Návrh systému perimetrické ochrany referenčního objektu v polních podmínkách

Bc. David Svoboda

Diplomová práce
2020

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav elektroniky a měření

Akademický rok: 2019/2020

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. David Svoboda**
Osobní číslo:	**A18633**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**Kombinovaná**
Téma práce:	**Návrh systému perimetrické ochrany referenčního objektu v polních podmínkách**
Téma práce anglicky:	**The Design of a Perimeter Protection System of a Field Reference Object**

Zásady pro vypracování

1. Objasněte specifika míst velení v poli a způsobu jejich ochrany. Identifikujte a analyzujte bezpečnostní hrozby, které místa velení ohrožují.
2. Specifikujte, co je to perimetrická ochrana a jaké je její místo v systému ochrany referenčních objektů.
3. Analyzujte možnosti zajištění perimetrické ochrany. Zaměřte se na technické prostředky a analyzujte jejich parametry. Posuďte jejich vhodnost pro zajištění perimetrické ochrany míst velení v poli.
4. Vytvořte model hypotetického místa velení v polních podmínkách. Na základě analýzy rizik navrhněte dva způsoby zajištění perimetrické ochrany zabezpečené oblasti místa velení. Návrhy posuďte a vyberte vhodnější.
5. Vybraný návrh zajištění perimetrické ochrany zabezpečené oblasti místa velení rozpracujte ve formě projektu.

Rozsah diplomové práce:
Rozsah příloh:
Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. ČESKÁ REPUBLIKA. Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. Česká republika, 2005.
2. ČESKÁ REPUBLIKA. Nařízení vlády č. 522/2005 Sb., nařízení vlády, kterým se stanoví seznam utajovaných informací. Česká republika, 2005.
3. ČESKÁ REPUBLIKA. Vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor. In: Sbírka zákonů České republiky. 2005, částka 179, 522-529.
4. ČESKÁ REPUBLIKA. Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů. Brno, 2005.
5. ČESKÁ REPUBLIKA. Rozkaz ministra obrany ČR č. 14/2013, Věstníku o ochraně utajovaných informací v rezortu Ministerstva obrany. In: Ministerstvo obrany, 2013, číslo 14.
6. ČESKÁ REPUBLIKA. Normativní výnos Ministerstva obrany č. 77/2013 Věstníku, Fyzická bezpečnost v rezortu Ministerstva obrany. In: Ministerstvo obrany, 2013, číslo 77.
7. LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management I. Zlín: VeRbuM, 2011. ISBN 978-80-87500-05-7.
8. VALOUCH, Jan. Projektování bezpečnostních systémů. Zlín: UTB, 2019. ISBN 978-80-7454-858-1.

Vedoucí diplomové práce: **doc. Ing. Luděk Lukáš, CSc.**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **9. prosince 2019**
Termín odevzdání diplomové práce: **29. května 2020**

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Milan Navrátil, Ph.D.
ředitel ústavu

Ve Zlíně dne 9. prosince 2019

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové 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 diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/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 diplomovou 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 – diplomovou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové 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 diplomové práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové 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 diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 13. srpna 2020

David Svoboda, v. r.
.....
podpis diplomanta

ABSTRAKT

Předmětem diplomové práce je vytvoření návrhu systému perimetrické ochrany hypotetického místa velení v polních podmínkách, které umožňuje nakládání s utajovanými informacemi. Teoretická část specifikuje místa velení v poli, systém ochrany a identifikuje bezpečnostní hrozby, které místa velení ohrožují. Pro možnost zpracování utajovaných informací je popsán legislativní rámec k zajištění fyzické bezpečnosti. Je popsáno začlenění perimetrické ochrany do systému fyzické bezpečnosti. V praktické části jsou analyzovány technické prostředky k zajištění perimetrické ochrany nestacionárního místa velení. Jsou navrženy dvě varianty ochrany perimetru, ze kterých je vybrána vhodnější, která je v poslední kapitole rozpracována ve formě ideového projektu.

Klíčová slova: místo velení, legislativa, fyzická bezpečnost, utajovaná informace, technický prostředek, perimetrická ochrana, projekt, zabezpečená oblast, operační středisko.

ABSTRACT

The subject of this diploma thesis is to design a perimeter protection system which would enable handling of classified information at a hypothetical place of command in field conditions. The theoretical part of the thesis specifies places of command in field, the protection system and identifies security threats which present a danger for the places of command. The possibility to handle classified information is defined through a legislative framework for providing physical security. The practical part of the thesis analyses technical means for securing perimeter protection of a nonstationary place of command. Two options of perimeter protection are proposed while selecting the more suitable one, which is then elaborated in the last chapter in the form of a conceptual design.

Key words: place of command, legislation, physical security, classified information, technical means, perimeter protection, design, secured area, operations center.

Na tomto místě bych rád poděkoval doc. Ing. Luďkovi Lukášovi, CSc. za odborné vedení, pravidelné konzultační hodiny, podnětné rady a věcné připomínky při tvorbě mé diplomové práce.

Velký dík patří také mým kolegům a kamarádům za podporu, a především mé rodině, která se vždy snažila poskytnout mi dostatek prostoru jak při samotném studiu, tak vypracování diplomové práce.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

K zajištění systému velení a řízení jsou pro velitele a jeho podřízené nezbytné funkce pořizování, sběru, správy, zpracování, ochrany a přenosu informací. Tyto procesní funkce jsou zajištěny prostřednictvím komunikační a informační podpory velení a řízení, které probíhá v komunikačních a informačních systémech a jsou nedílnou součástí míst velení. Pokud tyto činnosti probíhají v polních podmínkách, tedy v operacích či při cvičeních, kdy je nutné rozmístit síly a prostředky mimo stálou dislokaci, využívají se mobilní nebo rozmístitelná místa velení. Tato místa velení mají definováno svoje prostorové uspořádání a ohraničený perimetr. Zde vzniká potřeba tento definovaný prostor zabezpečit proti vniknutí pomocí vhodně zvoleného systému fyzické bezpečnosti. V dnešní moderní době je nutné, z důvodu bezpečnosti vlastních vojsk zabezpečit komunikaci utajovanou, která musí naplňovat podstatu plynoucí ze zákonů a norem. Převážně ze zákona č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti. Tento zákon přesně stanoví podmínky pro zpracování utajované informace a definuje podmínky její ochrany.

Cílem této práce je na základě analýzy rizik stanovit hrozby, které rozmístitelné místo velení ohrožují, navrhnout možnosti k zajištění perimetrické ochrany s využitím technických prostředků bezpečnostního průmyslu.

Teoretická část diplomové práce je tvořena dvěma kapitolami. První kapitola specifikuje místa velení v poli, přístupy k jejich ochraně a identifikuje bezpečnostní hrozby, které místa velení ohrožují. V závěru první kapitoly je definován legislativní rámec pro zabezpečení fyzické bezpečnosti místa velení. Ve druhé kapitole je specifikována perimetrická ochrana a její začlenění do celkové ochrany referenčních objektů. V našem případě perimetrická ochrana hypotetického operačního střediska vrtulníkové letky.

V praktické části jsou analyzovány možnosti zajištění perimetrické ochrany operačního střediska vrtulníkové letky pomocí technických prostředků bezpečnostního průmyslu a stanovena jejich vhodnost k zajištění nestacionární perimetrické ochrany. Dále je vytvořen hypotetický model operačního střediska vrtulníkové letky a navrženy dvě varianty zajištění perimetrické ochrany. Na základě multikriteriální analýzy je vybrána vhodnější varianta, která je v poslední kapitole rozpracována ve formě projektu.

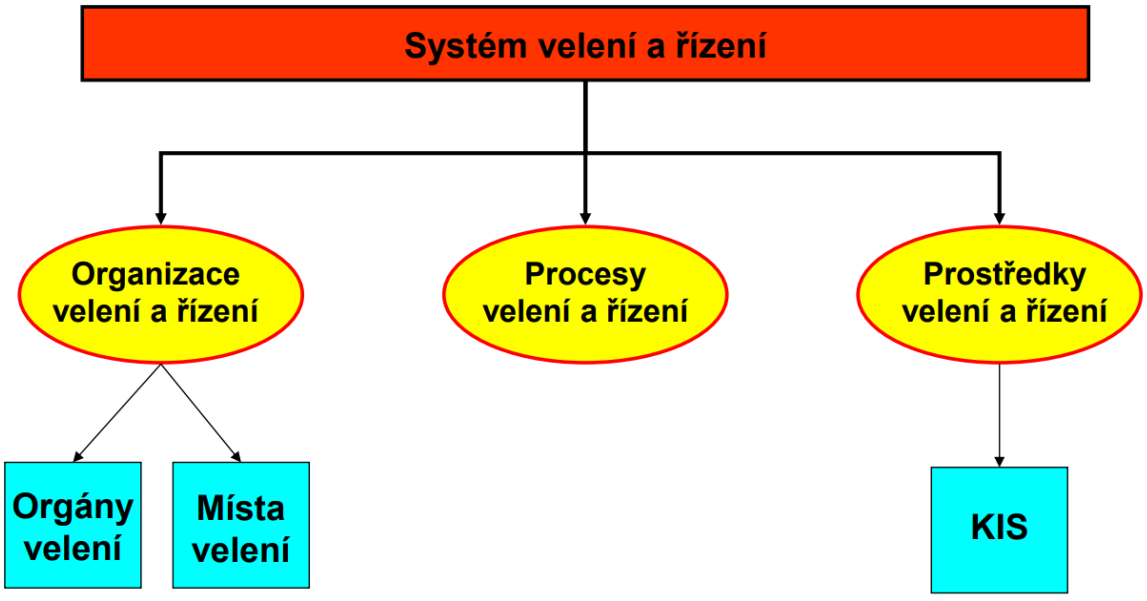
I. TEORETICKÁ ČÁST

1 SPECIFIKA MÍST VELENÍ V POLI A ZPŮSOBU JEJICH OCHRANY

Armáda České republiky v rámci svého působení plní různé úkoly. Plnění úkolů, kde jsou použity ozbrojené síly a je vykonávána vojenská činnost se nazývá vojenské operace. Tyto vojenské operace můžeme podle typu plněného úkolu dělit na bojové, nebojové a speciální. Ke splnění úkolů v rámci vojenských operací jsou tvořena úkolová uskupení jednotek, ve kterých musí být definován a zajištěn proces velení a řízení. Je nezbytné nastavit systém velení a řízení, který bude odpovídat požadavkům plněného úkolu.

Systém velení a řízení je tvořen z:

- organizace velení a řízení
  - orgánů velení a řízení
  - **míst velení**
- procesů velení a řízení
- prostředků velení a řízení [1]

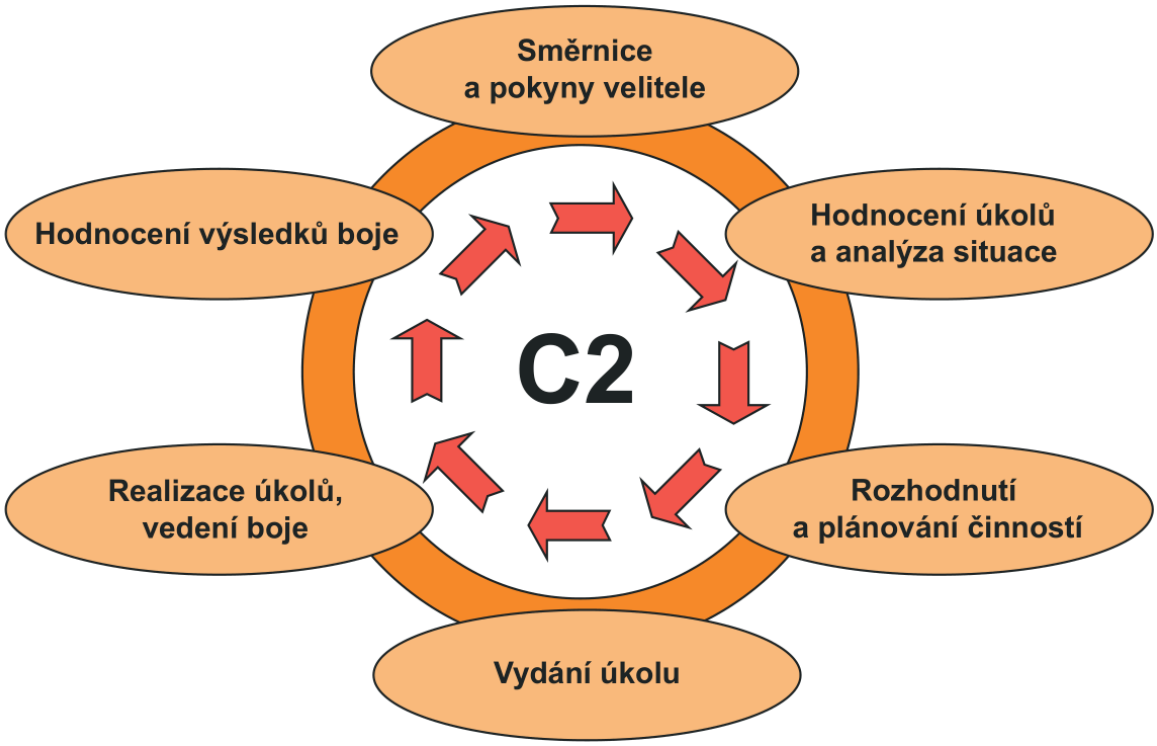


Obrázek 1 Systém velení a řízení [1]

1.1 Místa velení

Místa velení jsou základním prvkem jednotky, je zde realizováno velení a řízení silám a prostředkům v operaci. Jedná se o organizačně, funkčně a technicky uspořádaná a propojená

pracoviště velitele a štábu. Zabezpečují podporu pro velení a řízení s celkovým zaměřením na efektivní splnění stanovených úkolů. Velení a řízení spočívá v provádění opatření v oblastech personálu, výzbroje (vybavení, zařízení), komunikačních prostředků a zařízení, spojení, styčných činností a postupů využívaných velitelem v plánování, řízení, koordinování a kontrole sil ke splnění úkolů operace. Pro splnění cílů musí být místa velení schopna zabezpečit výměnu informací cestou komunikačních sítí a komunikačních a informačních systémů. Každé vytvářené místo velení musí být organizované tak, aby bylo možné plnohodnotně zabezpečit nepřetržitý proces velení a řízení, jak je vidět na obrázku 2. [2]



Obrázek 2 Proces velení a řízení [1]

V závislosti na situaci, úrovni velení a požadavku na mobilnost mohou být místa velení zřizována jako stacionární nebo mobilní. Při vytváření jednotlivých míst velení v operaci velitelé úkolových uskupení zpravidla tato místa přizpůsobují charakteru operace a plněným úkolům.

1.2 Funkce míst velení

Většina funkcí zajišťovaných místy velení je přímo spjata s vyhodnocováním a řízením činností v právě probíhající operaci, plánováním nastávajících činností nebo operací a poskytováním podpory velení a řízení.

Funkce, kterými MV přímo přispívá ke splnění těchto úkolů, jsou:

- tvorba a distribuce rozkazů
- informační management
- předkládání návrhů štábem pro přijetí rozhodnutí
- řízení operací
- vyhodnocování operací
- administrativní řízení místa velení
- přemísťování místa velení
- zajišťování ochrany místa velení
- vytváření taktického/operačního centra pro operace
- udržování kontinuity (nepřetržitosti) operací [2]

K zajištění úspěšného plnění všech funkcí míst velení je nutné zabezpečit, aby informační a komunikační prostředky místa velení umožňovaly provoz v režimu utajení „Tajné“ a v případech kooperace s aliančními partery „NATO secret“ a „Mission secret“.

1.3 Dělení míst velení

V závislosti na plánovaných úkolech, úrovni velení a požadavku na mobilnost mohou být místa velení zřizována jako stacionární nebo mobilní, stálá nebo dočasná. Místa velení můžeme také členit dle velikostí a typu jednotky, pro kterou je místo velení zřizováno.

1.3.1 Stacionární místa velení

Jsou budována zpravidla pro strategickou a v závislosti na situaci i pro operační úroveň velení. Představují utajované a zpravidla předem vybudované zabezpečené objekty, které jsou odolné vůči úderům vysoce přesných zbraní. Umožňují i dlouhodobý pobyt nezbytného počtu osob pro úspěšné splnění operace.

Jako stacionární místa velení mohou být využita:

- předem připravená chráněná pracoviště s vybudovanou komunikační a informační infrastrukturou

- stacionární vojenské objekty s předem vybudovanou komunikační a informační infrastrukturou
- stacionární civilní objekty s částečně vybudovanou komunikační infrastrukturou

1.3.2 Mobilní (rozmístitelná) místa velení

Mobilní místa velení jsou vytvářena pro operační, ale zejména pro taktickou úroveň velení. Jejich základem jsou mobilní velitelsko-štábní pracoviště, kde komunikačním jádrem jsou mobilní provozovny komunikačních a informačních systémů (KIS). Struktura mobilního místa velení odpovídá principu modulárního uspořádání. Je požadováno, aby místo velení úkolového uskupení bylo možné rozvinout jako kompletní celek, nebo je vybudovat rozděleně po modulech v závislosti na plněném úkolu, podmínkách terénu, vlastní bojové sestavě, nepříteli a času, který je k dispozici. V závislosti na stupni velení jsou mobilní místa velení obvykle složena z malého počtu vozidel, kontejnerů a stanů. Tyto systémy umožňují fyzicky spojit kontejnery a stany tak, aby vznikl jeden společný pracovní prostor s možností zvýšeného stupně zabezpečení, dle typu zpracovávaných informací.

Mobilní místa velení vybavená moderními prostředky velení a řízení poskytují velitelům a štábům:

- vysokou a kvalitní znalost aktuální situace a přesný společný operační obraz situace
- nástroje pro analýzu aktuální situace
- vysokou úroveň plánování boje, přípravy a distribuce formalizovaných bojových dokumentů
- aktualizaci bojových, technických a logistických údajů o jednotkách
- vysoké možnosti pozorování a průzkumu, zajištění včasnosti a přesnosti hlášení o aktuální situaci v průběhu operace
- tok informací převážně pomocí digitálních prostředků propojených v sítích
- prostředky pro digitální komunikaci, které zefektivňují přenos dat a hlasu a snižují možnosti negativního, elektronického působení nepřítele na komunikační a informační systémy míst velení

1.3.3 Stálá místa velení

Jsou zřizována pro práci velitele a štábu při plánování operace a zabezpečení velení vojskům při přípravě, provedení a ukončení operace.

Stálá místa velení tvoří:

- hlavní místo velení
- záložní místo velení

Hlavní místo velení je zřizováno na strategickém, operačně-taktickém i taktickém stupni velení až do stupně prapor. Je to místo, na kterém pracuje velitel s většinou svých hlavních funkcionářů a větší částí štábu. V hlavním místě velení se rovněž rozmísťují styčné skupiny od nadřízeného, podřízených, sousedů a spolupůsobících jednotek. Činnost na místě velení řídí náčelník štábu. Z tohoto místa se uskutečňuje velení podřízeným vojskům a řízení jejich přípravy, provedení a ukončení operace. Z hlavního místa velení musí být zabezpečeno spolehlivé spojení k nadřízenému, podřízeným, spolupůsobícím jednotkám a sousedům. Rozmísťuje se zpravidla za bojovou sestavou sil prvního sledu v takové vzdálenosti, aby bylo zabezpečeno spolehlivé velení a řízení vojsk.

Záložní místo velení je zřizováno na strategickém, operačně-taktickém i taktickém stupni velení až do stupně brigáda. Zabezpečuje zvýšení odolnosti systému velení a řízení. Působí zde vyčleněná část štábu, která je předurčena k převzetí velení v případě vyřazení nebo přemísťování hlavního místa velení. Proto je zpravidla po technické stránce vybudováno ve stejném rozsahu jako hlavní místo velení.

1.3.4 Dočasná místa velení

Jsou zpravidla budována pouze na omezenou dobu pro zabezpečení velení a řízení při plnění specifických úkolů v rámci operace. Rozhodování o jejich zřízení je v kompetenci velitele, který z tohoto místa zpravidla osobně řídí činnost. Technické prostředky pro dočasná místa velení jsou vyčleňovány z hlavního místa velení.

Dočasná místa velení (jako dočasné prvky velení a řízení vojsk) mohou být dále zřizována jako:

- taktické místo velení na stupni útvar (praporní ÚU), svazek (brigádní ÚU) a vyšším
- vzdušné místo velení

Prostředky velení a řízení jsou určeny k zajištění spolehlivého a nepřetržitého managementu informací, tvorbě a aktualizaci společného obrazu operační situace, k předávání rozkazů, nařízení, povelů, signálů, zpráv a hlášení mezi jednotlivými orgány velení a řízení na všech úrovních. Jsou určeny k zabezpečení velení vojskům a jejich řízení podle rozhodnutí velitele. Plnění těchto úkolů je úzce svázáno s komunikačními a informačními systémy. Základní prostředky velení a řízení představují především komunikační a informační systémy.

Komunikační a informační systém AČR

Srdcem každého zřizovaného místa velení, pro podporu všech výše uvedených činností, zabezpečení informační nadvlády a plnění požadavků na bezpečnost informací, je komunikační a informační systém, pokud je místo velení zřizováno v polních podmínkách jedná se polní informační a komunikační systém.

Komunikační a informační systémy a polní komunikační a informační systémy slouží k zajištění spolehlivé a nepřetržité dostupnosti informací, vytváření a aktualizaci společného obrazu o operační situaci, k předávání rozkazů, nařízení, povelů, signálů, zpráv a hlášení mezi jednotlivými orgány velení a řízení na všech úrovních.

1.4 Ochrana míst velení

Místa velení představují pro nepřítele významné cíle. Vyřazení místa velení může vážně narušit průběh operace a ohrozit splnění stanoveného úkolu. Charakter soudobých operací zvyšuje možnosti přímého napadení míst velení pozemním i vzdušným nepřítelem. Do popředí se dostává problematika ohrožení míst velení z kyberprostoru a narušení integrity a dostupnosti informací, které zásadní roli v procesech velení a řízení. Proto jsou přijímána a realizována opatření k jejich ochraně a obraně. Ochrana a obrana míst velení se tak stává jednou z priorit. Je zpravidla zajišťována jak silami a prostředky samotných míst velení, tak i silami útvarů a jednotek, které působí v jejich blízkosti. Ochranou míst velení se rozumí soubor opatření, kterými lze snížit účinek zbraní, působení nepřítele a průnik nepřítele do chráněného prostoru místa velení. Patří k nim využívání ochranných vlastností terénu, elektronických prostředků a zařízení, rozptýlení a maskování prvků míst velení, budování ochranných staveb, monitorování situace, zabezpečení utajovaných informací, protipožární opatření apod. Obrana míst velení spočívá v realizaci praktických opatření směrovaných k odhalení činnosti nepřítele a odražení útoků. Představuje aktivní činnosti, jimiž lze odhalovat, odrážet a ničit nepřítele. Rozsah úkolu nesmí být podceňován. Základem

zabezpečení ochrany a obrany míst velení je jejich utajení, což představuje přijetí a dodržování takových opatření, která nepříteli znemožní nebo maximálně ztíží odhalení místa velení a jeho komunikačních prostředků.

Ochrana a obrana míst velení je součástí ochrany sil (Force Protection – FP). Opatření k ochraně a obraně míst velení jsou realizována nepřetržitě, vzájemně se prolínají a doplňují a jejich souběžnou realizací se zvyšuje jejich účinnost. Pozornost je nutno věnovat i ochraně osob vjíždějících mimo střežené prostory a ochraně převážené dokumentace. Odpovědnost za ochranu a obranu míst velení odpovídá velitel, náčelník štábu (NŠ) kteří přijímají a organizují opatření a určení příslušníci štábu zajišťují jejich realizaci.

K ochraně a obraně míst velení je potřebné:

- zpracovat plán ochrany a obrany místa velení
- vyčlenit nezbytné síly a prostředky k ochraně a obraně místa velení
- organizovat střežení místa velení a jednotlivých pracovišť vyčleněnými jednotkami (skupinami, hlídkami) a vybavit je dostupnými senzory a čidly schopnými i za snížené viditelnosti včas zjistit možné ohrožení místa velení
- organizovat obranu místa velení proti pozemnímu a vzdušnému nepříteli vyčleněnými jednotkami
- organizovat monitorování radiační, chemické, biologické a hydrometeorologické situace
- provádět ženijní opatření k zodolnění místa velení a jeho prvků
- stanovit zabezpečení a režim provozu
- stanovit způsob manipulace s nosiči utajovaných informací a utajovanými předměty, jejich ukládání, kontrolu a hlášení výsledků
- stanovit způsob střežení, režim pohybu v blízkosti MV, vstupu do prostoru MV a jeho jednotlivých prvků
- stanovit režim života, pohybu osob i techniky a přijímat opatření k odstranění demaskujících příznaků
- stanovit způsob a prostředky pro systém včasného varování vojsk (organizační opatření, technika)

- podle možností vytvářet klamná místa velení

Pozornost musí být věnována i ochraně a obraně skupin nebo jednotlivých osob vyjíždějících mimo střežené prostory míst velení (např. velitel a příslušníci štábu vyjíždějící k podřízeným nebo na jiné MV). Spolu s ochranou a obranou osob je nutné zabezpečit i ochranu převážených informací.

1.5 Bezpečnostní hrozby, které místa velení ohrožují

Dle [3] je bezpečnost subjektů chápána jako stav, kde rizika plynoucí z hrozeb jsou minimalizován na akceptovatelnou úroveň. Má-li se subjektu zajistit bezpečnost, musí být známy základní hrozby které mu mohou způsobit újmu.

Definice hrozby a rizika:

„Hrozba je primární, mimo nás nezávisle existující, vnější fenomén, který může nebo chce poškodit nějakou konkrétní hodnotu. Závažnost hrozby je úměrná povaze hodnoty a toho, jak si danou hodnotu ceníme… Termín ohrožení je synonymem termínu hrozba. Riziko je pravděpodobnost, že dojde ke škodlivé události, jež postihne danou hodnotu. Riziko je možnost, že s určitou pravděpodobností vznikne událost, jež se liší od toho, co si přejeme. Riziko je odvozená závislá proměnná a dá určit nebo odhadnout tzv. analýzou rizik. Riziko je reakcí na hrozbu, též na stav naší připravenosti (zranitelnosti) a je spojeno s rozhodováním.“ [4]

Vojáci, působící v zahraničních operacích mimo území České republiky působí převážně v nestabilních regionech, kde je vlivem mnoha aspektů zhoršena bezpečnostní situace. Pro minimalizaci hrozeb a zmírnění dopadů zhoršené bezpečnostní situace je v AČR zřízen směr, který se nazývá Ochrana vojsk. Příslušníci z řad armády zabývající se ochranou vojsk mají za úkol připravit a realizovat plán fyzické bezpečnosti a operační bezpečnosti a spolu s dalšími klíčovými složkami se podílet na vytvoření vlastní ochranné služby.

Z pohledu ochrany vojsk můžeme hrozby rozdělit do následujících kategorií:

- úroveň 1 – do této kategorie zahrnujeme demonstrace, civilní nepokoje a teroristické agenty působící proti koaličním jednotkám
- úroveň 2 – zde řadíme například nepřátelské malé taktické jednotky nebo partizánské jednotky

- úroveň 3 – jedná se o těžké útoky nepřítele pomocí letectva, řízených střel, použití nukleárních, biologických a chemických zbraní

1.5.1 Identifikace a analýza bezpečnostních hrozeb

Pro úspěšné splnění operačního úkolu je před vybudováním operačního střediska vrtulníkové letky nutné navrhnout a stanovit bezpečnostní opatření k ochraně vlastních sil a prostředků. První fází je identifikace a analýza možných bezpečnostních hrozeb.

Můžeme předpokládat, že vyčleněné úkolové uskupení bude ve většině případů zasazeno do operačního prostředí se zásadně rozdílnými podmínkami než při působení na území ČR. Budou zde působit faktory ke kterým musíme při návrhu bezpečnostních opatření přihlížet.

Mezi tyto faktory patří:

- faktory operačního prostředí – k trvale působícím faktorům operačního prostředí patří terén, povětrnostní podmínky, denní a roční doba; terénní a klimatické podmínky (pouštní, hornaté a tropické); tyto faktory mohou negativně působit nejen na zbraně a bojovou techniku, ale i na zdravotní a psychický stav vojáků
- charakter státu – jedná se o následky vedení bojové činnosti zejména destrukce přehrad, průmyslových zařízení, hospodářské infrastruktury státu, vzniku radiačních nebo chemických havárií spojených s únikem radioaktivních, průmyslových toxických nebo biologických látek v jejichž důsledku mohou vzniknout rozsáhlé kontaminované prostory
- demografie, regionální a mezinárodní vztahy a vazby – do této skupiny faktorů řadíme negativní postoje civilního obyvatelstva v prostoru operace, které mohou být zapříčiněny neakceptováním náboženství, zvyků a obyčejů
- vojenské schopnosti stran zúčastněných v konfliktu – trvalou hrozbu ze strany nepřítele bude představovat asymetrický způsob vedení boje vyznačující se způsobením co největších ztrát příslušníkům ozbrojených sil
- vojenské schopnosti vlastních vojsk – logistické zabezpečení, interoperabilita se spojenci v operační, materiální, technické a administrativní oblasti a v oblasti procedur na všech organizačních úrovních, spolupráce s nevojenskými národními i mezinárodními, vládními a nevládními organizacemi a otevřenost k médiím

V souvislosti s výše uvedenými faktory můžeme identifikovat následující hrozby, které mohou negativně ovlivňovat chod operačního střediska vrtulníkové letky. Hrozby můžeme rozdělit do následujících kategorií:

1. Bojové

Hrozba útoku na vnější perimetr základny zahrnuje:

- komplexní útok veden převážně více osobami na určitý bod perimetru s cílem ho prolomit a vniknout do prostoru místa velení; nejedná se o eliminaci někoho nebo něčeho, ale primárním cílem je ohrožení celého místa velení
- hromadné používání improvizovaných výbušných zařízení (Improvised Explosive Device – IED)

Hrozba minometných a raketový útoků zahrnuje:

- útok je veden z pozice vzdáleného perimetru, útočníci jsou skryti – místo velení je vyzrazeno; není možné úplně přesně určit, kam raketa dopadne; nejedná se o eliminaci někoho, něčeho nebo celé základny, je to spíše ukázání jsme tady a víme o vás

Hrozba průniku narušitele do prostoru základny zahrnuje:

- sebevražedný atentátník používající IED nebo zbraní hromadného ničení (ZHN) - zpravidla jedna osoba (může být i více na více místech), může způsobit největší ztráty – je to cílený útok na hlavní funkcionáře, důležité objekty v místě velení
- průnik narušitele – narušitel nepozorovaně pronikne do zabezpečené oblasti

2. Technické

Přímé ohrožení technických prostředků operačního střediska vrtulníkové letky zahrnuje:

- únik informací – k úniku informací v polních podmínkách může dojít porušením pravidel administrativní, fyzické, personální, komunikační a počítačové bezpečnosti; dalším zdrojem úniku informací, může být kompromitující elektromagnetické vyzařování hardwarových komponent KIS
- nedostupnost systému a služeb – systém se stává nedostupný není-li schopen zabezpečit dostupnost požadovaných služeb pro velení řízení v operaci

- porušení integrity – za porušení integrity je považováno neautorizované vytvoření, modifikace nebo vymazání informace; při porušení integrity je narušena schopnost štábů řídit operace, může dojít k nežádoucímu účinku vlastních zbraní; toto riziko předpokládá vysokou úroveň technické vybavenosti a znalosti narušitele
- zamítnutý přístup – útok vede k zabránění v oprávněném přístupu k informacím, službám a zdrojům; jedná se o útok, při kterém nepřítel využije svých částečných znalostí o síťovém provozu a do síťového prostředí vyšle takové množství paketů informací, že zahltí síťovou infrastrukturu a tím naruší dostupnost služeb KIS
- zneužití připojení do systému – útok který umožní překonání přístupových pravidel do systému; nepřítel využije chyby uživatele v nakládání s přístupovými údaji (přístupové jméno a heslo) nebo chybně stanovených pravidel pro vytváření přístupových jmen a hesel a připojí se do systému jako uživatel, čímž je porušena důvěrnost a integrita, v nejhorším případě – získání oprávnění k administrátorskému účtu – i dostupnost.
- škodlivý kód – může proniknout do KIS komunikačním rozhraním a provádí škodlivé instrukce v KIS, je důsledkem narušení informační bezpečnosti; při této hrozbě se může například jednat o počítačový virus, červa, trojského koně nebo škodlivý kód monitorující zadávání údajů prostřednictvím klávesnice; škodlivý kód může narušit důvěrnost, integritu a dostupnost KIS
- hrozba technického výpadku může být výsledkem činnosti nepřítele, technické poruchy nebo vlivem extrémních klimatických podmínek; vzhledem k tomu, jak se zvyšuje role KIS při vedení bojové činnosti, používá se při návrhu KIS určených k použití v polních podmínkách redundantních zařízení, která umožňují překonávat jednotlivé výpadky nezávisle na zdroji poškození

3. Přírodní

Požár – vznik požáru ohrožující operační středisko vrtulníkové letky.

