Konceptuální návrh zabezpečení perspektivního výcvikového pracoviště

Conceptual design of security of training center

Bc. Veronika Svetláková

Diplomová práce
2013

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

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

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

Jméno a příjmení:	**Bc. Veronika SVETLÁKOVÁ**
Osobní číslo:	**A11729**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Konceptuální návrh zabezpečení perspektivního výcvikového pracoviště**

Zásady pro vypracování:

1. **Analyzujte požadavky ochrany utajovaných informací na výcvikové pracoviště.**
2. **Pojednejte o fyzické bezpečnosti v podmínkách MO.**
3. **Analyzujte požadavky MO na projekt fyzické bezpečnosti.**
4. **Specifikujte a zhodnoťte podmínky pro zajištění fyzické bezpečnosti výcvikového pracoviště.**
5. **Vypracujte konceptuální návrh systému fyzické bezpečnosti výcvikového pracoviště.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **Ochrana utajovaných informací. www.nbu.cz [online]. Národní bezpečnostní úřad [cit. 2012-11-29]. Dostupné z: http://www.nbu.cz/cs/ochrana-utajovanych-informaci/.**
2. **KINDL, Jiří. Projektování bezpečnostních systémů I. 2. vyd. Zlín: Univerzita Tomáše Bati, 2007, 134 s. ISBN 978-80-7318-554-1.**
3. **LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management I. 1. vyd. Zlín: VeRBuM, 2011, 316 s. ISBN 978-80-87500-05-7.**
4. **LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management II. 1. vyd. Zlín: VeRBuM, 2012, 387 s. ISBN 978-80-87500-19-4.**
5. **KŘEČEK, Stanislav. Příručka zabezpečovací techniky. Vyd. 3. aktualiz. S.l.: Cricetus, 2006, 313 s. ISBN 80-902938-2-4.**
6. **Skupina norem ČSN EN 50 130, 50 131, 50 132,50 133, ČSN EN 54.**
7. **Rozkaz Ministra obrany ČR č. 22/2006 Ochrana utajovaných informací v resortu MO.**
8. **Normativní výnos Ministerstva obrany č. 42/2006, Fyzická bezpečnost v resortu MO.**

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

Datum zadání diplomové práce: **8. února 2013**

Termín odevzdání diplomové práce: **3. června 2013**

Ve Zlíně dne 8. února 2013

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

doc. RNDr. Vojtěch Křesálek, CSc.
vedoucí ústavu

ABSTRAKT

Tato diplomová práce je zaměřena na vytvoření konceptuálního návrhu fyzické bezpečnosti modelového vojenského výcvikového pracoviště, ve kterém se nachází utajované informace.

Jsou zde objasněny požadavky fyzické bezpečnosti z hlediska utajovaných informací v resortu Ministerstva obrany. Pro zabezpečení objektu je využito poznatků a znalostí z oboru bezpečnostních technologií, projektování zabezpečovacích systémů v kombinaci s aplikováním fyzické ochrany, režimových opatření a technických prostředků se zaměřením na ochranu utajovaných informací.

V práci jsou specifikovány konkrétní požadavky na zabezpečení zvolených aktiv, bezpečnostní analýzou jsou vyhodnocena rizika a v závěru práce navrženy možnosti a způsoby zajištění fyzické bezpečnosti utajovaných informací modelového pracoviště.

Klíčová slova: fyzická bezpečnost, utajovaná informace, analýza rizik, zabezpečená oblast, návrh technických prostředků.

ABSTRACT

This thesis is focused on the conceptual creation design of physical security model in military training department, where are the secret information located. There are clarified requirements in physical security terms of this type of information at the Ministry of Defence. To secure of the building there are mentioned knowledge and expertise in the field of security technologies, projects of security systems in combination with the application of physical protection, regime support and technical means focusing on the protection of secret information.

In the work there are specified detailed security requirements of selected assets, according to security analysis are evaluated and at the end of the work there are presented possibilities and ways to protect the physical security of information in the model workplace.

Keywords: physical security, secret information, risk analysis, security area, the profile of technical means.

Ráda bych vyjádřila poděkování doc. Ing. Luďku Lukášovi, CSc. za odborné vedení, podnětné rady a upřímné připomínky při tvorbě mé diplomové práce.

Velký dík patří také mým kolegům za podporu a především mé rodině, která mi poskytla dostatek prostoru pro vypracování této práce a usilovně mě podporovala po celou dobu studia.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/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 diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně ……

podpis diplomanta

OBSAH

ÚVOD **10**

1 OCHRANA UTAJOVANÝCH INFORMACÍ **11**

1.1 POJEM UTAJOVANÁ INFORMACE 11

1.2 PRÁVNÍ VYMEZENÍ UTAJOVANÝCH INFORMACÍ V ČR 11

1.3 CHARAKTERISTIKA UTAJOVANÉ INFORMACE 12

1.4 STUPNĚ UTAJENÍ 12

1.5 DRUHY ZAJIŠTĚNÍ OCHRANY UTAJOVANÝCH INFORMACÍ 13

1.6 UTAJOVANÁ INFORMACE V ELEKTRONICKÉ PODOBĚ 16

1.7 OCHRANA UTAJOVANÝCH INFORMACÍ V REZORTU MO ČR 16

1.8 DÍLČÍ ZÁVĚR 17

2 FYZICKÁ BEZPEČNOST Z HLEDISKA UTAJOVANÝCH INFORMACÍ V REZORTU MO ČR **18**

2.1 OPATŘENÍ FYZICKÉ BEZPEČNOSTI 19

2.1.1 Režimová opatření 19

2.1.2 Ostraha 20

2.1.3 Technické prostředky 21

2.2 CERTIFIKACE A PODMÍNKY POUŽÍVÁNÍ TECHNICKÝCH PROSTŘEDKŮ 22

2.3 NÁVRH BEZPEČNOSTNÍHO PROJEKTU 23

2.4 DÍLČÍ ZÁVĚR 24

3 ZÁSADY ZPRACOVÁNÍ PROJEKTU FYZICKÉ BEZPEČNOSTI **25**

3.1 ČÁSTI PROJEKTU FYZICKÉ BEZPEČNOSTI PODLE TYPU KATEGORIE ZABEZPEČENÉ NEBO JEDNACÍ OBLASTI 25

3.2 URČENÍ A OCHRANA OBJEKTU, ZABEZPEČENÝCH OBLASTÍ A JEDNACÍCH OBLASTÍ 26

3.2.1 Zabezpečení zabezpečených oblastí 26

3.2.2 Zabezpečení jednacích oblastí 28

3.3 ZABEZPEČENÍ TECHNICKÉHO ZAŘÍZENÍ 29

3.4 VYHODNOCENÍ RIZIK 29

3.4.1 Klasifikace a řízení aktiv 30

3.4.2 Specifikace hrozeb 30

3.4.3 Hodnocení zranitelnosti 32

3.5 Bodové hodnocení opatření fyzické bezpečnosti 35

3.6 PROVOZNÍ ŘÁD OBJEKTU 36

3.7 TECHNICKÁ DOKUMENTACE PRO NAVRHOVANÁ OPATŘENÍ FYZICKÉ BEZPEČNOSTI OBJEKTU 37

3.8 VÝCHODISKA PŘI NÁVRHU BEZPEČNOSTNÍHO PROJEKTU 37

3.8.1 Bezpečnostní posouzení objektu 37

3.8.2 Stupeň zabezpečení 41
3.8.3 Třída prostředí 41
3.8.4 Volba a umístění komponentů zabezpečovacího systému 42
3.9 DÍLČÍ ZÁVĚR 42
4 VÝCHOZÍ PODMÍNKY PRO NÁVRH ZABEZPEČENÍ VÝCVIKOVÉHO PRACOVIŠTĚ 43
4.1 CHARAKTERISTIKA MODELOVÉHO PRACOVIŠTĚ 43
4.1.1 Klasifikace pracoviště 43
4.1.2 Prostorová dispozice pracoviště a jeho zranitelná místa 45
4.1.3 Opatření fyzické bezpečnosti vzhledem k pracovišti 46
4.1.4 Charakter aktiv 47
4.1.5 Charakter možného pachatele 48
4.2 ANALÝZA A POSOUZENÍ BEZPEČNOSTNÍCH RIZIK PRACOVIŠTĚ 48
4.2.1 Aktiva - identifikace, stupeň utajení a velikosti újmy 49
4.2.2 Identifikace rizik 49
4.2.3 Analýza rizik 51
4.2.4 Analýza souvztažnosti 52
4.2.5 Vyhodnocení zranitelnosti objektu 55
4.2.6 Vyhodnocení analýzy rizik 56
4.3 BODOVÉ OHODNOCENÍ BEZPEČNOSTI 57
4.4 URČENÍ OBJEKTU A ZABEZPEČENÝCH OBLASTÍ 57
4.5 DÍLČÍ ZÁVĚR 59
5 KONCEPTUÁLNÍ NÁVRH SYSTÉMU FYZICKÉ BEZPEČNOSTI VÝCVIKOVÉHO PRACOVIŠTĚ 60
5.1 URČENÍ REŽIMOVÝCH OPATŘENÍ 61
5.2 ZAJIŠTĚNÍ FYZICKÉ OSTRAHY 61
5.3 MECHANICKÉ ZÁBRANNÉ PROSTŘEDKY 62
5.3.1 Zabezpečená oblast kategorie Vyhrazené 62
5.3.2 Zabezpečená oblast kategorie Důvěrné 63
5.4 POPLACHOVÝ ZABEZPEČOVACÍ A TÍSŇOVÝ SYSTÉM 64
5.4.1 Ústředna PZTS 64
5.4.2 Detektory PZTS 66
5.5 INTEGROVANÝ PŘÍSTUPOVÝ SYSTÉM 70
5.5.1 Klávesnice DGP2-641R 72
5.5.2 Princip přístupu 73
5.6 ZAŘÍZENÍ PRO FYZICKÉ NIČENÍ NOSIČŮ INFORMACÍ 73
5.7 BODOVÉ HODNOCENÍ NAVRŽENÉHO ZABEZPEČENÍ 74
5.8 DÍLČÍ ZÁVĚR 74
ZÁVĚR 75
ZÁVĚR V ANGLIČTINĚ 76
SEZNAM POUŽITÉ LITERATURY 77

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK 80
SEZNAM OBRÁZKŮ 82
SEZNAM TABULEK 83
SEZNAM PŘÍLOH 84

ÚVOD

Vojenské výcvikové pracoviště, fyzická bezpečnost, ochrana utajovaných informací. Tři slovní spojení, která vytvořila námět pro tuto diplomovou práci.

Informace představují v současném světě technologií velmi vážené aktivum, i když opodstatnění potřeby jejich ochrany je pro bezpečnostní manažery mnohdy nelehký úkol. Pokud vezmeme v úvahu „zatěžující“ vlastnost informace, jakou je její stupeň utajení, vyvstane otázka, jaká nastavit pravidla pro její ochranu. Na tu nám dává z legislativního hlediska odpověď Národní bezpečnostní úřad, který stanovuje pravidla pro sestavení systémů bezpečnostních opatření. Odpověď na komplexní hledisko navrženého řešení s dodržením patřičných pravidel musí najít každý bezpečnostní manažer sám.

Ve své práci se zaměřím na rozsáhlou oblast bezpečnosti, jakou je fyzická bezpečnost z hlediska utajovaných informací. Na základě vyhodnocení bezpečnostní analýzy rizik navrhnu opatření fyzické bezpečnosti pro modelové vojenské výcvikové pracoviště, jehož aktiva nesou charakter utajení a je nezbytná jejich adekvátní ochrana.

V první části je charakterizována utajovaná informace, popsány druhy jejího zajištění a její ochrana v rezortu MO.

Poté následuje specifikace fyzické bezpečnosti z hlediska utajovaných informací v rezortu MO, způsoby opatření a zpracování návrhu bezpečnostního projektu.

Třetí část práce popisuje zásady zpracování projektu fyzické bezpečnosti, a to určení a ochranu zabezpečených a jednacích oblastí, vyhodnocení rizik, bodové ohodnocení opatření fyzické bezpečnosti a východiska návrhu bezpečnostního projektu.

Ve čtvrté části práce stanovím výchozí podmínky pro návrh zabezpečení modelového pracoviště. Nejprve budu charakterizovat pracoviště, vytýčím jeho prostorovou dispozici a zranitelná místa objektu, určím aktiva, která je potřeba chránit a provedu analýzu a posouzení bezpečnostních rizik pracoviště. Na základě vyhodnocení rizik vymezím minimální bodové ohodnocení požadovaných bezpečnostních opatření.

Na závěr bude navržen způsob naplnění požadavků na zabezpečení modelového vojenského pracoviště prostřednictvím opatření fyzické bezpečnosti.

1 OCHRANA UTAJOVANÝCH INFORMACÍ

Potenciální výcvikové pracoviště Ministerstva obrany, jež je předmětem této diplomové práce, je předurčeno k provádění výcviku vojenských profesionálů a speciálních skupin bezpečnostních sborů. Nástrojem pro výcvik jsou vojenské technické prostředky, obsahující utajovanou informaci kategorie Důvěrné a součástí pracoviště jsou prostory, ve kterých je uložena utajovaná informace kategorie Vyhrazené. Na základě těchto potřeb je nezbytné nejprve pojednat o ochraně utajovaných informací podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti, ve znění pozdějších zákonů, s dalším podrobným zaměřením na fyzickou bezpečnost.

1.1 Pojem utajovaná informace

Za utajovanou informaci můžeme považovat takovou informaci nebo věc, určenou původcem utajované informace, kterou je třeba vzhledem k zájmu České republiky chránit před vyzrazením, zneužitím, poškozením, zničením, neoprávněným rozmnožováním, ztrátou nebo odcizením a která může vznikat jen v oblastech, které stanoví vláda České republiky svým nařízením.

O tom, zda informace má být utajena, komu a za jakých podmínek může být zpřístupněna, rozhoduje držitel určité informace. Význam takového jednání spočívá ve znalosti obsahu informace a to představuje pro oprávněnou osobu výhodu jistého náskoku vůči jiným osobám, skupinám nebo organizacím.

1.2 Právní vymezení utajovaných informací v ČR

V České republice je platná právní úprava utajovaných informací zahrnuta v zákonech, nařízeních vlády a prováděcích vyhláškách NBÚ.

Zákon č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti (dále jen zákon č. 412/2005 Sb.) je současnou platnou právní úpravou problematiky utajovaných informací. Je zde definován samotný pojem utajované informace (dále jen UI) a v § 1 tohoto zákona jsou uvedeny zásady pro stanovení informací jako informací utajovaných, podmínky pro přístup k nim a další požadavky na jejich ochranu.

§ 139 odst. 1 zákona č. 412/2005 Sb. odkazuje na seznam utajovaných informací, uvedený v přílohách nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací ve znění nařízení vlády č. 240/2008 Sb.

1.3 Charakteristika utajované informace

Právní řád České republiky charakterizuje utajovanou informaci třemi základními znaky:

a) **Utajení** – znamená omezenou možnost přístupu k utajované informaci, které je dosaženo pomocí zvláštního režimu, jehož cílem je omezit znalost o obsahu této informace na určitý okruh osob. Režimem utajení je soubor pravidel, opatření a činností s cílem zajistit v maximální míře, aby s UI nepřišla do styku nepovolaná osoba a aby s informací nebylo nakládáno způsobem, který je nepřijatelný.

   Utajením je současně zajišťována důvěrnost, tzn. že neoprávněná osoba se s utajovanou informací nesetká ani neseznámí a také integrita, která znamená, že utajovaná informace nemůže být neoprávněnou osobou modifikována. [1]

b) **Újma –** Újmou zájmu České republiky se pro účely tohoto zákona rozumí poškození nebo ohrožení zájmu České republiky. Podle závažnosti poškození nebo ohrožení zájmu České republiky se újma člení na mimořádně vážnou újmu, vážnou újmu a prostou újmu. [2]

   Jako újmu zájmu ČR lze považovat oblasti politické, obrany státu, veřejné bezpečnosti, ekonomických zájmů, práv a svobod fyzických a právnických osob, ochranu zdraví a života fyzických osob.

c) **Sankce –** vzniká jako negativní následek při porušení zákona a souvisejících předpisů v souvislosti s utajovanými informacemi. Hrozba sankcí představuje prostředek, jakým stát prosazuje svůj zájem na ochraně utajovaných informací a na dodržování stanovených pravidel. Sankce mají několik podob, od majetkových až po omezení osobní svobody fyzické osoby. [1]

1.4 Stupně utajení

K vyjádření významu chráněného zájmu je stanovena klasifikace utajovaných informací do jednotlivých stupňů utajení. Každá utajovaná informace musí být označena příslušným stupněm utajení a tento stupeň musí být stanoven právně. Stupeň utajení UI se stanoví

podle významu chráněného zájmu, závažnosti obsahu utajované informace a s využitím seznamu utajovaných informací.

Dle ustanovení § 4 zákona č. 412/2005 Sb. se utajovaná informace dělí do čtyř stupňů utajení:

a) **„Vyhrazené“ (dále jen „V“) –** klasifikuje takovou informaci, jejíž vyzrazení neoprávněné osobě nebo zneužití, může být pro zájmy České republiky nevýhodné.

b) **„Důvěrné“ (dále jen „D“) –** tímto stupněm utajení je označována informace, jejíž vyzrazení nebo zneužití může způsobit prostou újmu zájmům České republiky.

c) **„Tajné“ (dále jen „T“) –** označujeme takovou informaci, jejíž vyzrazení neoprávněné osobě by mohlo způsobit vážnou újmu zájmům České republiky.

d) **„Přísně tajné“ (dále jen „PT“) –** je nejvyšším stupněm utajení. Tímto stupněm označujeme takovou informaci, jejíž vyzrazení neoprávněné osobě nebo její zneužití může způsobit mimořádnou újmu zájmům České republiky.

1.5 Druhy zajištění ochrany utajovaných informací

Ochrana UI je podle zákona zajišťována systémem opatření, jejichž cílem je zajistit ochranu utajovaných informací buď určitým způsobem (technické prostředky), nebo před určitou nežádoucí situací (přístup nepovolené osoby k UI) a při jejich zpracování, evidencí a nakládáním s utajovanou informací na určitém místě.

Primárním účelem prostředků ochrany utajovaných informací je jejich ochrana před neoprávněným nakládáním. Zákon definuje jednotlivé oblasti prostředků ochrany UI se zaměřením na specifické systémy opatření.

Personální bezpečnost

Personální bezpečnost je vnímána jako základní způsob zajištění ochrany utajovaných informací. Primárním cílem personální bezpečnosti je, aby se s utajovanou informací seznamovala pouze ta fyzická osoba, která ji nezbytně potřebuje pro výkon své funkce. K tomu je nutné, aby tato osoba splnila soubor podmínek a byl jí tak umožněn přístup k utajované informaci. Opatření personální bezpečnosti dále stanovují odpovědnou osobu za řádné plnění podmínek, které jsou požadovány po fyzické osobě a také povinnost odpovědné osoby jednou ročně zajistit u osob, které mají přístup k utajované informaci,

proškolení z právních předpisů v oblasti ochrany utajovaných informací a vedení přehledu o nich.

Zákon č. 412/2005 Sb. stanovuje čtyři stupně utajení, ke kterým má fyzická osoba přístup. Pro každý stupeň jsou stanoveny podmínky, které musí fyzická osoba splňovat (Tab. 1).

Tab. 1: Podmínky přístupu fyzické osoby k utajované informaci

Podmínky	**Důvěrné, Tajné, Přísně tajné**	**Vyhrazené**
Způsobilost k právním úkonům	**ANO**	**ANO**
Věk minimálně 18 let	**ANO**	**ANO**
Bezúhonnost	**ANO**	**ANO**
Státní občanství ČR, země EU, NATO	**ANO**	**NE**
Osobnostní způsobilost	**ANO**	**NE**
Bezpečnostní spolehlivost	**ANO**	**NE**
Splnění podmínek	**osvědčení**	**oznámení**

Průmyslová bezpečnost

Pojem průmyslová bezpečnost zahrnuje v zákoně č. 412/2005 Sb. podmínky přístupu podnikatele k utajované informaci a formy přístupu podnikatele k utajované informaci.

Podnikateli, který nezbytně k výkonu své činnosti potřebuje přístup k utajované informaci stupně utajení Důvěrné a vyšší, lze umožnit tento přístup, pokud je držitelem platného osvědčení podnikatele příslušného stupně utajení nebo vyššího, pokud zákon nestanoví jinak. Osvědčení podnikatele vydává Národní bezpečnostní úřad podnikateli, který splňuje podmínky pro jeho vydání stanovené v § 16 zákona, po provedeném bezpečnostním řízení. [3]

Pro stupeň utajení Vyhrazené dokládá podnikatel prohlášení, kterým doloží svou schopnost zabezpečit v souladu s platnou vyhláškou ochranu utajovaných informací a osvědčení pro daný stupeň utajení. Zmiňovanou vyhláškou je míněna vyhláška č. 450/2011 Sb., o průmyslové bezpečnosti, která ve svých přílohách obsahuje vzory žádostí, osvědčení, dotazníků a prohlášení.

Administrativní bezpečnost

Administrativní bezpečnost tvoří systém opatření, která by měla zabránit neoprávněné osobě ztížit nebo zabránit v přístupu k utajované informaci, nebo neoprávněný přístup či pokus přístup zaznamenat.

V zákoně jsou administrativní bezpečnosti věnovány § 21 až § 23 a dále jsou její pravidla uvedena ve vyhlášce č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací (dále jen vyhláška č. 529/2005 Sb.).

Uvedené legislativní vyhlášky určují způsoby ochrany utajovaných informací při jejich tvorbě, příjmu, evidenci, zpracování, přípravě, ukládání, vyřazování, skartaci, archivaci a jiné manipulaci. Ve vyhlášce je také uvedený způsob určování stupně utajení UI, jeho změny, zrušení a vyznačování na písemnostech, dále tvorba opisů, výpisů, kopií a překladů utajovaných dokumentů. Stanovené podmínky a povinnosti se týkají dokumentů v listinné i nelistinné podobě. Přílohou vyhlášky č. 529/2005 Sb. jsou vzory administrativních pomůcek.

Bezpečnost informačních a komunikačních systémů

Stále rostoucí význam má v současné době bezpečnost informačních systémů v oblasti utajovaných informací a s tím dochází k přiměřenému nárůstu významu informačních a komunikačních technologií (dále jen IKT).

Oblast IKT je legislativně řešena zákonem č. 412/2005 Sb. a vyhláškou č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor. Tato vyhláška se zabývá požadavky na informační systémy a podmínkami jeho bezpečného provozu v závislosti na stupni utajení UI, se kterými se v systému pracuje a na bezpečnostním provozním módu. Utajované informace lze zpracovávat a jinak s nimi manipulovat pouze v takových systémech, které jsou certifikovány Národním bezpečnostním úřadem a písemně schváleny do provozu a užívání odpovědnou osobou. Ve vyhlášce je specifikovaný obsah bezpečnostní dokumentace informačních systémů.

