Návrh realizace projektu fyzické bezpečnosti v zabezpečené a jednací oblasti objektu AČR

Bc. Radek Tobolík

Diplomová práce
2019

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2018/2019

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Radek Tobolík**
Osobní číslo:	**A17352**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Návrh realizace projektu fyzické bezpečnosti v zabezpečené a jednací oblasti objektu AČR**
Téma anglicky:	**A Proposal of a Physical Security Project in a Secure and Negotiation Area of the ACR**

Zásady pro vypracování:

1. **Specifikujte legislativní a bezpečnostní požadavky na zajištění fyzické bezpečnosti zabezpečené a jednací oblasti v objektu AČR. Zaměřte se jak na státní, tak resortní legislativu.**
2. **Objasněte specifika vytvoření projektu pro zajištění fyzické bezpečnosti zabezpečené a jednací oblasti objektu AČR.**
3. **Analyzujte bezpečnostní technologie pro zajištění fyzické bezpečnosti zabezpečené a jednací oblasti objektu AČR.**
4. **Vytvořte hypotetický model zabezpečené a jednací oblasti v objektu AČR. Navrhněte dvě varianty zajištění fyzické bezpečnosti, ty porovnejte a vyberte vhodnější.**
5. **Pro vybranou variantu fyzické bezpečnosti zabezpečené a jednací oblasti zpracujte projekt zajištění fyzické bezpečnosti pro zvolený stupeň utajení.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **Národní bezpečnostní úřad: Ochrana utajovaných informací[online]. Praha, 1998. Dostupné také z: https://www.nbu.cz/cs/ochrana-utajovanych-informaci/**
2. **KINDL, Jiří. Projektování bezpečnostních systémů I. 2. vyd. Zlín: Univerzita Tomáše Bati, 2007, 134 s. ISBN 978-80-7318-554-1.**
3. **LUĎĚK, Lukáš. Bezpečnostní technologie, systémy a management I. Zlín: VeRbuM, 2011, 316 s. ISBN 978-80-87500-05-7.**
4. **LUĎĚK, Lukáš. Bezpečnostní technologie, systémy a management IV. Zlín: VeRbuM, 2014, 390 s. ISBN 978-80-87500-57-6.**
5. **KŘEČEK, Stanislav. Příručka zabezpečovací techniky. Vyd. 3. aktualiz. S.l.: Cricetus, 2006, 313 s. ISBN 80-902938-2-4.**
6. **ČESKÁ REPUBLIKA. Rozkaz ministra obrany ČR č. 14/2013: Ochrana utajovaných informací v rezortu Ministerstva obrany. In: Ministerstvo obrany, 2013, číslo 14.**
7. **ČESKÁ REPUBLIKA. Normativní výnos Ministerstva obrany č. 77/2013: Fyzická bezpečnost v rezortu Ministerstva obrany. In: Ministerstvo obrany, 2013, číslo 77.**
8. **URBAN, Petr. Velitelství výcviku – Vojenská akademie ve Vyškově: Manažer systémů řízení bezpečnostních informací. Vyškov: Urban, 2018.**

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

Datum zadání diplomové práce: **30. listopadu 2018**

Termín odevzdání diplomové práce: **17. května 2019**

Ve Zlíně dne 14. prosince 2018

doc. Mgr. Milan Adámek, Ph.D.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

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/bakalářské 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 17. května 2019

Radek Tobolík, v. r.
podpis diplomanta

ABSTRAKT

Předmětem diplomové práce je systém opatření, řešící problematiku fyzické bezpečnosti v rezortu Ministerstva obrany. Teoretická část práce analyzuje platnou legislativu, kterou spravuje Národní bezpečnostní úřad. Tato legislativa je dále doplněna jednotlivými vnitřními předpisy Ministerstva obrany, které upřesňují podmínky ke schválení projektu fyzické bezpečnosti v objektu Armády České republiky (AČR). V praktické části diplomové práce jsou analyzovány bezpečnostní technologie, které jsou nezbytné k zajištění fyzické bezpečnosti v objektu AČR. Následně je vytvořen model hypoteticky zabezpečené oblasti (ZO) a jednací oblasti (JO) v objektu AČR. Na základě tohoto modelu je vypracován samotný „Projekt fyzické bezpečnosti“ ZO a JO v objektu AČR.

Klíčová slova: systém opatření, legislativa, projekt fyzické bezpečnosti, objekt AČR, zabezpečená oblast, jednací oblast.

ABSTRACT

The subject matter of my thesis is a system of measures solving the issue of physical security in the Defence Ministry resort. The theoretical part of the thesis describes the valid legislation which is in charge of National safety office. This legislation is also completed by particular regulations of Defence Ministry Resort which specify the conditions for approval of ´The Project of physical security in object of Czech Republic Army. In the practical part of my thesis the safety technologies are analysed which are necessary to guarantee physical security in Army of the Czech Republic (AČR). Afterwards the model of hypothetical secured area and negotiating area in object of AČR is created. On the basis of this model is the ´ Project of physical security in object of Czech Republic Army´ ZO and JO is created.

Keywords: system of measures, legislation, project of physical security, object of AČR, secured area, negotiating area.

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

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

„Každý, kdo se přestane učit, je starý, ať je mu dvacet nebo osmdesát. Každý, kdo se stále učí, zůstává mladý.“

Henry Ford

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

OBSAH

ÚVOD

V dnešní době se s fyzickou bezpečností můžeme setkat na každém kroku. Všichni více či méně musíme řešit otázky, jak vlastně zabezpečit ochranu osob, majetku, utajovaných informací. Tyto otázky a mnohé další, nám řeší jeden z druhů zajištění ochrany utajovaných informací, který se nazývá „fyzická bezpečnost“. V České republice je fyzická bezpečnost řešena zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. Fyzická bezpečnost je jedním z druhů bezpečnosti, který nám stanovuje systém opatření, jenž má neoprávněné osobě zabránit nebo ztížit přístup k utajovaným informacím, popřípadě přístup nebo pokus o něj zaznamenat. [1] Proto je snahou každého člověka, organizace zabezpečit (utajované) informace proti zlodějům nebo jiným nepovolaným osobám. Další zabezpečení se samozřejmě také provádí z důvodu náhlých požárů, povodní nebo výbuchů, ať už způsobeny lidskou činností nebo přírodními vlivy. Proto si musíme uvědomit, jak velké úsilí vynaložit k zabezpečení konkrétních prostorů nebo celých objektů. Na základě toho stanovujeme odpovídající prostory a prostředky fyzické ochrany, které by měly být voleny adekvátně nikoliv přehnaně nebo neuváženě. Pro odpovídající zajištění fyzické bezpečnosti se provádí analýza rizik. Analýza rizik stanovuje pořadí škodlivosti jednotlivých hrozeb. Mezi opatření fyzické bezpečnosti patří systém ochrany, který se dále řadí: ostraha, režimová opatření a technické prostředky.

Teoretická část diplomové práce je tvořena dvěma kapitolami. První kapitola specifikuje normativní a bezpečnostní požadavky na zajištění fyzické bezpečnosti, které nám stanovují legislativní předpisy pro státní a armádní sektor v ČR. Druhá kapitola se soustřeďuje na objasnění pravidel a stanovených postupů, nezbytných k vytvoření „Projektu fyzické bezpečnosti“ v zabezpečených a jednacích oblastech objektu AČR.

V praktické části jsou analyzovány a na příkladech uvedeny bezpečnostní technologie, sloužící k zajištění fyzické bezpečnosti, pro kategorie stupně utajení Důvěrné, Tajné a Přísně tajné, používané v zabezpečených a jednacích oblastech v objektech AČR. Dále na vytvořeném modelu v objektu AČR, můžeme vidět návrh dvou možných variant, které mají zajistit fyzickou bezpečnost těchto oblastí, za použití technických prostředků. Na základě multikriteriální analýzy, je vybrána vhodnější varianta, podle které je zpracován samostatný „Projekt fyzické bezpečnosti“.

I. TEORETICKÁ ČÁST

1 LEGISLATIVNÍ POŽADAVKY K ZAJIŠTĚNÍ FYZICKKÉ BEZPEČNOSTI V OBJEKTU AČR

V resortu Ministerstva obrany (MO) nebyla vždy pravidla bezpečnosti tak přísně nastavena jako se s nimi můžeme setkat v dnešní podobě. Do tohoto stavu procházela postupným vývojem. Po skončení druhé světové války byla ČSR/ČSSR pod vlivem SSSR a studené války, kde bylo skoro vše utajováno. Ministerstvo obrany nemělo jasně ucelené právní předpisy ohledně utajovaných informací. Převážně zásadní zlom nastal až po roce 1989, kde se konečně začaly zveřejňovat informace, které byly do té doby utajované. Mezi významný průlom patřil vstup České republiky do Severoatlantické aliance (NATO) dne 12. 3. 1999 a Evropské unie (EU) dne 1. 5. 2004. Na základě těchto partnerství se převážně vycházelo ze zákona č. 148/1998 Sb., o ochraně utajovaných skutečností, který nahradil zákon č. 102/1971 Sb., o ochraně státního tajemství. Tento zákon nám kopíroval podobnou legislativu, kterou v této době disponovaly státy NATO a EU. Na základě rozvoje státu, bylo nutné vytvořit ústřední správní úřad, který by dohlížel na plnění legislativních norem s pohledu bezpečnosti. Tento správní úřad byl nazván Národní bezpečnostní úřad (NBÚ). [2] V roce 2005 byl vydán nový zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, který na základě aktuálních doplňků (ve znění pozdějších předpisů) je stále platnou legislativní normou pro ČR.

Národní bezpečnostní úřad (NBÚ) je nejvyšší bezpečnostní autoritou v oblasti utajovaných informací (UI) v ČR. Byl zřízen zákonem č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů ke dni 1. srpna 1998. V dnešní době se NBÚ řídí zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. NBÚ je ústředním správním úřadem, který zajišťuje ochranu oblasti utajovaných informací a bezpečnostní způsobilosti. Vykonává tedy funkci správního úřadu, ale také ústředního úřadu. V čele NBÚ je ředitel, který může být zvolen nebo odvolán pouze výborem Poslanecké sněmovny. [3]

Pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů (IKS) včetně kryptografické ochrany vznikl 1. srpna 2017 v Brně Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). [4]

Hlavní úkoly NBÚ:

- rozhoduje o vydání nebo zrušení platnosti osvědčení fyzické osoby nebo osvědčení podnikatele,

- řeší ochranu utajovaných informací s vyplívajících závazků ochrany utajovaných informací v členství EU a NATO,
- je odpovědný za vedení ústředního registru a schvalování registrů v orgánech státu,
- v jeho působnosti je poskytování utajovaných informací v mezinárodním styku,
- provádí certifikaci technických prostředků, informačních systémů, kryptografických prostředků, kryptografických pracovišť a stínících komor,
- řeší otázky vývoje kryptografických prostředků,
- vydává prováděcí vyhlášky, které se týkají kryptografické ochrany, certifikace, průmyslové bezpečnosti, personální bezpečnosti, fyzické bezpečnosti, administrativní bezpečnosti, bezpečnosti informačních a komunikačních systémů,
- stanovuje seznam utajovaných informací atd. [5]

Z pohledu rezortu Ministerstva obrany, musí být jakákoliv komunikace s NBÚ schválena prostřednictvím **Odboru bezpečnosti Ministerstva obrany** (dále jen OB MO), který zastává roli schvalovacího mezičlánku s tímto úřadem.

OB MO je odpovědný za plnění úkolů, které stanovuje zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů a vnitřních předpisů řešících určené neutajované informace a kybernetickou bezpečnost v rezortu Ministerstva obrany. V čele odboru bezpečnosti Ministerstva obrany je bezpečnostní ředitel Ministerstva obrany-ředitel odboru bezpečnosti. [6]

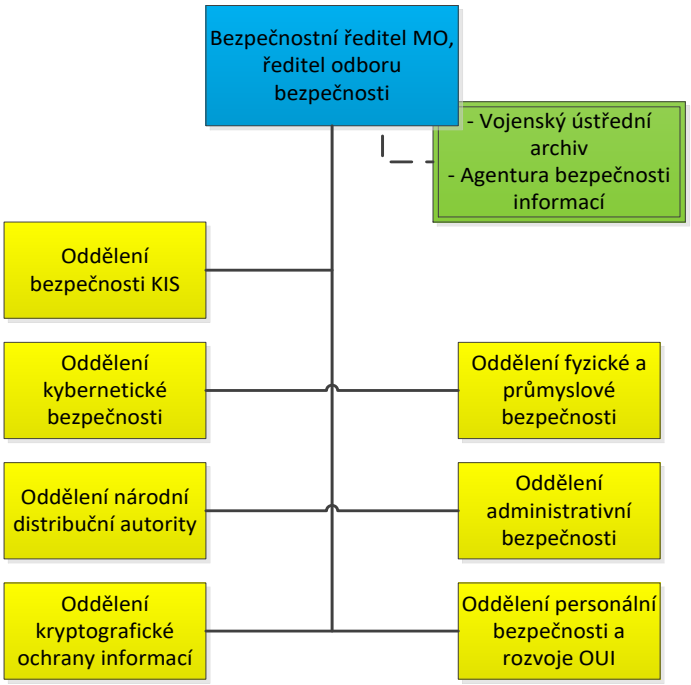
Odbor bezpečnosti se člení na jednotlivá oddělení:

- Oddělení bezpečnosti komunikačních a informačních systémů,
- Oddělení kybernetické bezpečnosti,
- Oddělení Národní distribuční autority,
- Oddělení kryptografické ochrany informací,
- Oddělení fyzické a průmyslové bezpečnosti,
- Oddělení administrativní bezpečnosti,
- Oddělení personální bezpečnosti a rozvoje ochrany utajovaných informací. [6]

OB MO řídí podřízené útvary-složky:

- Vojenský ústřední archiv,
- Agentura bezpečnosti informací (ABI).

Na obr. 1. můžeme vidět schéma rozdělení Odboru bezpečnosti v čele s bezpečnostním ředitelem Ministerstva obrany.



Obr. 1. Struktura Odboru bezpečnosti MO [6]

Bezpečnostní ředitel Ministerstva obrany, ředitel odboru bezpečnosti:

- je odpovědný za plnění povinností odpovědné osoby v souladu s § 67 zákona č. 412/2005. Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti,
- rozhoduje v rezortu MO o poskytnutí utajované informace stupně utajení Vyhrazené v mezinárodním styku,
- je odpovědný za koordinaci zavádění řízení bezpečnosti informací v rezortu MO v souladu s normou ISO/IEC 27001,
- je majetkovým hospodářem v rozsahu stanoveném RMO č. 48/2013 Věstníku Hospodaření a nakládání s majetkem v působnosti MO,
- zastává funkci předsedy Rady pro kybernetickou obranu MO,
- plní roli Commanding Officer podle SDIP (SECAN Doctrine and Information Publication) Nr. 293/1. [6]

Pro finální vytvoření „Projektu fyzické bezpečnosti“ v zabezpečené oblasti a jednací oblasti objektu AČR byla převážně použita níže popsaná platná legislativa, která se zaobírá problematikou fyzické bezpečnosti. V této kapitole jsou uvedeny jen nejdůležitější právní normy, které byly použity pro zpracování diplomové práce.

Mým úkolem nebylo přesně citovat legislativu, jak ji můžeme najít v zákoně a dalších interních normativních aktech. Hlavní podstata tkvěla, poskytnout stručné a jasné vysvětlení legislativy, řešící fyzickou bezpečnost jako celek s upřesňujícími právními vnitřními předpisy vydané Ministerstvem obrany, které jsou nezbytné k vytvoření Projektu fyzické bezpečnosti.

Právní normy a předpisy platné pro rezort Ministerstva obrany, fyzická bezpečnost:

- zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, 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.

Obr. 2. Bezpečnostní legislativa [2]

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

Parlament se usnesl na tomto zákoně České republiky dne 21. září 2005 s účinností od 1. ledna 2006. Zákon č. 412/2005 Sb., 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. [1]

V platném znění je zákon rozdělen do devíti částí, které obsahují celkem 161 paragrafů.

- ČÁST PRVNÍ Základní ustanovení (§ 1 až § 2),
- ČÁST DRUHÁ Ochrana utajovaných informací (§ 3 až § 79),
- ČÁST TŘETÍ Bezpečnostní způsobilost (§ 80 až § 88),
- ČÁST ČTVRTÁ Bezpečnostní řízení (§ 89 až § 135),
- ČÁST PÁTÁ Výkon státní správy (§ 136 až § 142),
- ČÁST ŠESTÁ Státní dozor (§ 143 až § 144),
- ČÁST SEDMÁ Kontrola činnosti úřadu (§145 až § 147),
- ČÁST OSMÁ Přestupky (§ 148 až § 156),
- ČÁST DEVÁTÁ Přechodná a závěrečná ustanovení (§ 157 až § 161). [7]

K zákonu č. 412/2005 Sb., patří provádějící 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 vyhlášky č. 453/2011 Sb.,
- 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). [8]

V oblasti ochrany utajovaných informací (OUI), je nezbytné ještě zmínit zákon č. 413/2005 Sb., o změně zákonů v souvislosti s přijetím zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů, který obsahuje změnu zákonů v souvislosti s přijetím zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti. Mezi nejdůležitější změny zákonů, patří například trestní řád, přístup k utajovaným informacím, změna občanského soudního řádu, změna zákona o požární ochraně, změna zákona o vynálezech a zlepšovacích návrzích atd. [9]

1.1.1 Předmět úpravy, vymezení pojmů a úvodní ustanovení

Zákon č. 412/2005 Sb., spolu s prováděcími právními předpisy, upravuje zásady pro stanovení informací jako informací utajovaných, podmínky pro přístup k nim a další požadavky na jejich ochranu. Stanovuje zásady citlivých činností a podmínky pro jejich výkon a s tím spojený výkon státní správy. Tento zákon definuje utajovanou informaci jako informaci v jakékoliv podobě zaznamenanou na jakémkoliv nosiči označené v souladu s tímto zákonem, jejíž vyzrazení nebo zneužití může způsobit újmu zájmu České republiky nebo může být pro tento zájem nevýhodné. Utajovanou informací může informace být pouze v případě, že je uvedená v seznamu utajovaných informací. [7] Tento seznam je uveden v nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací, ve znění pozdějších předpisů. Seznam obsahuje 20 příloh členěných dle ústředních orgánů státní správy. Každá příloha definuje rozsah stupňů utajení pro jednotlivé UI v dané oblasti své odpovídající působnosti. [10]

Rozdělení stupňů utajované informace spadá do čtyř kategorií:

1. **VYHRAZENÉ** (její vyzrazení neoprávněné osobě nebo zneužití může být nevýhodné pro zájmy ČR),
2. **DŮVĚRNÉ** (její vyzrazení nebo zneužití může způsobit prostou újmu zájmům ČR),

3. **TAJNÉ** (její vyzrazení neoprávněné osobě nebo zneužití může způsobit vážnou újmu zájmům ČR),
4. **PŘÍSNĚ TAJNÉ** (její vyzrazení neoprávněné osobě nebo zneužití může způsobit mimořádně vážnou újmu zájmům ČR). [1]

Při vniku stupně utajení určuje stupeň utajení původce této informace. Bez vědomí zhotovitele nesmí být stupeň utajení ponižován ani jinak měněn. V hlavě I úvodního ustanovení zákona č. 412/2005 Sb., jsou dále přesně definovány pojmy: újma zájmu ČR, vážná újma zájmu ČR, prostá újma zájmu ČR a nevýhodnost pro zájmy ČR. [1]

Druhy bezpečnosti, se kterými se můžeme setkat a které zajišťují ochranu utajovaných informací:

- Personální bezpečnost,
- Průmyslová bezpečnost,
- Administrativní bezpečnost,
- **Fyzická bezpečnost,**
- Bezpečnost informačních a komunikačních systémů,
- Kryptografická ochrana. [1]

1.1.2 Fyzická bezpečnost

Fyzická bezpečnost je druhem zajištění ochrany utajovaných informací a je upravena v **hlavě V** zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. Jak už bylo v úvodu řečeno, fyzickou bezpečnost tvoří systém opatření, která mají neoprávněné osobě zabránit nebo ztížit přístup k utajovaným informacím, popřípadě přístup nebo pokus o něj zaznamenat. Fyzická bezpečnost se zabývá ochranou utajovaných informací, která se nachází v objektech, kde jsou zřízeny zabezpečené oblasti (dále jen ZO) a jednací oblasti (dále jen JO). [7]

Objektem může být budova nebo jiný ohraničený prostor, ve kterém se nachází ZO nebo JO. V těchto objektech potom můžeme zpracovávat nebo manipulovat s utajovanou informací podle daného stupně utajení. Zabezpečenou oblastí a jednací oblastí je ohraničený prostor v objektu. [1]

Do zabezpečených oblastí můžeme ukládat utajované informace v analogové tištěné podobě nebo digitální podobě uložené na fyzickém nosiči. Stupeň utajení zabezpečené oblasti musí odpovídat nejvyššímu stupni utajované informace, kterou v zabezpečené oblasti

ukládáme nebo v ní zpracováváme. Zabezpečené oblasti se podle nejvyššího stupně utajení UI, která se v nich ukládá, a objekty se podle nejvyššího stupně utajení UI, která se v nich zpracovává, zařazují do kategorií Vyhrazené, Důvěrné, Tajné a Přísně tajné. [1]

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. [1]

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. [1]

Jednací oblast slouží pouze k pravidelnému projednávání utajované informace stupně utajení Tajné a Přísně tajné. [1] Aby v JO nedocházelo k nežádoucímu úniku nebo ohrožení projednávaných utajovaných informací, musí tuto skutečnost zajistit odpovědná osoba. Odpovědná osoba má dále za povinnost požádat prostřednictvím Národního bezpečnostního úřadu o provedení kontroly, zda v JO nedochází k nedovolenému použití technických prostředků určených k získávání informací. V případě nutnosti je možné požádat Úřad o provedení kontroly technických prostředků i v ZO kategorie Tajné a Přísně tajné. Neoprávněná osoba může do JO vstoupit pouze s osobou, která má do této JO vstup povolen. [7]

Opatření pro zajištění fyzické bezpečnosti jsou:

1. **ostraha,**
2. **režimová opatření,**
3. **technické prostředky**. [1]

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. [1]

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 na základě poplachového hlášení technických prostředků, umožní rychlý zásah, je-li zajištění ochrany UI narušeno;
- **Tajné –** nejméně jednou osobou u objektu a jednou další osobou, které poplachové hlášení technických prostředků umožní rychlý zásah, pokud je ochrana UI narušena;
- **Přísně tajné –** nejméně dvě osoby u objektu. [1]

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

- **Tajné –** nejméně jednou osobou u objektu a jednou další osobou, které poplachové hlášení technických prostředků umožní rychlý zásah, je-li provádění ochrany utajovaných informací narušeno;
- **Přísně tajné –** nejméně dvě osoby u objektu. [1]

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 systémy zabezpečení vstupů,
- 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. [1]

Technické prostředky dělíme na:

- mechanické zábranné prostředky,
- elektrická zámková zařízení a systémy pro kontrolu vstupů,
- 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. [1]

Pro každý certifikovaný nebo necertifikovaný technický prostředek je stanoveno bodové ohodnocení, které slouží pro vyplnění bodových hodnot v analýze rizik. Vyhodnocení rizik nám stanovuje míru zabezpečení těchto opatření pro konkrétní ZO a JO. [1]

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. Orgány státu, PO a FO mají za povinnost provádět náležitá opatření, která splňují právní rámec pro zajištění fyzické bezpečnosti v oblasti ochrany utajovaných informací. [7]

V případech, kdy se v objektu nachází zabezpečená oblast kategorie Vyhrazené, Důvěrné, Tajné nebo Přísně tajné nebo jednací oblast, nám zákon ukládá povinnost zpracovat Projekt fyzické bezpečnosti. [1] Tento projekt je detailně specifikován a popsán v druhé kapitole diplomové práce.

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

Tato vyhláška byla vydána NBÚ a 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. Její účinnost nabyla platnost stejně jako Zákon 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti a to dnem 1. ledna 2006. Můžeme zde najít aktualizaci některých pojmů, např. elektrická zabezpečovací signalizace (EZS), která byla nahrazena pojmem poplachový zabezpečovací a tísňový systém, dle normy ČSN EN 50131-1. Je však důležité používat stále platné názvy podle zákona 412/2005 Sb., a jeho prováděcích právních předpisů. Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků stanovuje jednotlivé bodové ohodnocení fyzické bezpečnosti, kde je kladen důraz na nejnižší míru zabezpečení ZO a JO. Mezi hlavní prioritu v této vyhlášce patří tedy vyhodnocení rizik a udělování certifikace technických prostředkům. [11]

Součástí vyhlášky jsou dvě přílohy, kde **Příloha č. 1** charakterizuje bodové ohodnocení ZO a JO a stanoví jejich nejnižší míru bezpečnosti. Příloha obsahuje také strukturu projek-

tu fyzické bezpečnosti, bodové ohodnocení ostrahy objektu a v neposlední řadě určuje použití technických prostředků po skončení platnosti jejich certifikátu. V **Příloze č. 2** můžeme vidět vzor certifikátu technického prostředku.

Při tvorbě projektu fyzické bezpečnosti vycházíme ze stanovených pojmů, které vyhláška jasně definuje.

1.2.1 Vymezení pojmů

- objekt – budova nebo jinak ohraničený prostor, kde se nacházejí ZO a JO,
- hranice objektu – plášť budovy, fyzické ohraničení nebo jinak vyznačená hranice,
- hranice ZO a JO – viditelně nebo stavebně upravený ohraničený prostor,
- určené místo, pro vstup/výstup osob a vjezd/výjezd dopravních prostředků,
- prostředky určené k přepravě osob, předmětů a materiálu,
- hrozba – možnost zneužití nebo vyzrazení UI,
- riziko – pravděpodobnost, že se určitá hrozba uskuteční,
- mimořádná situace – situace vyzrazení nebo zneužití UI,
- technický prostředek – stanovení bezpečnostního prvku sloužící k zaznamenání, zabránění nebo znesnadnění narušení ochrany objektu v ZO a JO,
- úschovný objekt – dle přílohy č. 1 definována úschovná schránka nebo trezor,
- vojenský materiál, vojenská technika, která může obsahovat utajovanou informaci. [11]

Každý objekt a ZO musí být náležitě zabezpečeny dle dané kategorie, do které spadají. Pro použití zabezpečení je možnost použít kombinaci opatření fyzické bezpečnosti. Pro stupeň Vyhrazené nám postačí mechanické zábranné prostředky. U stupně Důvěrné a Tajné musíme zvolit kombinaci mechanických zábranných prostředků a zařízení elektrické zabezpečovací signalizace. Pro kategorii Přísně tajné využíváme mechanické zábranné prostředky, zařízení elektrické zabezpečovací signalizace a speciální televizní systémy. Tyto systémy nám však nesmí narušit ochranu UI. Utajovaná informace se může ukládat pouze do ZO, protože JO nám slouží pouze k projednávání. UI musíme uložit v ZO jen do příslušné kategorie popřípadě vyšší, je-li tato bodová hodnota stanovena v projektu fyzické bezpečnosti. V této ZO se také zřizuje zařízení k ničení UI pro danou kategorii. [11]

Režim manipulace s klíči a identifikačními prostředky je podle této vyhlášky striktně nastaven, kde je splněna posloupnost jednotlivých kroků, které se musí dodržovat. Jedná se

především o způsob označení, přidělení a odevzdání klíčů do úschovny, možnost použití duplikátů a jejich evidence. Dále odpovědnost za klíče a identifikační prostředky k ZO a JO v jeho úschovném objektu, kde se ukládá UI stupně utajení Důvěrné a vyšší. V objektu, kde se ukládá UI kategorie Vyhrazené, je za manipulaci s klíči odpovědná určená osoba. Každá ZO a JO v době nepřítomnosti osob musí být uzamčena. Stejné podmínky platí i pro úschovný objekt. Osoby, které mají povoleno disponovat s klíči a identifikačními prostředky od JO, ZO a utajovaných objektů musí tyto klíče a identifikační prostředky ukládat v objektu, pokud není stanoveno odpovědnou osobou jinak. [11]

Ověření, zda použitá opatření splňují požadavky na fyzickou bezpečnost a vyhodnocení rizik stále splňuje stanovy projektu fyzické bezpečnosti, vyhodnocuje zpravidla pověřená osoba ne však později než 1x za 12 měsíců. K ověření technických prostředků se vychází z přílohy č. 1, která nám udává postupy funkčních zkoušek. Na základě vyhodnocení hrozeb se vyhodnocuje velikost rizika, která může být klasifikována jako malé, střední nebo velké. V posledním odstavci vyhláška hovoří o potřebných náležitostech k žádosti o certifikaci technických prostředků, kde je stanovena platnost certifikátu technického prostředku. [11]

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

Rozkaz ministra obrany (dále jen RMO) č. 14/2013 Věstníku Ochrana utajovaných informací v rezortu Ministerstva obrany, 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 (dále jen OZ) s výjimkou organizačních útvarů Vojenského zpravodajství. [12]

Tento rozkaz nabyl účinnosti 25. února 2013, zapsaného ve Věstníku Ministerstva obrany. Poslední změny byly vydány dne 9. ledna 2019 v rozkaze ministra obrany č. 3/2019, kterým se mění rozkaz ministra obrany č. 14/2013 Věstníku Ochrana utajovaných informací v rezortu Ministerstva obrany. RMO č. 3/2019 je veden pod číslem jednacím MO 244212/2018-OB MO. [12]

Tento rozkaz je zároveň služebním předpisem státního tajemníka Ministerstva obrany podle § 11 zákona č. 234/2014 Sb., o státní službě, ve znění pozdějších předpisů. [12]

1.3.1 Struktura RMO č. 14/2013 Věstníku ochrana UI v rezortu MO

Rozkaz ministra obrany č. 14/2013 Věstníku Ochrana utajovaných informací v rezortu Ministerstva obrany se skládá ze třech částí, hlava I až hlava XIII, které obsahují celkem 103 článků. Tento rozkaz upřesňuje legislativní normy pro potřeby Ministerstva obrany v její působnosti. [12]

1.3.1.1 Základní ustanovení

První část RMO č. 14/2013, upřesňuje účely tohoto rozkazu, obsahující základní pojmy:

- utajovaná informace,
- porušení povinností při ochraně utajovaných informací,
- technické zařízení (vojenský materiál),
- nosiče utajovaných informací,
- informační a komunikační systémy v rezortu Ministerstva obrany,
- akreditace – rozhodnutí o tom, že informační a komunikační systémy splňují podmínky s předpisy MO a certifikovanou bezpečnostní dokumentaci informačních nebo komunikačních systémů,
- bezpečnostní ředitel – který je výkonným orgánem ministra obrany v oblasti OUI,
- gestor systému – odpovědný za provoz informačních a komunikačních systémů,
- plnění úkolů AČR v polních podmínkách. [12]

1.3.1.2 Organizace ochrany utajovaných informací

V druhé části RMO je specifikována odpovědnost a povinnost při ochraně UI u zainteresovaných osob:

- **Bezpečnostní ředitel (BŘ)** odpovídá za realizaci systémových opatření personální, administrativní, průmyslové a fyzické bezpečnosti, bezpečnosti informačního a komunikačního systému a elektronických zařízení a kryptografické ochrany v rezortu Ministerstva obrany. V oblasti fyzické bezpečnosti je odpovědný za schvalování a následné vedení evidence projektů fyzické bezpečnosti, spadajících do rezortu MO. Bezpečnostní ředitel vede také přehled osob o vydání osvědčení fyzické osoby a osvědčení fyzické osoby pro cizí moc. BŘ je odpovědný za zřízení a provoz Centrálního registru MO, pomocného registru u organizačních celků, kde jsou evidovány dokumenty cizí moci. [12]

- **Vedoucí organizačního celku (VOC)** je odpovědný za bezpečnost v JO a ZO, dále zajišťuje, aby nedocházelo k neoprávněnému použití UI v komunikačních a informačních systémech, které nejsou schválené gestorem. Pokud je VOC schvalovatelem UI, může písemně povolit vytvoření kopií či opisů. Dále je VOC povinen stanovit bezpečnostní správu organizačního celku, obsadit role provozní a bezpečnostní správy u komunikačních a informačních systémů a zabezpečit zpracování, vedení a uložení projektů fyzické bezpečnosti. [12]

1.3.1.3 Bezpečnostní správa organizačního celku

Pro správný výkon ochrany utajovaných informací musí vedoucí organizačního celku stanovit bezpečnostní správu.

