďa, krupobitím alebo blízkej dopravy na pletivo, pretože takto vyvolané zmeny pôsobia v jednom okamžiku na viacej než jeden RFID tag súčasne. RFID tagy sa vďaka premyslenej analýze pohybu neustále automaticky kalibrujú a prispôbujú sa tak zmenám

v jednotlivéj mechanickej kvalite jednotlivých dielcov plotu (napr. Uvoľnenie závesu plotu). Detektory FLA obsahujú sofistikovaný algoritmus analýzy pohybu vo troch osách, ktorý umožňuje detekovať akúkoľvek snahu o sabotáž detektoru, a to aj v dennom DisArm režime. Tento systém teda vie vyhlásiť sabotážny poplach pri pokuse o odmontovaní tagu alebo časti pletiva vrátane RFID tagu a to aj v dobe, počas ktorej nie je perimetrická ochrana v režime zastreženia. Jednotky ďalej obsahujú optický tampér s detekciou odstránenia jednotky z montážnej podložky alebo navrtania kritu narušiteľom. [9]



Obr. 12 inštalácia RFID akcelerátorov v objekte

ZÁVER

Perimetrická ochrana je jednou z najnáročnejších častí zabezpečovacej techniky. Veľmi dôležitá je príprava pred samotnou inštaláciou. Bezpečnostné posúdenie objektu a následný výber vhodných prvkov perimetrických detekčných systémov je dôležitou súčasťou efektívneho a spoľahlivého zabezpečenia. Treba brať do úvahy pokyny výrobcov ktoré sú udávané v návodoch.

Zo SWOT analýzy, ktorá bola súčasťou tejto bakalárskej práce podrobne rozoberaná v praktickej časti vyplynulo, že najefektívnejšie zabezpečenie perimetru objektu nie je použitie perimetrických detekčných systémov ani fyzickej ostrahy ale ich kombinácia. Z analýzy jasne vyplýva, že tam, kde má jeden systém ochrany nedostatky, druhý systém dokáže efektívne tieto nedostatky eliminovať.

Vývojové trendy ktoré boli taktiež popísané v praktickej časti ukazujú veľký pokrok v oblasti perimetrických detekčných systémov. Jedná sa o efektívny systém ktorý dokáže spolupracovať z kamerovými systémami. Poukazuje na možné napadnutie a tým sa môžu kamerové systémy zamerať na danú oblasť natočiť objektív poprípade priblížiť priestor, kde vyhlasuje akceleračný RFID tag možné napadnutie. Zo SWOT analýzy vyplynulo, že tento systém efektívne nahrádza väčšinu nedostatkov perimetrických detekčných systémov a nedostatkov fyzickej ostrahy.

Veľkým nedostatkom v Českej republike je legislatívne prostredie ktoré nenapomáha súkromným bezpečnostným službám. Tie sa musia opierať o trestný zákonník a živnostenský zákon. V podstate týto ľudia majú rovnaké právomoci ako všetci ostatný čo veľa krát zneužívajú páchatelia pri krádežiach v obchodných domov. Pripravovaný zákon o súkromných bezpečnostných službách je hotový ale niekoľko rokov sa čaká na jeho definitívne schválenie.

Táto bakalárska práca slúži na komparáciu perimetrický detekčných systémov a fyzickej ostrahy.

ZÁVER V ANGLIČTINE

Perimeter protection is one of the most challenging parts security techniques. Very important is the preparation before installing itself. Safety assessment of the object, and then select the appropriate elements of perimeter detection systems is an important component of an effective and reliable security. Should be taken into account manufacturer's instructions that are given in instruction.

Zo SWOT analysis, which has been a part of this bachelor work, analyses detail in practical part showed that the most effective security perimeter building not use perimeter detection systems or physical security but their combination. The analysis clearly shows that where there is a protection system deficiencies, the second system can effectively eliminate these shortcomings.

Trends that have also been described in the practical part of the show progress in its perimeter detection systems. It is an efficient system that can work on CCTV. Points to a possible attack by a team of CCTV systems may focus on that area swing lens optionally approximate area where the RFID tag declares accelerative possible attack. From SWOT analysis showed that the system effectively replaced most of the shortcomings of perimeter detected systems and physical security weaknesses.

The great weakness in the Czech Republic is a legislative environment that is not conducive to private's security services. Tie must be underpinned by Penal Code and the Trade Act. In essence, these people have the same powers as all else that many times abused by criminals theft in department stores. The future law on private security services is done for several years but is awaiting its final approval.

This bachelor thesis serves to comparison perimeter detected systems and physical security.