Pokud se v informačních systémech zpracovává utajovaná informace stupně Důvěrné, Tajné, Přísně tajné, stanovuje vyhláška povinnost aplikovat opatření na ochranu UI před jejím únikem pomocí kompromitujícího elektromagnetického vyzařování z elektrických a elektronických zařízení. Pro tento účel je možné využít stínící komory, která musí být certifikována NBÚ.

Kryptografická ochrana

Kryptografickou ochranu tvoří soubor opatření, prostředků a metod při zpracování, přenosu, ukládání a archivaci utajovaných informací ve výpočetních a informačních systémech s využitím kryptografického materiálu a kryptografických metod. Kryptografická ochrana je zpracována kromě zákona č. 412/2005 Sb. i ve vyhlášce č. 432/2011 Sb., o zajištění kryptografické ochrany utajovaných informací a vyhlášce č. 525/2005 Sb., o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací.

Za kryptografický materiál je považován kryptografický prostředek, materiál k zajištění jeho funkce a kryptografický dokument. Použitý kryptografický prostředek musí být certifikován NBÚ. Jako kryptografický materiál je definována listina nebo jiný nosič informací obsahující utajovanou informaci kryptografické ochrany.

Fyzická bezpečnost

Fyzická bezpečnost je systém opatření, která mají neoprávněné osobě zabránit nebo ztížit přístup k utajovaným informacím, popřípadě přístup nebo pokus jej zaznamenat. Fyzickou bezpečností se budu podrobněji zabývat v následující samostatné kapitole.

1.6 Utajovaná informace v elektronické podobě

Je-li zpracována informace jako utajovaná, může se v souladu se zákonem vyskytovat v jakékoliv podobě na jakémkoliv nosiči. Informace, vytvořená pomocí výpočetní techniky, je označována jako utajovaný dokument v nelistinné podobě a může být uložena na různých paměťových médiích, tedy nosičích informací. Obdobně jsou označovány a evidovány nosiče utajovaných informací např. USB disky, pevné disky, CD-ROM, DVD, apod.

1.7 Ochrana utajovaných informací v rezortu MO ČR

Realizaci zákona č. 412/5005 Sb. v rezortu MO ČR upravuje Rozkaz ministra obrany (dále jen RMO) č. 22/2006, o ochraně utajovaných informací, ve znění pozdějších úprav. Mezi další důležité legislativní normy patří Normativní výnos bezpečnostního ředitele MO (dále jen NVMO) č. 42/2006, o fyzické bezpečnosti v rezortu MO, ve znění pozdějších úprav a příloha k nařízení vlády č. 522/2005 Sb., ve znění nařízení vlády č. 240/2008 Sb., která stanoví seznam utajovaných informací.

1.8 Dílčí závěr

Aby povinná osoba neměla pochybnosti o charakteru utajované informace, vždy musí být jasně vymezena obsahová stránka utajované informace, jakož i povinnosti při její ochraně před vyzrazením, zneužitím, poškozením, zničením, neoprávněným rozmnožováním, ztrátou nebo odcizením.

Specifikace takové ochrany je v České republice stanovena zákonem č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti. § 139 odst. 1 uvedeného zákona odkazuje na seznam utajovaných informací, uvedený v přílohách nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací ve znění nařízení vlády č. 240/2008 Sb.

Právní řád České republiky charakterizuje utajovanou informaci třemi základními znaky - utajení, újma a sankce. K vyjádření významu chráněného zájmu je stanovena klasifikace utajovaných informací do jednotlivých stupňů utajení, a to Vyhrazené, Důvěrné, Tajné a Přísně tajné.

Personální, průmyslová, administrativní, jakož i ochrana informačních a komunikačních systémů a kryptografická ochrana jsou určeny zákonem jako druhy zajištění ochrany utajovaných informací.

Fyzická bezpečnost tvoří základní téma této práce, a proto se jí budu věnovat podrobněji v následujících kapitolách a to primárně z pohledu ochrany utajovaných informací a technických prostředků potenciálního výcvikového pracoviště v rezortu Ministerstva obrany.

2 FYZICKÁ BEZPEČNOST Z HLEDISKA UTAJOVANÝCH INFORMACÍ V REZORTU MO ČR

Důležitou část aktiv rezortu MO ČR, potažmo Armády České republiky (dále jen AČR), tvoří z bezpečnostního hlediska zbraně, informace a technologie. Užitná i finanční hodnota výcvikových zařízení a samotných technologií je jedním z hlavních důvodů, proč je nutné zabývat se bezpečností objektů, ve kterých se nachází. Bezpečnost objektu musí být nastavena tak, aby eliminovala předpokládané hrozby a zde hraje primární roli systém fyzické bezpečnosti.

Fyzická bezpečnost z hlediska utajovaných informací se v rezortu MO zabývá problematikou ochrany vojenských objektů, ve kterých takové informace vznikají, jsou uchovávány a dochází s nimi k manipulaci. Je nutné, aby byla stanovena odpovědnost za přidělené prostory a ostatní zařízení pro organizační celky dislokované ve vojenském areálu. Určují se bezpečnostní manažeři rozlehlého objektu a jednotlivých organizačních celků, hranice objektu, odpovědnost za opatření fyzické bezpečnosti a způsob výkonu ostrahy rozlehlého objektu.

Opatření fyzické bezpečnosti organizuje vedoucí organizačního celku na základě stanovení kategorií a tříd zabezpečených oblastí a dále jednacích oblastí, nacházejících se v objektu. Objektem nemusí být pouze budova, ale také trakt budovy, patro nebo místnost, ale vždy musí být jasně vymezena hranice, v jejímž rámci existuje možnost kontroly osob a vozidel. Podle NVMO č. 42/2006 je zabezpečenou oblastí ohraničený prostor uvnitř objektu s uzamykatelnými vstupy. Jednací oblastí je ohraničený prostor uvnitř objektu určený pro pravidelné projednávání utajovaných informací stupňů Tajné a Přísně tajné. V objektu tedy může být více zabezpečených a jednacích oblastí. Vedoucí organizačního celku přihlíží při stanovování počtu a umístění zabezpečených oblastí, jednacích oblastí a objektů ke stavebním dispozicím a vlastnostem budovy.

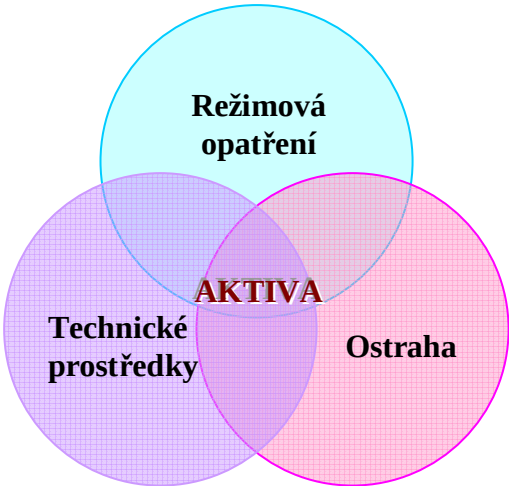
Minimalizaci nákladů na zabezpečení hranice objektu lze zajistit vhodným stanovením objektu, v němž se nacházejí zabezpečené oblasti kategorie Vyhrazené (areál, budova), do něhož je následně vydefinován objekt, ve kterém se nacházejí zabezpečené oblasti kategorie Důvěrné a vyšší, a jednací oblasti tak, aby objekt splňoval požadavky na zabezpečení hranice objektu pro zabezpečené oblasti dané kategorie (budova, poschodí,...).

Na základě vyhodnocení hrozeb a zranitelnosti utajované informace se stanovuje míra rizika jako „malá“, „střední“ nebo „velká“, kdy do rizik se zahrnují hrozby i v návaznosti na ochranu majetku, které mohou v konečném řešení stanovenou míru rizika zvyšovat.

Pokud vedoucí organizačního celku rozhodne o doplnění dalších bezpečnostních opatření pro zabezpečenou oblast kategorie Důvěrné a vyšší, nechá vypracovat návrh projektu fyzické bezpečnosti, který slouží po schválení nadřízeným orgánem jako podklad pro projekt fyzické bezpečnosti v rezortu MO.

2.1 Opatření fyzické bezpečnosti

Vstup do zabezpečené oblasti a výstup z ní musí být zajištěn s využitím opatření fyzické bezpečnosti. Základními opatřeními fyzické bezpečnosti jsou režimová opatření, fyzická ostraha a technické prostředky.



Obr. 1. Opatření fyzické bezpečnosti

2.1.1 Režimová opatření

Režimová opatření určují oprávnění osob a dopravních prostředků pro vstup/výstup a vjezd/výjezd do objektu, režim manipulace s klíči a identifikačními prostředky (elektrická zámková zařízení a systémy pro kontrolu vstupů), způsob manipulace s technickými prostředky a kontrolu dodržování těchto opatření. Režimová opatření také stanoví podmínky a způsob kontroly pohybu osob v objektu a vnášení/vynášení utajovaných informací z/do objektu.

Režimová opatření dle výše uvedeného stanoví vedoucí organizačního celku v provozním řádu objektu s využitím režimu manipulace s klíči a identifikačními údaji.

2.1.2 Ostraha

U objektu, ve kterém se nachází zabezpečená oblast nejvýše kategorie Vyhrazené, zabezpečují ostrahu zaměstnanci, příslušníci ozbrojených sil nebo zaměstnanci bezpečnostní ochranné služby, popř. se střežení objektu realizuje napojením na pult centrální ochrany[1], který umožňuje rychlý zásah. Konkrétní způsob ostrahy stanoví podle místních podmínek vedoucí organizačního celku, který za střeženou oblast odpovídá. [4]

U objektu, ve kterém se nachází zabezpečená oblast stupně utajení Důvěrné, Tajné a Přísně tajné, se ostraha zabezpečuje podle § 28 odst. 1 zákona a to následně podle kategorií:

a) Přísně tajné - nejméně dvěma osobami u objektu;

b) Tajné - nejméně jednou osobou u objektu a jednou další osobou, které poplachové hlášení technických prostředků umožní rychlý zásah, je-li provádění ochrany utajovaných informací narušeno;

c) Důvěrné - nejméně jednou osobou, které poplachové hlášení technických prostředků umožní rychlý zásah, je-li provádění ochrany utajovaných informací narušeno.

U objektu, ve kterém se nachází technické zařízení, které obsahuje utajovanou informaci stupně utajení:

a) Důvěrné - musí být ostraha typu 4 nebo vyšší – tj. ostrahu zabezpečují pouze příslušníci ozbrojených sil nebo ozbrojených sborů a je vykonávána způsobem nepravidelných obchůzek. Ostraha provádí obchůzky v intervalu ne větším než 6 hodin, v noci a v mimopracovní době se četnost obchůzek zvyšuje. V průběhu výkonu ostrahy musí být na stanovišti stálé ostrahy neustále přítomna nejméně jedna osoba určená k výkonu ostrahy.

[1] Dříve souhrnně označované pulty centrální ochrany jsou dle normy ČSN EN 50518-1 s účinností od 1. ledna 2011 nově pojmenovány jako dohledová a poplachová přijímací centra (dále jen DPPC)..

b) Tajné - musí být ostraha typu 4 – s pravidelnými obchůzkami v intervalu nepřesahujícím 4 hodiny nebo ostraha vyšší.

c) Přísně tajné – musí být ostraha typu 5 – tj. ostrahu zabezpečují pouze příslušníci ozbrojených sil nebo ozbrojených sborů a je vykonávána způsobem nepravidelných obchůzek. Ostraha provádí obchůzky po náhodně vybraných trasách v náhodných intervalech ne větších než 2 hodiny. V průběhu výkonu ostrahy musí být na stanovišti stálé ostrahy neustále přítomna nejméně jedna osoba určená pro výkon ostrahy. [8]

2.1.3 Technické prostředky

Použití jednotlivých technických prostředků při zajišťování ochrany objektů, zabezpečených oblastí a jednacích oblastí v rámci fyzické bezpečnosti stanovuje příloha č. 1 vyhlášky č. 528/2005 Sb.

Technická ochrana utajovaných informací je založena jak na mechanických zábranných systémech, tak na elektronických systémech, jejichž hlavní funkce spočívá v detekci a vyhodnocení hrozby vůči objektu. Technické prostředky představují detekční systém zabezpečující předávání informací v chráněném prostoru. Hlavním cílem použití technické ochrany je zvýšení účinnosti (efektivity) jiných forem ochrany objektu.

Hlavní funkce technických prostředků spočívá v tom, že velmi rychle reagují na změny a demaskující příznaky vyvolané pachatelem. Díky svým fyzikálním a jiným parametrům lze změny indikovat i na značné vzdálenosti.

Při výběru technických prostředků vždy vycházíme ze skutečnosti, že účinnost a úroveň celého systému zabezpečení je dána podle nejslabšího článku systému a použité technické prostředky musí splňovat podmínky vzájemné kompatibility v návaznosti na možné připojení na dohledové a poplachové přijímací centrum.

Pro potřeby ochrany UI se používají následující technické prostředky a jejich kombinace:

a) mechanické zábranné prostředky, kterými jsou úschovné objekty, zámky, dveře, mříže, fólie, bezpečnostní rámy a skla,

b) elektrická zámková zařízení a systémy pro kontrolu vstupu,

c) poplachové zabezpečovací systémy,

d) speciální televizní systémy,

e) tísňové systémy,

f) zařízení elektrické požární signalizace,

g) zařízení, které slouží k vyhledávání nebezpečných látek nebo předmětů,

h) zařízení pro fyzické ničení nosičů informací,

i) zařízení proti pasivnímu a aktivnímu odposlechu.

K zajištění ochrany zabezpečených a jednacích oblastí se používají certifikované technické prostředky, kdy jednotlivé typy těchto prostředků musí být navrženy tak, aby splnily úroveň ochrany požadovanou pro daný stupeň utajení, tzn. je nutné, aby byly dodrženy minimální požadované hodnoty hodnocení úrovně fyzické bezpečnosti uvedené v příloze č. 1 vyhlášky.

Necertifikované technické prostředky lze použít u zabezpečených oblastí kategorie Vyhrazené, při ochraně hranice objektu a dále pouze za předpokladu, že nesníží úroveň ochrany požadované pro daný stupeň utajení.

K zajištění ochrany projednávaných utajovaných informací vedoucí organizačního celku vyžádá prostřednictvím bezpečnostního ředitele kontrolu, zda v jednací oblasti nedochází k nedovolenému použití technických prostředků určených k získávání informací. V jednacích oblastech tuto kontrolu zajišťuje Národní bezpečnostní úřad v součinnosti se zpravodajskými službami a Policií České republiky. V ostatních případech realizuje tuto kontrolu pro potřeby ministerstva Vojenské zpravodajství. [7]

2.2 Certifikace a podmínky používání technických prostředků

Při výběru technických prostředků a jejich kombinací je vhodné volit certifikované prvky, abychom měli jistotu jejich správné funkčnosti a předešli tak možným komplikacím s elektromagnetickou kompatibilitou.

Certifikace je postup, kdy NBÚ ověřuje způsobilost technického prostředku k ochraně UI a tuto způsobilost potvrdí vydáním certifikátu technického prostředku. Certifikáty nebo jejich kopie, včetně příloh, jsou nedílnou součástí technické dokumentace bezpečnostního projektu. Bodové ohodnocení technického prostředku se uvádí v aktuálním seznamu certifikovaných technických prostředků ve Věstníku NBÚ.

Platnost certifikátu se stanovuje nejdéle na dobu pěti let. Po uplynutí této doby se prostředky smí používat pouze tehdy, jsou-li plně funkční a tato skutečnost byla prověřena funkční zkouškou, popř. se může nově nasazovat, je-li doloženo, že byl pořízen v rezortu MO v době platnosti certifikátu za podmínky uskutečnění funkční zkoušky ke dni nasazení.

2.3 Návrh bezpečnostního projektu

Rozhodne-li vedoucí organizačního celku o doplnění dalších opatření, která není schopen vyřešit ve své působnosti (vyžaduje-li výstavba technických prostředků investiční prostředky), ustanovená komise zabezpečí zpracování návrhu bezpečnostního projektu, který schvaluje vedoucí organizačního celku. Návrh bezpečnostního projektu se zpracovává podle přílohy č. 1 NVMO č. 42/2006, která obsahuje strukturovaný formulář návrhu bezpečnostního projektu, a to pouze pro zabezpečenou oblast kategorie Důvěrné a vyšší.

V návrhu bezpečnostního projektu komise uvádí zejména:

- popis budovy (rozsáhlého areálu),
- popis současných technických prostředků,
- tabulku bodového ohodnocení současného stavu opatření fyzické bezpečnosti v zabezpečené oblasti a jednací oblasti,
- kategorie a třídy zabezpečené oblasti včetně stanovení hranic a jejich vyznačení v nákresu,
- druh jednací oblasti v závislosti na utajovaných informacích, které se v ní pravidelně projednávají včetně stanovení hranic a jejich vyznačení v nákresu,
- objekty včetně stanovení hranic a jejich vyznačení v nákresu,
- specifikaci požadovaných technických prostředků,
- specifikaci požadovaných stavebních úprav,
- stanoviště určené pro stálý výkon ostrahy objektu, tj. místo, kam budou vyvedena výstupní hlášení z technických prostředků, které vycházejí z možnosti střežení v rámci budovy nebo areálu,

- tabulku bodového ohodnocení opatření fyzické bezpečnosti v navrhované zabezpečené oblasti a jednací oblasti. [7]

Stupeň utajení návrhu bezpečnostního projektu stanovuje zpracovatel v souladu se seznamem utajovaných informací.

2.4 Dílčí závěr

Požadavky na zabezpečení chráněných prostorů v rámci fyzické bezpečnosti, ve kterých se nachází zabezpečené oblasti k projednávání a ukládání utajovaných informací, definuje zákon a prováděcím předpisem zákona je vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků.

Fyzická bezpečnost v rezortu Ministerstva obrany je řešena normativním výnosem č. 42/2006, o fyzické bezpečnosti v rezortu MO, který vychází ze zákona a dalších vyhlášek: č. 526/2005 Sb., o průmyslové bezpečnosti, vyhlášky č. 527/2005 Sb., o personální bezpečnosti a Rozkazu ministra obrany č. 22/2006 Sb., o ochraně utajovaných informací v resortu MO.

Opatření fyzické bezpečnosti se podle zákona rozdělují do tří částí, jimiž jsou ostraha, režimová opatření a technické prostředky. Cílem těchto opatření je stanovit pravidla, aby nedošlo k neoprávněnému nakládaní s utajovanou informací. Předpokladem použití technických prostředků nejen v rezortu MO je jejich certifikace NBÚ, a to na dobu nejdéle pěti let.

Pokud nedostačují realizovaná opatření fyzické bezpečnosti pro zabezpečenou oblast kategorie Důvěrné a vyšší, schvaluje vedoucí organizačního celku návrh bezpečnostního projektu, jehož strukturu stanovuje příloha č. 1 k NVMO č. 42/2006.

Specifikace možných opatření podle návrhu bezpečnostního projektu je realizována v projektu fyzické bezpečnosti.

3 ZÁSADY ZPRACOVÁNÍ PROJEKTU FYZICKÉ BEZPEČNOSTI

K zabezpečení ochrany utajovaných informací a k realizaci opatření fyzické bezpečnosti odpovědná osoba (vedoucí organizačního celku) schvaluje a zabezpečuje projekt fyzické bezpečnosti a jeho aktualizaci. Vychází přitom z podmínek uvedených ve vyhlášce č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, přílohy č. 1 a č. 2, ve znění vyhlášek č. 19/2008 Sb. a č. 454/2011 Sb. Pro potřeby MO uvedenou vyhlášku upravuje NVMO č. 42/2006, o fyzické bezpečnosti v rezortu MO a příloha č. 1 k uvedenému NVMO, která obsahuje strukturovaný formulář návrhu bezpečnostního projektu .

Návrh bezpečnostního projektu musí vycházet z koncepce bezpečnosti, což je pro každou organizaci její bezpečnostní politika. Jde o souhrn řídicích a organizačních pokynů, pravidel, norem, nařízení, specifických bezpečnostních požadavků organizace, jejichž cílem je ochránit organizaci proti vloupání, rozkrádání, ale i jiným nekriminálním jevům ohrožujícím stabilní provoz organizace, jako jsou havárie, požáry, výpadky provozu, nedbalost, nepozornost pracovníků a podobně.

3.1 Části projektu fyzické bezpečnosti podle typu kategorie zabezpečené nebo jednací oblasti

Projekt fyzické bezpečnosti se zpracovává pro každý objekt a rozsah zpracování závisí na kategorii „PT“, „T“, „D“ a „V“ zabezpečené nebo jednací oblasti (Tab. 2).

Tab. 2: Části projektu fyzické bezpečnosti podle typu kategorie zabezpečené (ZO) nebo jednací oblasti (JO)

Část projektu	**JO “V“- “PT“ ZO “D“- “PT“**	**ZO „V“**
Určení objektu a zabezpečených oblastí nebo jednacích oblastí, včetně hranic	X	X
Určení kategorií a tříd zabezpečených oblastí	X	X
Vyhodnocení rizik	X	-
Způsob použití opatření fyzické bezpečnosti	X	X
Provozní řád objektu	X	-
Plán zabezpečení objektu a zabezpečených a jednacích oblastí v krizových situacích	X	-
Technická dokumentace	X	-

3.2 Určení a ochrana objektu, zabezpečených oblastí a jednacích oblastí

Určení objektu, zabezpečených a jednacích oblastí, včetně jejich hranic a určení kategorií a tříd zabezpečených oblastí se v projektu zpravidla popisuje:

- obecným úvodem (adresou), popisem areálu/budovy (popis hranic, počet budov/počet podlaží, vstupy, případně zabezpečení), okolím (především objekty, které by mohly mít vliv na bezpečnost), cizími subjekty v areálu/budově (počet, případně název a zaměření činnosti), schématem,
- stanovením objektu, jeho kategorie a hranic (hranici objektu zakreslit do výkresové části Technické dokumentace bezpečnosti), určením typu objektu,
- popisem zabezpečení objektu,
- stanovením zabezpečených oblastí, jejich hranic, určením typu, kategorií a tříd,
- popisem zabezpečení zabezpečených oblastí, stanovením technických prostředků, režimových opatření, fyzické ostrahy, bodového hodnocení bezpečnostních opatření. [5]

3.2.1 Zabezpečení zabezpečených oblastí

Ochrana zabezpečených oblastí je zajišťována systémem opatření fyzické bezpečnosti, a to kombinací režimových opatření, ostrahy a technických prostředků.