Bezpečnostní správu organizačního celku tvoří:

- bezpečnostní manažer,
- provozní a bezpečnostní správa informačních a komunikačních systémů,
- bezpečnostní správa kryptografické ochrany,
- pracoviště ochrany informací (POI), registr a pomocný registr,
- bezpečnostní zaměstnanec pro personální bezpečnost,
- správce technických prostředků. [12]

1.3.1.4 Fyzická bezpečnost

Za fyzickou bezpečnost u organizačního celku je odpovědný velitel organizačního celku (dále jen VOC). Velitel organizačního celku ve své působnosti je zejména odpovědný za:

- 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 (stanovuje pravidla manipulace s klíči a ukládání klíčů a identifikačních prostředků),
- průběžné kontroly fyzické bezpečnosti, a schvaluje shody úschovných objektů (stanovuje podmínky funkčních zkoušek u technických prostředků, kromě EZS),
- schvalování projektu fyzické bezpečnosti, kde stanovuje určitá pravidla ostrahy,
- zaslání podkladů odboru bezpečnosti MO, kde je definováno místo označení a uložení projektu fyzické bezpečnosti, odpovědní zaměstnanci za aktualizaci těchto projektů (tuto činnost zpravidla zastává bezpečnostní manažer),

- vyžadování prostřednictvím bezpečnostního ředitele kontroly na ZO a JO, například zda nejsou použity neschválené technické prostředky,
- způsob použití těchto technických prostředků a stanovení režimových opatření k zabezpečení UI v návaznosti na vyhodnocení rizik. [12]

Dále tento RMO definuje použití a zabezpečení informačních a komunikačních systémů a elektronických zařízení. Specifikuje náležitosti k použití kryptografických prostředků a její ochrany. V případě dislokačních změn, stěhování nebo zániku objektu nám RMO upřesňuje dané pravidla pro VOC jak zacházet s UI v objektu dokut není rozhodnuto jinak. Velitel musí stále dodržovat ochranu objektu po dobu nezbytně nutnou, dokud není objekt zrušen nebo schválen předávací protokol o předání objektu. Součástí tohoto předávacího protokolu musí být vyhotoveny seznamy se všemi rušenými přesouvanými položkami (nosiče UI, spisy, sběrače, kryptografický materiál atd.). [12]

Ochrana UI v polních podmínkách

Ochrana UI v polních podmínkách nachází využití zpravidla při nasazení v zahraničí, různých cvičení nebo výcviku. Velitel musí náležitě poučit své podřízené, jakým způsobem mohou zpracovávat utajované informace mimo objekt. Zpracované UI musí být vždy chráněny odpovědnou osobou (ostraha), kde je stanoven ochranný perimetr a prostor pro ukládání nosičů UI. Projekt fyzické bezpečnosti při cvičení, výcviku atd., který netrvá déle, jak 60 dnů se nezpracovává, pokud není stanoveno VOC jinak. Při zahraniční operaci (mise) musí být vytvořen projekt fyzické bezpečnosti vždy, pokud se nejedná pouze o krátkodobou rekognoskaci terénu. Seznam kryptografických prostředků se zhotovuje a zapisuje do oddělených dokumentů. [12]

Ochrana utajovaných informací v rámci mezinárodních styků

Ochrana utajovaných informací v rámci mezinárodních styků nám deklaruje podmínky vstupu do objektu Ministerstva obrany, ve kterých se ukládají nebo zpracovávají UI. Předmětem zájmu pro tuto ochranu je možnost povolení přístupu do těchto oblastí pro cizince (občany bez české státní příslušnosti). Povolení vstupu a možnost seznámit se s UI pro cizince vydává a schvaluje pouze: ministr obrany, náměstkové ministra obrany, náčelník Generálního štábu Armády České republiky (NGŠ), ředitel vojenského zpravodajství, vedoucí organizačních útvarů MO a velitelé vojenských škol. V případě že nedojde k seznámení s UI, povolení ke vstupu schvaluje VOC. Pokud je v objektu více organizačních celků povolení ke schválení vydává velitel rozsáhlého objektu. [12]

Kontrola ochrany utajovaných informací

K ochraně UI jsou MO realizovány kontroly, které se zakládají na písemném pověření k hloubkové kontrole u organizačního celku. Všechny kontrolní orgány i pověření zaměstnanci musí splňovat podmínky, které je opravňují ke kontrole, jako jsou platné osvědčení fyzické osoby, oznámení o splnění podmínek pro přístup k UI a poučení. V písemném pověření ke kontrole musí být jasně stanoveno, do jakého stupně utajení může daná osoba kontrolu vykonávat. [12]

V případě porušení ochrany utajovaných informací se musí tyto bezpečnostní incidenty (podle závažnosti incidentu) hlásit bezpečnostnímu řediteli MO a NBÚ. [12]

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

Normativní výnos Ministerstva obrany (dále jen 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. [13]

NVMO č. 77/2013 Věstníku, Fyzická bezpečnost v rezortu Ministerstva obrany nabyl účinností 9. července 2013. [13]

Předmětem úpravy NVMO č. 77/2013 Věstníku, Fyzická bezpečnost v rezortu Ministerstva obrany je stanovený systém opatření, který má v rezortu MO zabránit přístupu neoprávněných osob k utajovaným informacím, nebo tento přístup ztížit, popř. taková jednání zaznamenat. Tento výnos je zpravidla určen pro VOC a bezpečnostní manažery organizačních celků, kteří podle tohoto výnosu stanovují definovaná kritéria ve své působnosti. Do této kapitoly jsem začlenil první část výnosu, který upřesňuje důležité pojmy a stanovuje odpovědnost velitele rozsáhlého objektu, bezpečnostního manažera objektu a správce technických prostředků. Dále jsem specifikoval návrh a aktualizaci projektu fyzické bezpečnosti rozsáhlého objektu. Druhou část výnosu včetně příloh, která určuje organizaci fyzic-

ké bezpečnosti, a skladbu projektu fyzické bezpečnosti pro velitele organizačního celku jsem použil v kapitole: „Postup k vytvoření projektu fyzické bezpečnosti v objektu AČR“. [13]

1.4.1 Vymezení pojmů

Vymezení pojmů:

- objekt – stanovený prostor, který slouží převážně ke zpracování nebo projednávání utajovaných informací, může být tvořen částí areálu, budovou nebo jeho částí, skupinou místností nebo jen jedna místnost, v polních podmínkách musí být přesně definována hranice pro vytvoření zabezpečené oblasti,
- rozsáhlý objekt – je to objekt (areál vojenských kasáren), kde můžou být zabezpečené oblasti nebo jednací oblasti více organizačních celků,
- velitel rozsáhlého objektu – stanovený vedoucí, který je odpovědný za koordinaci a řízení společných opatření fyzické bezpečnosti v rozsáhlém objektu,
- vedoucí organizačního celku – osoba pověřená plněním povinností ve vztahu k fyzické bezpečnosti,
- identifikační prostředek – informace které jsou uloženy v systémech, které identifikují uživatele podle identifikačního čísla, kódu, hesla atd.,
- technický prostředek – zpravidla bezpečnostní prvek, který má zabránit, ztížit nebo zaznamenat narušení ZO, JO a slouží k ničení UI,
- úschovný objekt – trezor nebo jiná uzamykatelná schránka, dle přílohy č. 1.,
- klíč – mechanický klíč a číselná kombinace mechanických a elektronických zámků,
- návrh bezpečnostního projektu – kompletní analýza, která definuje současný stav fyzické bezpečnosti k ochraně UI, kde jeho obsahem je návrh instalace technických prostředků. [13]

1.4.2 Odpovědnost velitele rozsáhlého objektu

Velitel rozsáhlého objektu se stanovuje na základě rozkazu velitele posádky a stanovuje se především tam, kde je více organizačních celků v jednom objektu. V tomto rozkaze musí být dále definovány role bezpečnostního manažera rozsáhlého objektu, správce technických prostředků rozsáhlého objektu a jednotliví bezpečnostní manažeři organizačních celků. Tito bezpečnostní manažeři musí znát přesnou hranici rozsáhlého objektu a hranice svých objektů svého organizačního celku, za který jsou odpovědni. Za fyzickou bezpečnost

organizačních celků, které se nacházejí v prostorech v rámci rozsáhlého objektu, odpovídají jednotliví velitelé těchto celků, které jsou v areálu (objektu) dislokovány. [13]

Velitel rozsáhlého objektu v součinnosti s bezpečnostním manažerem rozsáhlého objektu zpracovává a aktualizuje projekt fyzické bezpečnosti rozsáhlého objektu. Projekt fyzické bezpečnosti rozsáhlého objektu obsahuje společná opatření fyzické bezpečnosti, které nám stanovují rozsáhlý objekt jako celek, jeho kategorie, hranice objektu, způsob zabezpečení technickými prostředky, ostrahu objektu a další důležitá společná opatření. [13]

Velitel organizačního celku, kterému byl přidělen objekt spadající do rozsáhlého objektu, má za povinnost dodávat podklady pro projekt fyzické bezpečnosti rozsáhlého objektu. Pokud má VOC svěřeného objektu v úmyslu provádět jakékoliv změny ve svém objektu, musí projednat tyto změny s ostatními veliteli organizačních celků. Po schválení změn může dodat podklady veliteli rozsáhlého objektu, který tyto změny aktualizuje do stávajícího projektu fyzické bezpečnosti rozsáhlého objektu. Projekt fyzické bezpečnosti rozsáhlého objektu se ukládá u velitele rozsáhlého objektu popřípadě u bezpečnostního manažera rozsáhlého objektu. [13]

1.4.3 Odpovědnost bezpečnostního manažera organizačního celku

Bezpečnostní manažer (dále jen BM) organizačního celku je přímo podřízen VOC. VOC ustanovuje BM do této role ve svém rozkaze. BM je hlavní klíčová postava každého velitele, protože je zodpovědný za splnění spousty důležitých povinností. Mezi jeho hlavní náplň patří vyhodnocování rizik, kde na základě těchto rizik stanovuje opatření fyzické bezpečnosti. BM se vyjadřuje ke všem předpokládaným realizačním projektům fyzické bezpečnosti, které konzultuje s příslušnými odpovědnými orgány. Podílí se, avšak ve většině případů přímo zabezpečuje zpracování návrhu bezpečnostního projektu pro daný organizační celek. Vyhotovený projekt fyzické bezpečnosti předkládá ke schválení VOC popřípadě veliteli rozsáhlého objektu. Dále je odpovědný za zřízení knihy návštěv do zabezpečených a jednacích oblastí, zajišťuje jejich evidenci a vytváří seznamy osob oprávněných ke vstupu do objektu. BM zpracovává zápisy o funkčních zkouškách, technických prostředcích a vede evidenci klíčů předaných do užívání a jejich duplikátů. Ve své působnosti kontroluje výkon na reakce ostrahy a činnost správce technických prostředků. V neposlední řadě plní další úkoly, které mu stanoví VOC ve své působnosti. [13]

1.4.4 Správce technických prostředků

Správce technických prostředků je také přímo podřízen VOC. VOC ho určuje ve svém rozkaze, ale navíc je odborně podřízen BM organizačního celku. Správce technických prostředků je odpovědný za osoby, nebo je dokonce může odborně řídit v případě, že používají instalované technické prostředky u organizačního celku. Správce technických prostředků se podílí na veškerém provozu technických prostředků, kde vede dokumentaci k těmto prostředkům. Má za úkol vykonávat kontrolu technických prostředků a v případě poruchy zajišťuje jejich servisní opravu. Vede si kompletní evidenci uživatelů, kde na základě povolení programuje identifikační karty pro přístup do systému. [13]

1.5 Dílčí závěr

Jednotlivé druhy ochrany utajovaných informací (OUI) nám stanovují povinnost UI chránit před zneužitím, vyzrazením, poškozením, nedovoleným šířením, ztrátou nebo odcizením. V rezortu ministerstva obrany mezi druhy OUI podílející se na ochraně utajovaných informací patří: administrativní bezpečnost, personální bezpečnost, průmyslová bezpečnost, kryptografická ochrana, bezpečnost informačních a komunikačních systémů, a jedna z nejdůležitějších, fyzická bezpečnost.

Specifikace fyzické bezpečnosti v České republice je ustanovena v zákoně č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti. Další legislativní předpis, který nám zajištuje OUI, patří do skupiny prováděcích vyhlášek, kterou je vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů. Pro zajištění ochrany fyzické bezpečnosti v objektech AČR jsou stanoveny doplňující vnitřní předpisy, vydané Ministerstvem obrany, mezi které patří 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. Oba tyto vnitřní předpisy Ministerstva obrany doplňují jednotlivé body fyzické bezpečnosti k zákonu 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti, které jsou nezbytně nutné pro vytvoření Projektu fyzické bezpečnosti v objektu Armády české republiky.

2 SPECIFIKA VYTVOŘENÍ PROJEKTU FYZICKÉ BEZPEČNOSTI ZABEZPEČENÉ A JEDNACÍ OBLASTI V OBJEKTU AČR

V předchozí kapitole byly definovány základní pravomoci velitele a velitele rozsáhlého objektu, který je hlavním organizátorem při vytváření projektu fyzické bezpečnosti u organizačního celku nebo rozsáhlého objektu. V této kapitole jsou charakterizována specifika vytvoření projektu fyzické bezpečnosti v objektu Armády České republiky. Hlavní podstata při vytvoření projektu fyzické bezpečnosti u organizačního celku MO, spočívá ve schváleném návrhu projektu fyzické bezpečnosti, ze kterého projekt fyzické bezpečnosti vychází. Postup k vytvoření návrhu projektu fyzické bezpečnosti stanovuje NVMO č. 77/2013 Věstníku, Fyzická bezpečnost v rezortu MO. Tento normativní výnos doplňuje zákon č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti, dále vyhláška č. 528/2003Sb., o fyzické bezpečnosti a certifikaci technických prostředků a RMO č. 14/2013 Věstníku Ochrana utajovaných informací v rezortu MO. **Návrh projektu fyzické bezpečnosti** zpracovává komise, která je stanovena na základě nařízení VOC. Komise obstarává potřebné podklady a opatření pro tento návrh projektu fyzické bezpečnosti. Na základě schváleného návrhu projektu fyzické bezpečnosti odborem bezpečnosti MO, se zpracuje finální **„Projekt fyzické bezpečnosti“**, který schvaluje velitel organizačního celku.

2.1 Organizace fyzické bezpečnosti

Velitel organizačního celku nebo rozsáhlého objektu je tedy v plné míře odpovědný za fyzickou bezpečnost svěřeného objektu ve své působnosti. Velitel při stanovení počtu zabezpečených oblastí, jednacích oblastí a objektů, vychází ze stavebních dispozic budovy, která je mu svěřená k užívání. Tyto oblasti je nutné budovat především v prostorech, kde je předpoklad využití současného stavu místností, které aspoň částečně splňují bezpečnostní požadavky. Jedná se především o tloušťku stěn, typ výplně zdiva, orientace a poloha místností. Dalším důležitým kritériem je vhodně zvolit objekt, který bude splňovat požadavky na minimalizaci nákladů zabezpečení hranice objektu. Hranice objektu jsou zpravidla areál nebo budova (oplocení areálu, plášť budovy), kde se nacházejí zabezpečené oblasti kategorie: Vyhrazené, Důvěrné, Tajné a Přísně tajné a u jednací oblasti stupně utajení Tajné a Přísně tajné. [13]

2.1.1 Návrh bezpečnostního projektu fyzické bezpečnosti

V případě nutnosti dalších opatření v oblasti fyzické bezpečnosti, vyžaduje-li to výstavba technických prostředků a investičních prostředků, které velitel nemůže vyřešit ve své působnosti, ustanovuje komisi. Komise zpracovává z poskytnutých podkladů návrh bezpečnostního projektu. Návrh bezpečnostního projektu se vypracovává pouze v případě zvolené kategorie Důvěrné a vyšší. Komise má zpravidla několik členů, kde v čele je ustanoven předseda komise. [13]

Členové komise pro vytvoření návrhu projektu fyzické bezpečnosti:

1. BM daného celku nebo BM rozsáhlého objektu,
2. pověřený pracovník nadřízeného stupně řízení z bezpečnosti informací,
3. zástupce ubytovací vojenské a stavební správy,
4. osoba odpovědná za provoz ZO a JO. [13]

Návrh bezpečnostního projektu se dělí na dvě etapy:

a) V první etapě se návrh bezpečnostního projektu musí vypracovat ve dvou výtiscích. Výtisk č. 1 se zasílá odboru bezpečnosti Ministerstva obrany, který jej posoudí a vyhodnotí splnění požadavků na základě zákona č. 412/2005 Sb., a vyhlášky č. 528/2005 Sb. Výtisk č. 2 se zakládá u organizačního celku. Odbor bezpečnosti je v kontaktu s bezpečnostním manažerem organizačního celku, který je odpovědný za zpracování návrhu projektu fyzické bezpečnosti. Pověřený zástupce odboru bezpečnosti osobně ověřuje v místě předpokládané instalace kontrolu technických prostředků, kde vyhotovuje výsledné stanovisko ve dvou výtiscích, jenž přikládá k návrhu bezpečnostního projektu. [13]
b) V druhé etapě se návrh bezpečnostního projektu vypracovává ve čtyřech výtiscích za předpokladu, požaduje-li se v rámci první etapy úpravy návrhu bezpečnostního projektu. Výtisk č. 1 až výtisk č. 3 se s průvodním spisem zasílá odboru bezpečnosti MO, výtisk č. 4 se zakládá u organizačního celku. Opět odbor bezpečnosti MO provede posouzení návrhu projektu bezpečnosti, na základě kterého bezpečnostní ředitel vydává stanovisko, jenž je vyhotoveno ve třech výtiscích. Výtisk č. 1 zasílá vojenské stavební a ubytovací správě, výtisk č. 2 zasílá sekci správy majetku MO a výtisk č. 3 si zakládá. Je-li zpracována na základě návrhu bezpečnosti prováděcí projektová dokumentace, odbor bezpečnosti ji posuzuje dle tohoto návrhu. [13]

2.1.2 Projekt fyzické bezpečnosti

Na základě schváleného návrhu projektu fyzické bezpečnosti odborem bezpečnosti MO se vypracuje projekt fyzické bezpečnosti pro každý objekt zvlášť. V případě že se nachází v areálu více objektů, může mít některé části společné. [13]

V případě, že se v jednom objektu nachází více ZO nebo JO, je možné tyto oblasti začlenit do jednoho společného bezpečnostního projektu. Projekt fyzické bezpečnosti je zpracován na základě splnění konkrétních podmínek v součinnosti s odborem bezpečnosti MO. Předmětem zájmu je zabezpečení technického zařízení, stanovení režimových opatření, technických prostředků a vhodně zvolená ostraha. [13]

2.1.3 Struktura projektu fyzické bezpečnosti:

1. Určení objektu, zabezpečených oblastí, včetně jejich hranic, určení kategorií a tříd zabezpečených oblastí:
    - popis areálu-budovy (podlaží, vstupy) schéma;
    - určení typu objektu, stanovení objektu, jeho kategorie a stanovení hranic ZO a JO v objektu;
    - zabezpečení objektu;
    - stanovení technických prostředků, režimových opatření, fyzické ostrahy a bodového hodnocení bezpečnostních opatření. [14]
2. Vyhodnocení rizik:
    - posouzení aktiv;
    - možné hrozby a zranitelnosti;
    - stanovení míry rizika (malé, střední nebo velké). [14]
3. Způsob použití opatření fyzické bezpečnosti:
    - zpracovaní bodového hodnocení pro každou ZO a JO zvlášť;
    - schéma obsahující vyznačení hranic objektu, zabezpečených a jednacích oblastí včetně použitých instalovaných technických prostředků;
    - použití technických prostředků včetně jejich základních parametrů;
    - certifikáty technických prostředků (certifikované od NBÚ) včetně příloh certifikátů;
    - prohlášení o shodě pro technické prostředky, které nejsou certifikované od NBÚ včetně popisu jejich použití. [14]

4. Provozní řád objektu:
    - režim pohybu osob a dopravních prostředků;
    - kritéria možnosti zpracování utajovaných informací v objektu;
    - provozní dokumentace k technickým prostředkům;
    - manipulace s klíči, ukládání hesel a manipulace s elektrickými nebo identifikačními zařízeními sloužící ke kontrole vstupu;
    - výkon ostrahy. [14]
5. Plán zabezpečení objektu a zabezpečených oblastí v krizových situacích:
    - stanovení opatření před možnými hrozbami;
    - postup při vzniku mimořádné situace (ochrana utajovaných informací). [14]
6. Seznam dokumentace. [14]

Všechny tyto a další potřebné podklady jsou vypracovány a znázorněny v praktické části diplomové práce při zpracovaném Projektu fyzické bezpečnosti v objektu AČR.

Mezi další povinnosti bezpečnostního manažera dále patří zpracovávání technické dokumentace, která je nedílnou součástí projektu fyzické bezpečnosti. Ke zpracování technické dokumentace se použijí doložené dokumenty, převzaté od dodavatele (vypracované podklady od 3 strany). Velitel organizačního celku, musí obdržet všechny vypracované podklady, které obsahují:

- projektovou dokumentaci,
- pravidla a doporučení zhotovitele veřejné zakázky, včetně návodů a pokynů pro užívání technických prostředků,
- kopie certifikátů vydaných od NBÚ,
- všechny doklady o splnění příslušných norem,
- provozní knihy zařízení elektrické zabezpečovací signalizace, elektrické požární signalizace, elektrické zařízení pro kontrolu vstupu, atd.). [13]

Jednotlivé stupně utajení, které jsou obsahem projektu fyzické bezpečnosti, stanovuje zpracovatel a VOC je schvaluje. Projekt fyzické bezpečnosti je uložen u bezpečnostního manažera nebo velitele organizačního celku. [13]

2.2 Technické prostředky, ostraha a manipulace s klíči

2.2.1 Technické prostředky v objektu AČR

Pro splnění podmínek použití technických prostředků v objektu AČR se vychází ze zákona 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti, které jsou uvedeny v § 30 odst. 1 tohoto zákona. Seznam platných certifikovaných prostředků, včetně bodového hodnocení aktualizuje a zveřejňuje Národní bezpečnostní úřad. Kontroly u organizačního celku AČR z důvodu zajištění ochrany projednávaných utajovaných informací v jednacích oblastech vyžaduje VOC prostřednictvím bezpečnostního ředitele MO. Jedná se zpravidla o kontrolu, zda nedochází k neoprávněnému použití technických prostředků k získávání informací. Kontrolu vykonávají pracovníci NBÚ v součinnosti se zpravodajskými službami a Policií České republiky. [13]

Všechny technické prostředky, které jsou určeny k instalaci v objektu AČR, musí mít vystaven certifikát od NBÚ, který je platný nejméně jeden rok od jeho instalace. Pro všechny ZO kategorie Tajné a Přísně tajné a JO, musí být zabezpečena identifikace prostřednictvím systému pro kontrolu vstupu, které je dohledově vyvedeno na stálé pracoviště ostrahy. VOC, písemně žádá NBÚ o vydání certifikátu pro daný technický prostředek prostřednictvím odboru bezpečnosti MO. K žádosti o vydání certifikátu VOC přikládá vlastní technický posudek prostředku, který vydává organizace pověřená k posuzování technických prostředků. Zkouška technického prostředku se zpracovává na základě funkčních zkoušek, které musí být v souladu s vyhláškou č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků. [13]

2.2.2 Ostraha objektu v rezortu MO

V objektu AČR, kde se nachází zabezpečená oblast kategorie Vyhrazené, a u objektu, kde není stanovena žádná zabezpečená oblast nebo jednací oblast se ostraha zajišťuje odpovědnou osobou. [13] Ostraha musí být prováděna minimálně v pracovní době, pokud VOC, který je za střežení objektu odpovědný, nestanoví jinak. [12]. V objektech AČR, kde se nachází ZO kategorie Důvěrné a vyšší, a u objektu, ve kterém se nachází JO, je ostraha zajištěna v rozsahu stanoveném dle zákona 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů a v příloze č. 1 k vyhlášce č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků ve znění

vyhlášky č. 204/2016 Sb., Vyhláška, kterou se mění vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů [13]

2.2.3 Manipulace s klíči, identifikační prostředky

Režim manipulace s klíči a identifikačními prostředky musí odpovídat směrnicím, které jsou stanoveny pro provozovaný systém, sloužící k zajištění ochrany UI. Za dodržování těchto pravidel jsou odpovědni pracovníci rezortu, kteří splňují podmínky pro daný stupeň utajení v objektech MO.

V režimu manipulace s klíči rozlišujeme v rezortu MO tyto klíče:

- klíč – normální klíč k běžnému použití;
- duplikát – klíč určený k nouzovému otevření;
- revizní klíč – klíč určený k nouzovému použití v úschovných objektech, kde je vyžadován elektrický uzavírací systém;
- hlavní klíč (generální) – klíč určený k použití u ZO a JO, určen k odemykání více zámků (lze použít pouze jako duplikát). [13]

Pro ukládání a manipulaci s klíči v zabezpečené oblasti kategorie Vyhrazené stanovuje pravidla VOC. Pravidla pro ukládání a manipulaci s klíči v ZO a JO kategorie Důvěrné a vyšší jsou určená dle přílohy č. 1 vyhlášky č. 528/2005 Sb. BM určuje přidělení klíčů od úschovných objektů, ZO a JO pouze odpovědné osobě na základě rozhodnutí VOC. Tyto klíče se ukládají pouze na vyčleněné místo (např. do úschovné schránky), které střeží ostraha (za předpokladu, že je na pracovišti ostrahy stále jeden člen). Dále mohou být klíče uloženy do schránek, které jsou vybaveny automatickým uzamykatelným systémem (softwarovým střežením, kamerovým systémem a elektrickou zabezpečovací signalizací) s průhlednou stěnou, umožňující okamžitou vizuální kontrolu uložené schránky s klíči. Schránka na klíče se vždy pečetí, není-li stanoveno VOC jinak. Duplikáty klíčů nesmí být nikdy uloženy na stejném místě. Vynášení klíčů z vojenského objektu je přísně zakázáno, je-li přesto nezbytné klíče z vojenského objektu vynést, povolení vydává pouze VOC. Duplikáty klíčů a revizních klíčů se ukládají pouze v místě, které určil VOC (zpravidla pracoviště ochrany informací). V případě nutnosti otevření úschovného objektu, ZO nebo JO za nepřítomnosti určené osoby, VOC ve svém rozkaze stanoví komisi v počtu nejméně tří členů. Jeden člen je určen předsedou komise. Stanovení členové komise musí splňovat podmínky přístupu k UI s platným poučením fyzické osoby patřičným nebo vyšším stup-

něm utajení. Všechny použité duplikáty klíčů předseda komise vrátí do úložny, kde musí být použitá schránka s klíči zapečetěna jeho vlastní pečetí. Na základě tohoto nařízení vyhotoví předseda komise písemný záznam ve dvou výtiscích, kde se uvádí důvod vstupu do úschovného objektu ZO nebo JO. Do záznamu dále popíše vložené nebo vyjmuté UI, uvede čas otevření a zavření a číslo použité pečetě. Výtisk č. 1 nechá v oblasti, která byla otevřena a výtisk č. 2 se uloží na pracoviště utajovaných informací. [13]

2.3 Fyzická bezpečnost v polních podmínkách

V polních podmínkách se ochrana UI, která je běžně zabezpečená prostřednictvím technických prostředků, zpravidla nahrazuje zvýšenou ostrahou. Zvýšená ostraha nahrazuje zabezpečení technických prostředků v objektu, ve kterém se nacházejí ZO kategorie Důvěrné a vyšší. V kategorii Důvěrné se střežení u objektu provádí nejméně dvěma osobami nebo nejméně jednou osobou a služebním psem. V kategorii Tajné a Přísně tajné se u objektu střežení zabezpečuje nejméně třemi osobami nebo nejméně dvěma osobami a služebním psem. Příslušníci ostrahy vykonávají obchůzky v nepravidelných sekvencích 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. [13]

V případě nutnosti zajistit ochranu UI na vojenském cvičení se na základě rozkazu velitele cvičení určuje 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. Jedná se o certifikované technické prostředky, zvýšenou ostrahu nebo jejich vzájemnou kombinaci. [13]

2.3.1 Projekt fyzické bezpečnosti v zahraničních operacích

Při vojenském výcviku nebo cvičení se projekt fyzické bezpečnosti nezpracovává, nestanoví-li velitel jinak. [12] Projekt fyzické bezpečnosti, který se zpracovává pro potřeby zahraniční operace, musí obsahovat:

- hranice objektu, kategorie a popis zabezpečeného objektu,
- zabezpečené oblasti v objektu, úložny UI, pracoviště s informačním systémem,
- popis hranice zabezpečených oblastí a jejich umístění,
- výkresovou dokumentaci a dokumentaci technických prostředků,

- režimová opatření fyzické bezpečnosti,
- způsoby zajištění ostrahy. [13]

2.4 Dílčí závěr

V druhé kapitole teoretické části diplomové práce je analyzován postup při vytváření „Projektu fyzické bezpečnosti“ v objektu AČR. Projekt fyzické bezpečnosti se musí vždy zpracovat nebo aktualizovat v případech, kdy se nachází v objektu AČR zabezpečená oblast kategorie Důvěrné, Tajné a Přísně tajné nebo jednací oblasti stupně utajení Tajné a Přísně tajné.

Za fyzickou bezpečnost v objektech AČR odpovídá v plné míře velitel organizačního celku nebo velitel rozsáhlého objektu. V případě nutnosti zřízení nové zabezpečené nebo jednací oblasti ustanovuje velitel komisi, která analyzuje hranice objektu a vypracuje „Návrh projektu fyzické bezpečnosti“ pro zabezpečenou nebo jednací oblast. Po schválení návrhu projektu fyzické bezpečnosti odborem bezpečnosti Ministerstva obrany se vypracuje samotný „Projekt fyzické bezpečnosti“, který schvaluje velitel organizačního celku nebo velitel rozsáhlého objektu.

Projekt fyzické bezpečnosti pro každou zabezpečenou oblast stupně utajení kategorie Důvěrné a vyšší nebo jednací oblast musí obsahovat pevně stanovenou strukturu na základě platné legislativy, kde jsou definovány všechny potřebné informace o tomto objektu. Mezi tyto informace patří určení objektu zabezpečených a jednacích oblastí včetně jejich hranic, určení kategorie, stupňů utajení a tříd, způsob použití opatření fyzické bezpečnosti, provozní řád objektu a plán zabezpečení objektu zabezpečených a jednacích oblastí v krizových situacích.

II. PRAKTICKÁ ČÁST

3 ANALÝZA BEZPEČNOSTNÍCH TECHNOLOGIÍ K ZAJIŠTĚNÍ FYZICKÉ BEZPEČNOSTI V ZO A JO OBJEKTU AČR

Pro zabezpečení utajovaných informací a aktiv v objektech armády České republiky je hlavní prioritou určení zabezpečených a jednacích oblastí, které se v objektu nacházejí. Objektem může být budova, areál nebo jinak ohraničený prostor, ve kterém se zpravidla tyto zabezpečené a jednací oblasti zřizují. [14] Objekt může obsahovat více vnořených objektů, kde například v jednom areálu - objektu je vnořeno více objektů – budov. Každý objekt musí mít jednoznačně vymezené hranice, v jejímž rámci je zajištěna kontrola osob popřípadě vjezd vozidel.

Zabezpečená oblast a jednací oblast je ohraničený prostor v objektu. V některých případech může mít zabezpečená a jednací oblast společnou hranici s objektem. Jednací oblast slouží pouze k projednávání utajovaných informací se stupněm utajení Tajné a Přísně tajné. Ve většině případů se jedná o jednu konkrétní místnost. Do objektu na základě projektu fyzické bezpečnosti se může vystavit více zabezpečených a jednacích oblastí.

V první části této kapitoly jsou popsány možnosti použitých technologií pro zabezpečené a jednací oblasti s tabulkami bodových hodnot, sloužící k výpočtu míry rizika pro konkrétní stupeň utajení. V druhé části kapitoly jsou definovány a na příkladech uvedeny technické prostředky, které se používají v zabezpečených a jednacích oblastech objektu Armády České republiky. Technické prostředky jsou ve většině případů vybrány z reálných objektů AČR, od firem, které se podílí na návrhu a vyhotovení projektových dokumentací.

Mezi hlavní požadavky na firmy, které se podílí na analýze fyzické bezpečnosti v objektech AČR a instalaci technických prostředků patří:

- bezpečnostní posouzení (obhlídka, rozhodnutí o účelnosti a rozsahu zabezpečení),
- technická studie a cenová kalkulace (technické a cenové řešení požadavku),
- projektová dokumentace (dokumentace k realizaci, materiál a montáž zařízení),
- realizace (instalace a nastavení mechanických a technických prostředků),
- technická podpora a servis (nepřetržitá technická podpora 24 hodin),
- revize (kontrola instalace, plnění norem a předpisů).

Tyto vybrané společnosti (firmy) se na základě výběrového řízení stávají členy komise, kde v součinnosti s ostatními členy komise zpracovávají potřebné podklady a opatření pro Návrh projektu fyzické bezpečnosti.

3.1 Technologie pro zajištění bezpečnosti zabezpečených oblastí objektu AČR

K rozsahu zabezpečení ZO v objektu AČR jsou vybrány mechanické a technické prostředky, které jsou voleny na základě požadavků potřebné kategorie, třídy a vyhodnocení rizik určené zabezpečené oblasti.

Nasazení mechanických a technických prostředků pro zabezpečenou oblast:

- **Vyhrazené** – mechanické zábranné prostředky,
- **Důvěrné** – mechanické zábranné prostředky, poplachové zabezpečovací a tísňové systémy,
- **Tajné a Přísně tajné** – mechanické zábranné prostředky, systémy pro kontrolu vstupů, poplachové zabezpečovací a tísňové systémy, speciální televizní systémy, které mohou být nahrazeny tísňovými systémy a zařízením elektrické požární signalizace.

Pokud je v zabezpečené oblasti kategorie Důvěrné a vyšší zabezpečena trvalá přítomnost pracujících osob, zabezpečení se provádí zpravidla mechanickými zábrannými prostředky a zařízením poplachových zabezpečovacích a tísňových systémů. V případě, že je v tomto objektu zřízena stálá ostraha, není vyžadován poplachový zabezpečovací systém. Pokud jsou nasazeny kamerové systémy, nesmí dojít k přímému snímání utajovaných informací. K zajištění fyzické ochrany se používají především certifikované technické prostředky. Necertifikované technické prostředky se mohou použít pouze v případě, pokud nedojde ke snížení bodového ohodnocení pro splnění nejnižší míry rizika pro konkrétní stupeň utajení zabezpečené oblasti. [14]

Zabezpečení pro hranice objektu musí odpovídat vždy nejvyšší kategorii zabezpečené oblasti, která se v objektu nachází. Technické prostředky se rovněž volí na základě vyhodnocení rizik. [14]

Tabulka, která určuje bodové ohodnocení míry rizika pro zabezpečenou oblast stupně utajení Důvěrné, Tajné a Přísně tajné je znázorněna níže.

Tab. 1. Zabezpečená oblast kategorie Důvěrné, Tajné a Přísně tajné [8]

ZABEZPEČENÁ OBLAST KATEGORIE Přísně Tajné	**Míra rizika**		
	malá	střední	velká
Povinné : (S1) + (S2) + (S3)	10	11	13
Povinné : (S4) + (S5) *	6	7	7
Nepovinné : (S6)	4	5	5
Celkový výsledek	**20**	**23**	**25**
ZABEZPEČENÁ OBLAST KATEGORIE Tajné	**Míra rizika**		
	malá	střední	velká
Povinné : (S1) + (S2) + (S3)	8	9	10
Povinné : (S4) + (S5) **	4	5	5
Nepovinné : (S6)	4	5	5
Celkový výsledek	**16**	**19**	**20**
ZABEZPEČENÁ OBLAST KATEGORIE Důvěrné	**Míra rizika**		
	malá	střední	velká
Povinné : (S1) + (S2) + (S3)	6	8	9
Povinné : (S4) + (S5)	2	3	3
Nepovinné : (S6)	3	3	4
Celkový výsledek	**11**	**14**	**16**

3.2 Technologie pro zajištění bezpečnosti jednacích oblastí objektu AČR

Zabezpečení jednací oblasti v objektu AČR se stanovuje taktéž na základě vyhodnocení rizik v návaznosti na stupni utajovaných informací, které se v jednací oblasti projednávají. V jednacích oblastech se pravidelně projednávají pouze utajované informace stupně utajení Tajné a Přísně tajné. Tyto oblasti se zabezpečují: mechanickými zábrannými prostředky, systémy pro kontrolu vstupu, zařízeními poplachových zabezpečovacích a tísňových systémů, speciálními televizními systémy, zařízeními elektrické požární signalizace, zařízeními proti aktivnímu a pasivnímu odposlechu utajované informace. Tísňové systémy mohou nahradit speciální televizní systémy. Necertifikované technické prostředky mohou být opět použity za předpokladu, že se neponíží stupeň ochrany dané kategorie utajení. Hranice objektu, ve které se jednací oblast nachází, musí splňovat rozsah použití technických prostředků a zabezpečení v návaznosti na stupni utajení projednávaných informací a vyhodnocení rizik. Hranice objektu je zabezpečena mechanickými zábrannými prostředky, zařízením elektrických zabezpečovacích systémů a speciálním televizním systémem. Pokud nastane situace, kdy hranice jednací oblasti je totožná s hranicí objektu, vychází se z použití zabezpečení fyzické bezpečnosti stanovené pro jednací oblast. K likvidaci utajovaných informací se v objektu pořizuje zařízení sloužící k ničení utajovaných informací. [14]

Tato zařízení musí být certifikována pro ničení utajovaných informací daného stupně utajení. Pro představu, nemůže nikdy nastat situace, že Přísně tajnou informaci budu skartovat v zařízení pro ničení utajovaných informací stupně utajení Důvěrné.