Živelní katastrofy – povodeň, zemětřesení, sněhová kalamita.

1.6 Dílčí závěr

Cílem této podkapitoly je objasnit problematiku míst velení v poli, začlenit je do systému velení a řízení v operaci a specifikovat jejich ochranu. Dále jsou zde identifikovány

bezpečnostní hrozby, které místa velení ohrožují. Při analýze hrozeb a tvorbě plánu ochrany vlastních vojsk je důležité hodnotit nepřítele z pohledu jeho vlastních schopností a stavu přípravy armády, neuchylovat se k závěrům vycházejících z vlastních doktrín. Pro naše účely a k naplnění cílů práce budeme nadále uvažovat o rozmístitelném místě velení **operačním středisku vrtulníkové letky, které je zabezpečeno komplexní ochranou ze strany spolu kooperujících koaličních partnerů**, a to rozmístěním místa velení v prostoru chráněné alianční základny. Nebudeme uvažovat ochranu před hrozbami jako jsou hrozba útoku na vnější perimetr základny, hrozba minometných a raketový útoků. Ochrana před těmito hrozbami není předmětem této práce. Práce bude dále zaměřena pouze na ochranu perimetru opačného střediska vrtulníkové letky, které musí být schopno zabezpečit zpracovávání utajovaných informací.

Specifikace a popis hypotetického operačního střediska vrtulníkové letky, jsou předmětem čtvrté kapitoly této práce.

1.7 Legislativní požadavky k zajištění fyzické bezpečnosti v AČR

Z důvodu nutnosti zpracovávání utajovaných informací (UI) do stupně utajení „Tajné“, NATO secret“ a „Mission secret“ je vhodné definovat právní předpisy, které nakládání z utajovanými informacemi v oblasti fyzické bezpečnosti, vymezují.

Právní normy a předpisy platné pro rezort Ministerstva obrany v oblasti fyzické bezpečnosti:

- zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti
- nařízení vlády č. 522/2005 Sb., nařízení vlády, kterým se stanoví seznam utajovaných informací
- vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor, ve znění pozdějších předpisů
- vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů
- rozkaz ministra obrany České republiky č. 14/2013 Věstníku, Ochrana utajovaných informací v rezortu Ministerstva obrany.

- normativní výnos Ministerstva obrany č. 77/2013 Věstníku, Fyzická bezpečnost v resortu Ministerstva obrany

1.7.1 Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti navázal na zákon 148/1998 Sb., o ochraně utajovaných skutečností, ve kterém se upravily podmínky přístupu k utajovaným informacím a upřesnily se požadavky na jejich ochranu.

Zákon č. 412/2005 Sb., je rozšířen o další právní předpisy, mezi které patří:

- vyhláška č. 363/2011 Sb., o personální bezpečnosti a o bezpečnostní způsobilosti, ve znění pozdějších předpisů
- vyhláška č. 405/2011 Sb., o průmyslové bezpečnosti ve znění vyhlášky č. 416/2013 Sb.
- vyhláška č. 432/2011 Sb., o zajištění kryptografické ochrany utajovaných informací, ve znění vyhlášky č. 417/2013 Sb.
- nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací, ve znění pozdějších předpisů
- vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor, ve znění pozdějších předpisů
- vyhláška 525/2005 Sb., o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací, ve znění vyhlášky č. 434/2011 Sb.
- vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů
- vyhláška č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací, ve znění pozdějších předpisů
- prováděcí právní předpisy k zákonu č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, zákon o kybernetické bezpečnosti v působnosti NÚKIB (Národní úřad pro kybernetickou a informační bezpečnost) [5]

1.7.1.1 Předmět úpravy, vymezení pojmů a úvodní ustanovení

Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti spolu s prováděcími právními předpisy upravuje zásady pro stanovení UI, podmínky přístupu k nim a další požadavky na jejich ochranu. Stanovuje pravidla a podmínky pro jejich výkon a s tím spojený činnost státní správy. Tento zákon definuje utajovanou informaci jako informaci v jakékoliv podobě zaznamenanou na jakémkoliv nosiči označenou v souladu s tímto zákonem, jejíž vyzrazení nebo zneužití může způsobit újmu zájmu České republiky nebo může být pro tento zájem nevýhodné. O UI mluvíme pouze v případě, že je uvedena v seznamu utajovaných informací. Seznam UI je uveden v nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací, ve znění pozdějších předpisů. [6]

Rozdělení stupňů utajované informace spadá do čtyř kategorií:

- **Vyhrazené** – její vyzrazení neoprávněné osobě nebo zneužití může být nevýhodné pro zájmy ČR
- **Důvěrné –** její vyzrazení nebo zneužití může způsobit prostou újmu zájmům ČR
- **Tajné –** její vyzrazení neoprávněné osobě nebo zneužití může způsobit vážnou újmu zájmům ČR
- **Přísně tajné** – její vyzrazení neoprávněné osobě nebo zneužití může způsobit mimořádně vážnou újmu zájmům ČR [6]

Stupeň utajení určuje tvůrce dokumentu při vzniku dokumentu. Bez vědomí zhotovitele nesmí být stupeň utajení ponižován ani jinak měněn. [6]

Druhy bezpečnosti, pomocí kterých je ochranu utajovaných informací zajištěna:

- personální bezpečnost
- průmyslová bezpečnost
- administrativní bezpečnost
- fyzická bezpečnost
- bezpečnost informačních a komunikačních systémů
- kryptografická ochrana [6]

1.7.1.2 Fyzická bezpečnost

Fyzická bezpečnost se zabývá ochranou utajovaných informací, nacházející se ve zřizovaných objektech, kde jsou umístěny zabezpečené oblasti (ZO) a jednací oblasti (JO). Objektem může být budova nebo jiný ohraničený prostor. V těchto objektech je dovoleno ukládat, zpracovávat nebo manipulovat s utajovanou informací. [6]

Do zabezpečených oblastí můžeme ukládat utajované informace v analogové podobě nebo digitální podobě uložené na fyzickém nosiči. Stupeň utajení zabezpečené oblasti musí odpovídat nejvyššímu stupni utajované informace, kterou v ní ukládáme nebo zpracováváme. Zabezpečené oblasti se podle stupně utajení UI zařazují do kategorií Vyhrazené, Důvěrné, Tajné a Přísně tajné.

Podle možnosti přístupu k utajované informaci dělíme tyto zabezpečené oblasti do tříd:

- třída I, kde při vstupu do této oblasti dochází k seznámení s utajovanou informací
- třída II, kde při vstupu do této oblasti nedochází k seznámení s utajovanou informací

Neoprávněná osoba může vstoupit pouze do zabezpečené oblasti třídy II, a to s osobou, která má do této oblasti povolen vstup. V odůvodněných případech s písemným souhlasem odpovědné osoby nebo jí pověřené osoby je možnost na dobu nezbytně nutnou změnit třídu I na třídu II, pokud je zajištěno, že k utajované informaci nemá přístup neoprávněná osoba. Dále musí odpovědná osoba učinit taková opatření, aby v JO nedošlo k ohrožení nebo úniku projednávaných UI. [6]

Jednací oblast slouží pouze k pravidelnému projednávání utajované informace stupně utajení Tajné a Přísně tajné. Odpovědná osoba musí zajistit, aby v JO nedocházelo k nežádoucímu úniku nebo ohrožení projednávaných utajovaných informací. Odpovědná osoba má dále za povinnost požádat prostřednictvím Národního bezpečnostního úřadu o provedení kontroly na přítomnost nežádoucích technických prostředků, pomocí kterých by mohla být UI ohrožena. Neoprávněná osoba může do JO vstoupit pouze s osobou oprávněnou.

K zajištění fyzické bezpečnosti jsou stanovována následující opatření:

- ostraha
- režimová opatření
- technické prostředky [6]

Ostrahu vykonávají zaměstnanci orgánu státu, právnické osoby nebo podnikající fyzické osoby, příslušníci ozbrojených sil nebo ozbrojených bezpečnostních sborů. Dále ostrahu mohou vykonávat příslušníci ozbrojených sil cizí moci anebo zaměstnanci bezpečnostní ochranné služby. [6]

Ostraha se nepřetržitě zajišťuje u objektu, ve kterém se nachází ZO kategorie:

- Vyhrazené – objekt bez ZO a JO, nebo objekt s nejvýše Vyhrazenou ZO, se ostraha zajišťuje v rozsahu stanoveném odpovědnou osobou
- Důvěrné – nejméně jednou osobou, kde je na základě poplachového hlášení technických prostředků umožněn rychlý zásah, je-li zajištění ochrany UI narušeno
- Tajné – nejméně jednou osobou u objektu a jednou další osobou, kde je na základě poplachové hlášení technických prostředků umožněn rychlý zásah, pokud je ochrana UI narušena
- Přísně tajné – nejméně dvě osoby u objektu [6]

Ostraha u objektu, v němž se nachází JO stupně utajení:

- Tajné – nejméně jednou osobou u objektu a jednou další osobou, kde poplachové hlášení technických prostředků umožní rychlý zásah, je-li ochrana utajovaných informací narušena
- Přísně tajné – nejméně dvě osoby u objektu [6]

Režimová opatření stanovují:

- oprávnění osob a dopravních prostředků pro vstup a vjezd do objektu, oprávnění osob pro vstup do ZO a JO a způsob kontroly těchto oprávnění
- způsob manipulace s klíči a identifikačními prostředky, které se používají pro kontrolu vstupu
- způsob manipulace s technickými prostředky a jejich používání
- oprávnění při výstupu osob a výjezdu dopravních prostředků z objektu, ZO a JO
- podmínky a způsob kontroly pohybu osob v objektu, ZO a JO
- způsob kontroly a vynášení UI z objektu, ZO a JO [6]

Technické prostředky dělíme na:

- mechanické zábranné prostředky
- elektrická zámková zařízení a systémy pro kontrolu vstupu
- zařízení elektrické zabezpečovací signalizace
- speciální televizní systémy
- tísňové systémy
- zařízení elektrické požární signalizace
- zařízení sloužící k vyhledávání nebezpečných látek nebo předmětů
- zařízení fyzického ničení nosičů informací
- zařízení proti pasivnímu a aktivnímu odposlechu UI [6]

Pro každý certifikovaný nebo necertifikovaný technický prostředek je stanoveno bodové ohodnocení, které slouží pro vyplnění bodových hodnot vyjadřující míru zabezpečení. Vyhodnocení rizik nám stanovuje míru zabezpečení těchto opatření pro konkrétní ZO a JO. [6]

Všechna opatření fyzické bezpečnosti musí jako celek splňovat nejnižší možnou míru bodového ohodnocení, na základě stanovené kategorie utajení UI. Samotné hodnocení rizik se vypracovává průběžně a v případě nutnosti musí být míra opatření fyzické bezpečnosti upravena. V případech, kdy se v objektu nachází zabezpečená oblast kategorie Vyhrazené, Důvěrné, Tajné nebo Přísně tajné nebo jednací oblast, zákon ukládá povinnost zpracovat Projekt fyzické bezpečnosti. [6]

1.7.2 Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů

Tato vyhláška byla vydána Národním bezpečnostním úřadem (NBÚ). Patří do skupiny prováděcích vyhlášek o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb., vyhlášky č. 454/2011Sb. a vyhlášky č. 204/2016 Sb. Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků stanovuje jednotlivé bodové ohodnocení fyzické bezpečnosti. V této vyhlášce je řešeno vyhodnocení rizik a udělování certifikace technických prostředkům. [7]

1.7.3 Rozkaz ministra obrany č. 14/2013 Věstníku Ochrana utajovaných informací v rezortu MO

Rozkaz ministra obrany (RMO) č. 14/2013 Věstníku Ochrana utajovaných informací v rezortu Ministerstva obrany (MO), slouží k zabezpečení realizace ustanovení zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů v rezortu Ministerstva obrany. Tento rozkaz je platný pro organizační celky MO, vojáky z povolání a občanské zaměstnance (OZ) s výjimkou organizačních útvarů Vojenského zpravodajství. [8]

První část RMO č. 14/2013, upřesňuje účely tohoto rozkazu, obsahující základní pojmy v druhé části RMO je specifikována odpovědnost a povinnost při ochraně UI u zainteresovaných osob jako je Bezpečnostní ředitel (BŘ), Vedoucí organizačního celku (VOC) a definuje bezpečnostní správu organizačního celku (OC).

Dále je předmětem úpravy fyzická bezpečnost u organizačního celku, za kterou odpovídá VOC. Rozkaz dále upravuje povinnosti VOC v oblasti fyzické bezpečnosti, jako je:

- vytyčení hranic u ZO a její zařazení do příslušné třídy a kategorie, kde může stanovit po nezbytně nutnou dobu třídu I na třídu II
- vydávání povolení ke vstupu do objektu, ZO a JO, stanovení pravidel manipulace s klíči a ukládání klíčů a identifikačních prostředků
- průběžná kontrola fyzické bezpečnosti, a schvalování shody úschovných objektů, stanovování podmínek funkčních zkoušek u technických prostředků, kromě PZS
- schvalování projektu fyzické bezpečnosti, stanovování pravidel ostrahy
- zaslání podkladů odboru bezpečnosti MO
- vyžadování kontroly ZO a JO, prostřednictvím bezpečnostního ředitele
- způsob použití technických prostředků a stanovení režimových opatření k zabezpečení UI [8]

Dále RMO definuje použití a zabezpečení informačních a komunikačních systémů a elektronických zařízení, náležitosti k použití kryptografických prostředků a její ochrany a ochrana UI v polních podmínkách. Před zasazením velitel musí náležitě poučit své podřízené o způsobu zpracovávání utajované informace. Zpracované UI musí být vždy chráněny odpovědnou osobou. Dále musí být stanoveno prostorové uspořádání ochranného perimetru

a prostor pro ukládání nosičů UI. Projekt fyzické bezpečnosti při působení v polních podmínkách, které netrvá déle než 60 dnů, se nezpracovává, pokud VOC nestanoví jinak. Při působení v zahraniční operaci musí být vytvořen projekt fyzické bezpečnosti vždy, pokud se nejedná pouze o krátkodobou rekognoskaci terénu. [8]

1.7.4 Normativní výnos Ministra obrany č. 77/2013 Věstníku, Fyzická bezpečnost v rezortu MO

Normativní výnos Ministerstva obrany (NVMO) 77/2013 Věstníku, Fyzická bezpečnost v rezortu Ministerstva obrany slouží k přesnému postupu řešení otázek fyzické bezpečnosti v rezortu MO. Ustanovení tohoto vnitřního předpisu MO je v souladu se zákonem 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, dle nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací, dále vyhláškou č. 405/2001 Sb., o průmyslové bezpečnosti, vyhláškou č. 363/2001 Sb., o personální bezpečnosti a o bezpečnostní způsobilosti, vyhláškou č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, a RMO č. 14/2013 Věstníku, Ochrana utajovaných informací v rezortu MO a nabyl účinností 9. července 2013. [9]

Předmětem úpravy NVMO je stanovení systému opatření, který má v rezortu MO zabránit přístupu neoprávněných osob k utajovaným informacím, nebo tento přístup ztížit, popřípadě taková jednání zaznamenat. První část výnosu upřesňuje důležité pojmy a stanovuje odpovědnost velitele rozsáhlého objektu, bezpečnostního manažera objektu a správce technických prostředků. Druhou část výnosu včetně příloh, určuje organizaci fyzické bezpečnosti, a skladbu projektu fyzické bezpečnosti pro velitele organizačního celku. [9]

Předmětem úpravy NVMO je i fyzická bezpečnost v polních podmínkách. V polních podmínkách se ochrana UI, která je běžně zabezpečována prostřednictvím technických prostředků, zpravidla nahrazuje zvýšenou ostrahou. Zvýšená ostraha nahrazuje zabezpečení technickými prostředky v objektu, ve kterém se nacházejí ZO stupně utajení Důvěrné a vyšší. Ve stupni utajení Důvěrné je stanoveno střežení u objektu nejméně dvěma osobami nebo nejméně jednou osobou a služebním psem. Ve stupni utajení Tajné a Přísně tajné je stanoveno střežení u objektu nejméně třemi osobami nebo nejméně dvěma osobami a služebním psem. Příslušníci ostrahy vykonávají obchůzky v nepravidelných intervalech. U kategorie Důvěrné – nepřesahující 4 hodiny, Tajné – nepřesahující 2 hodiny a u kategorie Přísně tajné – nepřesahující 1 hodinu. V objektu, ve kterém se nachází ZO kategorie

Vyhrazené, provádí zvýšenou kontrolu určená osoba nejméně jednou za 12 hodin, nestanoví-li VOC jinak. [9]

V případě nutnosti zajistit ochranu UI na vojenském cvičení se na základě rozkazu velitele cvičení zřizuje dozorčí a strážní služba. Organizace ochrany utajovaných informací, musí být popsána ve směrnicích dozorčí a strážní služby. V případě zahraniční operace se UI ukládají do ZO, které jsou opatřeny ochranou fyzické bezpečnosti pomocí certifikovaných technických prostředků, zvýšenou ostrahou nebo jejich vzájemnou kombinací. [9]

1.7.5 Dílčí závěr

V jednotlivých druzích bezpečnosti je stanoveno, jak zpracovávané utajované informace chránit před zneužitím, vyzrazením, poškozením, nedovoleným šířením, ztrátou a zcizením. Mezi tyto druhy bezpečnosti patří administrativní bezpečnost, personální bezpečnost, průmyslová bezpečnost, fyzická bezpečnost, kryptografická ochrana a bezpečnost informačních a komunikačních systémů. Fyzická bezpečnost je ze všech druhů bezpečnosti nejkomplexnější je ustanovena v zákoně č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti a dále upravována v dalších legislativních předpisech, které OUI zajišťují. Je to skupina prováděcích vyhlášek, do které patří vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů. Zajištění fyzické bezpečnosti v objektech AČR je stanoveno doplňujícími vnitřními předpisy vydanými Ministerstvem obrany. Jsou to Rozkaz ministra obrany č. 14/2013 Věstníku Ochrana utajovaných informací v rezortu Ministerstva obrany a Normativní výnos Ministra obrany č. 77/2013 Věstníku, Fyzická bezpečnost v rezortu Ministerstva obrany.

2 PERIMETRICKÁ OCHRANA A JEJÍ MÍSTO V SYSTÉMU FYZICKÉ BEZPEČNOSTI

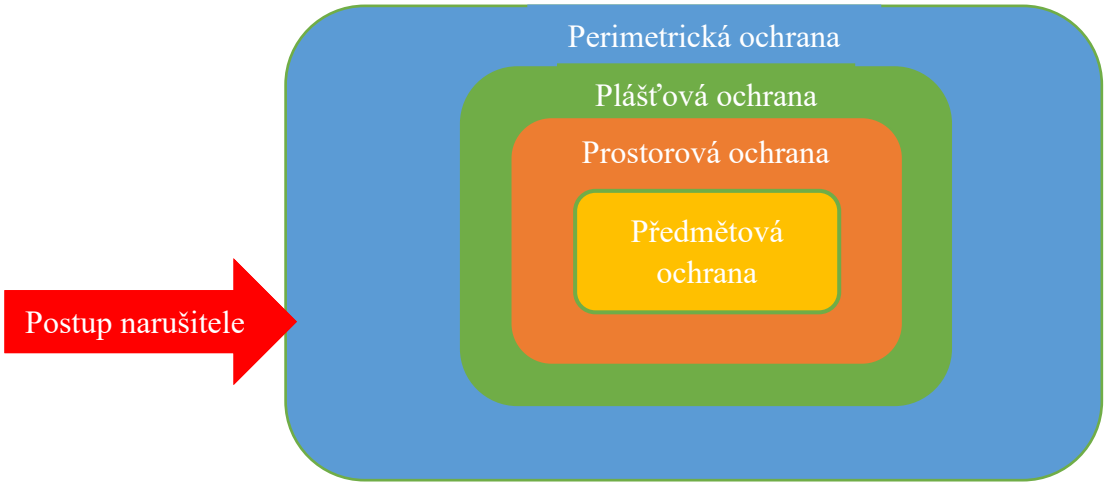
Cílem této kapitoly je popsání teoretického základu z oblasti perimetrické ochrany k zajištění fyzické bezpečnosti chráněného objektu, pomocí prvků fyzické ochrany. Fyzická ochrana, jako prostředek zajištění fyzické bezpečnosti chráněných objektů je využívána tam, kde požadujeme minimalizovat rizika ohrožení chráněných aktiv, plynoucích z bezpečnostních hrozeb, na akceptovatelnou úroveň. Při návrhu systému ochrany je však nutné mít vždy na paměti, že míra ochrany by měla odpovídat hodnotě chráněných aktiv. Dle pravidel ALARA by náklady na ochranu měly představovat 15% hodnoty aktiv.

2.1 Prostorové uspořádání systému fyzické bezpečnosti

Výše popsanou fyzickou ochranu můžeme pro lepší funkčnost, přehlednost a uspořádanost rozdělit do čtyř základních oblastí. Tyto oblasti jsou vymezeny podle rozdělení bariér, které musí narušitel chráněného objektu překonat, při postupu z vnějšího perimetru až k chráněnému aktivu. [3]

Základními stupni jsou:

- Předmětová ochrana
- Prostorová ochrana
- Plášťová ochrana
- Perimetrická ochrana



Obrázek 3 Uspořádání systému fyzické bezpečnosti [autor, převzato upraveno z [3]]

2.1.1 Předmětová ochrana

Je to zabezpečení drahých předmětů, obrazů, starožitností před odcizením. Detektory předmětové ochrany signalizují přítomnost pachatele u chráněného předmětu. Umožňují jejich trvalé střežení i v době, kdy prostorové detektory musí být z důvodu provozu vypnuté. Mezi nejvíce používané prvky poplachových zabezpečovacích a tísňových systémů v předmětové ochraně patří kapacitní detektory, kontaktní detektory, tlakové akustické detektory, závěsové detektory. [3]

2.1.2 Prostorová ochrana

Prostorová ochrana zabezpečuje prostor uvnitř střeženého objektu. Jejím úkolem je případného pachatele zpozdit, odhalit a znemožnit mu volný pohyb ve střeženém prostoru. Prostorová ochrana je tedy realizována ve vnitřních prostorech zabezpečovaných objektů. Detektory signalizují pohyb ve střeženém prostoru a poté po vyhodnocení ústřednou dojde k vyhlášení poplachu. Tím je chráněn prostor, kde jsou uloženy zájmová aktiva. [3]

2.1.3 Plášťová ochrana

Druhou ochranou z pohledu útočníka, kterou musí útočník překonat, je plášťová ochrana. Jedná se o souhrn bezpečnostních opatření fyzické bezpečnosti, tentokrát na plášti chráněného objektu. Cílem plášťové ochrany je odstrašit, znemožnit průchod, zpozdit anebo odhalit narušitele. Prvky plášťové ochrany tvoří především stěny, okna, dveře, zámky a zámkové systémy, mříže, bezpečnostní fólie, kamerové systémy a detektory narušení. [3]

2.1.4 Perimetrická ochrana

Perimetrická ochrana je první ochranou, kterou musí potencionální útočník překonat, aby dosáhl svého cíle. Jak je uvedeno v [3] „*Představuje souhrn bezpečnostních opatření fyzické bezpečnosti, uplatněných na obvodu pozemku (parcely) chráněného objektu a v prostoru mezi hranicí a chráněným objektem. Perimetrem (nebo také obvodem objektu) je jeho katastrální hranice, která bývá vymezena přírodními nebo umělými bariérami (plot, zeď, vodní tok). Cílem perimetrické ochrany je především odstrašení, odhalení a zpoždění narušitele. Perimetrická ochrana by měla signalizovat narušení obvodu objektu. Detektory narušení, použité v rámci perimetrické ochrany, mají obvykle delší dosah užší detekční charakteristiku, musí splňovat požadavky vyšší klimatické odolnosti a být odolné vůči planým poplachům. Vzhledem k různorodosti vnějšího venkovního středí i široké škále pohybujících se objektů bývá odolnost vůči planým poplachům problematickou.*“

2.1.4.1 Funkce odstrašení

Jedná se o psychologický efekt, kterým použitá bariéra působí na narušitele. Pokud je dostatečně robustní, vysoká a působí nepřekonatelně je možné, že se pachatel o narušení perimetru nepokusí anebo si to v průběhu pokusu rozmyslí. Hlavní roli v této oblasti perimetrické ochrany plní oplocení a doplňkové zábrany.

2.1.4.2 Funkce odhalení

Pokud nám nezafunguje odstrašující funkce perimetrické ochrany a pachatel se o překonání aplikovaných bariér pokusí, je nutné tento pokus co nejdříve detekovat, nejlépe ihned v jeho počátku. K detekci jsou určeny elektronické prvky poplachových zabezpečovacích systémů – detektory narušení. Odhalení následně vyhodnotíme, a to buď osobní přítomností ostrahy, nebo pomocí instalovaného kamerového systému.

2.1.4.3 Funkce zpoždění

Došlo-li k odhalení narušitele detekčním systémem včas, nachází se na hranici chráněného perimetru právě při překonávání mechanických zábranných systémů. MZS musí zabezpečit dostatečně dlouhou průlomovou odolnost potřebnou k vyhodnocení celé situace ostrahou a provedení zásahu k eliminaci narušitele.

2.2 Volba stupně zabezpečení

Při návrhu systému ochrany je nutné vhodně zvolit požadovaný stupeň zabezpečení. Volba stupně zabezpečení je závislá na schopnostech, znalostech, dovednostech, zkušenostech a technickém vybavení předpokládaného narušitele. Je také přímo úměrná míře významnosti chráněného objektu. Stupně zabezpečení jsou rozděleny do čtyř skupin podle míry rizika, které pachatel představuje.

2.2.1 Nízká riziko

Narušitel má nízké znalosti v oblasti poplachových a zabezpečovacích systémů a má omezený sortiment běžně dostupných nástrojů, které by využil k překonání aplikovaných technických prvků zajišťujících fyzickou bezpečnosti. [3]

2.2.2 Nízké – střední riziko

Narušitel má stále omezené znalosti v oblasti poplachových a zabezpečovacích systémů a používání běžného nářadí a přenosných přístrojů. [3]

2.2.3 Střední – vysoké riziko

Narušitel má znalosti v oblasti poplachových a zabezpečovacích systémů a má přístup k dostatečně velkému sortimentu nástrojů s přenosných elektronických přístrojů a zařízení. [3]

2.2.4 Vysoké riziko

Narušitel je zcela obeznámen se systémem ochrany, má připravený podrobný plán vniknutí a opuštění chráněného prostoru. Má velký sortiment přístrojů a nástrojů a také komponenty pro náhradu poplachových zabezpečovacích systémů. [3]

2.3 Faktory ovlivňující perimetrickou ochranu

Při návrhu perimetrického systému ochrany je nutné přihlížet k faktorům, které mají na volbu úrovně zabezpečení, volbu technických prvků a funkčnost systému ochrany zásadní vliv. Z důvodu zasazení technických prostředků v různě obtížných prostředích, musíme volit takové prvky, které budou místním podmínkám přizpůsobeny a dokážou spolehlivě pracovat.

Mezi tyto faktory patří:

- geografické faktory
- terénní faktory
- klimatické faktory
- sociální faktory
- faktory okolního prostředí

2.3.1 Geografické faktory

Celý systém ochrany je z geografického hlediska zasazen do prostoru, který ve většině případů nedokážeme ovlivnit. To znamená například v jaké krajině se střežený objekt nachází. V úvahu musíme brát i nadmořskou výšku chráněného objektu, která výrazně ovlivňuje podnebí, zejména výskyt mlh, intenzitu slunečního záření, množství a intenzitu srážek, rozmezí teplot, vlhkost apod. Při návrhu nestacionárního perimetrického systému jsou geografické faktory, pro které je systém ochrany navrhován, variabilní.

2.3.2 Terénní faktory

Terénní faktory jako je například reliéf terénu a terénní uspořádání dané oblasti si v nestacionární ochraně dokážeme přizpůsobit. První možností je volba místa výstavby prostředku, která je součástí rekognoskace před zasazením jednotky. Pokud jsme výběrem terénu omezeni můžeme následně provést ženijní úpravy terénu a terén si před zasazením jednotky upravit dle našich požadavků. Detektory používané ke střežení perimetru jsou náchylné zejména na nerovnosti terénu, proto nejčastější úpravou je jeho vyrovnání.

2.3.3 Klimatické faktory

Jedná se o klimatické změny v závislosti na ročním období. Například rostoucí tráva v zimním období sněhová pokrývka.

2.3.4 Sociální faktory

Do této skupiny faktorů řadíme sociální úroveň okolního obyvatelstva. Volba ochrany bude záviset na úrovni kriminality v okolí střeženého objektu. V případě nestacionární ochrany se jedná například o negativní postoje civilního obyvatelstva v prostoru operace, které mohou být zapříčiněny neakceptováním náboženství, zvyků a obyčejů.