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

a) „Přísně tajné“ – nejméně dvěma osobami na stálém stanovišti u objektu,

b) „Tajné“ – nejméně jednou osobou u objektu a 1 další osobou, které kombinace opatření elektrického zámkového zařízení a systémů pro kontrolu vstupů, zařízení elektrické zabezpečovací signalizace a zařízení elektrické požární signalizace umožní rychlý zásah v případě narušení ochrany UI,

c) „Důvěrné“ – nejméně jednou osobou, které kombinace elektrického zámkového zařízení systémů pro kontrolu vstupu a zařízení elektrické zabezpečovací signalizace umožnila rychlý zásah, dojde-li k narušení zabezpečených oblastí.

d) „Vyhrazené“ – ostraha se zajišťuje v rozsahu stanoveném odpovědnou osobou. [6]

Míra použití technických prostředků se stanoví v závislosti na kategorii („PT“, „T“, „D“, „V“) a třídě dané zabezpečené oblasti a vyhodnocení rizik.

Zabezpečené oblasti se podle přístupu k utajované informaci dělí do třídy I., kdy vstupem do této oblasti dochází k seznámení s utajovanou informací a do třídy II., kdy vstupem do této oblasti nedochází k seznamování s utajovanou informací. Neoprávněná osoba smí vstoupit pouze do zabezpečené oblasti třídy II., a to s osobou, která má do této oblasti povolen vstup. Pohyb do a ze zabezpečené oblasti musí být kontrolován opatřeními fyzické bezpečnosti.

Rozsah použití technických prostředků je pro jednotlivé kategorie stanoven:

a) kategorie „Vyhrazené“ – mechanické zábranné prostředky,

b) kategorie „Důvěrné“ – mechanické zábranné prostředky a poplachové zabezpečovací systémy,

c) kategorie „Tajné a Přísně tajné“ – mechanické zábranné prostředky, systémy pro kontrolu vstupu, poplachové zabezpečovací systémy, 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.

Zabezpečené oblasti kategorie Důvěrné a vyšší, v nichž je trvale zajištěna přítomnost zde pracujících osob, se zabezpečují zejména mechanickými zábrannými prostředky a poplachovými zabezpečovacími nebo tísňovými systémy. Plní-li tyto zabezpečené oblasti současně úlohu stanovišť určených pro stálý výkon ostrahy, nemusí být vybaveny zařízeními poplachových zabezpečovacích systémů. Při použití speciálních televizních systémů nesmí být narušena ochrana utajovaných informací. K zajištění ochrany zabezpečených oblastí se používají certifikované technické prostředky. [5]

Necertifikované technické prostředky se mohou použít za předpokladu, že se nesníží úroveň ochrany požadovaná pro daný certifikovaný stupeň utajení. Pro kategorii Vyhrazené je možné použít certifikované i necertifikované technické prostředky.

Zabezpečení zabezpečené oblasti se zajišťuje také na hranici objektu, ve kterém se tato oblast nachází. Rozsah použití technických prostředků je stanoven v závislosti na nejvyšší kategorii zabezpečené oblasti, která se nachází v objektu, na základě vyhodnocení rizik s ohledem na charakter hranice objektu:

a) pro zabezpečenou oblast kategorie „Vyhrazené“ – mechanické zábranné prostředky,

b) pro zabezpečenou oblast kategorie „Důvěrné“ a „Tajné“ – mechanické zábranné prostředky a poplachové zabezpečovací systémy,

c) pro zabezpečenou oblast kategorie „Tajné a Přísně tajné“ – mechanické zábranné prostředky, poplachové zabezpečovací systémy, speciální televizní systémy. [7]

Utajovaná informace se ukládá v zabezpečené oblasti, popřípadě v úschovném objektu, je-li jeho bodová hodnota použita v projektu fyzické bezpečnosti pro příslušnou zabezpečenou oblast.

V objektu je také zákonem stanoveno umístění zařízení fyzického ničení nosičů informací.

3.2.2 Zabezpečení jednacích oblastí

Ochrana zabezpečených oblastí je zajišťována systémem opatření fyzické bezpečnosti, kde se rozsah těchto opatření stanoví v závislosti na stupni utajovaných informací, které jsou v jednací oblasti pravidelně projednávány, a na vyhodnocení rizik.

Ostraha je u objektu, ve kterém se nachází jednací oblast, kde se pravidelně projednávají utajované informace stupňů utajení Přísně tajné a Tajné, zajišťována stejně jako u zabezpečených oblastí uvedených stupňů utajení.

Jednací oblasti pro pravidelné projednávání utajovaných informací stupňů utajení Tajné a Přísně tajné se zabezpečují mechanickými zábrannými prostředky, systémy pro kontrolu vstupů, zařízeními poplachových zabezpečovacích systémů, speciálními televizními systémy (lze je nahradit tísňovými systémy), zařízeními elektrické požární signalizace, zařízeními pro pasivní a aktivní odposlech utajované informace. K zajištění ochrany jednacích oblastí se používají certifikované technické prostředky. Necertifikované technické prostředky lze použít pouze za předpokladu, že se nesníží úroveň ochrany požadované pro daný stupeň utajení. [6]

V případě, že hranice objektu je totožná s hranicí jednací oblasti, je rozsah použití opatření fyzické bezpečnosti stanoven požadavky na zabezpečení jednací oblasti.

Orgán státu, právnická osoba nebo podnikající fyzická osoba jsou povinny provádět průběžně hodnocení rizik a poté upravovat míru opatření fyzické bezpečnosti a také pravidelně ověřovat, zda použitá opatření fyzické bezpečnosti odpovídají projektu fyzické

bezpečnosti a právním předpisům v oblasti ochrany utajovaných informací (nejméně však každých 12 měsíců).

3.3 Zabezpečení technického zařízení

V projektu fyzické bezpečnosti, který řeší ochranu technického zařízení, se rozpracují opatření fyzické bezpečnosti v návaznosti na technické prostředky a překážky, které zpomalují útočníka na cestě k utajované informaci v technickém zařízení a dále se stanovují časové limity zásahu ostrahy. V tomto případě se nezpracovávají tabulky bodového ohodnocení.

Ostraha uloženého technického zařízení obsahujícího utajovanou informaci stupně utajení:

a) „Přísně tajné“ – se zajišťuje typem 5 podle přílohy č. 1 vyhlášky č. 528/2005 Sb.,

b) „Tajné“ – se zajišťuje minimálně typem 4 podle výše uvedené přílohy,

c) „Důvěrné“ – se zajišťuje minimálně typem 3 podle uvedené přílohy,

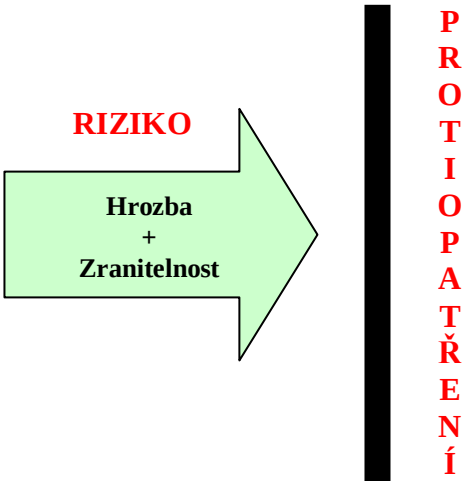
d) „Vyhrazené“ – se zajišťuje v rozsahu stanoveném odpovědnou osobou.

Odpovědná osoba také stanovuje časové limity pro zásah ostrahy v okamžiku narušení objektu útočníkem. Čas se určuje podle druhu a počtu technických zařízení a jiných překážek, které musí pachatel překonat při cestě k utajované informaci. Zásah je prováděn minimálně dvěma osobami. [6]

3.4 Vyhodnocení rizik

Rozsah, podmínky a způsob použití opatření fyzické bezpečnosti na ochranu chráněných prostorů se stanovuje na základě vyhodnocení rizik možného ohrožení.

Riziko lze chápat jako pravděpodobnost vzniku škody, tj. ohrožení lidského zdraví a životů, životního prostředí, majetkových a kulturních hodnot a také újmu v oblasti utajovaných informací. Pro účely analýzy rizik objektu s utajovanými informacemi je vhodnější riziko definovat prostřednictvím hrozby (nebezpečnosti) a zranitelnosti aktiva, které je třeba stanovit. Hrozba je potenciál poškodit analyzovaný cílový systém. Zranitelnost je dána odolností a vnímavostí cíle, který je potenciálně mimořádnou událostí ohrožen. [9]



Obr. 2. Systém zabezpečení aktiv

Vyhodnocení rizik a stanovení jejich míry v rezortu MO vychází z vyhlášky č. 528/2005 Sb. a dále interního předpisu v souladu s čl. 3 odst. 15 NVMO č. 42/2006.

Výše uvedená legislativa, vycházející ze zákona č. 412/2005 Sb., neurčuje blíže jakým způsobem se má v jednotlivých bodech vyhodnocení rizik postupovat, což považuji za nedostačující. Pro tuto potřebu budu používat další nástroje analýzy a managementu rizik, které podrobněji vypovídají o konkrétních krocích.

3.4.1 Klasifikace a řízení aktiv

Aktivy u organizačních celků MO (dále jen OC) mohou být informace, které jsou utajované, utajované dokumenty, technická zařízení, zbraně a technologie. Uvedená aktiva mohou být vyhodnocena různými stupni utajení, mohou vyžadovat různou úroveň bezpečnosti nebo zvláštní způsoby zacházení. U OC by měl proto existovat systém bezpečnostní klasifikace, který určuje adekvátní stupeň ochrany a který dává uživatelům informace o nutnosti zvláštního zacházení s konkrétním aktivem.

Je důležité posoudit hodnotu aktiva pro zájmové subjekty, např. zájem o získání utajované informace pro teroristické organizace, politické skupiny atd.

3.4.2 Specifikace hrozeb

Pod pojmem hrozba (ohrožení) se chápe označení konkrétního, fyzicky existujícího subjektu, jevu, okolnosti nebo události s potenciálem způsobit újmu (škodu, ztrátu), jako důsledek neoprávněného nakládání s utajovanou informací. Proces stanovení hrozby

spočívá v odhalení možných negativních událostí a jevů, které existují v různých podobách v bezpečnostním prostředí a které mohou přivodit ohrožení utajované informace. [10]

Cílem identifikace hrozeb je:

a) identifikace zdrojů ohrožení ve vztahu k ochraně utajovaných informací,

b) zjištění motivů a příčin ohrožení,

c) analýza výskytu hrozeb v minulosti,

d) stanovení velikosti každé identifikované hrozby. [10]

Předmětem analýzy bezpečnostního prostředí, jejímž cílem je zajistit věrohodné a aktuální informace o situaci a stavu vnějšího a vnitřního bezpečnostního prostředí vzhledem k možným hrozbám, mohou být informace o:

- charakteristikách okolí objektu, přírodních podmínkách v daném prostředí, rozsahu a závažnosti živelných pohrom, které by mohly objekt ohrozit;
- charakteristikách objektu, jeho struktuře, stavu ochrany;
- sociálních kriminogenních faktorech, a to jak vnějších, tak ve vztahu k vlastním zaměstnancům;
- možnosti využití zásahových jednotek, atd.

Po uzavření analýzy bezpečnostního prostředí následuje vytvoření seznamu jednotlivých hrozeb, které se mohou vztahovat k chráněnému prostoru, s jejich následným hodnocením. Takovými hrozbami mohou být například skutečnosti, uvedené v seznamu hrozeb v Příloze č. 1 (P I) této práce.

Hodnocením analyzovaných hrozeb bezpečnostního prostředí je slovní nebo číselné vyjádření ke každé hrozbě. Toho lze dosáhnout stanovením velikosti ohrožení, které může vzniknout na základě vzájemných vztahů různých faktorů (Tab. 3).

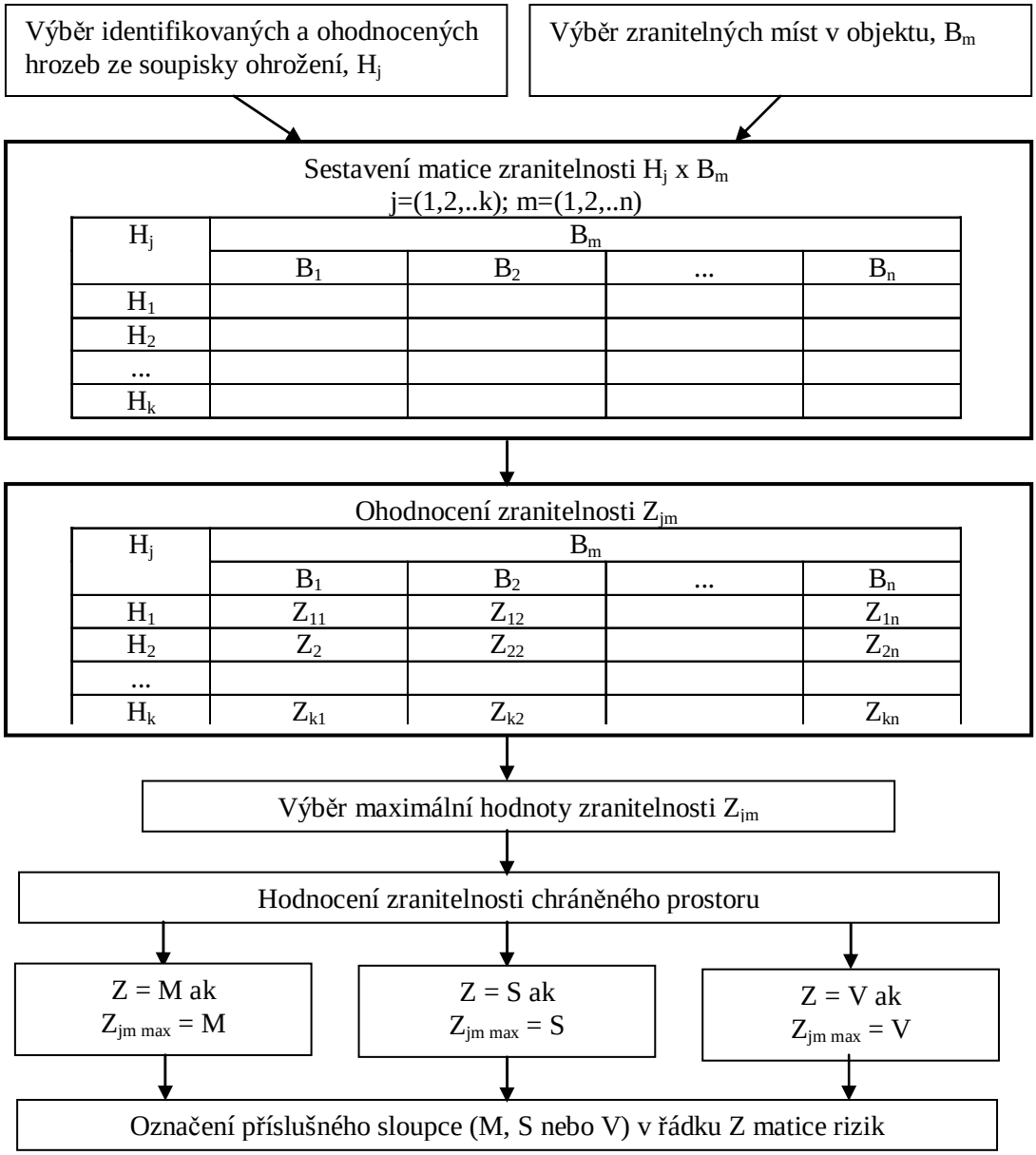
Tab. 3. Postup a kritéria hodnocení hrozeb [10]

Existuje zdroj ohrožení?	**Je známa motivace, záměr útočníka? Existují příčiny?**	**Existují příčiny výskytu z minulosti?**	**Hodnocení zranitelnosti**
Ano	Ano	Ano	Velké (V)
Ano	Ano	Ne	Velké (V)
Ano	Nejisté určení	Ne	Střední (S)
Ano	Ne	Ne	Malé (M)
Nejisté definování	Ne	Ne	Malé (M)
Nejisté definování	Nejisté definování	Ne	Malé (M)
Ne	Ne	Ne	Ohrožení neexistuje (0)

3.4.3 Hodnocení zranitelnosti

Spočívá v odhalení nejslabších článků - kritických míst v systému ochrany objektu anebo aktiva, které mohou být překonány identifikovanými hrozbami, osobami nápomocnými útočníkovi k získání neoprávněného přístupu k UI a manipulaci s ní a vyjadřuje možnost, jak může dané ohrožení narušit nebo ochromit bezpečnost objektu.

Příklad algoritmu hodnocení zranitelnosti chráněného prostoru znázorňuje obrázek (Obr. 3).



Obr. 3. Příklad algoritmu zranitelnosti chráněného prostoru [10]

Výběr identifikovaných a hodnocených hrozeb

Výsledkem stanovení zranitelnosti je výběr identifikovaných hrozeb ze soupisky ohrožení, které byly hodnoceny minimálně jako malé (M), na hrozby s hodnocením 0 se nebere ohled.

Výběr zranitelných míst objektu a chráněného prostoru

Zranitelná místa v objektu a chráněném prostoru B_m mohou být:

- B1: perimetr objektu, okolí objektu, přístupy k objektu,

- B2: stavební prvky objektu (stěny, podlahy, stropy, střechy),
- B3: otvorové výplně (vstupy, dveře, okna, větrací a technologické otvory),
- B4: zaměstnanci, cizí osoby,
- B5: způsob manipulace s utajovanými informacemi (např. ukládání, vytváření),
- B6: fyzická ochrana objektu a chráněného prostoru,
- B7: ochrana vnitřních prostorů technickými prostředky, režimová opatření. [10]

Hodnocení zranitelnosti

Hodnocení zranitelnosti vyjadřuje možnost využití zranitelného místa objektu nebo chráněného prostoru daným typem hrozby k ohrožení bezpečnosti objektu nebo utajované informace.

Stupnice hodnocení zranitelnosti může být následující:

- **malá zranitelnost (M) -** dané ohrožení může jen těžko využít zranitelného místa na ohrožení UI,
- **střední zranitelnost (S)** - pokud existuje možnost, že zranitelné místo bude daným ohrožením překonané,
- **velká zranitelnost (V)** - představuje vysokou pravděpodobnost zneužití zranitelného místa k získání přístupu k UI.

Tímto způsobem se hodnotí každý typ ohrožení H_j s každou skupinou zranitelných míst B_m a výsledek se zapíše do příslušného pole matice Z_{jm}. Výsledná zranitelnost objektu je daná hodnotou zranitelnosti toho zranitelného místa, které bylo ohodnoceno jako nejzranitelnější. [10]. Příklad matice hodnocení zranitelnosti znázorňuje tabulka (Tab. 4).

Tab. 4. Matice hodnocení zranitelnosti

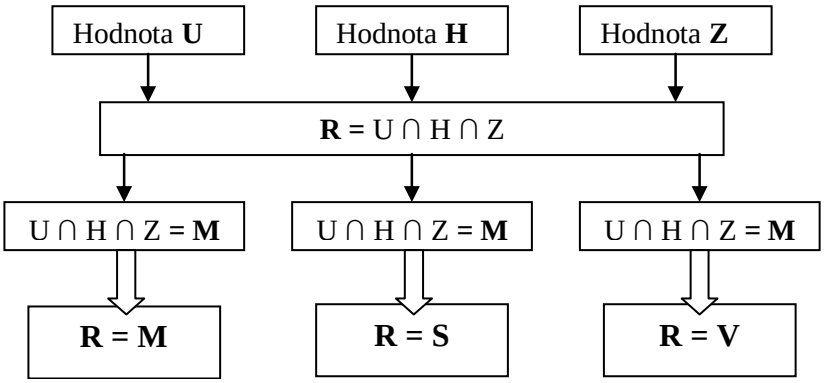
Hrozby H_j	**Zranitelná místa B_m**			
	B_1	**B_2**	**B_3**	**B_4**
H_3	Z_{31}	Z_{32}	Z_{33}	Z_{34}
H_4	Z_{41}	Z_{42}	Z_{43}	Z_{44}
H_5	Z_{51}	Z_{52}	Z_{53}	Z_{54}

Stanovení míry rizika

Míra rizika ohrožení (R) UI se stanoví jako funkce faktorů, a to **velikosti újmy (U)**, která může vzniknout jako následek neoprávněné manipulace s UI, **velikosti hrozby (H)**, která

byla identifikovaná v bezpečnostním prostředí chráněného prostoru a **zranitelnosti (Z)** objektu (Obr. 4).

Konečná míra rizika je stanovena jako průnik těchto faktorů – **R = U ∩ H ∩ Z.**



Obr. 4. Možný postup při stanovení míry rizika [10]

Tab. 5. Příklad použití matice rizik při určení míry rizika ohrožení UI [10]

Velikost újmy U	**Velikost ohrožení H**								
	MALÁ			STŘEDNÍ			VELKÁ		
	Zranitelnost Z								
	Malá	Střední	Velká	Malá	Střední	Velká	Malá	Střední	Velká
Nevýhodné pro zájmy ČR	M	M	M	M	S	S	S	S	V
Prostá újma	M	M	M	S	S	S	S	V	V
Vážná újma	M	S	S	S	S	V	V	V	V
Mimořádně vážná újma	S	S	S	S	V	V	V	V	V

Výsledná hodnota míry rizika ohrožení UI nadále slouží vedoucímu organizačního celku k posouzení dostatečnosti bezpečnostních opatření podle tabulek minimálních požadovaných bodových ohodnocení opatření fyzické bezpečnosti chráněných prostorů.

3.5 Bodové hodnocení opatření fyzické bezpečnosti

Míra zabezpečení opatřeními fyzické bezpečnosti jednacích a zabezpečených oblastí se stanovuje na základě bodového ohodnocení těchto opatření v závislosti na vyhodnocení

rizik. Bodové hodnoty pro konkrétní opatření specifikuje prováděcí předpis, a to příloha č. 1 vyhlášky č. 528/2005 Sb.

Jednotlivá opatření fyzické bezpečnosti musí splňovat alespoň nejnižší míru zabezpečení zabezpečené nebo jednací oblasti. Tato nejnižší míra se stanoví na základě vyhodnocení rizik a rozhodnutí o tom, jakého stupně utajení budou informace projednávané v jednací oblasti nebo na kategorii zabezpečené oblasti.

Příloha č. 1 vyhlášky 528/2005 Sb. obsahuje tabulky s bodovými hodnotami nejnižší míry zabezpečení bezpečnostních opatření. Po vyhodnocení rizik a přidělení bodového ohodnocení jednotlivým opatřením se rozhodne, zda jsou tato opatření dostačují nebo nikoliv. Pokud je dosaženo požadovaných bodových hodnot, ale z vyhodnocených hrozeb se opatření jeví jako nedostačující, je nutné zvážit použití dalších doplňujících opatření.