Vyhodnocování rizik se provádí průběžně. V případě potřeby se míra opatření fyzické bezpečnosti muže upravit. [14] Velitel organizačního celku, popřípadě bezpečnostní manažer daného celku musí zajistit průběžnou kontrolu, zda použitá opatření fyzické bezpečnosti splňují stanovená kritéria, odpovídající projektu fyzické bezpečnosti pro zabezpečené a jednací oblasti ve svěřeném objektu Armády České republiky.

Tab. 2. znázorňuje bodového ohodnocení míry rizika pro jednací oblast stupně utajení Tajné a Přísně tajné.

Tab. 2. Jednací oblast stupně utajení Tajné a Přísně tajné [8]

JEDNACÍ OBLAST pro pravidelné projednávání utajovaných informací stupňů utajení **Přísně Tajné**	**Míra rizika**		
	malá	střední	velká
Povinné : (S2) + (S3)	6	6	7
Povinné : (S4) + (S5) *	6	7	7
Nepovinné : (S6)	4	5	5
Celkový výsledek	**16**	**18**	**19**
JEDNACÍ OBLAST pro pravidelné projednávání utajovaných informací stupňů utajení **Tajné**	**Míra rizika**		
	malá	střední	velká
Povinné : (S2) + (S3)	5	5	6
Povinné : (S4) + (S5) **	4	5	5
Nepovinné : (S6)	4	5	5
Celkový výsledek	**13**	**15**	**16**

3.3 Technické prostředky, certifikace technických prostředků

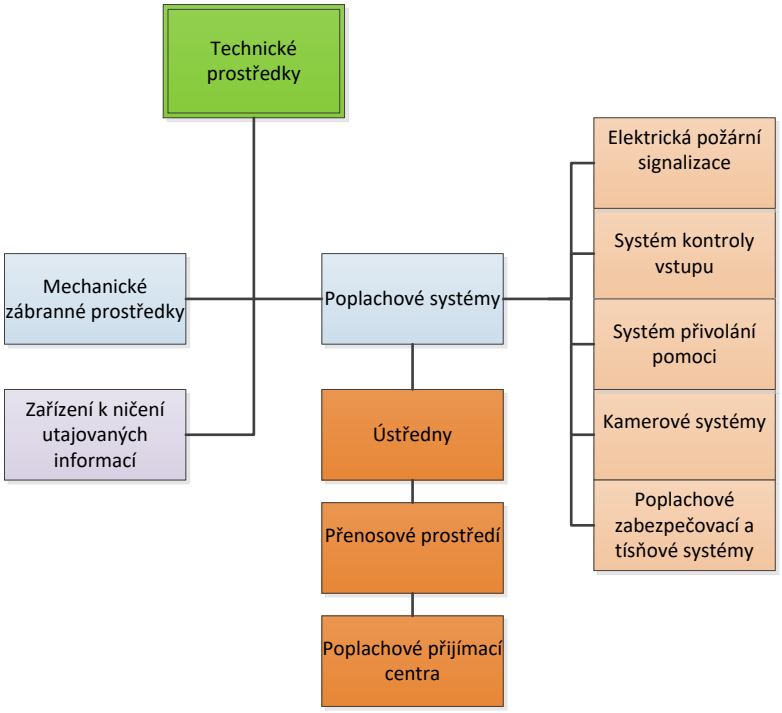
Technické prostředky v součinnosti s fyzickou ostrahou a režimovým opatřením doplňují fyzické zabezpečení daného objektu AČR. Hlavní podstatou těchto technických prostředků je odradit narušitele od jeho činu, nebo jeho snahu ztížit popřípadě zvýšit dobu překonání k přístupu k utajovaným informacím a dalším aktivům.

Technické prostředky, které slouží k ochraně utajovaných informací, jsou složeny z mechanických prostředků ochrany, kamerových systémů, systémů kontroly vstupu, požárních systémů, poplachových zebezpečovacích a tísňových systémů nebo poplachových systémů. Hlavní funkcí je detekce hrozby, která může nastat vůči vojenskému objektu AČR. [3]

Technické prostředky, sloužící k ochraně utajovaných informací v objektech AČR, můžeme rozdělit na:

- mechanické zábranné prostředky (MZP),
- elektrická zámková zařízení a systémy pro kontrolu vstupu (EKV),
- poplachové zabezpečovací a tísňové systémy (PZTS),
- kamerové systémy (CCTV),
- elektrické požární signalizace (EPS),
- zařízení sloužící k vyhledávání nebezpečných látek nebo předmětů,
- zařízení sloužící k ničení utajovaných informací,
- zařízení proti aktivnímu a pasivnímu odposlechu. [3]

Na obr. 3. můžeme vidět základní rozdělení technických prostředků ochrany.



Obr. 3. Technické prostředky ochrany

Do mechanických zábranných prostředků řadíme dveře, zámky, ploty, stavební prvky budov, komorové trezory, úschovné objekty apod. Do poplachových systémů patří systémy elektrické požární signalizace, systémy pro kontroly vstupu, systémy přivolání pomoci, kamerové systémy a poplachové zabezpečovací a tísňové systémy. K vyhodnocení signálů z naměřených detektorů slouží ústředny, které mohou být napojeny na dohledová poplachová a přijímací centra. [3]

Certifikace technických prostředků

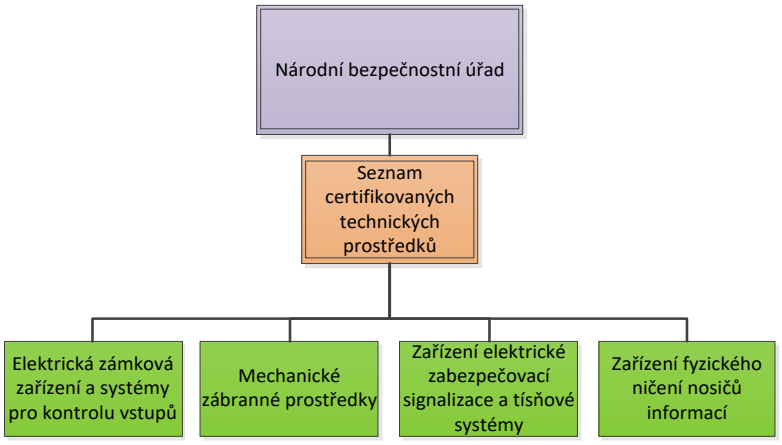
K zajištění ochrany v zabezpečených oblastech a jednacích oblastech objektu MO se používají certifikované technické prostředky, kde způsob certifikace stanovuje Příloha č. 1 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků.

Necertifikované technické prostředky je možné použít u zabezpečené oblasti kategorie Vyhrazené a dále pouze v případě, že není snížena úroveň stupně utajení.

Armáda České republiky nemá v současné době stanovený žádný upřesňující standard pro použití certifikovaných technických prostředků. Subjekt, který zajišťuje výběr technických prostředků k použití v zabezpečených a jednacích oblastech objektu AČR musí volit tyto prostředky pouze z certifikovaných prostředků, schválených NBÚ.

Národní bezpečnostní úřad schvaluje technické prostředky sloužící k ochraně utajované informace popřípadě aktiv. Schválení potvrzuje NBÚ vystavením „Certifikátu technického prostředku“. Všechny tyto certifikáty jsou neodlučitelnou součástí Projektu fyzické bezpečnosti pro zabezpečené a jednací oblasti pro určený stupeň utajení. Jednotlivé certifikované technické prostředky můžeme najít na stránkách NBÚ v seznamu certifikovaných technických prostředků.

Na obr. 4. můžeme vidět rozdělení certifikovaných technických prostředků podle NBÚ.



Obr. 4. Seznam certifikovaných technických prostředků [15]

Platnost Certifikátu technického prostředku se stanovuje nejdéle na dobu pěti let. Po uplynutí této doby platnosti certifikátu mohou být technické prostředky nadále používány za předpokladu splnění podmínky, že jsou plně funkční. Ověření se provádí funkční zkouškou, vykonanou minimálně jednou ročně. U mechanických zábranných prostředků

a zařízení ničení informací se funkční zkouška doloží zápisem, který schvaluje VOC. Ostatní technické prostředky mohou mít funkční zkoušku doloženou protokolem o zkoušce nebo záznamem v provozní knize. [16]

Míra zabezpečení zabezpečené oblasti a jednací oblasti se určuje podle bodových hodnot, na základě výsledku vyhodnocení rizik. Bodové ohodnocení musí odpovídat aspoň nejnižší možné míře vyhodnocení rizik pro stanovenou kategorii nebo stupeň utajení. Bodové hodnoty, sloužící k výpočtu stanovení míry rizika, se liší na základě použitých mechanických a technických prostředků. [3]

Každý certifikát, schválený NBÚ, musí obsahovat tyto údaje:

- evidenční číslo certifikátu,
- typové označení technického prostředku a název,
- identifikace výrobce technického prostředku,
- ověření způsobilosti technického prostředku daného typu,
- bodové hodnocení technického prostředku,
- datum vydání certifikátu a jeho platnost,
- úřední razítko s podpisem,
- přílohy. [14]

3.4 Mechanické zábranné prostředky

Mechanické zábranné prostředky jsou určeny k ochraně před útokem neoprávněné osoby. Kladou si za cíl narušitele co možná nejdéle zdržet před vniknutím, popřípadě úplně odradit od jeho počínání. Každý typ mechanických zábranných prostředků je překonatelný, ale záleží na kvalitě a odolnosti jeho překonání v čase. [14]

MZP jsou zejména prostředky sloužící k ohraničení prostor, jako jsou zdi, ploty vstupní otvory, bezpečnostní systémy skládající se z vrat, branek, dveří, oken. Můžou zde být použity mříže, bezpečnostní skla, fólie nebo vlastní uzamykací systémy. K MZP řadíme i prostředky individuální předmětové ochrany, které slouží samostatně, zejména jako úschovné objekty (trezory). [3]

Používané mechanické zábranné prostředky v objektech AČR:

- mříže (pevné, rolovací a otevíratelné),
- bezpečnostní dveře (zámky a cylindrické vložky),

- předmětová ochrana – úschovné objekty (trezory),
- úložny klíčů.

3.4.1 Mříže

Montáž mříží do zabezpečených nebo jednacích oblastí objektu AČR musí být vhodně zvolena pro konkrétní bezpečnostní třídu a stupeň utajení. Mříže rozdělujeme na základě konstrukce na pevné kotvené, rolovací (průhledné, neprůhledné) a otevírací. Otevírací mříže rozlišujeme jednokřídlé nebo dvoukřídlé (otočné, sklopné a posuvné). Konstrukce mříží musí být tuhá a stabilní. Po celé své ploše se nesmí prohnout ani roztáhnout. Všechny spoje prutů a příčníků musí být svařeny do formy nerozebíratelného celku. Hlavní důraz se klade na ukotvení mříží, které může být přímé nebo kolmé. [17]

V tab. 3. je uvedeno několik příkladů certifikovaných mříží, na základě jejich rozdělení podle čísla certifikátu, názvu, označení, kategorie použití a jejich bodového hodnocení potřebného pro dosazení k výpočtu míry rizika.

Tab. 3. Příklady certifikovaných mříží

Číslo certifikátu	Technický prostředek	Označení	Kategorie použití	Bodové ohodnocení	Platnost certifikátu
T0070/2018	Pevná mříž typ MS1	max. rozměr 1200 x 2700 mm	3	SS3=3	15. 11. 2021
				SS4=2	
T0013/2018	Bezpečnostní rolovací mříž	Typ RL P – RC 3	3	SS3=3 SS4=2	27. 02. 2021
T0033/2018	Křídlová mříž BESTSERVIS	Typ KMB	2	SS3=2 SS4=1	27. 03. 2021

3.4.2 Bezpečnostní dveře

Bezpečnostní dveře se rozdělují do šesti bezpečnostních tříd podle normy ČSN EN 1627 až ČSN ČN 1630 (RC1 až RC6), kde každá třída charakterizuje míru odolnosti před vniknutím neoprávněné osoby. [18] Základ bezpečnostních dveří tvoří rám dřevěné nebo železné konstrukce, ve kterém je uložen bodový bezpečnostní zámek s vnitřním rozvorovým systémem. Bezpečnostní dveře mohou být vyplněny zvukovou izolací, nehořlavou výplní proti požární odolnosti nebo ocelovou konstrukcí proti průniku. K usazení bezpečnostních dveří se zpravidla využívá odolných bezpečnostních závěsů proti vysazení. [17]

3.4.3 Typy zámků a cylindrických vložek

Zámky rozdělujeme podle systému na pevné (zapuštěné, polozapuštěné a nasazené), visací, lanové a speciální (elektronické a elektromagnetické). Podle typu otevírání dělíme zámky na ruční, mincové, kartové, heslové, klíčové atd. [17]

Cylindrické vložky jsou hlavní součástí zámků. Jedná se o válec s otvorem pro klíč, kde se nachází různý počet odpružených stavítek s blokovacími kolíky. Zámek tvoří dvě stejné cylindrické vložky, kde je zabráněno vsunutí klíče z obou stran. Je zde možnost vložit nadstavení mezi stavítko a blokovací kolík pro potřeby otočení vložky ve dvou různých polohách, což umožnuje vytvořit generální (hlavní) klíč, který se použije k otevření různých zámků. [17]

V tab. 4. jsou uvedeny příklady certifikovaných bezpečnostních dveří a cylindrické vložky schválené NBÚ.

Tab. 4. Příklady certifikovaných bezpečnostních dveří a cylindrické vložky

Číslo certifikátu	Technický prostředek	Označení	Kategorie použití	Bodové ohodnocení	Platnost certifikátu
T0009/2016	Bezpečnostní dveře SAPELI RC3	S dvojitou polodrážkou	3	SS3=3 SS4=2	21. 04. 2019
T0085/2016	Bezpečnostní dveře BEDEX	VARIO VD4 se zárubní MRB	4	SS3=4 SS4=3	22. 11. 2019
T0018/2016	Bezpečnostní cylindrická vložka EVVA ICS SGHK	Varianty provedení jsou v příloze	3 při splnění podmínek v příloze	SS4=3 SS4=3	18. 04. 2019

3.4.4 Předmětová ochrana

Předmětovou ochranu tvoří opatření vedoucí k zamezení zcizení chráněných aktiv nebo získání utajovaných informací. Jedná se zejména o úschovné objekty v zabezpečených oblastech objektu AČR. Úschovnými objekty jsou myšleny úschovné schránky, trezory, komorové trezory popřípadě úschovné kontejnery. [3]

Při výběru trezoru musíme vhodně zvolit odpovídající bezpečnostní třídu trezoru, kterou chceme použít do zabezpečené oblasti. Česká republika zařazuje trezory bezpečnostních tříd podle dvou norem. První je česká norma ČSN 916012 a druhá je evropská norma EN 1143-1. Norma EN 1143-1 definuje bezpečnost trezorů v případech, kdy je kladena větší

bezpečnost na trezory. Tato norma dělí trezory do sedmi bezpečnostních tříd. Norma ČSN 916012 rozlišuje celkem tři stupně bezpečnostních tříd. [19]

Bezpečnostních tříd je tedy sedm a označují se 0 až VI. Každý trezor, který je zařazen do příslušné bezpečnostní třídy, obsahuje typový štítek na vnitřní straně dveří, který je k trezoru pevně připevněn. Klasifikace trezorů je shodná v celé Evropské unii. [19]

Národní bezpečnostní úřad hodnotí úschovné objekty podle odolnosti proti násilnému vniknutí. Podle těchto hodnocení může úschovný objekt sloužit pro ukládání utajovaných informací odpovídající třídy utajení, za předpokladu umístění v zabezpečené oblasti objektu AČR. [20]

V tab. 5. můžeme vidět rozdělení bezpečnostních tříd pro ukládání utajovaných informací schválené Národním bezpečnostním úřadem.

Tab. 5. Třídy utajení úschovných objektů podle NBÚ [20]

Typ	Stupeň utajení	Pro utajované skutečnosti	Bezpečnostní třída
Typ 1A	V	„vyhrazené“	Z1
Typ 1B	V	„vyhrazené“	Z2
Typ 1C	V	„vyhrazené“	Z3
Typ 2	D	„důvěrné“	0
Typ 3	T	„tajné“	I
Typ 4	PT	„přísně tajné“	II, III, IV

3.4.5 Úložny klíčů

Úložny klíčů jsou zařízení, která slouží k bezpečnému uložení a evidování důležitých klíčů se kterými může manipulovat pouze pověřená osoba. Úložny klíčů umožnují elektronickou evidenci otevření a zavření schránek, popřípadě akustickou signalizaci se záznamem do paměti historie událostí. Otevření a zavření schránky probíhá na základě identifikace uživatele po přiložení bezkontaktní karty a zadáním potvrzujícího PIN kódu. Systém umožnuje nastavení různých časových prodlev potřebných k otevření – zavření schránek. V případě výpadku elektrického proudu systém obsahuje záložní napájení, které v případě výpadku proudu aktivuje napájecí akumulátory. Úložny klíčů řídí řídící jednotka, která ovládá elektromagnetické zámky jednotlivých schránek a snímá pomocí kontaktů přítomnost klíčů ve schránce. Zařízení je možné prostřednictvím LAN propojit se serverem. [21]

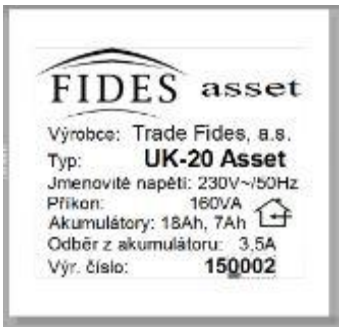
Většina objektů Armády České republiky je vybavena úložnami klíčů od firmy Raisa spol. s. r. o se sídlem v Kolíně, která je znázorněna na obr. 5.

Obr. 5. Úložna klíčů RAISA-UK20 [3]

V tabulce 6. jsou uvedena technická data úložny klíčů UK 20 s napájením prostřednictvím dvou zdrojů PWR 4A se štítkem, který se umísťuje v odklápěcím štítu klíčového trezoru.

Tab. 6. Technická specifikace úložny klíčů – UK 20 [22]

Rozměr	560x610x280 ŠxVxH	Montáž	na zeď	
Napájení	195 až 265VAC	Hmotnost	cca 60 kg	
Příkon	10W + 4,3W na sepnutý zámek	Materiál	kov	
Prostředí	třída II	Provozní teplota	minus10°C až +40°C	
Krytí	IP 30	Provozní vlkhost	10 až 80%	štítek UK-20 Asset



3.5 Poplachové systémy

Integrace poplachového systému v rezortu MO

Integrace poplachových systémů představuje využití technologických bezpečnostních prvků, mezi které řadíme: kamerové systémy (CCTV), systém kontroly vstupů, poplachové zabezpečovací a tísňové systémy, systémy přivolání pomoci a elektrické požární systémy. Tyto systémy můžou vzájemně spolupracovat (propojit se) nebo mohou být doplněny o systémy nepoplachové k potřebám zvýšení své efektivnosti. [23]

Mechanické zábranné prostředky mohou být na základě zvýšení ochrany fyzické bezpečnosti doplněny o detektory narušení, které můžeme aplikovat do perimetrické, prostorové, předmětové a plášťové ochrany. [3]

Detektory narušení doplňující mechanické zabezpečení:

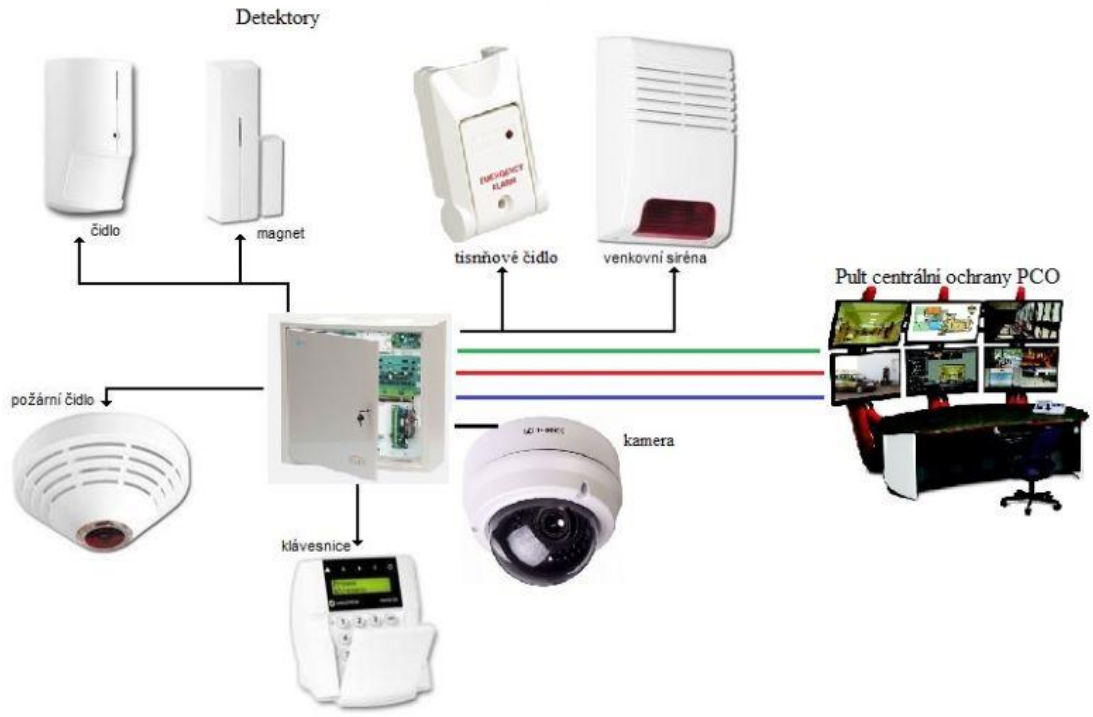
- IR závory a bariéry, mikrovlnné bariéry, štěrbinové kabely,
- magnetické kontakty, vibrační snímače, akustické detektory,
- detektory pasivní a aktivní IR, aktivní ultrazvukové a mikrovlnné,
- tlakové detektory, kontaktní detektory, tahové a kapacitní detektory. [3]

3.5.1 Poplachový zabezpečovací a tísňový systém

Poplachový zabezpečovací a tísňový systém (dále jen PZTS) byl dříve nazýván elektrický zabezpečovací systém nebo elektrická zabezpečovací signalizace. V současné době je snahou ucelit jednotný název „ Poplachový zabezpečovací a tísňový systém“. PZTS patří do poplachových systémů, kde hlavním úkolem je zefektivnit bezpečnost fyzické ochrany v součinnosti s mechanickými zábrannými prostředky při využití konkrétních detektorů, tísňových hlásičů nebo detektorů reagujících na změnu fyzikálních jevů. Jedná se o poplachový systém, přesněji digitální elektronický systém, který monitoruje střežený prostor a v případě narušení vyhlašuje poplach. [14]

Všechny komponenty PZTS musí být vzájemně kompatibilní, kde hlavní důraz je kladen na společnou kategorii zabezpečení. Data se přenáší od ústředny přenosovým prostředím na vzdálené Dohledové a Poplachové Přijímací centrum DDPC, (pult centrální ochrany PCO, mobil, sledovací PC atd.). Přenos probíhá prostřednictvím drátové nebo bezdrátové komunikace. PZTS je tedy tvořen souborem detektorů (senzorů), tísňových systémů, přenosových zařízení, ústředen a doplňkových zařízení, které jsou vzájemně mezi sebou propojeny. [3]

Na obr. 6. můžeme vidět jednoduché schéma PZTS, které na základě potřeb zabezpečení obsahuje magnetické kontakty, PIR detektory, tísňové detektory, kamerové systémy, požární hlásiče, akustické sirény atd. Všechny tyto prostředky jsou napojeny na ústředny, které prostřednictvím přenosového prostředí přenáší data (informace) do řídícího centra DDPC.



Obr. 6. Jednoduché schéma zapojení PZTS (upraveno) [25]

PZTS dělíme na:

- poplachový tísňový systém (PTS),
- poplachový zabezpečovací systém (PZS). [3]

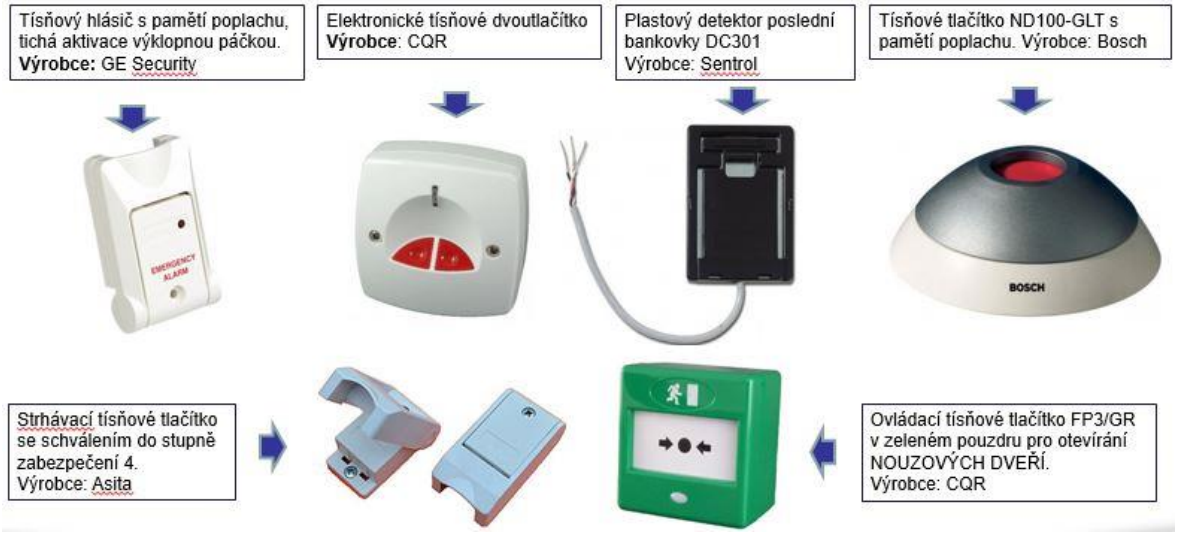
3.5.1.1 Poplachový tísňový systém

Poplachový tísňový systém (dále jen PTS) je zařízení, které na základě aktivace vygeneruje tísňový signál nebo zprávu. Mezi tyto zařízení patří spínače, lišty, tlačítka, dálkové ovladače atd. Všeobecně je možné nastavit přenos tísňového signálu na ústřednu, která zaznamená aktualizaci poplachu a prostřednictvím přenosového prostředí posílá k dalšímu vyhodnocení. [3]

Prvky tísňového hlášení:

- veřejné tísňové hlásiče,
- speciální tísňové hlásiče,
- automatické tísňové hlásiče,
- osobní tísňové hlásiče. [3]

Na obr. 7. jsou znázorněny prvky tísňových hlásičů s různými možnostmi aktivace poplachu.



Obr. 7. Různé druhy tísňových hlásičů [3]

3.5.1.2 Poplachový zabezpečovací systém

Poplachový zabezpečovací systém (dále jen PZS) je mnohem sofistikovanější než tísňový systém, protože obsahuje daleko více periférií, které se používají v plášťové, prostorové předmětové a obvodové ochraně. [3]

Používané detektory pro PZS, nazývané také jako senzory, snímače nebo čidla, jsou zařízení, která na základě měření požadované fyzikální veličiny reagují na změnu, která je aktivována při narušení střeženého prostoru nebo při neoprávněné manipulaci s tímto zařízením. [26]

Elektromechanické detektory narušení:

- mechanické detektory (drátové detektory, rozpěrné tyče, vibrační detektory),
- magnetické detektory (magnetické kontakty),
- tenzometrické detektory (závěsové detektory, váhové detektory, plotové detektory),
- kontaktní detektory (poplachové fólie, tapety a skla, fóliové polepy a pasivní kontaktní detektory rozbití skla),
- nášlapné detektory,
- diferenciální tlakové detektory. [14]

Elektromagnetické detektory

- pasivní infračervené detektory,
- infračervené bariéry a závory,

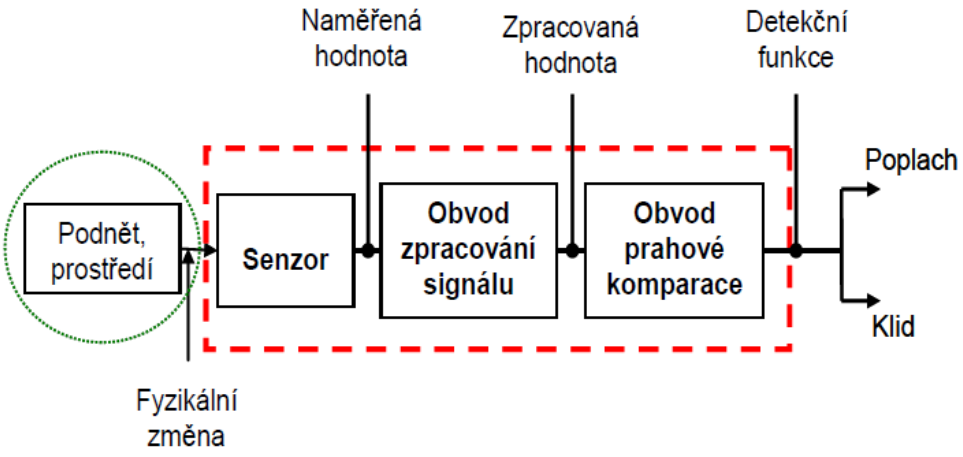
- mikrovlnné detektory,
- rádiové bariéry a detektory,
- štěrbinové detektory,
- kapacitní detektory,
- laserové radary. [14]

Elektroakustické detektory -

- pasivní detektory – Jedná se o detektory, které vyhodnocují akustický signál vznikající při překonání překážek anebo při pohybu v chráněném prostoru. Pasivní detektory obsahují pouze přijímač akustického signálu;
- aktivní detektory na základě Dopplerova jevu – Aktivní detektory vyhodnocují překonání překážek anebo pohyb ve střeženém objektu na základě změny charakteristiky akustické tlakové vlny vysílané detektorem. Tyto detektory obsahují vysílač i přijímač akustického signálu. [14]

K vzájemnému propojení mezi jednotlivými detektory slouží linkové moduly, kde modul obsahuje několik vstupů a výstupů pro jednotlivé soustředěné zapojení těchto komponent.

Detektor slouží jako hlavní zdroj informace potřebné k měření okolního prostředí jako je snímání dostupných fyzických a chemických veličin. Zpravidla převádí jeden druh energie na jiný druh energie - elektrické energie. Inteligentní senzory obsahují obvody, sloužící ke zpracování a analýze signálu v kompaktním provedení. Příklad vyhodnocovacích postupů inteligentního elektromechanického detektoru je znázorněn na obr. 8. [27]



Obr. 8. Funkce elektromechanického detektoru [27]

Detektorů je tedy celá řada. Pro představu níže jsou uvedeny a popsány tři detektory (senzory), které se instalují do zabezpečených a jednacích oblastí v objektu AČR. Jedná se o mechanické detektory, magnetické detektory, otřesové a pasivní infračervené detektory.

3.5.1.2.1 Mechanické detektory

Mechanické detektory, nazývané také jako spínače, jsou detektory, které jsou konstrukčně uzpůsobené pro zabudování do rámu proti západce dveří. Funkčně dosedají na vodivé plošky, uzavírající elektrický obvod. Při neoprávněném přerušení těchto kontaktů je vyvolán poplach. Mechanické detektory mohou být zapojeny a vyhodnocovány ústřednou PZS, která zabrání přechodu do stavu střežení, pokud některý z detektorů není uzamčen.[14]

3.5.1.2.2 Magnetické detektory (kontakty)

Magnetické detektory jsou prvky, používané v plášťové ochraně. Umísťující se na vstupní otvory, jako jsou dveře a okna. Funkčně jsou konstruovány jako dvojice komponent s jazýčkovými kontakty a permanentním magnetem. Zpravidla jeden z kontaktů je spínací a druhý rozpínací. Pro připojení se využívá čtyř vodičů, kde dva vodiče jsou spojeny s jazýčkovými kontakty a druhé dva jsou v magnetickém detektoru propojeny jako sabotážní smyčka. V případě že se zvětší vzdálenost mezi permanentním magnetem a jazýčkovými kontakty, nastává zeslabení intenzity magnetického pole, spínací jazýčkový kontakt se rozpojí a nastává vyhlášení poplachu. [14]

Na obr. 9. je uveden magnetický detektor JA – 181M od firmy Jablotron, používaný k detekci otevření nebo zavření dveří a oken. Tento detektor reaguje na oddálení magnetu od senzoru, který spouští poplach okamžitě nebo s nastaveným zpožděním. V tab. 7. pod obr. 9. můžeme vidět technickou specifikaci tohoto detektoru. [28]

Obr. 9. Magnetický detektor [28]

Tab. 7. Technická specifikace magnetického detektoru JA 181M [28]

Technická specifikace	
Podmínky provozování	ČTÚ VO-R/10/06.2009-9
Napájení	Lithiová baterie typ LS(T)14500 AA (3,6V / 2,4 Ah)
Komunikační pásmo	868,1 MHz, protokol Jablotron (není kompatibilní s jinými Jablotron EZS´)
Rozměry	elektronika:110 x 31 x 26 mm, 90g magnet: 56 x 16 x 15 mm
Komunikační dosah	cca 300m (přímá viditelnost)
Typická životnost baterie	cca 3 roky (pro max. 20 aktivací denně)
Rozsah pracovních teplot	-10 až +40 °C
Prostředí dle ČSN EN 50131-1	II. vnitřní všeobecné
Klasifikace	dle ČSN EN 50131-1, ČSN EN 50131-2-6, ČSN EN 50131-5-3 stupeň 2
Vstupy pro externí snímače	IN2 a TMP = rozpínací smyčky IN1=jednoduše vyvážená smyčka
Dále splňuje	ČSN ETSI EN 300220, ČSN EN50130-4, EN55022, ČSN EN 60950-1

3.5.1.2.3 Pasivní infračervené detektory

Pasivní infračervené detektory (PIR detektory) patří mezi nejpoužívanější prvky prostorové ochrany. Pyročlen umožňuje detekci pohybu na základě teploty pozadí střežené oblasti pomocí pyroeletrického jevu. PIR detektor snímá infračervené záření v určeném prostoru, kde na základě rozdílu elektrického náboje vznikající při průchodu IR záření optikou vyhodnocuje poplachový stav. Protože záření detekuje každé těleso s vyšší teplotou než nula, musí být pyročlen upraven pro citlivost rozsahu od 25 do 40 ° C. PIR detektory můžeme rozdělit podle typu vyhodnocování na analogové a digitální. Analogový PIR detektor využívá principu jednoduché elektroniky. V dnešní době se od analogových detektorů pomalu ustupuje a přechází se na digitální detektor. Digitální detektor ke své funkci využívá pokročilejší vyhodnocení IR záření z pyročlenu pomocí mikroprocesoru [29]

Na obr. 10. je znázorněn radiový PIR detektor pohybu OCTOPUS, který je možné připojit do linkového modulu. Tento detektor je vybaven kromě IR kanálu i vibračním snímačem, který zajistí střežení proti demontáži a změně nastavení. Po instalaci detektor předává do linkového výstupu informace typu jaký je stav poplachu, stav vibračního snímače a stav baterie. Tyto informace jsou do linkového výstupu zasílány každých 15 vteřin. [3]

Obr. 10. Rádiový detektor Octopus [22]

V tab. 8. můžeme vidět technickou specifikaci vybraného PIR detektoru.