2.3.5 Faktory okolního prostředí

Negativní faktory vyskytující se v chráněném objektu mohou ovlivňovat poplachový zabezpečovací systém a způsobovat falešné poplachy. Jedním z faktorů může být okolní doprava. Automobily mohou oslňovat detektory narušení svými světly. Kolejová doprava, hlavně železniční, způsobuje chvění okolního prostředí. V blízkosti lesních porostů, zemědělských ploch je častý výskyt zvěře a ptactva. Pohyb těchto zvířat může způsobovat nechtěné falešné poplachy. Dalším problémem je vysokofrekvenční rušení v blízkosti televizních vysílačů, radarových antén, systémů základnových stanic a podobných zařízení zvyšují nároky na elektromagnetickou odolnost použitých zařízení.

Na všechny tyto faktory musí být při návrhu systému perimetrické ochrany brán zřetel.

2.4 Perimetrická ochrana jako dílčí část zajištění fyzické bezpečnosti

Perimetrická ochrana je jednou ze 4 částí prostorového uspořádání funkční fyzické bezpečnosti. Opatření fyzické bezpečnosti jsou zajišťována kombinací prvků fyzické ostrahy, režimových opatření a prvků technické ochrany.

Obrázek 4 Fyzická bezpečnost [autor, převzato upraveno z [10]]

Pomocí vhodně zvolených opatření systému fyzické bezpečnosti, jsme schopni potenciálního narušitele odradit od jeho činu, zamezit jeho provedení, případně jej zpomalit při průniku k chráněným aktivům a získat dostatečný čas k jeho zadržení. [3]

2.4.1 Fyzická ostraha

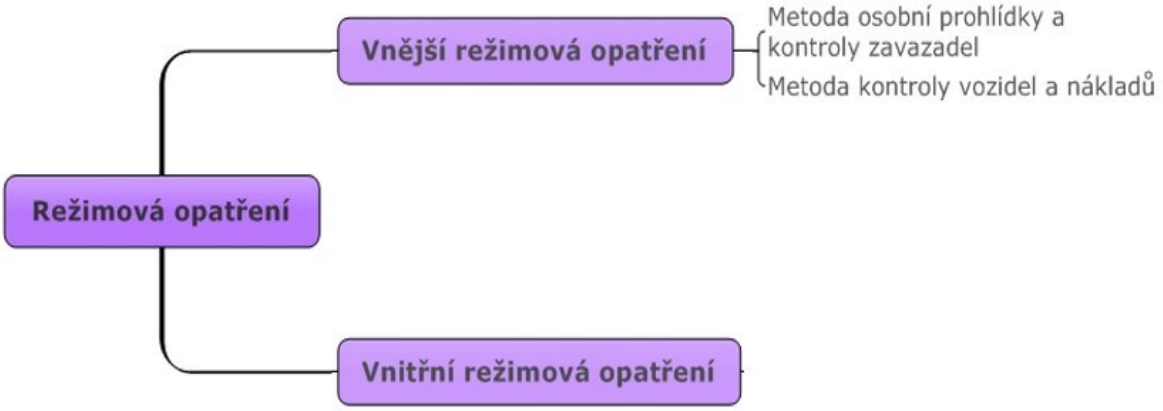
Fyzická ostraha může být zabezpečována silami vlastních vyškolených pracovníků, pracovníků bezpečnostních služeb, policistů nebo vojáků. K ochraně důležitých objektů je zřizována ostraha s nepřetržitým provozem. Fyzická ostraha společně s dobře nastavenými režimovými opatřeními zajišťuje chráněnému objektu vyšší bezpečnost a ochranu aktiv. Činnosti fyzické ostrahy mohou zahrnovat například nepravidelnou kontrolu chráněného perimetru, odhalení a zadržení narušitele, zamezení zcizení aktiv, realizaci protipožárních a havarijních opatření a kontrolní propustkovou činnost.

2.4.2 Režimová opatření

Tato opatření je možné definovat jako soubor administrativních, organizačních opatření a postupů pomocí kterých lze zajistit správné fungování systému fyzické bezpečnosti. Takto zaváděná režimová opatření, obsahují souhrn bezpečnostních postupů a pravidel, která jsou zpracována do bezpečnostních směrnic a v případě použití v AČR do stálých operačních postupů. Pro případ perimetrické ochrany se může jednat například o stanovení hranice vnějšího perimetru, poučení zainteresovaných osob o chování při vstupu do ZO atd.

Dělení režimový opatření:

- vnější režimová opatření – zahrnují vstupní a výstupní podmínky pro kontrolu pohybu osob a vozidel včetně postupů a opatření jakým způsobem kontrolu správně provádět
- vnitřní režimová opatření – zahrnují vymezení objektu nebo jeho části do kterých je umožněn vstup pouze oprávněným osobám; stanovují způsob vedení a uchování evidence o vstupu; režim manipulace s klíči a identifikačními kartami, metody osobní prohlídky, kontroly zavazadel, kontroly vozidel a nákladů



Obrázek 5 Dělení režimových opatření [11]

Režimová opatření se týkají činnosti vlastních zaměstnanců a pohybu dalších osob. Důsledné dodržování a vynucování stanovených opatření, je předpokladem pro celkovou funkčnost systému fyzické bezpečnosti. [12]

2.4.3 Technická ochrana

Jak je uvedeno v [3] je cílem technických prostředků podpora realizace režimových opatření, zkvalitnění činnost fyzické ostrahy a tím odrazení narušitele od jeho činu, případně významné ztížení činnost, nebo prodloužení doby potřebné k přístupu k chráněným aktivům.

Na technické prostředky vhodné pro použití k ochraně vnějšího perimetru, jsou kladeny vyšší nároky než na běžné technické prostředky, převážně v oblasti použití při stižených klimatických podmínkách. Pro potřeby zabezpečení perimetrické ochrany v mobilních a romístitelných pracovištích je situace výběru ještě ztížena, a to z důvodu kladení důrazu na rychlost vybudování, možnost opětovného složení a přesunu, bez závažného poškození.

Technickou ochranu, lépe řečeno technické prostředky využívané k technické ochraně je možné klasifikovat dle různých faktorů. Z mého pohledu je vhodné zmínit a dále pracovat s dělením technických prostředků dle fyzikálního principu. Jedná se aplikaci technických, elektronických a elektronicko-mechanických venkovních zabezpečovacích systémů, které je možné zařadit do následujících kategorií:

- Mechanický zábranné systémy
- Elektronické bezpečnostní systémy (poplachové systémy)

2.4.3.1 Mechanické zábranné systémy

Mechanické zábranné systémy jsou základním kamenem při tvorbě funkčního systému ochrany. Jde o vývojově nejstarší typ ochrany, který spočívá v zajištění aktiv pomocí mechanických zábran. Slouží k zabránění neoprávněnému nakládání s aktivy, případně vytvoření překážky, která ztíží přístup pachatele k chráněnému aktivu. Mechanické zabezpečovací prvky můžeme rozlišovat podle doby, po kterou jsou schopny odolat napadení pachatele, než dojde k jejich překonání, tento časový interval nazýváme průlomovou odolností. [13]

Průlomová odolnost MZS je dle [14] definována jako:

„Doba, kterou musí pachatel vynaložit na překonání mechanické pevnosti MZS se nazývá průlomová odolnost.“

Umělé oplocení

Umělá oplocení slouží k cílenému zabezpečení vstupu do perimetru vytvořené člověkem. Mohou být vyrobeny z mnoha materiálů, jako je například kov, kámen, dřevo, beton nebo umělá hmota.

Pevné bariéry (zdi)

Tato zábrana se používá převážně k ochraně velmi důležitých objektů, jako jsou například věznice, továrny, muniční sklady. Ve většině případů jsou betonové prefabrikované prvky zasazeny do předem připravených sloupků, které jsou zabetonovány do pevných základů. Takto vybudovaná zábrana jde dále pro zvýšení bezpečnosti rozšířit o oplocení, tímto nám vznikne dvojité oplocení, které může dosahovat výšky cca 5 m. Celý tento systém může být doplněn o prvky vrcholové ochrany. [13]

Obrázek 6 Příklady použití pevných bariér [15]

Ploty

Plot je člověkem vybudovaná bariéra, která má za úkol vytyčit hranici a má schopnost zabránit nebo zpomalit vstup na chráněný pozemek nepovolaným osobám. Při návrhu plotu se přihlíží k odstrašujícímu faktoru, což je vizuální vlastnost daného plotu, která působí na případného pachatele. Ploty mohou být sestrojeny z mnoha materiálů a pro zajištění fyzické bezpečnosti se používají ploty převážně z kovu tedy drátové. Drátěná oplocení se od sebe liší podle schopnosti zajištění bezpečnosti, které je dané především:

- tvarem a velikostí ok
- způsobem spoje v místě, kde se kříží oka
- kvalitou a tloušťkou materiálu
- výškou oplocení
- mobilitou [13]

Moderní ploty jsou tvořeny pevnou konstrukcí se sloupky zajištěnými proti vyvrácení a výplní z pletiva (např. čtvercové, cyklonové, svařované). Všechny kovové prvky musí být upraveny tak, aby odolávaly povětrnostním podmínkám. Dráty mohou být potaženy ochranou z umělé hmoty nebo jinak ošetřeny proti korozi. [13]

Podle typu chráněného objektu se mohou plotové systémy řadit do skupin:

- klasické drátěné oplocení (čtvercové pletivo, cyklonové pletivo, svařované pletivo)

- bezpečnostní oplocení (pletivo z vlnitého drátu, svařované zvlněné pletivo, drátěné panelové oplocení, bariéry a oplocení ze žiletkového drátu, mřížové oplocení palisádové oplocení)
- vysoce bezpečnostní oplocení (bezpečnostní plot přímého tvaru – rovný plot, bezpečnostní plot zakřiveného tvaru – zakřivený plot)
- mobilní oplocení [13]

Obrázek 7 Příklady různých typů oplocení [15]

Vstupy, vjezdy

Prvky k zajištění vstupů a vjezdů je rovněž možné rozdělit na stacionární a mobilní. Pokud se jedná o klasickou ochranu pevného perimetru můžeme sem zařadit brány, branky a vrata různých typů. Musí mít tedy tuhou konstrukci, pevné uchycení a bezpečný uzamykací systém. Ke speciálním propustím mohou patřit turnikety a závory. Vstupy a vjezdy v mobilních aplikacích jsou řešeny převážně pomocí bezpečnostních koridorů a instalací dalších bezpečnostních prvků, jako jsou například bezpečnostní železobetonové zátarasy a podobně. Tyto prvky slouží ke zpomalení a směrování potenciálních narušitelů perimetru. [13]

Vrcholová ochrana

Ochrana vrchní části plotů či zdí, která je doplňkovou ochranou zabraňující překonání mechanické zábrany přelezením. Působí na pachatele vysokým odstrašujícím dojmem. Do vrcholové ochrany zahrnujeme:

- konstrukce z ostnatého nebo žiletkového drátu
- pevné hroty
- pevné hřebeny
- otočné hroty a válce [13]

Obrázek 8 Příklady vrcholové ochrany [15]

Zábrana proti podhrabání

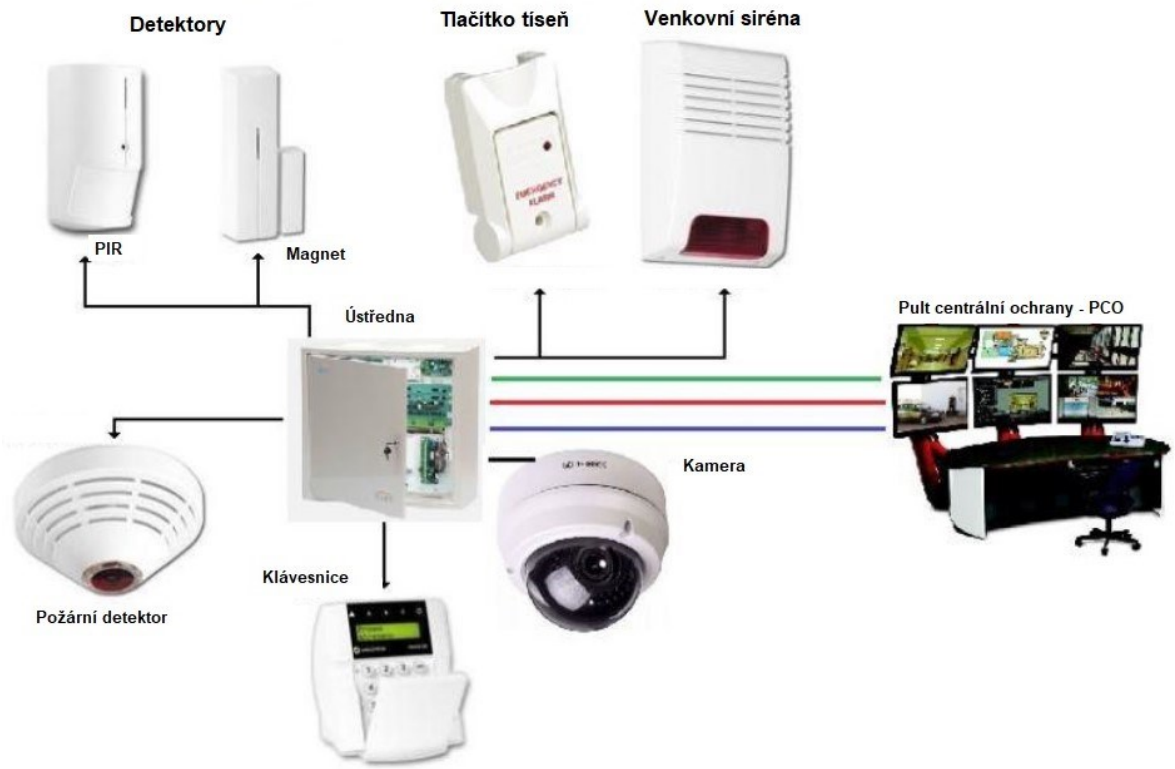
Bezpečnostní prvek vyrobený z převážně z betonu, nebo z jiného pevného materiálu, který se instaluje pod pletivo a tím zabraňuje překonání bariéry podhrabáním. [13]

Obrázek 9 Podhrabová deska [16]

2.4.3.2 Elektronické bezpečnostní systémy (poplachové systémy)

Elektronické bezpečnostní systémy perimetrické ochrany doplňují mechanické zábranné systémy a slouží k detekci, signalizaci a dohledu v případě narušení chráněného objektu. V oblasti perimetrické ochrany, kde je zajištěna trvalá přítomnost ostrahy jsou nejčastěji používány následující elektronické technické prostředky:

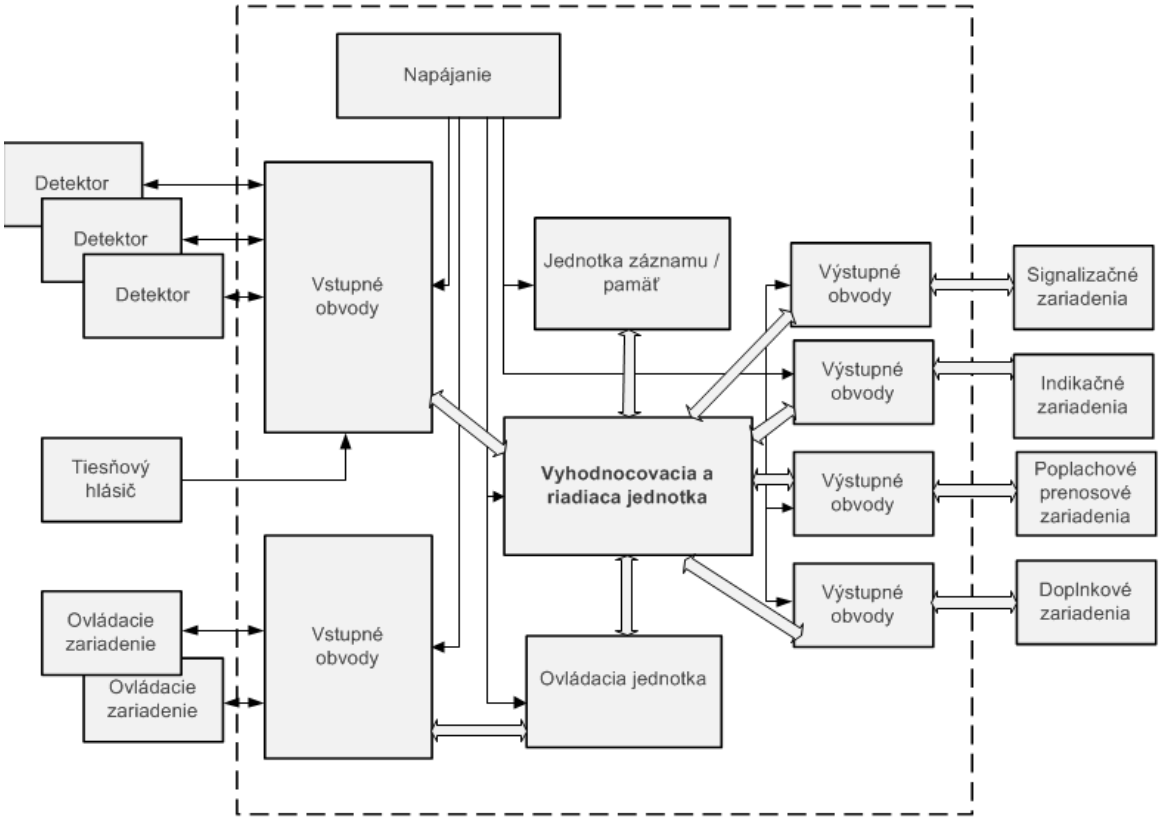
1. Poplachové zabezpečovací a tísňové systémy (PZTS)
2. Kamerové systémy (KS)
3. Elektronická kontrola vstupu (EKV)



Obrázek 10 Příklad sestavení EZS (upraveno) [17]

1. Poplachové zabezpečovací a tísňové systémy

Přidanou hodnotou využití poplachových zabezpečovacích a tísňových systémů v kombinací s mechanickými zábrannými systémy je, že informaci o narušení MZS získáme právě v době, kdy se narušitel na hranici chráněného perimetru o neoprávněné vniknutí pokouší nebo do perimetru právě vniknul. Tím docílíme zefektivnění bezpečnosti fyzické ochrany a získáme potřebný čas na vzniklou nežádoucí situaci reagovat. [3]



Obrázek 11 Blokové schéma PZTS [18]

Do skupiny technických prostředků PZTS řadíme:

- řídicí jednotky (ústředny)
- detektory narušení
- tísňová zařízení
- systémové moduly
- výstražná zařízení
- přenosová zařízení další doplňková zařízení

Řídicí jednotky (ústředny)

Ústředny PZTS jsou jádrem celého systému ochrany. Do ústředny jsou připojeny ostatní periferní zařízení, jako jsou například detektory narušení, ovládací prvky a signalizační prvky. Toto spojení je realizováno pomocí vodičů (drátově), pomocí vysokofrekvenčního signálu (bezdrátově) nebo pomocí využití obou těchto způsobů (hybridně). Drátové spojení slouží rovněž k napájení těchto periferních zařízení.

Pomocí ústředny můžeme se všemi zařízeními komunikovat, můžeme je uvádět do stavu zastřežení či klidu, a také zařízení diagnostikovat. Po přijetí poplachového signálu od detekčních prvků, ústředna signály vyhodnocuje a pokud splňují parametry pro vyhlášení poplachu prostřednictvím dostupných signalizačních prvků zabezpečí jeho vyhlášení. [19]

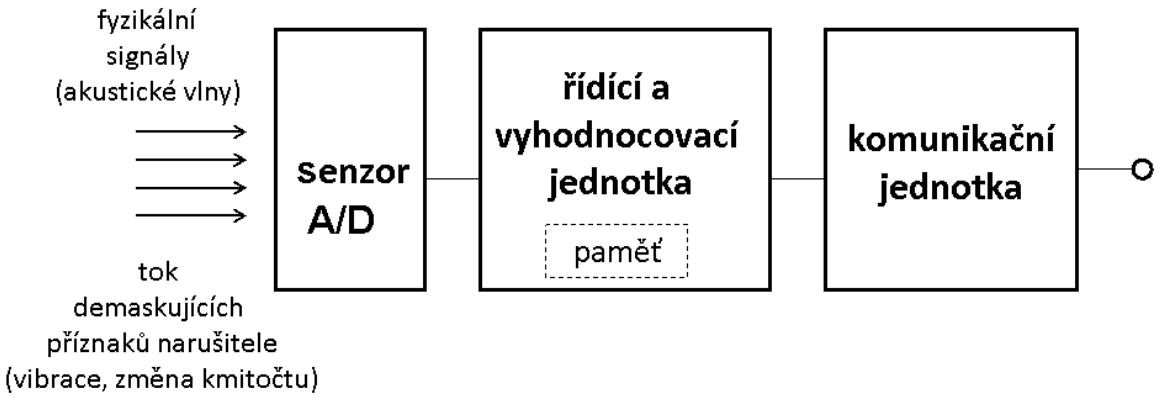
Ústředny PZTS rozdělujeme na:

- smyčkové ústředny
- ústředny s přímou adresací detektorů
- ústředny smíšeného typu
- bezdrátové ústředny [19]

Detektory narušení

Detektory narušení jsou další částí poplachových zabezpečovacích systémů. Základní funkcí detektorů je pomocí vyhodnocování fyzikálních změn v zastřeženém prostoru detekovat narušení a vyslat o tomto incidentu zprávu do řídící jednotky. [3]

Základním principem sofistikovaných detektorů je převod analogového signálu získaného z fyzikálních změn na vstupu detektoru na elektrický signál. Tento signál je pomocí řídící jednotky vyhodnocen a při splnění stanovených parametrů přes komunikační jednotku odeslán do ústředny.



Obrázek 12 Blokové schéma detektoru narušení [3]

Pro detekci narušení v perimetrickém systému ochrany jsou nejčastěji využívány infračervené a mikrovlnné závory, pasivní infračervené detektory, mikrovlnné detektory, duální detektory, štěrbinové kabely, deformační senzory, video detektory pohybu a plotové detekční systémy. [20]

Pro ochranu venkovního perimetru využíváme obvykle detektory narušení s užší detekční charakteristikou, a to pro svůj delší dosah. Musí splňovat požadavky na vyšší klimatické zatížení, být odolnější vůči falešným poplachům. Z důvodu klimatické odolnosti bývá tento typ detektorů často vybaveny vnitřním vyhříváním. Běžně je požadována voděodolnost a dokonalá těsnost, a to včetně přívodních kabelů. [3]

Detektory narušení pro perimetrickou ochranu můžeme dělit podle několika hledisek:

1. Rozdělení detektorů podle fyzikálního principu činnosti:
    - elektromechanické – pro perimetrickou ochranu je možné použít především diferenciální tlakové detektory, tenzometrické detektory, optovláknové detektory a akcelerometrické detektory
    - elektromagnetické – tento typ detektoru je založen na principu změny elektromagnetických vln při narušení chráněného perimetru narušitelem; sledovaným parametrem je změna vyzařování, přerušení paprsku a sledování odrazů elektromagnetických vln od narušitele; do skupiny těchto detektorů řadíme pasivní infračervené detektory, infračervené bariéry a závory, mikrovlnné bariéry a štěrbinové kabely
    - elektroakustické – princip těchto detektorů je založen na využití fyzikálního jevu šíření akustických tlakových vln, v perimetrické ochraně se využívá převážně šíření těchto vln po povrchu materiálu; typickým příkladem pro perimetrickou ochranu jsou mikrofonní a senzorové kabely
2. Rozdělení podle způsobu napájení:
    - napájené
        - aktivní – vyzařují signál do prostoru a tím zjišťují přítomnost narušitele; při narušení např. pohybem pachatele dojde ke změnám snímaných charakteristik v detekční zóně; nevýhodou je snadnější odhalení detektoru narušitelem a také současné použití více detektorů tohoto typu z důvodu vzájemného rušení; do této skupiny patří infračervené závory a bariéry, štěrbinové kabely, mikrovlnné detektory
        - pasivní – nevyzařují do prostoru žádný signál a na fyzikální změny v detekční zóně reagují pouze pasivně; jednou z výhod je nižší energetická náročnost a obtížnější zjistitelnost narušitelem; do této

skupiny patří pasivní infračervené detektory, mikrofonní kabely, diferenciální tlakové detektory

- nenapájené
    - destrukční – při detekci dojde k jejich trvalému zničení
    - nedestrukční – při detekci nedojde k jejich trvalému zničení

3. Rozdělení z hlediska viditelnosti detektoru pro pachatele:
    - skryté detektory
    - viditelné detektory
4. Rozdělení detektorů podle střežené oblasti:
    - prostorové – monitorování jevů ve střeženém prostoru
    - směrové – monitorování jevů v definovaném směru
    - bariérové – reakce na narušení bariéry
    - polohové – reakce na změnu polohy předmětu
5. Rozdělení detektorů podle tvaru snímací charakteristiky:
    - standardním rozsahem
    - širokoúhlým rozsahem
    - kruhovým rozsahem
    - svislou bariérou (záclonou)
    - vodorovnou bariérou
    - dlouhým dosahem [3]

Jak je vidět výše, detektory narušení je možné dělit podle mnoha hledisek a členit je do různých kategorií.

Tísňová zařízení

Tísňové hlásiče jakožto jeden z prvků technické ochrany slouží k odeslání informace o stavu ohrožení v chráněném perimetru. Odeslání tísňové informace může provést ostraha, další osoba v blízkosti tísňového hlásiče nebo neúmyslně samotný pachatel. [12]

V závislosti na účelu použití a obsluze rozdělujeme tísňové hlásiče na:

- veřejné tísňové hlásiče – na dobře viditelném místě umístěný, magnetický kontakt či mikrospínač, pomocí něhož uživatel, ostraha či jiná přítomná osoba může vyvolat tísňové hlášení; tyto veřejné hlásiče bývají pro zamezení náhodného použití opatřeny krycím sklem nebo jinou ochranou [12]

Obrázek 13 Tísňové tlačítko výklopné s pamětí poplachu [21]

- speciální tísňové hlásiče – elektromechanicky stejné jako předchozí hlásič, který je zapouzdřen do podoby tlačítka; neobsahuje ochranný kryt nebo pojistku proti nechtěnému použití, a to z důvodu nutnosti nepozorovaného spuštění tísňového hlášení v případě ohrožení zaměstnanců či ostrahy; dalším typem zařaditelným do této kategorie je osobní tísňový hlásič, který zaměstnanec nosí u sebe a v případě tísně vyhlásí poplach bezdrátově; tyto typy hlásičů je nutno pravidelně kontrolovat, nejlépe při zahájení směny [12]

Obrázek 14 Tísňové tlačítko ND100-GLT [22]

- automatické tísňové hlásiče – umožňují vyhlášení tísňového poplachu nezávisle na vůli obsluhy; tyto tísňové hlásiče se hojně využívány v bankovním sektoru [12]

Obrázek 15 Detektor poslední bankovky [23]

Systémové moduly (napájecí zdroje, vstupní a výstupní moduly)

Napájecí jednotka zajišťuje stabilní a trvalé napájení všech obvodů ústředen a ostatních kabelově připojených zařízení (detektorů, tísňových hlásičů, ovládacích, signalizačních a doplňkových zařízení). Hlavní obvody musí být dostatečně zálohovány náhradním zdrojem napětí. K tomuto účelu se používají bezúdržbové akumulátory.

Výstražná zařízení (majáky, sirény)

Zařízení, která na základě vyhlášení poplachového stavu produkují akustický nebo světelný poplachový signál. Úroveň akustického výkonu je velmi vysoká a slouží pro maximální znepříjemnění pobytu narušitele v prostoru nebo výrazné upozornění ostrahy na poplach. Jejich použití můžeme rozdělit na venkovní a vnitřní. U akustických zařízení je obvykle základním prvkem piezoelektrický akustický měnič doplněný o generátor kolísavého tónu a výkonový měnič. Výstražná zařízení se instalují na nedostupná místa, aby nebylo snadné je zničit či demontovat. [12]

Obrázek 16 Sirény a majáky [24]

Přenosová zařízení

Přenosová zařízení slouží k obousměrné komunikaci, přenosu poplachů a povelů mezi poplachovým systémem a vyhodnocovacím systémem přijímacího centra.

Další doplňková zařízení

Další doplňková zařízení jsou zařízení, která doplňují ovládání poplachového zabezpečovacího a tísňového systému (klávesnice, dálkové ovladače, tlačítka, biometrické prvky, čtečky karet a klíčenky).

Obrázek 17 Příklad dalších zařízení (upraveno) [25]

2. Kamerové systémy

Dříve převážně označován zkratkou CCTV (uzavřený televizní okruh) je integrován do bezpečnostních aplikací z důvodu dohledu nad chráněným prostorem a následné vizuální kontrole pachatele při vzniku narušení. V případě narušení umožňuje záznam pachatele. Záznam může následně sloužit jako důkazní materiál pro orgány policie. V dnešní době je na trhu dostatečné množství kamer v různých cenových relacích a širokou škálou funkcí. [26]

Složení kamery:

- objektiv
- obrazový senzor (CCD, CMOS, DPS)
- elektronická část s mikroprocesorem [26]

Klíčové parametry kamer

Noční vidění – díky infračervenému přísvitu instalovanému buď přímo do těla kamery nebo samostatně plní svoji funkci i v noci.

Objektiv – na trhu se vyskytují IP kamery s nevyměnitelnými a vyměnitelnými objektivy. Další možností jsou kamery s fixním objektivem (nelze změnit úhel záběru) anebo kamery s varifokálním objektivem, kde úhel zabíraného prostoru kamerou může být měněn.

WDR – kamery s funkcí WDR snímají obraz v širokém kontrastním poměru, což umožňuje využít kamery například i v místech s protisvětlem. Na trhu můžeme nalézt kamery s hardwarovým WDR (lepší, nákladnější) a se softwarově řešeným WDR (levnější, s nejasnými výsledky). [27]

Komprese obrazu – standardem u IP kamer je komprese obrazu pomocí kodeků H.264 a H.265. Rozdíl mezi velikostmi datových toků u těchto kodeků je cca 50 % ve prospěch kodeku H.265. V současnosti některém kamery využívají ke kompresi kodek H.265+, který je v závislosti na zabírané scéně úspornější o dalších cca 80 %. [28]

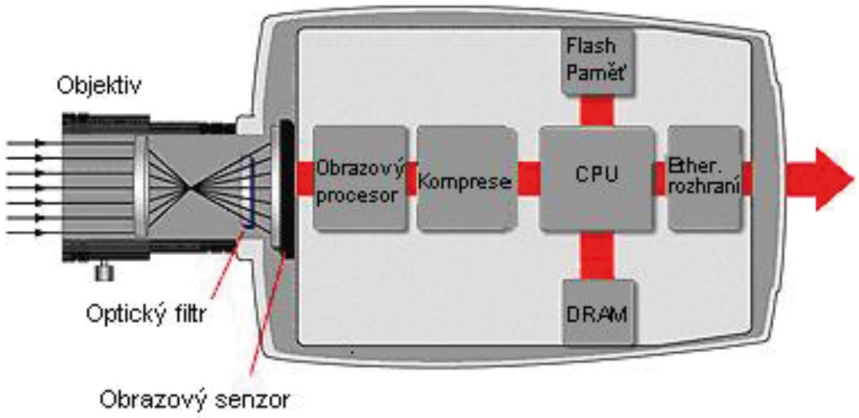
Redukce šumu – ve stižených světelných podmínkách dokáže potlačit šum obrazu.