3.6 Provozní řád objektu

Provozní řád je samostatný dokument, upravující primárně podmínky a způsob užívání objektu v pracovní i mimopracovní době. Stanovuje pravidla pro režim pohybu osob a dopravních prostředků, manipulaci s klíči a identifikačními údaji, technickými prostředky a pravidla pro výkon ostrahy v areálu, objektu, zabezpečených a jednacích oblastech.

Režim manipulace s klíči a identifikačními daty je nedílnou součástí opatření k ochraně UI a stanovuje se v provozním řádu objektu, který je součástí projektu fyzické bezpečnosti pro objekt, ve kterém se nacházejí zabezpečené oblasti kategorie Důvěrné a vyšší nebo jednací oblasti a nebo obojí.

Ochrana identifikačních dat je dána způsobem správy a nastavením přístupových práv v elektrických zámkových zařízeních a systémech pro kontrolu vstupu, poplachových zabezpečovacích a tísňových systémech (dále jen PTZS) a úložnách klíčů.

Režim manipulace s klíči od zabezpečené oblasti, kde se ukládají utajované informace stupně utajení „V“, stanovuje provozovatel objektu. Pro manipulaci s klíči od zabezpečené oblasti, kde se ukládají utajované informace stupně utajení „D“ a vyššího, jsou stanovena zvláštní pravidla pro manipulaci s hlavním klíčem, duplikátem a klíčem revizním.

V provozním řádu jsou také určeny zásady pro vytváření úložen klíčů od úschovných objektů podle kategorie zabezpečené a jednací oblasti, pravidla pro označování

jednotlivých klíčů a schránek na ně, vedení přehledu o pohybu schránek s klíči a postup při ztrátě a nouzových otevřeních zabezpečených prostorů.

3.7 Technická dokumentace pro navrhovaná opatření fyzické bezpečnosti objektu

Podle vyhlášky č. 528/2005 Sb. technická dokumentace pro navrhovaná opatření fyzické bezpečnosti obsahuje následující části:

a) výkresovou dokumentaci – obsahuje technické nákresy hranic objektu, jednotlivých zabezpečených a jednacích oblastí a rozmístění technických prostředků k ochraně utajované informace,

b) dokumentaci certifikovaných i necertifikovaných technických prostředků s jejich výčtem, kopiemi certifikátů a zápisy o posouzení shody, a to vše z doby instalace.

3.8 Východiska při návrhu bezpečnostního projektu

Při zavádění technických prostředků ochrany a jejich prvků ve vojenských objektech se používá řada technických norem, které klasifikují bezpečnost jednotlivých systémů do několika stupňů (ČSN EN 50 131-1 pro poplachové zabezpečovací a tísňové systémy). Jednotlivé zabezpečovací prvky jsou poté rozděleny do podskupin a mají přiděleny své bezpečnostní třídy (ČSN P ENV 1627 pro okna, dveře a uzávěry). [11]

Pro efektivní aplikování prostředků ochrany v objektu je nutné provést bezpečnostní posouzení objektu k identifikaci možných nebezpečí, klasifikovat správné prostředí, ve kterém se prvky technické bezpečnosti budou umisťovat a odhadnout možnou míru rizika, kterou pachatelé způsobí narušením objektu.

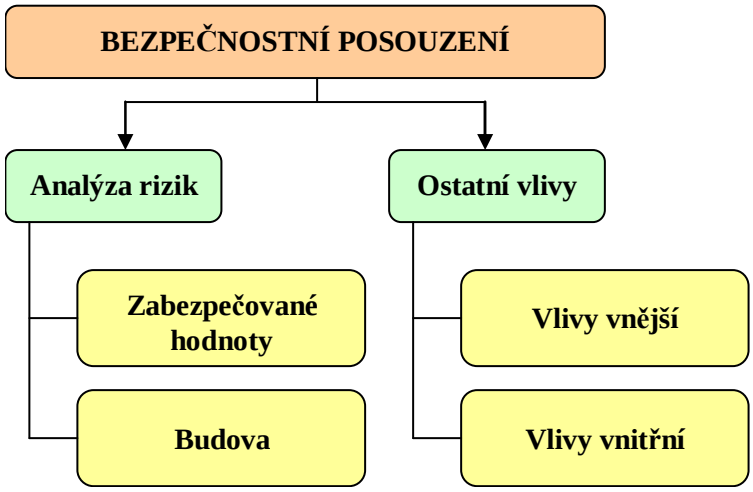
3.8.1 Bezpečnostní posouzení objektu

Bezpečnostní posouzení objektu je oblast, která je při návrhu bezpečnostního projektu v rezortu MO zahrnuta jen velmi okrajově. Význam bezpečnostního posouzení objektu spočívá zejména v získání a zpracování informací potřebných pro vytvoření návrhu PZTS.

Primární problematikou při sestavování návrhu projektu fyzické bezpečnosti je otázka, jaký majetek je potřeba ochraňovat, stanovit rozsah a charakter majetku, který se ve střežených prostorech nachází. Je proto nezbytné provést bezpečnostní posouzení střežených prostorů

s cílem odhalit faktory, které by mohly mít vliv v průběhu přípravy projektu na volbu komponentů a jejich umístění a stanovit požadovaný stupeň zabezpečení.

Bezpečnostní posouzení je založeno na vyhodnocení čtyř základních oblastí zájmu, které by měly být brány v úvahu při následném návrhu PZTS, respektive při zpracování projektové dokumentace. Jedná se o zabezpečované hodnoty, budovu, vnější a vnitřní vlivy. Tyto oblasti je možné klasifikovat do dvou skupin – analýza rizik a ostatní vlivy (Obr.5). Podrobnější výklad jednotlivých položek je možno nalézt v ČSN CLC/TS 50131-7. [12]



Obr. 5. Oblasti zájmu bezpečnostního posouzení [13]

Bezpečnostní posouzení – zabezpečované hodnoty

V této souvislosti je vhodné brát v úvahu následující faktory:

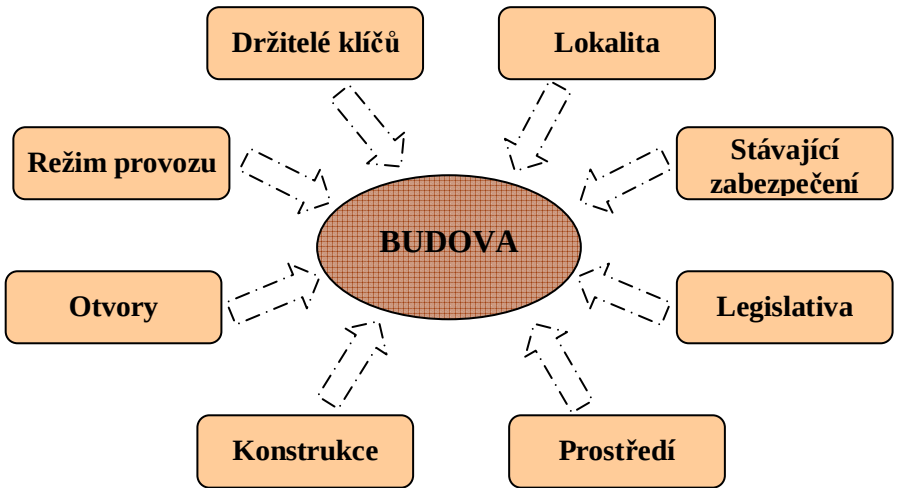
- **Druh majetku** – lze konstatovat, že míra rizika vloupání do objektu je přímo úměrná druhu aktiv, které se v objektu nacházejí, jejich atraktivitě pro pachatele nebo možnosti jejich snadného zpeněžení [13]. Pro oblast Ministerstva obrany lze brát v úvahu možnost loupeže, jejímž cílem by mohly být např. utajované informace (uložené v informačním systému nebo v listinné podobě) a speciální zbraňové (technické) systémy.
- **Hodnota majetku** – jedná se o zcela zásadní údaj nejen pro tvůrce návrhu PZTS, ale i pro pojišťovny, který výrazným způsobem ovlivňuje konečnou podobu zabezpečení objektu. Tato hodnota by měla zahrnovat nejen okamžitou peněžní hodnotu chráněného majetku, ale také případné následné výdaje související

se ztrátou, či osobní vztah k daným věcem. [13] Hodnota majetku Ministerstva obrany je dána jejím charakterem. V praxi to znamená zajistit zabezpečení vojenských prostředků, které mají ochraňovat svobodu a bezpečnost státu.

- **Množství nebo velikost** – zde se zaměřujeme především na snadnost odejmutí, následnou manipulaci, transport, ukrytí, či případné zpeněžení chráněných aktiv. [13]
- **Historie krádeží** – poukazuje se na četnost a způsoby vloupání při předcházejících krádežích u podobných objektů. [13]
- **Nebezpečí** – u tohoto bodu se bere v potaz vznik možného nebezpečí pro okolní prostředí a osoby v okolí, způsobené odcizením střeženého majetku nebo jeho zneužitím. [13]
- **Poškození** – mimo rizika krádeže aktiv se zohledňuje také škoda na majetku způsobená vandalismem či žhářstvím. [13]

Bezpečnostní posouzení – budova

Při obhlídce objektu MO je pro posouzení rizik vhodné brát v úvahu části budovy a ovlivňující faktory, uvedené ve schématu (Obr. 6):



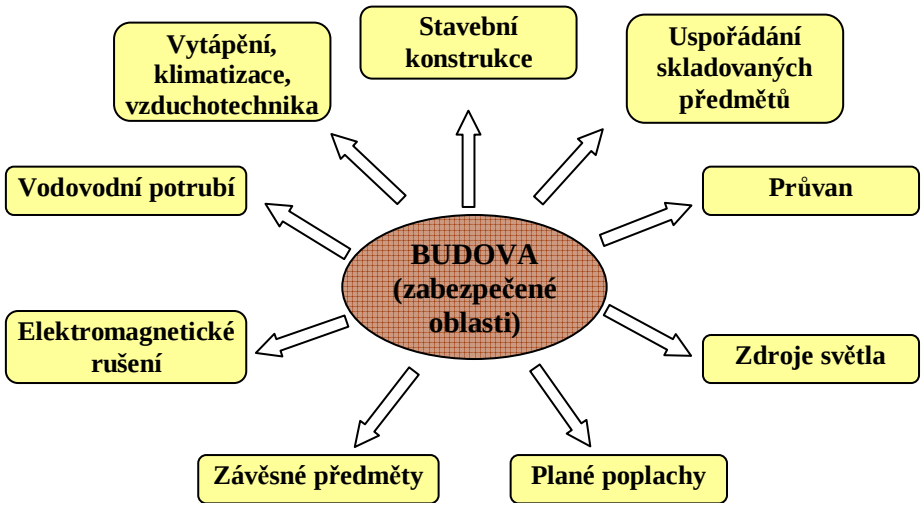
Obr. 6. Faktory ovlivňující bezpečnostní posouzení budovy

Bezpečnostní posouzení – vnitřní vlivy

Uvnitř posuzovaného vojenského objektu se může objevovat celá řada faktorů, působících na funkce PZTS. Na tyto činitele je nutné brát ohled při volbě komponentů, neméně

důležitý je lidský faktor uvnitř objektu, jehož negativní vlivy lze eliminovat jistými režimovými opatřeními.

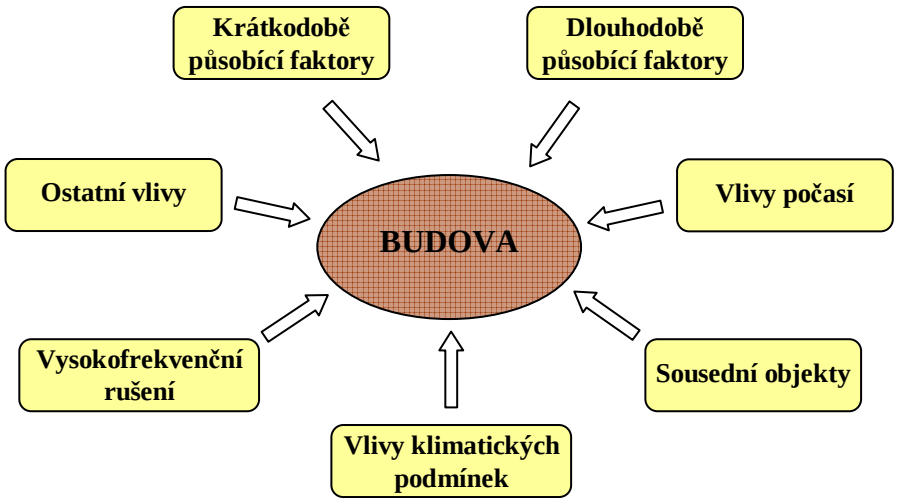
Nejčastější vnitřní vlivy [13] ukazuje obrázek (Obr. 7).



Obr. 7. Bezpečnostní posouzení – vnitřní vlivy

Bezpečnostní posouzení – vnější vlivy

Při bezpečnostním posouzení vojenského objektu z pohledu vnějších vlivů [13] je nutné si uvědomit, že tyto vlivy nelze nijak ovlivnit, ale musí se na ně brát zřetel, protože by mohly negativně ovlivnit funkce zařízení PZTS.



Obr. 8. Bezpečnostní posouzení – vnější vlivy

3.8.2 Stupeň zabezpečení

Stupeň zabezpečení systému PZTS, který podléhá potřebné úrovni zabezpečení podle analýzy rizik, definuje norma ČSN CLC/TS 50 131-7 (Tab. 6).

Tab. 6. Stupně zabezpečení systému PZTS ČSN CLC/TS 50 131-7 [13]

Stupeň zabezpečení		**Způsob napadení**
1.	Nízké riziko	Předpokládá se, že narušitelé mají malou znalost o technickém zabezpečení objektu a že mají k dispozici omezený sortiment snadno dostupných nástrojů.
2.	Nízké až střední riziko	Předpokládá se, že narušitelé mají určité znalosti o technickém zabezpečení objektu a že použijí základní sortiment nástrojů a přenosných přístrojů.
3.	Střední až vysoké riziko	Předpokládá se, že narušitelé jsou obeznámeni s technickým zabezpečením objektu a že mají úplný sortiment nástrojů a přenosných elektronických přístrojů.
4.	Vysoké riziko	Předpokládá se, že narušitelé mají podobné zdroje pro zpracování podrobného plánu vniknutí a mají kompletní sortiment zařízení včetně prostředků umožňujících nahradit rozhodující prvky technického zabezpečení objektu.

3.8.3 Třída prostředí

Norma ČSN CLC/TS 50 131-7 určuje čtyři třídy prostředí, na jejichž vlastnostech záleží při volbě a umisťování komponentů systémů PZTS.

Tab. 7. Třídy prostředí [14]

Třída		**Popis**
I.	Prostřední vnitřní	Funkčnost komponentu nesmí být ovlivněna běžným provozem ve vytápěných místnostech. Předpokládá se rozsah změn teplot v intervalu +5 °C až +40 °C a střední relativní vlhkost přibližně 75 % bez kondenzace.
II.	Prostředí vnitřní všeobecné	Komponenty musí být odolné vlivům prostředí, kde není udržována stálá teplota. Rozsah teplot se smí pohybovat v rozmezí -10 °C až +40 °C a střední relativní vlhkost přibližně 75 % bez kondenzace.
III.	Prostředí venkovní chráněné	Stav prvků by neměl být ovlivněn působením vlivů vyskytujících se vně budov. Nepočítá se s přímým ohrožením prvků vlivem nepříznivého počasí. Rozsah teplot se smí pohybovat v rozpětí -25 °C až +50 °C a střední relativní vlhkost přibližně 75 % bez kondenzace. Během roku se může změnit relativní vlhkost v rozmezí 85 % až 95 % po dobu 30 dní.
IV.	Prostřední venkovní všeobecné	Stav prvků by neměl být ovlivněn působením vlivů vyskytujících se vně budov a počítá se s přímým ohrožením prvků vlivem nepříznivého počasí. Rozsah teplot se smí pohybovat v rozmezí -25 °C až +60 °C a střední relativní vlhkost přibližně 75 % bez kondenzace. Během roku se může změnit relativní vlhkost v rozmezí 85 % až 95 % po dobu 30 dnů.

3.8.4 Volba a umístění komponentů zabezpečovacího systému

Volba komponentů je část návrhu zabezpečovacího systému objektu, kterou je nezbytné se zabývat po krocích, uvedených v předchozích kapitolách.

Při návrhu zabezpečení mají být voleny komponenty odpovídajícího stupně zabezpečení a třídy prostředí. Je třeba věnovat patřičnou pozornost minimalizaci planých poplachů. Je dobré volit certifikované prvky, protože se lze spolehnout na informace od výrobce o vlastnostech a testování výrobku a lze tím předejít případným dysfunkcím.

Umístění komponentů podle normy ČSN CLC/TS 50 131-7 stanovuje podmínky, za jakých se mají prvky systémů umístit do prostoru, který mají zabezpečovat a to s přihlédnutím k faktům, aby byly co nejlépe využity jejich funkce a zda-li jsou ke konkrétnímu umístění vůbec vhodné.

3.9 Dílčí závěr

Ve stávající rozsáhlé kapitole jsem se snažila analyzovat zásady návrhu projektu fyzické bezpečnosti v rezortu MO. Vycházela jsem z legislativních požadavků jak zákona a prováděcích vyhlášek, tak z rezortních rozkazů a normativního výnosu.

Byly zde specifikovány jednotlivé části projektu, mezi něž patří určení a ochrana objektu, zabezpečených a jednacích oblastí, popis způsobu zabezpečení technického zařízení, části technické dokumentace k projektu. Jako zcela nedostačují jsem shledala systém vyhodnocení rizik, kdy není blíže určeno, jakým způsobem se má v jednotlivých bodech postupovat. Možné hrozby, uvedené v šabloně bezpečnostního projektu, uvádí pouze základní škálu těchto hrozeb, takže nedostatečně poučená zodpovědná osoba nemusí být schopna další možné hrozby specifikovat, pojmenovat a vyhodnotit v návaznosti na zranitelnost objektu, zabezpečené nebo jednací oblasti. V této souvislosti by se jevilo jako vhodné vytvoření katalogu hrozeb, který by pomáhal zodpovědné osobě, jako pomocný podkladový materiál, při jejich specifikaci a vyhodnocení.

Potřeba vyhodnocení ohrožení aktiv v rezortu MO a následné určení bezpečnostních opatření vychází ze zákona. Vzhledem k hodnotě zabezpečovaného majetku MO s různými stupni utajení se mi jeví, dle výše uvedeného, šablona projektu fyzické bezpečnosti jako nedostatečná.

4 VÝCHOZÍ PODMÍNKY PRO NÁVRH ZABEZPEČENÍ VÝCVIKOVÉHO PRACOVIŠTĚ

V následující kapitole se budu zabývat výchozími podmínkami pro návrh zabezpečení modelového výcvikového pracoviště. Modelové pracoviště bude popsáno a umístěno ve stávající zástavbě areálu kasáren, popsán samotný modelový objekt, jeho okolí, specifikována aktiva, vyhledána a analyzována rizika a zranitelnost objektu s návazností na bodové ohodnocení a určení nejnižší míry zabezpečení modelového objektu perspektivního výcvikového pracoviště.

4.1 Charakteristika modelového pracoviště

4.1.1 Klasifikace pracoviště

Modelové vojenské výcvikové pracoviště (dále jen „MVVP“) je majetkem Ministerstva obrany ČR s celoarmádní působností. Je špičkovým a jedinečným pracovištěm v AČR, jehož posláním je naplnit velkou a poměrně rozmanitou škálu činností a požadavků v oblasti přípravy vojenských profesionálů a příslušníků dalších bezpečnostních jednotek.

MVVP je určeno k přípravě velitelů a štábů do stupně brigáda (včetně štábů krizového řízení) s využitím virtuální a konstruktivní simulace a zabezpečení výcviku velitelů a jednotek do stupně rota, výcviku osádek bojových vozidel a vybraných odborností dělostřelectva prostřednictvím více druhů simulátorů.

Virtuální simulace je simulace, při které reální lidé obsluhují simulované systémy (např. obsluhují simulátory bojových vozidel). Tyto simulace umožňují získávat a rozvíjet základní senzorické a psychomotorické schopnosti (řízení bojového vozidla, střelba z bojového vozidla atd.), rozhodovací schopnosti (např. rozdělení palebných prostředků k ničení nepřítele u své jednotky, rozhodovaní o směru postupu atd.) a komunikační schopnosti (např. rádiový provoz dle provozního řádu na základě smluvených signálů).

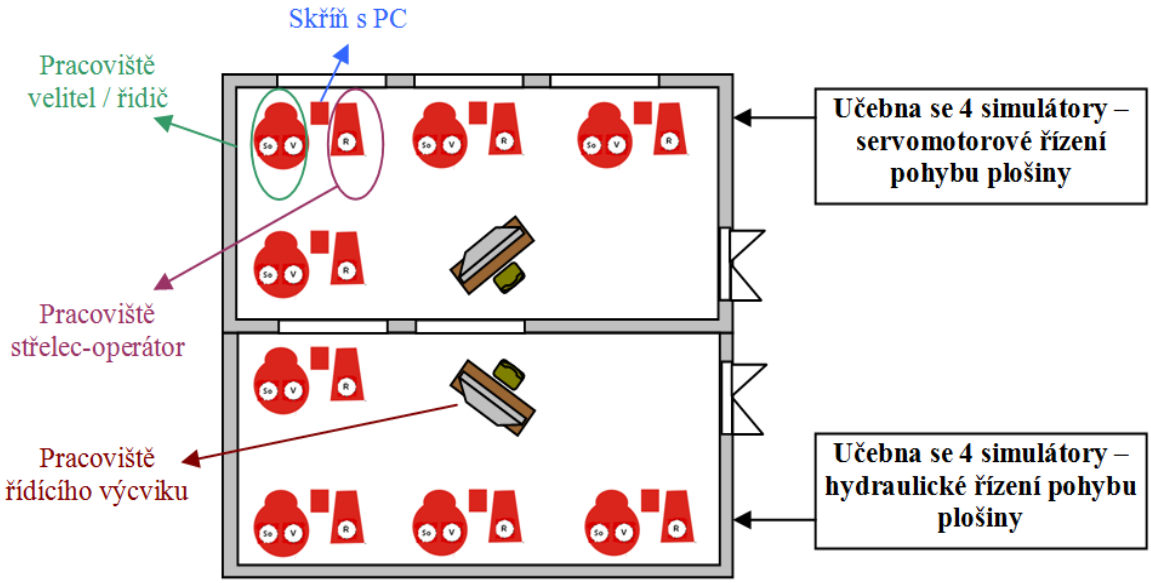
Konstruktivní simulace je výcviková simulace využívající sofistikované programové vybavení simulující syntetické prostřední bojiště. Konstruktivní simulací jsou cvičeni velitelé a jejich štáby v řízení bojových i nebojových operací. U této simulace „simulovaní“ lidé (matematické modely jejich myšlení) obsluhují a řídí simulované systémy (např. simulovanou bojovou techniku, simulované jednotky atd.). Reální lidé částečně ovlivňují

konstruktivní simulace vkládáním svých rozhodnutí, nemohou však ovlivňovat výsledky těchto simulací.