Tab. 8. Technická specifikace PIR detektoru [22]

Napájení	Lithiová baterie AA3.6V/2Ah	Dosah ve volném prostranství	asi 150 m
Dosah čidla	12m	Pracovní teploty	5 °C až +45 °C
Odběr včetně vysílání	50 µA,	Hmotnost	85 g
Interval výměny baterie	více jak 1 rok	Rozměry	66 x 110 x 45mm
Pracovní kmitočty	2 v ISM pásmu 868MHz		

3.5.2 Ústředny PZTS

Ústředna PZTS je drátově nebo bezdrátově propojena s detektory, které vyhodnocují v reálném čase jejich stavy. Pokud ústředna PZTS zaznamená poplachový stav u některého z detektorů, vyhlásí poplach. Poplach může být signalizován akustickými zařízeními, mezi která patří sirény, majáky atd. Tyto ústředny PZTS mohou dále informace o vzniklém poplachu přenášet prostřednictvím komunikačního rozhraní připojeného do DPPC. Základní strukturu ústředny PZTS tvoří plošný spoj s mikroprocesorem, který obsahuje zdrojovou část se vstupy pro zapojení jednotlivých prvků s detektory. [3]

Hlavní funkce ústředny PZTS:

- slouží k ovládání signalizace, přenosového, zapisovacího a jiného zařízení,
- přijímá a vyhodnocuje výstupní elektrické signály z připojených detektorů,
- poskytuje detektorům napájení,
- uvádí celý systém do stavu střežení nebo do stavu klidu,
- umožňuje diagnostiku celého systému PZTS. [3]

Ústředny PZTS rozdělujeme na:

- smyčkové ústředny,

- ústředny s přímou adresací detektorů,
- ústředny smíšeného typu,
- bezdrátové ústředny. [3]

3.5.2.1 Ústředny PZTS s bezdrátovým přenosem

Tyto ústředny v dnešní době patří mezi nejmodernější zařízení. Komunikace probíhá v pásmu telemetrie 433 MHz s výkony okolo 10mW. Přenos signálu je většinou 8 bitový, kódovaný a adresa detektoru je 4 bitová. Vhodný návrh zaručuje nízký klidový odběr. Reálný dosah ve volném prostoru je okolo 150 metrů. Mezi výhody patří rychlá a snadná instalace, snadné rozšíření dalšími prvky a snadná konfigurace. [30]

Systém ústředny s bezdrátovým přenosem můžeme rozdělit:

- systémy s jednosměrnou komunikací (detektor je vysílač, ústředna přijímač),
- systémy s obousměrnou komunikací (každý prvek je vybaven vysílací i přijímací složkou). [30]

3.5.2.2 Poplachové přenosové zařízení a doplňkové zařízení

Poplachové přenosové zařízení slouží k přenosu poplachu z poplachového systému do vyhodnocovacího systému příjímacího centra. Může se také využít k přenosu informací nebo povelů z poplachového centra do poplachových systémů. [24]

Doplňkové ovládací zařízení jsou zařízení, která doplňují ovládání poplachového zabezpečovacího a tísňového systému. Zpravidla se jedná o klávesnice, dálkové ovladače, tlačítka, biometrické prvky, čtečky karet a klíčenky. [24]

3.5.3 Kamerový systém CCTV

Kamerový systém slouží pro přenos a záznam videosignálu. Kamerový systém se skládá z kamerové sestavy, zobrazovacího zařízení, záznamových zařízení popřípadě dalších přídavných zařízení. Hlavní podstatou CCTV (Closed Circuit Television – uzavřený televizní okruh) systému je zobrazení a zachycení obrazu k následnému vyhodnocení. Mezi nejdůležitější funkce tedy patří generování obrazu, přenos video signálu a řídících signálů (analýza obrazu – zobrazení a uchování záznamu). [24] Kamerové systému členíme na analogové, digitální nebo hybridní. [23]

Kamerové systémy jsou vhodné k propojení s různými druhy poplachových systémů např. PZTS, SKV a EPS, sloužící ke zvýšení bezpečnosti v daném objektu. Další výhodou těchto systémů je napojení na dohledová poplachová přijímací centra a vzdálená centra s analogovým nebo digitálním záznamem. Samostatná integrace kamerového systému se odkazuje na ČSN CLC/TS 80398. [23]

Kamerový systém můžeme rozdělit na snímání obrazu (kamera), obrazová informace a její přenos, kde samotný záznam z kamer může být analogový nebo digitální. Snímání kamery dělíme na černobílé, barevné nebo kombinované. [32]

Rozdělení kamer CCTV podle konstrukce:

- standartní kamera (tělo ve tvaru krabice),
- kompaktní kamera (dodáváno jako komplet s objektivem a držákem),
- dome kamera (kopulovitý tvar, určené na montáž stropu nebo stěny),
- otočná kamera (univerzální kamera, otáčivost 360 ˚),
- desková kamera (malá velikost, instalace pro skrytou montáž),
- speciální kamery (kamery zabudované do komponent jako jsou pera, brýle, klíčenky atd.). [32]

V poslední době je v Armádě České republiky kladen velký důraz na střežení objektů pomocí kamerových systémů. Mezi jedny z nejlepších komponent kamerových systémů a příslušenství bezesporu patří značky: GEUTEBRÜCK, INTELEX, DALLMEIER, BOSCH, DRESEARCH a BRIEFCAM.

3.5.4 Systém kontroly vstupu

Systém kontroly vstupu (dále jen SKV) poskytuje oprávněným osobám vstup nebo výstup ze zabezpečeného prostoru v objektu. Systém kontroly vstupu zároveň umožňuje zamítnutí vstupu nebo odchodu neoprávněným osobám. [33]

V objektech AČR má SKV velice významné uplatnění, které spočívá v kontrole přístupu osob do objektu nebo jeho částí. Na základě ověření identifikace je umožněn osobám přístup do konkrétních prostor. Nejpoužívanějším prostředkem pro identifikaci osoby v SKV slouží čipová karta, která se přikládá ke čtecímu zařízení. Čtecí zařízení přečte údaje na kartě, vyhodnotí v řídící jednotce a ta podle přístupových práv umožní přístup do požadovaných prostor. V oblastech ve kterých je vyžadována identifikace na základě nejvyšších

stupňů zabezpečení, se můžeme setkat s biometrickými čtečkami, které slouží k ověření osoby podle otisku prstu, rozpoznání tváře, očí atd.

Řídící jednotka vyhodnocuje celý chod systému. Je zde uložena kompletní databáze uživatelů, jejich přidělení a určení práv s přístupem do jednotlivých zabezpečených oblastí objektu AČR. Každý pokus o vstup i neoprávněný, je automaticky uložen v řídící jednotce pro pozdější analýzu. [34]

V tab. 9. jsou uvedeny příklady certifikovaných systémů kontroly vstupu schválené NBÚ.

Tab. 9. Příklady certifikovaných systémů kontroly vstupu

Identifikační číslo	Název výrobku	Popis výrobku	Kategorie použití	Počet bodů dle BS	Platnost
T3002/2016	Systém kontroly vstupu	APS 400, APS mini PLUS	2-4	Na realizaci systému SS6=2 až 4 body	19. 05. 2019
T3008/2017	Řídící jednotka s dveřním modulem	ADC - M	2-4	Na realizaci systému SS6=2 až 4 body	10. 08. 2020
T3005/2018	Systém kontroly vstupu	BioSmart	2-4	Na realizaci systému SS6=2 až 4 body	04. 10. 2021

3.6 Elektrická požární signalizace

Elektrická požární signalizace (dále jen EPS) je požárně bezpečnostní zařízení pracující na principu hlásičů požárů, které slouží k signalizaci vzniku požáru. EPS tedy skládá z hlásiče požáru, ústředny EPS a doplňujících zařízení. [3]

K příjmu signálů z těchto hlásičů požáru slouží ústředna EPS. Ústřednu obsluhuje stálá obsluha, která včasně reaguje na detekci hlášeného požáru. Mezi základní druhy EPS patří:

- jednostupňová EPS – obsahuje jednu nebo více hlavních ústředen, kde jsou připojeny samočinné a tlačítkové hlásiče požáru,
- vícestupňová EPS – obsahuje hlavní a vedlejší ústředny, kde jsou připojeny samočinné a tlačítkové hlásiče požáru,

- EPS s kolektivní adresací – možnost zjistit z které linky přišel signál, bohužel není zde možnost zjistit konkrétní hlásič, který detekci vyhodnotil,
- EPS s individuální adresací – umožňuje identifikaci stavu jednotlivých hlásičů. [35]

Mezi základní funkce elektrické požární signalizace patří:

- detekce požáru s cílem detekovat požár co nejdříve,
- signalizace požáru s cílem vyslání akustických nebo optických signálů pro osoby, které můžou být ohroženy,
- předání informace určeným osobám k zajištění zásahu,
- aktivace činnosti zařízení k zabránění následného šíření požáru. [23]

Podle spuštění můžeme rozdělit požární hlásiče na:

- tlačítkové hlásiče – mechanické spuštění tlačítka hlásiče,
- samočinné hlásiče – reakce na změnu fyzikálních vlastností, automatické spuštění. [3]

Dále můžeme hlásiče rozdělit na základě sledovaných parametrů, mezi které patří teplotní hlásiče vyhodnocující zvyšování teploty, kouřové hlásiče vyhodnocující požár při zjištění aerosolů, hlásiče vyzařování plamene reagující v určité části spektra a na speciální hlásiče. [3]

3.7 Dílčí závěr

Třetí kapitola vysvětluje rozdělení jednotlivých technických prostředků, které jsou nedílnou součástí k zajištění fyzické bezpečnosti v rezortu MO. Pro většinu těchto technických prostředků jsou od NBÚ vydány certifikáty, podle přílohy č. 1 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků.

Prostředky, sloužící k ochraně utajovaných informací v zabezpečených a jednacích oblastech objektu AČR, rozdělujeme zpravidla do několika skupin. Jedná se o mechanické zábranné prostředky, elektrická zámková zařízení a systémy kontroly vstupu, poplachové zabezpečovací a tísňové systémy, kamerové systémy a elektrickou požární signalizaci.

V dnešní době je nabídka těchto technických zařízení tak obsáhlá (funkce, konektivita, cena, tvar, atd.), proto doporučuji před samotným výběrem technického prostředku stanovit potřebná kritéria, na základě kterých budeme požadovaný prostředek vybírat.

4 MODEL HYPOTETICKÉ ZABEZPEČENÉ A JEDNACÍ OBLASTI V OBJEKTU AČR

V této kapitole je znázorněn fiktivní objekt AČR včetně hypoteticky zvoleného modelu. Model je vytvořen ve dvou variantách, kde je zpracováno zajištění fyzické bezpečnosti ZO a JO v objektu AČR. Vhodnější varianta je potom rozpracována do samotného „Projektu fyzické bezpečnosti“, který je vypracován v poslední kapitole diplomové práce.

Na základě nařízení VOC, velitel může nařídit zpracování návrhu více variant zabezpečení fyzické bezpečnosti pro stanovené ZO a JO v objektu AČR. Komise všechny varianty uvede do návrhu projektu fyzické bezpečnosti k dalšímu posouzení.

Návrh bezpečnostního projektu fyzické bezpečnosti“ (viz. Kapitola 2.1.1) se vypracuje vždy před finálním „Projektem fyzické bezpečnosti“, ZO nebo JO objektu AČR. Návrh bezpečnostního projektu fyzické bezpečnosti sestavuje komise, kterou určí velitel organizačního celku. Komise je odpovědná za zpracování všech podkladů, mezi které patří stanovy fyzických bezpečnostních opatření, různé varianty výstavby technických prostředků, včetně bodových ohodnocení ZO a JO s doloženými výkresovými dokumentacemi. Vypracovaný „Návrh bezpečnostního projektu“ se zasílá ke schválení, které schvaluje ředitel odboru bezpečnosti Ministerstva obrany. Po schválení tohoto „Návrhu bezpečnostního projektu“ se může zpracovat samostatný „Projekt fyzické bezpečnosti“, včetně všech náležitostí (viz. Kapitola 2.1.2).

Návrh bezpečnostního projektu fyzické bezpečnosti

Návrh projektu fyzické bezpečnosti nebude v této diplomové práci vypracován v plném znění, protože po schválení OB MO (v případě více variant - zvolení vhodnější varianty) je to obsahově autenticky shodný dokument, na základě kterého se zpracuje „Projekt fyzické bezpečnosti“ (viz. Kapitola 5).

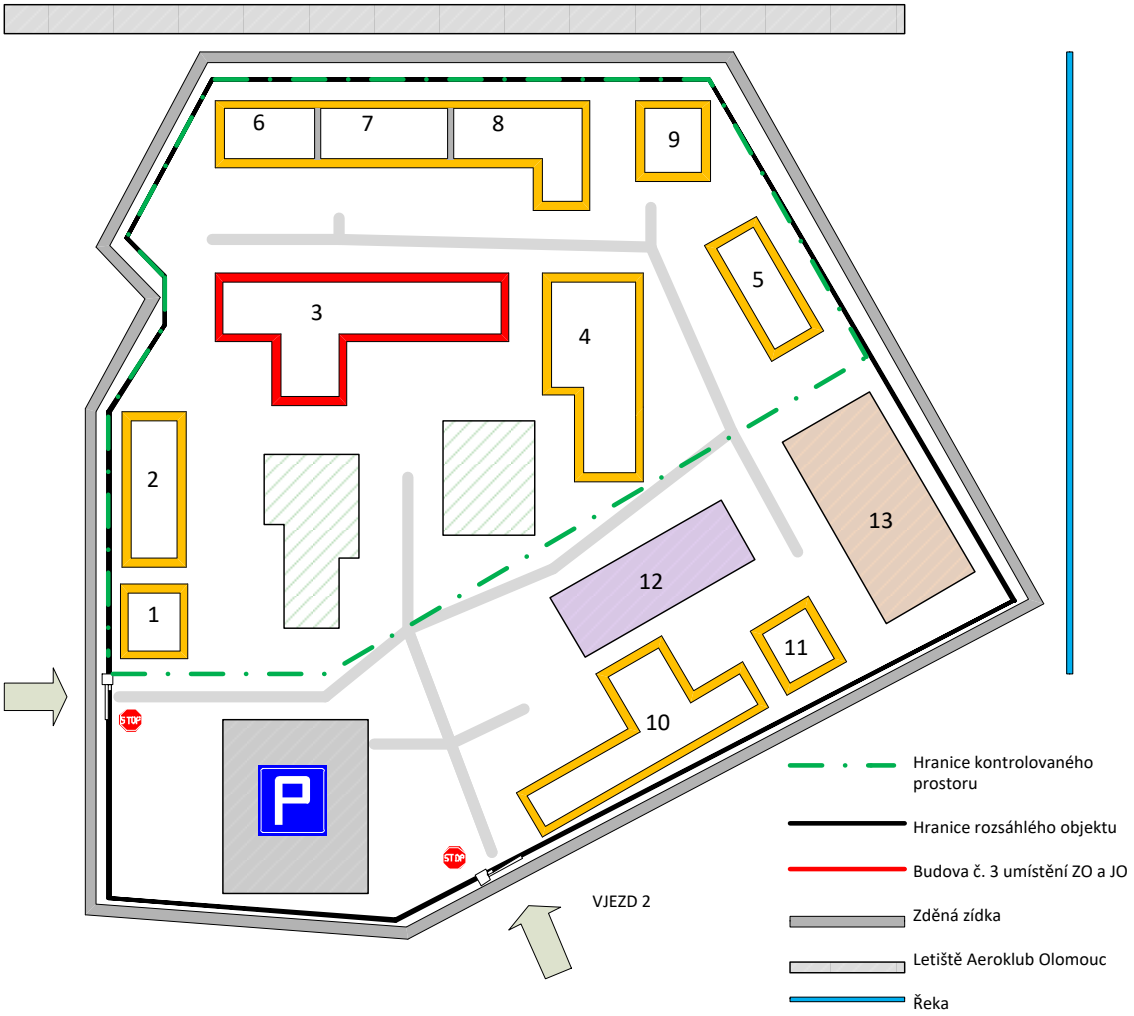
Z návrhu projektu fyzické bezpečnosti jsou zpracovány následující části:

- popis objektu Neředínských kasáren,
- požadavky velitele organizačního celku,
- hypotetický model zabezpečené a jednací oblasti v objektu AČR,
- návrh dvou variant k zajištění fyzické bezpečnosti v ZO a JO, výkresové schéma,
- vícekriteriální hodnocení, volba vhodnější varianty.

4.1 Charakteristika vojenského objektu

Jedná se o administrativní budovu č. 3 umístěnou v Neředínských kasárnách dislokovaných v Olomouci. Budova se skládá ze tří pater, kde jsou dvě nadzemní podlaží a jedno podzemní podlaží. Plášť budovy tvoří zdivo s betonovou omítkou, kde ve všech místnostech jsou nová plastová okna. Na vnějším plášti jsou instalovány hromosvody, okapové a svodové roury. Budova je po celkové rekonstrukci s novou fasádou. Střecha na budově je sedlová, nepochůzná. Do budovy je přístup z místní komunikace areálu hlavním vchodem a dvěma vjezdy.

Oddělení zájmové budovy od ostatních částí areálu je samostatná budova, která se nachází v západní okrajové části areálu Neředínských kasáren Olomouc (viz obrázek), vzdálené od celistvého oplocení 30 m. Budova č. 3 je obklopena přilehlými budovami č. 2, 4, 6, 7 a 8. Terén kolem objektu je rovinatý s travnatou a asfaltovou plochou.



Obr. 11. Fiktivní objekt Neředínských kasáren Olomouc

4.1.1 Nařízení velitele organizačního celku zájmového objektu AČR

Návrh možných variant k zajištění fyzické bezpečnosti zabezpečené nebo jednací oblasti vychází vždy z nařízení velitele organizačního celku nebo velitele rozsáhlého objektu na základě:

- analýzy stávajícího stavu fyzické bezpečnosti,
- stanovení potřeb zřízení nebo vybudování zabezpečených nebo jednacích oblastí dané kategorie nebo stupně utajení,
- návrh instalace technických prostředků do budovy a objektu v rezortu AČR,
- alokace finančních prostředků.

4.1.2 Požadavky velitele na zajištění fyzické bezpečnosti

Pro hypoteticky zvolený model jsou požadavky VOC na zabezpečení fyzické bezpečnosti u ZO a JO následující:

- stanovit hranice celého objektu kategorie „Vyhrazené“ v 1 patře budovy č. 3,
- určit zabezpečenou oblast kategorie „Tajné“ s možnosti využití jako úložna kryptografického materiálu a utajovaných informací,
- určit zabezpečenou oblast kategorie „Důvěrné“,
- určit jednací oblast k projednávání utajovaných informací stupně utajení „Tajné“,
- stanovit hranice objektu pro ZO kategorie Tajné, Důvěrné a JO stupně utajení Tajné, v případě možných stavebních úprav, vytvořit jednu společnou hranici objektu kategorie „Tajné“, kde budou umístěny tyto ZO a JO,
- navrhnout dvě možné varianty zabezpečení fyzické bezpečnosti u ZO a JO, zohlednit finanční prostředky, časovou náročnost, nutné stavební úpravy, technické prostředky a celkovou výhodnost,
- instalace zařízení proti aktivnímu a pasivnímu odposlechu do JO,
- celková kalkulace ceny stanovena do 1 100 000,- Kč včetně DPH,
- provést multikriteriální analýzu (na základě metody párového srovnání), k dalšímu zpracování zvolit vhodnější variantu,
- na základě schváleného návrhu projektu fyzické bezpečnosti vytvořit finální „Projekt fyzické bezpečnosti.“

V tab. 10. níže jsou upřesněny požadavky VOC na kategorii požadovaného stupně utajení a zařazení do tříd pro ZO a JO.

Tab. 10. Požadavky na ZO a JO, jejich kategorizace a zařazení do tříd

Název	"V"	"D"	"T"	"PT"	Tř. 1	Tř. 2	Míra rizika
ZO - 05	☐	☐	☑	☐	☐	☑	střední
ZO - 06	☐	☑	☐	☐	☑	☐	střední
JO - 01	☐	☐	☑	☐	☐	☐	střední

Určení technických prostředků

Veškeré požadavky na výstavbu technických prostředků pro zabezpečenou oblast kategorie Tajné, Důvěrné a jednací oblasti kategorie Tajné jsou uvedeny v tab. 11. níže. Dále tabulka obsahuje umístění ústředny a stanoviště stálého operačního dozorčí (SOD).

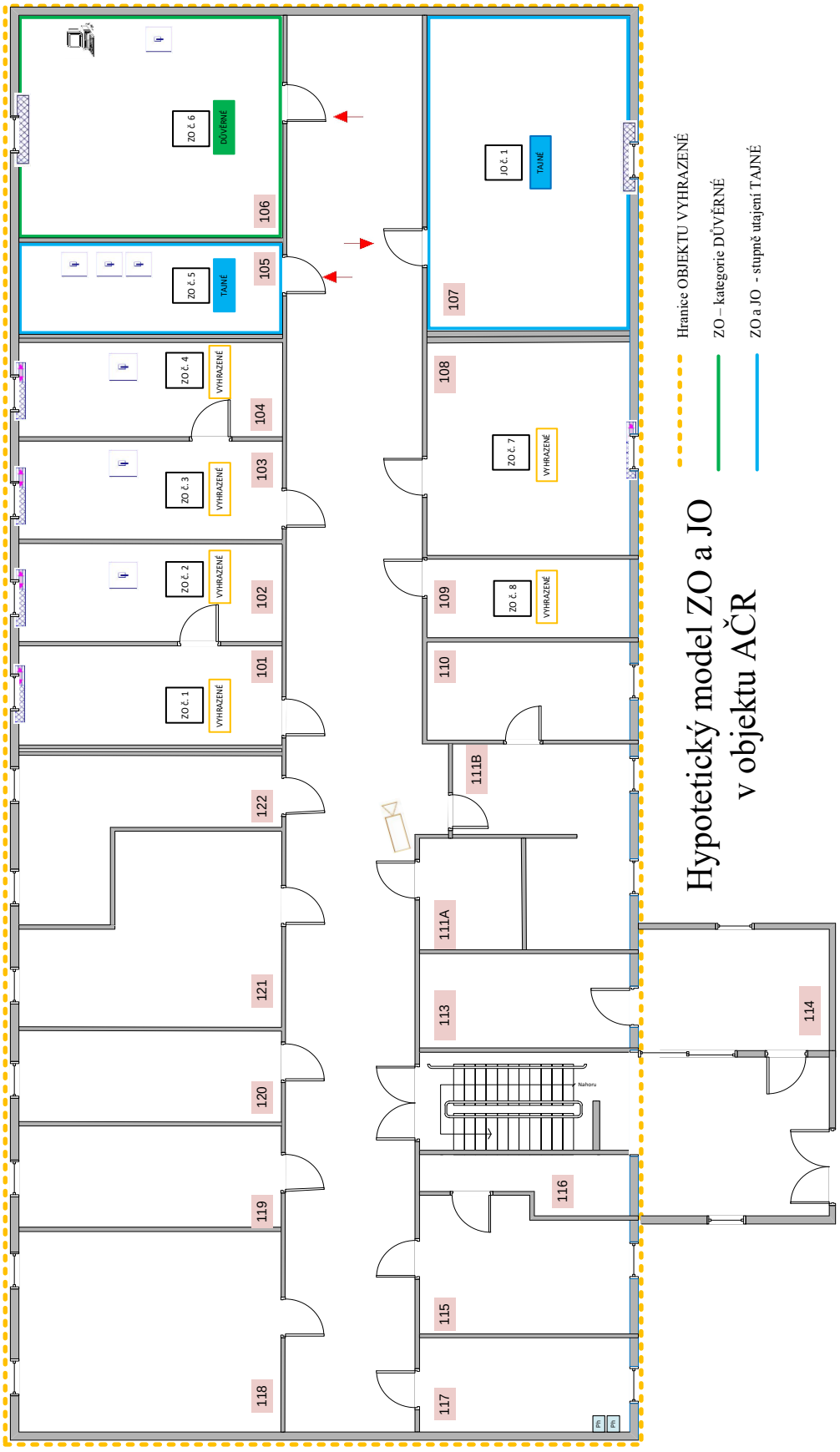
Tab. 11. Požadavky na výstavbu technických prostředků

Zab. oblast	Jed. oblast	Instalované systémy	Umístění ústředny	Ovládání ústředny	Místo vyvedení výstupního hlášení
☑	☑	EKV	Budova č. 3, 1. NP	správce tech. prostředků	stanoviště SOD budova č. 1
☑	☑	EPS u kategorie tajné	Budova č. 3, 1. NP		stanoviště SOD budova č. 1
☐	☑	CCTV	Budova č. 3, 1. NP		stanoviště SOD budova č. 1
☑	☑	PZTS	Budova č. 3, 1. NP	správce tech. prostředků	stanoviště SOD budova č. 1
☐	☑	NNI			
☐	☑	aktivní a pasivní odposlech			

4.2 Model hypotetické ZO a JO v objektu AČR

Navržený model objektu představuje budovu, která je v prvním patře budovy č. 3 se zabezpečenou oblastí kategorie Vyhrazené, Důvěrné, Tajné a jednou jednací oblastí stupně utajení Tajné. Hranice objektu je stanovena po celém obvodu budovy do stupně utajení „Vyhrazené“. Hranice vnořeného objektu ZO kategorie Důvěrné a Tajné a JO stupně utajení Tajné jsou stanoveny zvlášť, takže se jedná o více objektů v objektu. Pro splnění podmínek VOC k zajištění fyzické bezpečnosti těchto oblastí je vytvořen návrh dvou možných variant, které se reálně aplikují v objektech AČR.

Na obr. 12. je půdorys 1. patra, kde jsou znázorněny zabezpečené oblasti a jednací oblast s vyznačenou hranicí objektu kategorie Vyhrazené.



Obr. 12. Model hypotetické ZO a JO v objektu AČR

4.3 Návrh dvou variant k zajištění fyzické bezpečnosti ZO a JO

Na základě požadavků velitele organizačního celku jsou pro model navrženy dvě možné varianty, zajištěné fyzické bezpečnosti pro ZO kategorie Důvěrné, Tajné a JO stupně utajení Tajné umístěné ve stejném objektu.

Při vytváření návrhu těchto dvou variant byl kladen důraz především na stavební úpravy, instalaci technických prostředků a finanční kalkulaci. Níže popsané varianty se odlišují stavebními úpravami a instalací technických prostředků, které musí splnit bodové hodnoty pro konkrétní kategorii požadovaného stupně utajení.

Specifikace technických prostředků jsou navrhnuty v souladu s přílohou 1. vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků.

4.3.1 Návrh Varianty I

U 1. varianty byla navrhnuta stavební úprava, kde v objektu budovy mezi místnostmi 104 a 108 na pravé straně budovy, byla vystavena zděná příčka se vstupními dveřmi. Příčku bude tvořit zeď z plných cihel, nebo pórobetonových tvárnic tloušťky nejméně 200 mm. Do této zdi jsou zasazeny certifikované bezpečnostní dveře s elektromechanickým zámkem a vstupní klávesnicí. Na základě navržené příčky vznikl nový uzavřený bezpečnostní prostor, ve kterém jsou umístěny zabezpečené oblasti a jednací oblast. Pro celý tento prostor byla stanovena hranice objektu kategorie Tajné. Jedná se o vnoření dalšího objektu (objekt v objektu) s vymezenou hranicí daného stupně utajení, kde se nachází ZO-5 místnost 105 kategorie Tajné, sloužící jako úložna utajovaných informací a kryptografického materiálu, ZO-06 místnost 106 kategorie Důvěrné pro ukládání a zpracování UI a JO-01 místnost 107, sloužící k projednávání utajovaných informací do stupně utajení Tajné.

Výkresová dokumentace (včetně stavebních úprav) je znázorněna v DP - **Příloha č. 1.**

4.3.1.1 Instalace technických prostředků, finanční kalkulace

Požadavky na fyzickou bezpečnost u návrhu první varianty obnáší instalaci technických prostředků, které jsou zaneseny do tab. 12. V této tabulce je uvedena finanční kalkulace 1. varianty, včetně integračního HW a SW řešení.

Opatření fyzické bezpečnosti znázorňující instalaci technických prostředků je uvedena v DP ve výkresové dokumentaci **Příloha č. 2.**

Tab. 12. Varianta I - technické prostředky, cenová kalkulace

Technický prostředek	Bodové hodnocení	Počet kusů	Cena za kus (Kč)	Cena celkem (Kč)
Zabezpečená oblast kategorie Tajné (místnost 105)				
Bezpečnostní dveře	2	1	29 000	29 000
Uzamykací systém s kováním	1	1	12 000	12 000
Klávesnice paradox	1	1	8 000	8 000
Mobilní skříňový trezor EURON 2056 +kombinační zámek	3+2	2	27 000	54 000
Systém kontroly vstupu Granta	3	1	6 000	6 000
Ústředna Galaxy GD-520	3	1	7 600	7 600
PIR detektor CDX-DAM	2	1	2 200	2 200
Tísňový hlásič - ASITA MAS-TH	4	1	950	950
MG čidlo MAS-303	3	1	220	220
Kabeláž VL 06-6X0,22 (100m)		3	1000	3 000
Cena		122 970		
Zabezpečená oblast kategorie Důvěrné (místnost 106)				
Bezpečnostní dveře	2	1	29 000	29 000
Pevná mříž MS1	3	1	3 500	3 500
Detektor rozbití skla JA 110 B	2	1	850	850
Uzamykací systém s kováním	1	1	12 000	12 000
Klávesnice paradox	1	1	8 000	8 000
Úschovný objekt - dvoukřídlá skříň	2	2	15 500	31 000
Systém kontroly vstupu Granta	3	1	6 000	6 000
Ústředna Galaxy GD-520	3	1	7 600	7 600
PIR detektor CDX-DAM	2	1	2 200	2 200
MG čidlo MAS-303	2	2	220	440
Kabeláž VL 06-6X0,22 (100m)		5	1 000	5 000
Cena		105 590		
Jednací oblast kategorie Tajné (místnost 107)				
Bezpečnostní dveře	2	1	29 000	29 000
Pevná mříž MS1	3	1	3 500	3 500
Detektor rozbití skla JA 110 B	2	1	850	850
Uzamykací systém s kováním	2	1	12 000	12 000
Elektronický zámek BEFO 12 11		1	1 500	1 500
Klávesnice paradox	1	1	8 000	8 000
Sada pro detekci odposlechu SECUTEK OTP-02		1	14 000	14 000
Systém kontroly vstupu Granta	3	1	6 000	6 000
Tísňový hlásič - ASITA MAS-TH	4	1	950	950

Detektor hlásiče kouře CF 3000		1	1 500	1 500
Ústředna Galaxy GD-520	3	1	7 600	7 600
PIR detektor CDX-DAM	2	2	2 200	4 400
MG čidlo MAS-303	2	2	220	440
Kabeláž VL 06-6X0,22 (100m)		7	1 000	7 000
Faradayova klec		1	58 000	58 000
Cena		154 740		
Společná chodba, vstupní dveře				
Bezpečnostní dveře	2	1	29 000	29 000
Uzamykací systém s kováním	1	1	8 000	8 000
Systém kontroly vstupu APS-400	3	1	6 000	6 000
Ničič utajovaných informací Intimus	2	1	29 000	29 000
CCTV - ACTi TCM 1231		1	13 000	13 000
Výstavba zděné příčky		1	36 000	36 000
Cena		121 000		
Cena celkem (Kč)		504 300		

Jak vyplívá z výše uvedené tabulky, tak by celková cena za materiál měla být 504 300,- Kč bez DPH. Cena včetně 21% DPH pak bude 609 903,- Kč. Cena instalace a montáže zpravidla odpovídá 0,7 ceny materiálu. Celková cena instalačních a montážních prací by mohla být stanovena na 426 932,- Kč s DPH.

Finální cena za technické zabezpečení včetně instalačních a montážních prací by pak mohla být **1 036 835,- Kč s DPH.**

4.3.1.2 Bodové hodnocení – stanovení míry rizika

Bodové hodnocení a stanovená míra rizika pro ZO a JO jsou vypočteny v tabulkách, které jsou uvedeny v DP - **Příloha 6**, **Příloha 7 a Příloha 8**.

Na základě nařízení velitele jsou požadavky pro:

- ZO kategorie Tajné, střední míra rizika, která je minimálně 19 bodů;
- ZO kategorie Důvěrné, střední míra rizika, která je minimálně 14 bodů;
- JO kategorie Tajné, velká míra rizika, která je minimálně 16 bodů.

Výsledky získaných bodových hodnot VARIANTY I jsou dosazeny do tab. 13.

Tab. 13. Varianta I – výsledné bodové ohodnocení ZO a JO

ZABEZPEČENÁ OBLAST Tajné	**Míra rizika**			**DOSAŽENO**
	malá	střední	velká	22
Povinné : (S1) + (S2) + (S3)	8	9	10	
Povinné : (S4) + (S5) **	4	5	5	
Nepovinné : (S6)	4	5	5	
Celkový výsledek	**16**	**19**	**20**	
ZABEZPEČENÁ OBLAST Důvěrné	**Míra rizika**			**DOSAŽENO**
	malá	střední	velká	21
Povinné : (S1) + (S2) + (S3)	6	8	9	
Povinné : (S4) + (S5)	2	3	3	
Nepovinné : (S6)	3	3	4	
Celkový výsledek	**11**	**14**	**16**	
JEDNACÍ OBLAST Tajné	**Míra rizika**			**DOSAŽENO**
	malá	střední	velká	18
Povinné : (S2) + (S3)	5	5	6	
Povinné : (S4) + (S5) **	4	5	5	
Nepovinné : (S6)	4	5	5	
Celkový výsledek	**13**	**15**	**16**	

4.3.2 Návrh Varianty II

U 2. varianty byl stejně jako u 1. varianty vnořen do objektu další objekt, jen s tím rozdílem, že se jedná o dva objekty. První vnořený objekt má stanovenu hranici stupně utajení Tajné, kde je ZO kategorie Tajné a ZO kategorie Důvěrné. Druhý vnořený objekt má stanovenu hranici objektu rovněž do stupně utajení Tajné, kde je JO stupně utajení Tajné. Podle hypotetického modelu se stejně jako v první variantě v objektu nachází ZO-05 místnost č. 105 stupně utajení Tajné a ZO-06 místnost 106 stupně utajení Důvěrné. JO-01 místnost č. 107 stupně utajení Tajné. Pro požadovanou hranici obou vnořených objektů do stupně utajení „Tajné“ nebylo nutné provádět žádné rozsáhlé stavební úpravy.