Odmlžení obrazu – vyvažuje světelnost obrazu.

Kompenzace protisvětla – IP kamera bez WDR nedokáže v případě působení protisvětla zaznamenat celou scénu v dobré kvalitě. Musíme tedy zvolit preferenci části scény, která nás zajímá. Například venku za otevřenými dveřmi v prudkém světle (místnost bude tmavá) nebo co je ve tmavé místnosti, když jsou otevřené dveře (oblast u dveří bude přesvícená).

Elektronická stabilizace obrazu – v případě instalace IP kamery na nestabilní místo, jako jsou sloupy a podobně je obraz softwarově stabilizován.

Otočení obrazu – slouží k otočení obrazu na výšku například pro zabezpečení obvodu budov, nákladových ramp, příjezdových cest a podobně. [29]



Obrázek 18 Schéma principu činnosti IP kamery [30]

V oblasti bezpečnostních technologií probíhá neustálý rozvoj a ani kamery nejsou výjimkou. Dříve používané analogové kamery jsou nahrazovány moderními digitálními kamerami, které mohou být drátové či bezdrátové, jsou postaveny na přenosu digitálního signálu pomocí IP protokolu. Umožňují například rozpoznání osob, SPZ vozidel, detekci pohybu a vzdálený dohled pomocí internetu. Tento typ kamer je možné chápat jako samostatný počítač s kamerou. Má vlastní MAC a IP adresu díky čemuž je umožněna komunikace po síti. [29]

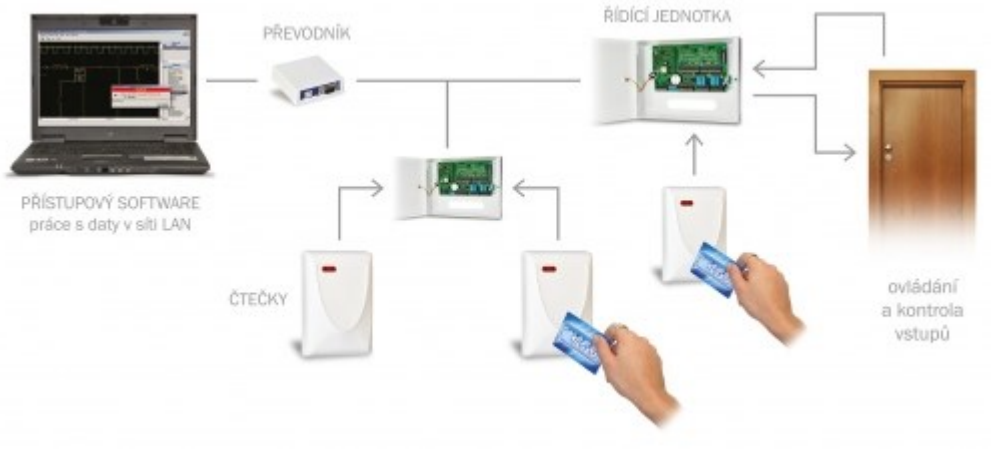
Trendy v oblasti kamerových systémů

Dnešní trendy v oblasti kamer se převážně zaměřují na několik zásadních oblastí. Jednou z oblastí je kybernetická bezpečnost kamerových systémů. Rozšiřují se pokročilé funkce a kamery jsou díky algoritmům a dostatečnému výpočetnímu výkonu schopny odhalit nebezpečný firmware, kterým se útočník snaží napadnout kameru a získat ji pod svoji kontrolu. Zároveň jsou kamery připraveny na ochranu celého systému tím, že umožňují infikované zařízení v systému rozpoznat, škodlivé zařízení nahlásit a tím ochránit ostatní prvky systému. Dalším významným inovativním prvkem je pokročilá komprese videa, kdy výrobci neustále inovují nové algoritmy. Neustálá inovace také probíhá v oblasti vylepšování kvality obrazu ve stižených světelných podmínkách.

3. Elektronická kontrola vstupu

Elektronická kontrola vstupu (EKV) je bezpečnostní systém sloužící k a regulaci vstupů osob do objektu. Umožňuje také monitorování pohybu osob v definovaných částech objektu nebo zónách. Na základě definovaných oprávnění EKV umožňuje autorizovaným osobám, po jejich identifikaci, přístup do příslušných prostor, zatímco ostatním je přístup zamítnut. Elektronická kontrola vstupu se v dnešní době stává standartním vybavením každého podniku nebo organizace. Výstupy z této aplikace bývají často využívány pro docházkové

systémy a pro přehled o přítomnosti a docházce zaměstnanců na pracovišti. Ověřování přístupových údajů může probíhat pomocí širokého spektra různých technologií, jako například zadání hesla do klávesnice, přiložení identifikační čtečky nebo karty, biometrické skenování, pomocí fyzického či elektronického klíče, ale také kombinací těchto metod. [31]



Obrázek 19 Příklad jednoduché aplikace EKV [32]

Dílčí závěr

Cílem této kapitoly bylo analyzovat začlenění perimetrické ochrany v systému ochrany referenčních objektů. Také objasnit z jakých prvků fyzické ochrany je perimetrická ochrana složena. A poskytnout detailnější teoretický aparát z oblasti prvků fyzického zabezpečení. Práce je dále detailněji směřována na prostředky perimetrické ochrany v systému ochrany fyzické bezpečnosti v polních podmínkách.

II. PRAKTICKÁ ČÁST

3 ANALÝZA ZAJIŠTĚNÍ NESTACIONÁRNÍ PERIMETRICKÉ OCHRANY V POLNÍCH PODMÍNKÁCH

Cílem diplomové práce je vytvoření návrhu systému perimetrické ochrany, který je součástí systému ochrany operačního střediska vrtulníkové letky v polních podmínkách pomocí vhodné perimetrické ochrany. Zajištění správně fungující perimetrické ochrany je možné docílit pomocí vhodné kombinace správně zvolených režimových opatření, činností ostrahy a technických prostředků, propojených vhodnými vazbami. Tato kapitola je zaměřena na analýzu technických prostředků, jejich parametrů a určení vhodnosti k zajištění nestacionární perimetrické ochrany v polních podmínkách. Z důvodu **omezené přepravní kapacity, jednoduchosti instalace a pořizovacích nákladů** je požadováno, aby byl systém ochrany tvořen následujícími technickými prostředky:

- mechanické zábranné systémy
- kamerový systém
- PZS s jedením typem perimetrických detektorů

Z důvodu rozsahu a stanoveného cíle diplomové práce nebude předmětem analýzy ústředna PZS a ostatních dílčí prvky PZS (jako jsou systémové moduly, výstražná zařízení atp.). Všechny prvky kamerového systému a PZS jsou pomocí strukturované kabeláže svedeny na pracoviště ostrahy RED, kde je umístěna ústředna i ostatní prvky PZS. V kontejneru ostrahy RED vykonává ostraha v nepřetržitém provozu službu.

3.1 Analýza technických prostředků jejich parametry a vhodnost

Pro praktickou aplikaci se v současné době nabízí rozsáhlý sortiment technických prostředků. Každý z nich má v závislosti na fyzikálním principu činnosti své výhody a nevýhody. Volba vhodného typu technických prostředků, pro konkrétní úlohu zabezpečení, závisí na zkušenostech a odborných znalostech navrhovatele systému perimetrické ochrany a na provozních podmínkách, které budou systém při jeho fungování ovlivňovat. Všechny vhodné prostředky instalované ve venkovních prostorech musí splňovat kategorizaci zařízení pro třídu prostředí IV. – Venkovní všeobecné a prvky které budou instalovány do kontejnerů třídu prostředí III. – Venkovní chráněné, a to převážně z důvodu velkých změn teplot a vlhkosti. Rozmístitelné části zařízení (ploty, detektor, kamery) musí být jednoduše sestavitelné, instalovatelné a opět rozložitelné a uložitelné s minimálními požadavky na doplňkové práce (např. výkopy, úpravu terénu).

3.1.1 Mechanické zábranné systémy nestacionární perimetrické ochrany

Jak bylo řečeno ve druhé kapitole mezi běžně používané mechanické zábranné systémy řadíme plotové systémy a zdi, jež mohou být v případě potřeby doplněny o brány, branky, ale také například žiletkové bariéry a různé typy vrcholových a podhrabových zábran. V nasazení těchto prvků k perimetrické ochraně rozmístitelných nebo mobilních prostředků, u kterých je kladen důraz na rychlost výstavby, omezený skladovací prostor a poměrně velkou flexibilitu při opuštění místa rozmístění se prostor výběru rapidně zužuje. Mechanické zábranné systémy můžeme pro naše potřeby rozdělit na stacionární (pevně zabudované) a mobilní (romístitelné, jednoduše smontovatelné a demontovatelné). Pro naše potřeby volíme pouze variantu mobilní. Musíme také přihlédnou k rozměrovým hodnotám plotu, zvolíme minimální výšku plotového dílce 2,15 m. Nižší ploty by nezabezpečovaly dostatečnou ochranu proti přelezení.

V našem případě můžeme uvažovat o použití následujících typů plotů a doplňků:

- mobilní oplocení Standard
- F2: standardní průhledný plot
- F2: střední průhledný plot
- F3: standardní a střední průhledný plot se středovou trubkou
- F4 secure: bezpečnostní plot proti přelezení
- F5 maxi: doplňkový průhledný plot
- mobilní oplocení vysoké bezpečnosti
- mobilní žiletková bariéra
- nástavec na ostnatý drát

3.1.1.1 Mobilní oplocení Standard

Plotové dílce mobilního oplocení Standard jsou vhodné pro oplocení různých akcí, kde nepředpokládáme vysokou zátěž. Z důvodu volby materiálu je jeho výhodou snadná manipulace.

Mobilní oplocení je možné ustavit za pomocí betonové patky, plastové patky nebo kovové patky. Spojení dílců je zabezpečeno mobilní spojkou. [33]

Technická specifikace plotového dílce:

- Šířka x výška: 3450 x 2020 mm
- Šířka x výška oka: 100 x 262 mm
- Průměr drátu vodorovný: 3,2 mm
- Průměr drátu svislý: 2,2 mm
- Průměr trubky vodorovný: 25,0 x 1,25 mm
- Průměr trubky svislý: 38 x 1,25 mm
- Hmotnost: 11,2 kg

Obrázek 20 Mobilní oplocení Standard 3,45 x 2,02 m [33]

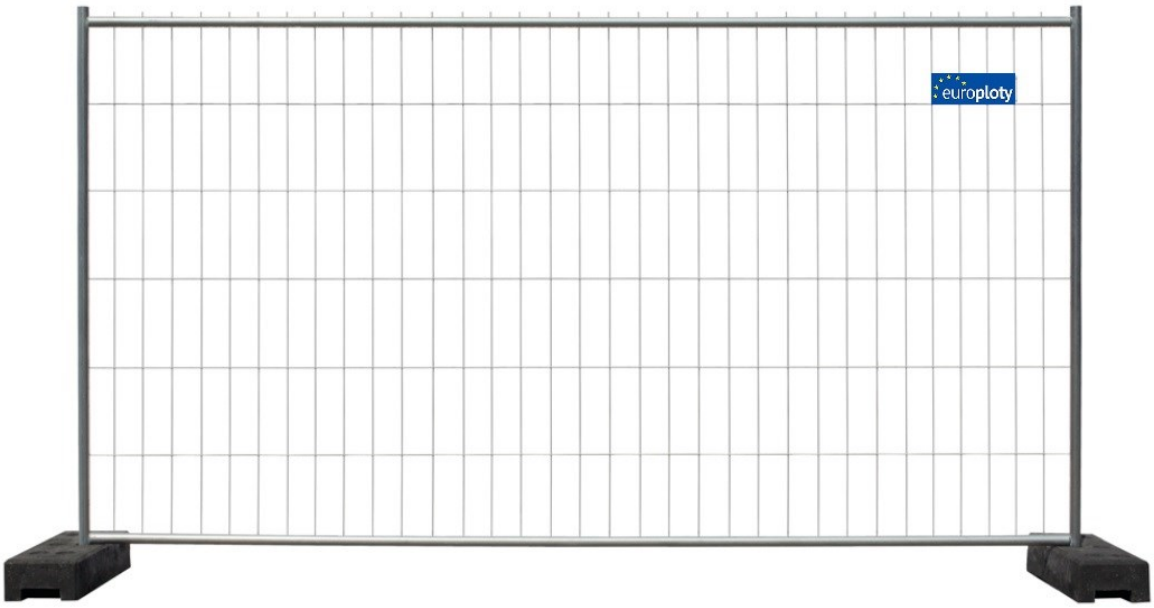
Tento plot je z důvodu nevhodné volby materiálu nedostatečně stabilní. Rovněž rozměr ok by nezabezpečil ochranu proti přelezení. Pro naše potřeby je **nevhodný**.

3.1.1.2 F2: Standardní průhledný plot

Tento standardní průhledový plot má stejné rozměry, je vyroben ze silnějších materiálů, jeho konstrukce je proto pevnější, ale na druhou stranu je o něco těžší což stěžuje manipulaci. Usazení a spojení je stejné.

Technická specifikace plotového dílce:

- Šířka x výška: 3454 x 2000 mm
- Šířka x výška oka: 100 x 300 mm
- Průměr drátu vodorovný: 4 mm
- Průměr drátu svislý: 3,5 mm
- Průměr trubky vodorovný: 27,0 x 1,5 mm
- Průměr trubky svislý: 41,5 x 1,5 mm
- Hmotnost: 16 kg [34]



Obrázek 21 F2: standardní průhledný plot [34]

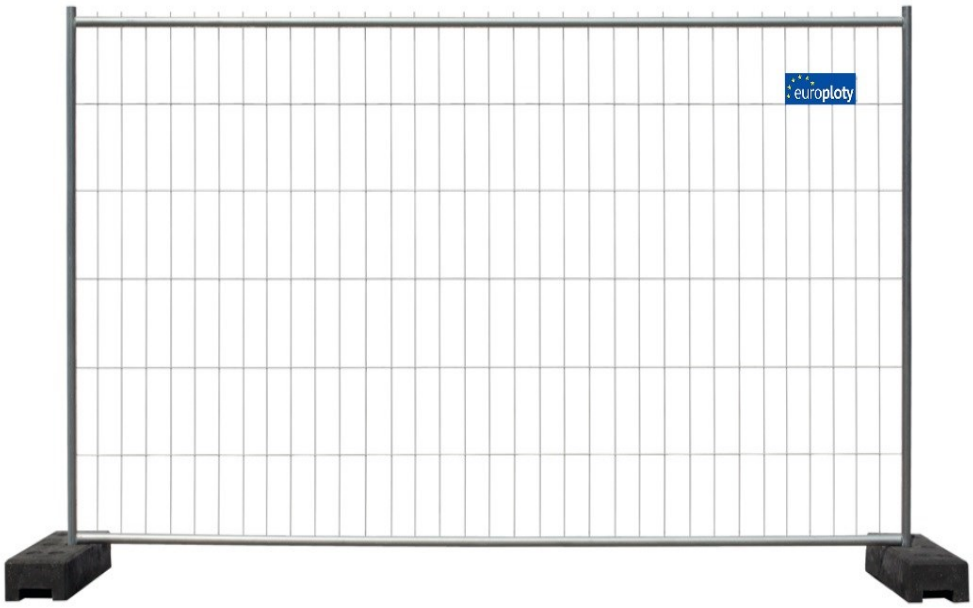
Plot této řady nabízí rozměrově stejné parametry jako předchozí, je ovšem vyroben ze silnějších materiálů. Opět je pro naši aplikaci **nevhodný,** protože nenabízí dostatečnou výšku.

3.1.1.3 F2: Střední průhledný plot

Střední průhledový plot je užší, je vyroben ze silnějších materiálů, jeho konstrukce je proto pevnější o něco těžší což stěžuje manipulaci. Positivem je menší šířka a tím pádem lepší skladnost. Usazení a spojení je stejné.

Technická specifikace plotového dílce:

- Šířka x výška: 2200 x 2000 mm
- Šířka x výška oka: 100 x 300 mm
- Průměr drátu vodorovný: 4 mm
- Průměr drátu svislý: 3,5 mm
- Průměr trubky vodorovný: 27,0 x 1,5 mm
- Průměr trubky svislý: 41,5 x 1,5 mm
- Hmotnost: 11,5 kg [34]

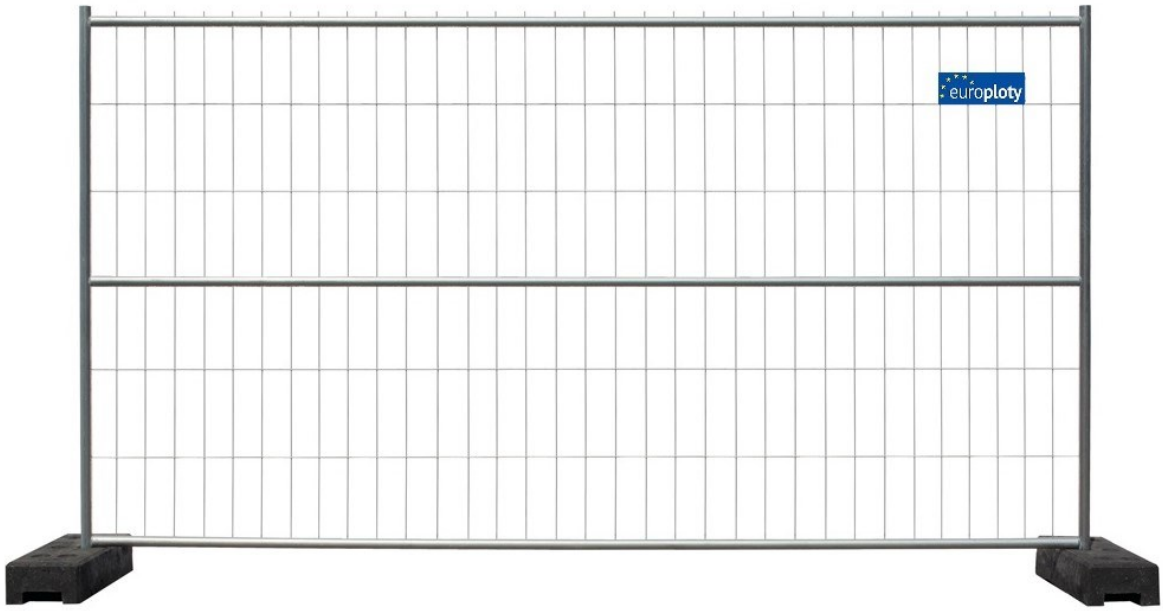


Obrázek 22 Střední průhledový plot [34]

Díky své výšce je tento plot také, pro naší aplikaci **nevhodný**.

3.1.1.4 F3: Standardní a střední průhledný plot se středovou trubkou

Standardní mobilní plotový panel s dodatečnou vodorovnou výztuhovou trubkou pro větší tuhost parametry jsou stejné jako u předchozích dvou plotů typu F2. [34]



Obrázek 23 F3 Standardní a střední průhledný plot se středovou trubkou [34]

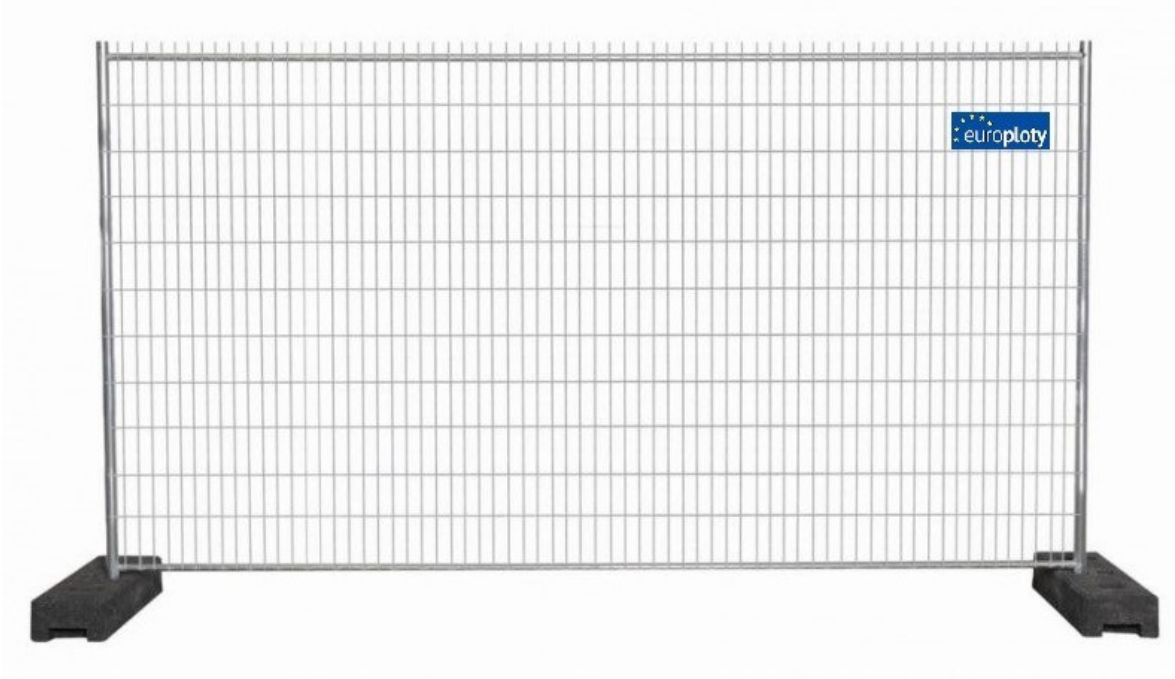
Opět díky velikosti ok malé výšce je pro nás **nevhodný**.

3.1.1.5 F4 secure: bezpečnostní plot proti přelezení

Mobilní plotový panel od stejného výrobce proti přelézání s menšími oky v pletivu. Tento plot je díky větší hustotě ok pevnější. Jeho nevýhodou je větší hmotnost a horší manipulace. Není vyráběn v užší variantě.

Technická specifikace plotového dílce:

- Šířka x výška: 3454 x 2000 mm
- Šířka x výška oka: 30 x 160 mm
- Průměr drátu vodorovný: 3 mm
- Průměr drátu svislý: 3 mm
- Průměr trubky vodorovný: 27,0 x 1,5 mm
- Průměr trubky svislý: 41,5 x 1,5 mm
- Hmotnost: 24 kg [34]



Obrázek 24 F4 secure: bezpečnostní plot proti prolezení [34]

Tento plot již disponuje užšími oky, které zabezpečují obtížnější přelezení, ale jeho výška není pro naší aplikaci dostatečná. Je pro nás **nevhodný**.

3.1.1.6 F5 maxi: doplňkový průhledný plot

Mobilní plotový panel s dodatečnou vodorovnou výztuhovou trubkou a menšími pletivovými oky ve zvýšené variantě.

Technická specifikace plotového dílce:

- Šířka x výška: 3454 x 2450 mm
- Šířka x výška oka: 50 x 300 mm
- Průměr drátu vodorovný: 4 mm
- Průměr drátu svislý: 4 mm
- Průměr trubky vodorovný: 27,0 x 1,5 mm
- Průměr trubky svislý: 41,5 x 1,5 mm
- Hmotnost: 33 kg [34]

Obrázek 25 F5 maxi: doplňkový průhledný plot [34]

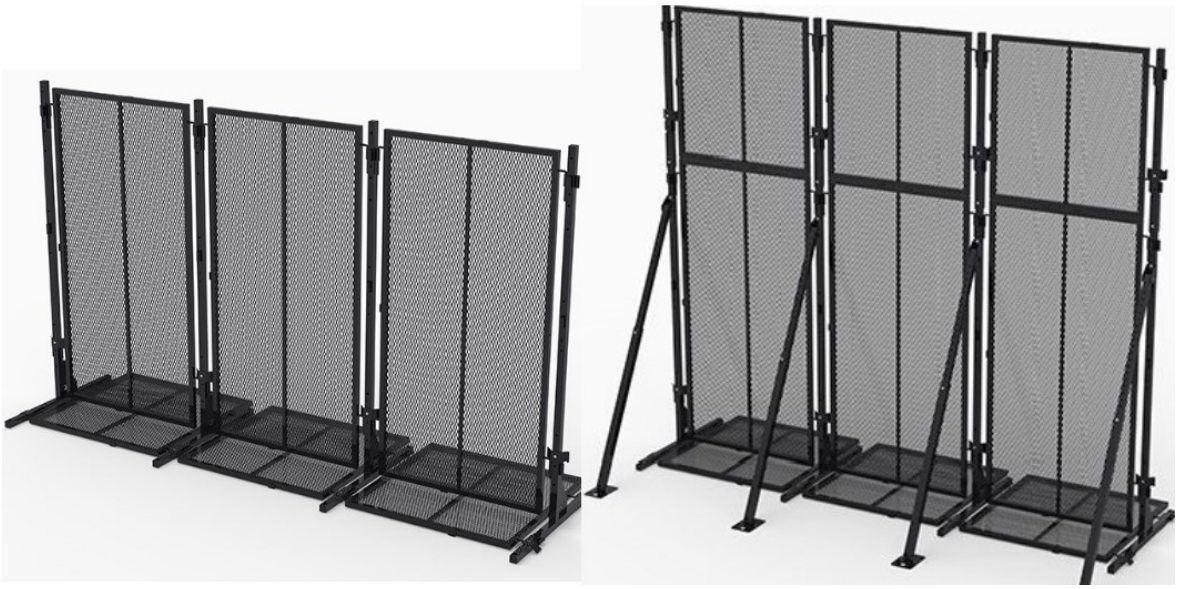
Tento plot je díky své výšce, menším okům a síle materiálu pro naši aplikaci **vhodný** nevýhodou může být vyšší hmotnost.

3.1.1.7 Mobilní oplocení vysoké bezpečnosti

Mobilní oplocení, které je nabízeno v několika variantách. Pro naši potřebu a našim podmínkám vyhovují varianty, které jsou zobrazené na obrázek 13. Tento plot je robustní, stabilní a velice modulární. Jeho nevýhodou je poměrně velká hmotnost.

Technická specifikace plotového dílce:

- Šířka x výška: 3454 x 2430/3066 mm
- Šířka x výška oka: 10 x 10 mm
- Průměr drátu vodorovný: 2 mm
- Průměr drátu svislý: 2 mm
- Hmotnost: 53/63 kg



Obrázek 26 Mobilní oplocení vysoké bezpečnosti [35]

Tento plot je také **vhodný** pro zabezpečení perimetru, a to převážně díky své pevnosti, výšce a stabilitě.

3.1.1.8 Mobilní žiletková bariéra

Doplňkovou možností je použití plotu s kombinací se žiletkovou mechanickou zábranou složenou ze tří žiletkových válců. Výška je 130 cm a délka 8 až 9 m. Ochranu proti korozi zajišťuje zinková úprava. Tento systém je velice rychle rozložitelný v řádu několika vteřin. [36]

Obrázek 27 Mobilní žiletková bariéra [36]

3.1.1.9 Nástavec na ostnatý drát

Nástavec představuje zahnuté rameno pod úhlem 45 stupňů. Nástavec se usazuje na plotový sloupek o průměru do 48 mm. Na tento nástavec se následně upevní tři řady ostnatého drátu. Délka ramene je 45 cm. [37]

Obrázek 28 Nástavec na ostnatý drát [37]

3.1.2 Elektronické bezpečnostní systémy nestacionární perimetrické ochrany

I u detektorů narušení je nutné přihlížet nejen k technickým vlastnostem, ale i ke vhodnosti pro mobilní aplikaci. Při rozhodování se do popředí dostávají typy detektorů, které budou funkční, snadno a znovu aplikovatelné, budou odolávat zvýšené námaze při častější manipulaci a v neposlední řadě možným ztíženým klimatickým podmínkám. V následující kapitole jsou analyzovány elektronické bezpečnostní systémy, které se v oblasti perimetrické ochrany používají. U vhodných technologií jsou uvedena konkrétní zařízení a definovány jejich parametry a vlastnosti.

3.1.2.1 Diferenciální tlakový detektor

Detektor je tvořen dvojicí nemrznoucí kapalinou naplněných a natlakovaných, pružných hadic. Při narušení perimetru dochází k rozdílnému zatížení hadic, vzniká zde rozdíl tlaků, který je vyhodnocován a zpracováván řídícím systémem perimetrického systému. Tento typ detektoru je vhodný k zabezpečení perimetrické ochrany rozsáhlého členitého terénu. Pro naší aplikaci je zcela **nevhodný**, a to z důvodu nutnosti zapouštění tlakových hadic pod povrch země.

3.1.2.2 Tenzometrický detektor

Detektor ze skupiny pasivních kontaktních detektorů pracuje na principu vyhodnocování změn odporu při narušení (např. přestřihávání, natažení) plotu. Detektor je začleněn do plotového tenzometrického systému, kde mechanické působení na dráty způsobí změnu odporu. Tato je neustále vyhodnocována a pokud překročí stanovenou mezní hodnotu dojde k vyhlášení poplachu.

Tenzometrické detektory **nejsou vhodné** k nestacionární perimetrické ochraně, a to z důvodu náročnosti montáže a podmínek, jak musí být montáž provedena. Řádně napnuté dráty plotu je nutné upevnit do tenzometrickách detektorů. K tomu je vhodné použít pevně

zabudované sloupky. Tyto podmínky nejsme u mobilního plotového systému v žádném případě schopni dosáhnout.

3.1.2.3 Optovláknový detektor

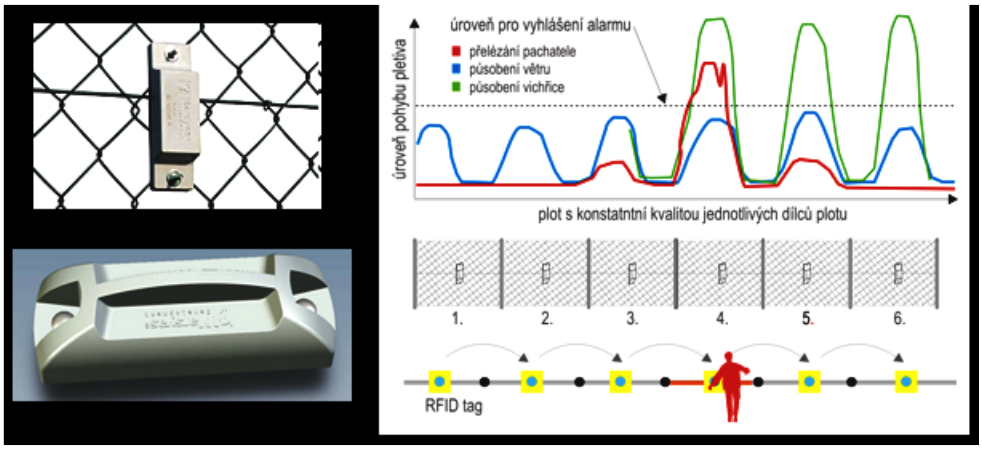
Optovláknové perimetrické detektory využívají ke své činnosti optická vlákna, jež jsou umístěna do země. Při pokusu o narušení dochází k mechanickému působení na optické vlákno a tím ovlivnění měřeného signálu na výstupu. Tyto signály jsou vyhodnocovány, po překročení stanovené hranice je vyhlášen poplach. [38]

Obrázek 29 Detekční systém s optovláknovým zemním/plotovým kabelem. [38]

Další z typů detektorů, který je pro použití v nestacionární perimetrické ochraně **zcela nevhodný** z důvodu nutnosti instalace optických drátů do země.