Učebny se simulátory (Obr. 9) jsou v objektu specifikovány následovně:

- v objektu se nachází pracoviště: dvě učebny virtuálních simulátorů různých typů bojové techniky,
- simulátory jsou umístěny na pohyblivých plošinách o šesti stupních volnosti
  - jedna sada simulátorů využívá servomotorové řízení pohybu plošiny,
  - druhá sada simulátorů využívá hydraulické řízení plošiny,
  - řízení obou systémů zabezpečuje samostatný počítač,
- v každé učebně jsou nainstalovány čtyři simulátory a pracoviště řídícího výcviku
  - každý simulátor se skládá ze dvou pracovišť (řidiče, velitele / střelce-operátora),
  - každé pracoviště je řízeno samostatným osobním počítačem (komerční, nezodolněný, bez úprav z hlediska vyzařování, rušení harmonickými kmitočty a z hlediska odolnosti vůči EMI),
  - každé pracoviště má osobní počítač jako prostředek vizualizace scény syntetického prostředí,
  - počítače každého pracoviště simulátoru jsou vzájemně propojeny do počítačové podsítě pomocí směrovačů (komerční, nezodolněný, bez úprav z hlediska vyzařování, rušení harmonickými kmitočty a z hlediska odolnosti vůči EMI) a datového kabelového rozvodu a také jsou připojeny na pracoviště řídícího výcviku
- všechna pracoviště simulátorů a pracoviště řídícího výcviku jsou připojeny na server umístěný v serverovně
  - místnost serverovny není stíněná vůči vnějšímu elektromagnetickému poli,
  - v místnosti serverovny nejsou provedeny žádné úpravy pro tlumení elektromagnetického vyzařování elektronických zařízení, instalovaných v serverovně,
  - místnosti (simulátory) jsou připojeny na servery kabely,

- všechny simulátory (nejen virtuální) jsou na výcvikovém pracovišti vzájemně propojeny kabelovou počítačovou sítí a také prostřednictvím WAN sítě na simulátory mimo výcvikové pracoviště.



Obr. 9. Učebny se simulátory

4.1.2 Prostorová dispozice pracoviště a jeho zranitelná místa

MVVP je dislokováno v celé stávající budově rozlehlého vojenského areálu, který se rozprostírá na kopci na periferii města. Areál je ohrazený plotem, má vlastní síť komunikací a uvnitř se nachází další samostatné subjekty.

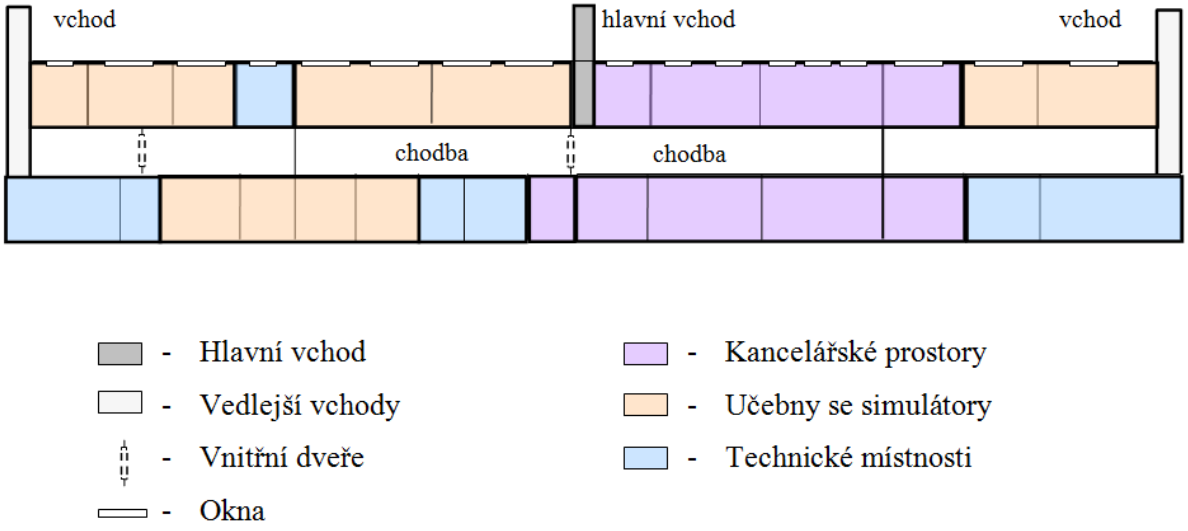
V okolí budovy se rozprostírá rozlehlé parkoviště, sklady, sportovní areál a komunikace.

Samotná budova MVVP a její střešní část jsou tvořeny panelovými díly a povrch střechy je pokrytý plechem. Střecha je pochůzná. Po celé její délce jsou zabudovány kopulové světlíky, které slouží k jejímu prosvětlení. Okna jsou umístěna po celé podélné straně objektu a jsou dřevěná, kastlová s obyčejnými skly bez mříží. Vstup do objektu je možný třemi vchody. Hlavní vstupní dveře jsou celokovové s prosklením, opatřeny běžným dveřním kováním bezpečnostním zámkem. Zbývají dva vchody se shodným typem dveří a obyčejným dveřním systémem.

Prostřední část objektu tvoří chodba, která rovnoměrně rozděluje prostory na 2 části. Chodba je ve dvou místech předělena dveřmi s bezpečnostním kováním a zámkem, čímž je

oddělena ta část MVVP, kde jsou umístěny učebny se simulátory. Do této části je umožněn vstup pouze zaměstnancům pracoviště a ostatním osobám s doprovodem.

Rozmístění výukových hal, prostorů pro administrativní a technickou činnost a učeben se simulátory je zřejmé z obrázku (Obr. 10). V budově se nenachází další subjekty.



Obr. 10. Prostorové uspořádání MVVP

Základní zranitelná místa v objektu jsou 3. Patří mezi ně dveře, okna i světlíky na střeše. Rozbitím skleněných dveřních výplní, vypáčením či odvrtáním zámku lze snadno překonat vchodové dveře. Okna a kopulové světlíky lze vysadit či vypáčit a rozbít skleněnou výplň.

Výše uvedená zranitelná místa lze překonat nejen fyzicky pomocí nástrojů, ale i nedodržením bezpečnostních opatření a následným neoprávněným vstupem do nežádoucích prostorů.

4.1.3 Opatření fyzické bezpečnosti vzhledem k pracovišti

MVVP je z hlediska fyzické ostrahy zajištěno pravidelnými obchůzkami příslušníky posádkové směny.

Režimová opatření jsou řešena ve vztahu k návštěvám. Každá osoba, vstupující do vojenského areálu a následně do modelového pracoviště, musí splňovat pravidla pro identifikaci ke vstupu. Těmi jsou pro stálé zaměstnance identifikační čipové karty, kterými lze ověřit totožnost a povolit vstup přes terminály u hlavního vchodu

do vojenského areálu, jakož i vjezd vozidel prostřednictvím další karty. Tyto identifikátory vydává správa vojenského areálu. [11]

Každý návštěvník (externí zaměstnanec, servisní pracovník, kontrola) vstupuje/vjíždí do prostorů MVVP na základě podané žádosti a povolení vedoucího pracovníka bez identifikačních médií, ale s doprovodem příslušníka pracoviště. Žádost o vstup obsahuje účel návštěvy, identifikační údaje osoby a předpokládaný čas pohybu po objektu, pro účel vjezdu vozidla jeho registrační značku a jméno řidiče. Organizace režimových opatření pro zahraniční návštěvy podléhá rozsáhlejšímu schvalovacímu procesu z bezpečnostních důvodů s konečnou podobou jako pro návštěvu místní. Ve vybraných případech je návštěva doprovázena příslušníky vojenské policie. Po objektu MVVP se lze pohybovat pouze v pracovní době, v době mimopracovní na základě oznámení vedoucímu pracoviště. [11]

Zabezpečení technickými prvky, tj. PZTS, ACCESS, CCTV atd. není na pracovišti řešeno.

Z hlediska fyzické bezpečnosti můžeme budovu označit jako rozsáhlou v komplexu ohraničeného vojenského areálu, která má určitou rozlohu a obsahuje moderní systémy, určené ke vzdělávání a výcviku vojáků. Právě z důvodu dislokace ve vojenském areálu je nutné přihlížet k lokálním provozním předpisům, které stanovují např. klíčový režim, označování budov a zabezpečení vstupů do nich, napojení PZTS na poplachové a DPPC operačního dozorčího[2], pravidla pro identifikaci ke vstupu do areálu a budovy, atd.

4.1.4 Charakter aktiv

Právě duševní vlastnictví těchto moderních systémů (softwarové databáze), které je potencionálně ohodnoceno na stovky miliónů korun a s ohledem na stupeň utajení, vede k nutnosti pečlivě zanalyzovat a navrhnout možné nejvhodnější a ekonomicky přijatelné zajištění ochrany majetku z pohledu fyzické bezpečnosti s ohledem na charakter utajení.

Neméně důležitou částí aktiv pracoviště jsou dokumenty listinného charakteru do stupně utajení Vyhrazené, které jsou plánovány ukládat v bezpečnostním trezoru a také hardwarové vybavení serverovny.

[2] Operační dozorčí – pracovník (voják z povolání) stálé operačně – dozorčí směny ve vojenském areálu.

4.1.5 Charakter možného pachatele

Významné ohrožení zde může vzhledem k charakteru aktiv představovat pachatel, jehož úmyslem bude zmocnit se softwarového vybavení simulátorů a hardwarových prostředků v serverovně. Z tohoto důvodu je třeba brát ohled na dodržování vnitřního řádu pracoviště a režimových opatření s doplněním zabezpečení technickými prostředky. Neméně důležité je zvážit možnost páchání trestné činnosti v podobě vynášení důležitých informací nebo kopií signifikantních dokumentů vlastními zaměstnanci. Řešením je použití vhodných metod personálního managementu při výběru pracovníků pro dané pracovní pozice.

4.2 Analýza a posouzení bezpečnostních rizik pracoviště

Analýzou se posuzuje efektivnost a účinnost stávající ochrany objektu a na jejím základě se vytváří podkladová dokumentace pro projekt fyzické bezpečnosti s návrhem na jeho ochranu.

Pro účel této práce jsem aplikovala bezpečnostní analýzu k identifikaci aktiv, vyhledání a ohodnocení rizik a zranitelnosti objektu a k návrhu opatření fyzické bezpečnosti s ohledem k ochraně utajovaných informací modelového výcvikového pracoviště. Každá z existujících metod analýzy rizik dle normy ČSN EN 31010 byla vytvořena pro specifický problém, proto je zapotřebí patřičný výběr univerzálních metod, které jsou vhodné také z pohledu souvztažnosti rizik.

Po výběru nejzávažnějších rizik, která ohrožují aktiva posuzovaného pracoviště, je na řadě jejich minimalizace na požadovanou úroveň vhodným způsobem zabezpečení, kdy by vynaložené náklady neměly přesáhnout 10%, výjimečně až 15% hodnoty aktiv (princip ALARP). [9]

Při stanovení celkové míry rizika ohrožení utajovaných informací u modelového výcvikového pracoviště je nezbytné vycházet z několika předpokladů, které po vzájemném průniku určí patřičnou míru rizika:

- vzájemné závislosti velikosti újmy způsobené jako důsledek neoprávněné manipulace s utajovanou informací,
- z pravděpodobnosti neoprávněné manipulace s utajovanou informací představující výběr identifikovaných a ohodnocených hrozeb,
- ze zranitelnosti chráněného prostoru.

4.2.1 Aktiva - identifikace, stupeň utajení a velikosti újmy

Na začátku postupu analýzy rizik je směrodatné stanovit její hranici, tzn. oddělit aktiva, která budou zahrnuta do analýzy, od ostatních. Vybraná aktiva MVVP (Tab. 8) budou ohodnocena stupněm utajení a v návaznosti na to stanovena velikost újmy zájmu ČR.

Tab. 8. Aktiva – identifikace, stupeň utajení a velikost újmy

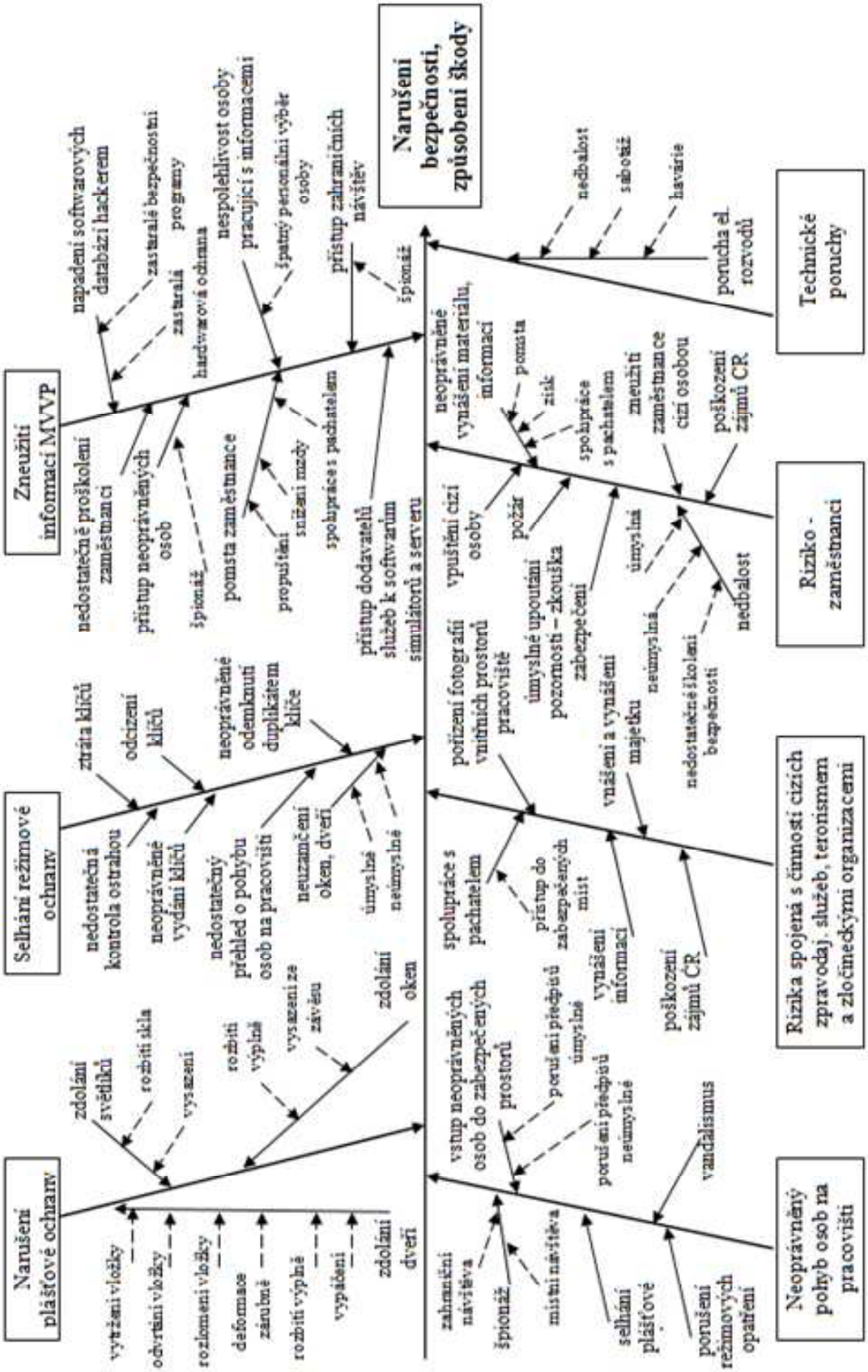
	Aktiva	Stupeň utajení	Velikost újmy
1.	Software	Důvěrné	Prostá
2.	Server	Důvěrné	Prostá
3.	Kryptografické zařízení	Důvěrné	Prostá
4.	Dokumentace	Vyhrazené	Nevhodné pro zájmy ČR

4.2.2 Identifikace rizik

Pro uvědomění si a identifikaci příčin rizik bezpečnostního prostředí MVVP vedoucích k následkům je nejprve zvolena grafická metoda Ishikawa[3] diagramu. Princip vychází ze základního pravidla, že každý následek má svou příčinu nebo kombinaci příčin, jak znázorňuje Obr. 10.

V kapitole 3.4 této práce jsem uvedla možný postup pro stanovení celkové míry ohrožení objektu a aktiv v něm. Při pokusu o praktickou aplikaci původně navrhovaného postupu pro výběr a hodnocení rizik jsem zjistila, že bude vhodné tento proces doplnit z pohledu souvztažnosti metodou rizik KARS.

[3] Ishikawa diagram je diagram příčin a následků, jehož cílem je nalezení pravděpodobnosti příčiny řešeného problému. Schéma popsal a zavedl Kaoru Ishikawa.



Obr. 11. Identifikace hrozeb - Ishikawa diagram příčin a následků

4.2.3 Analýza rizik

Po uzavření podrobné analýzy příčin a následků hrozeb bezpečnostního prostředí se vytvoření seznam možných rizik (Tab. 9), které se mohou vztahovat k chráněnému prostoru. Jednotlivá rizika jsou následně slovně ohodnocena. Toho lze dosáhnout stanovením velikosti ohrožení, které může vzniknout na základě vzájemných vztahů různých faktorů. Rizika jsou posuzována ze dvou hledisek, a to procesního, tedy způsobená lidským faktorem a strukturálního, která jsou způsobena technickými příčinami, kdy rizika z hlediska procesního jsou mnohem závažnější než ze strukturálního.

Tab. 9. Seznam možných komplexních ohrožení objektu

Ohrožení (H_1-H_{11})		**Zdroj ohrožení (ano-existuje, ne-neexistuje)**	**Příčina, motivace, záměr**	**Výskyt již dříve**	**Hodnocení (H;,M;S;V)**
Poloha a umístění objektu	H_1	Ne	Ne	Ne	0
Zabezpečení ochrany objektu a chráněného prostoru	H_2	Ano - pracovníci fyzické ostrahy	Ne - zisk, nedbalost, vydírání, neoprávněný přístup	Ne	Malé
	H_3	Lupič po přípravě	Ano - zisk, pomsta	Ne	Velké
	H_4	Ano - vandalismus	Ne - vyjádření odporu, poškození majetku	Ne	Malé
	H_5	Ano – dodavatelé služeb	Nelze stanovit s určitostí	Ne	Střední
Činnost cizích zpravodajských služeb, záškodníků, teroristických a zločineckých skupin	H_6	Ano - cizí zpravodajské služby	Nelze stanovit s určitostí	Ne	Střední
	H_7	Ano - teroristé	Ano – vydírání, vyvolání strachu	Ne	Velké
	H_8	Ano - skupina organizovaného zločinu	Nelze stanovit s určitostí	Ne	Střední
Technické poruchy	H_9	Ano - rozvod el. energie	Ne - havárie, požár	Ne	Malé
Zaměstnanci	H_{10}	Ano - vlastní zaměstnanci-oprávněné osoby	Ne - zisk, nedbalost, neznalost, vydírání	Ne	Malé
	H_{11}	Ano - vlastní zaměstnanci-neoprávněné osoby	Ano - pomsta, zisk, vydírání, nedostatečná ochrana	Ne	Střední

Výsledkem je celkové hodnocení ohrožení podle nejvyššího identifikovaného, v tomto případě ***VELKÉ***. Jednotlivá hodnocení ve slovní formě vychází z následujícího:

- **ohrožení neexistuje (0)**, když neexistuje (nebyl identifikovaný) zdroj ohrožení,
- **malé ohrožení (M)**, když existuje zdroj ohrožení, ale neexistuje motivace nebo záměr útočníka, a z minulosti nejsou známe případy výskytu ohrožení,

- **střední ohrožení (S)**, jakmile je identifikovaný zdroj ohrožení, ale nedá se s určitostí stanovit motivace nebo záměr útočníka, anebo možné příčiny ohrožení,
- **velké ohrožení (V)**, jakmile je zdroj ohrožení identifikovaný, je jednoznačně identifikovaný motiv nebo záměr útočníka anebo příčina ohrožení, v minulosti se už vyskytly (anebo doposud ještě nevyskytly) případy ohrožení v prostředí objektu (chráněného prostoru). [10]

4.2.4 Analýza souvztažnosti

Autorem této metody je vedoucí pracoviště studia a jazykové přípravy IOOLB (Institut ochrany obyvatelstva Lázně Bohdaneč), pan Ing. Štefan Pacinda, Ph.D. Podle Jakuba Nebelskeho[4] metoda KARS byla vyvinuta proto, aby podala zpracovatelům analýzy rizik odpověď na otázku, kterým rizikům se musíme věnovat primárně a která můžeme řešit s časovým odkladem. [15]

Vypracování analýzy souvztažnosti a hodnocení hrozeb

Pro ověření výsledků, získaných v předchozí analýze, jsem použila metodu souvztažnosti rizik, která řeší možnost vzájemného ovlivnění zvolených hrozeb z hlediska procesního (Tab. 10: hrozba 1-6) a strukturálního (Tab. 10: hrozba 7-14), vybraných dle Ishikawa diagramu. Při této metodě se postupuje tak, že jsou vyhledány hrozby, následuje jejich ohodnocení vyhledáním vzájemných vazeb vytvořením matice, jak ukazuje tabulka (Tab. 10). Jednotlivá ohrožení H_i/H_j jsou vynesena na osách X/Y a při vzájemném ovlivnění jim je přiřazena hodnota 1 a v opačném případě hodnota 0.

[4] NEBELSKY, Jakub. *Metody identifikace rizika území regionu Mladoboleslavsko*. Pardubice, 2009. Diplomova prace. Univerzita Pardubice. Vedouci prace doc. RNDr. Petr Linhart, CSc.