Výkresová dokumentace navrhované VARIANTY II je znázorněna v DP - **Příloha č. 3.**

4.3.2.1 Instalace technických prostředků, finanční kalkulace

Stejně jako v 1. variantě, opatření fyzické bezpečnosti představující instalaci technických prostředků je uvedeno v DP, jako výkresová dokumentace - **Příloha č. 4.**

Jednotlivé položky použitých technických prostředků včetně cenové kalkulace za jednotlivé prostředky jsou uvedeny v tab. 14.

Tab. 14. Varianta II - technické prostředky, cenová kalkulace

Technický prostředek	Bodové hodnocení	Počet kusů	Cena za kus (Kč)	Cena celkem (Kč)
Zabezpečená oblast kategorie Tajné (místnost 105)				
Bezpečnostní dveře	2	1	40 000	40 000
Uzamykací systém s kováním	1	1	12 000	12 000
Klávesnice Paradox	1	1	8 000	8 000
Mobilní skříňový trezor EURON 2056 +kombinační zámek	3 + 2	2	27 000	54 000
Systém kontroly vstupu GOLNOD	2	1	5 000	5 000
Ústředna Asset 804 Z	3	1	9 000	9 000
PIR detektor CDX-DAM	2	1	2 200	2 200
Tísňový hlásič - ASITA MAS-TH	3	1	950	950
MG čidlo MAS-203	2	1	220	220
Kabeláž VL 06-6X0,22 (100m)		3	1000	3 000
Cena		134 370		
Zabezpečená oblast kategorie Důvěrné (místnost 106)				
Bezpečnostní dveře	2	1	35 000	35 000
Pevná mříž MS1	3	1	3 500	3 500
Detektor rozbití skla JA 110 B	2	1	850	850
Uzamykací systém s kováním	1	1	12 000	12 000
Klávesnice paradox	1	1	8 000	8 000
Úschovný objekt - dvoukřídlá skříň	2	2	15 500	31 000
Systém kontroly vstupu GOLNOD	2	1	5 000	5 000
Ústředna Asset 804 Z	3	1	9 000	9 000
PIR detektor CDX-DAM	2	1	2 200	2 200
MG čidlo MAS-203	2	2	220	440
Kabeláž VL 06-6X0,22 (100m)		5	1 000	5 000
Cena		111 990		
Jednací oblast kategorie Tajné (místnost 107)				
Bezpečnostní dveře	2	1	35 000	35 000
Pevná mříž MS1	3	1	3 500	3 500
Detektor rozbití skla JA 110 B	2	1	850	850
Uzamykací systém s kováním	1	1	12 000	12 000
Elektronický zámek BEFO 12 11		1	1 500	1 500
Klávesnice paradox	1	1	8 000	8 000
Sada pro detekci odposlechu SECUTEK OTP-02		1	14 000	14 000
Systém kontroly vstupu Golnod	2	1	5 000	5 000

Tísňový hlásič - Asita MAS-TH	3	1	950	950
Detektor hlásiče kouře CF 3000		1	1 500	1 500
Ústředna Asset 804 Z	3	1	9 000	9 000
Ničič utajovaných informací Intimus	2	1	37 000	37 000
PIR detektor CDX-DAM	2	2	2 200	4 400
MG čidlo MAS-203	2	2	220	440
Kabeláž VL 06-6X0,22 (100m)		7	1 000	7 000
Faradaova klec		1	75 000	75 000
Cena		215 140		
Společná chodba, vstupní dveře				
CCTV - ACTi TCM 1231		1	13 000	13 000
Cena		13 000		
Cena celkem (Kč)		474 500		

Podle dosazené tabulky by výsledná cena za materiál v druhé variantě měla být 474 500,- Kč bez DPH. Cena včetně 21% DPH pak bude 574 145,- Kč. Cena instalace a montáže zpravidla odpovídá 0,7 ceny materiálu. Celková cena instalačních a montážních prací u druhé navrhované varianty může být stanovena na 401 900,- Kč s DPH.

Finální cena druhé navrhované varianty za technické zabezpečení včetně instalačních a montážních prací by pak mohla být **976 045,- Kč s DPH.**

Výsledná finanční kalkulace obou variant:

- **navrhovaná VARIANTA I = 1 036 835,- Kč**
- **navrhovaná VARIANTA II = 976 045,- Kč**

U obou variant jsme tedy splnily požadavky na finanční prostředky, které neměly překročit limit 1 100 000,- Kč.

Na základě porovnání výsledků obou variant vypočtených z tabulek, můžeme vidět, že druhá varianta je tedy o 60 790,- Kč levnější než varianta první. V konečném hodnocení multikriteriální analýzy, sice nižší cena může být zvýhodněna, ale protože se především jedná, o co nejlepší návrh zabezpečení fyzické bezpečnosti, jsou převážně upřednostněny jiné faktory hodnocení.

4.3.2.2 *Bodové hodnocení – stanovení míry rizika*

Bodové hodnocení a stanovení míry rizika pro ZO a JO druhé varianty, je opět vypočítáno a dosazeno do tabulek v DP - **Příloha 9**, **Příloha 10 a Příloha 11**.

Výsledky získaných bodových hodnot VARIANTY II jsou dosazeny do tabulky níže.

Tab. 15. Varianta II – výsledné bodové ohodnocení ZO a JO

ZABEZPEČENÁ OBLAST Tajné	**Míra rizika**			**DOSAŽENO**
	malá	střední	velká	21
Povinné : (S1) + (S2) + (S3)	8	9	10	
Povinné : (S4) + (S5) **	4	5	5	
Nepovinné : (S6)	4	5	5	
Celkový výsledek	**16**	**19**	**20**	
ZABEZPEČENÁ OBLAST Důvěrné	**Míra rizika**			**DOSAŽENO**
	malá	střední	velká	20
Povinné : (S1) + (S2) + (S3)	6	8	9	
Povinné : (S4) + (S5)	2	3	3	
Nepovinné : (S6)	3	3	4	
Celkový výsledek	**11**	**14**	**16**	
JEDNACÍ OBLAST Tajné	**Míra rizika**			**DOSAŽENO**
	malá	střední	velká	17
Povinné : (S2) + (S3)	5	5	6	
Povinné : (S4) + (S5) **	4	5	5	
Nepovinné : (S6)	4	5	5	
Celkový výsledek	**13**	**15**	**16**	

4.4 Multikriteriální analýza

Multikriteriální analýzou nebo vícekriteriálním rozhodováním rozumíme vybrání jedné varianty z více možných variant na základě většího množství kritérií. Je tedy nutné mít seznam více možných variant, z nichž rozhodnutí vybíráme. Pokud máme k dispozici patřičná kritéria i seznam posuzovaných variant, je nutné detailně uvážit, jakou konečnou formu by rozhodnutí mělo mít.

Rozhodovací úlohy, kde se výsledky rozhodnutí posuzují na základě více kritérií, můžeme nazývat úlohami s vícekriteriálního rozhodování, nebo někdy také nazývané jako multikriteriální. [36]

4.4.1 Vícekriteriální hodnocení – metoda párového srovnání

Pro výběr vhodnější varianty jsem použil Fullerovu metodu, tzv. metodu párového srovnání kritérií. Jedná se o metodu, kde se používá pro odhad vah pouze informace, které ze dvou kritérií je při párovém srovnání důležitější. Postupně se tedy srovnávají každá dvě kritéria mezi sebou, kde počet srovnání můžeme stanovit ze vzorce: [36]

$$\mathrm{N} = \frac{k}{2} = \frac{k(k-1)}{2}$$

Jednotlivá kritéria jsou očíslovaná pořadovým číslem 1, 2, 3,…k. Kde následně vznikne trojúhelníkové schéma s dvojřádky, které vytvoří pořadová čísla uspořádána tak, aby se tyto vzniklé dvojice neopakovaly. Potom si vyberu pro mě důležitější kritérium, které si označím. Počet označení i-tého kritéria je značeno ni. Samotný výpočet váhy kritéria se potom provede podle vzorce: [36]

$$v_i = \frac{ni}{N} \qquad i = 1, 2, 3, \ldots\ldots, k$$

Kde: Vi = váha kritéria i

Ni ´= počet označení kritéria

I = číselné označení kritéria

N = počet provedených srovnání [36]

Na základě těchto hodnot jsem si stanovil kritéria, podle kterých budu posuzovat vhodnější variantu na základě číselného označení. Jednotlivé váhy jsem tedy stanovil na základě Fullerovy metody (pomocí trojúhelníku).

Stanovená kritéria:

1. Splnění požadavků VOC;
2. Komfort osob v ZO a JO;
3. Úroveň bezpečnosti v ZO a JO;
4. Instalované technické prostředky;
5. Finanční náročnost;
6. Navýšení kategorie stupně utajení.

V tab. 16. můžeme vidět (na základě výpočtů) dosazené hodnoty jednotlivých vah kritérií.

Tab. 16. Jednotlivé váhy kritérií – Fullerova metoda

Číselné pořadí	Kritérium	Váha kritéria
1	Splnění požadavků VOC	0, 133
2	Komfort osob v ZO a JO	0, 267
3	Úroveň bezpečnosti v ZO a JO	0, 067
4	Instalované technické prostředky	0, 333
5	Finanční náročnost	0, 133
6	Navýšení kategorie stupně utajení	0, 067

Pro názorný příklad uvádím výpočet kritéria čísla 1:

$$N = \binom{k}{2} = \frac{k*(k-1)}{2} = \frac{6*(6-1)}{2} = \frac{30}{2} = 15$$

$$v_1 = \frac{n_1}{N} = \frac{2}{15} = 0{,}133$$

Pro porovnání vhodnější navržené varianty I a varianty II jsem následně vytvořil tabulku, do které jsem dosadil komisí o počtu 3. hodnotitelů určené hodnoty (tab. 17.) pro míru vyhovování pro každou variantu. Jedná se tedy o vyhodnocení pomocí jednotlivých kritérií a jejich vah.

Stupnice byla stanovena od 1 do 5, kde větší číslo více vyhovuje danému kritériu. Po dosazení těchto hodnot, jsem jednotlivé hodnoty u obou variant vynásobil vahami jednotlivých kritérií, kde jsem získal výsledný srovnávací součin. Po celkovém sečtení všech srovnávacích součinů pro každou variantu jsem dostal výsledek konečné vhodnější varianty. Jedná se tedy o konečný výsledek porovnání obou variant. Vícekriteriální hodnocení je znázorněno v tab. 18.

Tab. 17. Průměr míry výhodnosti

Číselné pořadí	Kritérium	Hodnotitel 1		Hodnotitel 2		Hodnotitel 3		Průměr míry výhodnosti varianty	
		Var. 1.	Var. 2.	Var. 1.	Var. 2.	Var. 1.	Var. 2.	Varianta I	Varianta II
1	Splnění požadavků VOC	5	3	4	3	5	3	5	3
2	Komfort osob v ZO a JO	4	3	5	3	4	3	4	3
3	Úroveň bezpečnosti v ZO a JO	4	4	4	4	4	4	4	4
4	Instalované technické prostředky	5	3	4	3	4	3	4	3
5	Finanční náročnost	2	4	3	4	2	4	2	4
6	Navýšení kategorie stupně utajení	4	3	4	3	5	3	4	3

Tab. 18. Porovnání navrhovaných variant

Číselné pořadí	Kritérium	Váha kritéria	Míra výhodnosti varianty		Srovnávací součin	
			Varianta I	Varianta II	Varianta I	Varianta II
1	Splnění požadavků VOC	0, 133	5	3	0,665	0,399
2	Komfort osob v ZO a JO	0, 267	4	3	1,068	0,801
3	Úroveň bezpečnosti v ZO a JO	0, 067	4	4	0,268	0,268
4	Instalované technické prostředky	0, 333	4	3	1,332	0,999
5	Finanční náročnost	0, 133	2	4	0,266	0,532
6	Navýšení kategorie stupně utajení	0, 067	4	3	0,268	0,201
Výsledný součet srovnávacích součinů					3,867	3,2

Pro výpočet srovnávacího součinu uvádím názorný příklad na 1 kritériu:

Výpočet = váha kritéria x míra výhodnosti varianty

Srovnávací součin = 0, 133 x 5 = 0, 665

Na základě vícekriteriálního zhodnocení podle Fullerovy metody hodnocených kritérií, nám tabulka jasně vykazuje výhodnější VARIANTU I. Proto bude veliteli organizačního celku tato varianta předložena.

4.4.2 Výběr vhodnější varianty

Na základě původních stanovených požadavků VOC k zabezpečení fyzické bezpečnosti ZO a JO předkládá komise (včetně připomínek) doporučení vhodnější varianty. Pokud velitel odsouhlasí výběr zvolené varianty, tato varianta se zapracuje včetně bodového ohodnocení pro ZO a JO do „Návrhu projektu fyzické bezpečnosti“ a následně se předloží k posouzení odboru bezpečnosti Ministerstva obrany.

Pro výběr vhodnějšího zabezpečení fyzické bezpečnosti u hypotetického modelu je v tomto případě na základě vícekriteriálního hodnocení vhodnější **první varianta**, která bude dosazena do „Projektu fyzické bezpečnosti“ v další kapitole.

Další rozhodující faktory pro výběr 1. varianty:

- stanovení hranice společného objektu do stupně utajení „Tajné“, kde jsou zřízeny zabezpečené oblasti stupně utajení Tajné, Důvěrné a jednací oblasti stupně utajení „Tajné“;

- samostatný vchod do hranice objektu stupně utajení „Tajné“, kde je větší předpoklad zajištění fyzické bezpečnosti pro zabezpečené oblasti a jednací oblast;
- bodové ohodnocení je u obou variant nadlimitní, ale v případě ukončení platnosti certifikátu (ponížení bodových hodnot na základě shody), budou všechny místnosti v plné míře splňovat potřebné bodové ohodnocení, protože nevznikne žádná změna potřebné kategorie stupně utajení.

4.5 Dílčí závěr

Na základě nařízení velitele organizačního celku nebo velitele rozsáhlého objektu při nově vznikající zabezpečené nebo jednací oblasti určuje velitel komisi, která zpracuje Návrh projektu fyzické bezpečnosti včetně návrhu nejvhodnějších technických prostředků pro tyto oblasti v objektu AČR.

Do tohoto návrhu komise uvede jednu nebo více možných variant s různými prvky zabezpečení, které musí splnit požadavky ochrany utajovaných informací pro stanovenou kategorii stupně utajení v ZO nebo JO objektu AČR. Pro určení vhodnější varianty se především posuzuje bodové ohodnocení, stavební úpravy a ekonomická výhodnost.

K tomuto vyhodnocení nejvhodnější varianty se zpravidla využívá posuzování variant na základě „Multikriteriální analýzy“. V praxi to znamená, vybrání jedné varianty s více možných variant. Cílem multikriteriálního rozhodnutí je tedy vybrat nejvhodnější variantu (na základě vhodnějších kritérií), popřípadě seřadit varianty podle stupnice výhodnosti.

Moje posouzení vhodnější varianty u navrženého modelu ZO a JO v hypotetickém objektu AČR bylo provedeno podle Fullerovy metody, kde jsem porovnával dvě varianty na základě párového srovnání jednotlivých kritérií.

Pokud VOC nemá další připomínky, tato varianta se zapracuje do Návrhu projektu fyzické bezpečnosti a potom se zasílá k dalšímu posouzení na odbor bezpečnosti Ministerstva obrany, který vydá vyjádření s výsledným stanoviskem.

Po vydání podpisu ředitele OB MO se souhlasem Návrhu projektu fyzické bezpečnosti nechá velitel zpracovat (zpravidla) bezpečnostního manažera organizačního celku samotný Projekt fyzické bezpečnosti, který opět schvaluje velitel.

5 PROJEKT FYZICKÉ BEZPEČNOSTI

Podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti, ve znění pozdějších předpisů, musí každý subjekt nakládající s utajovanými informacemi, ať se jedná o civilní osobu nebo orgán státní správy splňovat opatření nezbytná k zabezpečení utajovaných informací, než začne ve svých prostorách projednávat či ukládat utajované informace.

Pro každého, kdo nakládá s utajovanými informacemi je povinnost vypracovat dokument, ve kterém je popsán soubor přijatých opatření k ochraně těchto utajovaných informací. Tento dokument se nazývá „Projekt fyzické bezpečnosti.“ Utajované informace v zabezpečených nebo jednacích oblastech se mohou projednávat či ukládat až po samotném schválení Projektu fyzické bezpečnosti.

Projekt fyzické bezpečnosti se všemi náležitostmi je vypracován níže, na základě všech zmíněných podkladů z předchozích kapitol praktické i teoretické části. Jedná se o Projekt fyzické bezpečnosti postavený na modelu hypotetického objektu AČR, kde cílem projektu jsou dvě zabezpečené oblasti a jedna jednací oblast.

Všechny specifické údaje ve vypracovaném „Projektu fyzické bezpečnosti“ jsou vymyšlené, takže se jedná o neutajovaný dokument, sloužící jako vzor pro vyhotovení reálného „Projektu fyzické bezpečnosti.“

Podle NVMO č. 77/2013 Věstníku, Fyzická bezpečnost v resortu Ministerstva obrany, stupeň utajení jednotlivých částí Projektu fyzické bezpečnosti navrhuje zpracovatel a schvaluje vedoucí organizačního celku.

Vyplněné údaje „Projektu fyzické bezpečnosti“ jsem zanesl do šablony vydané Ministerstvem obrany.

VZOR - NEUTAJOVANÝ DOKUMENT

VOJENSKÝ ÚTVAR		
	VÚ 1111 Olomouc **160 00 Olomouc 6 -**	

Čj. 15-325/2019/DP-3255

Počet listů:

Přílohy neutajované:

Projekt fyzické bezpečnosti

Objektu ktg. „Tajné“

Hypotetického centra – Olomouc

v areálu Neředínských kasáren, budova č. 3

Schválil	Dne	Podpis
hodnost, titul, jméno a příjmení pplk. Ing. Lukáš Vomáčka	. března 2019	

VZOR - NEUTAJOVANÝ DOKUMENT

Organizační celek:	**VÚ 1111 Olomouc**
Dokument:	**Projekt fyzické bezpečnosti**

PŘEHLED POUŽITÝCH ZKRATEK A POJMŮ

Tabulka **Použité zkratky**

Zkratka	Význam zkratky
BT	Bezpečnostní třída
CCTV	Speciální televizní systémy (angl. zkratka Closed Circuit TeleVision)
DET	Zařízení sloužící k vyhledávání nebezpečných látek nebo předmětů
OPE	Zařízení proti pasivnímu a aktivnímu odposlechu utajovaných informací
EPS	Elektrická požární signalizace
EZS	Elektrický zabezpečovací systém (angl. zkratka Intruder Alarm Systém)
MZP	Mechanické zábranné prostředky (systémy)
NNI	Zařízení fyzického ničení nosičů informací
NP	Nadzemní podlaží
PP	Podzemní podlaží
UI	Utajovaná informace
OUI	Ochrana utajovaných informací
PCO	Plut centralizované ochrany (angl. zkratka ARC – alarm receiving centre)
VP	Vojenská policie
PD	Projektová dokumentace
PIR	Pasivní infračervený detektor (čidlo prostorové)
SKV	Systém kontroly vstupu
ZO	Zabezpečená oblast
OC	Organizační celek
NV MO	Normativní výnos Ministerstva obrany
KIS	Komunikační informační systém

1 VYHODNOCENÍ RIZIK

Vyhodnotit rizika a stanovit jejich míru je povinen, v souladu s vyhláškou č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů a dále dle interního předpisu v souladu s č. 3, odst. 9, NV MO č. 77/2013 Věstníku, bezpečnostní manažer OC.

bezpečnostní manažer VÚ 1111 Olomouc, kpt. Ing. Pavel Kůzlátko

1.1 SPECIFIKACE AKTIV

1.1.1 Aktiva, stupeň utajení a druh utajovaných informací

U organizačního celku (dále jen „OC“) dochází k trvalému ukládání a manipulaci s utajovanými informacemi (dále jen „UI“).

Aktivy UI u organizačního celku jsou:

- informace, které jsou utajované **ANO**
- utajované dokumenty **ANO**
- utajované systémy **NE**
- technické zařízení **NE**

1.2 STUPEŇ UTAJOVANÝCH INFORMACÍ

U OC se budou vyskytovat, vznikat a zpracovávat UI těchto stupňů utajení:

- Vyhrazené **ANO**
- Důvěrné **ANO**
- Tajné **ANO**
- Přísně Tajné **NE**

Nejvyšší stupeň utajované informace **Tajné**

1.2.1 Druh utajovaných informací

U OC se budou vyskytovat utajované informace vlastní nebo poskytnuté zpravidla spolupracujícími subjekty v rámci resortu Ministerstva obrany.

Charakter poskytovaných a u OC vznikajících UI vyplývá z nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací, ve znění nařízení vlády č. 240/2008 Sb. U OC se jedná především o UI v oblasti působnosti Ministerstva obrany, tj. přílohy č. 5 k uvedenému nařízení vlády.

Identifikace stupňů UI a jejich množství

Stupeň utajení UI	V	D	T	PT	Celkem
Předpokládaný rozsah výskytu v následujícím roce	**6**	**2**	**2**	**0**	**10**

Četnost manipulace s UI

Manipulace s utajovanými informacemi v podmínkách OC: pravidelná

1.2.2 Místa výskytu utajovaných informací

Ukládání a manipulace

Utajované informace se trvale ukládají pouze v zabezpečených oblastech (dále také „ZO“). S utajovanými informacemi lze manipulovat:

- v zabezpečené oblasti ANO
- v objektu mimo zabezpečenou oblast ANO
- v odůvodněných případech s písemným souhlasem vedoucího organizačního celku, mimo „objekt“.

Manipulovat s UI lze pouze za podmínek, stanovených v § 24, odst. 5, zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti (dále také „zákon“). Utajované informace mohou zpracovávat nebo s nimi jinak manipulovat pouze ty osoby, které splňují podmínky přístupu k UI příslušného stupně utajení stanovené zákonem (dále také „oprávněné osoby“).

1.3 VYHODNOCENÍ ZAJÍMAVOSTI, DŮSLEDKY ZNIČENÍ, POŠKOZENÍ A VYZRAZENÍ UTAJOVANÝCH INFORMACÍ

1.3.1 Vyhodnocení zajímavosti utajovaných informací

Zájem o získání UI ukládaných u OC pro níže uvedené subjekty na základě specifik jednotlivých utajovaných informací:

- zajímavost pro cizí zpravodajské služby **Střední**
- zajímavost pro terorismus, včetně mezinárodního **Střední**
- zajímavost pro jiné skupiny (politické cíle apod.) **Střední**

1.3.2 Některé výchozí bezpečnostní údaje

Upřesnění některých bezpečnostních údajů vztahujících se k objektu:

- vzdálenost budovy („objektu“) od služebny VP nebo PČR **do 500 m**
- přípojka plynu v budově **NE**
- přípojka pitné nebo užitkové vody v budově **ANO**
- náhradní zdroj elektrické energie **ANO**
- zdroj úniku škodlivin v lokalitě budovy nebo areálu **NE**
- oblast zvýšené trestné činnosti (kriminality) **NE**
- nepřetržitý výkon fyzické ostrahy areálu **ANO**
- zátopová oblast vodního toku **NE**
- připojení EZS na dohledové a poplachové centrum **ANO**

2 STANOVENÍ JEDNOTLIVÝCH HROZEB, ZRANITELNOSTI UI A JEJICH VYHODNOCENÍ

2.1 VYZRAZENÍ UI OPRÁVNĚNÝMI OSOBAMI

Úmyslné nebo neúmyslné porušení povinností oprávněných osob vyplývajících ze zákona a jeho prováděcích vyhlášek, zejména vyhlášky č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací, ve znění pozdějších předpisů, a dále z vnitřních předpisů MO souvisejících s ochranou UI.
Jedná se především o nedůsledné provádění kontrol z důvodu neznalosti nebo časové tísně, seznámení s informací osobu, které nemá OFO pro stejný stupeň utajení nebo vyšší. Dále nedodržení stanovených postupů při manipulaci s UI, sdělení UI příbuzným a známým. (pod vlivem drog, alkoholu atd.).

Bezpečnostním manažerem OC byla na základě vyhodnocení hrozeb a zranitelnosti utajovaných informací stanovena míra rizika na **malé riziko**

2.2 MANIPULACE S UI NEOPRÁVNĚNÝMI OSOBAMI

Zpravidla se jedná o náhodné seznámení se s UI nebo trestnou činnost (vloupání do objektu a ZO, přepadení oprávněné osoby, která s UI manipuluje, přenáší a přepravuje ji mimo „objekt“, nálezem utajovaného dokumentu apod.)

Jedná se o hrozbu, která představuje možnost seznámení se neoprávněných osob s UI bez známek porušení povinností poučených osob. Hrozba je zpravidla představována formou násilné trestné činnosti. Jedná se zpravidla o krádež utajovaných předmětů, jako jsou PC komponenty (pevné disky a digitální záznamové média), popřípadě jejich záměna.
Mezi další možné seznámení s UI může dojít při zanedbání povinností příslušníků při plnění služebních úkolů nebo jednáních s cizími příslušníky.

Bezpečnostním manažerem OC byla na základě vyhodnocení hrozeb a zranitelnosti utajovaných informací stanovena míra rizika na **střední riziko**

2.3 POŠKOZENÍ UI ŽIVELNÍ POHROMOU

Zahrnuje možnosti poškození nebo zničení UI živelní pohromou, zemětřesením, povodní, bleskem, požárem, vichřicí nebo omezení možnosti chránit UI v případě jejího vzniku, kdy se na odstraňování následků působení přírodních vlivů budou podílet nepovolané osoby, a dojde k neoprávněnému vniknutí do skříní zařízení s následným narušením provozu stálé spojovací sítě.

Bezpečnostním manažerem OC byla na základě vyhodnocení hrozeb a zranitelnosti utajovaných informací stanovena míra rizika na **malé riziko**

2.4 POŠKOZENÍ UI PRŮMYSLOVOU NEBO TECH. HAVÁRIÍ

Zahrnuje možnosti poškození nebo zničení UI průmyslovou a technologickou havárií (např. únikem nebezpečných chemických látek a přípravků ze stacionárních zdrojů, při jejich přepravě; únikem vody následkem poruchy na potrubí apod.) nebo omezení možnosti chránit UI za této situace.

Bezpečnostním manažerem OC byla na základě vyhodnocení hrozeb a zranitelnosti utajovaných informací stanovena míra rizika na **malé riziko**

2.5 ZTRÁTA UI NÁSLEDKEM TERORISTICKÉHO ÚTOKU

Možnost ztráty UI nebo omezení možnosti je chránit při teroristickém útoku jednotlivce nebo skupiny. Možností je dlouhodobé přerušení dodávek elektrické energie, výhružky o umístění výbušnin.

Bezpečnostním manažerem OC byla na základě vyhodnocení hrozeb a zranitelnosti utajovaných informací stanovena míra rizika na **malé riziko**

2.6 VYZRAZENÍ UI PASIVNÍM ODPOSLECHEM NEBO NASAZENÍM OPERATIVNÍ TECHNIKY

Získání UI odposlechem, nasazením operativní techniky. Pro zhodnocení hrozby je rozhodující skutečnost, zda UI mají charakter informací, které lze odposlechem získat a zda jsou z pohledu nasazení operativní techniky zajímavé. Zvláště v prostorech JO a pracovnách nakládající s IKS.

Bezpečnostním manažerem OC byla na základě vyhodnocení hrozeb a zranitelnosti utajovaných informací stanovena míra rizika na **střední riziko**

2.7 VYZRAZENÍ NEBO ZTRÁTA UI Z INFORMAČNÍHO SYSTÉMU

Možnosti úniku UI zpracovávaných v elektronické podobě, zničení nebo poškození dat charakteru UI, podmíněné snadným kopírováním nebo neoprávněným vstupem do IS nebo počítačové sítě.
Jedná se především o odesílání UI nezabezpečeným - nešifrovaným spojením, dále neoprávněné zpracování UI v nezabezpečených sítích (stínění atd.) a zavirovanými nosiči UI. Osoby nakládající s UI musí být pravidelně školeni, kde předmětem školení je používání internetu, mobilních telefonů a přenosných záznamových médií. Jsou seznámeni se zákazem zpracování UI na necertifikovaných prostředcích nebo jiných záznamových médiích.

Bezpečnostním manažerem OC byla na základě vyhodnocení hrozeb a zranitelnosti utajovaných informací stanovena míra rizika na **střední riziko**

2.8 POŠKOZENÍ (ZNIČENÍ) UI V OSTATNÍCH PŘÍPADECH

Možnosti ztráty, zcizení, poškození nebo zničení UI např. při ohrožení státu (válečné nebezpečí, útok cizí moci, snaha o destrukci demokratického zřízení vnitřními silami), při změně politické situace apod.

Bezpečnostním manažerem OC byla na základě vyhodnocení hrozeb a zranitelnosti utajovaných informací stanovena míra rizika na **malé riziko**

2.9 STANOVENÍ CELKOVÉ MÍRY RIZIKA

Při vyhodnocení rizik je zohledněn zejména druh, stupeň a rozsah UI, specifika manipulace s UI a jejich zranitelnost vůči specifikovaným hrozbám.

V návaznosti na popis hrozeb a vyhodnocení závažnosti hrozeb je míra jednotlivých rizik uvedena v následující tabulce:

Nejvyšší stupeň UI	**Tajné**
Předpokládané množství UI	**30**
Četnost manipulace	**pravidelná**
Vyzrazení UI oprávněnými osobami	**malé riziko**
Manipulace s UI neoprávněnými osobami	**střední riziko**
Poškození (zničení) UI živelní pohromou	**malé riziko**

Poškození (zničení) UI průmyslovou nebo technologickou havárií	**malé riziko**
Ztráta UI následkem teroristického útoku	**malé riziko**
Vyzrazení UI pasivním odposlechem nebo nasazením operativní techniky	**střední riziko**
Vyzrazení nebo ztráta UI z informačního systému	**střední riziko**
Poškození (zničení) UI v ostatních případech	**malé riziko**

Na základě zhodnocení jednotlivých rizik stanovil bezpečnostní manažer OC pro tento objekt celkovou míru rizika **střední riziko**

3 ÚVODNÍ USTANOVENÍ, AREÁL A BUDOVA

Vedoucí organizačního celku
plk. Ing. Lukáš Vomáčka
velitel

Neředín - kasárna, 772 00 Olomouc

3.1 POPIS AREÁLU

Jedná se o areál Neředínských kasáren v Olomouci, kde v těsném sousedství na severní straně je letiště Aeroklubu Olomouc. Z hlediska bezpečnosti je areál bezpečný, samostatně stojící, mimo městskou zástavbu. Do současné doby nebyly zaznamenány snahy o narušení hranic areálu kasáren. Do areálu kasáren jsou dva vjezdy a jeden vstup, které jsou trvale střeženy příslušníky ochranné směny VLS ČR, s. p.. Vjezd č. 1 a vstup je určen jako hlavní a vjezd č. 2 je určen jako záložní pro nouzové opuštění kasáren a zároveň využíván v pracovní dny ráno pro vjezd soukromých motorových vozidel zaměstnanců k parkování v prostoru Provozního střediska u budovy č. 10. Uvnitř areálu je komunikace s asfaltovým povrchem. Venkovní prostor areálu je oplocen po celém obvodu plným, celistvým oplocením. Oplocení je zčásti zděné, z části z ocelového plechu s betonovou podezdívkou. Oplocení poskytuje překážku proti pokusu o překonání lezením pod úhlem 45 stupňů. Dovnitř areálu je na vzpěrách natažen ve dvou řadách ostnatý drát. Okolo areálu je mírně zvlněný terén (pole, louky) obhospodařovaný cizími subjekty, podél východního oplocení vede vodoteč, která ústí do řeky Morava vzdálené cca 800 m. Kolem vodoteče je řídce náletový prostor.

Oplocení	ANO		Zčásti zděné a částečně z ocelového plechu s betonovou podezdívkou vysoké 2m.Vnitřně do areále pod úhlem 45 stupňů natažen ve dvou řadách ostnatý drát.		
Ostraha	ANO		Budova č. 001, 1. NP místnost č 101		
PCO v areálu	NE		Budova č. 002, 1 NP místnost 205. Prostor stálého operačního dozorčí rozsáhlého objektu kasáren.		
Počet vstupů	1	**Počet vjezdů**	2	**Počet budov**	13

Cizí subjekty v areálu

Název subjektu	Zaměření činnosti a umístění v areálu
Haryservis	**úklidová činnost**
Volareza Olomouc	**vaření obědů, prodej potravin - arma**

3.2 BUDOVA

Číslo budovy v centrální evidence (CE)	1
Název budovy	Štáb komunikačního centra – Neředínské kasárna Olomouc
Využití budovy	Administrativní budova

Bližší popis okolí budovy	Budova se skládá ze tří pater, kde jsou dvě nadzemní podlaží a jedno podzemní podlaží. Plášť budovy tvoří zdivo s betonovou omítkou, kde ve všech místnostech jsou nová plastová okna. Na vnějším plášti jsou instalovány hromosvody, okapové a svodové roury. Budova je po celkové rekonstrukci s novou fasádou. Střecha na budově je sedlová nepochůzná. Do budovy je přístup z místní komunikace areálu hlavním vchodem a dvěma vjezdy. Oddělení zájmové budovy od ostatních částí areálu je samostatná budova, která se nachází v západní okrajové části areálu Neředínských kasáren Olomouc, vzdálené od celistvého oplocení 30 m. Budova č. 3 je obklopena přilehlými budovami č. 2, 4, 6, 7 a 8. Terén kolem objektu je rovinatý s travnatou a asfaltovou plochou.		
Počet NP	**3**	**Počet PP**	**1**
Počet schodišť	**1**	**Počet výtahů**	**0**
Počet vstupu	**3**	**Počet vjezdů**	**0**
Konstrukce a stav budovy v době popisu:			
Stavební konstrukce	**Zděná**	**Stáří - stav**	**Moderní**
Střecha	**Nepochůzná**	**Okna budovy**	**Plast**
EZS	**ANO**	**PCO v budově**	**NE**
Cizí subjekty v budově	**NE**		
Vztah budovy k hranici „objektu“		**Hranice budovy tvoří částečně hranici "objektu"**	

3.3 „OBJEKT“, STANOVENÍ HRANICE, BEZPEČNOSTNÍ OPATŘENÍ

Popis „objektu“	
Umístění objektu	Budova č. 003, 1. NP, místnosti č. 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117,

	118, 119, 120, 121, 122.		
Popis hranice „objektu“	Tvoří ji částečně vnější část budovy.		
Nejvyšší kategorie UI v „objektu“		**Tajné**	
Režim návštěv „objektu“ (dle statě č. 3 přílohy č. 1 k vyhlášce)		**návštěvy s doprovodem**	
Návštěvy vstupují do kasáren přes dozorčího vchodu, který je zaznamená do knihy návštěv. Dále jsou doprovázeny navštívenou osobou. Vstup osob a vjezd vozidel je stanoven v Organizačním rozkaze velitele posádky rozsáhlého objektu.			
Ostraha u „objektu“ (dle statě č. 5 přílohy č. 1 k vyhlášce)		**více - zaměstnanci resortu a civilní agentura**	
Ostrahu objektu tvoří státní firma Vojenské lesy a statky ČR, s. p, kterou řídí a dohleduje (prostřednictvím EZS) stálý operační dozorčí Vojenské policie a jeho pomocník. Povinnosti ostrahy jsou zpracovány ve Směrnicích pro výkon služby.			
Vymezení hranice objektu v budově			
Podlaží	**1**	**Místnost číslo:**	**101 - 122**
Minimální síla obvodových zdí	**350 mm**	**Minimální síla vnitřních zdí**	**150 mm**
Minimální síla podlahové konstrukce	**350 mm**	**Minimální síla stropní (střešní) konstrukce**	**300 mm**
Stanoviště ostrahy	**u objektu**	**Počet stanovišť FO**	**1**
Počet vstupů do „objektu“	**1**	**Počet vjezdů**	**2**
„Objekt“ je typu (dle statě č. 3 a 6 přílohy č. 1 k vyhlášce)		**typ 3**	
Kontrola vstupu do „objektu“		**uzamykatelnou mechanickou zábranou**	
Stěny, podlahy a stropy jsou pevné konstrukce z cihel. Průlezné otvory jsou zabezpečeny MZP. Konstrukce areálu tvoří částečně hranici objektu.			