3.1.2.4 Plotový detekční systém – akcelerometrický detektor

Akcelerační detektor obsahuje RFID čip a 3-osý akcelerační senzor s elektronickým gyroskopem. Zařízení RFID jsou spolu s akcelerometry připevněno na konstrukci plotu. Akcelerometry měří vibrace plotu a pomocí RFID čipu, s využitím komunikace se sousedními RFID čipy, dochází k přenesení informace rádiovým kanálem do ústředny. Poplach je vyhlášen, pokud vyhodnocovaný signál odpovídá typem a amplitudou nastavenému signálu v řídícím systému. Detektory automaticky měří mechanickou kvalitu plotu, která se poté SW kalibruje a tím se eliminuje vyhlašování falešných poplachů. [39]



Obrázek 30 Plotový bezdrátový systém [38]

Tento plotový systém ochrany nemá žádné nevýhody, které by zabraňovaly jeho využití v ochraně perimetru mobilních prostředků a je pro naše využití **vhodný**. RFID technologii pro perimetrickou ochranu dodává firma Ronyo Technologies. Název produktu je Varia Perimeter a má tyto vlastnosti uvedené v tabulce 1.

Tabulka 1 Parametry detektoru FLA

Parametr	**Popis**
Prostředí	venkovní
Typ detektoru	3-osý akcelerační senzor
Radiová frekvence	868 MHz
Zdroj integrovoný/záložní	ano/ne
Výdrž baterie	cca 8let
Maximální počet detektorů	600
Nastavení pomocí PC	ano
Teplota provozní	-25 až +70 °C
Stupeň krytí	IP67
Typ výstupu	antimasking, poplach, porucha, tamper
Šířka/výška/hloubka	16,3/5,2/4,2 cm
Hmotnost	0,98 kg

3.1.2.5 Pasivní infračervený detektor

Pasivní infračervený detektor je schopen lokalizovat a vyhodnotit změny v infračervené části spektra, které vznikají při pohybu narušitele v detekčním prostoru. Detekčním prvkem zařízení je pyroelement. Pro zabezpečení detekce je snímaný prostor pomocí optiky segmentován na zóny. Dosah běžných PIR detektorů pro vnitřní použití je do 100 m. Venkovní pasivní infračervené detektory jsou vybaveny rozdílnou optikou, která dokáže prodloužit detekci až do vzdálenosti 200 m. Detektory pro vnější použití jsou obecně dražší, a to i z důvodu potřeby vyšší mechanické a klimatické odolnosti. [3]

Obrázek 31 Venkovní digitální PIR typ PRO E-100 H [40]

Tyto detektory jsou pro nestacionární, perimetrickou ochranu **vhodné**, jisté problémy vidím v použití tohoto detektoru v nepříznivých klimatických podmínkách, kde by mohlo docházet k vyššímu počtu planých poplachů. Dle parametrů jsem vybral detektor uvedený na obrázku 31.

Tabulka 2 Parametry digitálního PIR detektoru PRO E-100 H

Parametr	**Popis**
Prostředí	venkovní
Typ detektoru	PIR
Typ čočky	dlouhý dosah, křemíková, záclona
Dosah	21-150 m
Zdroj integrovoný/záložní	ne/ne
Integrované nastavování	ano
Integrovaná paměť historie	ano
Proud při poplachu	18 mA
Nastavení pomocí PC	ano
Napájecí napětí	12-24V DC, 24V AC
Teplota provozní	-20 až +65 °C / -40 až +65 °C
Rozhraní	RS485
Stupeň krytí	IP65
Typ výstupu	antimasking, poplach, porucha, tamper
Šířka/výška/hloubka	18,5/29/35,8 cm
Hmotnost	0,98 kg

Výše uvedený venkovní digitální PIR detektor poskytuje analýzu signálu pro střední a dlouhé vzdálenosti. Je zde možnost využít volby detekční charakteristiky typu „vějíř“ nebo typu „záclona“. Tento detektor je osazen kvalitní zrcadlovou optikou (verze H disponuje vyhříváním a křemíkovou čočkou), zabezpečuje antimasking, ochranu prostoru pod detektorem, detekuje změny pozice detektoru. Instalace je možná ve výšce od 2,5 až 4 m. Zařízení je dodáváno se stojanem pro skrytou montáž kabeláže a pro instalaci na sloupek nebo stěnu. Nastavení a testování detektoru je řešeno pomocí SW, který je součástí převodníku IFM-485-ST. [40]

3.1.2.6 Mikrovlnný a dvojitý mikrovlnný detektor

Tyto typy mikrovlnných detektorů se skládají z vysílače, přijímače a z vyhodnocovací elektroniky, umístěných ve schránce. Pracuje ve frekvenčním pásmu v okruhu 9,5 GHz. Vysílaný signál je vyzařován ve formě elektromagnetických vln plochou anténou. Odražené elektromagnetické vlny jsou přijímány a porovnávány s frekvencí vysílání. Pokud dojde vlivem vniknutí do zabezpečeného prostoru ke změnám kmitočtu přijímaného signálu, je vyhlášen poplach. Pro eliminaci planých poplachů se tyto detektory používají dvojitě. Tento dvojitý detektor obsahuje dva přijímací kanály, které pracují s amplitudově modulovaným signálem na pěti nosných frekvencích v pásmu kolem 10,5 GHz. Takto zvolený dvojitý detektor při zpracování signálu potlačuje vyhlašování planých poplachů při pohybu drobné zvěře, porostů a větví stromů. [12]

Obrázek 32 Digitální mikrovlnný detektor Murena [41]

Tyto detektory jsou pro nestacionární, perimetrickou ochranu **vhodné**, dle výrobce jsou zcela použitelné i v případě silných dešťů. Na obrázku je znázorněn digitální mikrovlnný detektor Murena, který je pro naší aplikaci použitelný.

Tabulka 3 Parametry digitálního mikrovlnného detektoru Murena

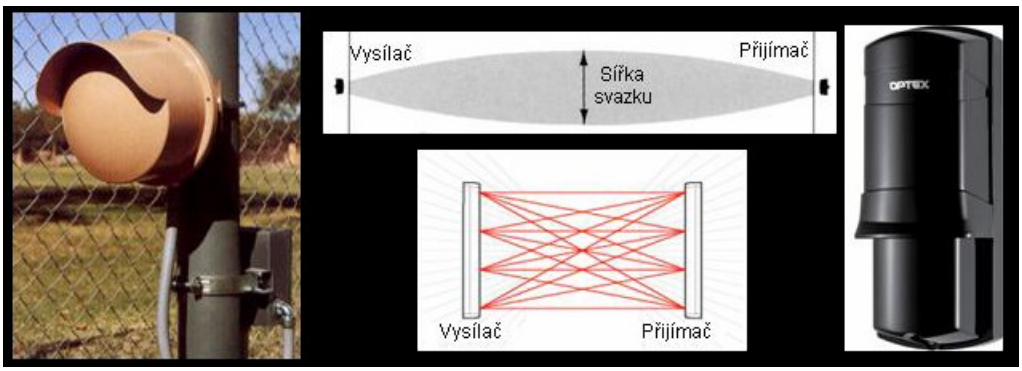
Parametr	**Popis**
Prostředí	venkovní
Typ detektoru	Doppler detektory s deskovou anténou
Frekvenční pásmo	X-band 9,9 GHz
Dosah	24 m
Zdroj integrovoný/záložní	ne/ne
AGC (aut. zesílení signálu)	ano
Integrované nastavování	ano
Integrovaná paměť historie	ano
Proud při poplachu	70 mA
Nastavení pomocí PC	ano
Napájecí napětí	10-14V DC, 12V AC
Teplota provozní	-35 až +65 °C
Rozhraní	RS485

Stupeň krytí	IP55
Typ výstupu	antimasking, poplach, porucha, tamper
Šířka/výška/hloubka	17,5/17,5/11,5 cm
Hmotnost	0,5 kg

Tento digitální mikrovlnný detektor pracuje s dvojí frekvencí a pomocí vyhodnocení Dopplerovského jevu je schopen detekovat vzdálenost, velikost a směr pohybu narušitele. Detektory jsou dodávány ve dvou základních variantách. První je s vyzařovací charakteristikou ve tvaru „vějíře“ pro pokrytí prostoru. Druhá, s vyřazovací charakteristikou ve tvaru „záclony", je vhodná pro ochranu fasád a vchodů objektů. Detektory jsou vybaveny doplňkovou analýzou pro vyhodnocení detekovaného signálu Fuzzy Logic. Detektory s označením PLUS disponují navíc integrovanou pamětí historie a průběhů a sběrnicí RS485 pro vzdálenou správu. [41]

3.1.2.7 Infračervená a mikrovlnná bariéra/závora

Infračervené a mikrovlnné bariéry/závory patří do skupiny přehradných detektorů. Jedná se o samostatně stojící nadzemní zařízení, které se obvykle umisťuje podél hranice chráněného perimetru. Tato zařízení jsou vždy složena z vysílače a přijímače. Vysílač vysílá do prostoru podél hranic střeženého pozemku svazek záření v mikrovlnném nebo v infračerveném pásmu. Protější zařízení vybavené přijímačem měří intenzitu tohoto záření. Narušitel při překonávání prostoru mezi vysílačem a přijímačem zastíněním ovlivní změnu intenzity přijímaného signálu do přijímacího záření, čímž je detekováno narušení perimetru a vyhlášen poplach. Moderní systémy emitované záření modulují čímž obě zařízení mohou i navzájem komunikovat (např. zvýšit intenzitu záření, pokud začíná padat mlha). [38]



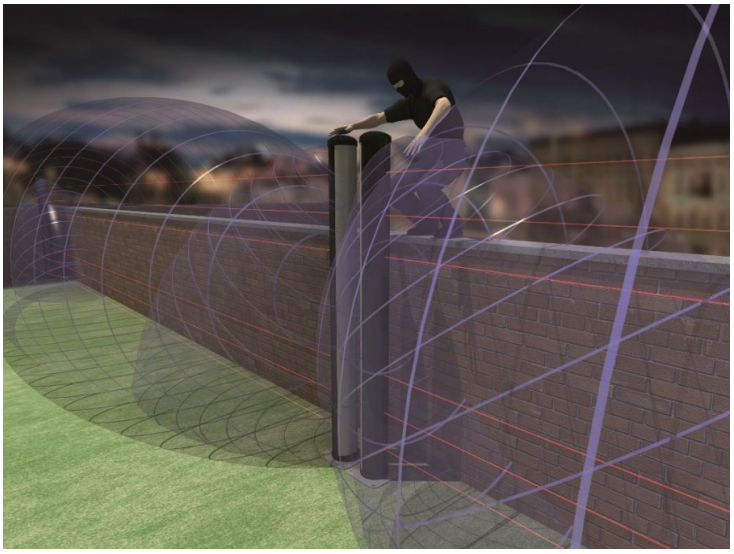
Obrázek 33 Mikrovlnná a infračervená bariéra [38]

Tyto detektory jsou pro nestacionární, perimetrickou ochranu použitelné, ale často při nepříznivých podmínkách mají nevýhodu ve velkém množství planých poplachů. Ta je do

jisté míry odstraněna kombinací těchto dvou technologií v jednom zařízení. Proto tyto prvky hodnotím jako **nevhodné**.

3.1.2.8 Kombinovaná (mikrovlnná – infračervená) bariéra

Toto detekční zařízení je doporučené použít v případě obtížných podmínek s výrazným negativním působením okolního prostředí. Kombinovaná zařízení jsou spojením technologií mikrovlnných a infračervených detektorů v jednom zařízení. Principiálně vycházíme z myšlenky nízké pravděpodobnosti, že nastanou takové negativní klimatické jevy, které vyvolají falešný poplach současně u detekčních prvků obou technologií pracujících na různých fyzikálních principech. Pro vyhlášení poplachu je nutné, aby došlo k detekci narušení na obou částech detektoru, a to současně nebo s velmi malou časovou odchylkou. Tímto se snažíme eliminovat negativní vliv nepříznivého prostředí na množství falešných poplachů. [12]



Obrázek 34 Duální MW/IR bariéra Pythagoras3 [42]

Kombinace IR a MW bariéry omezuje četnost falešných poplachů. Má větší variabilitu nastavení a přístupu k vyhlašování signálu. Tako technologie je pro naší aplikaci **vhodná**. Pro naší aplikaci jsem vybral duální MW/IR bariéru Pythagoras3.

Tabulka 4 *Parametry duální MW/IR bariéry Pythagoras3*

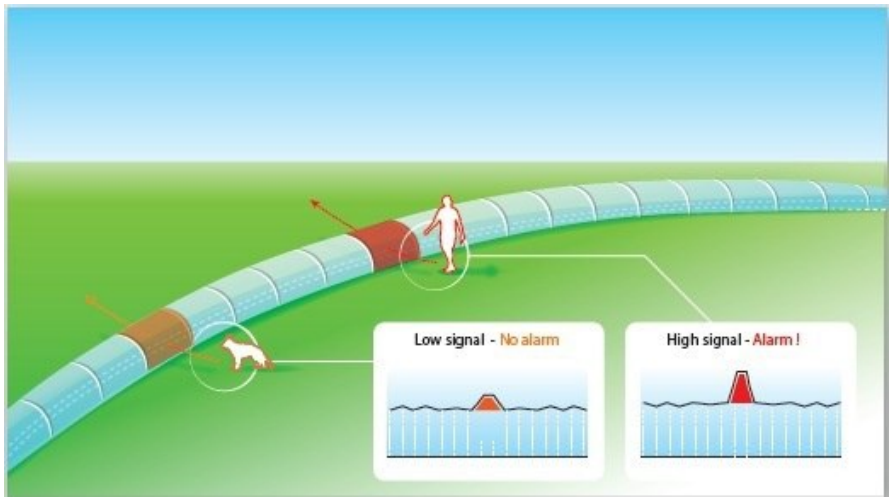
Parametr	**Popis**
Záložní baterie	ano
AGC (aut. zesílení signálu)	ano
Integrované nastavování	ano
Integrovaná paměť historie	ano
Proud při poplachu	410 mA
Nastavení pomocí PC	ano

Dosah	160 m
Napájecí napětí	12V DC, 13.8V DC, 230V AC
Teplota provozní	-35 až +65 °C
Rozhraní	RS485
Stupeň krytí	IP44
Typ výstupu	antimasking, poplach, porucha, tamper
Další vlastnosti	proud pro vyhřívání IR 1020 mA
Šířka/výška/hloubka	16/200/16 cm
Záložní baterie	22 kg

Bariéra kombinující technologie infračervených a mikrovlnných bariér. Tato bariéra se dá využít v několika módech nastavení. První možností je nastavení priority vysoké citlivosti detekce a to tím, že vyhlášení poplachu způsobí narušení alespoň jednoho ze systémů. Druhý způsob znamená, že každá z technologií má svůj časovač a při aktivaci pouze otevře časové okno, během něhož čeká na potvrzení poplachu z druhé technologie. Tedy velice stabilní detekce. Systém je opět vybaven rozhraním pro vzdálenou správu. Vyhodnocení detekovaných signálů je prováděno inteligentní analýzou. [42]

3.1.2.9 Štěrbinové kabely

Kolem chráněného perimetru je nutno instalovat dvojici kabelů (vysílací, přijímací), a to zakopáním pod povrch země. Prostřednictvím štěrbin v obou kabelech se z vysílacího kabelu část energie elektromagnetického pole vyzáří do okolí a část z takto vyzářené energie pomocí přijímacího kabelu zachycujeme a řídící jednotce analyzujeme. Pokud dojde k narušení perimetru, dojde ke změně přijímaného signálu a vyhlášení poplachu. Dnes používané systémy umožňují bodovou detekci to znamená, že dokážeme určit místo vzniku narušení perimetru s přesností na metry. [12]

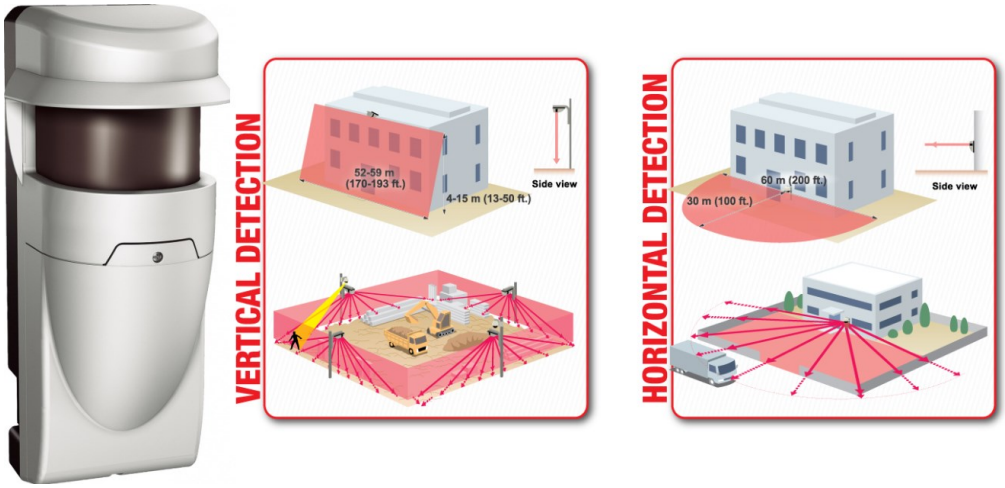


Obrázek 35 Zemní detekční systém na principu štěrbinových kabelů [43]

Zabezpečení mobilní perimetrické ochrany pomocí štěrbinových kabelů je stejně jako u podobných typů ochran **nevhodné**, proto v této práci nebude podrobněji charakterizována.

3.1.2.10 Laserový detektor

Laserové detektory používají pro detekci narušení ve střeženém perimetru laserový paprsek v oblasti vlnové délky 905 nm. Systém je vhodný pro mobilní i stacionární aplikace. Základním prvkem tohoto systému je detekční jednotka. Zaměřovače vysílají laserové modulované paprsky, které se po odrazu od okolních předmětů rozptýlí a část se vrací zpět na vstup přijímací části. Po zpracování odražených paprsků je k dispozici informace o okamžité vzdálenosti těchto předmětů. Laserový detektor nejprve prostor zmapuje a pak přejde do režimu střežení. Reálná situace v perimetru je řídícím systémem vyhodnocována a při vstupu narušitele do střeženého prostoru dojde ke splnění podmínek pro vyhlášení poplachu. Systém reaguje dle nastavených parametrů.



Obrázek 36 Laserový detektor OPTEX RLS 3060SH [44]

Laserová technologie se jeví pro případ našeho použití jako **vhodná**. Pro naší aplikaci jsem zvolil laserový detektor OPTEX RLS 3060 SH. Tento detektor má několik způsobů aplikace horizontální nebo vertikální.

Tabulka 5 Parametry laserového detektoru Optex RLS-3060SE

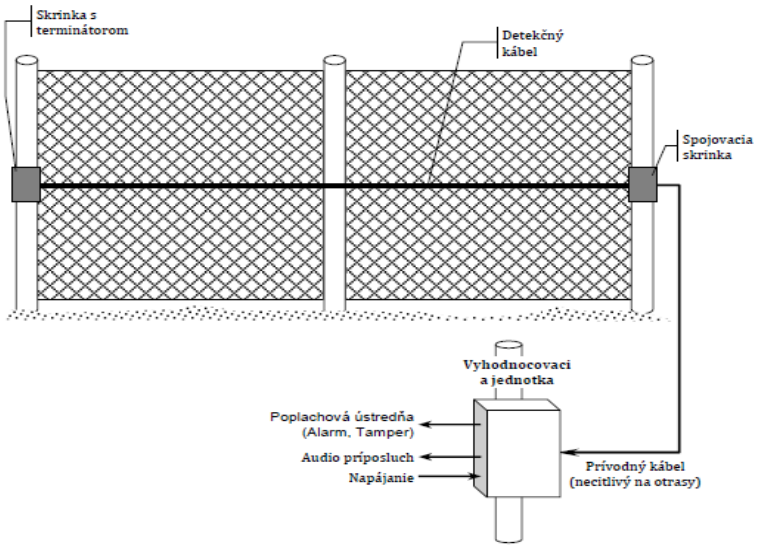
Parametr	**Popis**
Vyhřívání	ano
Další vlastnosti	přímé ovládání PTZ kamery, vyhřívání 12V DC 1,6A, horizontální i vertikální instalace
Napájecí napětí	24V AC/DC
Stupeň krytí	IP66
Počet výstupů	7
Nastavení pomocí PC	ano

Dosah detektoru	30 m
Max. skenovací úhel	190 °
Teplota provozní	-40 až +60 °C
Proud při poplachu	800 mA
Rozhraní	ethernet RJ45
Typ výstupu	antimasking, poplach, porucha, tamper
Úhlové rozlišení	0,25 °
Montážní výška	0,7 až 15 m
Šířka/výška/hloubka	14,4/33,4/15,5 cm
Hmotnost	4 kg

Tento typ laserového detektoru je možné připojit přímo přes IP rozhraní a napájení zajistit prostřednictvím PoE. Nevýhodou tohoto systému může být vyšší pořizovací cena.

3.1.2.11 Mikrofonní kabel

Koncept těchto detekčních systémů je založen na principu snímání nízkofrekvenčního signálu v akustickém frekvenčním pásmu. Při překonávání oplocení jsou detekovány vznikající vibrace v materiálu plotu, které se šíří ve formě povrchové akustické vlny způsobující miniaturní deformace detekčního kabelu. Tyto deformace způsobují vytvoření elektrického signálu zpravidla v podobě časově proměnného napětí. Vyhodnocovací jednotka snímá napětí a analyzuje, zda se jedná o falešný poplach, sabotáž nebo se o charakteristické složky signálu typického pro porušení plotu. Aby se omezil počet falešných poplachů, je vhodné doplnit celý systém o senzory snímající vlhkost a rychlost větru. [3]



Obrázek 37 Příklad uspořádání aplikace mikrofonního kabelu [3]

Po zesílení umožňuje reálný odposlech a tím obsluze odhadnout povahu narušení plotového systému a rozlišení falešných poplachů od skutečných. Díky této charakteristické vlastnosti byl pro kabely použit pojem mikrofonní. Detekční systém pro detekci překonání

obvodového plotu se skládá z vyhodnocovací jednotky a detekčního kabelu namontovaného na plotovém systému. [3]

Zabezpečení mobilní perimetrické ochrany pomocí mikrofonních kabelů, je stejně jako u podobných typů ochran **nevhodné**, proto v této práci opět nebude podrobněji charakterizována.

3.1.3 Kamerové systémy

Dalším prvkem pro zajištění bezpečnosti, kterou od perimetrického systému vyžadujeme, je použití kamerového systému. V této kapitole již nebudeme uvažovat o aplikaci analogových typů kamerových systémů a budeme volit IP kamery. Nespornou výhodou při použití v kombinaci s detektory perimetrické ochrany je možnost jejich vzájemné provázanosti, kdy při detekci narušení perimetru instalovanými detektory dojde k automatickému natočení konkrétní kamery ve směru místa narušení. Vzniklý incident je možné vyhodnotit a pokud se nejedná o planý poplach, narušitelův postup sledovat a zároveň zaznamenáván. První IP kamery se na trhu objevili okolo roku 1996 a prošly poměrně razantním vývojem. V následujícím textu jsou IP kamery rozděleny do kategorií. U každé kategorie je proveden popis principů kamery a u vhodných kamer je vybrán konkrétní produkt a provedena bližší analýza parametrů.

3.1.3.1 Fixní IP kamery a fixní IP dome kamery

V případě fixní IP kamery se jedná o kameru, u které po montáži již není možné vzdálené natočení. Její výhodou je použití širokého spektra objektivů. Je dostupná v mnoha provedeních pro vnitřní i venkovní použití. Fixní IP dome kamery jsou navíc zasazeny do těla, které na první pohled znemožňuje identifikaci zorného pole kamery. Označení dome pocházející z anglického slova a znamená kopule. Označuje specifický tvar krytů. Mezi nevýhodu těchto kamer můžeme zařadit nevariabilitu objektivů. [30]

Obrázek 38 Příklad fixní kamery a fixní IP dome kamery [45]

Fixní IP kamery i fixní IP dome kamery **nejsou vhodné** pro naší aplikaci převážně z důvodu snížení modularity kamerového systému, a proto nebudou dále rozpracovány.

3.1.3.2 IP PTZ kamery

Jak je uvedeno [30] *„Označení PTZ pochází z anglického Pan (panorámovat neboli pohyb po horizontální ose), Tilt (náklon, pohyb po vertikální ose) a Zoom (zvětšení, schopnost objektivu s variabilní ohniskovou vzdáleností).“*

Hlavní výhodou IP PTZ kamery je možnost automatického či manuálního nastavování snímaného zorného pole a vzdálenosti pomocí polohovacích mechanizmů. Za pomocí automatického polohování je možné, na základě podnětů vyhodnocených inteligentní analýzou obrazu, či na základě předem naprogramovaných tras pro zachycení co nejvhodnějšího zorného pole, dosáhnout co nejvyšší efektivity dohledu nad střeženým prostorem. [30]

Mechanické a nemechanické IP PTZ kamery

Mechanické IP PTZ kamery jsou zejména vyhledávané pro možnost skryté instalace. Výhodou je neslyšitelnost veškerých pohybů a prostorově nízké nároky na montáž. Bývá převážně osazena kvalitním obrazovým snímačem a širokoúhlým objektivem. Při volbě této kamery musíme počítat s omezenou možností pohybu kamery. Ovládání těchto kamer zajišťuje operátor, který je součástí ochrany objektu. V nabídce najdeme převážně kamery tohoto typu pro vnitřní použití. [30]

Obrázek 39 Nemechanická IP PTZ kamera [45]

Mechanický a nemechanický typ kamery je pro naší modulární, mobilní, venkovní aplikaci perimetrické ochrany **nevhodný**. Nebudeme jej tedy nadále analyzovat.

IP PTZ dome kamery

Jedná se o nejrozšířenější typ IP kamer, vhodných pro vnitřní i venkovní použití. Do těchto kamer jsou aplikovány veškeré pokročilé technologie. Velkou výhodou je možnost neomezeného pohybu objektivu v jednotlivých osách a díky zasazení technologie kamery do dome krytu poskytují stiženou identifikaci právě sledovaného prostoru. [30]

Obrázek 40 IP PTZ dome kamera [45]

Výše zmíněné kamery mají široké portfolio volitelných funkcí a vlastností od kterých se odvíjí i koncová cena samotného zařízení.

Tento typ IP kamery je **vhodný** pro naše podmínky, nabízí širokou škálu technických funkcí, a její aplikace zabezpečí modulárnost celého kamerového systému. Dále jsou vybrány dva typy těchto kamer, které budou analyzovány a budou uvedeny jejich parametry.

DAHUA SD5A432XA-HNR

První zvolenou kamerou je venkovní IP PTZ kamera. Mezi její hlavní výhody patří její odolnost, která dle normy ČSN EN 62262 dosahuje kategorie IK 10. Další její výhodou je výkonný IR přísvit, jehož udávaný dosah je do 150 m. Kamera nabízí výkonný optický zoom a funkci WDR pro aplikace s možností nepříznivých světelných podmínek. Neméně zajímavá je funkce automatické detekce osob.

Obrázek 41 IP PTZ kamera DAHUA SD5A432XA-HNR [46]

Tabulka 6 Parametry IP PTZ kamery DAHUA SD5A432XA-HNR

Parametr	**Popis**
Prostředí	venkovní
Režim den/noc	ano (mechanický IR filtr)
IR přísvit	ano, 150 m
Snímací čip	1/2.8" STARVIS CMOS
Objektiv – parametry	4.9 mm–156 mm, F1.35-4.4, 32x zoom
AI (automatická clona)	ano
Citlivost (barevný obraz/ČB)	0,005/0,0005 lux
Audio vstup/výstup	ano/ano
Podporované protokoly	IPv4/ IPv6, HTTP, HTTPS, SSL, TCP/IP, UDP, UPnP, ICMP, IGMP, SNMP,RTSP, RTP, SMTP, NTP, DHCP, DNS, PPPOE, DDNS, FTP, IP Filter, QoS,Bonjour, 802.1x
Další vlastnosti	AGC, BLC, WDR(120dB), AWB/ATW, FF, podpora PSIA, CGI
Napájecí napětí	24V AC, PoE+ (IEEE 802.3at)
Maximální snímkovací rychlost	60 fps
Max. datový tok IP	20 Mbps
Max. rozlišení	2688 x 1520 (4 MPx)
Podporované kodeky	H.264, H.264+, H.265, H.265+, MJPEG
Podpora ONVIF	Profile G, Profile S, Profile T

Lokální úložiště	microSD/SDHC
SDK	ano
Podporované VMS	Digifort, Security Center, DSS Pro
Stupeň krytí	IP67
Teplota provozní	-40 ~ +70 °C
Příkon (max.)	20 W
Antivandal provedení	IK10
Šířka/výška/hloubka	19/33,2/19 cm
Hmotnost	4,7 kg

HIKVISION DS-2DE3A404IW-DE – IP PTZ KAMERA

Druhá kamera je také vhodná pro venkovní použití a disponuje IR přísvitem až do vzdálenosti 50 m. Rozměr snímače 1/2,8" zabezpečí lepší práci ve stižených světelných podmínkách. Tato kamera má funkci sledování osob, chytré detekce a chytrého nahrávaní. Je montována do anti otřesového krytu s ochranou proti vodě a prach IP66 a mechanickou odolností IK 10. Součástí je i integrovaná ochrana před bleskem a přepětím.

Obrázek 42 HIKVISION DS-2DE3A404IW-DE – IP PTZ KAMERA [47]

Tabulka 7 Parametry IP PTZ kamery HIKVISION DS-2DE3A404IW-DE

Parametr	**Popis**
Prostředí	venkovní
Režim den/noc	ano (mechanický IR filtr)
IR přísvit	ano, 50 m
Snímací čip	1/2,8" Progressive Scan CMOS
Objektiv – parametry	2,8 - 12 mm, F1.5-2.7, 4x zoom

AI (automatická clona)	ano
Citlivost (barevný obraz/ČB)	0,005/0,0001 lux
Audio vstup/výstup	ano/ano
Podporované protokoly	IPv4/IPv6, HTTP, HTTPS, 802.1X, QoS, FTP, SMTP, UPnP, SNMP, DNS,
Další vlastnosti	WDR (120 dB), detekce obličeje, detekce pohybu, detekce průchodu, detekce zanechání zavazadla, detekce odstranění objektu
Napájecí napětí	12V AC, PoE+ (IEEE 802.3at) max 15W
Maximální snímkovací rychlost	25 fps
Max. datový tok IP	8 Mbps
Max. rozlišení	2688 x 1520 (4 MPx)
Podporované kodeky	H.264, H.264+, H.265, H.265+, MJPEG
Podpora ONVIF	Profile G, Profile S, Profile T
Lokální úložiště	microSD/SDHC
SDK	ano
Podporované VMS	Digifort, Security Center, DSS Pro
Stupeň krytí	IP66
Teplota provozní	-30 ~ 60 °C
Příkon (max.)	60 W
Antivandal provedení	ne
Šířka/výška/hloubka	17,9/12,1/18,2 cm
Hmotnost	1,125 kg

3.2 Dílčí závěr

Cílem této kapitoly bylo vybrat vhodné technické prostředky k zabezpečení perimetrické ochrany operačního střediska vrtulníkové letky, působící v polních podmínkách. Tyto prostředky analyzovat a blíže specifikovat. Při výstavbě operačního střediska vrtulníkové letky, které je chráněno navrhovanou perimetrickou ochranou je nutné dbát na jeho modularitu, účinnost v široké škále klimatických podmínek, jeho opětovnou montáž a demontáž, snadnou skladovatelnost a přemístitelnost. Všechny tyto podmínky budou zohledněny při návrhu variant, které jsou předmětem 4 kapitoly této práce.