Tab. 10. Sestavení matice souvztažnosti

H_i		H_j														
Konkrétní identifikované hrozby		1	2	3	4	5	6	7	8	9	10	11	12	13	14	ΣK_j
1	Selhání práce ostrahy		0	1	0	0	0	1	1	1	1	1	1	0	0	***7***
2	Vytvoření duplikátu klíče	0		1	0	0	0	0	1	0	1	1	1	0	0	***5***
3	Spolupráce s pachatelem	0	1		1	1	1	0	1	0	1	1	0	1	1	***9***
4	Zneužití informací	0	0	0		0	0	1	0	1	1	1	1	1	0	***6***
5	Neuzamčení dveří	0	0	1	0		0	0	1	1	1	1	1	0	0	***6***
6	Neuzavření oken	0	0	0	0	0		1	1	0	1	1	1	0	0	***5***
7	Vloupání oknem	0	0	0	1	0	0		1	0	1	1	1	0	0	***5***
8	Neoprávněný vstup osob	0	1	1	1	1	1	1		1	0	1	1	0	0	***9***
9	Vloupání dveřmi	0	1	0	1	1	0	0	1		1	1	1	0	0	***7***
10	Poškození majetku	1	1	1	1	0	0	1	1	1		1	0	1	1	***9***
11	Krádež majetku	1	0	0	1	0	0	0	1	0	1		0	1	0	***12***
12	Vnášení nebezp. předmětů	0	0	1	1	1	1	0	1	0	1	0		1	0	***7***
13	Výpadek el. proudu	1	0	0	0	0	0	0	1	0	1	1	1		0	***5***
14	Přelezení plotu	0	0	0	0	0	0	1	1	1	1	1	0	0		***5***
ΣK_{ih}		***3***	***4***	***6***	***7***	***4***	***3***	***6***	***12***	***6***	***12***	***12***	***9***	***5***	2	

Výsledné hodnoty se ve sloupcích a řádcích sečtou a podle vzorců (1) a (2) se vypočítají hodnoty K_{ih} a $K_{jh,}$ procentuálně vyjadřující počet návazných hrozeb H_j, jejichž vyvolání může být způsobeno hrozbou H_i.

$$K_{ir} = \left[\sum K_{ih} \div (x - 1)\right] * 100 \quad (1)$$

$$K_{jr} = \left[\sum K_{jh} \div (x - 1)\right] * 100 \quad (2)$$

Dle výše uvedených vzorců jsou následně vypočítány hodnoty koeficientů jednotlivých hrozeb (Tab. 11) a odtud se určí minimální a maximální hodnoty koeficientů K_{ih} a $K_{jh.}$ Ty jsou výchozími hodnotami pro výpočet os grafu.

Tab. 11. Hodnoty koeficientů K_{ih} a K_{jh}

Hrozba	1	2	3	4	5	6	7	8	9	10	11	12	13	14
K_{ih}	23,1	30,8	46,2	53,8	30,8	23,1	46,2	92,3	46,2	92,3	92,3	69,2	38,5	15,4
K_{jh}	53,8	38,5	69,2	46,2	46,2	38,5	38,5	69,2	53,8	69,2	92,3	53,8	38,5	38,5

Výpočet os grafu

Minimální a maximální hodnoty koeficientů K_{ih} a K_{jh} jsou následující:

K_{ih} min = 15,4 K_{ih} max = 92,3

K_{jh} min = 38,5 K_{jh} max = 92,3

Osy grafu souvztažnosti jsou vypočítány podle vzorců (3) a (4):

$$O_1 = \left[\left(K_{ih}\ \max - K_{ih}\ \min\right) \div 100\right] * s[\%] \quad (3)$$

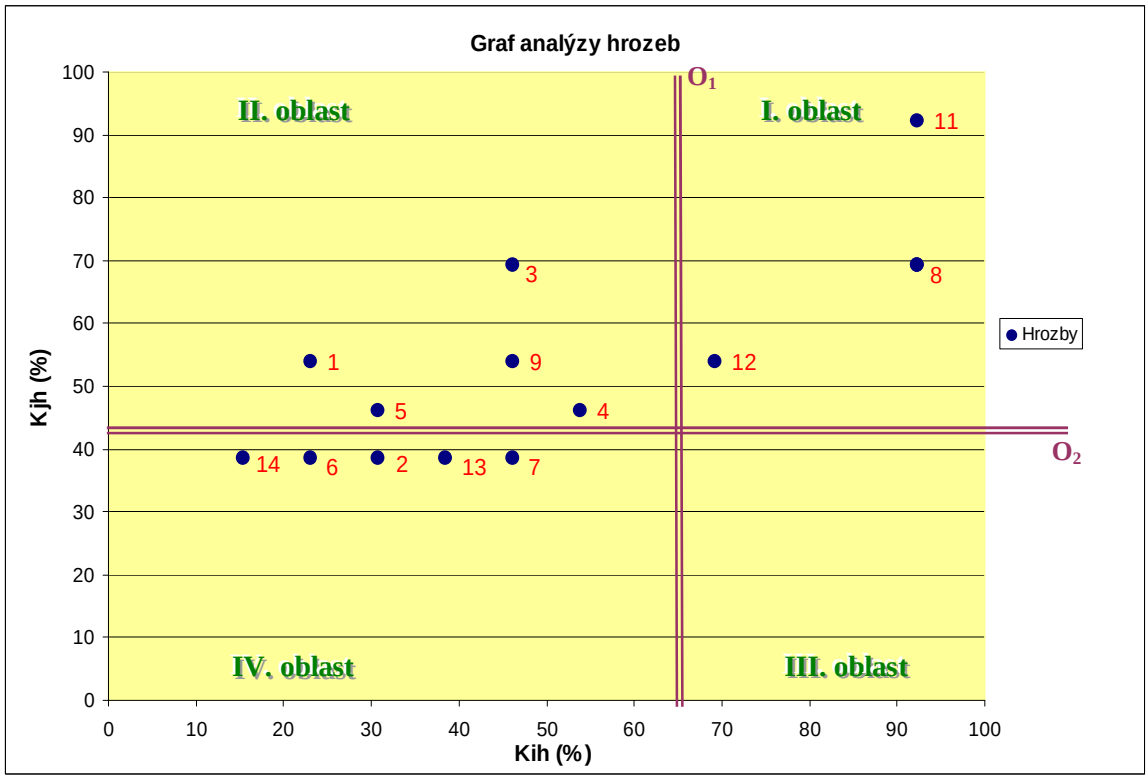
$$O_2 = \left[\left(K_{jh}\ \max - K_{jh}\ \min\right) \div 100\right] * s[\%] \quad (4)$$

kde s = spolehlivost (0-100) – v tomto případě 80. Z uvedeného tedy vyplývá, že:

O_1 = 61,52 O_2 = 43,04

Graf souvztažnosti

Výsledná závažnost analýzy provázanosti jednotlivých hrozeb je přehledně znázorněna na obrázku (Obr. 11), kde jsou tyto hrozby rozděleny podle závažnosti (Tab. 12) do kvadrantů.



Obr. 12. Graf analýzy souvztažnosti hrozeb

Tab. 12. Závažnost provázanosti hrozeb z hlediska procesního a strukturálního

Závažnost provázanosti hrozeb z hlediska procesního a strukturálního	
I. oblast	Primárně a sekundárně nebezpečné hrozby
II. oblast	Sekundárně nebezpečné hrozby
III. oblast	Žádná primárně nebezpečná oblast hrozeb
IV. oblast	Relativní bezpečnost

Výše provedenou analýzou souvztažnosti hrozeb jsem došla k závěru, že nejčastější vybrané hrozby z Ishikawa diagramu, která mohou následně přerůst v rizika v Tab. 9, patří do oblasti primárně a sekundárně nebezpečných hrozeb a shodují se tedy s celkovým hodnocením rizik – VELKÉ.

4.2.5 Vyhodnocení zranitelnosti objektu

Zranitelná místa v objektu a chráněném prostoru, zvolená v kapitole 3.4.3 a seznam ohrožení dle Tab. 9, použiji pro sestavení matice zranitelnosti modelového pracoviště (Tab. 13).

Tab. 13. Matice zranitelnosti MVVP

Ohrožení H_j	**Zranitelná místa B_m**						
	B_1	**B_2**	**B_3**	**B_4**	**B_5**	**B_6**	**B_7**
H_2	M	M	S	M	M	M	S
H_3	S	S	S	S	S	S	S
H_4	M	M	M	M	M	M	M
H_5	M	M	S	S	M	S	M
H_6	M	S	S	S	M	M	M
H_7	M	M	S	S	M	S	S
H_8	M	M	S	S	S	S	S
H_9	M	M	M	M	S	M	S
H_{10}	M	M	M	M	S	M	S
H_{11}	M	M	M	S	S	M	S

Matice zranitelnosti nám má říci, jak mohou jednotlivé typy ohrožení využít zranitelné místo objektu na ohrožení bezpečnosti pracoviště a utajovaných informací. Z výše uvedené tabulky tedy vyplývá celková zranitelnost, což je hodnocení ***STŘEDNÍ***, jelikož hodnocení zranitelnosti VELKÁ se v matici nevyskytuje.

Nyní mohu ze zjištěných závěrů velikosti ohrožení (kapitola 4.2.3), výsledné velikosti zranitelnosti (kapitola 4.2.5) a stanovené míry újmy (Tab. 8) stanovit výslednou pravděpodobnou míru rizika v objektu (Tab. 14).

Tab. 14. Celková míra rizika modelového pracoviště

Velikost újmy U	**Velikost ohrožení H**								
	MALÁ			STŘEDNÍ			VELKÁ		
	Zranitelnost Z								
	Malá	Střední	Velká	Malá	Střední	Velká	Malá	Střední	Velká
Nevýhodné pro zájmy ČR	M	M	M	M	S	S	S	**S**	V
Prostá újma	M	M	M	S	S	S	S	**V**	V
Vážná újma	M	S	S	S	S	V	V	V	V
Mimořádně vážná újma	S	S	S	S	V	V	V	V	V

Pravděpodobná výsledná míra ohrožení (vychází se z největšího možného ohrožení)**:**

- stupeň utajení aktiva „V“ – nevýhodné pro zájmy ČR – míra ohrožení ***STŘEDNÍ,***
- stupeň utajení aktiva „D“ – prostá újma – míra ohrožení ***VELKÁ.***

Výsledná míra rizika je dle výše uvedených výsledků stanovena jako **VELKÁ** a nyní bude tato hodnota použita k určení bodové hodnoty zabezpečených oblastí.

4.2.6 Vyhodnocení analýzy rizik

Pro analýzu rizik bylo použito několik metod, jejichž cílem bylo zhodnocení rizik v oblasti fyzické bezpečnosti z několika pohledů.

Pomocí Ishikawa diagramu byly zvoleny hrozby, které mohou vést k různým následkům v mnoha oblastech, páchané různými druhy pachatelů. Z nich nejzávažnější byly vyhodnoceny neoprávněný přístup osob, krádež majetku, spolupráce s pachatelem a poškození majetku (Obr. 12). Zde lze vycházet z Paretova pravidla 80/20, kdy 20 % možných rizik způsobí 80 % škod. Tyto hrozby se prolínají s vyhodnocením ohrožení objektu dle Tab. 9, odkud největší možné ohrožení a způsobení škod vyplývá od lupiče s přípravou a teroristy.

4.3 Bodové ohodnocení bezpečnosti

V závislosti na vyhodnocení rizik a stupni utajovaných informací se stanovuje minimální bodové ohodnocení zabezpečených a jednacích oblastí, a to na základě tabulek bodových hodnot nejnižší míry zabezpečení dle příloha č. 1 vyhlášky č. 528/2005 Sb.

U modelového výcvikového pracoviště jsou uložena aktiva, jejichž stupeň utajení je kategorie **Důvěrné** a **Vyhrazené**. Míra rizika ohrožení utajovaných informací byla vyhodnocena jako **VELKÁ**. Z uvedeného vyplývá, že bodová hodnota zabezpečení zabezpečené oblasti „D“ by měla činit minimálně 16 bodů (Tab. 15) a bodová hodnota zabezpečení zabezpečené oblasti „V“ minimálně 3 body (Tab. 16).

Tab. 15. Bodové hodnoty zabezpečené oblasti kategorie Důvěrné [8]

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**

Tab. 16. Bodové hodnoty zabezpečené oblasti kategorie Vyhrazené [8]

ZABEZPEČENÁ OBLAST KATEGORIE Vyhrazené sloužící k ukládání utajované informace v komponentách informačního systému nebo kryptografickém prostředku nebo která vyžaduje zvláštní režim nakládání	
Povinné : (S1) + (S2) + (S3)	2
Nepovinné : (S4) + (S5) + (S6)	1
Celkový výsledek	**3**

4.4 Určení objektu a zabezpečených oblastí

Určení objektu a jeho hranice

Budova, ve které se bude nacházet modelové výcvikové pracoviště s utajovanými informacemi, je jednopodlažní. Objektem je určena levá část budovy, která je ohraničena ze dvou vnějších stran pláštěm budovy, tj. betonovými prefabrikáty s kastlovými okny s běžným sklem a ta je také hranicí zvoleného objektu s utajovanými informacemi.

Zbývající dvě strany tvoří betonové stěny s dveřmi. Objekt jsem určila typu 1 podle přílohy č. 1 k vyhlášce č. 528/2005 Sb., kdy podlahy, strop a stěny budovy jsou sice z pevného materiálu, ale okna se nenachází ve výšce alespoň 5,5 m nad terénem, což neumožňuje vyšší bodové ohodnocení. Bodové hodnocení objektu S3 = 1.

Vymezení zabezpečených oblastí

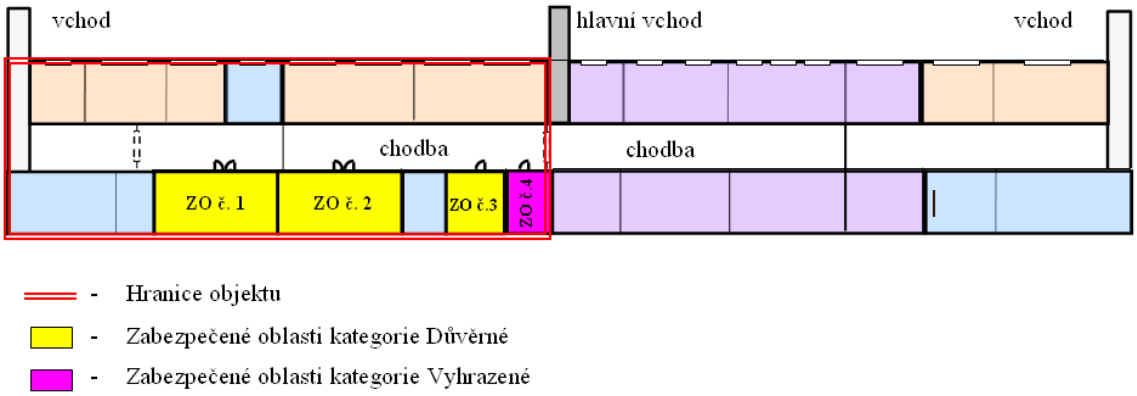
Ve zvoleném objektu jsou stanoveny následující zabezpečené oblasti:

a) **ZO č. 1, ZO č. 2: Učebny se simulátory**
   - *Typ*: 2, SS3 = 2 body. Zabezpečené oblasti mají stěny, stropy a podlahy z betonu do tloušťky 100 mm.
   - *Kategorie*: Zabezpečenými oblastmi jsou učebny se simulátory, ve kterých se nachází softwarové databáze stupně utajení Důvěrné. Samostatné řídící počítače simulátorů budou zabezpečeny jako úschovné objekty. V místnostech nejsou stálí pracovníci.
   - *Třída:* II - Při vstupu do této oblasti nedochází ke styku s utajovanou informací.

b) **ZO č. 3**: **Serverovna**
   - *Typ*: 2, SS3 = 2 body. Zabezpečená oblast má stěny, strop a podlahu z betonu do tloušťky 100 mm.
   - *Kategorie*: Zabezpečenou oblastí je místnost se serverem a kryptografickým zařízením stupně utajení Důvěrné. V místnosti nejsou stálí pracovníci.
   - *Třída:* II - Při vstupu do této oblasti nedochází ke styku s utajovanou informací.

c) **ZO č. 4**: **Kancelář**
   - *Typ*: 2, SS3 = 2 body. Zabezpečená oblast má stěny, strop a podlahu z betonu do tloušťky 100 mm.
   - *Kategorie*: Zabezpečenou oblastí je kancelářský prostor, ve kterém budou ukládány informace stupně utajení Vyhrazené a stále pracující osoba.
   - *Třída:* II - Při vstupu do této oblasti nedochází ke styku s utajovanou informací.

Určení objektu, jeho hranice a vymezení zabezpečených oblastí je znázorněno na obrázku (Obr. 13).



Obr. 13. Zobrazení hranice objektu a zabezpečených oblastí

4.5 Dílčí závěr

Cílem této kapitoly bylo stanovení výchozích podmínek pro návrh zabezpečení a celkové míry rizika modelového pracoviště.

Klasifikací pracoviště byl otevřen náhled do skladby systému moderních výcvikových prostředků, a to virtuálních simulátorů. V několika odstavcích jsem popsala dispozici pracoviště ve vojenském areálu, stavební objekt, do jehož je navrhováno jeho umístění, stávající opatření fyzické bezpečnosti, charakter aktiv pracoviště a charakter možného pachatele.

Stěžejní částí této kapitoly byla analýza a posouzení bezpečnostních rizik pracoviště, ke které bylo použito několik metod.

Nejprve bylo nezbytné identifikovat aktiva, určit jejich stupeň utajení a velikost újmy. Identifikované příčiny pomocí Ishikawa diagramu, vedoucí k následku narušení bezpečnosti, se prolínaly do všech vážných hrozeb, jež byly sestaveny na základě procesního a strukturálního hlediska. Pro ověření výsledků jsem zvolila metodu souvztažnosti, při které byla ověřována vzájemná ovlivnitelnost jednotlivých hrozeb. Na jejím konci vznikl graf, kde se jednotlivé hrozby rozdělily podle závažnosti do čtyř kvadrantů a výsledná závažnost stanovena jako velká. Následným krokem jsem vytvořila matici zranitelnosti objektu a vyhodnotila zranitelnost jako střední. Celková míra rizika byla zpracována z velikosti ohrožení, zranitelnosti a velikosti újmy a určena jako VELKÁ.

Závěr této kapitoly tvoří bodové ohodnocení pracoviště na základě vyhodnocení rizik a určení objektu, jeho hranic a vymezení zabezpečených oblastí.

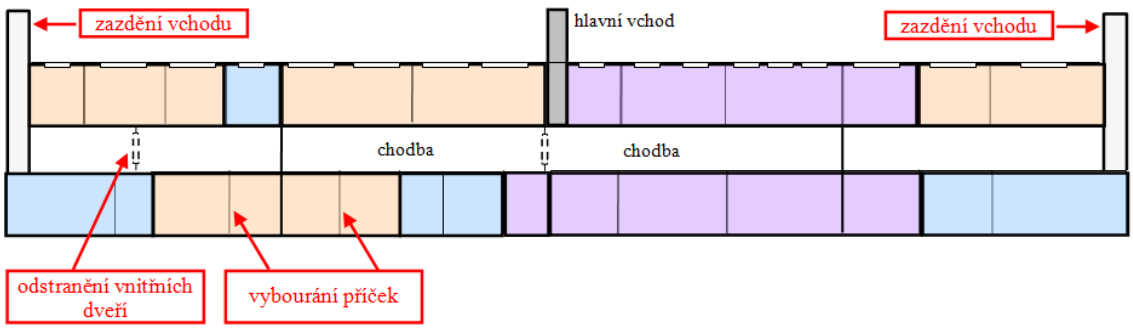
5 KONCEPTUÁLNÍ NÁVRH SYSTÉMU FYZICKÉ BEZPEČNOSTI VÝCVIKOVÉHO PRACOVIŠTĚ

Zajištění systému fyzické bezpečnosti spočívá v kombinaci opatření fyzické ostrahy, režimových opatření a technických prostředků v návaznosti na stanovení objektu, jeho hranice a zabezpečených oblastí.

Při návrhu zabezpečení budu vycházet z určených kategorií „D“ a „V“ pro jednotlivé zabezpečené oblasti a jejich minimálního bodového hodnocení, abych naplnila celkový počet bodů míry rizika. U zabezpečené oblasti kategorie Vyhrazené jsou to 3 body a kategorie Důvěrné 16 bodů. Pro přehlednost budou bodová ohodnocení všech oblastí zobrazena v tabulkách v příloze práce.

Dle zákona č. 412/2005 Sb. je rozsah technických prostředků pro zabezpečení nejvyšší kategorie zabezpečené oblasti, tedy Důvěrné, stanoven na mechanické zábranné systémy a poplachové a zabezpečovací tísňové systémy. Na základě stanovení míry rizika jako „velké“, kdy se do rizik zahrnují hrozby i v návaznosti na ochranu majetku a tím se konečná míra rizika zvyšuje, bych volila jako doplnění použití integrovaného přístupového systému.

Před zahájením bezpečnostních opatření bych navrhla stavební úpravy v podobě zazdění stávajících dvou bočních vchodů do budovy a odstranění vnitřních dveří na chodbě. Zůstaly by pouze jedny vnitřní dveře pro vstup do zabezpečeného objektu. Dále bych vybourala příčky ve stávajících místnostech tak, že by ze čtyř místností vznikly místnosti dvě, kde budou následně umístěny simulátory kategorie Důvěrné (Obr. 14).



Obr. 14. Provedení stavebních úprav

5.1 Určení režimových opatření

Režimová opatření jsou souborem organizačně administrativních opatření a postupů směřujících k zajištění požadovaných podmínek pro smysluplnou funkci zabezpečovacího systému a jeho sladění s provozem chráněného objektu.

Hlavní vchod do budovy bude zajištěn bezpečnostními dveřmi včetně zámkového systému a jeho prvku, jímž je bezpečnostní cylindrická vložka. Náhradní klíče budou uschovány v tubě, která je označená a uložená u operačního dozorčího. Doplňkovým opatřením ve prospěch režimových opatření a fyzické ochrany by nadále zůstalo k zabezpečení dveří použití pečetě, kterou má každý zaměstnanec k dispozici.

V rámci vnějších režimových opatření k zajištění zabezpečeného objektu kategorie „V“ je ochrana pracoviště zajišťována opatřeními, které stanoví velitel vojenského areálu a to v podobě podmínek vnášení a vynášení materiálu při vstupu a vjezdu do areálu.

Vnitřní režimová opatření se týkají především omezení podmínek při vstupu a pohybu osob na pracovišti. Každá osoba (cvičící osoba, externí zaměstnanec, servisní pracovník, kontrola, návštěva i zahraniční), vstupující do MVVP, musí splňovat pravidla pro identifikaci ke vstupu do zabezpečeného objektu. Pro tuto potřebu bude do další části práce zakomponován integrovaný systém kontroly vstupů (ACCESS). Kromě detekce pohybu osob po pracovišti je jeho výhodou především omezení pohybu osob jen do vybraných oblastí.

Návštěvy, vstupující do objektu, musí být po celou dobu pobytu v něm doprovázeny. Jejich evidenci zaznamená systém kontroly vstupů na základě přiděleného identifikátoru.

Režimová opatření dle výše uvedeného stanoví vedoucí organizačního celku v provozním řádu objektu.

5.2 Zajištění fyzické ostrahy

Dle NVMO č. 42/2006, o fyzické bezpečnosti v rezortu MO, musí být ostraha pro kategorii utajovaných informací Důvěrné zajištěna nejméně jednou osobou, které poplachové hlášení technických prostředků umožní rychlý zásah, je-li provádění ochrany utajovaných informací narušeno.

Ostraha je v areálu zabezpečována příslušníky ozbrojených sil a je vykonávána způsobem pravidelných obchůzek. V průběhu výkonu ostrahy, včetně doby obchůzky, je na stanovišti stálé ostrahy soustavně přítomna nejméně jedna osoba pro tento výkon.

Budova MVVP je kontrolována ostrahou a zabezpečené oblasti budou napojeny na dohledové a poplachové přijímací centrum, umístěné u ostrahy (operačního dozorčího). Pokud shledá příslušník ostrahy při obchůzce narušení objektu, uvědomí telefonicky určené pracovníky MVVP o vzniklé události a ti pak dále řeší situaci prostřednictvím vojenské, popřípadě státní policie.

5.3 Mechanické zábranné prostředky

5.3.1 Zabezpečená oblast kategorie Vyhrazené

MZS budou použity pro ZO č. 4, což je kancelářská místnost. Oblast byla stanovena typu 2, proto pro zabezpečení dveří a uzávěrů budou aplikovány mechanické zábranné prostředky bezpečnostní třídy RC 2 podle ČSN EN 1627, aby byla dodržena minimální bodová hodnota zabezpečené oblasti.

Pro ukládání utajovaných informací v tištěné listinné podobě použiji skříňový trezor, který odpovídá certifikačním požadavkům NBÚ a splňuje bezpečnostní třídu pro danou zabezpečenou oblast.

Všechny vyspecifikované prvky MZS jsou uvedeny v tabulkách (Tab. 17, Tab. 18).

Tab. 17. Zabezpečení vstupu do ZO č. 4

Technický prostředek	Typ	Výrobce	Bezpečnostní třída	NBÚ
Bezpečnostní dveře vchodové	BEDEX STANDARD 2	MRB	2	SS3=2 SS4=1
Bezpečnostní kování	802	Rostex	3	SS4=2
Cylindrická vložka	ABLOY CY 300N	Abloy Oy	3	SS4=2

Tab. 18. Úschovný objekt pro ZO č. 4

Technický prostředek	Typ	Výrobce	Bezpečnostní třída	NBÚ
Nábytkový trezor	NTR/11-61 M	Safetronics	0	SS1=2 SS2=2

5.3.2 Zabezpečená oblast kategorie Důvěrné

Tři zabezpečené oblasti kategorie Důvěrné budou na vstupu zabezpečeny systémem kontroly vstupů. Oblast byla stanovena typu 2, proto pro zabezpečení dveří a uzávěrů budou aplikovány mechanické zábranné prostředky bezpečnostní třídy RC 2 podle ČSN EN 1627, aby byla dodržena minimální bodová hodnota zabezpečené oblasti. V místnostech se simulátory budou dveře dvoukřídlé, v serverovně jednokřídlé.

Z toho důvodu musí být vybrány vhodné a certifikované bezpečnostní dveře, elektromechanický zámek, bezpečnostní kování a cylindrická vložka. Vybrané prostředky jsou uvedeny v tabulce (Tab. 19).

Tab. 19. Zabezpečení vstupu do ZO č. 3

Technický prostředek	Typ	Výrobce	Bezpečnostní třída	NBÚ
Bezpečnostní dveře pro kontrolu vstupu	F6/2 Abloy	SHERLOCK	2	SS3=2 SS4=1
Zárubeň	CG6	SHERLOCK	-	-
Elektromechanický zámek	Abloy EL 460	ASSA ABLOY	3	SS4=2
Bezpečnostní kování	R1/Cr	ROSTEX	3	SS4=2
Cylindrická vložka	Guard 550	GUARD-MUDROCH	3	SS4=2

Tab. 20. Zabezpečení vstupu do ZO č. 1 a ZO č. 2

Technický prostředek	Typ	Výrobce	Bezpečnostní třída	NBÚ
Bezpečnostní dveře pro kontrolu vstupu	DN3	NAPAKO	3	SS3=2 SS4=1
Elektromechanický zámek	Abloy EL 460	ASSA ABLOY	3	SS4=2
Bezpečnostní kování	RX1-50 Solid	ROSTEX	3	SS4=2
Cylindrická vložka	Guard 550	GUARD-MUDROCH	3	SS4=2

5.4 Poplachový zabezpečovací a tísňový systém

PZTS bude tvořit hlavní systém prostředků zabezpečení zabezpečených oblastí. V rámci zabezpečeného objektu se bude PZTS vztahovat k plášťové a prostorové ochraně.

Podle normy ČSN CLC/TS 50 131-7 je nutné nejprve zvolit stupeň zabezpečení, což pro oblasti kategorie Důvěrné bude odpovídat stupni 2 – nízké až střední riziko, kdy se předpokládá, že narušitelé mají určité znalosti o PZTS a že použijí základní sortiment nástrojů a přenosných přístrojů.

Dále norma určí pro stupeň zabezpečení minimální úroveň střežení, kdy pro stupeň 2 je třeba vzít v úvahu obvodové dveře, okna a ostatní otvory, vyhodnocení rizik pracoviště a stavební konstrukci.

Třída prostředí jednotlivých komponentů systému by měla odpovídat podmínkám prostředí, v němž budou používány, v tomto případě se jedná o třídu 1 – prostředí vnitřní. Funkčnost komponentů nesmí být ovlivněna běžným provozem ve vytápěných místnostech. Předpokládá se rozsah změn teplot v intervalu +5 °C až +40 °C a střední relativní vlhkost přibližně 75 % bez kondenzace [14].

Při návrhu systému a volbě komponentů poplachového zabezpečovacího systému (dále jen PZS) mají být použity dle přílohy č.1 k vyhlášce č. 528/2005 Sb. prvky, odpovídající stupni zabezpečení 2, tedy bodová hodnota PZS odpovídat SS91=2 a bodová hodnota instalace zařízení PZS SS92=2.

Jelikož NBÚ pro fyzickou bezpečnost zabezpečené oblasti kategorie Důvěrné nepožaduje poplachový tísňový systém a jeho opodstatnění by se nenašlo ani vzhledem k charakteru pracoviště, nebude v této práci realizován.

5.4.1 Ústředna PZTS

Pro systém PZTS by se jevila jako vhodná zabezpečovací ústředna DIGIPLEX EVO 192 (Obr. 15) od firmy Paradox, schválená také NBÚ pro stupeň 3.

Ústřednu lze rozdělit na 8 podsystémů, maximální počet zón v systému je 192 a počet uživatelských kódů je 999. Přímo na ústředně je napojeno 5 programovatelných výstupů, a to 4 optické relé 50 mA a 1 relé 5A. Ústředna podporuje až 254 rozšiřujících sběrnicových modulů, na něž mohou být napojena externí zařízení (klávesnice, detektory, expandéry), která mohou být volně naprogramována např. na poplach, samoochranu, tíseň,

požár, vstupní/výstupní smyčka, technickou smyčku a další. Klávesnice má programovatelný výstup, který může být naprogramován např. vnitřní sirénu, spínač vnějšího osvětlení, spouštění telefonního komunikátoru, řízení paměti detektorů, apod..

Další vlastnosti ústředny DIGIPLEX EVO 192:

- integrované vlastnosti přístupového systému,
- automatická úspora, podsvícení klávesnic dle času,
- PGM1 může být využito jako vstup pro 2-drátový kouřový detektor,
- paměť na 2048 událostí,
- zabudovaná baterie reálného času,
- napájecí zdroj 1,7 A,
- 1 sledovaný okruh sirény, výstupu a telefonní linky,
- tlačítko systémového nastavení do továrních hodnot. [16]

Obr. 15. Ústředna PTZS [16]

Ústředna bude v objektu MVVP nainstalována v místnosti serverovny v horní polovině stěny. Do tohoto místa bude přivedeno samostatně jištěné a přepěťově chráněné napájecí vedení z hlavního rozvaděče NN, datová linka a napájecí vedení od koncentrátorů a klávesnic. Dále bude do ústředny přivedeno vedení od detektorů, zapojených přímo na smyčkách ústředny.

Vstupní klávesnice, která bude umístěna u vstupních dveří z vnějšího prostoru, slouží ke komunikaci ústředny s uživatelem. Jsou na ní zobrazovány stavové informace o průběhu ochrany, např. zapnutí, vypnutí nebo pozastavení zabezpečení nebo nízký stav baterie. Informace o stavu objektu je předávána uživateli formou textu na displeji klávesnice a akustickým signálem.

5.4.2 Detektory PZTS

PLÁŠŤOVÁ OCHRANA

Prvky plášťové ochrany slouží, jak už sám jejich název napovídá, k hlídání otevření, popř. destrukce prostupů pláště budovy (oken, dveří, vrat). [17]

Zabezpečený objekt MVVP byl stanoven kategorie Vyhrazené, kdy dle požadavků NBÚ stačí zabezpečení pouze prostředky MZS. Jelikož se v objektu nachází zabezpečené oblasti kategorie Důvěrné, bude na jejich ochranu na celý zabezpečený objekt nainstalován poplachový zabezpečovací a tísňový systém, jehož prvky plášťové ochrany zajistí zároveň bezpečnost pro okna budovy.

Okna objektu MVVP jsou kastlová s běžným sklem bez přídavných mříží. Vnitřní dveře pro vstup do zabezpečeného objektu jsou plné bez mříží.

Na vstupech do všech místností se vstupem z nechráněných prostor a na otevíratelných křídlech dřevěných oken budou umístěny magnetické kontakty QST-GN. Skla budou chráněna duálními detektory tříštění skla FG1625TAS.

Magnetické kontakty

Magnetický kontakt je tvořený dvojicí dílů, a to permanentním magnetem, připevněným na pohyblivou část okna (dveří) a jazýčkovým kontaktem, který se připevní na jeho rám. Permanentní magnet je většinou zmagnetovaný váleček z feritu a jazýčkový kontakt je tvořený zatavenou skleněnou trubičkou naplněnou vzácným plynem a jsou v ní umístěny dva feromagnetické kontakty. V klidovém režimu jsou obě části od sebe odděleny. Pokud dojde k rozepnutí částí magnetického kontaktu nad hranici otevření vstupu, je vyvoláno poplachové hlášení.

U plastového magnetického kontaktu se svorkovnicí QST-GN od výrobce Elmdene (Obr. 16) dojde k vyhlášení poplachu při vzájemné změně polohy spínače a ovládacího magnetu, tj. při otevření dveří nebo oken. K dalším technickým parametrům magnetického kontaktu QST-GN patří vestavěné rezistory 1k/1k a pracovní vzdálenost max. 20 mm. [18] Prvek je certifikovaný NBÚ pro stupeň 2.

Obr. 16. Magnetický kontakt QST-GN [18]

Duální detektor tříštění skla FG1625TAS

Duální detektor tříštění skla FG1625TAS od výrobce Honeywell (Obr. 17), certifikovaný NBÚ pro stupeň 2, je navržený pro rozpoznávání charakteristického zvuku skla. Principem funkce je detekce tříštění skla na základě změn tlaku vzduchu v místnosti a pomocí detekce zvuku rozbíjeného skla. Snímač zvuku a snímač tlaku pracují s různými snímacími frekvencemi. Díky porovnávání nízko a vysokofrekvenčních signálů se změnami akustického tlaku, tj. tříštění skla musí být detekováno oběma snímači, jsou spolehlivě eliminovány falešné poplachy.

FG1625TAS lze použít i pro skleněné plochy s nalepenou bezpečnostní fólií a nabízí dosah až 7,6 m. Jednotlivé detekce jsou indikovány LED diodami a poplachový signál přenášen přes výstupní relé. [19]

Obr. 17. Detektor tříštění skla FG1625TAS [19]

V objektu MVVP bude uvedený detektor nainstalovaný ve vybraných místnostech v blízkosti oken, kde mohou vznikat falešné poplachy v důsledku jejich nesprávného uzavření a následného chvění oken z důvodu jejich stáří.

PROSTOROVÁ OCHRANA

Centrálními body budovy, kam se umísťují prvky prostorové ochrany, jsou schodišťové přístupy či výstupy, haly, spojovací chodby, kancelářské prostory a vnitřní komunikační uzly.

Světlíky na chodbách v zabezpečeném objektu MVVP navrhuji chránit PIR detektory EV 105, prostory chodeb PIR detektory CX 702 a kanceláře a učebny PIR detektory RXC-ST (CORE). Všechny uvedené detektory splňují certifikaci NBÚ pro bodové hodnocení SS92=2.

EV 105

Mezi nejvíce rozšířené detektory pohybu patří pasivní infračervené detektory, jejichž funkce spočívá v zachycení pohybu objektu, jehož teplota se liší od teploty střeženého okolí.

Do této skupiny lze zařadit i EV 105 (Obr. 18) od firmy UTC Fire & Security. Jde o pohybový detektor s precizní zrcadlovou optikou s proměnlivým ohniskem. Díky zrcadlové optice je infračervené záření, které vychází ze snímaného prostoru, rozděleno na detekční zóny a pomocí lomu nebo odrazu infračerveného paprsku přivedeno na senzor detektoru, který je citlivý na infračervené záření. Tím dojde k jeho zahřátí a vzniku povrchového elektrického náboje, který elektronika zesílí a při dostatečné úrovni vyhodnotí jako poplach.

Technické parametry detektoru:

- pokrytí: 7 záclon po 12 m,
- úhel záběru: 86°,
- napájecí napětí: 8 - 15 V,
- proudová spotřeba: klidový stav - 5 mA, v poplachu, LED zapnuta - 10 mA,
- výstupy: poplach - NC kontakt, 100 mA při 28 V, tamper - NC kontakt, 100 mA při 28 V,
- montážní výška: 1,8 až 3 m,
- prostředí: -10 °C až +55 °C; max. 90 % vlhkost. [20]

Obr. 18. PIR detektor EV 105 [20]

Uvedený detektor bude v prostorách MVVP umístěný na chodbách k zabezpečení světlíků ve střeše. K úplnému zajištění prostoru bude použito více detektorů tak, aby pokrývaly celou střeženou plochu. Vícenásobné použití detektoru je bezpečné, protože ty se vzájemně neovlivňují a tudíž je jejich aplikace v prostorách vhodná.

CX 702

Infračervený dvojitě stíněný PIR detektor firmy OPTEX CX 702 (Obr. 19) je svými vlastnostmi předurčen k použití v prostorách, kde je požadována vysoká účinnost a detekční spolehlivost. Jednoduché otočení čočky umožní volit mezi dosahem 21 m x 21 m širokým úhlem 85° nebo 45 m x 2,4 m dlouhým dosahem. Díky dvojitému těsnění optiky je odolný vůči hmyzu a prachu. K dalším vlastnostem patří ochrana proti vysokofrekvenčnímu záření, horizontální nastavení oblasti detekce ve 3 úrovních a nastavitelný čítač pulzů.

Technické parametry detektoru:

- napájecí napětí: 9,5 - 16 V,
- proudová spotřeba: 8 mA, max. 11 mA při 12 V,
- výstupy: poplach - NC kontakt, 28 V/0,2 A, tamper – NC, sepne při otevření krytu, 28 V/0,1 A,
- montážní výška: 1,5 až 3,6 m,
- rychlost detekce: 0,3 – 1,5 m/s,
- citlivost: 1,6 °C na 0,6 m/s,
- prostředí: -20 °C až +50 °C; max. 95 % vlhkost. [21]

Obr. 19. PIR detektor CX 702 [21]

Výborných vlastností tohoto detektoru bude využito při zastřežení chodeb v objektu MVVP. Budou umístěny v rozích a doplňovat tak PIR detektory EV 105.

RXC-ST (CORE)

Dalším použitým infračerveným detektorem bude RXC-ST (CORE) (Obr. 20) výrobce Optex s půlkulovitou optikou s Quad Zone Logic a polovodičovým poplachovým výstupem. RX-ST (CORE) pokrývá střeženou oblast celkem 78 detekčními zónami v rozsahu 12 m x 12 m širokým úhlem 85° nebo jej lze navolit na dosah dlouhý 18 m a široký 8 m. V každém místě střeženého prostoru se ověřuje více než čtyřmi detekčními zónami, zda je třeba vyhlásit či nevyhlásit poplach. Detektory mají díky vyhodnocovací technologii Quad Zone Logic větší přesnost jak při detekci osob, tak i zvířat.

Technické parametry detektoru:

- napájecí napětí: 9,5 - 16 V,
- proudová spotřeba: 8 mA, max. 11 mA při 12 V,
- výstupy: poplach - NC kontakt, 24 V/0,2 A, tamper – NC,
- montážní výška: 1,5 až 2,5 m,
- poplachová perioda: 2,5 s,
- prostředí: -20 °C až +50 °C. [22]

Obr. 20. PIR detektor RXC-ST [22]

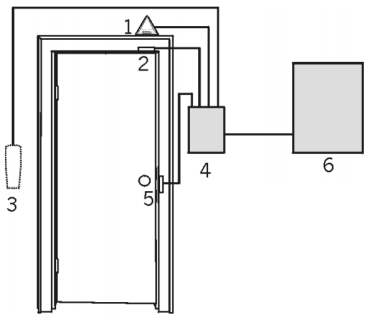
Specifikovaný detektor bude umístěn v rozích všech kanceláří, včetně zabezpečené oblasti č. 4 v kategorii Vyhrazené a také ve všech učebnách se simulátory, včetně ZO č. 1 a ZO č. 2. Také ZO č. 3 - serverovna bude chráněna tímto detektorem.

5.5 Integrovaný přístupový systém

Přístupový systém umožňuje spolehlivé sledování, evidenci a řízení průchodů osob v souladu s jejich oprávněním a režimovými opatřeními objektu, prostřednictvím specializovaných snímačů průchodu a přístupových mechanizmů, instalovaných v rámci systému jako celku.

Pro potřeby zajištění bezpečnosti kategorie zabezpečené oblasti Důvěrné nemusí být dle požadavků NBÚ použitý přístupový systém. Já bych ale rozšiřující instalaci navrhla nejen vzhledem k zabezpečení, ale i k ovládání požadovaných funkcí, jako je kontrola a řízení pohybu osob na pracovišti (která je dle analýzy rizik nedostačující), řízení a evidenci cvičících jednotek na jednotlivých simulátorech, respektive učebnách. Uložené evidenční údaje by bylo možné v budoucnu využít pro urychlení práce s přidělováním přístupových práv jednotlivým osobám a také ke statistickým účelům.

Pro jednotlivé dveře, určené k registrování a ovládání vstupu, je nutné vytvořit v systému „přístupový bod“ se čtečkou a elektromechanickým zámkem. Přístupový bod (Obr. 21) lze vytvořit pomocí klávesnice DGP2-641R LCD se zabudovanou čtečkou. Klávesnice je připojena přes sběrnici RS 485 k ústředně DIGIPLEX EVO 192, která je srdcem již navrženého systému PZTS.



Obr. 21. Schéma přístupového bodu [23]

Popis obrázku:

1 - Odchodové tlačítko BT-004 (Obr. 22) místo detektoru na vstupu.

2 - Dveřní kontakt v provedení magnet detekuje otevření dveří a deaktivuje dveřní zámek.

3 - Čtečka na obrácené straně zdi – není v tomto případě použita.

4 - Klávesnice s integrovanou čtečkou – DGP2 641R LCD.

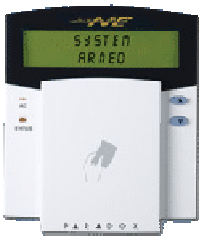
5 - Dveřní zámek.

6 - Ústředna DIGIPLEX EVO.

Obr. 22. Odchodové tlačítko BT-004 [24]

5.5.1 Klávesnice DGP2-641R

Klávesnice DGP2-641R (Obr. 22) se skládá ze zabudované čtečky Proximity a modulu DGP-ACM1P. Na její vstupy se připojí magnetický kontakt (QST-GN) pro detekci otevření a zavření dveří a odchodové tlačítko. Programovatelný výstup je určený pro ovládání dveřního zámku (AbloyEL 460) přes pomocné relé. V případě, že uživatel má povolený vstup do dveří, relé po přiložení karty sepne. Dveřní zámek je aktivován a otevře dveře. Elektromechanický zámek a dveřní kontakt jsou již navrženy mezi mechanickými zábrannými prostředky.



Obr. 23. Klávesnice DGP2-641R [23]

Pokud je čtečka / klávesnice připojena na napětí, začne její anténa nepřetržitě vysílat elektromagnetické budící pole. V okamžiku, kdy se karta vloží do tohoto pole, indukuje její anténa toto pole a energii získanou indukcí napájí vnitřní obvody karty. Karta odvysílá svoje identifikační číslo čtečce a ta vyhodnotí, zda se jedná o vysílání v korektním formátu. Pokud byl formát dat vyhodnocen jako správný, dojde ke zpracování a odeslání dat z čtečky do modulu, do kterého je připojena. Modul po sběrnici BUS pošle data do ústředny a ta vyhodnotí, zda karta má oprávnění k požadované akci. [23]

Technické parametry klávesnice:

- napájecí napětí: 11 – 16 V, max. 100 mA,
- frekvence budícího pole čtečky: 125kHz,
- vysílání: 12500 a 15625 kHz,
- pouze pro vnitřní prostředí: 0°C - 50°C. [23]

5.5.2 Princip přístupu

Každý uživatel musí mít specifikováno, do které skupiny dveří a v jaký časový interval má přístup povolen. Po přiložení karty se dle oprávnění aktivuje dveřní zámek.

a) **Vstup kartou -** přiložením karty ke čtečce je aktivován dveřní zámek, který dveře otevře.

b) **Vstup kartou s vypnutím podsystému -** přiložením karty dojde k vypnutí podsystému a k aktivaci dveřního zámku.

c) **Násilné otevření dveří -** při narušení dveřního kontaktu bez předchozího přiložení platné karty je vyhlášen poplach.

d) **Odchod – klika / koule -** dveře se otevřou klikou pouze z vnitřní strany. Z vnější strany jsou dveře vybaveny koulí.

e) **Odchod a zapnutí systému kartou** - po uzavření dveří se ke čtečce dvakrát přiloží karta s intervalem 5 s a dojde k zapnutí podsystému.

f) **Zapnutí kódem a odchod** - na klávesnici se zadá kód a tím dojde k zapnutí příslušného podsystému.

Přístupové body budou nainstalovány u všech dveří do zabezpečených oblastí a u vstupu do zabezpečeného objektu. Bude jimi možné po přiložení přístupové karty evidovat a regulovat vstup do uvedených chráněných prostorů.

5.6 Zařízení pro fyzické ničení nosičů informací

Zařízení pro fyzické ničení nosičů informací je doplňkovým technickým prvkem v zajištění bezpečnosti utajovaných informací. Zařízení bude umístěno v zabezpečené oblasti č. 4, která je kategorie Vyhrazené k ničení papíru, CD a plastových identifikačních karet. Pro tuto funkci jsem vybrala skartovač JAWS S4 (Obr. 24).

Obr. 24. Skartovač JAWS 24 [25]

5.7 Bodové hodnocení navrženého zabezpečení

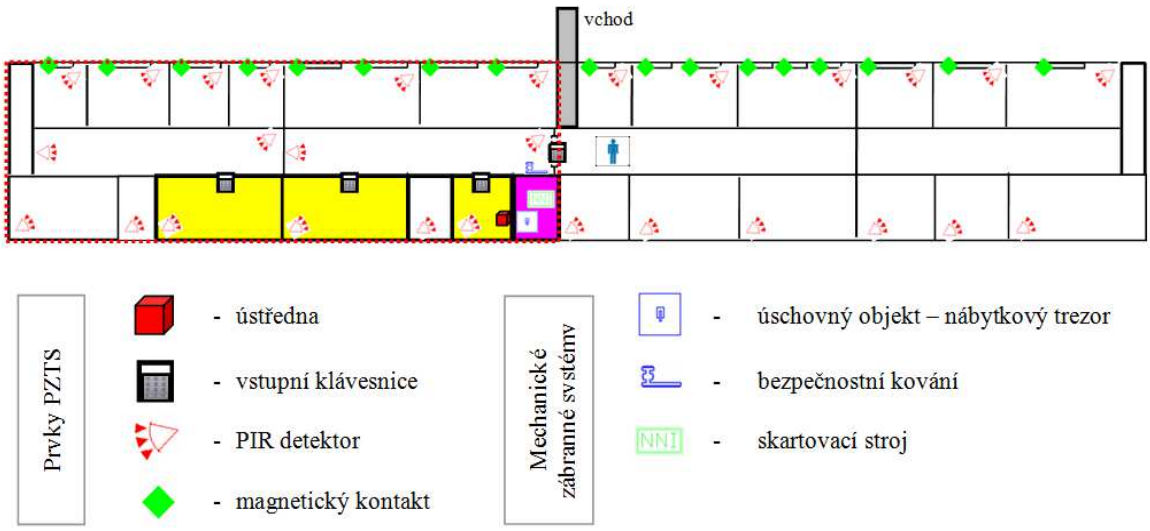
Ve stávající kapitole jsem po zhodnocení analýzy rizik navrhla jednotlivá opatření fyzické bezpečnosti pro zabezpečené oblasti.

Výsledné bodové ohodnocení jednotlivých opatření dle stanovené minimální bodové hodnoty NBÚ pro zabezpečenou oblast kategorie Důvěrné je uvedeno v tabulce v Příloze č. 2 (P II) této práce.

Minimální bodové ohodnocení zabezpečení pro kategorii Vyhrazené je splněno, především díky začlenění zabezpečené oblasti do PZTS. Ochrana samotných dokumentů je zajištěna úschovným objektem v místnosti.

5.8 Dílčí závěr

V kapitole 5 práce jsem na základně výsledků provedené analýzy rizik navrhla pro zabezpečené oblasti kategorie Vyhrazené a Důvěrné opatření fyzické bezpečnosti. Jsou jimi systém ochrany pomocí režimových opatření s využitím fyzické ostrahy a komplexní návrh technických prostředků poplachového zabezpečovacího systému včetně integrovaného systému kontroly přístupu (Obr. 25). Na doplnění specifikovaných opatření dle NBÚ pro zabezpečené oblasti jsem vybrala zařízení fyzického ničení nosičů informací.



Obr. 25. Návrh řešení zabezpečení MVVP technickými prostředky

ZÁVĚR

Cílem této diplomové práce je konceptuální návrh opatření fyzické bezpečnosti, kterými by bylo možné chránit perspektivní vojenské výcvikové pracoviště. Utajované informace, uložené v jeho nejhodnotnějších aktivech v podobě softwarových databází spolu s podpůrnými technickými prostředky a užitnou hodnotou pracoviště, se staly předmětem mých návrhů k zajištění jejich ochrany.

V teoretické části práce jsem se zabývala problematikou utajované informace, charakteristikou zabezpečených a jednacích oblastí, specifikací jednotlivých druhů ochrany podle ustanovení Národního bezpečnostního úřadu a vymezením zabezpečení v rezortu Ministerstva obrany. Zaměřila jsem se na analýzu systému fyzické bezpečnosti v rezortu MO a podrobnou bezpečnostní analýzu rizik, která je součástí projektu fyzické bezpečnosti. Dále jsem vymezila zásady zpracování projektu fyzické bezpečnosti a specifikovala východiska bezpečnostního projektu.

Ve stěžejní části práce jsem definovala výchozí podmínky pro návrh zabezpečení modelového pracoviště v návaznosti na legislativní požadavky Národního bezpečnostního úřadu a požadavky Ministerstva obrany na fyzickou bezpečnost. Spolu s charakteristikou pracoviště jsem specifikovala jeho aktiva a pomocí kombinace několika metod analýzy rizik jsem vyhledala nejzávažnější rizika, vyhodnotila zranitelnost zabezpečovaného objektu a určila celkovou míru rizika. Na jejím základě jsem vyjádřila minimální bodové ohodnocení pro jednotlivé zabezpečené oblasti na pracovišti a navrhla opatření systému fyzické bezpečnosti v oblasti režimových opatření, fyzické ostrahy a technických prostředků.

Návrhy na naplnění požadavků na zabezpečení ochrany utajovaných informací v oblasti fyzické bezpečnosti byly koncipovány s důrazem na podmínky NBÚ a MO a reálné technické řešení. Mohou být využity jako podklad pro zpracování návrhu projektu fyzické bezpečnosti pracoviště v případě realizace této akvizice v rezortu MO.

Jsem si vědoma toho, že navržená opatření fyzické bezpečnosti nemusí být finálním řešením, a že úkolem bezpečnostního manažera je potřeba vhodně vyvažovat, co je opravdu nutné, a co už je nepřijatelné z hlediska přílišného omezování lidí, protože dokonalý systém ochrany není možné vytvořit.

ZÁVĚR V ANGLIČTINĚ

The purpose of this thesis is the conceptual draft of physical security measures, which could protect prospective military training centre. Secret information situated in its most valuable assets in the form of database software together with supporting technical means and value of workplace, became the targets of my offer to provide their protection.

In the theoretical part of the work I introduced secret information, the description of secure and dealing areas with specifications of individual sorts of protection in according to the National Security Office and the definition of security department in the Ministry of Defence. I presented the analysis of the physical security of the Ministry of Defence and detailed security risk analysis, which is part of the physical security. I also defined the principles of processing physical security project and specify the basis of the safety project.

In the main part of the thesis I defined initial conditions for security profile model workplace in relation to the legislative requirements of the National Security Office and Defense Department requirements for physical security. Along with the description of the workplace, I specify its assets and using the combination of risk analysis methods I found the most serious risks and identified the vulnerability of the protected objects and determine the total level of risk. Due to the basis, I expressed the minimum score for each secured area of the workplace and proposed measures of physical security of the regime measures, physical security and technical resources.

Proposals for the implementation of the protection requirements of secret information in the field of physical security were arranged with condition of on the NSO and MD and real technical solution. They can be used as a basis for the drafting of physical security project for the realization of this acquisitions in the MD.

I am aware that the proposed physical security measures may not be the final solution, and the task of the security manager is needed to balance properly what is really necessary and what is unacceptable focusing on people influence, because a perfect protection system can not be created.

SEZNAM POUŽITÉ LITERATURY

[1] MUSIL, Rudolf. *Ochrana utajovaných skutečností*. Vyd. 1. Praha: Eurounion, 2001, 379 s. ISBN 80-858-5893-2.

[2] ČESKO. Zákon č. 412 ze dne 21. září 2005 o ochraně utajovaných informací a bezpečnostní způsobilosti, ve znění pozdějších předpisů. In: *Sbírka zákonů České republiky*. 2005, částka 143, s. 7526-7576. ISSN 1211-1244. Dostupné také z: http://aplikace.mvcr.cz/archiv2008/sbirka/1998/sb039-98.pdf.

[3] Obecně k průmyslové bezpečnosti. In: *Www.nbu.cz* [online]. [2005] [cit.2013-02-06]. Dostupné z: http://www.nbu.cz/cs/ochrana-utajovanych-informaci/...

[4] ČESKO. Rozkaz ministra obrany č. 22/2006: Ochrana utajovaných informací v rezortu MO. In: *Věstník MO, r. 2006, částka 13*. 2006.

[5] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management I*. 1. vyd. Zlín: VeRBuM, 2011, 316 s. ISBN 978-80-87500-05-7.

[6] ČESKO. Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb. a vyhlášky č. 454/2011 Sb. In: *http:// www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/vyhlaska-c-5282005/*. 2005. [cit.2013-02-06].

[7] ČESKO. Normativní výnos bezpečnostního ředitele MO č. 42/2006: Fyzická bezpečnost v rezortu MO. In: *Věstník MO, r. 2006, částka 29*. 2006.

[8] ČESKO. Příloha č. 1 k vyhlášce č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb. a vyhlášky č. 454/2011 Sb. [online] In: *http://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/ vyhlaska-c-5282005*. 2005.

[9] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management II*. 1. vyd. Zlín: VeRBuM, 2012, 387 s. ISBN 978-80-87500-19-4.

[10] HOFREITER, Ladislav. *Zásady a princípy analýzy rizík v oblasti fyzickej a objektovej bezpečnosti* [online]. Žilina: Fakulta špeciálneho inžinierstva ŽU v Žiline,
2006. 34 s. [cit.2013-02-27]. Metodika. Žilinská univerzita v Žiline. Dostupné z: http ://www.nbusr.sk/ ipublisher/files/...

[11] SVETLÁKOVÁ, Veronika. *Modernizace zabezpečovacího systému výcvikového pracoviště*. Zlín, 2010. Bakalářská práce. Univerzita Tomáše Bati, Fakulta aplikované informatiky. Vedoucí práce doc. Ing. Luděk Lukáš, CSc.

[12] VALOUCH, Jan. Projektování bezpečnostních systémů. Vyd. 1. Ve Zlíně: Univerzita Tomáše Bati ve Zlíně, 2012. 152 s. ISBN 978-80-7454-230-5.

[13] ČSN CLC/TS 50131-7. *Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 7: Pokyny pro aplikace.* Praha: ÚNMZ, 2011. 44 s. Třídící znak 334591.

[14] KINDL, Jiří. *Projektování bezpečnostních systémů I.* 2. vyd. Zlín: Univerzita Tomáše Bati, 2007, 134 s. ISBN 978-80-7318-554-1.

[15] MAXIMOV, Alexey. *Obecné příčiny afghánského problému z pohledu evropské bezpečnosti*. Zlín, 2012. Diplomová práce. Univerzita Tomáše Bati, Fakulta aplikované informatiky. Vedoucí práce JUDr. Vladimír LAUCKÝ.

[16] Zabezpečovací ústředna DIGIPLEX EVO192. In: *Eurosat CS: Specializovaný velkoobchod na zabezpečovací technologie* [online]. [cit. 2013-04-20]. Dostupné z: http://www.eurosat.cz/3034-evo192.html.

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

[18] Magnetický kontakt se svorkovnicí a EOL rezistory 1k/1k, pracovní mezera 20mm. In: *ADI Global Distribution* [online]. © ADI Global Distribution-2013 [cit. 2013-04-20]. Dostupné z: http://www.adiglobal.cz/iiWWW/cz/produkty110.nsf/

[19] Detektor tříštění skla s dosahem až 7,6m i pro skla s fóliemi. In: *ADI Global Distribution* [online]. © 2013 [cit. 2013-04-20]. Dostupné z: http://www.adiglobal.cz/iiWWW/cz/produkty110.nsf/...

[20] EV105. In: *Techfors* [online]. © 2012 [cit. 2013-04-21]. Dostupné z: http://www.techfors.eu/products/ev105/.

[21] PIR s otočnou čočkou – CX-702. In: *Euroalarm* [online]. © 2007 [cit. 2013-04-21]. Dostupné z: http://www.euroalarm.cz/zabezpecovaci-technika/zabezpeceni/detektory/infra-pir/cx-702.

[22] RXC-ST. In: *A1 com: Bezpečnostní systémy-specializovaný velkoobchod* [online]. [cit. 2013-04-21]. Dostupné z: http://www.a1com.cz/3162/rxc-st/.

[23] EVO 48, EVO 192 – Nadstavba přístupu – Manuál. In: *Elektro-Mahl s.r.o.* [online]. ©2002-2013 [cit. 2013-04-22]. Dostupné z: http://www.elektro-mahl.cz/dokumenty/DIGIPLEX/EVO-48-192-ACC-manual.pdf.

[24] BT-004 – EXIT tlačítko METAL. In: *VARIANT plus: Komplexní řešení elektronických systémů budov* [online]. © 2008 – 2010 [cit. 2013-04-22]. Dostupné z: http://www.variant.cz/zbozi/1003-080-bt-004.

[25] Skartovač JAWS S4. In: *ILH* [online]. © 2005-2013 [cit. 2013-04-22]. Dostupné z: http://www.ilh.cz/p.axd/cs/Skartova%C4%8D.JAWS.S4.html.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACCESS	Access Control System.
AČR	Armáda České republiky.
ALARP	As Low As Reasonably Practicable.
CCTV	Closed Circuit Television.
CD	Compact Disc.
CD-ROM	Compact Disc Read-Only Memory.
ČR	Česká republika.
D	Důvěrné.
DPPC	Dohledové a poplachové přijímací centrum.
DVD	Digital Versatile Disc.
EMI	Elektromagnetická interference.
EU	Evropská unie.
IKT	Informační a komunikační technologie.
IOOLB	Institut ochrany obyvatelstva Lázně Bohdaneč.
MO	Ministerstvo obrany.
MVVP	Modelové vojenské výcvikové pracoviště.
NBÚ	Národní bezpečnostní úřad.
NVMO	Normativní výnos Ministerstva obrany.
OC	Organizační celek.
PT	Přísně tajné.
PTZS	Poplachové zabezpečovací a tísňové systémy.
PZS	Poplachový zabezpečovací systém.
RMO	Rozkaz ministra obrany.
T	Tajné.

UI	Utajovaná informace.
USB	Universal Serial Bus.
V	Vyhrazené.
WAN	Wide Area Network.

SEZNAM OBRÁZKŮ

Obr. 1. Opatření fyzické bezpečnosti 19
Obr. 2. Systém zabezpečení aktiv 30
Obr. 3. Příklad algoritmu zranitelnosti chráněného prostoru [10] 33
Obr. 4. Možný postup při stanovení míry rizika [10] 35
Obr. 5. Oblasti zájmu bezpečnostního posouzení [13] 38
Obr. 6. Faktory ovlivňující bezpečnostní posouzení budovy 39
Obr. 7. Bezpečnostní posouzení – vnitřní vlivy 40
Obr. 8. Bezpečnostní posouzení – vnější vlivy 40
Obr. 9. Učebny se simulátory 45
Obr. 10. Prostorové uspořádání MVVP 46
Obr. 11. Identifikace hrozeb - Ishikawa diagram příčin a následků 50
Obr. 12. Graf analýzy souvztažnosti hrozeb 54
Obr. 13. Zobrazení hranice objektu a zabezpečených oblastí 59
Obr. 14. Provedení stavebních úprav 60
Obr. 15. Ústředna PTZS [16] 65
Obr. 16. Magnetický kontakt QST-GN [18] 67
Obr. 17. Detektor tříštění skla FG1625TAS [19] 67
Obr. 18. PIR detektor EV 105 [20] 68
Obr. 19. PIR detektor CX 702 [21] 69
Obr. 20. PIR detektor RXC-ST [22] 70
Obr. 21. Schéma přístupového bodu [23] 71
Obr. 22. Odchodové tlačítko BT-004 [24] 72
Obr. 23. Klávesnice DGP2-641R [23] 72
Obr. 24. Skartovač JAWS 24 [25] 73
Obr. 25. Návrh řešení zabezpečení MVVP technickými prostředky 74

SEZNAM TABULEK

Tab. 1: Podmínky přístupu fyzické osoby k utajované informaci 14
Tab. 2: Části projektu fyzické bezpečnosti podle typu kategorie zabezpečené (ZO) nebo jednací oblasti (JO) 25
Tab. 3. Postup a kritéria hodnocení hrozeb [10] 32
Tab. 4. Matice hodnocení zranitelnosti 34
Tab. 5. Příklad použití matice rizik při určení míry rizika ohrožení UI [10] 35
Tab. 6. Stupně zabezpečení systému PZTS ČSN CLC/TS 50 131-7 [13] 41
Tab. 7. Třídy prostředí [14] 41
Tab. 8. Aktiva – identifikace, stupeň utajení a velikost újmy 49
Tab. 9. Seznam možných komplexních ohrožení objektu 51
Tab. 10. Sestavení matice souvztažnosti 53
Tab. 11. Hodnoty koeficientů K_{ih} a K_{jh} 53
Tab. 12. Závažnost provázanosti hrozeb z hlediska procesního a strukturálního 55
Tab. 13. Matice zranitelnosti MVVP 55
Tab. 14. Celková míra rizika modelového pracoviště 56
Tab. 15. Bodové hodnoty zabezpečené oblasti kategorie Důvěrné [8] 57
Tab. 16. Bodové hodnoty zabezpečené oblasti kategorie Vyhrazené [8] 57
Tab. 17. Zabezpečení vstupu do ZO č. 4 62
Tab. 18. Úschovný objekt pro ZO č. 4 63
Tab. 19. Zabezpečení vstupu do ZO č. 3 63
Tab. 20. Zabezpečení vstupu do ZO č. 1 a ZO č. 2 63

SEZNAM PŘÍLOH

P I: Příklady hodnocení hrozeb

P II: Bodové hodnocení navrženého řešení zabezpečení kategorie Důvěrné

P I: PŘÍKLADY HODNOCENÍ HROZEB

Hrozba		**Zdroj hrozby**	**Příčina**	**Výskyt již dříve**	**Hodnocení (H;,M;S;V)**
Z hlediska polohy a umístění objektu	H_1	Výrobní objekty	Havárie, zdroje nebezpečných látek		
	H_2	Stacionární zdroje nebezpečných látek			
	H_3	Mobilní zdroje nebezpečných látek	Blízkost komunikace a rozvodů		
	H_4	Dopravní nehody	Blízkost komunikace, železnice,let. koridoru		
	H_5	Jaderná zařízení	Havárie		
	H_6	Vodní nádrže	Protržení hráze		
Zabezpečení ochrany objektu a chráněného prostoru	H_7	Náhodný lupič	Zisk		
	H_8	Lupič po přípravě	Zisk, pomsta		
	H_9	Vandalismus	Vyjádření odporu, poškození majetku		
	H_{10}	Návštěvy	Zisk, zvědavost, nedostatečná režimová opatření		
	H_{11}	Dodavatelé			
Činnost cizích zpravodajských služeb, záškodníků, teroristických a zločineckých skupin	H_{12}	Cizí zpravodajské služby	Poškození zájmů, politické, vojenské, ekonomické zájmy		
	H_{13}	Komerční zpravodajské služby			
	H_{14}	Teroristé	Pomsta, vyvolání strachu, vydírání		
	H_{15}	Odpůrci	Poškození zájmů		
	H_{16}	Skupina organizovaného zločinu	Zisk, poškození zájmů, pomsta,...		
	H_{17}	Záškodníci	Pomsta, poškození zájmů, sabotáž,...		
Technické poruchy	H_{18}	Rozvod el. energie	Havárie, požár, zaplavení,		
	H_{19}	Rozvod vody			
	H_{20}	Rozvod a zásobníky plynu			
	H_{21}	Ústřední topení			
Zaměstnanci	H_{22}	Vlastní zaměstnanci-oprávněné osoby	Zisk, nedbalost, neznalost, vydírání,..		
	H_{23}	Vlastní zaměstnanci-oprávněné osoby	Pomsta, zisk, vydírání, nedostatečná ochrana		
	H_{24}	Servisní služby, obslužný personál	Zisk, častá migrace, nedostatečná ochrana		
	H_{25}	Pracovníci FO	Zisk, nedbalost, vydírání, neoprávněný přístup		
Okolní objekty	H_{26}	Výrobní objekty, zdroje nebezpečných látek	Havárie, blízkost objektu		
Výjimečný stav, nouzový stav	H_{27}	Povodně a záplavy	Blízkost vodního zdroje, objekt v záplavové oblasti		
	H_{28}	Požár	Blesk, sabotáž, havárie,...		
	H_{29}	Sesuv půdy	Geologické podmínky		
	H_{30}	Narušení veřejného pořádku	Extremismus, sociální nepokoje		

P II: BODOVÉ OHODNOCENÍ NAVRŽENÉHO ZABEZPEČENÍ KATEGORIE „D“

Zabezpečená oblast	Hranice zabezpečené oblasti je v celé své délce shodná s hranicí objektu.				ne
číslo	1,2,3	**Stupeň utajení DOB:**	AČR-	MVVP	**Míra rizika**
kategorie	"D"	neutajovaná	stránka č.:	1	
třída	II.		z celkem:	1	velká
označení					
účel	Úložna utajovaných skutečností nebo předmětů.				

Bezpečnostní opatření	**Typ**	**Bodové hodnocení**
Úschovný objekt	nehodnoceno	SS1 = 0 bodů
Zámek úschovného objektu	nehodnoceno	SS2 = 0 bodů
Celkové hodnocení úschovného objektu a jeho zámku	= SS1 x SS2	**S1 = 0 bodů**
Zabezpečená oblast	typ 2	SS3 = 2 body
Uzamykací systém	typ 2	SS4 = 2 body
Celkové hodnocení místnosti a jejího uzamykacího systému	= SS3 x SS4	**S2 = 4 body**
Objekt	typ 1	**S3 = 1 bod**
Kontrola vstupu	typ 2	SS6 = 2 body
Režim návštěv	s doprovodem	SS7 = 3 body
Celkové hodnocení kontroly vstupu	= SS6 + SS7	**S4 = 5 bodů**
Ostraha	typ 4	SS8 = 4 body
Zařízení EZS	typ 2	SS91 = 2 body
Instalace zařízení EZS	typ 2	SS92 = 2 body
mezivýsledek (SS91+SS92)xSS92/OBL/2		SS9 = 2 body
Celkové hodnocení ostrahy a systému EZS	= SS8 + SS9	**S5 = 6 bodů**
Fyzické bariéry	nehodnoceno	SS10 = 0 bodů
Kontrola vstupu v přístup.bodech bariéry	není realizována	SS11 = 0 bodů
Namátkové vstupní a výstupní prohlídky	nejsou prováděny	SS12 = 0 bodů
Perimetrický detekční systém (PDS)	není realizován	SS13 = 0 bodů
Bezpečnostní osvětlení perimetru	není realizováno	SS14 = 0 bodů
Speciální televizní systém na perimetru	není realizován	SS15 = 0 bodů
Celkové hodnocení ochrany perimetru	=(SS10xSS11)+SS12 +SS13+SS14+SS15	**S6 = 0 bodů**
Celkový výsledek		**16 bodů**