ZOZNAM POUŽITÉ LITERATÚRY

- [1] *Mvcr.cz* [online]. 2013. vyd. Praha: Ministerstvo Vnitřní České republiky, 2013 [cit. 2013-05-13]. Dostupné z: <http://www.mvcr.cz/clanek/navrh-zakona-o-soukrome-bezpecnostni-cinnosti.aspx>
- [2] Česká republika. Živnostenský zákon. In: *455/1991 Sb.* 02.10.1991, roč. 1991, č. 455, 87/1991. Dostupné z: <http://www.zakonyprolidi.cz/cs/1991-455>
- [3] *Perimetrická ochrana* [online]. 2012 [cit. 2013-05-21]. Dostupné z: <http://www.suntech.sk/nase-portfolio/perimetricka-ochrana/>
- [4] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management I.* 1.vyd. Zlín : VeRBuM, 2011. 316 s. ISBN 978-80-87500-05-7.
- [5] MACHÁČEK, Martin. *Encyklopedie fyziky.* Praha : Mladá fronta, 1999. 408 s. ISBN 80-204-0237-3.
- [6] IVANKA, Ján. *Systematizace bezpečnostního průmyslu I.* Zlín : Univerzita Tomáše Bati ve Zlíně, 2009. 123 s. ISBN 978-80-7318-850-4.
- [7] VALOUCH, Jan. *Projektování bezpečnostních systémů.* Zlín : Univerzita Tomáše Bati ve Zlíně, 2012. 155 s. ISBN 978-80-7454-230-5.
- [8] TNI 33 4591-3. *Poplachové systémy-Poplachové zabezpečovací a tísňové systémy- Část 3: Uvedení PZTS do provozu a jeho následná provoz, údržba a servis- Komentář k ČSN CLC/TS 50131-7:2011.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2012. 12 s.
- [9] *Euroalarm* [online].2011. 2007 [cit. 2011-07-31]. Bezdrátový perimetr. Dostupné z WWW:<http://www.euroalarm.cz/zabezpecovaci-technika/zabezpecovaci-systemy/perimetr/bezdratovy-perimetr/>.
- [10] *Eurosat CS* [online]. 2011 [cit. 2011-04-12]. IR závora AX - 200 ALFA. Dostupné z WWW: <<http://www.eurosat.cz/1780-ax-200-alfa-plus.html>>.
- [11] PINKER, Jiří. *Mikroprocesory a Mikropočítače.* Praha : BEN- technická literatura, 2004. 220 s. ISBN 80-7300-110-1
- [12] MC9S08QG4CPAE Data Sheet [online]. Freescale Semiconductor,2011 [cit. 2012-01-25].

[13] LAUCKÝ, Vladimír. Technologie komerční bezpečnosti II.2.vyd. Zlín : UTB Zlín, 2007. 123 s. ISBN 978-80-7318-631-9

[14] Česká republika. Trestní zákoník. In: *40/2009 Sb.* 08.01.2009, roč. 2009, č. 40, 11/2009. Dostupné z: <http://www.zakonyprolidi.cz/cs/2009-40>

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

Cm	centimeter
Č.	číslo
ČR	Česká republika
EZS	elektronická zabezpečovacia signalizácia
Hz	Hertz
Kč.	Korun českých
kHz	kilohertz
ODS	Občanská demokratická strana
Odst.	Odstavec
PDS	perimetricke detekčné systémy
PIR	passive infrared sensor
Sb.	sbírka
SBS	Súkromné bezpečnostné služby
SWOT	strenght waeknesses opportunities threats
USA	United States of America

ZOZNAM OBRÁZKOV

<i>Obr. 1 Stráženie plotov</i>	20
<i>Obr. 2 Infračervené závory</i>	20
<i>Obr. 3 Mikrovlnné bariéry</i>	21
<i>Obr. 4 Zemné detekčné káble</i>	21
<i>Obr. 5 Žiletkový systém</i>	22
<i>Obr. 6 Elektromagnetické spektrum</i>	24
<i>Obr. 7 Štrbinový kabel</i>	26
<i>Obr. 8 Duálny detektor</i>	27
<i>Obr. 9 SWOT matica</i>	40
<i>Obr. 10 Doporučené lhůty funkčních zkoušek [14] (upravil Valouch, 2012).....</i>	42
<i>Obr. 11 Minimálna doba napájania náhradným napájecím zdrojom</i>	43
<i>Obr. 12 inštalácia RFID akcelerátorov v objekte.....</i>	50

ZOZNAM TABULIEK

Tabuľka 1. Analýza PDS	47
Tabuľka 2. Analýza fyzickej ostrahy	47