4 MODEL HYPOTETICKÉHO MÍSTA VELENÍ V POLNÍCH PODMÍNKÁCH

V této části diplomové práce je popsáno smyšlené místo velení začleněné do organizační struktury Vzdušných sil AČR. Je vytvořen model místa velení, pro něž jsou posléze zapracovány dva návrhy systémů perimetrické ochrany. Na základě vícekriteriálního rozhodování je vybrána jedna z navržených variant a rozpracována do projektu. Tento projekt je předmětem poslední kapitoly diplomové práce. Hypotetický projekt místa velení je zpracován pro případ použití operačního střediska vrtulníkové letky v nasazení mimo Českou republiku, tedy pro plnění hypotetické zahraniční operace na podporu míru. Organizačně je plánováno zařazení vyčleněné jednotky pod velení NATO.

Vytvořený hypotetický návrh operačního střediska vrtulníkové letky musí zabezpečit prostor a prostředky pro následující pracoviště:

Skupina plnění úkolů

- pracoviště velitele
- pracoviště k přípravě letových úkolů I
- pracoviště k přípravě letových úkolů II
- operační pracoviště
- zpravodajské pracoviště

Skupina řízení

- pracoviště vyhodnocení a analýzy
- pracoviště ochrany

Skupina podpory

- pracoviště KIS/OUI
- pracoviště logistické podpory
- pracoviště meteorologické služby
- pracoviště personalistiky
- pracoviště zdravotnického zabezpečení

4.1 Popis místa velení

Operační středisko vrtulníkové letky je situováno do komplexu rozmístitelných prvků, které jsou tvořeny z pogumovaných stanů s podpůrnou ocelovou konstrukcí typů SU 711 a SU 660. Příklad jednoho ze stanů označeného SU 711 je zobrazen na obrázku 43.

Obrázek 43 Příklad sestaveného stanu SU 711 [48]

Dalšími v sestavě používanými stany jsou stany SU 660. Oba tyto stany jsou v případě vystavění využívány pro zasazení pracovišť pro orgány velení a řízení v operaci. Základní technické parametry stanů jsou uvedeny v tabulce 8.

Tabulka 8 Technické parametry stanů SU660 a SU 711

Technické parametry	SU 660	SU 711
Vnější rozměry	6000 x 6000 x 3300 mm	11000 x 6600 x 3500 mm
Vnitřní rozměry	6000 x 5360 x 3000 mm	11000 x 6000 x 3200 mm
Hmotnost	140 kg	180 kg
Čas výstavby	20 min	35 min
Užitná plocha	33 m²	71 m²
Teplotní odolnost	-40 °C až +70 °C	-40 °C až +70 °C
Odolnost proti proudění vzduchu	do 100 km.h-1	do 100 km.h-1

Mezi další prvky, ze kterých je operační středisko složeno jsou přepravní kontejnery typu ISO-1 C. Tyto kontejnery slouží pro uložení převáženého materiálu, a protože jsou izolovány a vybaveny osvětlením, topením a klimatizací, jsou po rozvinutí prostředku využity k umístění pracovišť pro operační personál.

Obrázek 44 Kontejnery ISO 1 C [49]

Tento typ kontejnerů je manipulovatelný podle ČSN ISO 3874 všemi prostředky schválenými pro kategorii kontejnerů ISO 1 C. Technické parametry přepravních kontejnerů ISO 1 C jsou uvedeny v tabulce 9.

Tabulka 9 Technické parametry kontejneru ISO 1 C

Vnější rozměry	6058 x 2438 x 2438 mm
Vnitřní rozměry	5870 x 2330 x 2200 cm
Hmotnost	2500 kg
Povolená užitečná nosnost	21500 kg
Maximální hmotnost	24000 kg

Do kontejnerů tohoto typu jsou mimo převáženého materiálu situovány veškeré komunikační a informační technologie, pro zabezpečení připojení k datové síti. Tyto prostředky jsou v kontejnerech zastavěny na pevno a při použití a přepravě se nedemontují.

Operační středisko vrtulníkové letky je také vybaveno přechodovými stany S2K480 a SK650. Oba typy stanů slouží k vytvoření přechodů mezi stany SU711, SU660 a kontejnery. Operační stany jsou jimi propojeny a v případě stanu S2K480 doplněny o propojení s kontejnery ISO 1 C. Toto propojení je zrealizováno pomocí přechodových modulů. Základní technické parametry jsou uvedeny v tabulce 10.

Tabulka 10 Technické parametry stanů S2K480 a SK650

Technické parametry	**S2K480**	**SK650**
Vnější rozměry	8200 x 4200 x 3100 mm	6500 x 6500 x 3300 mm
Vnitřní rozměry	7600 x 3600 x 2800 mm	6000 x 6000 x 3000 mm
Hmotnost	150 kg	150 kg
Čas výstavby	35 min	30 min
Užitná plocha	32 m²	40 m²
Teplotní odolnost	-40 °C až +70 °C	-40 °C až +70 °C
Odolnost proti proudění vzduchu	do 100 km.h-1	do 100 km.h-1

Obrázek 45 Příklad propojení stanu SU711 pomocí S2K480 s kontejnery ISO 1 C [48]

Veškeré stany jsou vybaveny hygienickými, termoizolačními vložkami, sluneční clonou, klimatizační jednotkou, topným agregátem, osvětlením, elektroinstalací a podkladovými podlahami.

Aby bylo možné vytvořit v operačním středisku vrtulníkové letky všechna potřebná pracoviště je nutné zabezpečit, aby celkový obvod chráněného perimetru, který je ohraničen mobilním plotem, měřil minimálně 200 m a maximálně 250 m. Celkové počty využitých prvků operačního střediska letky jsou stanoveny na základě požadavků na obsazení jednotlivých tabulkových míst vyčleňovaného úkolového uskupení praporního typu. Toto operační středisko vrtulníkové letky je navrhováno natolik modulárně aby umožňovalo zasazení jednotky od počtu cca 40 osob v té nejnižší a nejméně nákladné variantě, pro zabezpečení jednodušších úkolů. Až po maximální variantu koncipovanou pro celkový počet nasazených cca 120 osob. Celkový počet stanů a kontejnerů je uveden v tabulce 11.

Tabulka 11 Přehled prvků použité varianty

Název	Počet
Kontejner ISO 1C	13 kusů
Stan SU711	2 kusy
Stan SU660	2 kusy
Stan S2K480	1 kus
Stan SK650	1 kus

Půdorys výsledného hypotetického komplexu, složeného z výše uvedených prvků je uveden na obrázku 47.

Obrázek 46 Půdorys výsledného hypotetického komplexu

4.2 Začlenění místa velení pod mnohonárodnostní velitelství

Místo velení, pro které je zpracován návrh perimetrického systému ochrany je začleněno do struktury místa velení spolupůsobících jednotek v rámci NATO a jako takové je zřizováno v připravených, zabezpečených místech – základnách NATO. Ochrana vnějšího perimetru celé základny NATO je zabezpečena pomocí bariér a překážek, je stanovena kontrola přístupů na základnu, přes stanoviště vstupní kontroly. K ochraně proti vnějšímu napadení jsou vybudovány strážní věže. Dále je pro bezpečnost celé základny vybudován vyhledávací a pozorovací systém a systém varování v případě napadení.

Obrázek 47 Ochrana základny zabezpečena aliančními partnery. [50]

Hypotetické místo velení je tedy rozmístitelné operační středisko vrtulníkové letky. Tento systém je vyroben pro potřeby zasazení vrtulníkové letky mimo stálou dislokaci a získání schopnosti propojení informačních toků v rámci NATO s názvem ACCS.

Obrázek 48 Operační středisko letky [50]

Z důvodu začlenění jednotky do brigádního úkolového uskupení NATO je nutné, pro plnění operačních úkolů, zabezpečit podporu informačních toků s nadřízeným a národním velitelstvím a zároveň vytvořit podmínky pro plánování, řízení a vyhodnocování plněných úkolů. Informační tok, související s velením a řízením jednotky, může být klasifikován až do stupně utajení „Tajné“ nebo v případě komunikace s aliančními partnery „NATO secret“ a Mission secret“.

4.3 Analýza rizik

Smyslem tvorby analýzy rizik je identifikace bezpečnostních hrozeb představující riziko pro chráněná aktiva. Definujeme zranitelnost chráněných aktiv těmito hrozbami a případný negativní dopad na chráněná aktiva. Analýza rizik je zásadním materiálem na základě, kterého u určených rizik stanovujeme doporučení o nejvhodnějším přístupu pro zvládání, řízení rizik. [51]

Analýza rizik zahrnuje:

- vymezení aktiv systému
- vymezení hrozeb
- určení pravděpodobnosti výskytu událostí
- určení velikosti dopadu
- stanovení hodnoty velikosti rizika
- seřazení rizik podle závažnosti [52]

4.3.1 Vymezení aktiv

K dalšímu postupu a nalézání východisek práce je nutné blíže specifikovat chráněná aktiva. Mezi nejdůležitější aktiva operačního střediska vrtulníkové letky patří **spolu s personálem také informace** zejména **utajované**, které se v zabezpečené oblasti zpracovávají.

Dalšími aktivy operačního střediska vrtulníkové letky jsou technické prvky systému jako jsou **servery**, **pracovní stanice, aktivní síťové prvky**, **zobrazovací a záznamová zařízení, aplikační, programové vybavení a komunikační prostředky**.

Samostatnou částí aktiv, kde musí být řešena otázka bezpečnosti a zabezpečení jsou **kryptografická a šifrovací** zařízení.

Dalšími chráněnými aktivy je v našem případě **veškerý materiál** a převážně **zbraně** a **munice**.

Chráněná aktiva nacházející se uvnitř chráněného perimetru mají nevyčíslitelnou hodnotu, a to převážně z důvodu ochrany utajovaných skutečností. V případě vyzrazení nebo narušení integrity chráněných dat může dojít k vyzrazení podrobností o právě plněném úkolu. To může mít za následek jeho nesplnění nebo dokonce zapříčinit ztráty na lidských životech a velkých materiálních škodách.

4.3.2 Vymezení hrozeb

Hrozby jsou definovány již v první kapitole. K vymezení hrozeb, které mohou působit na chráněná aktiva v perimetru zvoleného nestacionárního místa velení byla použita delfská analytická metoda a metoda extrapolace trendů.

V této kapitole uvedené hrozby jsou ty, proti kterým, může být vytyčená perimetrická ochrana, která je předmětem této práce, účinná. Ostatní hrozby, které zde nejsou zmíněny, jsou potlačovány jinými typy ochran patřících do celkové ochrany alianční základny. Tuto ochranu zabezpečují jednotky a síly aliančních partnerů, jak je uvedeno v první kapitole této práce.

Mezi hrozby ohrožující aktivum operačního střediska vrtulníkové letky patří:

- únik utajovaných informací
- průnik narušitele
- nedostupnost služeb
- porušení integrity dat
- zamítnutý přístup
- zanesení škodlivého kódu
- zneužití připojení do systému
- požár

Velkou část hrozeb jsme schopni eliminovat zabráněním přístupu neautorizovaných osob bez doprovodu do zabezpečené oblasti.

4.3.3 Určení pravděpodobnosti výskytu

Pro každou definovanou hrozbu je nutné stanovit pravděpodobnost jejího výskytu. Její odhad se stanovuje na základě známých informací a zkušeností, takzvaným expertním posouzením. Každá kategorie výskytu je procentuálně vyjádřena v rovnoměrném rozložení pravděpodobnosti, jak je uvedeno v tabulce 12.

Tabulka 12 Stanovení pravděpodobnosti výskytu

Kategorie výskytu	**Numerické vyjádření pravděpodobnosti výskytu**	**Rozsah pravděpodobnosti (%)**
Četný	5	81-100
Pravděpodobný	4	61-80
Občasný	3	41-60
Velmi malý	2	21-40
Nepravděpodobný	1	0-20

Expertním odhadem stanovíme u hrozeb pravděpodobnosti expozice.

Tabulka 13 Pravděpodobnost výskytu definovaných hrozeb

Hrozba	**Vyjádření pravděpodobnosti výskytu**
Únik utajovaných informací	3
Průnik narušitele	3
Nedostupnost systému a služeb	3
Výpadek technického zařízení	3
Porušení integrity dat	2
Zamítnutý přístup	2
Zanesení škodlivého kódu	2
Zneužití připojení do systému	2
Požár	2

Při určení pravděpodobnosti výskytu výše uvedených hrozeb, je přihlíženo k ostatním bezpečnostním opatřením, která z důvodu rozsahu práce nejsou detailněji popisována. Jedná se především o prvky administrativní a personální bezpečnosti, dále bezpečnosti informačních a komunikačních systémů, kryptografické ochrany a požární ochrany.

4.3.4 Určení velikosti dopadu

Hodnocení velikosti dopadu konkrétní hrozby na konkrétní aktivum je vyjádřeno číselnou hodnotou. Tato hodnota představuje vyjádření dopadu hrozby na funkčnost místa velení při plnění operačních úkolů. Pro hodnocení lze použít následující stupnici následků popisující závažnost dopadu pro každou hrozbu samostatně.

Tabulka 14 Stanovení hodnocení velikosti dopadu

Kategorie velikosti dopadu	**Numerické vyjádření**	**Popis dopadu**
Likvidační	5	Ztráty na životech, technice a materiálu který už nemůže být nahrazen. Může dojít ke zničení místa velení a důležitých prvků komunikace. Zničení místa velení, které nadále neplní svoji funkci.

Velká	4	Těžká až smrtelná zranění, technika je poškozena a její oprava zabere práci od 400 do 1000 normohodin. Místo velení je poškozeno, není možno nadále využívat dle stanovených pravidel.
Větší	3	Na živé síle způsobí lehká až těžká zranění, technika je poškozena a její oprava zabere práci od 100 do 400 normohodin. Místo velení je poškozeno, není možno nadále využívat dle stanovených pravidel. Jsou nutné rozsáhlé opravy, při kterých ho není možné používat.
Malá	2	Na živé síle způsobí drobná až lehká zranění, technika je poškozena a její oprava zabere práci od 60 do 100 normohodin. Místo velení je mírně poškozeno, během oprav je možné ho nadále používat.
Nevýznamná	1	Na živé síle nezpůsobí žádná nebo jen drobná zranění, technika není poškozena nebo jen drobně její oprava zabere práci od 40 do 60 normohodin. Místo velení není poškozeno nebo jen drobně, což nemá vliv na plnohodnotné využívání.

Expertním odhadem stanovíme u hrozeb velikost dopadu na chráněná aktiva.

Tabulka 15 Stanovení kategorie dopadu u hrozeb

Hrozba	**Numerické vyjádření**
Únik utajovaných informací	5
Průnik narušitele	5
Nedostupnost systému a služeb	2
Výpadek technického zařízení	3
Porušení integrity dat	3
Zamítnutý přístup	2
Zanesení škodlivého kódu	2
Zneužití připojení do systému	2
Požár	5

4.3.5 Stanovení hodnoty velikosti rizika

Tabulka 16 Stanovení hodnoty rizika

Hrozba	**Pravděpodobnost výskytu**	**Hodnocení velikosti dopadu**	**Výše rizika**
Únik utajovaných informací	3	5	15
Průnik narušitele	3	5	15
Nedostupnost systému a služeb	3	2	6
Výpadek technického zařízení	3	3	9
Porušení integrity dat	2	3	6
Zamítnutý přístup	2	2	2
Zanesení škodlivého kódu	2	2	4
Zneužití připojení do systému	2	2	4
Požár	2	5	10

4.3.6 Dílčí závěr

Na základě analýzy rizik bylo zjištěno, že nejvyšší míra rizika, které nejsme schopni akceptovat pramení z následujících hrozeb:

- únik utajovaných informací
- průnik narušitele

Ostatní vymezená rizika jsou akceptovatelná, a to převážně z důvodu ošetření ostatními prvky bezpečnosti. V případě nedostupnosti systému a služeb, porušení integrity dat, zamítnutého přístupu do systému, zanesení škodlivého kódu a zneužití připojení do systému můžeme uvažovat dva způsoby vzniku těchto incidentů:

- prvním způsobem je hrozba průniku neznámého narušitele, který bude příčinou vzniku bezpečnostního incidentu a tím narušení aktiv
- druhým způsobem vzniku bezpečnostního incidentu a ohrožení aktiv je případ, kdy bezpečnostní riziko představuje činnost autorizované osoby, který má oprávněný přístup do operačního střediska vrtulníkové letky; tento druhý způsob působení hrozby je minimalizován prostřednictvím ostatních prvků bezpečnosti, jakými jsou převážně administrativní bezpečnost, personální bezpečnost, bezpečnost informačních a komunikačních systémů a kryptografická bezpečnost

Proti působení těchto hrozeb jsou dále vytvořeny dvě varianty perimetrické ochrany operačního střediska vrtulníkové letky.

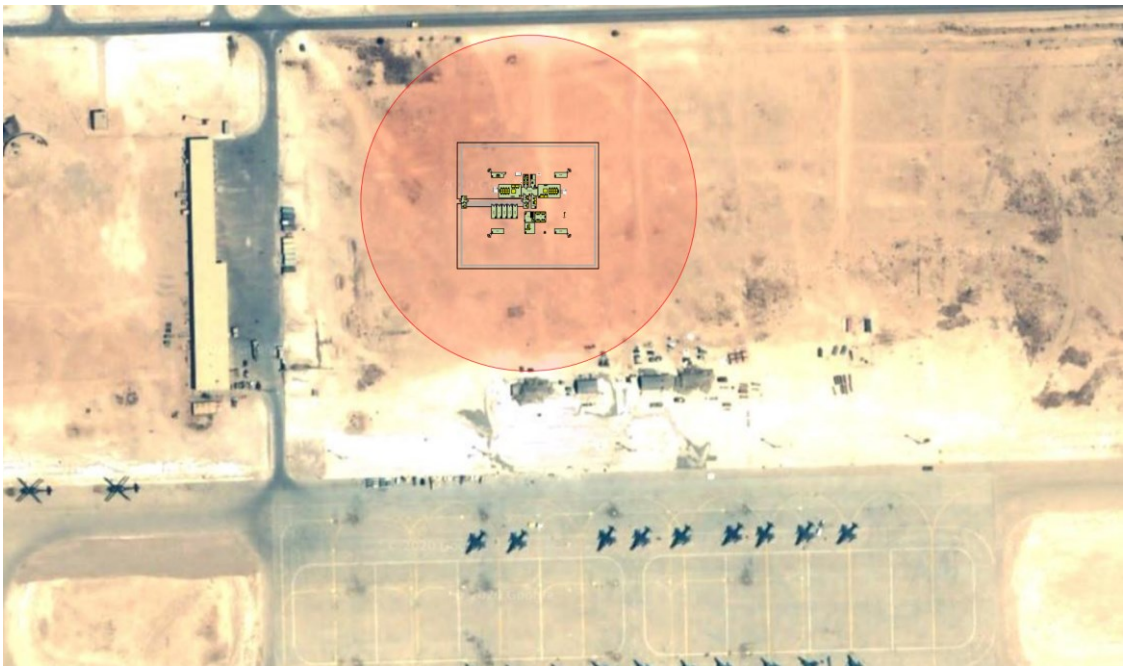
4.4 Návrh variant perimetrické ochrany

Dle požadavků zadavatele je při navrhování jednotlivých variant nutné důsledně dbát na jednoduchost a zároveň funkčnost celého systému perimetrické ochrany operačního střediska vrtulníkové jednotky. Zadavatelem byly stanoveny požadavky použití jednoho detekčního systému narušení perimetru, jehož funkčnost bude rozšířena o dohledový kamerový systém, který má zároveň sloužit k vyhodnocování vyhlášených poplachů ve střežené oblasti. Dalším požadavkem je použití perimetrického systému operačního střediska vrtulníkové letky ve více možnostech rozmístění vnitřcích pracovišť, stanů a kontejnerů tedy na jeho vysokou modularitu rozmístění technických prvků.

Navrhovaná opatření proti působení definovaných hrozeb je možné rozdělit do dvou skupin. První opatření je vedeno proti úniku informací, které je způsobeno zachytáváním

kompromitujícího elektromagnetického vyzařování narušitelem. Vzhledem ke koncepci a návrhu celého systému místa velení má výrobce povinnost před certifikací systému provést měření tohoto nežádoucího vyzařování. Není samozřejmě možné, a to převážně z důvodu používání informačních technologií ke zpracování UI ve stanech, zabezpečit šíření elektromagnetického vyzařování do okolního prostředí.

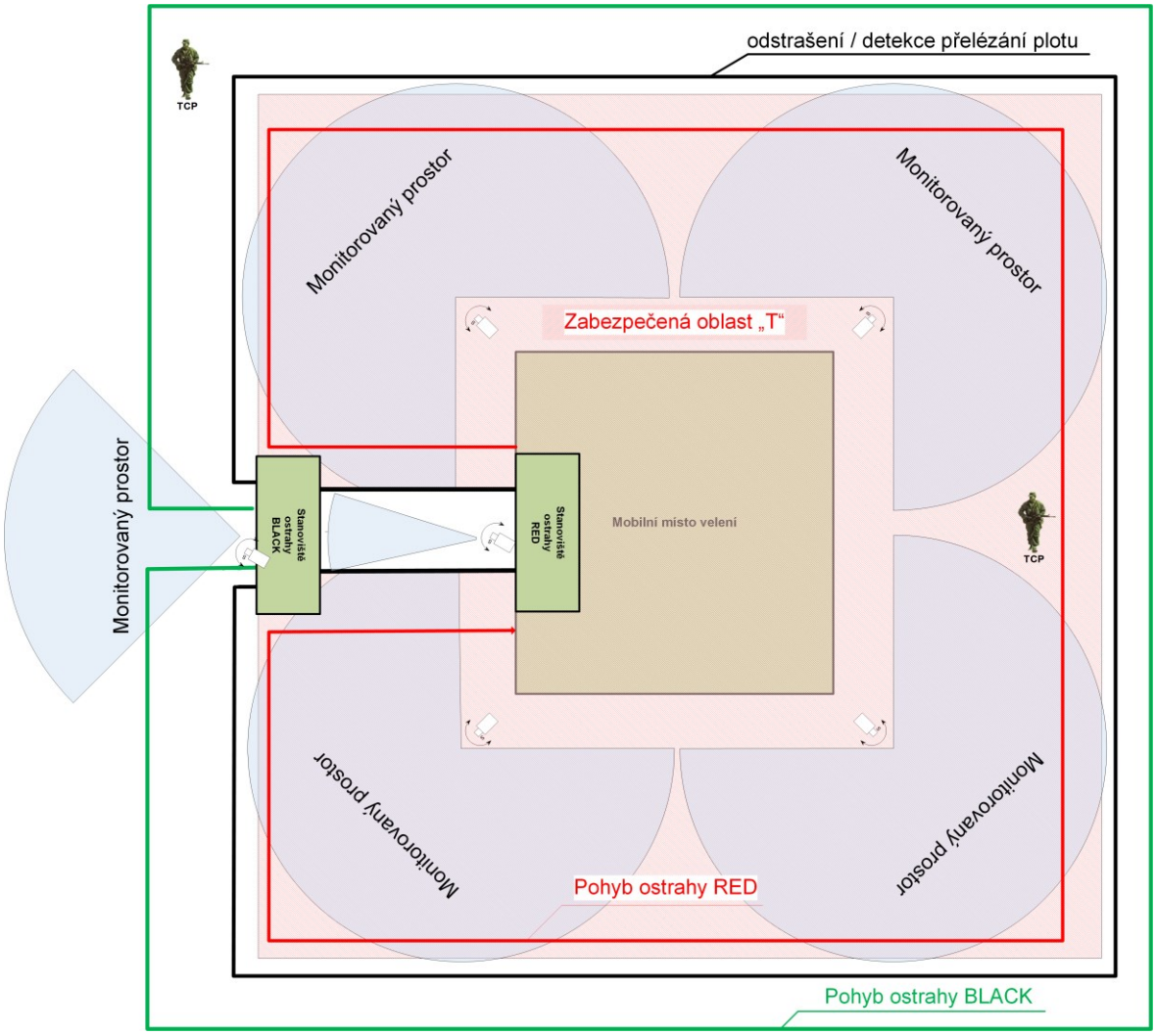
Proto je u obou dvou variant nutné zabezpečit snížení rizika zachytávání kompromitujícího elektromagnetického vyzařování (KEV). Jednou z podmínek je určení vhodného místa výstavby, které musí splňovat podmínky volného perimetru kolem rozmístěného informačního systému. Dle zákona musí tento perimetr dosahovat vzdálenosti nejméně 100 m. Obrázek 49 znázorňuje kruhový perimetr o stanoveném poloměru.



Obrázek 49 Příklad výstavby místa velení v bezpečném perimetru 100 m.

Tento perimetr není žádným způsobem vytyčen je stanoven ve směrnicích ostrahy vnějšího perimetru. Pro naše potřeby, použijeme označení **vnější perimetr operačního střediska vrtulníkové letky**. Odpovědnost za zabezpečení nepřítomnosti osob, techniky a dalších nežádoucích prvků má strážní hlídka (ostraha perimetru BLACK), která je složena ze tří vojáků. Tato strážní hlídka má povinnost v nepravidelných obchůzkách, ve stanoveném intervalu, provádět kontrolní obchůzku se zaměřením na vizuální kontrolu instalovaného mobilního plotu, který je hranicí mezi vnějším a vnitřním perimetrem operačního střediska vrtulníkové jednotky (linie zelené barvy na obrázku 50). Tato strážní hlídka v žádném případě nesmí vstupovat do zabezpečené oblasti stupně utajení Tajné, která je vyznačena na obrázku 50, operačního střediska vrtulníkové letky.

Druhé opatření musí působit proti možnosti přímého odposlechu utajené informace z bezprostřední blízkosti místa velení a průniku narušitele. Ke snížení tohoto typu rizika je nutno znemožnit narušiteli nepozorovaně vniknout do bezprostřední blízkosti operačního střediska vrtulníkové letky. K tomuto úkolu je v systému ochrany vybudován bezpečnostní plot (černá linie na obrázku 50). Ochranu zabezpečené oblasti stupně utajení Tajné mají za úkol zabezpečit tři vojáci tato směna je zde nazvána ostraha perimetru RED. Tato ostraha má za úkol formou nepravidelných obchůzek provádět fyzickou kontrolu vnitřního perimetru zabezpečené oblasti stupně utajení Tajné (linie červené barvy na obrázku 50).



Obrázek 50 Principiální schéma ochrany

V každé variantě je počítáno s variabilním rozložením kontejnerů dle požadavků instalace konkrétních technických prvků navrhované perimetrické ochrany. Na základě požadavků jsou vytvořeny dva návrhy řešení perimetrické ochrany:

- První návrh řešení perimetrické ochrany – detekční varianta

- Druhý návrh řešení perimetrické ochrany – odstrašující varianta

4.4.1 První návrh řešení perimetrické ochrany – detekční varianta

Tato varianta řešení je navrhována s cílem detekovat narušitele ještě před vniknutím do chráněného perimetru. Při pokusu o vniknutí je narušení detekováno pomocí instalovaného plotového detekčního systému. Vzhledem k propojení detekčních prvků s dohledovým kamerovým systémem ostraha RED dále kontroluje stav narušení a dva příslušníci ostrahy BLACK narušitele zneškodní. Grafický návrh varianty je uveden v příloze 1.

První varianta řešení perimetrické ochrany se skládá z těchto prvků fyzické bezpečnosti:

- ústředna PZS, SW, dohled, ovládání, kabeláž
- mobilní plot s vrcholovou ochranou
- plotový detekční systém
- kamerový systém

Ústředna PZS, SW, dohled, ovládání, kabeláž

PZS je navržen jako sběrnicový, zvolená ústředna je typ GALAXY GD-520, je instalována na stěnu kontejneru na pracovišti OUI v kontejneru ostrahy RED. Ovládání systému je umožněno z klávesnice, která je nainstalována na stanovišti ostrahy RED. Konfigurační a přehledový SW je instalován na aplikačním serveru u ostrahy RED. Uživatelská obsluha a dohled nad systémem ochrany je vyveden pomocí sítě LAN na stanoviště ostrahy RED do kontejneru ostrahy RED a na pracoviště ostrahy BLACK do kontejneru ostrahy BLACK.

Mobilní plot s vrcholovou ochranou

Na základě analýzy plotových systémů jsem do této varianty vybral mobilní plotový systém F5 maxi doplňkový průhledný plot, který je instalován pomocí plastových patek. Tyto jsou usazeny do stabilizačních ocelových základen. Dále je plot doplněn o ostnatý drát, který je usazen do jednostranných ocelových nástavců. Tento plot je dostatečně pevný a pokud je usazen do zvolených základen a zatížen plastovou patkou a následně ukotven dvěma kotevními kolíky k zemi, je i dostatečně stabilní.

Obrázek 51 Použité prvky MZS varianta 1

Plotový detekční systém

K dohledu nad narušením perimetru je do této varianty vybrán plotový detekční systém od firmy Varya Perimeter. Detekce narušení pracuje na principu 3-osých akceleračních detektorů FLA viz. obrázek 30, které zaznamenávají jakýkoli pohyb prvku, na který jsou detektory instalovány. Komunikace mezi jednotlivými detektory probíhá bezdrátově pomocí technologie RFID. Technická data jsou uvedena ve třetí kapitole v *Tabulka 1*. Výhodu v použití tohoto systému vidím v jednoduché instalaci, snadné údržbě a dostupné ceně. Dle výrobce je možné tento plotový systém aplikovat i na mobilní typ oplocení. Pro instalaci je nutné k tagu FLA doobjednat dva montážní díly typu T14. Odpadá zde problém s napínáním plotu, které by mohlo být příčinou vyhlašování planých poplachů. V případě aplikace tohoto systému je nutné zabezpečit, aby nedocházelo k prorůstání dřevin, keřů a trávy do plotových dílců, toto by mělo za následek nárůst planých poplachů. Je také zakázáno na plot instalovat jakékoli cedule nebo jiné prvky tohoto typu.

Pro naši aplikaci tohoto systému na mobilní typ oplocení je vhodné instalovat 1 tag FLA-06 na každý plotový dílec, a to z důvodu eliminace planých poplachů při špatných meteorologických podmínkách. Plotový detekční systém je navržen jako neuzavřený, proto je nutné použít dvě FLM monitorovací jednotky, tyto jednotky jsou umístěny v kontejneru ostrahy BLACK a je požadováno, aby umístění těchto jednotek bylo řešeno variabilně.

