Ochrana informací v rezortu Ministerstva obrany České republiky

Marcela Minaříková

Bakalářská práce
2019

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav krizového řízení
akademický rok: 2018/2019

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

Jméno a příjmení:	**Marcela Minaříková**
Osobní číslo:	**L16048**
Studijní program:	**B3909 Procesní inženýrství**
Studijní obor:	**Ovládání rizik**
Forma studia:	**kombinovaná**

Téma práce: **Ochrana informací v rezortu Ministerstva obrany České republiky**

Zásady pro vypracování:

1. **Zpracujte rešerši na dané téma s důrazem na monografie, studie a analytické materiály z provenience orgánů státní správy.**
2. **Analyzujte proces ochrany informací v rezortu Ministerstva obrany České republiky.**
3. **Navrhněte opatření k případnému zkvalitnění procesu ochrany informací v předmětném rezortu**
4. **Navrhněte modelové pracoviště pro kvalitní ukládání a zpracovávání utajovaných informací.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

[1] ČESKO. Zákon č. 412 ze dne 21. září 2005 o ochraně utajovaných informací a o bezpečnostní způsobilosti.

[2] STODOLA, J. Filosofie informace – metateoretická anylýza pojmu informace a hlavních paradigmat informační vědy. Brno. Filosofická fakulta, Masarykova univerzita. 2015. ISBN 978-80-210-8011-9.

[3] DRASTICH, M. Systém managementu bezpečnosti informací. Praha. Grada Publishing, a.s.. 2011. ISBN 978-80-247-4251-9.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce:	**doc. RSDr. Václav Lošek, CSc.** Ústav ochrany obyvatelstva
Datum zadání bakalářské práce:	**30. listopadu 2018**
Termín odevzdání bakalářské práce:	**15. května 2019**

V Uherském Hradišti dne 30. listopadu 2018

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta logistiky a krizového řízení

doc. Ing. Zuzana Tučková, Ph.D.
děkanka

Ing. et Ing. Jiří Konečný, Ph.D.
ředitel ústavu

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že:

- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- 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;
- podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

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

V Uherském Hradišti, dne: 15. 5. 2019

Jméno a příjmení studenta: Marcela Minaříková

.....
podpis studenta

ABSTRAKT

Záměrem této bakalářské práce je metodou analýzy zhodnotit současný stav v legislativě týkající se ochrany informací v České republice se zaměřením na proces ochrany informací a kybernetické ochrany v rezortu Ministerstva obrany s důrazem na informace utajované. V případě zjištění nedostatků budou navrhnuta možná řešení. V praktické části bude v návaznosti na vyhodnocení možných hrozeb a stanovení míry rizika vytvořen modelový zabezpečený objekt pro uchovávání a zpracovávání utajovaných informací. Pro tento objekt bude vytvořen projekt fyzické bezpečnosti.

Klíčová slova: informace, utajovaná informace, bezpečnost, riziko, projekt.

ABSTRACT

Intent of this esay is to evaluate by analysis the current status (condition) of the legislative concerning informaton security in the Czech Republic with the focus to the process of information security and cyber security within Ministry of Defence with emphasis on classified information. In the event of shortages, possible measures will be proposed. In the practical part of the esay the model of the secured object will be developed based on the evaluation of possible threats and risks for keeping and processing of classified information. For the object mentioned above a project of the physical security will be developed.

Keywords: information, classified information, safety, risk, project.

OBSAH

ÚVOD

Informace je každodenní nezbytná potřeba člověka. Každodenně získáváme nespočet informací různého charakteru, které pro nás mají odlišnou důležitost a cennost. Cenné a důležité informace se lidstvo od nepaměti snaží uchovávat pro další generace nebo chránit proti konkurenčnímu boji.

V systému státní správy je získávání, ukládání a ochrana informací důležitou zásadou pro zachování funkčnosti a bezpečnosti nejen jednotlivých rezortů, ale hlavně pro zachování bezpečnosti, celistvosti a svrchovanosti celého státu. Rezort Ministerstva obrany získává, zpracovává a uchovává informace důležité pro obranu státu a také informace, vyplývající z členství České republiky v Severoatlantické alianci NATO a EU.

Cílem této práce je analyzovat legislativní dokumenty a bibliografii vztahující se na ochranu informací v České republice se zaměřením na vnitřní předpisy a celkový proces ochrany informací v rezortu Ministerstva obrany. Vzhledem k množství informací a jejich důležitost pro jmenovaný rezort, bude práce převážně zaměřena na proces ochrany utajovaných informací.

V praktické části bude navržen a popsán proces vytvoření modelového zabezpečeného objektu a jeho projektu fyzické bezpečnosti, určeného k zpracování a ukládání utajovaných informací do stupně utajení „Důvěrné“, který bude fiktivně vytvořen v areálu Kasáren Dědice ve Vyškově.

I. TEORETICKÁ ČÁST

1 INFORMACE A JEJÍ HISTORIE

Pojem informace pochází z latinského slova „informatio“, které původně vyjadřovalo utváření něčeho, vrytí, vytesání. Postupem času se začalo používat ve spojení se vznikem myšlenky a v dnešní společnosti má široký rozsah vztahující se téměř ke všemu.

S pojmem informace se lidstvo setkává denně již od dob pravěku. Již pravěcí lidé si byli vědomi důležitostí informací, i když tento pojem vyjadřoval spíše informace spojené s obživou a přežitím. I v této době se tehdejší lidé snažili o uchování získaných informací dalším generacím. Důkazem toho jsou objevené a v některých případech dodnes dochované rytiny v jeskyních znázorňující proces získání ohně, lovu zvěře nebo výrobu jednoduchých nástrojů usnadňující jejich život. S vývojem lidstva se vyvíjel i pojem informace.

Velkým mezníkem bylo objevení písma, které se právě stalo důležitým prostředkem k zaznamenávání, předávání a uchovávání informací.

V každé době si společnost uvědomovala a třídila informace na ty důležité, nedůležité a ty, které je potřeba chránit proti úniku, ať už z důvodu vyzrazení zdroje obživy, tajných receptů nebo z důvodu získání nevýhodnosti při válečných konfliktech. V každé společnosti se tak vytvářel proces ochrany informací. Od střežení jeskyní nebo místností, kde se informace nacházela, přes zachování mlčenlivosti pod výhružkami smrti ke složitějším procesům, jako pečetění dokumentů a vznik základů jednoduchých šifrování, předchůdce dnešní kryptografie. Tímto začali vznikat nové způsoby ochrany informací, ať už to bylo pečetění listin s předávanou informací nebo střežení místností s důležitými informacemi až po šifrování - dnešní kryptografii.

V současné době, kdy se společnost dožaduje stále většího množství informací, se informace – pravdivé i nepravdivé, šíří a předávají celou řadou prostředků, jako například média, internet, sociální sítě a jejich ochrana před zneužitím je s nástupem moderní doby a vzniku „kyberprostoru“ čím dál náročnější a složitější, i když se společnost v závěsu snaží vyvíjet technologie, které by únik informací ztěžovaly a zmírňovaly.

2 ZÁKLADNÍ LEGISLATIVNÍ DOKUMENTY A VYBRANÉ POJMY

Problematika ochrany informací je legislativně řešena třemi zásadními zákony, které nastavují tento proces a dále je upřesňován vyhláškami a prováděcími právními předpisy Národního bezpečnostního úřadu. Pro podmínky rezortu MO je legislativa dále rozšířena o vnitřní předpisy, které rozpracovávají a aplikují danou problematiku do podmínek MO. Níže jsou uvedeny základní legislativní dokumenty.

2.1 Legislativní dokumenty

Zákony české republiky:

- Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů,
- 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,
- Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

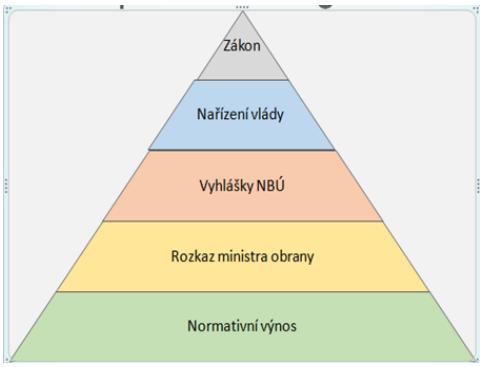
Vyhlášky Národního bezpečnostního úřadu a prováděcí právní předpisy

- 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.,
- Vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor, ve znění vyhlášky č. 453/2011 Sb.,
- Vyhláška č. 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,
- Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam 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.

Vnitřní předpisy MO

- RMO č. 14/2013 ve znění RMO č. 3/2019 Věstníku Ochrana utajovaných informací v rezortu Ministerstva obrany,
- RMO č. 33/2012 ve znění RMO č. 98/2014 Věstníku o personální bezpečnosti v rezortu Ministerstva obrany,
- NV MO č. 85/2013 Věstníku Bezpečnost informačních a komunikačních systémů a elektronických zařízení nakládajících s utajovanými informacemi v rezortu Ministerstva obrany,
- NV MO č. 39/2013 Věstníku Ochrana utajovaných informací před jejich únikem vlivem kompromitujícího vyzařování,
- NV MO č. 111/2013 Věstníku Kryptografická ochrana utajovaných informací v rezortu Ministerstva obrany.



Obrázek 1: Hierarchie legislativních dokumentů

Zdroj: archiv VeV-VA Vyškov

2.2 Vybrané pojmy

Po provedení analýzy výše uvedených legislativních dokumentů a vzhledem k jejich rozsáhlosti uvádím jen výčet základních pojmů, zásadních pro zpracování této práce.

Dle Zákona č. 412 ze dne 21. září 2005, o ochraně utajovaných informací a o bezpečnostní způsobilosti rozumíme níže uvedenými pojmy:

- **utajovanou informací** informace v jakékoliv podobě zaznamenaná na jakémkoliv nosiči označená v souladu s tímto zákonem, jejíž vyzrazení nebo zneužití může

způsobit újmu zájmu České republiky nebo může být pro tento zájem nevýhodné, a která je uvedena v seznamu utajovaných informací,

- **zájmem České republiky** zachování její ústavnosti, svrchovanosti a územní celistvosti, zajištění vnitřního pořádku a bezpečnosti, mezinárodních závazků a obrany, ochrana ekonomiky a ochrana života nebo zdraví fyzických osob,
- **odpovědnou osobou** - subjekt, který je v oblasti ochrany utajovaných informací zodpovědný za výkon určitých opatření, je mu zákonem svěřeno plnění povinností plynoucích z ustanovení zákona. Je-li zřízena funkce bezpečnostního ředitele, je tento přímo podřízen odpovědné osobě,
- **původcem utajované informace** orgán státu, právnická osoba nebo podnikající fyzická osoba u níž utajovaná informace vznikla,
- **cizí mocí** cizí stát nebo jeho orgán anebo nadnárodní nebo mezinárodní organizace nebo její orgán,
- **neoprávněnou osobou** fyzická nebo právnická osoba, která nesplňuje podmínky přístupu
  k utajované informaci stanovené tímto zákonem,
- **poučením** písemný záznam o seznámení fyzické osoby s jejími právy a povinnostmi v oblasti ochrany utajovaných informací a s následky jejich porušení. [9]

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 stanovil ve svém rozkaze č. 14/2013 ze dne 25. února 2013, ve znění Rozkazu Ministra obrany č. 3/2019 níže uvedené pojmy:

- **technickým zařízením** vojenský materiál, který je definován v § 2 písm. k) vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 454/2011 Sb., a § 30 odst. 1 vyhlášky č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací,
- **nosičem utajované informace** – dokument, technické zařízení nebo jeho část, která obsahuje utajovanou informaci,
- **informačním systémem v rezortu Ministerstva obrany** – jeden nebo více počítačů, jejich programové vybavení, periferní zařízení, správa systému, personální obsluha, procesy nebo prostředky, které tvoří celek schopný sbírat, tvořit, zpracovávat, ukládat, zobrazovat nebo přenášet utajované informace včetně kryptografických prostředků používaných pro daný informační systém,

- **komunikačním systémem v rezortu Ministerstva obrany** – systém, který zajišťuje přenos utajovaných informací mezi koncovými uživateli. Zahrnuje koncové komunikační zařízení, přenosové prostředí, prostředky kryptografické ochrany, správu systému, personální obsluhu a provozní podmínky a postupy,
- **elektronickým zařízením** – zařízení, které umožňuje kopírování, záznam, zobrazení nebo převod utajované informace, není součástí informačního nebo komunikačního systému,
- **akreditací** – strukturovaný proces založený na výsledcích hodnocení dílčích oblastí bezpečnosti informací, v rámci něhož se formálně rozhoduje o tom, zda implementace informačního nebo komunikačního systému nebo jejich propojení je ve shodě s vnitřními předpisy rezortu Ministerstva obrany a certifikovanou bezpečnostní dokumentací informačního systému nebo schválenou bezpečnostní dokumentací komunikačního systému,
- **bezpečnostním ředitelem** – bezpečnostní ředitel Ministerstva obrany-ředitel odboru bezpečnosti, který je výkonným orgánem ministra obrany pro oblast ochrany utajovaných informací,
- **gestorem systému** – vedoucí organizačního celku, který odpovídá za celý životní cyklus utajovaného informačního nebo komunikačního systému včetně jejich bezpečnosti,
- **organizačním celkem** – organizační celek ve smyslu Organizačního řádu Ministerstva obrany;[1]
- **zaměstnancem** – zaměstnanec ve smyslu Organizačního řádu Ministerstva obrany;
- **vedoucím organizačního celku** – představený nebo vedoucí zaměstnanec ve smyslu Organizačního řádu Ministerstva obrany, který řídí organizační celek.[2] **Chyba! enalezen zdroj odkazů.**

2.2.1 Stupně utajení

Pro klasifikování utajené informace jsou stanoveny níže uvedené stupně utajení:

[1] Organizačním celkem se v rezortu MO označuje: Vojenský útvar, Vojenské zařízení apod.

[2] Vedoucím organizačního celku je např. velitel vojenského útvaru, ředitel vojenského zařízení.

a) Přísně tajné (PT) - jestliže by vyzrazení takto klasifikované informace neoprávněné osobě nebo její jiné zneužití mohlo způsobit mimořádně vážnou újmu zájmům České republiky,

b) Tajné (T) - jestliže by vyzrazení takto klasifikované informace neoprávněné osobě nebo její jiné zneužití mohlo způsobit vážnou újmu zájmům České republiky,

c) Důvěrné (D), jestliže by vyzrazení takto klasifikované informace neoprávněné osobě nebo její jiné zneužití mohlo způsobit prostou újmu zájmům České republiky,

d) Vyhrazené (V), jestliže by vyzrazení takto klasifikované informace neoprávněné osobě nebo její jiné zneužití mohlo být nevýhodné pro zájmy České republiky. [9]

Přísně tajné	**Mimořádně vážná újma**
Tajné	**Vážná újma**
Důvěrné	**Prostá újma**
Vyhrazené	**Nevýhodnost**

Tabulka 1: Závislost stupně utajení na újmu zájmu České republiky

Zdroj: Zákon č. 412/2005o ochraně utajovaných informací a o bezpečnostní způsobilosti, upraveno autorem

3 ORGÁNY ZASTŘEŠUJÍCÍ OCHRANU INFORMACÍ

3.1 Národní bezpečnostní úřad (NBÚ)

Národní bezpečnostní úřad je ústředním správním úřadem pro oblast ochrany utajovaných informací a oblast bezpečnostní způsobilosti. Byl zřízen dnem 1. srpna 1998, tehdy platným zákonem č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů. Nyní se řídí platným Zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. Pro Českou republiku je NBÚ hlavním orgánem státní správy pro zabezpečení oblasti ochrany utajovaných informací v souladu se závazky vyplývajícími z členství České republiky v Evropské unii, Organizaci Severoatlantické smlouvy a z mezinárodních smluv, kterými je Česká republika vázána. [11]

Hlavními úkoly NBÚ zejména je:

- rozhodování o vydání osvědčení fyzické osoby („Důvěrné“, „Tajné“, Přísně tajné“ a Osvědčení cizí moci), osvědčení podnikatele a o vydání dokladu o bezpečnostní způsobilosti fyzické osoby a o zrušení platnosti osvědčení fyzické osoby, osvědčení podnikatele a dokladu,
- plnění úkolů v oblasti ochrany utajovaných informací v souladu se závazky vyplývajícími z členství České republiky v Evropské unii, Organizaci Severoatlantické smlouvy a z mezinárodních smluv, jimiž je Česká republika vázána,
- ve stanovených případech povoluje poskytování utajovaných informací v mezinárodním styku, vede ústřední registr a schvaluje zřízení registrů,
- provádí výkon kontroly a ukládá sankce za nedodržení povinností stanovených zákonem. [11]

3.2 Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB)

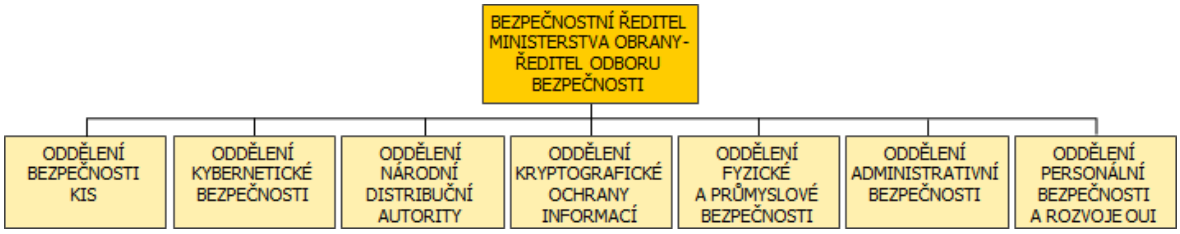
NÚKIB vznikl dne 1. srpna 2017 Zákonem č. 205/2017 Sb., kterým se změnil Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) a je ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů kryptografické ochrany. Je správním orgánem a zajišťuje problematiku v oblasti kybernetické bezpečnosti, ochrany utajovaných informací, kryptografickou ochranu a oblast informačních

a komunikačních systémů. Dále se zastřešuje problematiku veřejně regulované služby navigačního systému Galileo (PRS).

V čele úřadu stojí ředitel, který se pravidelně účastní jednání Bezpečnostní rady státu a je stálým pracovním členem Výboru pro kybernetickou bezpečnost. [11]

3.3 Odbor bezpečnosti Ministerstva obrany

Odbor bezpečnosti MO odpovídá za plnění úkolů stanovených zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), a zákonem č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů. Dále odpovídá za nastavení systému řízení bezpečnosti informací včetně kontroly jeho dodržování, ochrany určených neutajovaných informací a kybernetické bezpečnosti v rezortu Ministerstva obrany. V čele odboru bezpečnosti Ministerstva obrany stojí bezpečnostní ředitel-ředitel odboru bezpečnosti. Odbor má sedm oddělení zabezpečující jednotlivé oblasti ochrany informací.



Obrázek 2: Organizační struktura OB MO

Zdroj: Odbor bezpečnosti Ministerstva obrany

4 BEZPEČNOST INFORMACÍ V REZORTU MINISTERSTVA OBRANY (MO)

Ochrana informací v resortu Ministerstva obrany (MO) se řídí a aplikuje zákony platné pro Českou republiku, vyhláškami Národního bezpečnostního úřadu, jeho prováděcími právními předpisy a vnitřními předpisy MO. Je souborem pro realizaci systémových opatření personální, administrativní, průmyslové a fyzické bezpečnosti, bezpečnosti informačního systému, komunikačního systému a elektronických zařízení a kryptografické ochrany. V rezortu MO je ustanoven bezpečnostní ředitel, který mimo jiné odpovídá za zabezpečení součinnosti rezortu Ministerstva obrany s Národním bezpečnostním úřadem, Národním úřadem pro kybernetickou a informační bezpečnost a ostatními správními úřady v oblasti ochrany utajovaných informací. **Chyba! Nenalezen zdroj odkazů.**

Bezpečnost informací v rezortu MO je organizována a řízena v souladu se základní kategorizací informací:

- **utajované informace** – klasifikované dle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti,
- **určené neutajované informace** – neklasifikované informace, označení je určeno vnitřními předpisy rezortu MO, předání mimo rezort je realizováno pouze datovou schránkou
- **veřejné informace** – informace určené ke zveřejnění

Ochrana utajovaných informací je souladu se zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů v rezortu MO zajišťována v následujících oblastech:

- **personální bezpečností**
- **průmyslovou bezpečností**,
- **administrativní bezpečností**
- **fyzickou bezpečností**,
- **bezpečností informačních nebo komunikačních systémů**
- **kryptografickou ochranou**
- **kybernetickou ochranou**

4.1 Personální bezpečnost

Personální bezpečnost je primárně zaměřena na výběr, výchovu a obranu fyzických osob, které mají mít přístup k utajovaným informacím. Tyto osoby musí splňovat podmínky a být prověřeny na určitý stupeň utajení NBÚ, kromě prověření na stupeň utajení Vyhrazené, které za splnění níže uvedených podmínek vydává VOC.

4.1.1 Podmínky fyzických osob pro seznamování se s jednotlivými stupni utajení

Způsob a rozsah ověřování podmínek, které musí fyzická osoba splnit, aby jí byl umožněn přístup k utajované informaci, se liší podle stupňů utajení, k nimž má mít fyzická osoba přístup. [11]

4.1.2 Seznamování se s UI se stupněm utajení Vyhrazené („V)

Osvědčení fyzický osoby pro seznamování se se stupněm utajení Vyhrazené („V“) vydává VOC a fyzická osoba musí doložit a splňovat:

- svéprávnost (prokazuje se prohlášením fyzické osoby o svéprávnosti),
- věk minimálně 18 let (dokládá se občanským průkazem nebo cestovním dokladem),
- bezúhonnost (dokládá se výpisem z evidence Rejstříku trestů, který nesmí být starší 3 měsíců). [9]

Na základě splnění výše uvedených podmínek vydá VOC „Oznámení o splnění podmínek pro přístup k utajované informaci stupně utajení Vyhrazené“, které VOC vlastnoručně podepíše, vyhotoví kopii, kterou založí do spisu[3] zaměstnance spolu s prohlášením fyzické osoby o svéprávnosti a výpisem z evidence Rejstříku trestů poučením zaměstnanci. Originál oznámení předá zaměstnanci.

Zaměstnanec má dále povinnost:

- písemně oznamovat vedoucímu organizačního celku všechny změny údajů obsažené v podkladových materiálech, a to do 15 dnů ode dne, kdy změna nastala včetně odcizení (ztráty, poškození) oznámení a požádat o vydání nového oznámení**,**
- písemně oznámit obdržení osvědčení fyzické osoby nebo dokladu[4],

[3] Příloha č. 1

[4] Vydá NBÚ

- odevzdat do 15 dnů oznámení vedoucímu organizačního celku, u kterého je služebně nebo pracovně zařazen:
  - zanikla-li platnost oznámení, protože zaměstnanec přestal splňovat podmínky pro jeho vydání,
  - skončil-li jeho služební nebo pracovní poměr v rezortu Ministerstva obrany;
  - po obdržení písemného vyrozumění o zániku platnosti oznámení z důvodu nepředložení podkladových materiálů k ověření splnění podmínek pro vydání oznámení,
  - obdržel-li osvědčení fyzické osoby nebo doklad,
  - jednou ročně se zúčastnit proškolení z právních předpisů v oblasti ochrany utajovaných informací,
- prokazovat se originály oznámení (doklad) a poučení. [15]

4.1.3 Seznamování se s UI se stupněm utajení Důvěrné („D“), Tajné („T“) a Přísně tajné („PT“)

Ověření pro výše uvedené stupně provádí Národní bezpečnostní úřad (dále jen NBÚ). Vyplněnou a řádně odůvodněnou žádost o vydání osvědčení fyzické osoby odevzdává zaměstnanec za účelem potvrzení vedoucímu organizačního celku, který ji zašle bezpečnostnímu řediteli Ministerstva obrany-řediteli odboru. Po potvrzení žádosti bezpečnostním ředitelem zahájí zaměstnanec žádost o prověření s NBÚ.

Žadatel musí NBÚ dle zákona č. 412/2005 Sb., poskytnout následující podklady:

- prohlášení o svéprávnosti,
- prohlášení k osobnostní způsobilosti,
- prohlášení o zproštění povinnosti mlčenlivosti,
- věcně a místně příslušného správce daně a jiné osoby zúčastněné na správě daní podle § 52 odst. 2 daňového řádu, a to v plném rozsahu údajů za účelem provedení bezpečnostního řízení,
- aktuální fotografie 35 x 45 mm,
- vyplněný dotazník fyzické osoby v listinné i elektronické podobě. [11]

K žádosti rovněž doloží následující písemnosti:

- rodný nebo křestní list, popřípadě další obdobné doklady,
- potvrzení zaměstnavatele o příjmech s uvedením jejich výše po odečtení povinných zákonných odvodů (čistý příjem),

- v případě jiného druhu příjmu daňové přiznání. [11]

Zaměstnanec je povinen požádat NBÚ o potvrzení přijetí žádosti fyzické osoby a do 8 dnů, od obdržení, jej předložit VOC.

Vedoucí organizačního celku vyhotoví z předloženého potvrzení přijetí žádosti fyzické osoby 3 kopie. Jednu kopii zašle do 5 dnů odboru bezpečnosti Ministerstva obrany, druhou předá příslušnému personálnímu orgánu, třetí si ponechá a přijetí žádosti fyzické osoby NBÚ zaznamená v přehledu služebních míst a seznamu osob poučených pro styk s utajovanými informacemi.

Po prověření zaměstnance a vydání osvědčení fyzické osoby jej zaměstnanec odevzdá nejpozději do 8 dnů od doručení VOC, který ho zaměstnanci vrátí po zhotovení jeho kopie a provede poučení zaměstnance. [15]

4.1.4 Platnost osvědčení fyzické osoby dle zákona č. 412/2005 Sb.

- pro stupeň **Důvěrné** 9 let,
- pro stupeň **Tajné** 7 let,
- pro stupeň **Přísně tajné** 5 let od data vydání.

4.1.5 Osvědčení cizí moci

Česká republika vstoupila dne 12. března 1999 do Severoatlantické aliance NATO a dnem 1. května 2004 do Evropské unie (EU), čímž se ČR mino jiné zavázala dodržovat zásady ochrany utajovaných informací těchto organizací. Jednou z hlavních zásad je, aby se s utajovanou informací mohyly seznamovat a mít k ní přístup pouze osoby, které byly prověřeny NBÚ a bylo jim vydáno osvědčení příslušné cizí moci a potřebují tyto informace při výkonu své funkce nebo plní úkol, při kterém je nutné, aby se s těmito informacemi seznámily.

4.1.6 Utajované informace EU

Utajované informace EU jsou klasifikovány čtyřmi stupni utajení a označují se:

- **TRÈS SECRET UE/EU TOP SECRET** – informace a materiály, jejichž neoprávněné vyzrazení by mohlo výjimečně závažně poškodit základní zájmy Evropské unie nebo jednoho či více členských států,
- **SECRET UE** – informace a materiály, jejichž neoprávněné vyzrazení by mohlo vážně poškodit základní zájmy Evropské unie nebo jednoho či více členských států,

- **CONFIDENTIEL UE** – tento stupeň se použije pro informace a materiály, jejichž neoprávněné vyzrazení by mohlo poškodit základní zájmy Evropské unie nebo jednoho či více členských států,
- **RESTREINT UE** – informace a materiály, jejichž neoprávněné vyzrazení by mohlo být nevýhodné pro zájmy Evropské unie nebo jednoho či více členských států.

4.1.7 Utajované informace NATO

Pokud je fyzická osoba určená k seznamování se s dokumenty NATO, které jsou neutajované, pošle žádost NBÚ a uvede důvod, proč se s daným dokumentem potřebuje seznámit. Při potřebě seznámit se s dokumentem označeným stupně utajení NATO CONFIDENTIAL a vyšším, musí být s určenou osobou provedena NBÚ bezpečnostní prověrka.

Utajované informace NATO jsou také klasifikovány do čtyřmi stupni utajení a označují se:

- **COSMIC TOP SECRET (CTS)** – neoprávněné vyzrazení takto označené informace nebo materiálu by způsobilo NATO mimořádně vážnou škodu,
- **NATO SECRET (NS)** – neoprávněné vyzrazení takto označené informace nebo materiálu by způsobilo NATO vážnou škodu,
- **NATO CONFIDENTIAL (NC)** – neoprávněné vyzrazení takto označené informace nebo materiálu by poškodilo zájmy NATO,
- **NATO RESTRICTED (NR)** – neoprávněné vyzrazení takto označené informace nebo materiálu by bylo pro zájmy nebo působnost NATO nevýhodné.

Dokumenty, které nejsou utajovány, jsou označovány **NATO UNCLASSIFIED**.

V případě potřeby utajování dokumentů, které se týkají oblasti zbraní hromadného ničení, je tato informace označována **ATOMAL**.

4.1.8 Další povinnosti VOC k zabezpečení personální bezpečnosti

Vedoucí organizačního celku (dále VOC) je povinen jednou ročně zajistit zpracování personálního záměru, ve kterém jsou uvedeny funkce a požadavek na prověření určitého stupně utajení, které musí zaměstnanec splňovat při výkonu dané funkce. Dále je VOC odpovědnou osobou, která je povinna zabezpečit proškolení zaměstnanců, kteří jsou určeni k seznamování se s utajovanými informacemi. Školení musí být realizováno jednou ročně a VOC je povinen vést záznamy o proškolení. [11]

- plnění úkolů v oblasti ochrany utajovaných informací v souladu se závazky vyplývajícími z členství České republiky v Evropské unii, Organizaci Severoatlantické smlouvy a z mezinárodních smluv, jimiž je Česká republika vázána,
- ve stanovených případech povoluje poskytování utajovaných informací v mezinárodním styku, vede ústřední registr a schvaluje zřízení registrů,
- provádí výkon kontroly a ukládá sankce za nedodržení povinností stanovených zákonem. [11]

4.2 Průmyslová bezpečnost

Prováděcím předpisem pro oblast průmyslové bezpečnosti je vyhláška č. 526/2005 Sb. o stanovení vzorů používaných v oblasti průmyslové bezpečnosti a o seznamech písemností
a jejich náležitostech nutných k ověření splnění podmínek pro vydání osvědčení podnikatele a o způsobu podání žádosti podnikatele (vyhláška o průmyslové bezpečnosti), ve znění vyhlášky č. 11/2008 Sb.
V rezortu MO je problematika průmyslové bezpečnosti řešena v ojedinělých případech a vzhledem k rozsahu této práce nebude dále analyzována.

4.3 Administrativní bezpečnost

Administrativní bezpečnost zastřešuje celou řadu opatření, která jsou nutná při práci s utajovaným dokumentem ať v listinné nebo nelistinné podobě. Zahrnuje tvorbu, zpracování, příjem, odesílání, ukládání, přepravu, přenášení, skartační řízení a archivaci dokumentu. [11]
Pro potřeby MO jsou definovány činnosti a vztahy v RMO č. 14/2013 Věstníku, Ochrana utajovaných informací v rezortu Ministerstva obrany, které jsou dále podrobněji rozpracovány a upřesněny podrobnosti vedení evidence, převzetí, předání, ukládání, ničení a manipulace s dokumentem obsahujícím utajovanou informaci v souladu s vyhláškou č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací, ve znění pozdějších předpisů ve NV MO č. 8/2018.

4.3.1 Základní ustanovení

Vyhláškou č. 529 ze dne 15. prosince 2005, o administrativní bezpečnosti a o registrech utajovaných informací je stanoveno:

- způsob vyznačování náležitostí na utajované informaci v listinné a nelistinné podobě,
- druhy administrativních pomůcek, jejich náležitosti a organizační a technické poža-

davky na jejich vedení, a rozsah podkladových materiálů stupně utajení Vyhrazené k utajované informaci stupně utajení Vyhrazené,

- náležitosti souhlasu k pořizování opisu, kopie, výpisu a překladu utajovaného dokumentu, způsob vyznačování náležitostí na nich a způsob pořizování výpisu,
- podrobnosti k přepravě, přenášení, převzetí a zapůjčování utajovaného dokumentu a k další manipulaci s tím související, včetně organizačního zajištění těchto činností, požadavků na přenosné schránky a obaly a vyznačování příslušných náležitostí na nich,
- organizaci a činnost ústředního registru, registru, pomocného registru a činnost kontrolního bodu, obsah písemné žádosti o zřízení registru, podmínky zřízení, obsah

  a způsob vedení registru a rozsah změn v registru, oznamovaných Národnímu bezpečnostnímu úřadu,
- způsob označování a postupy při manipulaci s kryptografickým materiálem stanoví vyhláška o zajištění kryptografické ochrany utajovaných informací. [8]

4.3.2 Vymezení základních pojmů

Vyhláškou 529/2005 Sb. o administrativní bezpečnosti a o registrech utajovaných informací ve znění pozdějších předpisů je definováno:

- **zásilkou** utajovaný dokument vybavený k přepravě, přepravovaný nebo doručený na místo určení do ukončení její přepravy a jejího otevření,
- **přepravou zásilky** její dopravení mimo objekt[5] orgánu státu, právnické osoby nebo podnikající fyzické osoby za účelem jejího doručení adresátovi,
- **přenášením utajovaného dokumentu** jeho dopravení mimo objekt orgánu státu, právnické osoby nebo podnikající fyzické osoby, jehož účelem není doručení,
- **přenosnou schránkou** jakýkoliv druh aktovky, kufříku, kufru, přenosné bezpečnostní schránky nebo kurýrního vaku, který je při přepravě nebo přenášení utajovaného dokumentu zajištěn proti neoprávněné manipulaci s jejím obsahem, například

[5] Objektem je budova nebo jiný ohraničený prostor, ve kterém se zpravidla nachází zabezpečená oblast nebo jednací oblast. [9]

uzamčením mechanickým nebo kódovým zámkem nebo pečetěním, plombováním a opatřen na vhodném místě názvem a adresou orgánu státu, právnické osoby nebo podnikající fyzické osoby a nápisem: "V případě nálezu neotevírejte a předejte neprodleně útvaru Policie ČR nebo Národnímu bezpečnostnímu úřadu!",

- **originálem utajovaného dokumentu** výtisk utajovaného dokumentu doručeného nebo výtisk utajovaného dokumentu vzniklého, uvedený v rozdělovníku,
- **spisem spojení dokumentů týkajících se téže věci**; spis může dále vzniknout spojením sběrného archu s dokumenty, kterým bylo přiděleno číslo jednací nebo evidenční označení ze samostatné evidence, nebo spojením sběrných archů. [8]

NV MO č. 8/2018 je dále stanoveno:

- **organizačním celkem** – organizační celek ve smyslu RMO č. 22/2017 Věstníku, Zásady tvorby organizační struktury a vnitřní systemizace organizačních celků rezortu Ministerstva obrany, organizační útvar Ministerstva obrany jako služebního úřadu přímo podřízený ministrovi obrany a Úřad pro obrannou standardizaci, katalogizaci a státní ověřování jakosti,
- **utajovaným dokumentem v listinné podobě** - dokument v listinné podobě obsahující utajovanou informaci,
- **utajovaným dokumentem v nelistinné podobě** - dokument v digitální podobě obsahující utajovanou informací,
- **čistopisem utajovaného dokumentu** - prvopis nebo stejnopis prvopisu[6] utajovaného dokumentu. [16]

4.3.3 Evidence a označování utajovaného dokumentu

Při vytvoření vlastního utajovaného dokumentu musí být náležitosti předepsané Vyhláškou č. 529/2005 Sb. Záhlaví dokumentu musí být označeno názvem subjektu MO, číslem jednacím utajovaného dokumentu (Čj.), stupeň utajení, datum vzniku a místo, číslo výtisku, počet listů, počet utajovaných a neutajovaných příloh v listinné podobě a počet jejich listů, případně počet a druh utajovaných a neutajovaných příloh v nelistinné podobě. Výše uve-

[6] Prvopisem je originální dokument zaznamenávající projev vůle osoby, který je osvědčen jejím vlastnoručním podpisem nebo obdobným autentizačním prvkem stanoveným jiným právním předpisem

dené údaje se uvedou na čelní straně dokumentu, počet příloh a počet jejich stran se uvedou jako zlomek, kdy čitatele je počet příloh a jmenovatelem celkový počet jejich listů.[7] Pokud jsou přílohy v nelistinné podobě, uvede se stejným vyjádřením počet příloh a jejich podoba.[8]

Na utajovaném dokumentu se mohou vyznačit i další potřebné údaje.

Přílohy k utajovanému dokumentu se označují v pravém horním rohu prvního listu číslem jednacím dokumentu, kterého jsou přílohou a to textem „Příloha č. .. k čj….“ Pokud je příloha neutajovaná, uvede se „Neutajovaná příloha č. k čj….“. [8]

Veškeré UI, v působnosti OC, se evidují v jednacím protokolu. Za evidenci odpovídá osoba, kterou tímto pověřil vedoucí OC.

Označování dokumentů cizí moci je popsáno v kapitole 4.1.2.

4.4 Fyzická bezpečnost

Fyzickou bezpečnost vytváří systém opatření, která mají neoprávněné osobě zabránit nebo ztížit přístup k utajovaným informacím, popřípadě přístup nebo pokus o něj zaznamenat. Pro zabezpečení ochrany utajovaných informací v rámci fyzické bezpečnosti se určují objekty, zabezpečené oblasti a jednací oblasti, ke kterým jsou zpracovávány projekty fyzické bezpečnosti. [11]

Způsob a rozsah upravuje vyhláška č. 528/2005 Sb. ze dne 14. prosince 2005 o fyzické bezpečnosti a certifikaci technických prostředků, kterou je definováno:

- **objektem** budova nebo jiný ohraničený prostor, ve kterém se zpravidla nacházejí zabezpečené nebo jednací oblasti,
- **hranicí objektu** plášť budovy, fyzická bariéra (oplocení) nebo jinak viditelně vymezená hranice,
- **hranicí zabezpečené oblasti nebo jednací oblasti** stavebně nebo jinak viditelně ohraničený prostor,
- **vstupem do objektu, zabezpečené oblasti nebo jednací oblasti** místo určené pro vstup a výstup osob a místo určené pro vjezd a výjezd dopravních prostředků,

[7] Počet příloh: 7/15

[8] Počet příloh: 2/1 + 1 CD

- **dopravními prostředky** pozemní, podzemní, vzdušné a vodní prostředky určené k přepravě osob, předmětů a materiálu,
- **hrozbou** možnost vyzrazení nebo zneužití utajované informace při narušení fyzické bezpečnosti,
- **rizikem** pravděpodobnost, že se určitá hrozba uskuteční,
- **mimořádnou situací** stav, kdy bezprostředně hrozí, že dojde k vyzrazení nebo zneužití utajované informace,
- **technickým prostředkem** bezpečnostní prvek, jehož použitím se zabraňuje, ztěžuje, oznamuje nebo zaznamenává narušení zabezpečení ochrany objektu, zabezpečené oblasti nebo jednací oblasti, a dále ničí utajované informace,
- **úschovným objektem** trezor nebo jiná uzamykatelná schránka stanovená v příloze č. 1 této vyhlášky,
- **technickým zařízením** vojenský materiál[9] zejména elektronická, fototechnická, chemická, fyzikálně-chemická, radiotechnická, optická a mechanická vojenská technika a vojenská výzbroj, který obsahuje utajovanou informaci. [7]

4.4.1 Objekt

Objektem je budova nebo část budovy, ve které se nachází jedna nebo více zabezpečených popřípadě jednacích oblastí.

4.4.2 Zabezpečená oblast

Zabezpečená oblast slouží k ukládání utajované informace, která se ukládá v trezoru nebo jiné uzamykatelné schránce. Zabezpečené oblasti se řadí do kategorií a to podle nejvyššího stupně utajení utajované informace, která se v nich ukládá (Přísně tajné, Tajné, Důvěrné, nebo Vyhrazené). Zabezpečené oblasti se podle toho, jestli při vstupu dochází k seznámení s utajovanou informací, dále dělí do dvou tříd. Třída I, kdy vstupem do zabezpečené oblasti dochází k seznámení s utajovanou informací (např. vyvěšené utajované mapy) a třída II., kdy vstupem do zabezpečené oblasti nedochází k seznámení s utajovanou informací. [11]

[9] Dle § 2 odst. 7 zákona č. 219/1999 Sb., o ozbrojených silách České republiky, ve znění pozdějších předpisů Vojenský materiál tvoří vojenská výstroj, vojenská výzbroj, vojenská technika a určená technická zařízení, které jsou užívány k plnění nebo zabezpečení úkolů ozbrojených sil.

4.4.3 Zabezpečení zabezpečené oblasti

Zabezpečená oblast musí být zabezpečována v závislosti na její kategorii, třídě a vyhodnocení rizik těmito technickými prostředky:

- **pro kategorii Vyhrazené** - mechanické zábranné prostředky,
- **pro kategorii Důvěrné** - mechanické zábranné prostředky a zařízení elektrické zabezpečovací signalizace,
- **pro kategorii Tajné a Přísně tajné** - mechanické zábranné prostředky, systémy pro kontrolu vstupů, zařízení elektrické zabezpečovací signalizace, speciální televizní systémy, zařízení elektrické požární signalizace. Speciální televizní systémy lze nahradit tísňovými systémy. Při použití speciálních televizních systémů nesmí být narušena ochrana utajovaných informací. [7]

4.4.4 Jednací oblast

Utajovanou informaci stupně utajení Přísně tajné nebo Tajné lze pravidelně projednávat pouze v jednací oblasti. Zabezpečení zabezpečené a jednací oblasti a objektu je zajišťováno kombinací opatření fyzické bezpečnosti, které jsou ostraha, režimová opatření a technické prostředky. Výkon ostrahy, rozsah použití opatření fyzické bezpečnosti a rozsah použití technických prostředků se stanoví v závislosti na stupni utajovaných informací a na vyhodnocení rizik v projektu fyzické bezpečnosti. Pro ochranu utajovaných informací se používají certifikované nebo necertifikované technické prostředky v závislosti na kategorii a vyhodnocení rizik. [11]

Vyhláškou č. 528/2005 Sb. je stanoveno, že pravidelné projednávání UI probíhá v jednací oblasti. Není však upřesněno, o jaký interval se jedná. Z logiky věci lze tedy soudit, že pravidelnost se dá stanovit z intervalu mezi dvěma posledními jednáními.

4.4.5 Zabezpečení jednací oblasti

Zabezpečení jednací oblasti je zajišťováno kombinací opatření fyzické bezpečnosti a musí být zabezpečeno:

Režimové opatření, které stanoví:

- oprávnění osob a dopravních prostředků pro vstup do objektu, stanovení oprávnění osob pro vstup do zabezpečené oblasti a jednací oblasti a způsob kontroly těchto oprávnění,
- kontrolní opatření při vstupu do objektu, zabezpečených a jednacích oblastí a způsob kontroly těchto opatření,

- podmínky a způsob kontroly pohybu osob v objektu, zabezpečené oblasti a jednací oblasti a způsob kontroly a vynášení utajovaných informací z objektu, zabezpečené oblasti a jednací oblasti,
- režim manipulace s klíči a identifikačními prostředky, zejména způsob jejich označování, přidělování, úschovy a evidence,
- režim manipulace s technickými prostředky a jejich používání,
- režim pohybu utajovaných informací v objektu, zabezpečené oblasti a jednací oblasti. [7]

V příloze č. 1 Vyhlášky 528/2005 Sb. o fyzické bezpečnosti a certifikaci technických prostředků, je stanoveno bodové hodnocení jednotlivých režimových opatření, součtem musí být splněny podmínky fyzické bezpečnosti pro jednotlivé kategorie utajovaných informací.

4.4.6 Certifikace technických prostředků

Certifikací technických prostředků pro ochranu utajovaných informací se rozumí posouzení technických parametrů výrobků a zařízení používaných k ochraně utajovaných informací

a vystavení certifikátu na základě odborného posudku odborného pracoviště, který zahrnuje certifikát shody od certifikačního orgánu.

NBÚ vydává certifikáty na následující technické prostředky:

- mechanické zábranné prostředky,
- elektrická zámková zařízení a systémy pro kontrolu vstupů,
- zařízení elektrické zabezpečovací signalizace,
- tísňové systémy,
- zařízení fyzického ničení nosičů informací nebo dat. [11]

4.5 Bezpečnost informačních nebo komunikačních systémů

Bezpečnost informačních nebo komunikačních systémů zahrnuje systém opatření, jehož cílem je zajištění bezpečného nakládání s utajovanými informacemi ukládanými nebo zpracovávanými v těchto systémech. Prováděcím předpisem je vyhláška č. 523/2005 Sb. o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor a v rezortu MO dále upřesněna pro podmínky rezortu RMO č. 14/2013 Ochrana utajovaných informací

v rezortu Ministerstva obrany a NV MO 85/2013 Věstníku Bezpečnost informačních a komunikačních systémů a elektronických zařízení nakládajících s utajovanými informacemi v rezortu Ministerstva obrany.

4.5.1 Základní pojmy definované rozkazem Ministra obrany č. 14/2013

- **nosičem utajované informace** – dokument, technické zařízení nebo jeho část, která obsahuje utajovanou informaci,
- **informačním systémem v rezortu Ministerstva obrany** – jeden nebo více počítačů, jejich programové vybavení, periferní zařízení, správa systému, personální obsluha, procesy nebo prostředky, které tvoří celek schopný sbírat, tvořit, zpracovávat, ukládat, zobrazovat nebo přenášet utajované informace včetně kryptografických prostředků používaných pro daný informační systém,
- **komunikačním systémem v rezortu Ministerstva obrany** – systém, který zajišťuje přenos utajovaných informací mezi koncovými uživateli. Zahrnuje koncové komunikační zařízení, přenosové prostředí, prostředky kryptografické ochrany, správu systému, personální obsluhu a provozní podmínky a postupy,
- **elektronickým zařízením** – zařízení, které umožňuje kopírování, záznam, zobrazení nebo převod utajované informace, není součástí informačního nebo komunikačního systému. [14]

4.5.2 Cíle a strategie bezpečnosti systémů

Hlavním cílem bezpečnosti systémů je ochrana aktiv, stanovení odpovědnosti uživatele za jeho činnost v systému a minimalizace rizika selhání v oblasti důvěrnosti, integrity a dostupnosti informací. Veškeré nosiče, které utajovanou informaci obsahují, musí být dostatečně chráněny. Utajované informace lze uchovávat nebo zpracovávat pouze v certifikovaných systémech.

4.5.3 Zajištění bezpečnosti při využívání IKS

Bezpečnost KIS se uplatňuje v závislosti na stupni utajení informací a předpokládaným hrozbám, kterým jsou vystaveny a ty musí být touto bezpečností trvale pokryty. Hrozby dělíme do tří základních skupin a to:

- **vnitřní hrozby** – hrozby zapříčiněné chybou uživatele, ať už úmyslnou nebo neúmyslnou, které mají za příčinu ztrátu, zničení, modifikaci, nebo kompromitaci dat,

- **vnější hrozby** – hrozby způsobené náhodně nebo úmyslně neautorizovaných osobou,
- **nepředvídané hrozby** – hrozby, které nelze předvídat (např. živelná pohroma, technická závada).

Jednotlivá bezpečnostní opatření v rámci systému se realizují takovým způsobem a v takových oblastech, aby se dosáhlo dostatečné bezpečnosti s optimálními náklady a minimálním omezením požadovaných funkčních vlastností systému.

Veškerá aktiva systému využívají pouze oprávnění uživatelé a pouze k účelům, které souvisejí s plněním jejich pracovních nebo služebních úkolů.

4.6 Kryptografická ochrana

Kryptografii můžeme popsat, jako metodu převodu zpráv, do takové podoby, že jejich přečtení vyžaduje speciální znalost.

4.6.1 Počátky šifrování

Vznik šifrování sahá do doby několika tisíciletí před našim letopočtem, kdy začali vznikat první jednoduché šifry, které sloužili především při válečných konfliktech. 2. století před našim letopočtem sestavil řecký voják a historik Polybios první účinný kód s universálním použitím pro posílání optických vzkazů na větší vzdálenost, který se nejspíše stal nezbytným komunikačním nástrojem v Římské říši. O dvě staletí dříve vynalezl Řek Aeneas typ telegrafu, jehož text se ale neuchoval. [1] Postupem se přidávali další vynálezci šifer, které se stávali složitější, a hůř se k nim hledal klíč. Dnes tenhle obor nazýváme kryptografií.

V novodobé historii se stal velkým mezníkem v šifrování stroj Enigma, který v roce 1918 vynalezl Němec Arthur Scherbius a dodnes je považován za jeden z nejslavnějších šifrovacích strojů v dějinách. Enigma byla nejdříve využívána v civilním sektoru, poté v námořnictvu a během druhé světové války se stala klíčovým prvkem pro zasílání šifrovaných depeší v německé armádě. Navzdory dokonalému propracování způsobu šifrování zpráv, byla Enigma pokořena a její klíč šifrování byl polskými, britskými a francouzskými rozvědkami, které si k tomuto najímali matematiky, křížovkáře, šachisty, prolomení. Velkou měrou však svými chybami a stereotypním nastavováním klíčů k prolomení přispěli samotní Němci. [10]

Obrázek 3: Šifrovací stroj Enigma

Zdroj: https://www.shutterstock.com/cs/image-photo/bletchley-england-june-21-2015-enigma-719004586?src=mvuy5A3Sjk15uIrtOdtwyw-1-0

4.6.2 Proces kryptografické bezpečnosti

Zajištění kryptografické bezpečnosti je v rezortu Ministerstva obrany realizováno v souladu se Zákonem č. 412/2005 Sb., Vyhláškou č. 432/2011 Sb. a NV MO č. 111/2013 a je tvořena systémem opatření na ochranu UI použitím:

- kryptografických metod a
- kryptografických materiálů při zpracování, přenosu nebo ukládání UI.

Prostředky, které jsou využívány pro kryptografickou ochranu, musí být certifikovány národním bezpečnostním úřadem.

V rezortu MO je kryptografická realizována vyškoleným pracovníkem a kryptografické prostředky mají svůj režim zabezpečení v souladu s výše uvedenou legislativou.

4.7 Kybernetická bezpečnost

Kybernetika je vědním oborem, který se zabývá obecnými principy řízení a přenosu informací ve strojích, živých organismech a společenstvích.

Kybernetické útoky využívají pokročilých metod a jsou podrobně plánované s jasným a trvalým cílem. Rozsah těchto cílených útoků proti informačním a komunikačním technologiím přesahuje národní a přesouvá se do globálního měřítka.

Přijetím Zákona č. 181/2014 Sb. o kybernetické bezpečnosti byl vytvořen zásadní mezník ve vnímání kybernetické bezpečnosti a došlo tak ke zkvalitňování budování opatření pro zabezpečení kybernetické ochrany. Samotný vznik Národního úřadu pro kybernetickou a informační bezpečnost svědčí o snaze kybernetickým útokům v co nejvyšší možné míře zamezit.

4.7.1 Důležité pojmy

Zákonem č. 181/2014 Sb. o kybernetické bezpečnosti jsou stanoveny následující pojmy

- **kybernetickým prostorem** digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací,
- **kritickou informační infrastrukturou** prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti,
- **bezpečností informací** zajištění důvěrnosti, integrity a dostupnosti informací,
- **významným informačním systémem** informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci,
- **správcem informačního systému** orgán nebo osoba, které určují účel zpracování informací a podmínky provozování informačního systému,
- **správcem komunikačního systému** orgán nebo osoba, které určují účel komunikačního systému a podmínky jeho provozování,
- **provozovatelem informačního nebo komunikačního systému** orgán nebo osoba zajišťující funkčnost technických a programových prostředků tvořících informační nebo komunikační systém a významnou sítí síť elektronických komunikací zajišťující přímé zahraniční propojení do veřejných komunikačních sítí nebo zajišťující přímé připojení ke kritické informační infrastruktuře. [20]

4.7.2 Kybernetické hrozby

Kybernetické hrozby lze rozdělit:

- na útoky kriminálních skupin a jednotlivců, s motivací získání finančního obnosu, kdy je většinou používáno vydírání nebo „nabourání“ bankovnictví jiné osoby,

- na útoky státních aktérů, kde se většinou jedná o špionáž zájmových osob nebo organizací, průmyslovou špionáž nebo útoky na infrastrukturu,
- teroristických skupin, které takto šíří nábor do svých skupin a získávají finanční zdroje.

4.7.3 Organizace zajištění kybernetické bezpečnosti v rezortu MO

V rezortu MO musí být zajišťován efektivní systém pro kybernetickou bezpečnost a kybernetickou obranu komunikační a informační infrastruktury - vlastní části kybernetického prostoru, toto zajišťují níže uvedené organizace.

- **Rada pro kybernetickou bezpečnost MO**, která vznikla v roce 2010 a je vrcholový orgánem pro řízení systému a orgánů kybernetické obrany. Je hlavní poradní a koordinační orgán ministra obrany v oblasti kybernetické obrany a kontaktním orgánem pro národní autoritu odpovědnou za kybernetickou bezpečnost České republiky

Předsedou rady je bezpečnostní ředitel MO, členové zastupují složky rezortu MO.

- **Centrum CIRC**, které je jedním z hlavních organizačních prvků MO pro zabezpečení kybernetické ochrany je, které je organizační strukturou zařazeno pod Agenturu komunikačních a informačních technologií (AKIS). Jeho úkolem identifikace a odhalování bezpečnostních hrozeb a incidentů. CIRC nepřetržitě monitoruje důležitých segmenty datových sítí rezortu a provádí jejich analýzu, vyhodnocování a předávání získaných informací. Dále připravuje protiopatření, nástroje a postupy k rychlé reakci na bezpečnostní hrozby, pomáhá k ochraně dat v informačních systémech a technických prostředků v rezortu MO. Je aktivním prostředkem napomáhajícím k šetření kybernetických incidentů.

V rezortu obrany jsou zpracovány koncepční a strategické dokumenty, ve kterých jsou zapracovány požadavky, vize a z toho vyplývající povinnosti a úkoly pro rezort MO v návaznosti na plnění závazků vyplývajících z členství České republiky v Severoatlantické alianci NATO a EU. V posledních letech se výrazně zkvalitnilo i interní vzdělávání vlastního personálu v této oblasti.

II. PRAKTICKÁ ČÁST

5 PROJEKT FYZICKÉ BEZPEČNOSTI

5.1 Vyhodnocení rizik

Vyhodnocení rizik a stanovení jejich míry je v souladu s vyhláškou 528/2005 Sb. a déle v souladu s čl. 3 interního předpisu NV MO č. 77/2013, povinnost vedoucí organizačního celku.

5.2 Specifikace aktiv

- aktivem pro organizační celek jsou utajované dokumenty v listinné i nelistinné podobě,
- manipulace probíhá nepravidelně
- u OC se budou vyskytovat utajované informace vlastní nebo poskytnuté zpravidla spolupracujícími subjekty v rámci resortu Ministerstva obrany,
- nejvyšším stupněm utajení v OC budou informace se stupněm utajení Důvěrné.

Stupeň utajení informace	**Předpokládaný počet UI za rok**
Vyhrazené	120
Důvěrné	90
Tajné	0
Přísně tajné	0

Tabulka 2: Předpokládáný počet aktiv u OC

Zdroj: autor

5.3 Vyhodnocení zajímavosti UI

- zajímavost pro cizí zpravodajské služby – nízká
- zajímavost pro terorizmus – nízká
- zajímavost pro jiné skupiny (politické, náboženské apod.) - nízká

5.4 Stanovení jednotlivých hrozeb a jejich vyhodnocení

Pro navržení modelového objektu pro ukládání a zpracovávání utajovaných informací je důležité stanovení a vyhodnocení možných hrozeb pro únik nebo zneužití utajovaných informací a předejitím již v prvopočátku.

5.4.1 Hrozba neoprávněného nakládání s UI poučenými osobami.

Poučené osoby si plní povinnosti vůči utajovaným informací dle Zákona č. 412/2005 Sb. o ochranné utajovaných informací. Vzhledem k úmyslnému nebo neúmyslnému selhání lidského faktoru může nejčastěji dojít k:

- ztrátě utajované informace,
- neúmyslnému vyzrazení neoprávněné osobě,
- úmyslnému vyzrazení neoprávněné osobě za účelem osobního nebo finančního prospěchu,
- chybnému označení stupněm utajení,
- neoprávněnému pořizování kopií.

Eliminaci těchto rizik lze předcházet prověřením osob určených k seznamování se s utajovanými informacemi a jejich řádné proškolení v oblasti nakládání s UI.

Provedením analýzy četnosti těchto hrozeb v resortu MO byla míra rizika vyhodnocena jako nízká až střední.

5.4.2 Hrozba neoprávněného nakládání s UI neoprávněnou osobou

Vzhledem k režimu ochrany informací v rezortu MO a téměř nemožnému přístupu neoprávněné osoby k UI, byla tato hrozba vyhodnocena jako mírná, avšak vzhledem k působení lidského faktoru ji nelze zcela vyloučit. Při posuzování hroby byly vnímány následující rizika:

- selhání lidského faktoru a úmyslné vyzrazení UT,
- neoprávněné vynášení UI ze zabezpečeného objektu a její ztráta,
- neoprávněný vstup do zabezpečené oblasti,
- násilné vniknutí neoprávněné osoby do zabezpečené oblasti,
- odcizení UI při přenášení nebo přepravě.

5.4.3 Hrozba teroristického útoku

Hrozba úniku UI z rezortu MO byla posouzena vzhledem k historické absenci této události, jako žádná až mírná. V případě zhoršení bezpečnostní situace v České republice by však byla hrozba reálná a hodnocená vyšším stupněm rizika.

5.4.4 Hrozba ztráty UI vlivem přírodních katastrof a technických závad

Ztrátou UI vlivem přírodních katastrof je myšleno její nenávratné poškození UI vlivem přírodních živlů. Nejčastěji hrozí:

- vznik požáru a shoření UI,
- povodně a zničení UI zatopením,

- poničení zabezpečené oblasti silným větrem.

Této hrozbě lze předcházet výběrem vhodného objektu pro ukládání a zpracovávání UI. Pokud je to možné, objekt volit ve větší vzdálenosti od vodních toků, volit objekt s pevnou a nezchátralou konstrukcí. Největší pravděpodobností vzniku této hrozby je vznik požáru, který může být způsoben selháním technického vybavení budovy (například závada na elektroinstalaci) nebo selháním lidského faktoru (například kouření na nepovolených místech, práce s otevřeným ohně). Proti požáru je nutné objekt vybavit příslušnými prostředky požární ochrany, požárními směrnicemi, personál řádně proškolit v oblasti prevence požární ochrany. Míra rizika je stanovena jako střední.

5.4.5 Hrozba zneužití UI pasivním odposlechem nebo nasazením operativní techniky

Hrozba cíleného nebo náhodného odposlechu nebo pozorování je vzhledem k umístění budovy malá. V zabezpečené oblasti bude provedena prohlídka proti nasazenému odposlechu. Dále bude této hrozbě předcházeno důkladným dodržováním režimových opatření.

5.4.6 Hrozba vyzrazení nebo ztráty UI únikem z informačního systému

Hrozba úniku UI zpracovávaných v elektronické podobě, zničení nebo poškození dat charakteru UI, podmíněné snadným kopírováním nebo neoprávněným vstupem do IS nebo počítačové sítě je vzhledem k nutnosti používání certifikovaných zařízení s příslušným stupněm utajení hodnocena jako mírná.

5.4.7 Stanovení celkové míry rizika

Na základě provedené analýzy a vyhodnocení možných hrozeb byla míra rizika vyhodnocena jako mírná.

Hodnocená hrozba	Stanovená míra rizika	Možné opatření
Hrozba neoprávněného nakládání s UI poučenými osobami	Střední	Důkladné prověření zaměstnanců a jejich řádné proškolení
Hrozba neoprávněného nakládání s UI neoprávněnou osobou	Mírná	Zabezpečení režimu vstupu do objektu a zabezpečené oblasti, zvýšení fyzické a personální ochrany, důsledné plnění zásad při přenášení a přepravě UI.
Hrozba teroristického útoku	Mírná	Vyžadování včasných a úplných zpravodajských informací o hrozbě teroristického útoku.
Hrozba ztráty UI vlivem přírodních katastrof nebo technických závad	Střední	Vhodný a uvážený výběr objektu pro ukládání a zpracovávání UI, řádná prevence požární ochrany personálu a vybavení objektu protipožární ochrany.
Hrozba zneužití UI pasivním odposlechem nebo nasazením operativní techniky	Mírná	Výběr budovy, ke které není snadný přístup a možné pozorování z prostorů mimo areál, prohlídka zabezpečené oblasti
Hrozba vyzrazení nebo ztráty UI únikem z informačního systému	Mírná	Pro zpracování utajovaných informací používat pouze certifikované informační systémy

Tabulka 3: Přehled vyhodnocovaných hrozeb

Zdroj: autor

5.5 Určení objektu a zabezpečených oblastí včetně jejich hranic určení kategorií, tříd zabezpečených oblastí

5.5.1 Popis areálu Kasáren Dědice

Areál Kasáren Dědice se nachází v severozápadní části města Vyškova. V areálu působí několik organizačních celků MO. Velitelství výcviku-Vojenská Akademie je jednou z největších organizačních složek sídlící v areálu. Zabezpečuje výuku a výcvik nejen nově zrekrutovaným vojákům, ale i vojákům, kteří zde absolvují nejrůznější kurzy. Dále jsou zde pořádány konference, semináře, porady atd. Kumulace osob v tomto areálu je proto každodenně velká. Většina budov, které jsou využívány převážně jako učebny, ubytovací prostory, kanceláře a sklady, je zděných a byly postaveny v 80-tých letech 20. století. K areálu vede jedna příjezdová cesta, která dále pokračuje do Vojenského výcvikového prostoru (dále jen VVP). Podél této komunikace jsou dva vstupy do areálu tzv. brána „JIH“ a brána „SEVER“, které jsou střeženy nepřetržitě a slouží ke vstupu a vjezdu zaměstnanců a návštěv.

Obrázek 4: Areál Kasáren Dědice

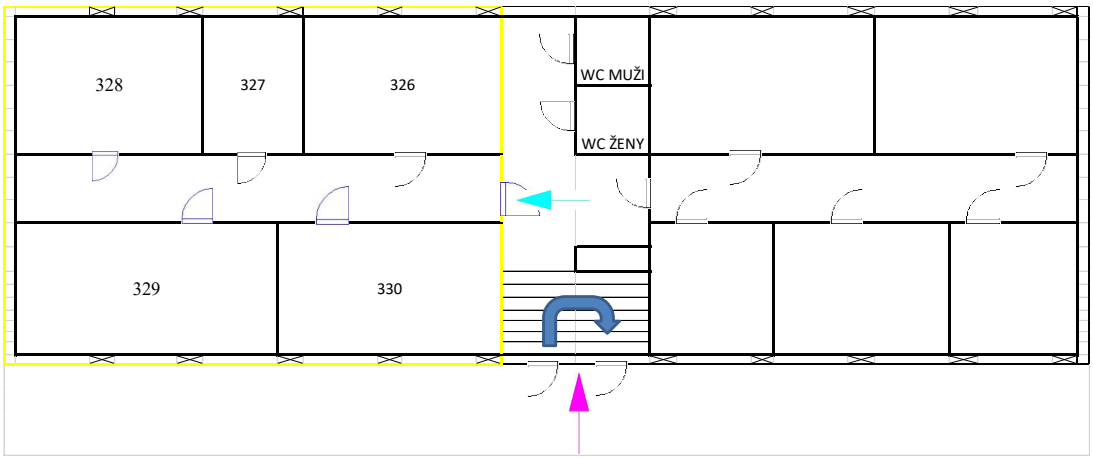
Zdroj: https://www.google.cz/maps

5.5.2 Popis budovy

Pro vytvoření modelového objektu pro ukládání a zpracování utajovaných informací byla vzhledem k vyhodnocen analýzy rizik a jejich eliminaci, zvolena budova, která byla pro tyto potřeby označen jako budova A, konkrétně část třetího nadzemního podlaží této budovy. Budova se nachází zhruba ve středu areálu Kasáren Dědice. Z velké části je obklopena dalšími budovami areálu a je v dostatečné vzdálenosti do hlavní komunikace a jiných cizích subjektů, což významně snižuje riziko zneužití UI vlivem kompromitujícího vyzařování. Budova je čtyřpatrová, zděná s plastovými okny a rovnou střechou. Do budovy vede jeden vstup, který se po pracovní době zamyká a pečetí.

5.5.3 Popis objektu stanovení hranice, bezpečnostní opatření

Objekt bude vybudován v části třetího nadzemního podlaží uvedené budovy. Vstup do patra je po středovém schodišti nebo výtahem.



Obrázek 5: Ohraničení zabezpečeného objektu s vyznačenými vstupy

Zdroj: autor

5.5.4 Identifikace zabezpečených oblastí a jednacích oblastí

V zabezpečeném objektu bude vybudována zabezpečená oblast a to pro stupně utajení Vyhrazené a Důvěrné. Jelikož zabezpečená oblast bude sloužit pro ukládání a manipulaci s dokumenty do stupně utajení Důvěrné a při vstupu do zabezpečené oblasti nebude docházet k seznámení s utajovanými informacemi, byla zabezpečená oblast zařazena do **kategorie Důvěrné, třídy II**.

5.6 Způsob použití prostředků fyzické bezpečnosti a technických prostředků

5.6.1 Úschovné objekty

Pro ukládání utajovaných dokumentů bude instalován jeden úschovný **objekt typu 1C** a to mobilní skříňový trezor ROOBUS Office 21, certifikovaný NBÚ, který splňuje bezpečnostní požadavky třídy Z3 dle platné normy ČSN 91 6012, který je vybaven certifikovaným uzamykacím systémem.

S1 = 3 body

5.6.2 Zabezpečená oblast

Zabezpečenou oblastí se stupněm utajení Důvěrné je místnosti č. 329, v ostatních místnostech zabezpečené oblasti jsou kanceláře pracovníků, kteří jsou určeni k seznamování se s utajenými informacemi. Zabezpečenou oblast tvoří ze dvou stran vyztužené betonové panely o minimální tloušťce 150 mm, které jsou zároveň opláštěním budovy a ze dvou stran stěny vystavěné z cihel o tloušťce minimálně 100 mm. Průlezné otvory jsou v minimální výšce nad 5,5 m a nelze se k nim lehce dostat z jiné části budovy, např. ze střechy, okapů, hromosvodu nebo z jiné místnosti po parapetu. Vstup do zabezpečené oblasti je zabezpečen bezpečnostními dveřmi s označením AD/RC2, certifikované NBÚ a dle normy ČSN EN 1627 splňují třídu bezpečnosti RC 2. Na základě výše uvedené analýzy zabezpečené oblasti byla vyhodnocena jako:

Zabezpečená oblast typ 2

Bodové hodnocení: SS3 = 2 body

5.6.3 Uzamykací systémy určené k uzamykání ZO

Bezpečnostní dveře zabezpečené oblasti jsou vybaveny bezpečnostním kováním ROSTEX R3 bezpečnostní cylindrickou vložkou FAB 3000 Hd. Uzamykací systém a jeho komponenty jsou certifikovány NBÚ a splňují dle ČSN EN 1627 požadavky bezpečnostní třídy RC 3.

Uzamykací systém typ 2

Bodové hodnocení: SS4 = 2 body

Celkové bobové hodnocení zabezpečené: S2 = SS3xSS4 = 4

5.6.4 Hranice objektu

Stropy, podlahy a stěny mají nepoškozenou pevnou stavební konstrukci z cihel a betonových panelů. Hranice objektu jsou ze tří částí zároveň opláštění budovy, které je tvořené vyztuženými betonovými panely o minimální tloušťce 150mm. Jednu hranici tvoří příčka oddělující chodbu od schodiště a zabezpečený objekt, která je vyzděna. Objekt se nachází ve 3. np, tudíž jsou průlezné otvory (okna) výšce vyšší než 5,5 m nad terénem m a nelze se k nim lehce dostat z jiné části budovy, např. ze střechy, okapů, hromosvodu nebo z jiné místnosti po parapetu, stromů apod. Na základě výše uvedeného tento objekt vyhodnocen jako:

Objekt typ 3

Bodové hodnocení: S3 = 3 body

5.6.5 Kontrola vstupu

Vstup do zabezpečené oblasti i objektu je vybaven certifikovaným systémem kontroly vstupu COLNOD 5. Systém splňuje požadavky ČSN EN 60839-11-1 a k přístupu je používán identifikační prvek, čímž je čipová karta a PIN.

Systém kontroly vstupu typ 2

Bodové hodnocení: SS6 = 2 body

5.6.6 Namátkové prohlídky

Namátkové prohlídky jsou realizovány ostrahou nepravidelně a náhodně při příchodu nebo odchodu zaměstnanců i návštěv.

Bodové hodnocení: SS12 = 1 body

5.6.7 Režim návštěv v objektu

Návštěvy s doprovodem

Návštěvy se musí v objektu pohybovat pouze s doprovodem odpovědné osoby. O návštěvách je vedena evidence i identifikačními údaji návštěv i jejich doprovodu a je veden časový záznam o příchodu i odchodu návštěv.

Bodové hodnocení: SS7 = 3 body

5.6.8 Ostraha

Nepřetržitou ostrahu zabezpečují příslušníci bezpečnostní ochranné služby ve složení tří osob. Obchůzky jsou realizovány po pracovní době v náhodných intervalech vyplývajících z vyhodnocení rizik areálu tak, aby vždy jeden z příslušníků zůstal na stanovišti. Stanoviště ostrahy je od ZO vzdáleno přibližně 300 m. Dále ostrahu vybraných objektů zabezpečuje stálý operační dozorčí a jeho pomocník v nepravidelných intervalech tak, aby vždy jeden zůstal na stanovišti, kde jsou vyvedené veškeré výstupy EZS a EPS. Stanoviště stálého operačního dozorčího je od ZO vzdáleno přibližně 200 m. Žádná z výše uvedených ostrah nemá přístup do zabezpečeného objektu, kontroluje pouze uzavření ZO, neporušenost dveří, oken a další viditelná narušení a v případě potřeby povolá oprávněnou osobu, která je uvedena jak na vstupu do objektu, tak ve směrnících pro ostrahu, které jsou písemně zpracovány a schváleny VOC. Vzhledem k faktu, že obchůzky nejsou po celých 24 hodin prováděny v intervalu menším než 6 hodin a jsou přizpůsobovány provozu v areálu, byla ostraha vyhodnocena jako:

Ostraha typ 3

Bodové hodnocení: SS8 = 3 body

5.6.9 Zařízení elektrické zabezpečovací signalizace

Prostory zabezpečeného objektu a zabezpečené oblasti jsou vybaveny prvky elektronického zabezpečovacího systému, které jsou certifikovány NBÚ a splňující normu ČSN EN 50131-1 ed. 2 Poplachové systémy - Poplachové zabezpečovací a tísňové systémy pro stupeň zabezpečení 2 nízké až střední riziko. Tísňový systém splňuje požadavky normy ČSN EN 50134-1 Poplachové systémy – Systém přivolání pomoci a je certifikován NBÚ.

Do zabezpečeného objektu a ZO byly využity následující prvky EZS:

- ústředna PZTS a ACS typ ASSET 801Z
- sběrnicový PIR detektor pohybu typ, který je sestaven s ústředny JA-106K, sběrnicového modulu JA-114E, bezdrátové modulu JA-154E a ovládacího segmentu JA-192E
- detektor otevření (magnetický kontakt) typ DC106
- tísňový hlásič typ ISC-PB1-100 (ND100-GLT)

Zabezpečení EZS bylo vyhodnoceno jako typ 2

Bodové hodnocení: SS91 = 2 body

5.6.10 Instalace zařízení EZS

Z vnější strany vstupních dveří do zabezpečeného objektu i ZO je instalována klávesnice s LCD displejem zabezpečující vstup do zabezpečeného objektu, ve dveřích jsou instalovány detektory otevření na principu magnetického kontaktu. Další prvky plášťové ochrany nejsou z důvodu umístění ve výšce nad 5,5 m a nelze k nim lehce proniknout, použity. Prostorová ochrana je instalována v zabezpečeném objektu i v ZO a to detektory PIR. V zabezpečené oblasti je vyveden tísňový hlásič.

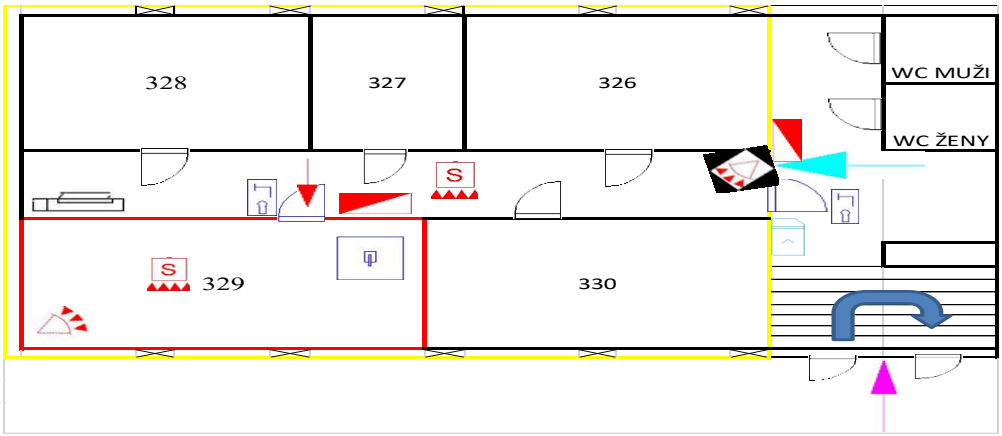
Instalace EZS typ 2

Bodové hodnocení: ZO - SS92 = 2 body

OBL – SS92 = 2 body

Pro vypočtení hodnoty SS9 je použit vzorec SS9 = (SS91 + SS92)/2 x SS92/OBL z čehož plyne následující: SS9 = (2+2)/2 x 2/2 = 2.

Celkové bodové hodnocení SS9 = 2



Obrázek 6: Výkresová dokumentace s vyznačením použitých prvků FB

Zdroj: autor

5.6.11 Perimetr

5.6.12 Fyzické bariéry

Perimetrem, po celém obvodu areálu, je fyzická bariéra typu 2 o minimální výšce 2,15 m, tvořena převážně pletivem a plechovým plotem. V některých částech je bariéra doplněna o šikmé vzpěry, které vyčnívají směrem ven pod úhlem 45° o délce přibližně 500 mm. Tato podmínka však není splněna po celé délce perimetru, ale jen v místech, která byla vyhodnocena, jako riziková. Na základě tohoto je fyzická bariéra vyhodnocena jako:

Fyzická bariéra typ 2

Bodové hodnocení: SS10 = 2 body

5.6.13 Kontrola vstupu ve všech přístupových bodech perimetru

Po celém obvodu perimetru jsou dva přístupové body, které jsou nonstop střeženy ostrahou, která vyžaduje při vstupu, vjezdu nebo odchodu a odjezdu povolení (identifikační karty) pro vstup do areálu. Zároveň provádí namátkové kontroly.

Bodové hodnocení: SS11 = 1 bod

5.6.14 Perimetrický detekční systém (PDS)

Není nainstalován.

Bodové hodnocení: SS13 = 0 bodů

5.6.15 Bezpečnostní osvětlení perimetru:

Není nainstalován.

Bodové hodnocení: SS14 = 0 bodů

5.6.16 Speciální televizní systém na perimetru:

Není nainstalován.

Bodové hodnocení: SS15 = 0 bod

Celkové hodnocení ochrany perimetru vypočteme následovně:

$$S6 = (SS10 \times SS11) + SS12 + SS13 + SS14 + SS15$$

$$S6 = (2x1) + 1 + 0 + 0 + 0$$

$$\mathbf{S6 = 3}$$

5.6.17 Zařízení fyzického ničení nosičů informací nebo dat

V zabezpečeném objektu se nachází zařízení fyzického ničení informací nebo dat a to certifikovaný skartovací stroj typ EBA 2326 C s řezem 4x40 mm, čím splňuje podmínky pro ničení informací se stupněm Důvěrné a nižší.

5.7 Bodové hodnoty nejnižší míry zabezpečení fyzické bezpečnosti

Tabulka bodového hodnocení musí obsahovat záhlaví:

Název zabezpečené oblasti: místnost č. 329 budovy A v areálu Kasáren Dědice

Název zabezpečeného objektu: hranici zabezpečeného objektu tvoří část řetího patra

Kategorie zabezpečené oblasti: Důvěrné

Třída zabezpečené oblasti: Třída II

Typ zabezpečené oblasti: Typ 1

Účel zabezpečené oblasti: zabezpečené oblasti se ukládají a zpracovávají UI se stupněm utajení Vyhrazené a Důvěrné. Zabezpečená oblast není využívána jako pracoviště se stálou přítomností zaměstnanců.

BEZPEČNOSTNÍ OPATŘENÍ	TYP	BODOVÉ OHODNOCENÍ
Úschovné objekty	❑ T. 4 – 4 body ❑ **T. 3 – 3 body** ❑ T. 2 – 2 body	SS1 = 3
Zámky úschovných objektů	❑ T. 4 – 4 body ❑ **T. 3 – 3 body** ❑ T. 2 – 2 body	SS2 = 2
Celkové hodnocení úschovného objektu a jeho zámku	S1 = SS1 x SS2	**S1= 6**
Zabezpečené oblasti	❑ T. 4 – 4 body ❑ T. 3 – 3 body ❑ **T. 2 – 2 body** ❑ T. 1 – 1 bod	SS3 = 2
Uzamykací systém zabezpečené oblasti	❑ T. 4 – 4 body ❑ T. 3 – 3 body ❑ **T. 2 – 2 body** ❑ T. 1 – 1 bod	SS4 = 2
Celkové ohodnocení zabezpečené oblasti a jejího uzamykacího systému	S2 = SS3 x SS4	**S2 = 4**
Objekt	❑ T. 4 – 4 body ❑ **T. 3 – 3 body** ❑ T. 2 – 2 body	**S3 = 3**

	❑ T. 1 – 1 bod	
Systém kontroly vstupu	❑ T. 4 – 4 body ❑ T. 3 – 3 body ❑ **T. 2 – 2 body** ❑ T. 1 – 1 bod	SS6 = 2
Režim návštěv v objektu a) Návštěvy s doprovodem b) Návštěvy bez doprovodu c) Návštěvy bez kontroly	❑ **ad a) – 3 bod** ❑ ad b) – 1 bod ❑ ad c) – nehodnoceno	SS7 = 3
Celkové hodnocení kontroly vstupu	S4 = SS6 + SS7	**S4 = 5**
Ostraha	❑ T. 5 – 5bodů ❑ T. 4 – 4 body ❑ **T. 3 – 3 body** ❑ T. 2 – 2 body ❑ T. 1 – 1 bod	SS8 = 3
Zařízení elektrické zabezpečovací signalizace	❑ T. 4 – 4 body ❑ T. 3 – 3 body ❑ **T. 2 – 2 body** ❑ T. 1 – 1 bod	SS91= 2
Instalace zařízení elektrické zabezpečovací signalizace	❑ T. 4 – 4 body ❑ T. 3 – 3 body ❑ **T. 2 – 2 body** ❑ T. 1 – 1 bod	SS92 = 2
Mezivýsledek (SS 9)		SS9 = 2
Celkové hodnocení ostrahy a systému EZS	S5 = SS8 + SS9	**S5 = 5**
Fyzické bariéry	❑ T. 4 – 4 body ❑ T. 3 – 3 body ❑ **T. 2 – 2 body** ❑ T. 1 –1 bodů	SS10 = 2
Kontrola vstupu v přístupových bodech perimetru a) Kontrola je realizována b) Kontrola není realizována	❑ **ad a) – 1 bod** ❑ ad b) – 0 bodů	SS11 = 1
Namátkové vstupní a výstupní prohlídky a) Prohlídky jsou prováděny b) Prohlídky nejsou prováděny	❑ **ad a) – 1 bod** ❑ ad b) – 0 bodů	SS12 = 1

Perimetrický detekční systém (PDS) - certifikovaný Úřadem - necertifikovaný Úřadem	 2 body 1 bod	SS13 = 0
Bezpečnostní osvětlení perimetru	2 body	SS14 = 0
Speciální televizní systém na perimetru	2 body	SS15 = 0
Celkové hodnocení ochrany perimetru	S6 = (SS10 x SS11) + SS12 + SS13 + SS14 + SS15	**S6= 3**

Tabulka 4: Přehled bodového hodnocení jednotlivých prvků

Zdroj: Příloha č. 1 Vyhlášky č. 528/2005 Sb.
ve znění pozdějších předpisů, upraveno autorem.

Aby byly splněny podmínky fyzické bezpečnosti ve výše analyzované zabezpečené oblasti kategorie Důvěrné v návaznosti na vyhodnocené míře rizika – malá, musí být v souladu s bodem 12 Přílohy č. 1 novely Vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, splněny následné bodové hodnoty

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**

Tabulka 5: Minimální bodové hodnocení v souladu s mírou rizika

Zdroj: Příloha č. 1 Vyhlášky č. 528/2005 Sb. ve znění pozdějších předpisů,
upraveno autorem.

ZABEZPEČENÁ OBLAST KATEGORIE Důvěrné	malá
Povinné : (S1) + (S2) + (S3) = 6 + 4 + 3	13
Povinné : (S4) + (S5) = 5 + 5	10
Nepovinné : (S6) = 3	3
Celkový výsledek	**26**

Tabulka 6: Vypočtené bodové hodnocení

Zdroj: Příloha č. 1 Vyhlášky č. 528/2005 Sb. ve znění pozdějších předpisů,

upraveno autorem.

Prostředky fyzické bezpečnosti, které byly použity při návrhu modelového objektu, plně vyhovují a dostačují k zabezpečení objektu kategorie Důvěrné nejen při malé míře rizika, ale v případě událostí, které by míru rizika zvýšily, jsou tyto prostředky fyzického zabezpečení dostačující.

5.8 Technická dokumentace projektu fyzické bezpečnosti

Technickou dokumentaci stanovuje a popisuje Příloha č. 1 Vyhlášky č. 528/2005 Sb. ve znění pozdějších předpisů.

5.8.1 Výkresová dokumentace

Ve výkresové dokumentaci jsou vyznačeny hranice zabezpečeného objektu, zabezpečené oblasti a dále použití a rozmístění jednotlivých prvků fyzické ochrany. Výkresová dokumentace je přílohou č. 1 této práce.

5.8.2 Dokumentace technických prostředků

Obsahuje zejména názvy, typy, počty a rozmístění jednotlivých prvků fyzické bezpečnosti, které byly použity pro zabezpečení zabezpečeného objektu a ZO. Dále obsahuje kopie certifikátů nebo zápisů o shodě případně i jejich přílohy, které musí být při jejich pořízení platné.

5.9 Provozní řád

Provozní řád je nedílnou součástí projektu fyzické bezpečnosti, jeho náležitosti jsou stanoveny a popsány v Příloha č. 1 Vyhlášky č. 528/2005 Sb. ve znění pozdějších předpisů.

5.9.1 Režim pohybu dopravních prostředků a osob v areálu

Režim pohybu dopravních prostředků je stanoven interním předpisem MO. Vozidla, které se mohou pohybovat po areálu, jsou buď vozidla rezortu MO, nebo civilní vozidla pracovníků tohoto areálu, které musí mít vjezd povolen VOC a při vjezdu do areálu je tímto povolením musí prokázat a při pohybu po areálu a parkování musí být tímto povolením označeny.

Vstup do areálu mají osoby, které zde vykonávají služební nebo pracovní činnost nebo návštěvy za účelem jednání, školení, konferencí apod., dále příslušníci kurzů konaných

u VeV-VA. V obou případech vydává VOC dočasné povolení vstupu nebo navštívenku a pobyt těchto osob je časově zaznamenán.

5.9.2 Režim pohybu dopravních prostředků a osob v budově

V budově, ve které se nachází zabezpečená oblast, není pohyb vozidel možný. Vstup mají povoleny ty osoby, kterým byl povolen vstup do areálu. Do zabezpečeného objektu mohou samostatně vstupovat pouze osoby, kterým byly předány prostředky potřebné ke vstupu do tohoto objektu (klíče od dveří, kódy EZS, identifikační prvky SKV atd.) a toto předání bylo protokolárně zdokumentované. Návštěvy mají vstup do zabezpečeného objektu povolen pouze v doprovodu těchto osob a jejich pobyt je časově zaznamenán.

5.9.3 Pohyb osob v zabezpečeném objektu a zabezpečené oblasti

Do zabezpečeného objektu mohou samostatně vstupovat pouze osoby, kterým byly předány prostředky potřebné ke vstupu do tohoto objektu (klíče od dveří, kódy EZS, identifikační prvky SKV atd.) a toto předání bylo protokolárně zdokumentované. Návštěvy mají vstup do zabezpečeného objektu povolen pouze v doprovodu těchto osob. Při vstupu návštěvy

do zabezpečené oblasti se do knihy vstupů zaznamenává:

- jméno, podpis a identifikace osoby – číslo vojenského nebo občanského průkazu nebo jiného osobního průkazu,
- datum a čas příchodu a odchodu,
- důvod vstupu,
- jméno a podpis doprovázející osoby.

5.9.4 Režim pohybu utajovaných informací v zabezpečeném objektu

S utajovanými informacemi v zabezpečeném objektu mimo zabezpečenou oblast možné pouze v souladu se Zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti a to oprávněné osoby, které splňují požadavky přístupu k UI příslušného stupně utajení a vždy musí být zajištěno, že k UI nebude mít přístup neoprávněná osoba. V odůvodněných případech je možné zpracovávat UI mimo zabezpečený objekt, musí k tomu však být vydán písemný souhlas VOC a musí být zajištěno, že k UT nebude mít přístup neoprávněná osoba.

5.9.5 Pravidla pro zacházení s provozní dokumentací a technickými prostředky

Dokumentace technických prostředků je uložena v zabezpečené oblasti. Za její úplnost, uložení, aktualizaci, provádění a zaznamenávání předepsaných revizí a kontrol, odpovídá bezpečnostní manažer OC.

5.9.6 Mechanické zábranné prostředky a prostředky EZS a EPS

Mechanické zábranné prostředky a prostředky EZS instalované v zabezpečeném objektu a ZO mohou používat pouze oprávněné osoby, kterým byly protokolárně přiděleny vstupní prostředky a jsou k této obsluze vyškoleny a poučeny výrobcem, dodavatelem, servisní firmou nebo osobou tímto určenou. Prostředky EPS mohou být používány pouze v souladu s pokyny příslušného HZS.

U prostředků fyzické bezpečnosti jsou, z důvodu ověření funkčnosti systému fyzické ochrany, minimálně 1 x ročně prováděny pravidelné funkční zkoušky. Za jejich provádění zodpovídá bezpečnostní manažer OC.

Funkční zkoušky a periodické revize doložené písemně revizními zprávami, se provádějí ihned při instalaci, nebo pokud dojde např. k rozšíření EZS, výměny některých prvků apod. Údaje o provozu EZS se evidují v provozní knize EZS.

5.9.7 Pokyny pro používání zařízení pro ničení nosičů informací a dat

K ničení utajovaný informace lze použít pouze skartovací stroj se stejným stupněm utajení, jako má ničená informace nebo se stupněm vyšším. Skartační zařízení musí být certifikované NBÚ. Při skartaci musí být dodržovány pokyny pro obsluhu skartovacího stroje, dle dokumentace výrobce a obsluhovat jej může pouze oprávněná osoba, aby nedošlo k neoprávněnému seznámení s utajovanou informací. Zabezpečená oblast je vybavena certifikovaným skartovacím zařízením pro stupeň utajení Důvěrné.

Na skartovacím stroji se provádějí periodické revize ve stejných lhůtách, jako revize přenosných elektrických spotřebičů a minimálně jedenkrát ročně funkční zkouška.

Za jejich provádění zodpovídá bezpečnostní manažer OC.

5.9.8 Pravidla pro manipulaci s klíči a identifikačními prostředky a jejich duplikátů

Režim manipulace s klíči a identifikačními daty je založen na protokolárním předání vstupních prostředků zabezpečeného objektu, zabezpečené oblasti a úschovných objektů

oprávněným osobám. Klíče a identifikační prostředky jsou vydány pouze oprávněným osobám a o tomto je veden záznam. Klíče a identifikační prostředky jsou ukládány v elektronické úložně na stanovišti stálého operačního dozorčího, kde je zároveň veden záznam o jejich vyzvedávání, které je stanoveno pouze na pracovní dobu. Ve výjimečných případech může VOC povolit výdej klíčů i mimo pracovní dobu. Ztráta musí být neprodleně hlášena bezpečnostnímu manažerovi OC, který zabezpečí nouzové střežení zabezpečeného objektu pomocí střežení fyzickými osobami do doby výměny prvku, u kterého proběhla ztráta klíčů nebo identifikačních prostředků.
Duplikáty jsou uloženy v označené a zapečetěné tubě v trezoru bezpečnostního manažera celku, který vede knihu o jejich výdeji.

5.9.9 Pravidla pro výkon ostrahy

Ostrahu zabezpečují příslušníci bezpečnostní ochranné služby ve složení tří osob. Obchůzky jsou realizovány po pracovní době v náhodných intervalech vyplývajících z vyhodnocení rizik areálu tak, aby vždy jeden z příslušníků zůstal na stanovišti. Stanoviště ostrahy
je od ZO vzdáleno přibližně 300 m. Dále ostrahu vybraných objektů zabezpečuje stálý operační dozorčí a jeho pomocník v nepravidelných intervalech tak, aby vždy jeden zůstal na stanovišti, kde jsou vyvedené veškeré výstupy EZS a EPS. Stanoviště stálého operačního dozorčího je od ZO vzdáleno přibližně 200 m. Ostraha je dále povinna provádět vizuální kontrolu neporušení mechanických zábranných prostředků na vstupu zabezpečené oblasti, nepoškození průlezných otvorů nebo jiné časti opláštění objektu. V případě zjištění závady to neprodleně hlásí stálému operačnímu dozorčímu, který dále postupuje dle směrnic pro výkon služby.

5.10 Pokyny pro ochranu UI v případě vzniku mimořádné události

Pokyny pro ochranu UI v případě vzniku mimořádné události musí být vypracovány na každou hrozbu hodnocenou při stanovování míry rizika. Vzhledem k rozsahu a v mnoha případech opakujícími se pokyny, byly pro účel této práce zpracovány pokyny, jen k vybraným hrozbám.

5.10.1 Vyzrazení UI oprávněnou osobou

Činnost oprávněné osoby

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

Činnost bezpečnostního manažera OC

- 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.

Činnost vedoucí organizačního celku

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

5.10.2 Poškození nebo zničení UI živelnou pohromou - požárem

Činnost oprávněné osoby

- ukončit manipulaci s UI a uložit je do úschovného objektu nebo připravit UI k evakuaci,
- v závislosti na rozsahu požáru jej dostupnými hasebními prostředky požár uhasit,
- opustit ohrožený prostor,
- postupovat dle požárních poplachových směrnic,
- přivolat hasičský záchranný sbor,

Činnost bezpečnostního manažera

- 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 opatřeních provede zápis.

Činnost vedoucího 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.

Za dodržování Plánu zabezpečení objektu, zabezpečených oblastí a jednací oblasti v krizových situacích odpovídá VOC, bezpečnostní manažer, všechny oprávněné osoby v příslušném rozsahu, které s tímto plánem byly seznámeny, a o seznámení je veden písemný záznam.

Praktická část byla soustředěna na vytvoření modelového zabezpečeného objektu a jeho projektu fyzické bezpečnosti. V úvodu byly stanoveny a vyhodnoceny hrozby, které by mohly vzniknout, a na základě tohoto byla stanovena míra rizika, které bylo stanoveno jako malé. Dále byly postupně hodnoceny a posuzovány jednotlivé prvky fyzické bezpečnosti v souladu s Přílohou č. 1 Vyhlášky č. 528/2005 Sb. a bylo postupně vyhodnocováno bodové hodnocení jednotlivých prostředků FB. V poslední fázi je zpracována provozní dokumentace.

ZÁVĚR

Cílem této bakalářské práce bylo analyzovat legislativní dokumenty a bibliografii vztahující se na ochranu informací v České republice se zaměřením na vnitřní předpisy a celkový proces ochrany informací v rezortu Ministerstva obrany důrazem na utajované informace, jejich zpracování a ukládání a při zjištění nedostatků navržení možných řešení. V praktické části bylo cílem navrhnout modelový zabezpečený objekt pro ukládání a zapracovávání utajovaných informací.

V první kapitole byl jen letmo nastíněn historický význam pojmu informace a krátkou definicí tento pojem objasněn. V teoretické části byl uveden přehled legislativních dokumentů pro oblast ochrany informací platných pro Českou republiku, který byl doplněn o vnitřní předpisy týkající se ochrany utajovaných informací v rezortu MO, při čemž byla provedena jejich analýza, ze které je patrné, že vnitřní předpisy dále detailně popisují a upřesňují proces ochrany utajovaných informací v podmínkách tohoto rezortu. Zmíněné byly i některé zásady pro nakládání s dokumenty cizí moci. Legislativní rámec tohoto tématu je velmi široký a komplexně zahrnuje všechny oblasti ochrany utajovaných informací, kterým byla věnována další z kapitol. Dále byly v této části povrchově nastíněny úkoly a pravomoci organizací zastřešující danou problematiku. V legislativě ani v procesu ochrany utajovaných informací jsem neshledala žádný nedostatek a tudíž nenavrhla žádné opatření.

V praktické části byl vytvořen fiktivní model zabezpečené oblasti pro uchovávání a zpracovávání utajovaných informací do stupně utajení Důvěrné a následně vytvořen projekt fyzické bezpečnosti, který byl zpracován v souladu s Přílohou č. 1 Vyhlášky č. 528/2005 Sb. včetně všech náležitostí touto vyhláškou stanovených. Na základě vyhodnocených hrozeb byla stanovena míra rizika, od které se model odvíjel. Vzhledem k použitým prostředkům fyzické ochrany byla minimální bodová hodnota překročena, což však znamená, že i při vzniku neočekávané hrozny a tím i případným zvýšení míry rizika, zabezpečený objekt plně vyhovuje podmínkám pro ukládání a zpracovávání utajovaných informací do stupně utajení Důvěrné.

Veškeré použité informace o umístění zabezpečeného objektu nebo ZO a ostatní údaje včetně počtu aktiv u organizačního celku, parametrů prostředků fyzické ochrany jsou fiktivní a byly použity pouze pro účely této práce a nastínění procesu vytvoření projektu fyzické bezpečnosti.

SEZNAM POUŽITÉ LITERATURY

[1] BERLOQUIN, Pierre. *Skryté kódy a velkolepé projekty: tajné jazyky od starověku po současnost*. Praha: Knižní klub, 2011. Universum (Knižní klub). ISBN 978-80-242-2847-1.

[2] CEJPEK, Jiří. *Informace, komunikace a myšlení: úvod do informační vědy*. 1. Praha: Karolinum, 1998. ISBN 80-718-4767-4.

[3] ČESKO. Nařízení vlády č. 522 ze dne 7. prosince 2005, kterým se stanoví seznam utajovaných informací. In: *Sbírka zákonů České republiky*. 2005, částka 179, 522-529. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu.

[4] ČESKO. Vyhláška č. 363 ze dne 23. listopadu 2011, o personální bezpečnosti a o bezpečnostní způsobilosti. In: *Sbírka zákonů České republiky*. 2011, částka 127, 362-363. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu.

[5] ČESKO. Vyhláška č. 432 ze dne 16. prosince 2011, o zajištění kryptografické ochrany utajovaných informací. In: *Sbírka zákonů České republiky*. 2011, částka 150, 429-435. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu.

[6] ČESKO. Vyhláška č. 523 ze dne 5. prosince 2005, o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor. In: *Sbírka zákonů České republiky*. 2005, částka 179, 522-529. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu.

[7] ČESKO. Vyhláška č. 528 ze dne 14. prosince 2005, o fyzické bezpečnosti a certifikaci technických prostředků. In: *Sbírka zákonů České republiky*. 2005, částka 179, 522-529. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu.

[8] ČESKO. Vyhláška č. 529 ze dne 15. prosince 2005, o administrativní bezpečnosti a o registrech utajovaných informací. In: *Sbírka zákonů České republiky*. 2005, částka 179, 522-529. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu.

[9] ČESKO. Zákon č. 412 ze dne 21. září 2005, o ochraně utajovaných informací a o bezpečnostní způsobilosti. In: *Sbírka zákonů České republiky*. 2005, částka 143, 412-413. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu.

[10] 100+1: *Zahraniční zajímavost* [online]. Brno: Extra Publishing, 2016 [cit. 2019-02-24]. ISSN 1804-9907. Dostupné z: https://www.stoplusjednicka.cz/nepokoritelna-enigma.

[11] Ochrana utajovaných informací: Národní bezpečnostní úřad [online]. [cit. 2019-02-24]. Dostupné z: https://www.nbu.cz/cs/ochrana-utajovanych-informaci-rozcestnik

[12] ŘEHKA, Karel. Informační válka. Praha: Academia, 2017. XXI. století. ISBN 978-80-200-2770-2.

[13] Vznik vojenského zpravodajství v Československu a jeho počátky. *Vojenské zpravodajství* [online]. [cit. 2019-02-25]. Dostupné z: https://www.vzcr.cz/historie#vznik-vojenskeho-zpravodajstvi-v-ceskoslovensku-a-jeho-pocatkysdfhsfbasfbsfn.

[14] ČESKO. Rozkaz Ministra obrany: Ochrana utajovaných informací v rezortu Ministerstva obrany. In: Praha, 2013, ročník 2013, číslo 14.

[15] ČESKO. Rozkaz Ministra obrany: O personální bezpečnosti v rezortu Ministerstva obrany ve znění Rozkazu Ministra obrany č. 98/2014. In: Praha, 2012, ročník 2012, číslo 33.

[16] ČESKO. Normativní výnos Ministra obrany: Administrativní bezpečnost v rezortu Ministerstva obrany. In: Praha, 2018, ročník 2018, číslo 8.

[17] ČESKO. Vyhláška č. 259/2012 Sb.: Vyhláška o podrobnostech výkonu spisové služby. In: *Sbírka zákonů České republiky*. Praha, 2012, ročník 2012, částka 258-261. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu.

[18] Záchrana archiválií. *Vojenský historický archiv* [online]. Praha [cit. 2019-04-28]. Dostupné z: http://www.vuapraha.cz/node/15

[19] ČESKO. Vyhláška č. 528/2005 Sb., ve znění vyhlášky č. 204/2016 Sb: Příloha č. 1. In: Praha, 2005.

[20] ČESKO. Zákon č. 181 ze dne 23. července 2014, o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: *Sbírka zákonů České republiky*. 2014, částka 75. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AČR	Armáda České republiky
Čj.	Číslo jednací
EPS	Elektronická požární signalizace
EU	Evropská unie
FB	Fyzická bezpečnost
EZS	Elektronický zabezpečovací systém
HZS	Hasičský záchranný sbor
MO	Ministerstvo obrany
NBÚ	Národní bezpečnostní úřad
NÚKBI	Národní úřad pro kybernetickou a informační bezpečnost
NV MO	Normativní výnos Ministra obrany
OB MO	Odbor bezpečnosti Ministerstva obrany
OC	Organizační celek
PIR	Prostorové čidlo
RMO	Rozkaz Ministra obrany
SKV	Systém kontroly vstupu
UI	Utajovaná informace
VeV-VA	Velitelství výcviku-Vojenská akademie ve Vyškově
VOC	Vedoucí organizačního celku
ZO	Zabezpečená oblast

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: SPIS K POUČENÉ OSOBĚ

Evidenční číslo

MINISTERSTVO OBRANY

SPIS

K POUČENÉ OSOBĚ

VYHRAZENÉ

PŘÍJMENÍ:

JMÉNO:

SPIS ZALOŽEN DNE:

OZNÁMENÍ VYDÁNO DNE:

Splnění podmínek ověřeno dne:	Podpis:

Obsah spisu

Poř. č.	Název dokladu	Číslo jednací, ev. č.	Počet listů	Poznámka
1	Prohlášení fyzické osoby o svéprávnosti			
2	Výpis z evidence Rejstříku trestů			
3	Oznámení			
4	Poučení			
5	Prohlášení fyzické osoby o svéprávnosti			
6	Výpis z evidence Rejstříku trestů			
7	Prohlášení fyzické osoby o svéprávnosti			
8	Výpis z evidence Rejstříku trestů			
9	Prohlášení fyzické osoby o svéprávnosti			
10	Výpis z evidence Rejstříku trestů			
11	Prohlášení fyzické osoby o svéprávnosti			
12	Výpis z evidence Rejstříku trestů			
13	*(další řádky doplňovat podle potřeby)*			

PŘÍLOHA P II: VZOR POUČENÍ FYZICKÉ OSOBY

Příloha 11 k RMO č. 33/2012 Věstníku

Poučení fyzické osoby o ochraně utajovaných informací a o bezpečnostní způsobilosti
(Vzor)

Vojenský útvar (vojenské zařízení) 9967 Stožec
(uvést číslo organizačního celku a místo dislokace)

P o u č e n í

podle § 60 odst. 3 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti

(BRIEFING)
According to § 60 par. 3 of the Act N. 412/2005 Coll., on the Protection of Classified Information

Níže uvedená osoba byla seznámena s jejími právy a povinnostmi v oblasti ochrany utajovaných informací. Byla seznámena s obsahem zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů (dále jen „zákon“) a s obsahem prováděcích právních předpisů. Byla seznámena s povinnostmi, které jsou stanoveny v § 65 a § 66 odst. 1 zákona, zejména s povinností:

The person named below has been briefed on his/her rights and duties in the area of protection of classified information. He/she has been acquainted with the content of the Act N. 412/2005 Coll., on the protection of classified information and security eligibility (hereinafter „the Act“), and with the content of implementing legal regulations. He/she has been acquainted with duties laid down in § 65 and § 66 par. 1 of the Act, in particular with the following:

a) dodržovat stanovené povinnosti při ochraně utajovaných informací,
a) to comply with imposed obligations in protecting classified information;

b) zachovávat mlčenlivost o utajované informaci, k níž má nebo měla přístup, pokud není této povinnosti oprávněným orgánem zproštěna,
b) to hold classified information in confidence, to which he/she has or had access, unless he/she has been released from this duty by the responsible authority;

c) neumožnit přístup k utajované informaci neoprávněné osobě.
c) to prevent access by unauthorized persons to classified information.

Dále byla seznámena se všemi následky porušení povinností stanovených zákonem, zejména s nebezpečím trestního stíhání nebo uložení sankce za spáchání správního deliktu.

Further he/she has been briefed on all consequences arising from the breach of duties imposed by the Act, in particular on the danger of a criminal prosecution or imposing sanction for committing an administrative infraction.

Níže uvedená osoba **byla – nebyla**[*)] seznámena s předpisy NATO
byla – nebyla[*)] seznámena s předpisy EU
byla – nebyla[*)] seznámena s předpisy WEU

III *The person named below*
IV ***has been – has not been***[*)] *briefed on the regulations of the NATO*
V ***has been – has not been***[*)] *briefed on the regulations of the EU*
VI ***has been – has not been***[*)] *briefed on the regulations of the WEU*

VII V *(In)*……. dne *(Date)*……

Poučení provedl
The briefing made by

Jméno a příjmení
Name and surname

Podpis
Signature

Otisk razítka
Stamp

Poučená osoba
The briefed person

Jméno a příjmení
Name and surname

Datum narození
Date of birth

Podpis
Signature

[*)] Nehodící se škrtněte