Vymezení hranice objektu perimetrem					
Fyzické bariéry (dle bodu 6.1 přílohy č. 1 k vyhlášce)			**nejsou realizovány**		
Zde můžete uvést bližší informace k výše uvedenému					
Kontrola vstupu ve všech přístupových bodech perimetru (dle bodu 6.2 přílohy č. 1 k vyhlášce)			**je realizována**		
Namátkové vstupní a výstupní prohlídky			**jsou realizovány**		
Perimetrický detekční systém (PDS) (dle bodu 6.3 přílohy č. 1 k vyhlášce)			**není realizován**		
Objekt je střežen fyzickou ostrahou 24/7 a kamerovým systémem, který je dohledován u dozorčího posádky. Klíče od objektu jsou ukládány u ostrahy. Vstup do objektu je zabezpečen SKV.					
Bezpečnostní osvětlení perimetru (dle bodu 6.4 přílohy č. 1 k vyhlášce)			**je realizováno**		
Zde můžete uvést bližší informace k výše uvedenému					
Speciální televizní systém na perimetru (dle bodu 6.5 přílohy č. 1 k vyhlášce)			**je realizován**		
Přehled použitých technických prostředků					
MZS	**ANO**	**EZS**	**ANO**	**PCO**	**ANO**
CCTV	**ANO**	**SKV**	**ANO**	**EPS**	**ANO**
DET	**NE**		**OPE**	**NE**	
Zařízení fyzického ničení nosičů informací (NNI)			**ANO**	**typ 4**	
NNI je umístěn na chodbě v zabezpečené hranici objektu kategorie Tajné.					

4 ZABEZPEČENÉ A JEDNACÍ OBLASTI V OBJEKTU

V „objektu“ se nacházejí zabezpečené a jednací oblasti. Každá tato oblast v objektu je popsána, včetně celkového bodového ohodnocení dané oblasti. Hranice vnořeného objektu je stanovena na kategorii Tajné.

Číslo zabezpečené oblasti	Kategorie zabezpečené oblasti
ZO č. T-05	**Tajné**
ZO č. D-06	**Důvěrné**
JO č. T-01	**Tajné**

4.1 ZABEZPEČENÉ OBLASTI A JEDNACÍ OBLAST

4.1.1 Zabezpečená oblast T-05

Kategorie	Tajné	**Třída**	II.
Zabezpečená oblast je označena:T-05			
místnost č. 105, 1.NP, budova č. 03			
Minimální síla obvodových zdí	350 mm	**Minimální síla vnitřních zdí**	150 mm
Minimální síla podlahové konstrukce	350 mm	**Minimální síla stropní konstrukce**	300 mm
Počet vstupů	1	**Počet oken**	0
Účel místnosti	**Úložna utajovaných informací**		
Výška oken nad terénem			méně než 5,5 m

4.1.2 Zabezpečená oblast D-06

Kategorie	Důvěrné	**Třída**	I.
Zabezpečená oblast je označena:D-06			
místnost č. 106, 1.NP, budova č. 03			

Minimální síla obvodových zdí	350 mm	**Minimální síla vnitřních zdí**	150 mm
Minimální síla podlahové konstrukce	350 mm	**Minimální síla stropní konstrukce**	300 mm
Počet vstupů	1	**Počet oken**	1
Účel místnosti	**Pracoviště s KIS**		
Výška oken nad terénem			méně než 5,5 m

4.1.3 Jednací oblast T-01

Nejvyšší stupeň utajení projednávaných UI			Tajné
Jednací oblast je označena:T-01			
místnost č. 108, 1.NP, budova č. 03			
Minimální síla obvodových zdí	350 mm	**Minimální síla vnitřních zdí**	150 mm
Minimální síla podlahové konstrukce	350 mm	**Minimální síla stropní konstrukce**	300 mm
Počet vstupů	1	**Počet oken**	1
Účel místnosti	**Jednací oblast**		
Výška oken nad terénem			méně než 5,5 m

4.2 SPECIFIKA BODOVÉHO ODHODNOCENÍ U ZO A JO

4.2.1 Úschovný objekt

ZO -05 Typ: typ 3 Bodové hodnocení: SS1 = 3 body

ZO -06 Typ: typ 2 Bodové hodnocení: SS1 = 2 body

V souladu s ČSN EN 1143-1+A1 musí být úschovný objekt typu 3 osazen zámkem minimálně třídy A podle ČSN EN 1300+A1 (zámek typu 2, bod 1.2.3. přílohy).[11]

ZO/KAT.	Název dle certifikátu	Číslo cert.	Platnost	Body	Listů cert.
ZO-05/T	Mobilní skříňový trezor EURON 2056	T0235/2019	31. 12. 2023	3	
ZO-06/D	Dvoukřídlá archivační skříň typ ASV 1	T0158/2019	31. 12. 2021	2	

4.2.2 Zámek úschovného objektu u ZO-05 a ZO-06

Pro ZO-05, ZO-06, jsou stanoveny bodové hodnoty:

Typ: typ 2 Bodové hodnocení: SS2 = 2 body

Zámek typu 2 je certifikovaný NBÚ v rámci certifikace úschovného objektu a splňuje požadavky bezpečnostní třídy A podle ČSN EN 1300+A1.

4.2.3 Zabezpečené oblasti a jednací oblast

Pro ZO-05, ZO-06 a JO-01, jsou stejné bodové hodnoty, na základě přílohy č. 1 k vyhlášce č. 528/2005 Sb., ve znění vyhlášky č. 204/2016 Sb.

Typ: typ 2 Bodové hodnocení: SS3 = 2 body

ZO/KAT.	Název dle certifikátu	Číslo cert.	Platnost	Body	Listů cert.
ZO-05/T ZO-06/D JO-01/T	Bezpečnostní dveře - Sapeli	T0020/2017	26. 01. 2020	2	
ZO-05/T JO-01/T	Pevná mříž MS-1	T0070/2018	15. 11. 2021	3	

4.2.4 Uzamykací systém zabezpečených oblastí a jednací oblasti

Pro ZO-05, ZO-06, jsou stanoveny bodové hodnoty:

Typ: typ 1 Bodové hodnocení: SS4 = 2 body

Uzamykací systém typu 1 je certifikovaný NBÚ. Uzamykací systém a jeho komponenty musí splňovat požadavky bezpečnostní třídy RC 2 podle ČSN EN 1627.

Pro JO-01, jsou stanoveny bodové hodnoty:

Typ: typ 2 Bodové hodnocení: SS4 = 2 body

Uzamykací systém typu 2 je certifikovaný NBÚ. Uzamykací systém a jeho komponenty musí splňovat požadavky bezpečnostní třídy RC 3 podle ČSN EN 1627.

4.2.5 Systém kontroly vstupu

Pro ZO-05, ZO-06 a JO-01, jsou stejné bodové hodnoty, na základě přílohy č. 1 k vyhlášce č. 528/2005 Sb., ve znění vyhlášky č. 204/2016 Sb.

Typ: typ 3 Bodové hodnocení: SS6 = 3 body

ZO/KAT.	Název dle certifikátu	Číslo cert.	Platnost	Body	Listů cert.
Tajné	Systém kontroly vstupu GRANTA	T3002/2017	12. 01. 2020	3	

4.2.6 Režim návštěv

Typ: s doprovodem Bodové hodnocení: SS7 = 3 body

Návštěvy musí být doprovázeny po celou dobu pobytu v objektu. Dále musí být vedena evidence údajů o návštěvách, jenž obsahuje identifikaci návštěv, doprovázejících osob a časové údaje o tom, kdy byla návštěva vykonána.

4.2.7 Ostraha

Typ: typ 3 Bodové hodnocení: SS8 = 3 body

Ostrahu vykonávají zaměstnanci bezpečnostní ochranné služby a příslušníci ozbrojených sil. Intervaly obchůzek jsou specifikovány ve směrnicích u stálého operačního dozorčího a ostrahy objektu. Na stanovišti ostrahy v době obchůzky, musí být přítomna nejméně jedna osoba pro výkon ostrahy.

4.2.8 Zařízení EZS

Pro ZO-05, ZO-06 a JO-01, jsou stejné bodové hodnoty, na základě přílohy č. 1 k vyhlášce č. 528/2005 Sb., ve znění vyhlášky č. 204/2016 Sb.

Typ: typ 3 Bodové hodnocení: SS91 = 3 body

Zařízení EZS typu 3 musí být certifikováno NBÚ. Dále musí plnit požadavky podle ČSN EN 50131-1 ed. 2 pro stupeň zabezpečení 3 střední až vysoké riziko.

ZO/KAT.	Název dle certifikátu	Číslo cert.	Platnost	Body	Listů cert.
ZO-05/T ZO-06/D JO-01/T	Ústředna Galaxy GD-520	T1086/2018	15. 11. 2021	3	
ZO-05/T ZO-06/D JO-01/T	Duální detektor CDX - DAM	T1013/2018	22. 03. 2021	3	
ZO-05/T JO-01/T	Tísňový hlásič - ASITA MAS-TH	T1023/2017	11. 04. 2020	4	
ZO-05/T ZO-06/D JO-01/T	MG čidlo MAS-303	T1020/2017	25. 04. 2020	3	
ZO-06/D JO-01/T	Detektor rozbití skla JA 110 B	T1013/2019	21. 04. 2021	2	
JO-01/T	Sada pro detekci odposlechu SECUTEK OTP-02				
JO-01/T	Detektor hlásiče kouře CF 3000				

4.2.9 Instalace zařízení EZS

Pro ZO-05, ZO-06 a JO-01, jsou stejné bodové hodnoty, na základě přílohy č. 1 k vyhlášce č. 528/2005 Sb., ve znění vyhlášky č. 204/2016 Sb.

Typ: typ 3 Bodové hodnocení: SS92 = 3 body

Instalace typu 3 je realizována v rozsahu: prostorové ochrany, plášťové ochrany a tísňového systému nebo CCTV snímající nepřetržitě průlezné otvory.

4.2.10 Fyzické bariéry

Typ: nehodnoceno Bodové hodnocení: SS10 = 0 bodů

4.2.11 Kontrola vstupu v přístupových bodech perimetru

Typ: není realizována Bodové hodnocení: SS11 = 0 bodů

4.2.12 Namátkové vstupní a výstupní prohlídky

Typ: nejsou prováděny Bodové hodnocení: SS12 = 0 bodů

4.2.13 Perimetrický detekční systém (PDS)

Typ:	není realizován	Bodové hodnocení:	SS13 = 0 bodů

4.2.14 Bezpečnostní osvětlení perimetru

Typ:	není realizováno	Bodové hodnocení:	SS14 = 0 bodů

4.2.15 Kamerový systém CCTV – doplněk perimetru

Typ:	je realizován	Bodové hodnocení:	SS15 = 2 body

Kamerový systém je instalován na hlavní chodbě, který zajišťuje snímání hlavních dveří ke vstupu do vnořeného objektu s hranicí objektu stanovenou na stupeň utajení kategorie „Tajné“, kde jsou dislokovány místnosti ZO-05, ZO-06 a JO-01.

4.3 VÝPOČET CELKOVÉHO BODOVÉHO OHODNOCENÍ ZO A JO

Protože výpočet bodových hodnot byl již použit při návrhu vhodnější varianty, jsou výsledky znázorněny v příloze diplomové práce.

4.3.1 Celkové bodové ohodnocení ZO-05 kategorie „Tajné“

- **Příloha 6** - Bodové ohodnocení ZO-05 kategorie „Tajné“.

4.3.2 Celkové bodové ohodnocení ZO-06 kategorie „Důvěrné“

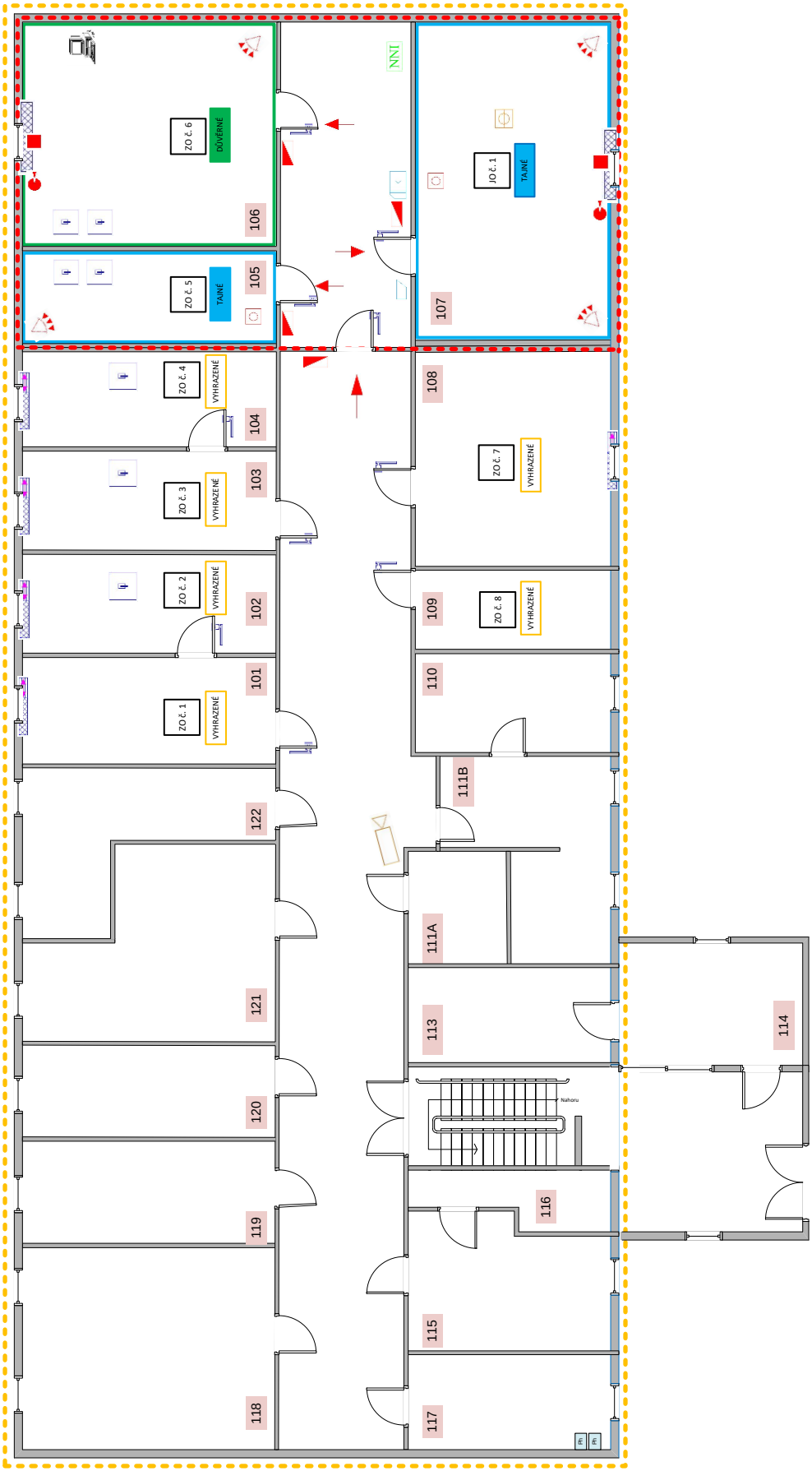
- **Příloha 7** - Bodové ohodnocení ZO-06 kategorie „Důvěrné“.

4.3.3 Celkové bodové ohodnocení JO-01 stupně utajení „Tajné“

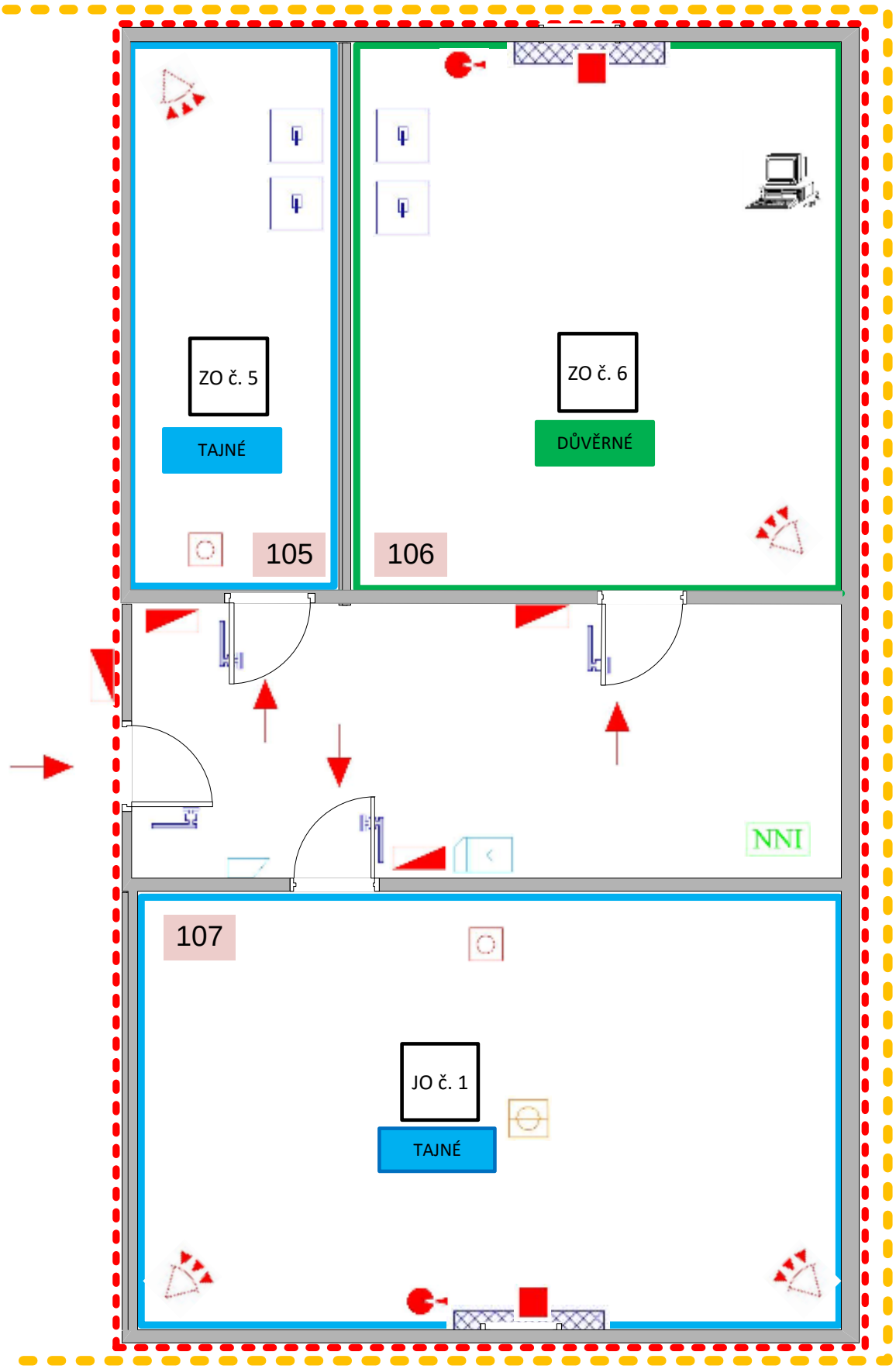
- **Příloha 7** - Bodové ohodnocení JO-01 stupně utajení „Tajné“.

5 OBJEKT – STANOVENÍ HRANICE ZO A JO

5.1 ROZMÍSTĚNÍ TECHNICKÝCH PROSTŘEDKŮ



5.1.1 Hranice ZO, JO a rozmístění technických prostředků



5.1.2 Legenda

Vysvětlivky a popis jednotlivých technických prostředků je uveden v příloze DP.

- **Příloha 5 –** Legenda technických prostředků

5.2 ZPŮSOB POUŽITÍ OPATŘENÍ FYZICKÉ BEZPEČNOSTI DOKUMENTACE TECHNICKÝCH PROSTŘEDKŮ

Posouzení shody necertifikovaných technických prostředků **žádné**

Certifikáty technických prostředků včetně příloh k certifikátu, jsou nedílnou součástí Projektu fyzické bezpečnosti.

6 PROVOZNÍ ŘÁD OBJEKTU

6.1 PRAVIDLA PRO REŽIM POHYBU OSOB A DOPRAVNÍCH PROSTŘEDKŮ

6.1.1 Areál

Režim pohybu dopravních prostředků je stanoven provozním řádem rozsáhlého objektu. Do objektu kasáren posádky Olomouc povolit vjezd služebních vozidel na základě předložení Příkazu k použití techniky. Vjezd soukromých motorových vozidel povolit pouze na základě předložení Povolení k vjezdu a parkování v objektu kasáren Olomouc. Povolení k vjezdu soukromého motorového vozidla není přenosné na jiné vozidlo.

Režim pohybu osob je stanoven interním přepisem VOC.
U komunikačního centra řešit v souladu se zákonem, Vyhláškou NBÚ č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků ve znění pozdějších vyhlášek, NVMO č. 77/2013 Věstníku – Fyzická bezpečnost v resortu Ministerstva obrany ve znění pozdějších předpisů a dalších vnitřních předpisů.

Vstup osob řešit v souladu s rozkazem MO č. 14/2013 Ochrana utajovaných informací v resortu Ministerstva obrany ve znění pozdějších předpisů. Průkazky a povolení ke vstupu vydávat prostřednictvím bezpečnostního manažera objektu na základě písemné žádosti o povolení ke vstupu nebo vjezdu schválené VOC. Ke vstupu a vjezdu do kasáren používat hlavní bránu č. 1. O povolení vstupu písemně informovat stálého operačního dozorčího.

6.1.2 Budova

Vstup do budovy mají pouze příslušníci s povolením ke vstupu, kde do budovy vstupují na základě prokázání totožnosti prostřednictvím identifikačních čipových karet. Dveře je možné dálkově odjistit ze stanoviště fyzické ochrany stálého operačního dozorčího rozsáhlého objektu.

6.1.3 Objekt

Do „objektu“ mohou samostatně vstupovat pouze ty osoby, které byly protokolárně předány prostředky potřebné ke vstupu do „objektu“ (klíče od vstupních dveří, kódy EZS, identifikační prvky SKV apod.).

Seznam oprávněných osob ke vstupu vede: **kpt. Ing. Pavel Kůzlátko**

Režim manipulace s klíči zajišťuje: **kpt. Ing. Pavel Kůzlátko**

6.1.4 Zabezpečená a jednací oblast

Do zabezpečené nebo jednací oblasti mohou samostatně vstupovat pouze ty oprávněné osoby, kterým byly protokolárně přiděleny prostředky potřebné ke vstupu do zabezpečené a jednací oblasti (klíče od vstupních dveří, kód EZS, identifikační prvek SKV s nadefinovaným právem vstupu apod.). Neoprávněná osoba může vstoupit pouze do zabezpečené oblasti třídy II, a to s osobou, která má do této oblasti vstup povolen, přičemž musí být utajované materiály nebo utajované dokumenty uloženy v úschovném objektu nebo zakryty.

Seznam oprávněných osob, které mohou do ZO a JO vstupovat samostatně, vede: **kpt. Ing. Pavel Kůzlátko**

Režim manipulace s klíči zajišťuje: **kpt. Ing. Pavel Kůzlátko**

6.1.5 Režim návštěv

V objektu je stanoven režim návštěv s doprovodem. Všechny návštěvy se zapisují do knihy návštěv. Osoby, které mohou manipulovat s UI, jsou uvedeny v „Redukovaný přehled systemizovaných míst (SM) a seznam osob poučených pro styk s UI“.

Do zabezpečené nebo jednací oblasti mohou návštěvy vstupovat pouze v doprovodu oprávněné osoby, která může do zabezpečené oblasti vstupovat samostatně.

Návštěvy se evidují v: **Kniha návštěv**

Vedení evidence návštěv zajišťuje: **kpt. Ing. Pavel Kůzlátko**

Návštěva je označena: **Visačka s textem „Návštěva“**

Návštěva je doprovázena způsobem: **po celou dobu pobytu v objektu**

6.2 REŽIM POHYBU UTAJOVANÝCH INFORMACÍ V OBJEKTU

S utajovanými informacemi (dále jen „UI“) lze manipulovat v „objektu“ (mimo zabezpečenou oblast), pokud jsou splněny požadavky § 24, odst. 5, písm. b), zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti (dále jen „zákon“). S UI mohou v „objektu“ manipulovat pouze oprávněné osoby, které splňují požadavky přístupu k UI příslušného stupně utajení stanovené zákonem, za předpokladu, že je zajiště-

no, že k UI nebude mít přístup neoprávněná osoba. Veškeré UI, v působnosti OC, se evidují v jednacím protokolu. Za evidenci odpovídá osoba, kterou tímto pověřil vedoucí OC. Při manipulaci s UI mezi oprávněnými osobami se používají administrativní pomůcky v souladu s § 3, vyhlášky č. 529/2005 Sb., které se ukládají v souladu s §3, odst. 8 citované vyhlášky.

Utajované informace se mohou, v souladu s § 24, odst. 5, písm. c) zákona v odůvodněných případech zpracovávat mimo „objekt“, pokud je zajištěno, že k UI nemá přístup neoprávněná osoba. Písemný souhlas k manipulaci mimo „objekt“ je oprávněn vydat vedoucí OC.

Přenášení a přepravu UI lze provádět pouze v souladu s vyhláškou č. 529/2005 Sb., a Hl. VI, RMO č. 14/2013 Věstníku.

Vedením jednacího protokolu (UI) je pověřen (a): **o. z. Ing. Pavel Potočka**

7 PROVOZNÍ DOKUMENTACE K TECHNICKÝM PROSTŘEDKŮM

7.1 MECHANICKÉ ZÁBRANNÉ PROSTŘEDKY

Jednotlivé mechanické zábranné prostředky (dále jen „MZP“) instalované v ZO používají pouze oprávněné osoby, kterým byly protokolárně přiděleny vstupní prostředky. Tyto osoby jsou s obsluhou a používáním MZP seznámeny a poučeny v souladu s pokyny pro používání stanovenými výrobcem, dodavatelem, případně servisní firmou.

Přidělování vstupních prostředků zajišťuje: **kpt. Ing. Pavel Kůzlátko**

Správce technických prostředků: **nrtm. Jakub Zlatý**

Datum instalace technických prostředků: **25. února 2019**

Pravidelné funkční zkoušky jsou prováděny minimálně 1x za 12 měsíců v rámci ověřování, zda použitá opatření fyzické bezpečnosti a vyhodnocení rizik odpovídají projektu fyzické bezpečnosti a platným právním předpisům.

Funkční zkoušku provádí: **Trade FIDES, a.s.**

Pokyny pro používání technických prostředků: **V případě poruchy volat správce technických prostředků.**

7.2 ELEKTRICKÝ ZABEZPEČOVACÍ SYSTÉM

Elektrický zabezpečovací systém, který chrání „objekt“ a zabezpečenou nebo jednací oblast, mohou obsluhovat pouze ty osoby, kterým byl protokolárně předán prostředek k jeho ovládání (kód, identifikační karta apod.). Vstupní prostředky mohou být přiděleny pouze osobám, které splňují požadavky přístupu k UI příslušného stupně utajení stanovené zákonem.

Funkční zkoušky a periodické revize doložené písemně revizními zprávami, se provádějí ihned, pokud dojde např. k rozšíření EZS, výměně ústředny EZS apod. Údaje o provozu EZS se evidují v provozní knize EZS.

Přidělování vstupních prostředků zajišťuje: **kpt. Ing. Pavel Kůzlátko**

Provozní knihu vede: **kpt. Ing. Pavel Kůzlátko**

Správce technických prostředků: **nrtm. Jakub Zlatý**

Pravidelné funkční zkoušky jsou prováděny minimálně 1x za 12 měsíců v rámci ověřování, zda použitá opatření fyzické bezpečnosti a vyhodnocení rizik odpovídají projektu fyzické bezpečnosti a platným právním předpisům.

Funkční zkoušku provádí: **Trade FIDES, a.s.**

Pokyny pro používání technických prostředků **V případě poruchy volat správce technických prostředků.**

7.3 SPECIÁLNÍ TELEVIZNÍ SYSTÉM

Pokyny pro používání speciálních televizních systémů jsou specifikovány v projektové dokumentaci, případně v instrukcích dodaných výrobcem, dodavatelem nebo servisní firmou.

Provozní knihu vede: **kpt. Ing. Pavel Kůzlátko**

Správce technických prostředků: **nrtm. Jakub Zlatý**

Pravidelné funkční zkoušky jsou prováděny minimálně 1x za 12 měsíců v rámci ověřování, zda použitá opatření fyzické bezpečnosti a vyhodnocení rizik odpovídají projektu fyzické bezpečnosti a platným právním předpisům.

Funkční zkoušku provádí: **Trade FIDES, a.s.**

Pokyny pro používání technických prostředků: **V případě poruchy volat správce technických prostředků.**

7.4 ELEKTRICKÁ POŽÁRNÍ SIGNALIZACE

Pokyny pro používání prostředků elektrické požární signalizace (dále také „EPS“) jsou specifikovány v projektové dokumentaci, případně v instrukcích dodaných výrobcem, dodavatelem nebo servisní organizací. Veškerá manipulace s EPS musí být v souladu s podmínkami stanovenými příslušným HZS.

Provozní knihu vede: **kpt. Ing. Pavel Kůzlátko**

Správce technických prostředků: **nrtm. Jakub Zlatý**

Pravidelné funkční zkoušky jsou prováděny minimálně 1x za 12 měsíců v rámci ověřování, zda použitá opatření fyzické bezpečnosti a vyhodnocení rizik odpovídají projektu fyzické bezpečnosti a platným právním předpisům.

Funkční zkoušku provádí: **Trade FIDES, a.s.**

Pokyny pro používání technických prostředků: **V případě poruchy volat správce technických prostředků.**

7.5 SYSTÉM KONTROLY VSTUPU

Identifikační prvky systému kontroly vstupu (dále také „SKV“) mohou být protokolárně přiděleny pouze osobám, které mohou samostatně vstupovat do příslušného chráněného prostoru, např. identifikační prvky SKV s nadefinovaným právem vstupu do zabezpečené oblasti nesmí být přiděleny osobám, které nesplňují požadavky přístupu k UI příslušného stupně utajení stanovené zákonem.

Povinností uživatele je zajišťovat pravidelné revizní kontroly, a to v periodách stanovených výrobcem, dodavatelem nebo servisní firmou, případně vždy, když dojde k poškození SKV.

Provozní knihu vede: **kpt. Ing. Pavel Kůzlátko**

Správce technických prostředků: **nrtm. Jakub Zlatý**

Pravidelné funkční zkoušky jsou prováděny minimálně 1x za 12 měsíců v rámci ověřování, zda použitá opatření fyzické bezpečnosti a vyhodnocení rizik odpovídají projektu fyzické bezpečnosti a platným právním předpisům.

Funkční zkoušku provádí: **Trade FIDES, a.s.**

Pokyny pro používání technických prostředků: **V případě poruchy volat správce technických prostředků.**

7.6 ZAŘÍZENÍ SLOUŽÍCÍ K VYHLEDÁVÁNÍ NEBEZPEČNÝCH LÁTEK A PŘEDMĚTŮ

Veškerá manipulace se zařízením je v kompetenci obsluhy zařízení, která má povinnost, zajistit splnění všech podmínek stanovených výrobcem, dodavatelem případně servisní organizací.

Provozní knihu vede: **rtm. Martin Prchlavý**

Zařízení má přiděleno: **rtm. Martin Prchlavý**

Pravidelné funkční zkoušky jsou prováděny minimálně 1x za 12 měsíců v rámci ověřování, zda použitá opatření fyzické bezpečnosti a vyhodnocení rizik odpovídají projektu fyzické bezpečnosti a platným právním předpisům.

Funkční zkoušku provádí: **Vojenský výzkumný ústav Brno**

7.7 ZAŘÍZENÍ PROTI PASIVNÍMU A AKTIVNÍMU ODPOSLECHU UI

Při používání zařízení jsou dodržována veškerá pravidla stanovená výrobcem, dodavatelem, případně servisní organizací.

Provozní knihu vede: **rtm. Martin Prchlavý**

Správce technických prostředků: **rtm. Martin Prchlavý**

Pravidelné funkční zkoušky jsou prováděny minimálně 1x za 12 měsíců v rámci ověřování, zda použitá opatření fyzické bezpečnosti a vyhodnocení rizik odpovídají projektu fyzické bezpečnosti a platným právním předpisům.

Funkční zkoušku provádí: **externí firma**

7.8 POKYNY POUŽÍVÁNÍ ZAŘÍZENÍ FYZICKÉHO NIČENÍ NOSIČŮ INFORMACÍ

Utajované informace příslušného stupně utajení lze skartovat pouze na skartovacím stroji, který je NBÚ certifikován pro stejný stupeň utajení jako příslušná UI nebo pro stupeň utajení vyšší. Při skartaci musí být dodržovány pokyny pro obsluhu skartovacího stroje, dle dokumentace výrobce.

Na skartovacím stroji se provádějí periodické revize ve stejných lhůtách jako revize přenosných elektrických spotřebičů.

Revizi provádí: **kpt. Ing. Pavel Kůzlátko**

Zařízení má přiděleno: **kpt. Ing. Pavel Kůzlátko**

Pravidelné funkční zkoušky jsou prováděny minimálně 1x za 12 měsíců v rámci ověřování, zda použitá opatření fyzické bezpečnosti a vyhodnocení rizik odpovídají projektu fyzické bezpečnosti a platným právním předpisům.

Funkční zkoušku provádí: **kpt. Ing. Pavel Kůzlátko**

7.9 MANIPULACI S KLÍČI A IDENTIFIKAČNÍMI DATY

Režim manipulace s klíči a identifikačními daty je založen na protokolárním předání vstupních prostředků (MZS, EZS, SKV) „objektů“, zabezpečených oblastí, jednacích oblastí a úschovných objektů oprávněným osobám.

Režim manipulace s klíči a identifikačními daty musí být v souladu s § 8 vyhlášky č. 528/2005 Sb., a čl. 9, NV MO č. 77/2013 Věstníku.

Seznam přidělených klíčů vede: **kpt. Ing. Pavel Kůzlátko**

Seznam přidělených identifikačních dat EZS vede: **osoba pověřená vedením seznamu klíčů**

Seznam přidělených identifikačních dat SKV vede: **osoba pověřená vedením seznamu klíčů**

Způsob označení klíčů a identifikačních dat vstupních prostředků: **v souladu s vnitřními předpisy**

7.10 ÚSCHOVNA A EVIDENCE VSTUPNÍCH PROSTŘEDKŮ

Evidence vstupních prostředků je vedena v rámci **knihy výdeje klíčů**

Vstupní prostředky přidělené k dennímu užívání, jsou uloženy **BM ÚTVARU**

Knihu výdeje klíčů vede: **kpt. Ing. Pavel Kůzlátko**

Elektronickou úložnu spravuje: **kpt. Ing. Pavel Kůzlátko**

V případě ztráty, vyzrazení vstupních prostředků, či zjištění jiného porušení klíčového režimu jsou oprávněné osoby povinny zajistit odstranění závady a stanovení náhradního způsobu ochrany UI do doby přijetí nápravných opatření. Oprávněné osoby jsou povinny postupovat v souladu čl. 9, NV MO č. 77/2013 Věstníku a zabránit vyzrazení UI.

7.11 UKLÁDÁNÍ DUPLIKÁTŮ KLÍČŮ

Klíče od dveří (mříží) do ZO a JO: č 1 – 8 jsou uloženy u BM útvaru budova č. 03, 1. NP místnost 103.

Klíče od úschovného objektu: č 1 – 8 jsou uloženy u BM útvaru budova č. 03, 1. NP místnost 103.

Duplikáty klíčů vstupních dveří do objektů, ZO a JO jsou uloženy u BM. Označení obálek s duplikáty klíčů, kombinací zámků a nevydaných klíčů je v souladu s NVMO.

7.12 POPIS REŽIMOVÝCH OPATŘENÍ PRO OCHRANU JEDNACÍCH OBLASTÍ

V „objektu“ je umístěna jednací oblast **ANO**

V jednací oblasti budou projednávány utajované informace stupně Tajné

Jednací oblast je zajištěna prostředky proti pasivnímu a aktivnímu odposlechu utajovaných informací. Zajištění odpovídá požadavkům vyhlášky č. 528/2005 Sb., kapitola č. 10.

Obranná prohlídka provedena dne: 21. 01. 2019

Zpráva o provedení a průběhu obranné prohlídky je uložena jako příloha PFB. Za provedení obranné prohlídky je odpovědný vedoucí OC. Osoby pověřené vedením provozní knihy a správce technického zařízení jsou definovány v kapitole 7.2.

7.13 PRAVIDLA PRO VÝKON OSTRAHY

<table>
<tr><th colspan="7">Způsob výkonu ostrahy</th></tr>
<tr><td colspan="2"></td><td colspan="2">Počet stanovišť</td><td colspan="3">Počet příslušníků</td></tr>
<tr><td>V provozní době</td><td>06.00 – 18.00</td><td colspan="2">- 1 -</td><td colspan="3">- 3 -</td></tr>
<tr><td>Mimo provozní době</td><td>18.00 – 06.00</td><td colspan="2">- 1 -</td><td colspan="3">- 3 -</td></tr>
<tr><td colspan="4">Ostraha u objektu</td><td colspan="3">ANO</td></tr>
<tr><td colspan="4">Stanoviště stálé ostrahy je od ZO vzdáleno méně než 500 m</td><td colspan="3">ANO</td></tr>
<tr><td colspan="4">Stanoviště stálé ostrahy je od ZO vzdáleno více než 500 m, ale zásah ostrahy bude proveden do 5 minut od přijetí poplašného signálu</td><td colspan="3">ANO</td></tr>
<tr><td colspan="4">Sledování výstupů technických prostředků</td><td colspan="3">ANO</td></tr>
<tr><td colspan="2">Sledované systémy technického zabezpečení</td><td>EZS</td><td>EPS</td><td>CCTV</td><td>SKV</td><td>---</td></tr>
<tr><td colspan="4">Vyvedení výstupů technických prostředků na stanoviště určené pro stálý výkon ostrahy</td><td colspan="3">ANO</td></tr>
<tr><td colspan="2">Systémy monitorované na stanovišti určené pro stálý výkon ostrahy</td><td>EZS</td><td>EPS</td><td>SKV</td><td>CCTV</td><td>---</td></tr>
<tr><td colspan="4">Obchůzková činnost</td><td colspan="3">ANO</td></tr>
<tr><td colspan="7">Interval obchůzek a způsob obchůzkové činnosti</td></tr>
<tr><td colspan="7">Interval obchůzek a způsob obchůzkové činnosti je specifikován v interních předpisech rozsáhlého objektu Neředínských kasáren – Olomouc.</td></tr>
<tr><td colspan="4">Provádění kontrol osob a dopravních prostředků při vstupu do objektu a při výstupu z objektu</td><td colspan="3">ANO</td></tr>
</table>

Provádění namátkových vstupních a výstupních prohlídek v objektu	**ANO**

7.14 PRAVIDLA PRO OHLAŠOVACÍ POVINNOST

Oprávněné osoby mají povinnost oznamovat mimořádné situace v souvislosti s ochranou UI osobám či subjektům uvedeným v tabulce, které jsou dle povahy mimořádné situace povolávány:

Vedoucí organizačního celku			
V provozní době	405 111	**Mobilní telefon**	756 251 333
Mimo provozní dobu	605 874 325	**Jiné spojení**	
Bezpečnostní manažer			
V provozní době	401 999	**Mobilní telefon**	724 666 999
Mimo provozní dobu	604 111 222	**Jiné spojení**	
Další oprávněná osoba			
V provozní době	402 658	**Mobilní telefon**	604 222 333
Mimo provozní dobu	608 999 222	**Jiné spojení**	
Telefonní linka na ostrahu		402 000	
Tísňová linka VP		402 155	
Integrovaný záchranný systém		112	
Hasičský záchranný sbor města		150	
Záchranná služba		155	

Opatření provozního řádu jsou závazná pro všechny zaměstnance a příslušníky ozbrojených sil OC včetně dodavatelských firem, případně jiných dalších uživatelů „objektů“.

8 PLÁN ZABEZPEČENÍ OBJEKTU, ZABEZPEČENÝCH OBLASTÍ A JEDNACÍCH OBLASTÍ V KRIZOVÝCH SITUACÍCH

8.1 ÚVODNÍ USTANOVENÍ, OBECNÉ ZÁSADY ŘEŠENÍ MIMOŘÁDNÝCH A KRIZOVÝCH SITUACÍ

Mimořádnou situaci, dle § 2, písm. i), vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů, je stav, kdy bezprostředně hrozí, že dojde k vyzrazení nebo zneužití UI.

Obecné zásady řešení mimořádných situací popisují obecně činnost jednotlivých osob podílejících se na ochraně UI.

8.1.1 Oprávněné osoby

Všechny oprávněné osoby při zjištění ohrožení UI, jsou povinny zamezit všemi dostupnými prostředky vyzrazení UI, případně minimalizovat dopad seznámení s UI neoprávněnou osobou. Neposkytovat žádné informace nepovolaným osobám, zvláště sdělovacím prostředkům. Všechny dotazy směřovat na vedoucího organizačního celku.

8.1.2 Bezpečnostní manažer

Bezpečnostní manažer je osobou pověřenou za ochranu UI, rozhoduje samostatně, případně ve spolupráci s vedoucím organizačního celku a kvalifikovanými subjekty, o postupech při odstranění následků mimořádné situace, o postupech eliminace jejich dopadů, zajištění provozu „objektů“ a zabezpečených oblastí v době mimořádné situace apod.

8.1.3 Vedoucí organizačního celku

Za komplexní ochranu UI v působnosti organizačního celku odpovídá vedoucí organizačního celku. Došlo-li ke vzniku mimořádné situace, je vedoucí organizačního celku povinen zhodnotit mimořádnou situaci a rozsah jejich následků. Zhodnotit kvalitu a úroveň dosud přijatých opatření, případně vydat nová bezpečnostní opatření k úspěšnému řešení mimořádné situace. V případě spáchání trestného činu informuje orgány činné v trestním řízení, pokud tak již nebylo učiněno.

8.2 POKYNY PRO OCHRANU UI V PŘÍPADĚ VZNIKU MIMOŘÁDNÉ SITUACE

8.2.1 Vyzrazení UI oprávněnými osobami

Oprávněné osoby

- zamezit další manipulaci s UI neoprávněnými osobami;
- informovat nadřízené a dále se řídit jejich pokyny.

Bezpečnostní manažer

- ověří věrohodnost informací o vyzrazení UI;
- pozastaví veškerou manipulaci s UI a provede kontrolu jejich úplnosti;
- prověří funkčnost režimových opatření a provede nápravná opatření;
- prověří zásady administrativní a personální bezpečnosti a provede nápravná opatření;
- řeší porušení zásad ochrany UI a realizuje opatření ke zvýšení ochrany UI;
- informuje vedoucího organizačního celku o vzniku mimořádné situace.

Vedoucí organizačního celku

- při prokázané manipulaci s UI neoprávněnými osobami nařídí realizaci prohlídek všech osob odcházejících z „objektu“;
- koordinuje činnost při řešení zásad ochrany UI;
- provede oznámení orgánům činným v trestním řízení (po zhodnocení, zda došlo ke spáchání trestného činu).

8.2.2 Manipulace UI neoprávněnými osobami

8.2.2.1 Vloupání

Oprávněné osoby

- vyrozumět nadřízené (VP) a zajistit místo činu;
- zabránit manipulaci s UI neoprávněnými osobami v případě narušení úschovného objektu;
- znemožnit jakoukoliv manipulaci s předměty v místě vloupání;
- v případě kontaktu s pachatelem uvést jeho co nejpodrobnější popis a trasu jeho úniku.

Bezpečnostní manažer

- dostavit se na pracoviště a provést prověrku úplnosti UI;
- zjistit, zda skutečně došlo k manipulaci s UI neoprávněnými osobami;
- v případě poškození zabezpečené oblasti nebo úschovného objektu realizovat opatření k ochraně UI (v případě potřeby zajistit náhradní uložení UI nebo výkon ostrahy na místě);
- zajistit podmínky a poskytnout součinnost při vyšetřování vloupání Vojenské policii;
- přesně zdokumentovat průběh manipulace s UI neoprávněnými osobami, zjistit, zda nedošlo k porušení zásad režimové ochrany nebo porušení postupů administrativní bezpečnosti, prověřit funkčnost prostředků technické ochrany a způsob jejich překonání.

Vedoucí organizačního celku

- koordinuje činnost s Vojenskou policií;
- provede oznámení orgánům činným v trestním řízení.

8.2.2.2 Loupežné přepadení

Oprávněné osoby

- přivolat pomoc (pokud jí to situace dovoluje);
- zajistit místo činu a do příchodu Vojenské policie zabránit jakékoliv manipulaci s předměty v místě loupežného přepadení;
- chránit UI před vydáním neoprávněné osobě a pod pohrůžkou vydat jen nezbytně nutné;
- zajistit minimalizaci škod;
- neposkytovat informace jiným osobám mimo bezpečnostního manažera, vedoucího organizačního celku, VP a orgánům činných v trestním řízení.

Bezpečnostní manažer

- vydat pokyny a koordinovat činnost oprávněných osob;
- provést předběžné šetření mimořádné situace;
- informovat vedoucího organizačního celku, pokud tak již nebylo učiněno;
- spolupracovat při řešení mimořádné situace s Vojenskou policií.

Vedoucí organizačního celku

- přijmout opatření k ochraně UI;
- provést oznámení orgánům činným trestním řízení.

8.2.3 Poškození, zničení UI živelní pohromou

8.2.3.1 Požár

Oprávněné osoby

- ukončit manipulaci s UI a uložit je do úschovného objektu nebo připravit UI k evakuaci;
- opustit ohrožený prostor (pokud nebude vydán jiný pokyn);
- postupovat dle požárních poplachových směrnic;
- přivolat hasičský záchranný sbor;
- dostupnými hasebními prostředky požár uhasit.

Bezpečnostní manažer

- zhodnotí situaci a nařídí okamžité ukončení manipulace s UI;
- v případě ponechání UI v úschovném objektu zabezpečí provedení aktivace technického zabezpečení a opuštění ohroženého prostoru;
- řídí se pokyny velitele zásahu HZS;
- po likvidaci požáru provede kontrolu úplnosti UI a vyhodnotí, jestli nedošlo k manipulaci s UI neoprávněnými osobami;
- o průběhu mimořádných situací, rozsahu škod a přijatých opatření provede zápis.

Vedoucí organizačního celku

- zhodnotí situaci a rozhodne o opatřeních k ochraně UI (podle situace určí, zda UI zůstanou v úschovném objektu nebo bude provedena jejich evakuace);
- v případě, že došlo k manipulaci s UI neoprávněnou osobou, informuje orgány činné v trestním řízení.

8.2.3.2 Povodeň, technologické havárie, havárie inženýrských sítí v budově

Oprávněné osoby

- postupovat dle požárních a evakuačních směrnic;
- pro zamezení vzniku větších škod neprodleně uzavřít hlavní uzávěr vody a plynu;
- ukončit manipulaci s UI a uložit je do úschovného objektu nebo připravit UI k evakuaci;
- opustit ohrožený prostor (pokud nebude vydán jiný pokyn).

Bezpečnostní manažer

- zhodnotí situaci a rozhodne o opatřeních k ochraně UI;
- v případě ponechání UI v úschovném objektu provede aktivaci technického zabezpečení a opustí ohrožený prostor;
- realizuje kontrolu úplnosti UI a vyhodnotí, zda nedošlo k manipulaci s UI neoprávněnými osobami;
- o průběhu mimořádné situace, rozsahu škod a přijatých opatření zpracuje zápis.

Vedoucí organizačního celku

- zhodnotí situaci a rozhodne o opatření k ochraně UI (podle situace určí, zda UI zůstanou v úschovném objetu nebo bude provedena jejich evakuace);
- v případě neoprávněné manipulace s UI postupuje dle specifikace uvedené v předchozí kapitole.

8.2.3.3 Jiná ohrožení živelnými pohromami

- v případě jiných živelních pohrom (větrná smršť, úder blesku apod.) postupovat dle konkrétní situace obdobně jako v uvedených případech;
- v těchto případech jsou bezpečnostní manažer a vedoucí organizačního celku povinni přijmout opatření (z opatření vyjmenovaných v předchozích kapitolách), které budou v daných podmínkách nejlépe řešit ochranu UI.

8.2.4 Poškození (zničení) UI průmyslovou nebo technologickou havárií

K zničení nebo poškození UI průmyslovou havárií může dojít následkem úniku nebo výbuchu nebezpečných chemických látek a přípravků v přímé blízkosti „objektu“. V případě hrozby zničení nebo poškození UI průmyslovou nebo technologickou havárií je nutné postupovat obdobně jako v případech živelních pohrom.

8.2.4.1 Bezpečnostní manažer a Vedoucí organizačního celku

- informují se o původu vzniku průmyslové havárie a přijímají adekvátní opatření (evakuace osob nebo naopak setrvání v budově, uzavření oken apod.);
- koordinují činnost s kompetentními orgány podílejícími se na likvidaci dané situace;
- vyhodnocují změny ve vývoji situace a pružně reagují na daný stav.

V závislosti na situaci zejména:

- posoudí, do jaké míry může událost ohrozit bezpečnost UI a zdraví osob;
- informují se u složek a orgánů (HZS, Městský úřad apod.), které se podílí na likvidaci následků průmyslové havárie, na zdroj průmyslové havárie a vhodná opatření k zajištění zdraví a bezpečnosti osob;
- přijímají rozhodnutí o evakuaci osob na UI;
- zabezpečují provoz „objektu“, zabezpečených oblastí a jednacích oblastí v podmínkách likvidace následků havárie;
- obnovují režim ochrany UI na úroveň před havárií.

8.2.5 Ztráta UI následkem teroristického útoku

8.2.5.1 Uložení výbušniny (nález podezřelého předmětu)

Oprávněné osoby

- ukončí neprodleně manipulaci s UI, informují bezpečnostního manažera, vedoucího organizačního celku a Vojenskou policii;
- uloží UI do úschovného objektu nebo připraví jejich evakuaci;
- řídí se pokyny výše uvedených osob.

Bezpečnostní manažer

- koordinuje nařízenou evakuaci UI;
- po ukončení evakuace provádí prověrku úplnosti UI a prověří, zda nedošlo k manipulaci s UI neoprávněnou osobou.

Vedoucí organizačního celku

- vyhodnotí situaci a případně nařídí evakuaci UI;
- při spáchání trestného činu informuje orgány činné v trestním řízení;
- organizuje bezpečnostní opatření k ochraně UI na úroveň před vznikem mimořádné situace.

8.2.5.2 Telefonická pohrůžka uložení výbušniny

Bezpečnostní manažer a Vedoucí organizačního celku

- v případě nevyrozumění VP provedou její informování a následně koordinují činnost s VP;
- rozhodnou o evakuaci UI;

- provedou fyzickou kontrolu UI a vyhodnotí míru škod.

8.2.5.3 Doručení podezřelé zásilky

Bezpečnostní manažer a Vedoucí organizačního celku

- v případě nevyrozumění VP provedou její informování a následně koordinují činnost s VP;
- rozhodnou o evakuaci UI.

8.2.5.4 Přímý útok ozbrojeného pachatele nebo skupiny

Oprávněné osoby

- chovají se tak, aby pachatele nevyprovokovaly k neadekvátní reakci;
- chrání UI a pod pohrůžkou vydají jen nezbytně nutné s ohledem na vlastní bezpečnost;
- získávají co nejvíce poznatků potřebných k pozdější identifikaci pachatele (popis, hlas, chování, výzbroj apod.);
- pokud to lze realizovat bez povšimnutí pachatele, přivolají pomoc, respektive varují okolí;
- po odchodu pachatele okamžitě uvědomí Vojenskou policii, bezpečnostního manažera a vedoucího organizačního celku;
- neposkytují informace jiným osobám mimo výše uvedené a orgánů činných v trestním řízení.

Bezpečnostní manažer

- provede oznámení VP;
- přijme opatření k další ochraně UI.

Vedoucí organizačního celku

- koordinuje činnost s VP.

8.2.6 Vyzrazení UI pasivním odposlechem nebo nasazením operativní bezpečnosti

Bezpečnostní manažer a Vedoucí organizačního celku

- provést okamžitá opatření k zamezení úniku informací tvořící UI;
- v případě prokazatelného podezření na únik informací nasazením operativní techniky, zajistit provedení obranné prohlídky;
- obnovit režim se stavem před únikem informací;
- provést oznámení orgánům činným v trestním řízení (po vyhodnocení, zda došlo ke spáchání trestného činu).

8.2.7 Vyzrazení nebo ztráta UI z informačního systému

Postupy řešení mimořádné situace, související se ztrátou nebo poškozením UI zpracovávaných pomocí informačního systému, jsou obdobné jako při řešení mimořádných situací

týkajících se UI v listinné podobě. Především je nutné okamžitě zabránit další manipulaci s UI neoprávněnou osobou a dalšímu úniku UI (změna přístupového jména a hesla – autentizace, zabavení neoprávněné kopie apod.)
Konkrétní opatření jsou uvedena ve zvlášť zpracované bezpečnostní dokumentaci informačního systému.

8.2.8 Poškození UI při krizovém stavu

Vedoucí organizačního celku

- svolá oprávněné osoby;
- přijímá adekvátní opatření s ohledem na aktuální vývoj bezpečnostní situace;
- vyhodnocuje bezpečnostní situaci;
- provádí dílčí organizační, režimová a administrativní opatření směřující k ochraně UI;
- organizuje ukončení manipulace s UI a jejich evakuaci (případně skartaci);
- řídí se pokyny nadřízených v rámci resortu.

8.2.9 Poškození stavebně opevňovacího materiálu

Vedoucí organizačního celku

- svolá oprávněné osoby;
- přijímá adekvátní opatření s ohledem na aktuální vývoj bezpečnostní situaci;
- vyhodnocuje bezpečnostní situaci;
- provádí dílčí organizační, režimová a administrativní opatření směřující k ochraně UI;
- organizuje ukončení manipulace s UI a jejich evakuaci (případně skartaci);
- řídí se pokyny nadřízených v rámci resortu.

9 ODPOVĚDNOST ZA DODRŽOVÁNÍ PLÁNU

Za dodržování Plánu zabezpečení objektu, zabezpečených oblastí a jednací oblasti v krizových situacích odpovídá vedoucí organizačního celku, bezpečnostní manažer, všechny oprávněné osoby v příslušném rozsahu. Jejich seznámení s tímto plánem je provedeno prokazatelným způsobem.

Za aktuálnost opatření tohoto plánu odpovídá vedoucí organizačního celku.

ZÁVĚR

Cílem diplomové práce bylo vytvořit návrh realizace „Projektu fyzické bezpečnosti“ v zabezpečené a jednací oblasti objektu Armády České republiky. Předmětem mojí snahy bylo stanovit přehled z oblasti fyzické bezpečnosti, který je nezbytné znát před samotným vytvořením „Projektu fyzické bezpečnosti“. Diplomová práce byla rozdělena na dvě základní části, na část teoretickou a část praktickou. Teoretická část práce byla popsána ve dvou kapitolách a praktická část byla zpracována ve třech kapitolách.

V první kapitole teoretické části jsem se soustředil na analýzu všech potřebných norem a legislativních předpisů nezbytných k zajištění fyzické bezpečnosti v ČR. Největší pozornost byla tedy věnována fyzické bezpečnosti podílející se na ochraně utajovaných informací. V této kapitole jsme se dále mohli dozvědět, že utajované informace můžou obsahovat analogovou nebo digitální podobu a je potřeba je chránit před zneužitím, vyzrazením, poškozením, nedovoleným šířením nebo odcizením. Z legislativních předpisů a norem byl podrobněji popsán zákon 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti. Tento zákon nám popsal jednotlivé kategorie stupně utajení: Vyhrazené, Důvěrné, Tajné a Přísně tajné. Další z legislativních předpisů, byla zmíněna Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů, která klade důraz na nejnižší možnou míru zabezpečení v zabezpečených a jednacích oblastech. Součástí vyhlášky byly přílohy, které nám charakterizovaly bodové ohodnocení v zabezpečených a jednacích oblastech, strukturu projektu fyzické bezpečnosti a použití technických prostředků. Jako doplňující vnitřní předpisy pro zajištění ochrany utajovaných informací v objektech AČR, které vydalo Ministerstvo obrany, byl uveden 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. Oba tyto vnitřní předpisy vydané Ministerstvem obrany nám upřesnily jednotlivé body fyzické bezpečnosti, které se uplatňují v objektech AČR.

V druhé kapitole teoretické části byl analyzován soubor pravidel, který poukázal na specifické požadavky potřebné k vytvoření Projektu fyzické bezpečnosti v objektech AČR. Byly zde uvedeny požadavky stanovující postup při zřízení nově vznikající zabezpečené nebo jednací oblasti včetně vytyčení hranic objektu. Dále v této kapitole byly popsány role velitele rozsáhlého objektu, velitele organizačního celku, bezpečnostního manažera a dalších

zainteresovaných osob podílejících se na tvorbě Návrhu projektu fyzické bezpečnosti a Projektu fyzické bezpečnosti v objektech AČR.

V 3 kapitole je vysvětleno a popsáno rozdělení jednotlivých technických prostředků sloužících k zajištění ochrany utajovaných informací. Tyto technické prostředky byly rozděleny na mechanické zábranné prostředky, elektrická zámková zařízení, systémy pro kontrolu vstupu, poplachové zabezpečovací a tísnivé systémy, kamerové systémy a elektrická požární signalizace. Pro většinu technických prostředků jsem uvedl názorné příklady používané v objektech AČR, které obsahovaly detailní popisy včetně technických specifikací a obrázků.

V 4 kapitole jsem navrhl model s hypoteticky zabezpečenými oblastmi kategorie stupně utajení Důvěrné, Tajné a jednu jednací oblast stupně utajení Tajné. Na tomto vytvořeném modelu jsem si stanovil podmínky potřebné k zajištění ochrany utajovaných informací pro zabezpečené oblasti a jednací oblast, které běžně stanovuje velitel organizačního celku. Abych splnil tyto podmínky, vytvořil jsem návrh dvou možných variant, které měly zajistit fyzickou bezpečnost těchto oblastí za použití technických prostředků. Na základě multikriteriální analýzy jsem vybral vhodnější variantu k zajištění ochrany utajovaných informací zabezpečených oblastí a jednací oblasti modelu hypotetického objektu AČR. Tato zvolená varianta byla dosazena do samotného Projektu fyzické bezpečnosti v poslední kapitole praktické části diplomové práce.

V poslední kapitole jsem vytvořil zmíněný finální „Projekt fyzické bezpečnosti“ pro zabezpečenou a jednací oblast objektu AČR. Objekt byl zvolen ve fiktivně vymyšlených Neředínských kasárnách v Olomouci. Samotný Projekt fyzické bezpečnosti byl zapracován do šablony vydané Ministerstvem obrany, která se běžně pro tento účel používá. Tomuto projektu jsem stanovil kategorii stupně utajení – Neutajované, protože se jedná pouze o vzor vyplněný smyšlenými informacemi.

Všeobecně není jednoduché si někde přečíst nebo vyhledat reálné Návrhy projektu fyzické bezpečnosti nebo samotné Projekty fyzické bezpečnosti. Proto si myslím, že tato diplomová práce může být dobrým vodítkem a pomocníkem při vytváření Projektu fyzické bezpečnosti třeba pro začínající bezpečnostní důstojníky pracující ve státním sektoru.

Výsledkem této diplomové práce, jako velké pozitivum hodnotím prohloubení znalostí z oblasti fyzické bezpečnosti, které určitě uplatním ve své pracovní profesi do budoucna.

SEZNAM POUŽITÉ LITERATURY

[1] Národní bezpečnostní úřad: Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů[online]. Praha, 2005. Dostupné také z: https://www.nbu.cz/cs/pravni-predpisy/zakon-c-412-2005/1122-uplne-zneni-zakona-c-412-2005/

[2] LUŇÁČEK, Oldřich. Fyzická bezpečnost - K209: Normy v oblasti bezpečnosti informací Soubor [online]. Brno. Univerzita obrany [cit. 2019-01-01]. Dostupné z: https://moodle.unob.cz/pluginfile.php/18154/mod_resource/content/8/Normy%20v%20oblasti%20bezpe%C4%8Dnosti.pdf¨

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

[4] Národní úřad pro kybernetickou a informační bezpečnost: NÚKIB [online]. Brno, 2017 [cit. 2019-04-27]. Dostupné z: https://www.nukib.cz/cs/o-nukib/

[5] Národní bezpečnostní úřad: Hlavní úkoly [online]. Praha, 2005. [cit. 2019-01-01]. Dostupné také z: https://www.nbu.cz/cs/o-nas/953-hlavni-ukoly-nbu/

[6] Intranet MO: Struktura, působnost [online]. In: Ministerstvo obrany [cit. 2019-01-29].

[7] Zákony pro lidi.cz: Zákon č. 412/2005 Sb. Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti [online]. Česká republika, 2005 [cit. 2019-01-02]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-412/zneni-20180307

[8] Národní bezpečnostní úřad: Prováděcí právní předpisy [online]. Praha, 1998 [cit. 2019-01-02]. Dostupné z: https://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/

[9] Zákony pro lidi.cz: Zákon č. 413/2005 Sb. Zákon o změně zákonů v souvislosti s přijetím zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti [online]. Praha, 2005 [cit. 2019-01-02]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-413

[10] Zákon pro lidi.cz: Nařízení vlády č. 522/2005 Sb. Nařízení vlády, kterým se stanoví seznam utajovaných informací [online]. Česká republika, 2005 [cit. 2019-01-02]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-522

[11] Národní bezpečnostní úřad: Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů[online]. Brno, 2005 [cit. 2019-04-27]. Dostupné z: https://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/1087-vyhlaska-c-5282005/

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

[13] ČESKÁ REPUBLIKA. Normativní výnos Ministerstva obrany č. 77/2013 Věstníku, Fyzická bezpečnost v rezortu Ministerstva obrany. In: Ministerstvo obrany, 2013, číslo 77.

[14] LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management I. Zlín: VeRbuM, 2011. ISBN 978-80-87500-05-7.

[15] Národní bezpečnostní úřad: Seznam certifikovaných technických prostředků [online]. Praha [cit. 2019-02-03]. Dostupné z: https://www.nbu.cz/cs/informacni-centrum/seznamy/seznam-certifikovanych-technickych-prostredku/

[16] Národní bezpečnostní úřad: Fyzická bezpečnost [online]. Praha [cit. 2019-02-03]. Dostupné z: https://www.nbu.cz/cs/nejcastejsi-dotazy/946-fyzicka-bezpecnost/

[17] Uhlář, J. Technická ochrana objektů - 1. Díl (Mechanické zábranné systémy II. Katedra technických prostředků bezpečnostních služeb, Praha: PA ČR, 2004, ISBN 80-7251- 172-6.

[18] HT dveře [online]. [cit. 2019-02-20]. Dostupné z: https://www.htdvere.cz/poradna/cim-se-odlisuji-bezpecnostni-tridy-dveri/

[19] OK - PRODUKT: Bezpečnostní třídy trezorů [online]. Brno, 2008 [cit. 2019-02-03]. Dostupné z: http://www.ok-produkt.cz/bezpecnostni-tridy-trezoru/t-120/

[20] ČESKÉ TREZORY Jínová: Trezorové normy [online]. [cit. 2019-02-03]. Dostupné z: http://www.jinova.cz/trezorove-normy

[21] RAISA spol. s r.o: Úložny klíčů [online]. [cit. 2019-02-21]. Dostupné z: https://www.raisa.cz/page/ulozny-klicu

[22] ASSET Projektování 2016, Trade FIDES, a.s.: Projektování systému ASSET [online]. [cit. 2019-02-24]. Dostupné z: https://docplayer.cz/18754425-Asset-projektovani-2016.html

[23] VALOUCH, Jan. Projektování integrovaných systémů. Druhé vydání. Zlín: UTB, 2015. ISBN 978-80-7454-557-3.

[24] VALOUCH, Jan. Projektování integrovaných systémů. Zlín: UTB, 2013. ISBN 978-80-7454-296-1.

[25] Zabezpečovací technika damacom: Zabezpečovací ústředna [online]. [cit. 2019-02-24]. Dostupné z: https://www.alarmshop.cz/el-zabezpecovaci-system---ezs

[26] KŘEČEK, Stanislav. Příručka zabezpečovací techniky. Vyd. 3. aktualiz. S.l.: Cricetus, 2006, 313 s. ISBN 80-902938-2-4.

[27] HALOUZKA, Kamil. Fyzická bezpečnost: Perimetrické zabezpečovací systémy. 2015, (CZ.1.01/2.2.00/15.0070).

[28] JABLOSHOP.cz: JA-181M Bezdrátový magnetický detektor, bez baterie [online]. [cit. 2019-02-24]. Dostupné z: https://www.jabloshop.cz/ja-181m-bezdratovy-magneticky-detektor

[29] STAVEBNÍ KLUB profi: Pasivní infračervené detektory - PIR [online]. [cit. 2019-02-25]. Dostupné z: https://www.stavebniklub.cz/33/pasivni-infracervene-detektory-pir-uniqueidmRRWSbk196FNf8-jVUh4Epdmo-R2YgJtttJVFFohsn0/

[30] IVANKA, Ján. Systematizace bezpečnostního průmyslu. Druhé vydání. Zlín: UTB, 2011. ISBN 978-80-7454-122-3.

[31] KŘEČEK, Stanislav. Příručka zabezpečovací techniky. Blatná.: Cricetus, 2003, 351 s. ISBN 80-902938-2-4.

[32] Hlídací kamery: Rozdělení a druhy bezpečnostních kamer CCTV [online]. 2011 [cit. 2019-02-21]. Dostupné z: http://www.hlidacikamery.cz/druhy-kamer/

[33] LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management IV. Zlín: VeRbuM, 2014. ISBN 978-80-87500-57-6.

[34] Trade Fides: Technologické prostředky [online]. 2n. l. [cit. 2019-02-21]. Dostupné z: https://fides.cz/technologicke-prostredky/ekv.html

[35] Eaton Elektrotechnika: Elektrická požární signalizace EPS [online]. 2015 [cit. 2019-02-03]. Dostupné z: http://www.eatonelektrotechnika.cz/cz/elektricka-pozarni-signalizace-eps.html

[36] KORVINY, Petr. Teoretické základy vícekriteriálního rozhodování. [online]. [cit. 2018-04-04]. Dostupné z: https://korviny.cz/Korviny/soubory/teorie_mca.pdf

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AČR Armáda České republiky.

BM Bezpečnostní manažer.

BŘ Bezpečnostní ředitel.

CCTV Speciální televizní systémy (Closed Circuit Televizion).

ČR Česká republika.

DP Diplomová práce.

DPPC Dohledové a Poplachové Přijímací Centrum

EKV Elektrická kontrola vstupu.

EPS Elektrická požární signalizace.

EU Evropská unie.

EZS Elektrický zabezpečovací systém.

IKS Informační komunikační systém.

JO Jednací oblast.

MO Ministerstvo obrany.

MZP Mechanické zábranné prostředky.

NATO Severoatlantická aliance.

NBÚ Národní bezpečnostní úřad (často zkráceně se uvádí „Úřad“).

NNI Zařízení fyzického ničení nosičů informací.

NP Nadzemní podlaží.

NÚKIB Národní úřad pro kybernetickou a informační bezpečnost.

NV MO Normativní výnos Ministerstva obrany.

OB Odbor bezpečnosti.

OB MO Odbor bezpečnosti Ministerstva obrany.

OC Organizační celek.

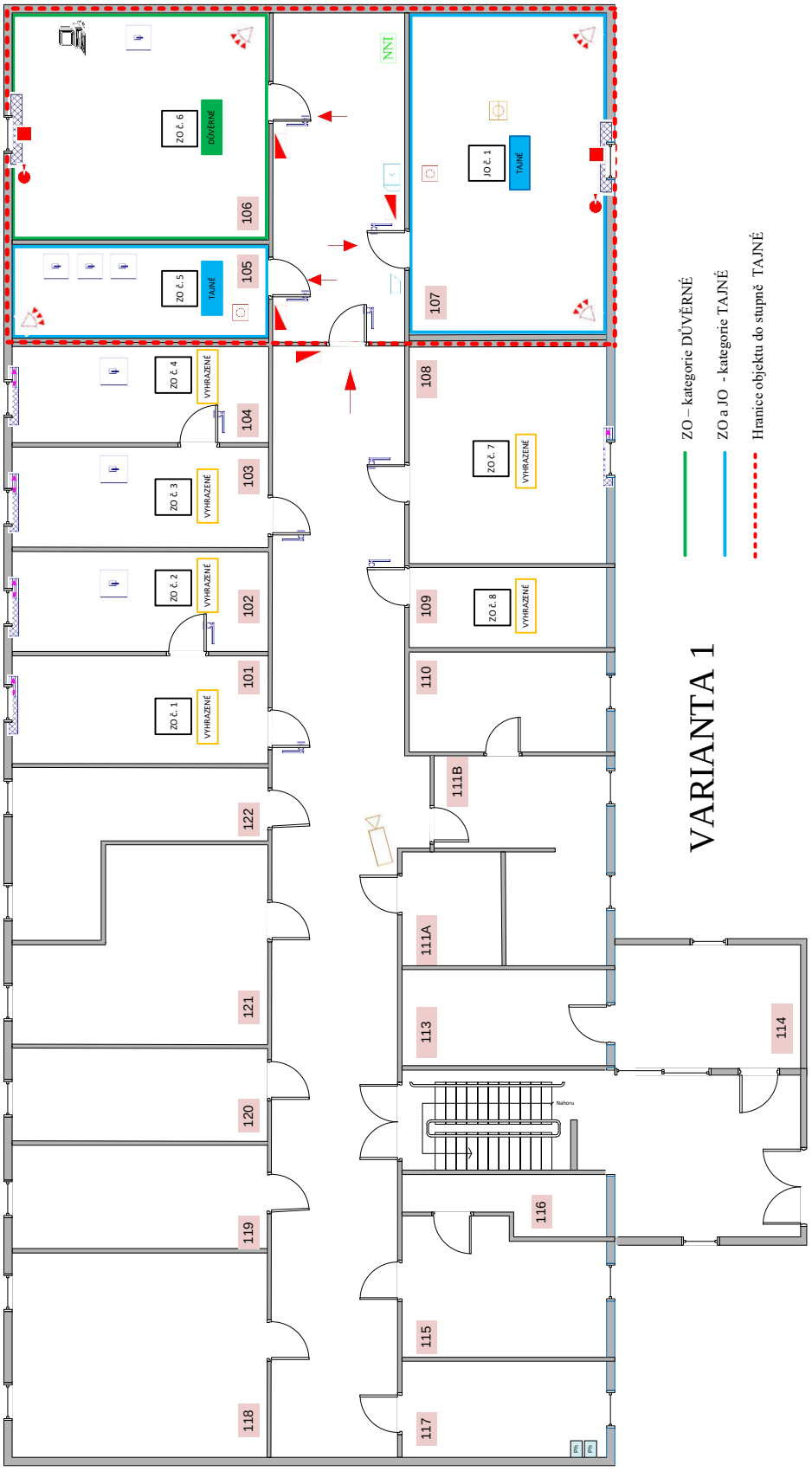
OPE	Zařízení proti pasivnímu a aktivnímu odposlechu UI.
OUI	Ochrana utajovaných informací.
PCO	Pult centralizované ochrany.
PIR	Pasivní infračervený detektor (prostorové čidlo).
PTS	Poplachový tísňový systém.
PZS	Poplachový zabezpečovací systém.
PZTS	Poplachové zabezpečovací a tísnivé systémy.
RMO	Rozkaz ministra obrany.
SKV	Systém kontroly vstupu.
SOD	Stálý operační dozorčí.
UI	Utajovaná informace.
VOC	Velitel organizačního celku.
ZO	Zabezpečená oblast.

SEZNAM OBRÁZKŮ

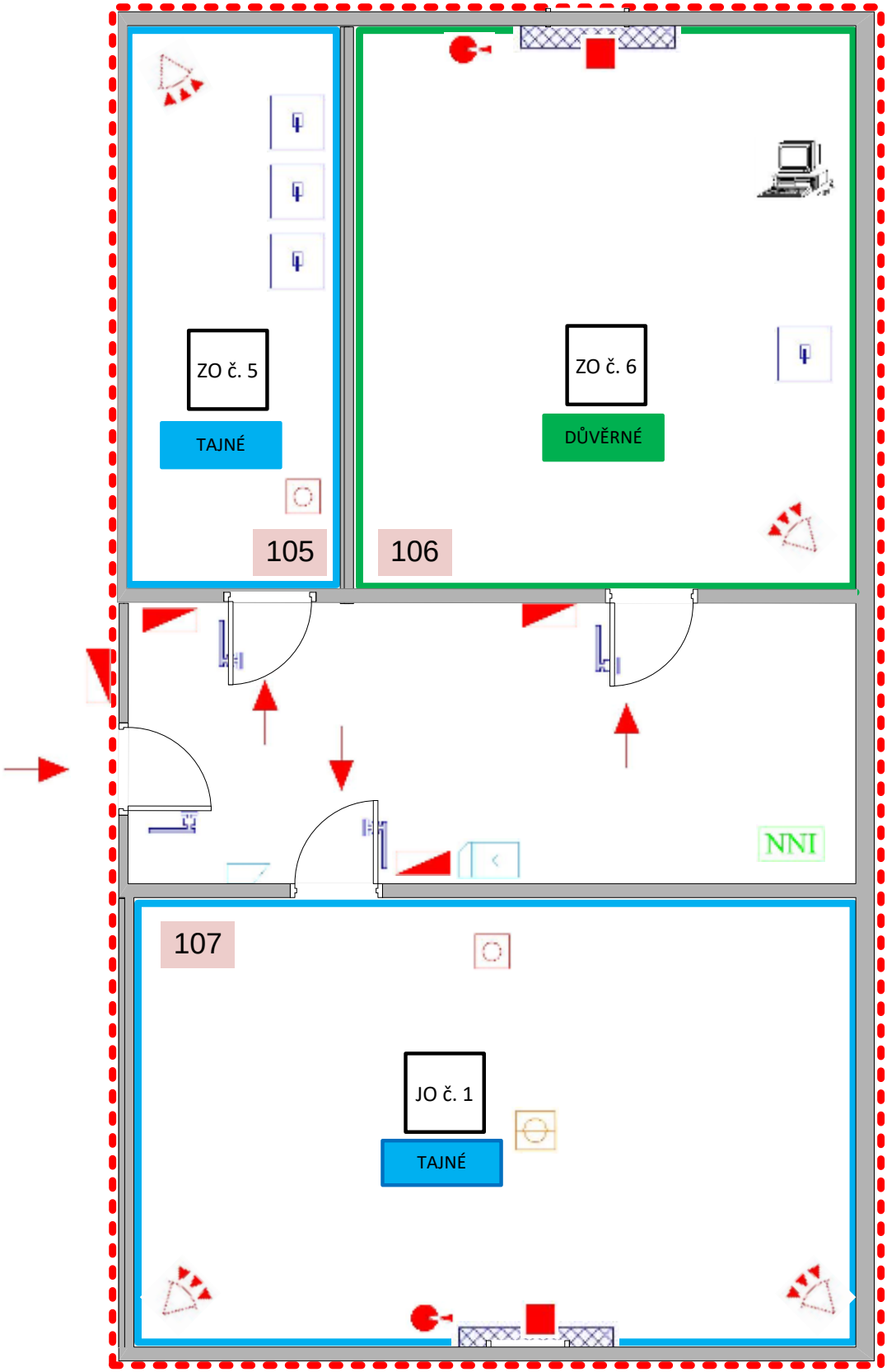
SEZNAM TABULEK

SEZNAM PŘÍLOH

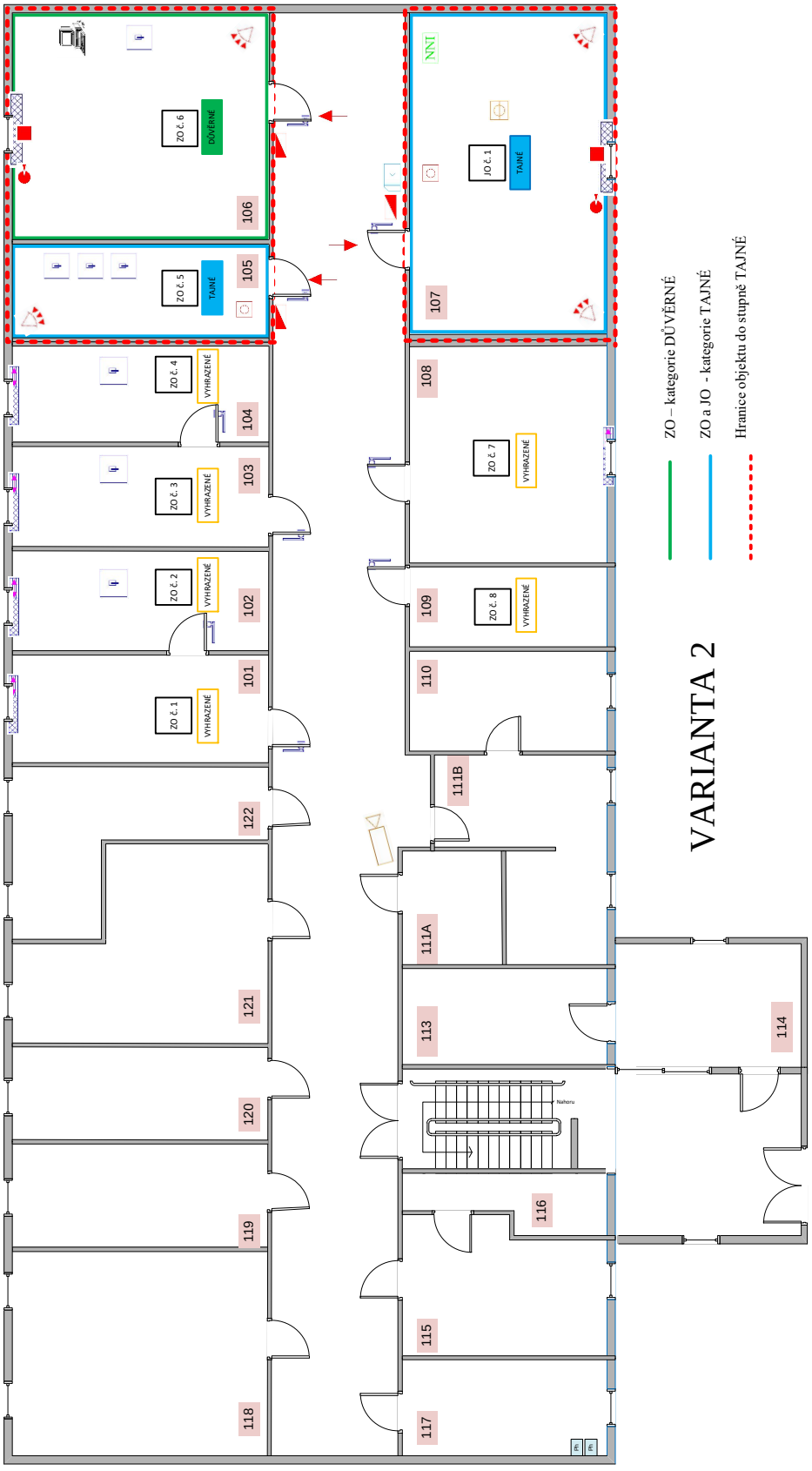
P 1: MODEL - NÁVRH VARIANTY I



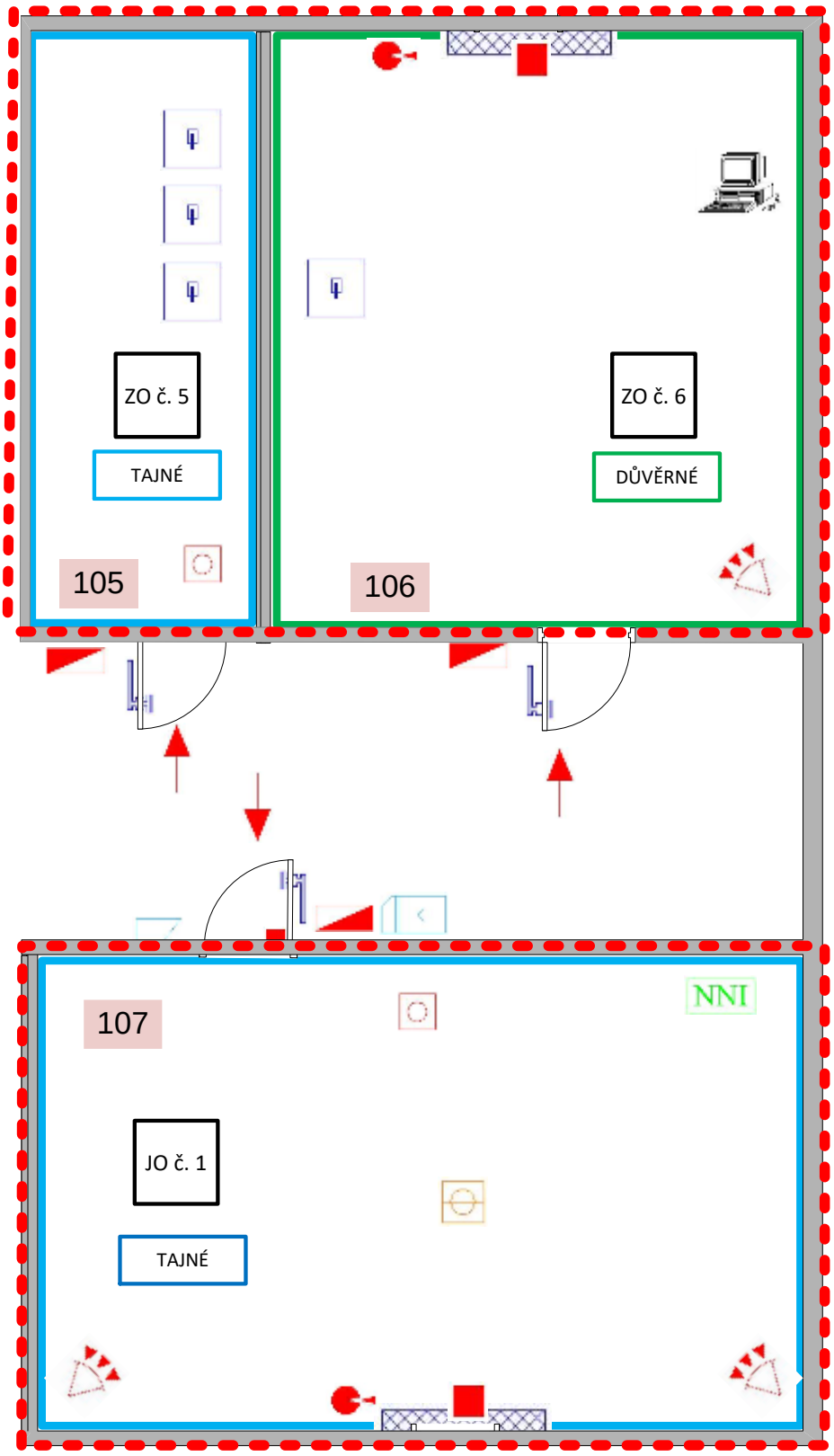
P 2: INSTALACE TECHNICKÝCH PROSTŘEDKŮ VARIANTY I



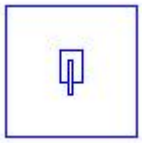
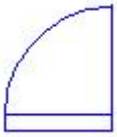
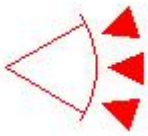
P 3: MODEL - NÁVRH VARIANTY II

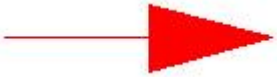


P 4: INTALACE TECHNICKÝCH PROSTŘEDKŮ VARIANTY II



P 5: LEGENDA K TECHNICKÝM PROSTŘEDKŮM

	Úschovný objekt (trezor)
	Bezpečnostní dveře (modré zbarvení linky)
	Bezpečnostní uzamykací systém s kováním v provedení knoflík-klika
	Okno
	Mříž pevná
	Kamera vnitřní
	Zařízení fyzického ničení nosičů informací (skartovací stroj)
	Ovládání klávesnice EZS
	Elektrický zámek
	Požární signalizace
	Tísňový hlásič tlačítkový
	PIR vějíř (čidlo prostorové infrapasivní)

	Čidlo rozbití skla
	Magnetické čidlo otevření
	Bezpečnostní uzamykací systém s kováním v provedení klika-klika
	Optický hlásič kouře
	Odchozí tlačítko
	Tlačítkový hlásič
	Signalizace optická
	Vstup do zabezpečené (jednací) oblasti
	Informační systém nakládající s utajovanými informacemi

P 6: BODOVÉ OHODNOCENÍ ZO-05 KAT. „TAJNÉ“-VARIANTA I

Zabezpečená oblast	Hranice zabezpečené oblasti je v celé své délce shodná s hranicí objektu.			ne	
číslo	ZO 5	**Stupeň utajení PFB:**	Subjekt:	VÚ 1111	**Míra rizika**
kategorie	"T"	neutajovaná	stránka č.:		
třída	II.		z celkem:		střední
označení	Kancelář č.105 v 1.NP budovy 3				
účel	Úložna utajovaných skutečností nebo předmětů, pracoviště s KIS, jednací místnost.				

Bezpečnostní opatření	**Typ**	**Bodové hodnocení**
Úschovný objekt	typ 3	SS1 = 3 body
Zámek úschovného objektu	typ 2	SS2 = 2 body
Celkové hodnocení úschovného objektu a jeho zámku	**= SS1 x SS2**	**S1 = 6 bodů**
Zabezpečená oblast	typ 2	SS3 = 2 body
Uzamykací systém	typ 1	SS4 = 1 bod
Celkové hodnocení místnosti a jejího uzamykacího systému	**= SS3 x SS4**	**S2 = 2 body**
Objekt	nehodnoceno	**S3 = 0 bodů**
Kontrola vstupu	typ 3	SS6 = 3 body
Režim návštěv	s doprovodem	SS7 = 3 body
Celkové hodnocení kontroly vstupu	**= SS6 + SS7**	**S4 = 6 bodů**
Ostraha	typ 3	SS8 = 3 body
Zařízení EZS	typ 3	SS91 = 3 body
Instalace zařízení EZS	typ 3	SS92 = 3 body
mezivýsledek (SS91+SS92)xSS92/OBL/2		SS9 = 3 body
Celkové hodnocení strážní služby a systému EZS	**= SS8 + SS9**	**S5 = 6 bodů**
Fyzické bariéry	nehodnoceno	SS10 = 0 bodů
Kontrola vstupu v přístup.bodech bariéry	není realizována	SS11 = 0 bodů
Namátkové vstupní a výstupní prohlídky	nejsou prováděn	SS12 = 0 bodů
Perimetrický detekční systém (PDS)	není realizován	SS13 = 0 bodů
Bezpečnostní osvětlení perimetru	není realizováno	SS14 = 0 bodů
Kamerový systém CCTV - doplněk perimetru	je realizován	SS15 = 2 body
Celkové hodnocení ochrany perimetru	**=(SS10xSS11)+SS12 +SS13+SS14+SS15**	**S6 = 2 body**
Celkový výsledek		**22 bodů**

Zabezpečená oblast kategorie:		**Dosažené body**	**Míra rizika**		
			malá	**střední**	**velká**
T	Povinné: (S1) + (S2) + (S3)	**8**	8 splněno	9 nesplněno	10 nesplněno
	Povinné: (S4) + (S5)	**12**	4 splněno	5 splněno	5 splněno
	Nepovinné: (S6)	**2**	4	5	5
	Celkový výsledek	**22**	**16 splněno**	**19 nesplněno**	**20 nesplněno**

P 7: BODOVÉ OHODNOCENÍ ZO-06 KAT. „DŮVĚRNÉ“-VARIANTA I

Zabezpečená oblast	Hranice zabezpečené oblasti je v celé své délce shodná s hranicí objektu.			ne	
číslo	ZO 06	**Stupeň utajení PFB:**	Subjekt:	VÚ 1111	**Míra rizika**
kategorie	"D"		stránka č.:		
třída	I.		z celkem:		střední
označení	Kancelář č.106 v 1.NP budovy 3				
účel	Kancelář, uložna utajovaných skutečností nebo předmětů				

Bezpečnostní opatření	Typ	Bodové hodnocení
Úschovný objekt	typ 2	SS1 = 2 body
Zámek úschovného objektu	typ 2	SS2 = 2 body
Celkové hodnocení úschovného objektu a jeho zámku	**= SS1 x SS2**	**S1 = 4 body**
Zabezpečená oblast	typ 2	SS3 = 2 body
Uzamykací systém	typ 1	SS4 = 1 bod
Celkové hodnocení místnosti a jejího uzamykacího systému	**= SS3 x SS4**	**S2 = 2 body**
Objekt	nehodnoceno	**S3 = 0 bodů**
Kontrola vstupu	typ 3	SS6 = 3 body
Režim návštěv	s doprovodem	SS7 = 3 body
Celkové hodnocení kontroly vstupu	**= SS6 + SS7**	**S4 = 6 bodů**
Ostraha	typ 3	SS8 = 3 body
Zařízení EZS	typ 3	SS91 = 3 body
Instalace zařízení EZS	typ 3	SS92 = 3 body
mezivýsledek (SS91+SS92)xSS92/OBL/2		SS9 = 4 body
Celkové hodnocení strážní služby a systému EZS	**= SS8 + SS9**	**S5 = 7 bodů**
Fyzické bariéry	nehodnoceno	SS10 = 0 bodů
Kontrola vstupu v přístup.bodech bariéry	není realizována	SS11 = 0 bodů
Namátkové vstupní a výstupní prohlídky	nejsou prováděny	SS12 = 0 bodů
Perimetrický detekční systém (PDS)	není realizován	SS13 = 0 bodů
Bezpečnostní osvětlení perimetru	není realizováno	SS14 = 0 bodů
Kamerový systém CCTV - doplněk perimetru	je realizován	SS15 = 2 body
Celkové hodnocení ochrany perimetru	**=(SS10xSS11)+SS12 +SS13+SS14+SS15**	**S6 = 2 body**
Celkový výsledek		**21 bodů**

Zabezpečená oblast kategorie:		Dosažené body	Míra rizika		
			malá	střední	velká
D	Povinné: (S1) + (S2) + (S3)	**6**	6 splněno	8 nesplněno	9 nesplněno
	Povinné: (S4) + (S5)	**13**	2 splněno	3 splněno	3 splněno
	Nepovinné: (S6)	**2**	3	3	4
	Celkový výsledek	**21**	**11 splněno**	**14 nesplněno**	**16 nesplněno**

P 8: BODOVÉ OHODNOCENÍ JO-01 ST. UTAJ. „TAJNÉ“-VARIANTA I

Zabezpečená oblast	Hranice zabezpečené oblasti je v celé své délce shodná s hranicí objektu.			ne	
číslo	JO - 01	**Stupeň utajení PFB:**	Subjekt:	VÚ 1111	**Míra rizika**
kategorie	"T"		stránka č.:		
třída	I.		z celkem:		střední
označení	Kancelář č.107 v 1.NP budovy 3				
účel	Jednací místnost				

Bezpečnostní opatření	Typ	Bodové hodnocení
Úschovný objekt	nehodnoceno	SS1 = 0 bodů
Zámek úschovného objektu	nehodnoceno	SS2 = 0 bodů
Celkové hodnocení úschovného objektu a jeho zámku	**= SS1 x SS2**	**S1 = 0 bodů**
Zabezpečená oblast	typ 2	SS3 = 2 body
Uzamykací systém	typ 2	SS4 = 2 body
Celkové hodnocení místnosti a jejího uzamykacího systému	**= SS3 x SS4**	**S2 = 4 body**
Objekt	nehodnoceno	**S3 = 0 bodů**
Kontrola vstupu	typ 3	SS6 = 3 body
Režim návštěv	s doprovodem	SS7 = 3 body
Celkové hodnocení kontroly vstupu	**= SS6 + SS7**	**S4 = 6 bodů**
Ostraha	typ 3	SS8 = 3 body
Zařízení EZS	typ 3	SS91 = 3 body
Instalace zařízení EZS	typ 3	SS92 = 3 body
mezivýsledek (SS91+SS92)xSS92/OBL/2		SS9 = 3 body
Celkové hodnocení strážní služby a systému EZS	**= SS8 + SS9**	**S5 = 6 bodů**
Fyzické bariéry	nehodnoceno	SS10 = 0 bodů
Kontrola vstupu v přístup.bodech bariéry	není realizována	SS11 = 0 bodů
Namátkové vstupní a výstupní prohlídky	nejsou prováděn	SS12 = 0 bodů
Perimetrický detekční systém (PDS)	není realizován	SS13 = 0 bodů
Bezpečnostní osvětlení perimetru	není realizováno	SS14 = 0 bodů
Kamerový systém CCTV - doplněk perimetru	je realizován	SS15 = 2 body
Celkové hodnocení ochrany perimetru	**=(SS10xSS11)+SS12 +SS13+SS14+SS15**	**S6 = 2 body**
Celkový výsledek		**18 bodů**

Zabezpečená oblast kategorie:		Dosažené body	Míra rizika		
			malá	střední	velká
T	Povinné: (S2) + (S3)	4	5 nesplněno	5 nesplněno	6 nesplněno
	Povinné: (S4) + (S5)	12	4 splněno	5 splněno	5 splněno
	Nepovinné: (S6)	2	4	5	5
	Celkový výsledek	**18**	**13 nesplněno**	**15 nesplněno**	**16 nesplněno**

P 9: BODOVÉ OHODNOCENÍ ZO-05 KAT. „TAJNÉ“-VARIANTA II

Zabezpečená oblast	Hranice zabezpečené oblasti je v celé své délce shodná s hranicí objektu.			ne	
číslo	ZO 5	**Stupeň utajení PFB:**	Subjekt:	VÚ 1111	**Míra rizika**
kategorie	"T"	neutajovaná	stránka č.:		
třída	II.		z celkem:		střední
označení	Kancelář č.105 v 1.NP budovy 3				
účel	Úložna utajovaných skutečností nebo předmětů, pracoviště s KIS, jednací místnost.				

Bezpečnostní opatření	Typ	Bodové hodnocení
Úschovný objekt	typ 3	SS1 = 3 body
Zámek úschovného objektu	typ 2	SS2 = 2 body
Celkové hodnocení úschovného objektu a jeho zámku	**= SS1 x SS2**	**S1 = 6 bodů**
Zabezpečená oblast	typ 2	SS3 = 2 body
Uzamykací systém	typ 1	SS4 = 1 bod
Celkové hodnocení místnosti a jejího uzamykacího systému	**= SS3 x SS4**	**S2 = 2 body**
Objekt	nehodnoceno	**S3 = 0 bodů**
Kontrola vstupu	typ 2	SS6 = 2 body
Režim návštěv	s doprovodem	SS7 = 3 body
Celkové hodnocení kontroly vstupu	**= SS6 + SS7**	**S4 = 5 bodů**
Ostraha	typ 3	SS8 = 3 body
Zařízení EZS	typ 3	SS91 = 3 body
Instalace zařízení EZS	typ 3	SS92 = 3 body
mezivýsledek (SS91+SS92)xSS92/OBL/2		SS9 = 3 body
Celkové hodnocení strážní služby a systému EZS	**= SS8 + SS9**	**S5 = 6 bodů**
Fyzické bariéry	nehodnoceno	SS10 = 0 bodů
Kontrola vstupu v přístup.bodech bariéry	není realizována	SS11 = 0 bodů
Namátkové vstupní a výstupní prohlídky	nejsou prováděn	SS12 = 0 bodů
Perimetrický detekční systém (PDS)	není realizován	SS13 = 0 bodů
Bezpečnostní osvětlení perimetru	není realizováno	SS14 = 0 bodů
Kamerový systém CCTV - doplněk perimetru	je realizován	SS15 = 2 body
Celkové hodnocení ochrany perimetru	**=(SS10xSS11)+SS12 +SS13+SS14+SS15**	**S6 = 2 body**
Celkový výsledek		**21 bodů**

Zabezpečená oblast kategorie:		Dosažené body	Míra rizika		
			malá	střední	velká
T	Povinné: (S1) + (S2) + (S3)	**8**	8 splněno	9 nesplněno	10 nesplněno
	Povinné: (S4) + (S5)	**11**	4 splněno	5 splněno	5 splněno
	Nepovinné: (S6)	**2**	4	5	5
	Celkový výsledek	**21**	**16 splněno**	**19 nesplněno**	**20 nesplněno**

P 10: BODOVÉ OHODNOCENÍ ZO-06 KAT. „DŮVĚRNÉ“-VARIANTA II

Zabezpečená oblast	Hranice zabezpečené oblasti je v celé své délce shodná s hranicí objektu.			ne	
číslo	ZO 06	**Stupeň utajení PFB:**	Subjekt:	VÚ 1111	**Míra rizika**
kategorie	"D"		stránka č.:		
třída	I.		z celkem:		střední
označení	Kancelář č.106 v 1.NP budovy 3				
účel	Kancelář, uložna utajovaných skutečností nebo předmětů				

Bezpečnostní opatření	Typ	Bodové hodnocení
Úschovný objekt	typ 2	SS1 = 2 body
Zámek úschovného objektu	typ 2	SS2 = 2 body
Celkové hodnocení úschovného objektu a jeho zámku	**= SS1 x SS2**	**S1 = 4 body**
Zabezpečená oblast	typ 2	SS3 = 2 body
Uzamykací systém	typ 1	SS4 = 1 bod
Celkové hodnocení místnosti a jejího uzamykacího systému	**= SS3 x SS4**	**S2 = 2 body**
Objekt	nehodnoceno	**S3 = 0 bodů**
Kontrola vstupu	typ 2	SS6 = 2 body
Režim návštěv	s doprovodem	SS7 = 3 body
Celkové hodnocení kontroly vstupu	**= SS6 + SS7**	**S4 = 5 bodů**
Ostraha	typ 3	SS8 = 3 body
Zařízení EZS	typ 3	SS91 = 3 body
Instalace zařízení EZS	typ 3	SS92 = 3 body
mezivýsledek (SS91+SS92)xSS92/OBL/2		SS9 = 4 body
Celkové hodnocení strážní služby a systému EZS	**= SS8 + SS9**	**S5 = 7 bodů**
Fyzické bariéry	nehodnoceno	SS10 = 0 bodů
Kontrola vstupu v přístup.bodech bariéry	není realizována	SS11 = 0 bodů
Namátkové vstupní a výstupní prohlídky	nejsou prováděny	SS12 = 0 bodů
Perimetrický detekční systém (PDS)	není realizován	SS13 = 0 bodů
Bezpečnostní osvětlení perimetru	není realizováno	SS14 = 0 bodů
Kamerový systém CCTV - doplněk perimetru	je realizován	SS15 = 2 body
Celkové hodnocení ochrany perimetru	**=(SS10xSS11)+SS12 +SS13+SS14+SS15**	**S6 = 2 body**
Celkový výsledek		**20 bodů**

Zabezpečená oblast kategorie:		Dosažené body	Míra rizika		
			malá	střední	velká
D	Povinné: (S1) + (S2) + (S3)	6	6 splněno	8 nesplněno	9 nesplněno
	Povinné: (S4) + (S5)	12	2 splněno	3 splněno	3 splněno
	Nepovinné: (S6)	2	3	3	4
	Celkový výsledek	**20**	**11 splněno**	**14 nesplněno**	**16 nesplněno**

P 11: BODOVÉ OHODNOCENÍ JO-01 ST. UTAJ. „TAJNÉ“-VARIANTA II

Zabezpečená oblast	Hranice zabezpečené oblasti je v celé své délce shodná s hranicí objektu.			ne	
číslo	JO - 01	**Stupeň utajení PFB:**	Subjekt:	VÚ 1111	**Míra rizika**
kategorie	"T"		stránka č.:		
třída	I.		z celkem:		velká
označení	Kancelář č.107 v 1.NP budovy 3				
účel	Jednací místnost				

Bezpečnostní opatření	Typ	Bodové hodnocení
Úschovný objekt	nehodnoceno	SS1 = 0 bodů
Zámek úschovného objektu	nehodnoceno	SS2 = 0 bodů
Celkové hodnocení úschovného objektu a jeho zámku	**= SS1 x SS2**	**S1 = 0 bodů**
Zabezpečená oblast	typ 2	SS3 = 2 body
Uzamykací systém	typ 2	SS4 = 2 body
Celkové hodnocení místnosti a jejího uzamykacího systému	**= SS3 x SS4**	**S2 = 4 body**
Objekt	nehodnoceno	**S3 = 0 bodů**
Kontrola vstupu	typ 2	SS6 = 2 body
Režim návštěv	s doprovodem	SS7 = 3 body
Celkové hodnocení kontroly vstupu	**= SS6 + SS7**	**S4 = 5 bodů**
Ostraha	typ 3	SS8 = 3 body
Zařízení EZS	typ 3	SS91 = 3 body
Instalace zařízení EZS	typ 3	SS92 = 3 body
mezivýsledek (SS91+SS92)xSS92/OBL/2		SS9 = 3 body
Celkové hodnocení strážní služby a systému EZS	**= SS8 + SS9**	**S5 = 6 bodů**
Fyzické bariéry	nehodnoceno	SS10 = 0 bodů
Kontrola vstupu v přístup.bodech bariéry	není realizována	SS11 = 0 bodů
Namátkové vstupní a výstupní prohlídky	nejsou prováděny	SS12 = 0 bodů
Perimetrický detekční systém (PDS)	není realizován	SS13 = 0 bodů
Bezpečnostní osvětlení perimetru	není realizováno	SS14 = 0 bodů
Kamerový systém CCTV - doplněk perimetru	je realizován	SS15 = 2 body
Celkové hodnocení ochrany perimetru	**=(SS10xSS11)+SS12 +SS13+SS14+SS15**	**S6 = 2 body**
Celkový výsledek		**17 bodů**

Zabezpečená oblast kategorie:		Dosažené body	Míra rizika		
			malá	střední	velká
T	Povinné: (S2) + (S3)	4	5 nesplněno	5 nesplněno	6 nesplněno
	Povinné: (S4) + (S5)	11	4 splněno	5 splněno	5 splněno
	Nepovinné: (S6)	2	4	5	5
	Celkový výsledek	**17**	**13 nesplněno**	**15 nesplněno**	**16 nesplněno**