Dále jsou svedeny pomocí LAN do centrální jednotky označené FLU. Tato jednotka je umístěna v kontejneru ostrahy RED. V tomto kontejneru je umístěna i PZS ústředna do které je jednotka FLU připojena přes FLE expandér a pomocí RS 485. V kontejneru ostrahy RED na stanovišti, kde ostraha vykonává službu v nepřetržitém režimu, je umístěn aplikační server a dohledové pracoviště, kde ostraha uživatelsky dohlíží stav plotového detekčního systému.

Kamerový systém

Celý perimetr je zabezpečen pomocí kamerového systému, který se skládá z dvou kamer HIKVISION DS-2DE3A404IW-DE viz obrázek 42 a čtyř kamer DAHUA SD5A432XA-HNR viz obrázek 41. Kamery Hikvision jsou nainstalovány na kontejnerech ostrahy BLACK a ostrahy RED. Tyto kamery slouží k zabezpečení dohledu před vstupy do kontejnerů. Kamera, která je umístěna na kontejneru ostrahy RED je zároveň určena k dohledu nad skladišti zbraní. Kamery Dahua jsou umístěny na skladových kontejnerech a kontejneru KIS. Tyto kamery primárně slouží k dohledu nad ochranou perimetru. Systém Varya Perimeter je v oblasti dohledu nad plotovým systémem schopen při narušení perimetru zcela automaticky navést dané PTZ kamery na místo detekce narušení perimetru. Veškeré kamery jsou připojeny prostřednictvím LAN do FLU centrální jednotky.

Stanovení nákladů

Tabulka 17 Stanovení nákladů 1. návrhu

Materiál	Počet kusů	Cena za kus (Kč)	Cena celkem (Kč)
F5 maxi doplňkový průhledný plot	75	2 999,-	224 925 Kč
Plastová patka	78	249,-	19 422 Kč
Stabilizační ocelová základna	78	780,-	60 840 Kč
Bezpečnostní spojka	75	93,-	6 975 Kč
Jednostranný ocelový nástavec	78	266,-	20 748 Kč
Sada proti nadzvihnutí	78	204	15 912 Kč
Ostnatý drát	1000 m	5,-	5 000 Kč
Ústředna galaxy GD 520	1	18 000,-	18 000 Kč
Ovládací a programovací klávesnice	1	3 890,-	3 890 Kč
FLA 06 RFID tag	65	2 900,-	188 500 Kč
Plech pro montáž FLA-06	130	50,-	6 500 Kč
FLM monitorovací jednotka	2	28 480,-	56 960 Kč
FLU centrální jednotka	1	28 230,-	28 230 Kč
Modul reléový se svorkovnicí a přepínacím NC/NO kontaktem	1	250,-	250 Kč
Expandér se 16 výstupy 2EOL	1	7 350,-	7 350 Kč
SW Varia Perimeter	1	10 000,-	10 000 Kč
IP kamera Hikvision	2	8 819,-	17 638 Kč
IP kamera Dahua	4	28 386,-	113 544 Kč
Vnitřní světelná siréna	2	350,-	700 Kč
PoE switch 24x 10/100/l000 Base-T	1	17 000,-	17 000 Kč
PoE switch 4x 10/100/l000 Base-T	5	4 800,-	24 000 Kč
Software IP CAM	1	38 000,-	38 000 Kč
UPS 1500 VA	6	6 800,-	40 800 Kč
Ostatní materiál	1	20 000,-	20 000 Kč
Celková cena			945 184 Kč

Dílčí závěr

Navrhovaná varianta k zabezpečení její správné funkce vyžaduje stanovení režimových opatření. Je nutné definovat povinnosti a procedury ostrahy a chování ostatních příslušníků operačního střediska vrtulníkové letky. Mezi tato opatření patří kontrola vnější hranice plotu, kterou mají za úkol provádět příslušníci ostrahy BLACK formou nepravidelných obchůzek. Dále také režim vstupu do střeženého perimetru uživateli.

4.4.2 Druhý návrh řešení perimetrické ochrany – odstrašující varianta

Druhý návrh řešení je zaměřen na odstrašení potencionálního narušitele kombinací mechanických zábranných systémů a zvýšenou činností ostrahy BLACK. Přesto při nepozorovaném překonání mechanických záchranných systémů je narušení detekováno pomocí instalovaného laserového detekčního systému. V této variantě je také propojen detekční systém s dohledovým kamerovým systémem. V tomto případě dochází ke společnému zásahu příslušníků ostrahy. Grafický návrh varianty je uveden v příloze 2.

Druhá varianta řešení perimetrické ochrany se skládá z těchto prvků fyzické bezpečnosti:

- ústředna PZS, SW, dohled, ovládání, kabeláž
- mobilní plot s mobilní žiletkovou bariérou
- laserový detektor
- kamerový systém

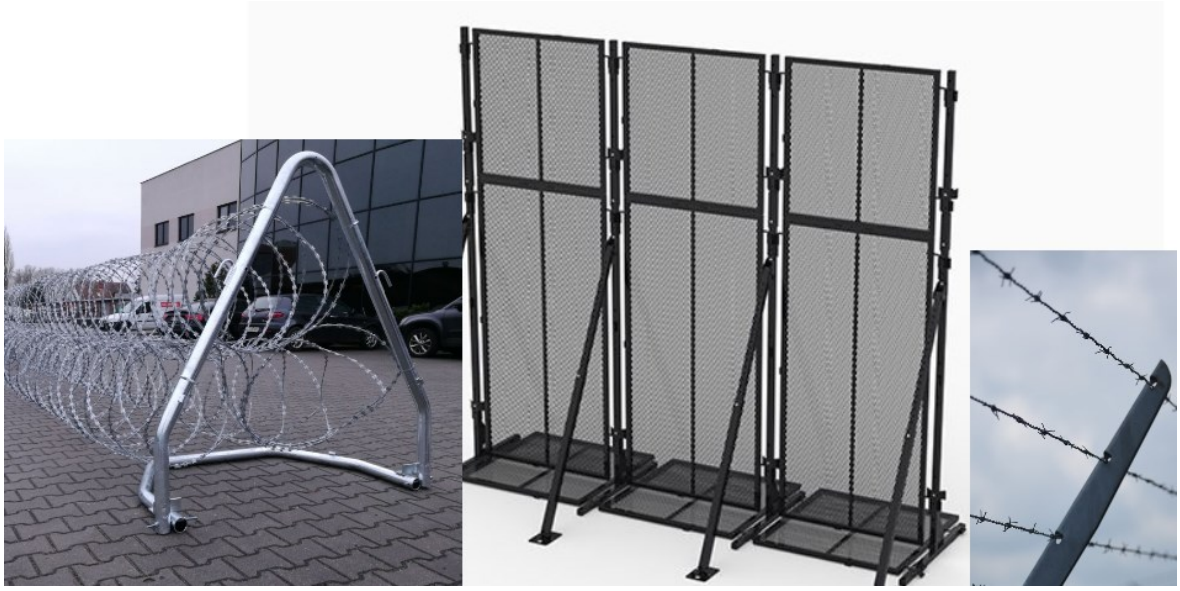
Ústředna PZS, SW, dohled, ovládání, kabeláž

Stejně jako v prvním návrhu je PZS navržen jako sběrnicový, zvolená ústředna je typ GALAXY GD-520, je instalována na stěnu kontejneru na pracovišti OUI v kontejneru ostrahy RED. Ovládání systému je umožněno z klávesnice, která je nainstalována na stanovišti ostrahy RED. Konfigurační a přehledový SW je instalován na aplikačním serveru u ostrahy RED. Uživatelská obsluha a dohled nad systémem ochrany je vyveden pomocí sítě LAN na stanoviště ostrahy RED do kontejneru ostrahy RED a na pracoviště ostrahy BLACK do kontejneru ostrahy BLACK.

Mobilní plot doplněný mobilní žiletkovou bariérou

Na základě analýzy plotových systémů jsem do této varianty vybral mobilní oplocení vysoké bezpečnosti. Tento plot působí více odstrašujícím dojmem, je vyšší a pevnější. Zajištění jeho

stability je provedeno aplikací pytlů naplněných pískem, které jsou položeny na spodní část plotu z vnitřní strany. Kolem vnější strany plotu jsou dále rozmístěny mobilní žiletkové bariéry, které nám znemožní nepozorované překonání plotu a jako vrcholová ochrana je doplněn o aplikaci ostnatého drátu. Další výhodou plotu je jeho vysoká variabilita sestavení.



Obrázek 52 Použité prvky MZS varianta 2

Laserový detektor

K detekci narušení perimetru jsou v této variantě použity laserové detektory OPTEX RLS 3060SH. Tento detektor byl specifikován ve třetí kapitole. Pro perimetrickou ochranu jsou využity tři kusy laserových detektorů, které jsou upevněny na velitelském, logistickém a skladovém kontejneru, jak je uvedeno v příloze 2. Pro komunikaci s ústřednou, kamerovým systémem a dohledovým pracovištěm, jsou detektory připojeny přes místní síť LAN.

Kamerový systém

Celý perimetr je zabezpečen pomocí kamerového systému, který doplňuje laserové detektory, slouží také k automaticky naváděné vizuální kontrole perimetru v případě vyhlášení poplachu. Skládá se z dvou kamer HIKVISION DS-2DE3A404IW-DE viz obrázek 42 a čtyř kamer DAHUA SD5A432XA-HNR viz obrázek 41. Kamery Hikvision jsou stejně jako v první variantě nainstalovány na kontejnerech ostrahy BLACK a ostrahy RED. Tyto kamery slouží k zabezpečení dohledu místa před vstupními dveřmi kontejnerů. Kamera umístěna na kontejneru ostrahy RED je zároveň určena k dohledu nad skladišti zbraní. Kamery Dahua jsou umístěny na stejných místech jako laserové detektory a primárně slouží k dohledu nad ochranou perimetru. Celý systém je rozdělen do zón a je schopen při

narušení perimetru zcela automaticky navést dané PTZ kamery na místo detekce narušení perimetru. Všechny kamery jsou připojeny do systému prostřednictvím LAN.

Stanovení nákladů

Tabulka 18 Stanovení nákladů 2. návrhu

Materiál	Počet kusů	Cena za kus (Kč)	Cena celkem (Kč)
mobilní oplocení vysoké bezpečnosti	60	5 500 Kč	330 000 Kč
mobilní žiletková bariéra	20	17 281 Kč	345 620 Kč
Ústředna galaxy GD 520	1	18 000 Kč	18 000 Kč
Jednostranný ocelový nástavec	60	300,-	18 000 Kč
Ostnatý drát	1000 m	5,-	5 000 Kč
Ovládací a programovací klávesnice	1	3 890 Kč	3 890 Kč
Laserový lokátor OPTEX RLS 3060SH	3	126 432 Kč	379 296 Kč
IP kamera Hikvision	2	8 819 Kč	17 638 Kč
IP kamera Dahua	3	28 386 Kč	85 158 Kč
Vnitřní světelná siréna	2	350 Kč	700 Kč
PoE switch 24x 10/100/l000 Base-T	1	17 000 Kč	17 000 Kč
PoE switch 4x 10/100/l000 Base-T	5	4 800 Kč	24 000 Kč
Software IP CAM	1	38 000 Kč	38 000 Kč
UPS 1500 VA	6	6 800 Kč	40 800 Kč
Ostatní materiál	1	20 000 Kč	20 000 Kč
Celková cena			1 343 102 Kč

4.4.3 Dílčí závěr

Obě navrhované varianty jsou složeny z mechanických zábranných systémů, poplachového zabezpečovacího systému a doplněny o dohledový kamerový systém. Do výsledné cenové kalkulace nejsou započítány náklady na montáž perimetrického systému, a to z důvodu provádění montáže výrobcem operačního střediska vrtulníkové letky a tím pádem téměř totožné ceny.

Výsledná cenová kalkulace u obou variant je:

- první navrhovaná variant 945 184,- Kč

- druhá navrhovaná varianta 1 343 102,- Kč

4.5 Multikriteriální analýza

Multikriteriální hodnocení variant je statistická metoda, která nám usnadňuje výběr vhodnější varianty z více navrhovaných variant podle definovaných kritérií. Jednotlivým kritériím jsou přiřazeny váhy podle dané preference zadavatelů. Výsledkem je výčet variant a jejich výsledné bodové ohodnocení na základě kterého je zvolena nejvhodnější varianta.

Na základě provedeného šetření u hlavních funkcionářů velení a řízení a technického personálu využívající operační středisko vrtulníkové letky byla stanovena následující kritéria

- úroveň zabezpečení
- náročnost rozvinutí a svinutí
- finanční nákladnost
- odolnost
- skladnost
- velikost perimetru

Určíme počet srovnání.

$$N = \binom{k}{2} = \frac{k * (k-1)}{2} = \frac{6 * (6-1)}{2} = 15$$

Pomocí metody párového srovnání v trojúhelníkovém schématu určíme počet preferenčních bodů a následně vypočítáme hodnotu váhy kritérií.

- úroveň zabezpečení = 5; $v_1 = \frac{n_1}{N} = \frac{5}{15} = 0{,}333$
- náročnost rozvinutí a svinutí = 2,5; $v_2 = \frac{n_2}{N} = \frac{2{,}5}{15} = 0{,}167$
- finanční nákladnost = 1; $v_3 = \frac{n_3}{N} = \frac{1}{15} = 0{,}067$
- odolnost = 1,5; $v_4 = \frac{n_4}{N} = \frac{1{,}5}{15} = 0{,}1$
- skladnost = 2; $v_5 = \frac{n_5}{N} = \frac{2}{15} = 0{,}133$
- velikost perimetru = 3; $v_6 = \frac{n_6}{N} = \frac{3}{15} = 0{,}2$

Nyní je nutné zvolit, jak jednotlivé varianty naplňují jednotlivá kritéria. Opět s pomocí hlavních uživatelů operačního střediska vrtulníkové letky a zabezpečujícího personálu, kteří jsou rozděleni do skupin velení (COM), řízení (CON) a technický personál (KIS). Nejprve byly těmto členům jednotlivé varianty presentovány a následně, členové stanovili, na číselné řadě od 1 do 10, jak jednotlivé varianty, podle jejich názoru, naplňují jednotlivá hodnotící kritéria. Jejich hodnocení bylo zprůměrováno a zaokrouhleno na celé číslo.

Tabulka 19 Posouzení naplnění kritérií jednotlivými návrhy

Název hodnotícího kritéria	COM		CON		KIS		Naplnění kritéria	
	N1	N2	N1	N2	N1	N2	Návrh 1	Návrh 2
úroveň zabezpečení	9	8	8	9	10	8	9	8
náročnost rozvinutí a svinutí	7	9	6	7	6	8	6	8
finanční nákladnost	7	6	9	5	8	6	8	6
odolnost	8	6	9	6	9	6	9	6
skladnost	5	3	7	4	6	4	6	4
velikost perimetru	7	6	7	5	5	4	7	5

Po posouzení naplnění hodnotících kritérií jednotlivými navrhovanými variantami je nutné stanovit výhodnější variantu systému perimetrické ochrany operačního střediska vrtulníkové letky. Konečný počet bodů pro jednotlivé varianty je uveden v následující tabulce.

Tabulka 20 Celkové porovnání navrhovaných variant

Název hodnotícího kritéria	Naplnění kritéria		Váha kritéria	Naplnění kritéria	
	N1	N2		Návrh 1	Návrh 2
úroveň zabezpečení	9	8	0,333	2,997	2,664
náročnost rozvinutí a svinutí	6	8	0,167	1,002	1,336
finanční nákladnost	8	6	0,067	0,536	0,402
odolnost	9	6	0,1	0,9	0,6
skladnost	6	4	0,133	0,798	0,532
velikost perimetru	7	5	0,2	1,4	1
Výsledné srovnání vhodnosti návrhů				7,633	6,534

Pomocí Fullerovy metody multikriteriálního hodnocení dvou navrhovaných variant perimetrické ochrany operačního střediska vrtulníkové letky, dle definovaných hodnotících kritérií bylo určeno, že vhodnějším návrhem řešení je 1. NÁVRH.

5 IDEOVÝ PROJEKT ZAJIŠTĚNÍ PERIMETRICKÉ OCHRANY OPERAČNÍHO STŘEDISKA VRTULNÍKOVÉ LETKY

Cílem této kapitoly je zpracovat ideový projekt systému perimetrické ochrany hypotetického operačního střediska vrtulníkové letky. Toto středisko je koncipováno jako rozmístitelné místo velení vrtulníkové letky s širokou škálou možností rozmístění prostředků a pracovišť.

5.1 Záměr realizace

Projekt je zpracován z důvodu posílení zabezpečení fyzické bezpečnosti operačního střediska vrtulníkové jednotky. Předmětem projektu je kompletní dodávka funkční, nestacionární perimetrické ochrany, složena z vhodných technických prostředků nestacionární perimetrické ochrany. Tyto prvky jsou součástí celkového komplexu zajištění fyzické bezpečnosti. Veškeré prostředky jakožto i celý zhotovený systém perimetrické ochrany musí být certifikován NÚKIB pro zpracování utajovaných informací do stupně utajení „Tajné“, „NATO secret“ a „Mission secret“, a to převážně z důvodu zamezení negativního vlivu na současné technické řešení operačního střediska vrtulníkové letky.

5.2 Popis místa instalace návrhu perimetrické ochrany

Operační středisko vrtulníkové letky je situováno do komplexu rozmístitelných prvků, které jsou tvořeny z pogumovaných stanů s podpůrnou ocelovou konstrukcí typů SU 711 a SU 660 a přepravních kontejnerů typu ISO-1 C. Operační středisko je také vybaveno přechodovými stany S2K480 a SK 650, oba typy stanů slouží k vytvoření přechodů mezi stany SU 711, SU660 a kontejnery. Operační stany jsou jimi propojeny a v případě S2K480 doplněny o propojení s kontejnery ISO 1 C.

Celkové počty využitých prvků operačního střediska letky jsou stanoveny na základě požadavků na obsazení jednotlivých tabulkových míst, vyčleňovaného úkolového uskupení praporního typu. Toto operační středisko vrtulníkové letky je navrhováno natolik modulárně, aby umožňovalo zasazení jednotky od počtu cca 40 osob v té nejnižší a nejméně nákladné variantě, pro zabezpečení jednodušších úkolů. Až po maximální variantu koncipovanou pro celkový počet nasazených cca 120 osob. Celkové vnější rozměry hypotetického operačního střediska vrtulníkové letky jsou 36 x 36 m. Půdorys výsledného hypotetického komplexu, složeného z výše uvedených prvků je uveden na následujícím obrázku.

Obrázek 53 Půdorys výsledného hypotetického komplexu

Operační středisko vrtulníkové letky musí mít zabezpečen jediný vstup do perimetru, a to přes kontejner ostrahy, kde je vykonávána služba v nepřetržitém režimu.

5.2.1 Podmínky výstavby operačního střediska letky

Místo zasazení operačního střediska vrtulníkové letky musí být zvoleno nejlépe na pevném, nenasákavém podkladu, v případě nerovností je nutné předem místo výstavby ženijně upravit. Nesmí se zde nacházet kameny, keře, stromy a jiné podobné nežádoucí prvky, které by mohly způsobit poškození materiálu.

5.2.2 Obsluha

Všichni příslušníci obsluhy splňují kvalifikaci v elektrotechnice §4 Pracovníci poučení dle vyhlášky 50/1978 Sb., o odborné způsobilosti v elektrotechnice, minimálně jeden příslušník musí splňovat kvalifikaci v elektrotechnice §6 Pracovníci pro samostatnou činnost dle vyhlášky 50/1978 Sb. Všichni příslušníci procházejí školením a mají za povinnost znát a

dodržovat zásady použití, které jsou uvedeny v provozní a technické dokumentaci rozmístitelného prostředku.

5.2.3 Současný stav zabezpečení

Operační středisko vrtulníkové letky, nedisponuje v současné chvíli, žádnými technickými prostředky k zajištění perimetrické ochrany. Při působení mimo stálou dislokaci je nutné pro výstavbu zabezpečené oblasti, zapůjčit plot o celkové délce 200 metrů, což přináší pravidelné nežádoucí časové i finanční náklady. Chybějící technické prostředky jsou nahrazeny zvýšenou ostrahou zabezpečené oblasti, která provádí střežení perimetru nepravidelnými obchůzkami.

5.3 Požadavky zadavatele projektu

Dle požadavků zadavatele je při navrhování jednotlivých variant nutné důsledně dbát na jednoduchost a zároveň funkčnost celého systému perimetrické ochrany operačního střediska vrtulníkové jednotky. Zároveň je nezbytné splnění požadavků zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti a souvisejících předpisů, a to převážně v souvislosti s vydáním certifikace NÚKIB. Je stanoven požadavek zadavatele v použití pouze jednoho detekčního systému narušení perimetru, jehož funkčnost bude rozšířena o dohledový kamerový systém. Dalším požadavkem je použití perimetrického systému operačního střediska vrtulníkové letky ve více variantách rozmístění vnitřcích pracovišť, stanů a kontejnerů, na jeho vysokou modularitu rozmístění technických prvků. A tím i umístění technologií systému perimetrické ochrany.

5.3.1 Stupeň zabezpečení

Z důvodu začlenění jednotky do brigádního úkolového uskupení NATO je operační středisko vrtulníkové letky koncipováno jako zabezpečená oblast stupně utajení „Tajné“, „NATO secret“ a Mission secret“. S tím souvisí i požadavky na certifikaci technických prostředků perimetrické ochrany.

5.3.2 Třídy prostředí

Z hlediska prostředí je nutné, aby všechny prvky systému perimetrické ochrany, které jsou určeny pro venkovní použití splňovaly třídu prostředí Třída IV. – Venkovní všeobecné a prvky které budou instalovány do kontejnerů Třída III. – Venkovní chráněné, a to převážně z důvodu velkých změn teplot a vlhkosti.

5.3.3 Propojení s nepoplachovými aplikacemi

Mezi požadavky zadavatele není propojení systému s nepoplachovými aplikacemi například evidence kontroly vstupu, evidence docházky apod.

5.4 Návrh řešení systému ochrany

S přihlédnutím k požadavkům zadavatele je systém složen z následujících prvků:

- ústředna PZS, SW, dohled, ovládání, kabeláž
- mobilní plot s vrcholovou ochranou
- plotový detekční systém
- kamerový systém

Umístění prvků perimetrické ochrany operačního střediska vrtulníkové letky je uveden v příloze č. 1.

5.4.1 Ústředna PZS, SW, dohled, ovládání, kabeláž

PZS je navržen jako sběrnicový, zvolená ústředna je typ GALAXY GD-520, je instalována na stěnu kontejneru na pracovišti OUI v kontejneru ostrahy RED. Ovládání systému je umožněno z klávesnice, která je nainstalována na stanovišti ostrahy RED. Konfigurační a přehledový SW je instalován na aplikačním serveru v kontejneru ostrahy RED. Uživatelská obsluha a dohled nad poplachovým zabezpečovacím systémem je vyveden pomocí sítě LAN na stanoviště ostrahy RED do kontejneru ostrahy RED. Systém PZS je zálohován vlastním zálohovaným zdrojem vně ústředny dle ČSN EN 50131-1 ed2, který je umístěn na pracovišti OUI. Kabeláž je vedena vnitřními kabelovými rozvody zakončenými v datových schránách na vnějším plášti kontejneru. Takto je zabezpečeno kabelové spojení mezi jednotlivými subsystémy v odlišných kontejnerech, kabely mezi kontejnery a subsystémy jsou vedeny v zabezpečeném perimetru volně.

5.4.2 Mobilní plot s vrcholovou ochranou

Na základě analýzy plotových systémů jsem do této varianty zvolil mobilní plotový systém F5 maxi doplňkový průhledný plot, který je instalován pomocí plastových patek. Tyto jsou usazeny do stabilizačních ocelových základen. Dále je plot doplněn o ostnatý drát, který je usazen do jednostranných ocelových nástavců. Tento plot je dostatečně pevný a pokud je

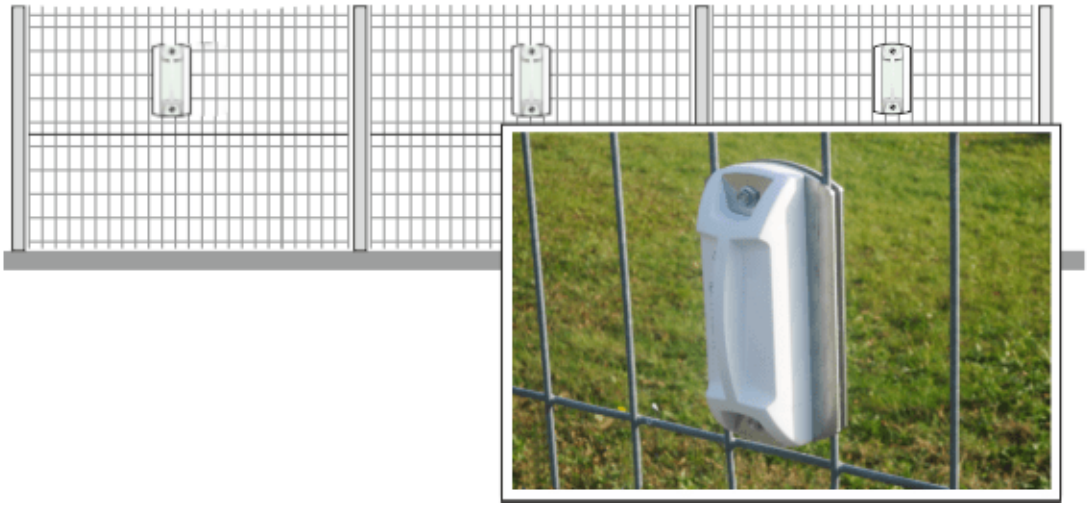
usazen do zvolených základen a zatížen plastovou patkou a následně ukotven dvěma kotevními kolíky k zemi, je i dostatečně stabilní.

Obrázek 54 Dílčí části MZS

K zabezpečení perimetru, jehož obvod měří 240 metrů bude pořízeno 75 plotových dílců F5 maxi doplňkový průhledný plot, 78 stabilizačních ocelových základen, 78 plastových patek, 75 bezpečnostních spojek, 78 jednostranných ocelových nástavců, 1000 metrů ostnatého drátu.

5.4.3 Plotový detekční systém

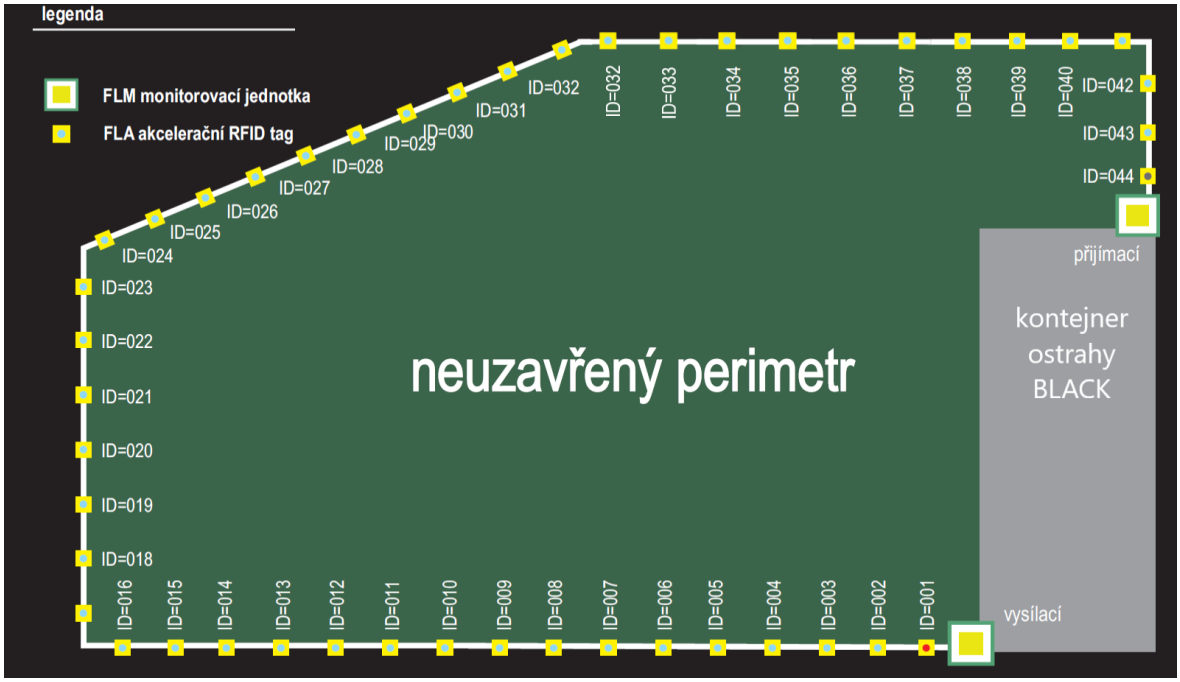
K zabezpečení detekce narušení perimetru přelézajícím narušitelem nebo prostříháváním plotu je vybudován detekční plotový systém od firmy Varya Perimeter. Detekce narušení pracuje na principu 3-osých akceleračních detektorů FLA, které zaznamenávají jakýkoli pohyb prvku, na který jsou detektory instalovány. Komunikace mezi jednotlivými detektory probíhá bezdrátově pomocí technologie RFID. Technická data plotového detekčního systému jsou uvedena ve třetí kapitole v Tabulka 1. Tento detekční plotový systém je možné aplikovat i na mobilní typ oplocení. Pro instalaci je nutné k tagu FLA doobjednat dva montážní díly typu T14. Pro spolehlivou funkci tohoto systému je nutné zabezpečit, aby nedocházelo k prorůstání dřevin, keřů a trávy do plotových dílců. Toto by mělo za následek nárůst planých poplachů. Je také zakázáno na plot instalovat jakékoli cedule nebo jiné prvky tohoto typu. Konkrétní instalace tagů je zobrazena na obrázku č. 55.



Obrázek 55 Příklad instalace tagu FLA [39]

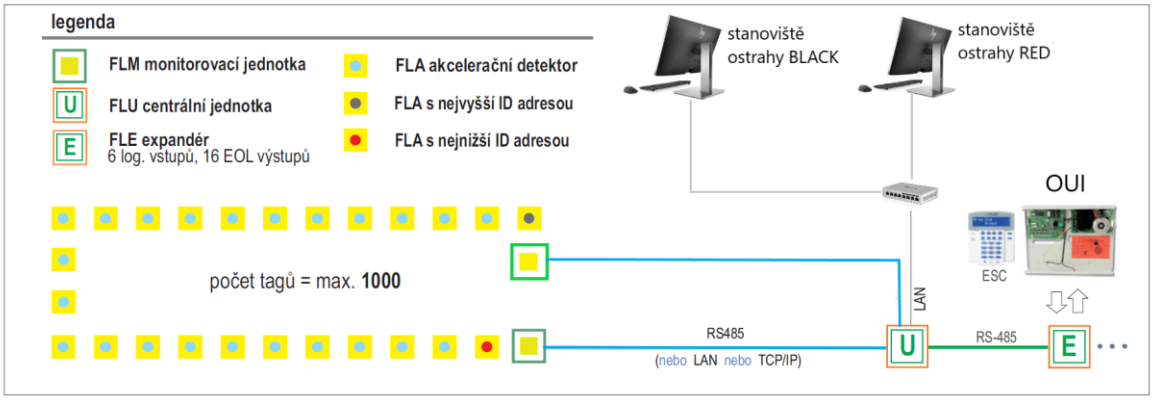
Z důvodu eliminace planých poplachů při špatných meteorologických podmínkách bude provedena instalace 1 tagu FLA-06 na každý plotový dílec. Dodávka sytému pro naší aplikaci bude obsahovat 65 tagů FLA-06 a 130 montážních dílků typu T14.

Plotový systém je z důvodu pozdější modularity navržen jako neuzavřený, proto je nutné použít dvě FLM monitorovací jednotky. Tyto jednotky jsou umístěny v kontejneru ostrahy BLACK a jejich umístění je variabilní a lze jej přemístit na jiné místo v operačním středisku vrtulníkové letky. V případě přemístění je nutné zabezpečit správné vedení kabeláže.



Obrázek 56 Návrh rozmístění FLA a FLM [39]

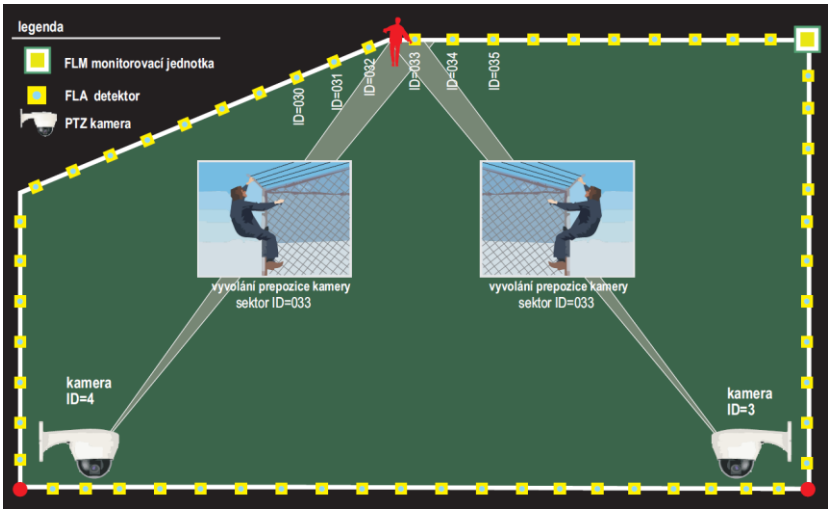
Jednotky FLM jsou pomocí LAN připojeny do centrální jednotky označené FLU. Tato jednotka je umístěna v kontejneru ostrahy RED. V tomto kontejneru je umístěna i PZS ústředna, do které je jednotka FLU připojena přes FLE expandér a pomocí rozhraní RS 485. V kontejneru ostrahy RED je na stanovišti, kde ostraha vykonává službu v nepřetržitém režimu, umístěno dohledové pracoviště, kde ostraha uživatelsky dohlíží stav plotového systému a aplikační server, kde je nainstalován potřebný software, který je součástí dodávky.



Obrázek 57 Rozmístění komponent plotového systému [39]

5.4.4 Kamerový systém

Celý perimetr je zabezpečen pomocí kamerového systému, který se skládá z dvou kamer HIKVISION DS-2DE3A404IW-DE viz obrázek 42 a čtyř kamer DAHUA SD5A432XA-HNR viz obrázek 42. Kamery Hikvision jsou nainstalovány na kontejnerech ostrahy BLACK a ostrahy RED. Tyto kamery slouží k zabezpečení dohledu před vstupy do kontejnerů, potažmo do jednotlivých zabezpečených perimetrů. Kamera, která je umístěna na kontejneru ostrahy RED je zároveň určena k dohledu nad skladišti zbraní, tyto kamery disponují detekcí pohybu a infračerveným přísvitem. Kamery Dahua jsou umístěny na skladových kontejnerech a kontejneru KIS, tyto kamery primárně slouží k dohledu nad chráněným perimetrem a v případě detekce narušitele k vyhodnocování situace při narušení. Systém Varya Perimeter je v oblasti dohledu nad plotovým systémem schopen při narušení perimetru zcela automaticky navést dané PTZ kamery na místo, kde bylo detekováno narušení perimetru. Všechny kamery jsou připojeny prostřednictvím LAN do FLU centrální jednotky. Systém Varya Perimeter umí řídit najednou několik PTZ kamer. Systém navádění kamer je natolik variabilní že dokáže sledovat více bodů narušení v jeden okamžik. Nastavení je možné konfigurovat, dle aktuálních požadavků uživatele.



Obrázek 58 Ukázka namíření kamer na místo narušení [39]

5.4.5 Cenová kalkulace

Tabulka 21 Přehled materiálu

Materiál	Počet kusů	Cena za kus (Kč)	Cena celkem (Kč)
F5 maxi doplňkový průhledný plot	75	2 999,-	224 925 Kč
Plastová patka	78	249,-	19 422 Kč
Stabilizační ocelová základna	78	780,-	60 840 Kč
Bezpečnostní spojka	75	93,-	6 975 Kč
Jednostrannch ocelový nástavec	78	266,-	20 748 Kč
Sada proti nadzvihnutí	78	204	15 912 Kč
Ostnatý drát	1000 m	5,-	5 000 Kč
Ústředna galaxy GD 520	1	18 000,-	18 000 Kč
Ovládací a programovací klávesnice	1	3 890,-	3 890 Kč
FLA 06 RFID tag	65	2 900,-	188 500 Kč
Plech pro montáž FLA-06	130	50,-	6 500 Kč
FLM monitorovací jednotka	2	28 480,-	56 960 Kč
FLU centrální jednotka	1	28 230,-	28 230 Kč
Modul reléový se svorkovnicí a přepínacím NC/NO kontaktem	1	250,-	250 Kč
Expandér se 16 výstupy 2EOL	1	7 350,-	7 350 Kč
SW Varia Perimeter	1	10 000,-	10 000 Kč
IP kamera Hikvision	2	8 819,-	17 638 Kč
IP kamera Dahua	4	28 386,-	113 544 Kč
Vnitřní světelná siréna	2	350,-	700 Kč
PoE switch 24x 10/100/l000 Base-T	1	17 000,-	17 000 Kč
PoE switch 4x 10/100/l000 Base-T	5	4 800,-	24 000 Kč
Software IP CAM	1	38 000,-	38 000 Kč
UPS 1500 VA	6	6 800,-	40 800 Kč
Ostatní materiál	1	20 000,-	20 000 Kč
Celková cena			945 184 Kč

Ve výše uvedené tabulce je stanovena výsledná cena za materiál vybrané varianty perimetrické ochrany operačního střediska vrtulníkové letky. Cena instalace a montáže je po dohodě se zadavatelem stanovena na 661 000,-.

Celková cena projektu je 1 606 812,- Kč bez DPH

5.5 Začlenění perimetrického systému do komplexu fyzické bezpečnosti

Fyzická bezpečnost je složena z:

- Výkonu ostrahy
- Režimových opatření
- Technických prostředků

K zabezpečení ostrahy operačního střediska vrtulníkové letky je zřizována strážní služba, která se skládá ze dvou prvků:

1. Ostraha perimetru RED– tato ostraha je složena z 3 osob

    1 x dozorčí ZO – označen žlutou rukávovou páskou

    2 x ostraha ZO technik – označen červenou rukávovou páskou

Úkolem příslušníků ostrahy RED je střežení vnitřního perimetru operačního střediska letky, a zabezpečení technické podpory. Střežení se provádí pomocí systému nepravidelných obchůzek. Interval těchto obchůzek nesmí přesáhnou 1 hodinu. Během obchůzky se také zaměřují na vizuální kontrolu plotu z jeho vnitřní strany a důslednou kontrolu celého vnitřního perimetru se zaměřením na kontrolu kabeláže a datových rozvodů. Velitel této ostrahy je podřízen NŠ. Jakékoli události a průběh činnosti služby je povinen hlásit na TOC a zaznamenat do knihy předání a převzetí služby. Tato kniha je umístěna na stanovišti ostrahy RED.

Na stanovišti ostrahy RED je zřízeno dohledové pracoviště ostrahy perimetrického systému operačního střediska vrtulníkové jednotky. Toto pracoviště, je připojeno do celého systému ochrany pomocí sítě LAN. Pracoviště umožňuje realizovat dohled prostoru před kontejnerem ostrahy RED. Je zde možnost ovládání kamery. Další možností je dohled nad celkovým chráněným perimetrem pomocí všech kamer, instalovaných v perimetrickém systému. Systém je nastaven tak, že v případě vyhlášení narušení perimetru, pokud je to možné dojde k automatickému natočení kamery, kterou v tento okamžik obsluha neovládá.

Pokud není ani jedna z takovýchto kamer volná, je převzato ovládání jakékoli vhodné kamery. Ze stanoviště ostrahy RED je umožněn dohled a konfigurace nad stavem všech dílčích systémů (plotového detekčního systému, IP kamerového dohledového systému). Zastřežení a odstřežení jednotlivých podsystémů perimetrické ochrany, je možné z dohledového pracoviště ostrahy RED. Vyhlášení poplachu je také indikováno světelnou sirénou v kontejneru ostrahy RED.

2. Ostraha perimetru BLACK – tato ostraha je složena z 3 osob

    1 x velitel stráže – označen bílou rukávovou páskou

    2 x strážný – označen červenou rukávovou páskou

Úkolem příslušníků ostrahy BLACK je zabezpečení vstupu pouze oprávněným osobám do střeženého perimetru a provádění střežení vnějšího perimetru operačního střediska letky. Střežení se provádí pomocí systému nepravidelných obchůzek. Interval těchto obchůzek nesmí přesáhnou 1 hodinu. Během obchůzky se také zaměřují na vizuální kontrolu plotu z jeho vnější strany. Velitel této ostrahy je podřízen veliteli ostrahy RED. Jakékoli události a průběh činnosti služby je povinen hlásit veliteli ostrahy RED a zaznamenat do knihy předání a převzetí služby. Tato kniha je umístěna na stanovišti ostrahy BLACK.

Na stanovišti ostrahy BLACK je zřízeno dohledové pracoviště perimetrického systému operačního střediska vrtulníkové jednotky. Toto pracoviště, je připojeno do celého systému ochrany pomocí sítě LAN. Pracoviště umožňuje dohled prostoru před kontejnerem ostrahy BLACK s možností ovládání kamery před jeho vstupem. Další možností je dohled nad celkovým chráněným perimetrem pomocí ovládání všech kamer instalovaných v perimetrickém systému. Systém je nastaven tak, že v případě vyhlášení poplachu o narušení perimetru, pokud je to možné, dojde k automatickému natočení kamery, kterou v tento okamžik obsluha neovládá. Pokud není ani jedna z takovýchto kamer volná, je převzato ovládání jakékoli vhodné kamery. Vyhlášení poplachu je indikováno světelnou sirénou v kontejneru ostrahy BLACK.

Režim vstupu

Samostatně vstupovat do zabezpečeného prostoru smí pouze oprávněné osoby, které splňují zákonem stanovené podmínky pro přístup k utajovaným informacím alespoň stupně utajení Tajné (prokáží se osvědčením fyzické osoby na T nebo PT, platným poučením a jsou zařazeni na systemizovaném místě s tímto stupněm utajení). Seznam oprávněných osob schválený velitelem operace vede BM. Ostatním osobám (návštěvám) je povolen vstup

pouze v doprovodu oprávněné osoby. Oprávněná osoba musí zabezpečit, aby se návštěva neseznámila s utajovanými informacemi. Návštěva musí být doprovázena po celou dobu pobytu v tomto objektu. Návštěvám povoluje vstup BM, BSTO, STO. Před vstupem do tohoto prostoru musí být návštěva zapsána do knihy návštěv na stanovišti ostrahy BLACK. Za návštěvu po celou dobu odpovídá doprovod.
Z důvodu rozlišení jednotlivých osob (oprávněné, návštěva) jsou příslušníci jednotky vybaveni ID kartou, kterou jsou povinni nosit viditelně na oděvu.

5.6 Závěrečná ustanovení

Celková dodávka perimetrické ochrany operačního střediska vrtulníkové letky musí obsahovat kompletní zadávací dokumentaci. Tato dokumentace musí být předána zadavateli zakázky, před zahájením prací, ke schválení. Při vzniku změn v projektu, musí být tyto změny projednány se zadavatelem projektu.

Součástí projektu je dodání veškeré technické a provozní dokumentace, školení technického personálu a uživatelů systému a zajištění záručních oprav. Seznam požadované dokumentace bude předložen zhotoviteli před zahájením projektu.

ZÁVĚR

Cílem diplomové práce bylo vytvořit dva návrhy zabezpečení perimetrické ochrany smyšleného, rozmístitelného operačního střediska vrtulníkové letky. Návrhy posoudit a na základě požadavků zástupců prvků velení, řízení a personálu komunikačních a informačních systémů vybrat vhodnější variantu. Vybraný návrh rozpracovat ve formě ideového projektu. Diplomová práce byla rozdělena na dvě části teoretickou a praktickou.

Teoretická část diplomové práce byla rozdělena do dvou kapitol. První kapitola byla zaměřena na objasnění problematiky míst velení v poli a popsány způsoby jejich ochrany. Dozvěděli jsme se, jak jsou místa velení začleněna v systému velení a řízení Armády České republiky. Byl zde popsán celkový proces velení a řízení, jako nikdy nekončící koloběh činností, jejichž cílem je úspěšné splnění operace. Také se zde můžeme dozvědět jaké jsou hlavní funkce míst velení a podle jakých kritérií je můžeme členit. Dále zde byly identifikovány a analyzovány bezpečnostní hrozby, které místa velení ohrožují. Zde bylo nutné specifikovat bezpečnostní hrozby a stanovit které jsou předmětem ochrany, sil a prostředků aliančních partnerů a které hrozby jsme schopni minimalizovat silami a prostředky vlastními. Došli jsme ke zjištění, že hypotetickým místem velení je operační středisko vrtulníkové letky a stanovili požadavek na možnost nakládání s utajovanými informacemi do stupně utajení „Tajné“, „NATO secret“ a „Mission Secret“. Z toho důvodu byla v závěru první kapitoly definována legislativa k zajištění fyzické bezpečnosti při zpracovávání utajovaných informací. Z legislativních předpisů byly popsány zákon 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti, ve kterém jsou utajované informace členěny do kategorií: Vyhrazené, Důvěrné, Tajné a Přísně tajné. Další popisovaným předpisem byla Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů a vnitřní předpisy pro zajištění ochrany utajovaných informací v objektech AČR, vydané ministerstvem obrany Rozkaz ministra obrany 14/2013, Věstníku o ochraně utajovaných informací v rezortu Ministerstva obrany a Normativní výnos Ministra obrany 77/2013 Věstníku, Fyzická bezpečnost v rezortu Ministerstva obrany. Zde byly upřesněny jednotlivé body fyzické bezpečnosti a bezpečnost utajovaných informací v polních podmínkách. Druhá kapitola byla věnována problematice perimetrické ochrany, jako dílčího prvku fyzické bezpečnosti, kterou je možné rozdělit na předmětovou, prostorovou, plášťovou a perimetrickou ochranu. Také zde bylo popsáno zajištění fyzické bezpečnosti, jako vhodně zvolené kombinace fyzické ostrahy, režimových opatření a prostředků technické ochrany.

Praktická část diplomové práce byla rozdělena do tří kapitol. Ve třetí kapitole byly analyzovány možnosti zajištění perimetrické ochrany se zaměřením na technické prostředky, které jsou k nestacionární perimetrické ochraně vhodné. Upřesnili jsme požadavky zadavatele projektu se zaměřením na omezení přepravní kapacity, jednoduchosti instalace a nízkých pořizovacích nákladů. Z mechanických zábranných systémů se jednalo o analýzu mobilních plotů, vrcholové a doplňkové ochrany. Z oblasti elektronických bezpečnostních systémů byly jako vhodné vybrány systémy založeny na akcelerometrických, pasivních infračervených, mikrovlnných a laserových detektorech a mikrovlnných a infračervených závorách. Také byly analyzovány kamerové systémy a jako vhodné vybrány IP PTZ dome kamery. Ve čtvrté kapitole byl vytvořen model hypotetického místa velení v polních podmínkách a provedena analýza rizik. V závěru čtvrté kapitoly byly vytvořeny dva návrhy perimetrické ochrany hypotetického operačního střediska vrtulníkové letky. První byl pojmenován detekční varianta a druhý odstrašující varianta. Pomocí multikriteriální analýzy a ve spolupráci s uživateli z oblasti velení, řízení a KIS byla vybrána detekční varianta jako vhodnější. Tato varianta byla v páté kapitole rozpracována ve formě ideového projektu.

Protože pracuji s mobilními prostředky AČR domnívám se, že tato diplomová práce může být základem pro vytvoření projektu vznikající perimetrické ochrany některého z nestacionárních komunikačních a informačních systémů, které tvoří základ rozmístitelného místa velení, požívaného v Armádě České republiky.

SEZNAM POUŽITÉ LITERATURY

[1] *Velení, řízení a součinnost v operacích pod národním velením* [online]. In: . Univerzita obrany Brno [cit. 2020-08-08]. Dostupné z: https://moodle.unob.cz/pluginfile.php/42089/mod_resource/content/1/T%2013%2C14%20Velen%C3%AD%2C%C5%99%C3%ADzen%C3%AD%20a%20sou%C4%8Dinnost%20v%20operac%C3%ADch%20pod%20n%C3%A1rodn%C3%ADm%20velen%C3%ADm.pdf

[2] ČERNÝ, Jiří. *Velení vojskům a štábní práce* [online]. [cit. 2020-08-08]. Dostupné z: http://docplayer.cz/8542402-Studijni-opora-cast-i-7-semestr-zpracoval-pplk-ing-jiri-cerny-ph-d.html

[3] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management I.* 1. vydání. Zlín: Radim Bačuvčík - VeRBuM, 2011. ISBN 978-80-87500-05-7.

[4] ZEMAN, Petr, ed. *Česká bezpečnostní terminologie: výklad základních pojmů*. 1. vyd. Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2002. ISBN 8021030372.

[5] NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD. *Prováděcí právní předpisy* [online]. Praha [cit. 2020-07-12]. Dostupné z: https://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/

[6] ČESKÁ REPUBLIKA. *Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti*. In: . Zákony pro lidi.cz [online]: © AION CS 2010-2020, 2005, ročník 2005, číslo 412. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-412

[7] NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD. *Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů* [online]. Brno [cit. 2020-07-12]. Dostupné z: https://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/1087-vyhlaska-c-5282005/

[8] ČESKÁ REPUBLIKA. *Rozkaz ministra obrany ČR č. 14/2013, Věstníku o ochraně utajovaných informací v rezortu Ministerstva obrany.* In: . Ministerstvo obrany, ročník 2013, číslo 14.

[9] ČESKÁ REPUBLIKA. *Normativní výnos Ministerstva obrany č. 77/2013*. In: . Ministerstvo obrany, ročník 2013, číslo 77.

[10] LAPKOVÁ, Dora. *Presentace: Technologie komerční bezpečnosti I: Fyzická ostraha*. Zlín, 2018.

[11] LAPKOVÁ, Dora. *Presentace: Technologie komerční bezpečnosti I: Režimová opatření*. Zlín, 2018.

[12] UHLÁŘ, Jan. *Technická ochrana objektů: Elektrické zabezpečovací systémy II*. 2. vyd. Praha: Policejní akademie České republiky v Praze, 2009. ISBN 9788072513130.

[13] UHLÁŘ, Jan. *Technická ochrana objektů: Mechanické zábranné systémy II*. Vyd. 1. Praha: Vydavatelství PA ČR, 2004. ISBN 80-7251-172-6.

[14] IVANKA, Ján. *Mechanické zábranné systémy*. Vydání druhé. Zlín: Univerzita Tomáše Bati ve Zlíně, 2014. ISBN 978-80-7454-427-9.

[15] KOŇAŘÍK, Jiří. *Ochrana perimetru mechanickými zábrannými systémy*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010, 58 s. Dostupné z:

http://hdl.handle.net/10563/14644. Tomas Bata University in Zlín. Faculty of Applied Informatics, Ústav elektrotechniky a měření. Vedoucí práce Kameník, Jiří.

[16] Podhrabové desky. *Podhrabove-desky-plot.cz* [online]. [cit. 2020-07-04]. Dostupné z: http://www.podhrabove-desky-plot.cz/podhrabove-desky/

[17] *Zabezpečovací technika damacom: El. zabezpečovací systém* [online]. [cit. 2020-06-21]. Dostupné z: https://www.alarmshop.cz/el-zabezpecovaci-system---ezs

[18] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management V.* 1. vydání. Zlín: Radim Bačuvčík - VeRBuM, 2015. ISBN 978-80-87500-67-5.

[19] *Atp journal: Ústředny poplachového zabezpečovacího a tísňového systému* [online]. [cit. 2020-06-22]. Dostupné z: https://www.atpjournal.sk/budovy/rubriky/prehladove-clanky/ustredny-poplachoveho-zabezpecovaciho-atisnoveho-systemu.html?page_id=14869

[20] *Security technologies: Perimetrické systémy (PER)* [online]. [cit. 2020-06-21]. Dostupné z: https://www.security.cz/perimetricke-systemy-per--2420.html

[21] *ADI a resideo company: Tísňové NC/NO tlačítko výklopné s pamětí poplachu* [online]. [cit. 2020-06-29]. Dostupné z: https://adiglobal.cz/cz/produkty110:86380/tisnove-nc-no-tlacitko-vyklopne-s-pameti-poplachu

[22] *ADI a resideo company: Tísňové tlačítko ND100-GLT s konvenční technologií - reléovým výstupem* [online]. [cit. 2020-06-29]. Dostupné z: https://adiglobal.cz/cz/produkty110:13411342/tisnove-tlacitko-nd100-glt-s-konvencni-technologii-releovym-vystupem

[23] *ADI a resideo company: Detektor poslední bankovky* [online]. [cit. 2020-06-29]. Dostupné z: https://adiglobal.cz/cz/produkty110:11004470/detektor-posledni-bankovky

[24] *ABSOLON Alarm: Sirény a majáky - Strana 2* [online]. [cit. 2020-06-30]. Dostupné z: https://www.absolon.cz/katalog/pzts--ezs_74/sireny-a-majaky_392/_strana=2

[25] *Atp journal: Ústředny poplachového zabezpečovacího a tísňového systému* [online]. Univerzita Tomáše Bati ve Zlíně [cit. 2020-06-29]. Dostupné z: https://www.atpjournal.sk/budovy/rubriky/prehladove-clanky/ustredny-poplachoveho-zabezpecovaciho-atisnoveho-systemu.html?page_id=14869

[26] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management II.* 1. vydání. Zlín: Radim Bačuvčík - VeRBuM, 2012. ISBN 978-80-87500-19-4.

[27] Funkce Wide Dynamic Range (WDR). *IPSecure.cz* [online]. [cit. 2020-07-02]. Dostupné z: https://www.ipsecure.cz/clanky/technicke-pojmy/funkce-wide-dynamic-range/

[28] Komprese H.265 / H.265+ již brzy v nabídce!. *VIAKOM* [online]. [cit. 2020-07-02]. Dostupné z: https://www.viakom.cz/komprese-h-265-h-265-jiz-brzy-v-nabidce/article-104

[29] Jak vybrat vhodnou IP kameru?. *IPSecure.cz* [online]. [cit. 2020-07-01]. Dostupné z: https://www.ipsecure.cz/clanky/rady-a-tipy/jak-vybrat-vhodnou-ip-kameru/

[30] ŠEVČÍK, Jiří. Princip činnosti, typy a komunikační rozhraní IP kamer. *TZB info* [online]. [cit. 2020-06-30]. Dostupné z: https://elektro.tzb-info.cz/10480-princip-cinnosti-typy-a-komunikacni-rozhrani-ip-kamer

[31] Elektronická kontrola vstupu (EKV). *FIDES* [online]. [cit. 2020-07-02]. Dostupné z: https://fides.cz/technologicke-prostredky/ekv.html

[32] Přístupové systémy. *Tomáš Koníček, s.r.o.* [online]. [cit. 2020-07-02]. Dostupné z: https://www.tomaskonicek.cz/pristupove-systemy-851

[33] *STAVO-SHOP.CZ: Mobilní oplocení Standard 3,45 x 2,02 m* [online]. [cit. 2020-06-19]. Dostupné z: https://www.stavo-shop.cz/mobilni-oploceni-standard-345-x-202-m?gclid=CjwKCAjwxLH3BRApEiwAqX9arUpbNmgR6mkabo-lU__uHQhskqWQnrqxW-C7lF_-BT9sEk3g3KfssRoCd0UQAvD_BwE

[34] *Europloty: Mobilní oplocení* [online]. [cit. 2020-06-19]. Dostupné z: https://www.europloty.cz/mobilni-oploceni

[35] *Kibosecurity.com: Mobilní oplocení vysoké bezpečnosti* [online]. [cit. 2020-06-20]. Dostupné z: https://kibosecurity.com/leasing/mobile-high-security-fencing

[36] *PLETIVADOBRÝ: Mobilní žiletková bariéra* [online]. [cit. 2020-06-20]. Dostupné z: https://www.levne-pletivo.cz/bezpecnostni-oploceni/mobilni-ziletkova-bariera/

[37] Bavolet na ostnatý drát. *Pavelka ploty pro váš dům* [online]. [cit. 2020-07-18]. Dostupné z: https://www.ploty-pavelka.cz/ostnaty-a-ziletkovy-drat-a-prislusenstvi/bavolet-na-ostnaty-drat-pro-sloupek-48-zn-jednostranny/

[38] BURDA, Karel a Ondřej LUTERA. Venkovní detektory poplachových systémů. *Elktrorevue* [online]. 2012, 2012(2), 1-5 [cit. 2020-06-26]. ISSN 1213-1539. Dostupné z: http://www.elektrorevue.cz/cz/download/venkovni-detektory-poplachovych-systemu/

[39] *Ronyo technologies: Varya Perimeter* [online]. [cit. 2020-06-26]. Dostupné z: https://www.ronyo.eu/cs/technologies/varya-perimeter/

[40] PRO E-100H. *Abbas.cz* [online]. [cit. 2020-07-19]. Dostupné z: https://katalog.abbas.cz/pro-e100h-s25188/

[41] MURENA 24 PLUS. *Abbas.cz* [online]. [cit. 2020-07-19]. Dostupné z: https://katalog.abbas.cz/murena-24-plus-s17683/

[42] Pythagoras3 160 6IR Doppler. *Abbas.cz* [online]. [cit. 2020-07-19]. Dostupné z: https://katalog.abbas.cz/pythagoras-3-160-6ir-doppler-s24620/

[43] *Abbas: Zemní detekční systém* [online]. [cit. 2020-06-27]. Dostupné z: https://katalog.abbas.cz/talpa-zemni-detekcni-system-s29432/

[44] OPTEX RLS 3060SH. *Abbas.cz* [online]. [cit. 2020-07-19]. Dostupné z: https://katalog.abbas.cz/optex-rls-3060sh-s31143/

[45] Princip činnosti, typy a komunikační rozhraní IP kamer. *Atp journal* [online]. [cit. 2020-07-01]. Dostupné z: https://www.atpjournal.sk/budovy/rubriky/prehladove-clanky/princip-cinnosti-typyakomunikacnirozhrani-ip-kamer.html?page_id=15814

[46] DAHUA SD5A432XA-HNR. *Abbas.cz* [online]. [cit. 2020-07-20]. Dostupné z: https://katalog.abbas.cz/sd5a432xahnr-s35294/

[47] IP PTZ DOME kamera DS-2DE3A404IW-DE. *Hikvision.cz* [online]. [cit. 2020-07-20]. Dostupné z: https://www.kamery-hikvision.cz/4mp/7827-ds-2de3a404iw-de28-12mm-ip-ptz-kamera-4mp-4x-opt-zoom-audio-ir-do-50m.html

[48] Stanové systémy řady SK (Koridorové). *Ultimate.cz* [online]. [cit. 2020-07-08]. Dostupné z: http://www.ultimate.cz/stany/koridorove/

[49] KONTEJNER ISO 1C SKLADOVÝ. *Karbox.cz* [online]. [cit. 2020-08-09]. Dostupné z: http://www.karbox.cz/kontejner-iso-1c-skladovy

[50] Mobilní operační středisko letky. *Mise.army.cz* [online]. [cit. 2020-07-06]. Dostupné z: http://www.mise.army.cz/aktualni-mise/afghanistan-sarana/zpravodajstvi/mobilni-operacni-stredisko-letky-38544/

[51] ČERMÁK, Miroslav. *Řízení informačních rizik v praxi*. V Tribunu EU vyd. 1. Brno: Tribun EU, 2009. Knihovnicka.cz. ISBN 978-80-7399-731-1.

[52] URBAN, Petr. *Velitelství výcviku - Vojenská akademie ve Vyškově: Manažer systémů řízení bezpečnostních informací [CD]*. Vyškov, 2018.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACCS	Air Command & Control systém
AČR	Armáda České republiky
BM	Bezpečnostní manažer
BŘ	Bezpečnostní ředitel
BSTO	Bezpečnostní správce terminálové oblasti
CCD	Charge-CoupledDevice
CCTV	Uzavřený televizní okruh, kamerový systém
CMOS	Complementary Metal Oxide Semiconductor
COM	Command (velení)
NOC	Control (řízení)
CPU	Central processing unit (centrální procesorová jednotka)
ČR	Česká republika
DPPC	Dohledové a poplachové přijímací centrum
DPS	Digital Pixel System
EKV	Elektrická kontrola vstupu
EPS	Elektrická požární signalizace
EZS	Elektrický zabezpečovací systém
FP	Ochrana vojsk (Force protection)
HD	Vysoké rozlišení
IP	Internetový protokol
IR	Infra red (infračervené záření)
JO	Jednací oblast
KEV	Kompromitující elektromagnetické vyzařování
KIS	Komunikační a informační systém
LAN	Lokální síť

LCD	Liquid Crystal Display (displej z tekutých krystalů)
MAC	Medium Access Control (řízení přístupu k médiu)
MO	Ministerstvo obrany
MV	Místo velení
MZS	Mechanické zábranné systémy
NATO	Severoatlantická aliance
NŠ	Náčelník štábu
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
NV MO	Normativní výnos Ministerstva obrany
OC	Organizační celek
OUI	Ochrana utajovaných informací
OZ	Občanský zaměstnanec
PC	Osobní počítač
PCO	Pult centralizované ochrany
PIR	Pasivní infračervený detektor
PTS	Poplachový tísňový systém
PTZ	Pan | Tilt | Zoom (posun, natočení a přiblížení)
PZS	Poplachový zabezpečovací systém
PZTS	Poplachový zabezpečovací a tísňový systém
RMO	Rozkaz ministra obrany
RFID	Radio-Frequency Identification (Radiofrekvenční identifikace)
STO	Správce terminálové oblasti
UI	Utajovaná informace
VOC	Velitel organizačního celku
ZO	Zabezpečená oblast

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH