Modernizace zabezpečovacího systému výcvikového pracoviště

Modernization of the security system of a training center

Veronika Svetláková

Bakalářská práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2010/2011

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

Jméno a příjmení:	**Veronika SVETLÁKOVÁ**
Osobní číslo:	**A08011**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Modernizace zabezpečovacího systému výcvikového pracoviště**

Zásady pro vypracování:

1. **Objasněte požadavky na zabezpečení vojenských objektů.**
2. **Specifikujte a analyzujte strukturu specifického vojenského objektu.**
3. **Analyzujte systém fyzické bezpečnosti specifického vojenského objektu.**
4. **Navrhněte možnosti a způsoby zlepšení fyzické bezpečnosti specifického vojenského objektu.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **ČERNÝ, J., IVANKA, J., a kol. Systemizace bezpečnostního průmyslu I. 2. vydání, Zlín: UTB, 2006. 135 s. ISBN 80-7318-402-8**
2. **LAUCKÝ, V. Řízení technologických procesů v průmyslu komerční bezpečnosti. 2. vydání, Zlín: UTB, 2006. 101 s. ISBN 80-7318-432-X**
3. **KINDL, J. Projektování bezpečnostních systémů. Zlín: UTB, 2007. 134 s. ISBN 978-80-7318-554-1**
4. **KŘEČEK, S. a kol. Příručka zabezpečovací techniky. 3. vydání, Blatná: Cricetus, 2006. 313s. ISBN 80-902938-2-4**
5. **UHLÁŘ, J. Technická ochrana objektů II. díl, Elektrické zabezpečovací systémy II. 1. vydání, Praha: PA, 2005. 229 s. ISBN 80-7251-189-0**
6. **ČANDÍK, Marek. Objektová bezpečnost II. 1. vydání, UTB Zlín, 2004. 100 s. ISBN 80-7318-217-3**

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

Datum zadání bakalářské práce: **25. února 2011**

Termín odevzdání bakalářské práce: **23. května 2011**

Ve Zlíně dne 25. února 2011

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

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

ABSTRAKT

Tato bakalářská práce je zaměřena na analýzu fyzické bezpečnosti specifického vojenského objektu a modernizaci zabezpečovacího systému výcvikového pracoviště.

Jsou zde objasněny požadavky fyzické bezpečnosti v resortu Ministerstva obrany. Je využito poznatků z oboru bezpečnostních technologií a projektování bezpečnostních systémů v kombinaci s aplikováním fyzické ochrany, režimových opatření a elektrických a mechanických zábranných prostředků pro zabezpečení objektu.

Popsány jsou jednotlivé použité bezpečnostní systémy a jejich prvky při současném stavu zabezpečení objektu specifického vojenského zařízení a v závěru práce jsou navrženy možnosti a způsoby zlepšení fyzické bezpečnosti objektu.

Klíčová slova: fyzická bezpečnost, zabezpečení vojenského objektu, poplachový zabezpečovací systém, systém kontroly vstupu

ABSTRACT

This bachelor work is focused on analyzing the physical safety of the specific military area and renovating of the security system in the training department.

There are mentioned the requirements of physical security at resort of the Ministry of Defence. Also there is used knowledge in the field of security technology and design of security systems in combination with applying physical protection, the regime measures and electrical and mechanical barriers for protection of property.

There are described the various security systems and their features in the current security status of specific military equipment. In the conclusion there are proposed options and ways to improve the physical security of the building.

Keywords: physical security, security, military building, analysis, security alarm system, access control system

Ráda bych touto cestou poděkovala doc. Ing. Luďkovi Lukášovi, CSc. za vedení, podnětné rady, připomínky a informace při tvorbě mé bakalářské práce, spolupracovníkům za podporu a týmu pracovníků firmy JIMI CZ, a.s. za poskytnutí materiálů a podkladů pro práci.

Velký dík také patří mé rodině, která mě usilovně podporovala po celou dobu studia.

Prohlašuji, že

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

Prohlašuji,

- že jsem na bakalářské práci pracovala samostatně a použitou literaturu jsem citovala. V případě publikace výsledků budu uvedena jako spoluautorka.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….…….

podpis diplomanta

OBSAH

ÚVOD

S rozvojem moderních technologií pro vzdělávání a výcvik vojáků, které se stále více využívají v Armádě České republiky (dále jen AČR), vznikají nové nároky na zabránění přístupu neoprávněných osob do vojenského objektu, na ztížení přístupu do vybraných objektů nebo na monitorování činnosti osob v těchto objektech a prostorech. Užitná i finanční hodnota výcvikových zařízení a samotných technologií je jedním z hlavních důvodů, proč je nutné zabývat se bezpečností takových objektů. Bezpečnost objektu musí být nastavena tak, aby eliminovala předpokládané hrozby. Ty mohou vycházet jak od jednotlivých pachatelů, tak teroristických nebo kriminálních skupin (organizací).
Eliminaci hrozeb, respektive snižování jejich potenciálu, lze řešit systémem ochran.

Systém ochrany vychází ze selhání dvou faktorů, a to:

- lidského, kdy jde o přístup jedince k bezpečnostní problematice,
- prostředí, kdy jde o vytvoření bezpečného prostředí, které eliminuje jakoukoliv potencionální hrozbu narušení bezpečnosti.

Nutnost těchto opatření lze doložit několika příklady selhání systému objektové ochrany. Pro informaci uvádím následující [1]:

- 4. srpna 1993 - z muničního skladu vojenské posádky ve Slaném na Kladensku zmizelo 36 pistolí a střelivo,
- prosinec 1994 - dva maskovaní vojáci přepadli v areálu Ministerstva obrany v Praze strážné a ukradli jim šest samopalů,
- říjen 1995 - skupina maskovaných osob přepadla dozorčího posádky v Hodoníně a odcizila 29 pistolí,
- červenec 1996 - desítky granátů a střelivo odcizili z muničního skladu v Radošově na Karlovarsku dva vojíni,
- červen 1999 - krádež rekordního počtu zbraní v Žatci na Lounsku: voják základní služby odcizil více než 1000 pistolí, osm samopalů a další zbraně,
- září 2000 - ze skladu v Bohuslavicích nad Vláří na Zlínsku zmizelo pět tun nebezpečné výbušniny trinitrotoluenu,
- listopad 2001 - řízenou protitankovou střelu a dva ruční protitankové granáty odcizil voják z Liberce v Čermné nad Orlicí,

- květen 2002 - u vojenského útvaru v Rožmitále pod Třemšínem se ztratilo 130 granátů,
- září 2002 - ze skladu ve výcvikovém prostoru Boletice na Českokrumlovsku zmizely dvě bedny se 40 ručními granáty,
- červenec 2010 – vloupání do budovy Generálního štábu AČR s minimálními škodami. [2]

Ve své práci se zaměřím na analýzu fyzické bezpečnosti specifického vojenského objektu a modernizace zabezpečovacího systému výcvikového pracoviště.

V první části práce jsou popsány požadavky na zabezpečení chráněných prostorů a specifikace fyzické bezpečnosti v rezortu Ministerstva obrany. Poté následuje určení, funkce a prostorová dispozice specifického vojenského zařízení. Druhá část práce popisuje současný stav zabezpečení speciálního výcvikové zařízení v analýze systému fyzické bezpečnosti. V závěru jsou navržena opatření ke zlepšení stavu fyzické bezpečnosti uvedeného objektu.

Součástí této práce nejsou žádné fotografie prostorů specifického vojenského objektu ani jeho okolí z důvodu bezpečnostních opatření, vztahujících se k vojenskému areálu.

I. TEORETICKÁ ČÁST

1 POŽADAVKY NA ZABEZPEČENÍ CHRÁNĚNÝCH PROSTORŮ

1.1 Problematika fyzické bezpečnosti

Fyzická bezpečnost je systém opatření, která mají neoprávněné osobě zabránit nebo ztížit přístup k utajovaným informacím, popřípadě přístup nebo pokus o něj zaznamenat pomocí ostrahy, režimových opatření a nasazení technických prostředků. [3]

Realizace stanovených opatření vychází ze zákona č. 412/2005 Sb., (dále jen „zákon“) o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. Tento zákon ukládá odpovědným osobám orgánů státu a právnickým i podnikajícím fyzickým osobám (podnikatelům), které mají přístup k utajovaným informacím, řadu povinností. Mezi ně patří i povinnost realizovat opatření fyzické bezpečnosti.

S utajovanými informacemi ve smyslu zákona lze manipulovat pouze v prostorech k tomu určených a těmi jsou objekty, zabezpečené oblasti a jednací oblasti.

1. Objektem je budova nebo jiný ohraničený prostor, ve kterém se nachází zabezpečená oblast nebo jednací oblast.
2. Zabezpečenou oblastí je ohraničený prostor v objektu.
3. Jednací oblastí je ohraničený prostor v objektu. Utajovanou informaci stupně utajení Přísně tajné nebo Tajné lze pravidelně projednávat pouze v jednací oblasti. [4]

Utajované informace podle nejvyššího stupně utajení, které se v zabezpečené oblasti ukládají, se rozdělují na Přísně tajné, Tajné, Důvěrné a Vyhrazené.

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

Fyzická ochrana je nepřetržitě zajišťována u objektu, ve kterém se nachází zabezpečená oblast kategorie Přísně tajné, Tajné a Důvěrné, a to jednou nebo dvěma osobami v kombinaci s technickými prostředky zabezpečení, umožňujícími rychlý zásah, je-li provádění ochrany utajovaných informací narušeno. Zajištění bezpečnosti u oblasti kategorie nejvýše Vyhrazené se ostraha zabezpečuje v rozsahu stanoveném odpovědnou osobou.

Ostraha se zabezpečuje zaměstnanci orgánu státu, právnické osoby nebo podnikající fyzické osoby, o jejichž objekt jde, příslušníky ozbrojených sil nebo ozbrojených sborů nebo příslušníky ozbrojených sil cizí moci anebo zaměstnanci bezpečnostní ochranné služby. [4]

Režimová opatření určují oprávnění osob a dopravních prostředků pro vstup/výstup a vjezd/výjezd do objektu, klíčový režim a manipulaci s 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.

Technickými prostředky jsou zejména mechanické zábranné prostředky, elektrická zámková zařízení a systémy pro kontrolu vstupů, zařízení elektrické zabezpečovací signalizace, speciální televizní systémy, tísňové systémy, zařízení elektrické požární signalizace, zařízení sloužící k vyhledávání nebezpečných látek nebo předmětů, zařízení fyzického ničení nosičů informací, zařízení proti pasivnímu a aktivnímu odposlechu utajované informace. [4]

Opatření fyzické bezpečnosti nebo kombinace více těchto opatření musí odpovídat alespoň nejnižší míře zabezpečení jednací oblasti nebo zabezpečené oblasti a stanoví se v závislosti na vyhodnocení rizik a na stupni utajení utajovaných informací, které jsou v jednací oblasti pravidelně projednávány, nebo na kategorii zabezpečené oblasti. [4] Tato opatření stanoví pověřená osoba v bezpečnostním projektu.

Prováděcím předpisem zákona je vyhláška č. 528/2005 Sb. (ve znění vyhlášky č. 19/2008 Sb.), o fyzické bezpečnosti a certifikaci technických prostředků, která stanovuje bodové ohodnocení jednotlivých opatření fyzické bezpečnosti, nejnižší míru zabezpečení zabezpečené oblasti a jednací oblasti, základní metodu hodnocení rizik, další požadavky na opatření fyzické bezpečnosti a náležitosti certifikace technického prostředku vzhledem ke stupni utajení. [5]

1.2 Specifikace fyzické bezpečnosti v resortu Ministerstva obrany

1.2.1 Fyzická bezpečnost

Pravidla pro fyzickou bezpečnost v rezortu Ministerstva obrany (dále jen „MO“) jsou stanovena v normativním výnosu č. 42/2006, o fyzické bezpečnosti v rezortu MO (dále jen „výnos“). Výnos vychází ze zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti 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, o ochraně utajovaných informací v resortu MO.

Výnos stanovuje odpovědnost za přidělené ubytovací prostory a ostatní zařízení pro organizační celky dislokované ve vojenském areálu. Stanovují se bezpečnostní manažeři rozlehlého objektu a jednotlivých organizačních celků, hranice objektu, odpovědnost za opatření fyzické bezpečnosti na hranici rozsáhlého objektu 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. Na základě vyhodnocení rizik a zranitelnosti utajované informace se stanovuje míra rizika jako „malá“, „střední“ nebo „velká“ a vedoucí organizačního celku schvaluje a realizuje projekt fyzické bezpečnosti.

1.2.2 Ochrana vojenského objektu

K jednotnému postupu při stanovení a zajištění bezpečnostních opatření, která mají chránit vojenský objekt ve smyslu zabránění, popř. ztížení tohoto jednání nebo zaznamenání neoprávněného přístupu do vojenského objektu a do prostorů, ve kterých se tento majetek nachází, slouží RMO č. 6/2009, o ochraně vojenského objektu, ve znění pozdějších úprav (dále jen „rozkaz“). Tento stanovuje pravidla bezpečnostních opatření, ochranu objektu prostřednictvím dodavatele a kontrolu při ochraně budov či jiných prostor v užívání AČR v souladu se zákonem č. 219/2000 Sb., o majetku České republiky a jejím vystupování v právních vztazích a zákonem č. 222/1999 Sb., o zajišťování obrany České republiky, ve znění pozdějších předpisů. Ochranu objektu dále upřesňují vnitřní směrnice rozsáhlého vojenského objektu.

Rozkaz neřeší problematiku zajišťování fyzické bezpečnosti u vojenského objektu, ve kterém se nachází zabezpečená nebo jednací oblast.

Ochrana objektu se zajišťuje ostrahou, režimovými opatřeními nebo technickými prostředky nebo jejich vhodnou kombinací. Velitel objektu zpracuje návrh na stanovení stupně ochrany objektu v souladu s požadavky, které vyplývají z tabulky (Tab. 1):

Tab. 1. Stanovení stupně ochrany objektu a minimální bezpečnostní opatření [6]

Stupeň ochrany objektu	**Minimální bezpečnostní opatření**	**Možnost zajišťovat fyzickou ochranu prostřednictvím dodavatele**
I.	technické prostředky	ANO
II.	technické prostředky nebo technické prostředky a fyzická ochrana zaměstnancem	ANO
III.	technické prostředky a fyzická ochrana zaměstnancem	ANO
IV.	technické prostředky a fyzická ochrana, kterou zajišťují příslušníci Armády České Republiky	NE

Příklad zařazení vojenského objektu do stupně ochrany objektu bez přihlédnutí ke specifickým podmínkám a charakteru objektu [6]:

I. stupeň - bytové domy, zabezpečené úkryty apod.,
II. stupeň - ubytovny, objekty technické podpory, objekty vyřazené z užívání apod.,
III. stupeň - administrativní budovy, sklady matriálu, výcviková zařízení apod.,
IV. stupeň - sklady zbraní a munice, objekty komunikačních uzlů, bojová stanoviště apod.

Fyzická ostraha musí zajistit kontrolu oprávněnosti vstupu osob a vjezdu vozidel do areálu v rámci režimových opatření a kontrolu vnášení (vynášení), dovážení (vyvážení) vyspecifikovaného materiálu. Ochranu objektu lze provádět vlastními silami z řad vojáků nebo prostřednictvím dodavatele. Při výběru dodavatele je nutno dbát na to, aby jeho zaměstnanci, kteří budou určeni k ochraně objektu, splňovali podmínku bezúhonnosti, zdravotní způsobilosti, fyzické a psychické odolnosti, státního občanství České republiky,

věkové hranice 21 let a více a podle konkrétních podmínek také odborné kvalifikace (např. držitel řidičského průkazu, zbrojního průkazu, odbornost k používání technických prostředků nebo osvědčení fyzické osoby). [6] Systém ochrany objektu lidskou silou se prolíná se systémem režimové ochrany.

Režimová ochrana definuje soubor administrativních a organizačních opatření k zajištění požadovaných podmínek pro funkci zabezpečovacího systému. Prakticky se s nimi lze setkat ve formě směrnic nebo doporučení, na základě kterých se mohou například vydávat vstupní propustky, provádět časová omezení přístupu do areálu nebo střeženého prostoru [10]. Režimová opatření lze rozdělit na vnější a vnitřní. Jak vyplývá z jejich názvu, pravidla charakterizují nutná opatření pro externí a interní režim zabezpečení.

Podle rozkazu jsou stanoveny požadavky na režimovou ochranu vojenského objektu takto [6]:

a) musí být číselně označeny budovy, vchody a další místa, důležitá z hlediska ochrany objektu,
b) všechny vstupy do budov musí být ve funkčním stavu,
c) na vstupy do budov musí být umístěna označení s údajem, která osoba odpovídá za jejich ochranu,
d) u nepoužívaných objektů musí být provedena opatření proti neoprávněnému vstupu – zabezpečeno jejich uzamčení a uzavření oken, zazdění (uzavření prkny) vybouraných otvorů, u poškozeného oplocení nutno provést úpravy proti možnému vniknutí,
e) musí být zpracován plán kontroly vojenského objektu a postupy při zjištění narušení ochrany objektu.

Dále lze vstupovat do vojenského objektu na základě:

- stálého oprávnění, které se přiděluje zaměstnanci, který má ve vojenském objektu pracoviště pravidelného výkonu práce,
- prozatímního oprávnění, které se přiděluje osobě, která potřebuje vstupovat do vojenského objektu dočasně,
- jednorázového oprávnění, které se přiděluje osobě pro jednorázový vstup.

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). Pro efektivní aplikování prostředků ochrany v objektu je nutné klasifikovat správné prostředí, ve kterém se prvky technické bezpečnosti podle normy ČSN EN 50 131-1 nacházejí a odhadnout možnou míru rizika, kterou pachatelé způsobí narušením objektu. Pro přehlednost jsou výše jmenované normy uvedeny v tabulkách pod tímto textem i se stručným popisem. Podmínky pro systémy kontroly a řízení vstupu jsou popsány v normě ČSN EN 50 133-1.

Tab. 2. Stupně zabezpečení dle ČSN EN 50 131-1 [7]

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.

Tab. 3. Bezpečnostní třídy dle ČSN P ENV 1627 [8]

Bezpečnostní třída	**Způsob napadení**
1	Příležitostný zloděj zkouší rozbít okno, dveře nebo okenice užitím fyzického násilí např. kopáním, naražením ramenem, zdviháním, vytrháváním.
2	Příležitostný zloděj dále zkouší rozbít okno, dveře nebo okenice užitím jednoduchých nástrojů, např. šroubováku a páčidla.
3	Zloděj zkouší zajistit přístup použitím dalšího šroubováku a páčidla.
4	Zkušený zloděj dále používá pily, kladiva, sekery, sekáče a přenosné akumulátorové vrtačky.
5	Zkušený zloděj dále používá elektrické nářadí, např. vrtačku, přímočarou pilu, úhlovou brusku o průměru kotouče maximálně 125 mm.
6	Zkušený zloděj dále používá výkonné elektrické nářadí např. vrtačku, přímočarou pilu a úhlovou brusku o průměru kotouče maximálně 230 mm.

Tab. 4. Klasifikace prostředí dle normy ČSN EN 50 131-1 [11]

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.

Požadavky na zabezpečení chráněných prostorů v rámci fyzické bezpečnosti, ve kterých se nachází zabezpečené oblasti k projednávání a ukládání utajovaných informací, definuje zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti 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 č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti 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.

Ochrana vojenského objektu, kterou řeší RMO č. 6/2009, o ochraně vojenského objektu, v souladu se zákonem č. 219/2000 Sb., o majetku České republiky a jejím vystupování v právních vztazích a zákonem č. 222/1999 Sb., o zajišťování obrany České republiky, se týká zajišťování fyzické bezpečnosti u vojenského objektu, ve kterém se nenachází zabezpečená nebo jednací oblast.

2 SPECIFIKACE VOJENSKÉHO VÝCVIKOVÉHO ZAŘÍZENÍ

2.1 Určení, funkce a prostorová dispozice speciálního pracoviště

Speciální výcvikové zařízení (dále jen „SVZ“) je výcvikovým pracovištěm Ministerstva obrany ČR s celoarmádní působností. Vzniklo v roce 2003 jako výsledek zavádění simulační a trenažérové techniky pro zvýšení efektivnosti přípravy vojenských profesionálů AČR.

SVZ je určeno k přípravě velitelů a štábů do stupně brigáda (včetně štábů krizového řízení) s využitím konstruktivní simulace[1] a zabezpečení výcviku velitelů a jednotek do stupně rota, výcviku osádek bojových vozidel a vybraných odborností dělostřelectva prostřednictvím virtuální[2] a živé simulace[3].

Vzhledem k tomu, že SVZ je špičkovým a jedinečným pracovištěm v AČR, je jeho posláním naplnit velkou a poměrně rozmanitou škálu činností a požadavků.

Proto jsou i funkce SVZ zaměřeny a rozděleny do tří oblastí.

1. Všeobecné povinnosti SVZ v oblasti výcviku jsou zaměřeny na:

- plnění výcvikových úkolů ve prospěch sil AČR a sil jiných organizací státní správy, odpovědných za obranu v ČR a za oblast krizového řízení,
- přípravu velitelů a štábu s využitím simulačních technologií,
- počítačovou podporu štábů taktických celků AČR nebo armád jiných států prováděných zdokonalovacími metodami výcviku,
- počítačovou podporu cvičení štábů krizového managementu,
- výcvik velitelů, jednotek a obsluh v řízení palby dělostřelectvem,

---

[1] 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.

[2] Virtuální simulace je pro potřeby této práce chápána jako výcviková simulace využívající speciální technická zařízení, která představují věrné nebo určitým způsobem redukované modely skutečných bojových vozidel a prostředků (tanků, bojových vozidel, transportérů, letadel, vrtulníků apod.) a pomocí kterých jsou osádky bojových vozidel a prostředků cvičen v jejich obsluze, v střelecké,řidičské taktické přípravě.

[3] Živá simulace je pro potřeby této práce chápána jako výcviková simulace polního výcviku vojsk, ve které jsou využívány skutečné zbraně, zbraňové a bojové systémy. Palba z těchto zbraní a systému je simulována cvičnou municí a signalizačními prostředky, ale účinek zbraně na cíl je simulován laserovým paprskem.

- výcvik řidičů bojových vozidel na virtuálních simulátorech,
- výcvik střelců (operátorů) bojových vozidel,
- výcvik jednotek a osádek v taktické a střelecké přípravě.

2. Všeobecné povinnosti v oblasti koncepce a rozvoje SVZ jsou zaměřeny na:
   - plnění akvizičních úkolů souvisejících s plánovaným zaváděním nových bojových nebo jiných prostředků do AČR,
   - sledování poznatků a zkušeností z praxe vojsk a jejich uplatňování ve své činnosti,
   - trvalý rozvoj simulačních a podpůrných systémů zavedených nebo zaváděných do AČR.
3. Všeobecné povinnosti v oblasti vědy, výzkumu a specifické činnosti jsou zaměřeny na:
   - uskutečňování aplikovaného výzkumu v oblasti konstruktivní, virtuální a živé simulace a využití výsledků výzkumu k výcviku vojáků a jiných osob,
   - šíření nových poznatků vědeckého výzkumu, pedagogických a výcvikových činností účastí jeho zaměstnanců na odborných konferencích a seminářích v ČR i v zahraničí a jejich organizování v ČR.

Speciální výcvikové zařízení je takticko - technologicky a organizačně sestaveno tak, aby bylo schopno plnit úkoly, specifikované k zajištění přípravy vojenských profesionálů. Skládá se ze dvou oddělení.

2.1.1 Oddělení 1

Oddělení 1 (dále jen O1) je vybaveno soupravami osobních počítačů, vzájemně propojenými do sítě, s nainstalovanými simulačními programy, které tvoří základ k provádění cvičení pomocí konstruktivní simulace. Řízení výcviku je prováděno pomocí pracovních stanic ovládaných operátory, na kterých jsou provozovány tyto výcvikové prostředky:

- taktický simulátor, umožňující vytvářet libovolnou taktickou situaci,
- záznamové zařízení, umožňující záznam veškeré činnosti cvičících včetně hlasové komunikace,
- systém pro ovládání virtuálních simulátorů, které je umožněno umísťovat před cvičením i v jeho průběhu do požadovaného prostoru operace, který umožňuje podle

požadavků cvičících „doplňovat“ simulátory střelivem a PHM, „opravovat“ jejich poškození nebo je „obnovovat“ po zničení,

- projekční systém sestávající ze dvou datových projektorů a pláten pro projekci 2D[4] a 3D[5] pohledů na virtuálního bojiště,
- komunikační systém, umožňující simulované rádiové propojení mezi cvičícími a operátory simulačního systému a včetně spojení pro tzv. rozehru,
- komunikační zařízení (interkom), umožňující řídícímu cvičení vydávat hlasové pokyny do všech místností O1.

Speciální výcvikové zařízení využívá k přípravě vojenských profesionálů virtuální simulátory dvou kvalitativních typů. Jsou tzv. simulátory označované jako VS-I a simulátory VS-II. Simulátory VS-I představují tzv. „full mission“ virtuální simulátory. To znamená, že to jsou tzv. „věrné kopie“ skutečných bojových nebo jiných prostředků a systémů. Chování, vlastnosti a ovládání simulátoru jakož i umístění, tvar, vnější projev ovládačů, přepínačů a signalizačních prvků v něm instalovaných odpovídají skutečným ovládacím a signalizačním prvkům reálného vozidla. Vnitřní prostor simulátoru je téměř identický s vnitřním prostorem skutečné bojové techniky. Uvedené simulátory jsou umístěny na pohyblivých plošinách k simulaci pohybu vozidla při jízdě v terénu.

Simulátory VS-II představují zjednodušené verze modelů bojových a jiných vozidel. Konstrukce simulátoru umožňuje tzv. rekonfiguraci. Většinu virtuálních simulátorů VS-II lze nakonfigurovat na modifikace T-72M4Cz, BVP-2, T-72M, Mi-24, Mi-17. Jedinečným simulátorem VS-II je simulátor pro provoz lehkého pozorovacího systému LOS a simulátory sesednuté pěchoty. Simulátory jsou ovládány běžnými periferními zařízeními typu COTS[6] (joystick, monitor, klávesnice, volant, pedály a řadicí páka). Na monitoru simulátoru se cvičícímu zobrazují nejdůležitější signalizační a ovládací prvky (přepínače, vypínače apod.), provozní hodnoty vozidla a výhled do virtuálního prostředí. Taktéž jsou všechny simulátory vybaveny komunikačním systémem.

---

[4] 2D – dvojdimenzionální pohled na „bojiště“ (v tomto případě pohled na umístění a stav objektů na mapovém podkladu)

[5] 3D – trojdimenzionální pohled na „bojiště“ (v tomto případě pohled na umístění a stav objektů v syntetickém provozu zobrazujícím skutečný nebo hypotetický terén)

[6] COTS – Commertial Off The Self (komerční výrobky určené k prodeji,pronájmu nebo licencovanému využití)

Uvedené virtuální simulátory jsou vzájemně propojeny do společného syntetického prostředí.

Propojení prostředků konstruktivní simulace s virtuálními simulátory umožňuje provádět plnohodnotný výcvik mechanizovaných a tankových jednotek až do stupně rota. K výcviku dělostřeleckých jednotek využívá O1 odbornou učebnu jako komplex osobních počítačů s nainstalovaným simulačním programem, s trenažéry průzkumných kombinovaných souprav předsunutých dělostřeleckých pozorovatelů a trenažéry taktických počítačů, které jsou základním prvkem automatizovaného systému řízení palby dělostřeleckého oddílu.

2.1.2 Oddělení 2

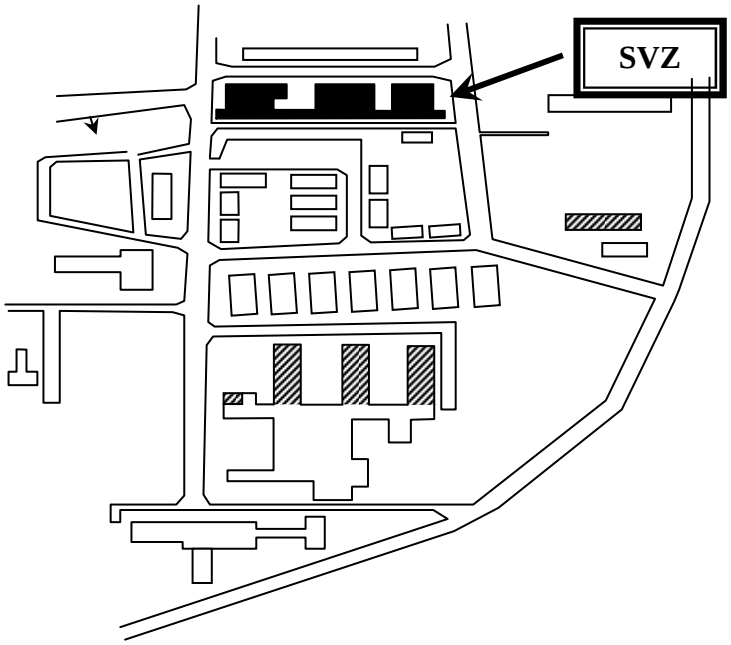
Oddělení 2 (dále jen „O2“) zabezpečuje zejména cvičení v polních podmínkách s využitím prostředků živé simulace. Oddělení podporuje polní cvičení soubojovým simulátorem MILES. Do struktury oddělení je zařazeno také Univerzální cvičiště jízdy tanku pod vodou.

Soubojový simulátor MILES umožňuje provádění soupeřských cvičení jednotek v taktické přípravě. Jedná se o soupravu laserových vysílačů a přijímačů. Vysílače se umisťují na reálné pěchotní a vozidlové zbraně. Přijímače se umisťují na trupy, helmy a techniku cvičících. Pokud přijímač zachytí laserový paprsek, indikuje zásah a podle stanovených algoritmů je vojákovi signalizována (zvukově i opticky) míra zranění nebo usmrcení a u techniky ztrátu vybraných schopností (mobility, palební schopnosti) nebo zničení. Kromě výcviku vojsk AČR, oddělení O2 provádí a zabezpečuje i cvičení pro složky silových ministerstev ČR, např. přípravu specialistů pro potlačování (řešení úkolů) davového odporu, řešení úkolů spojených s bojem proti terorismu, výcvik speciálních jednotek a vojenské policie a výcvik specialistů individuální likvidace vybraných osob (ostřelovačů).

Univerzální cvičiště jízdy tanku pod vodou je určeno k výcviku osádek tanků pro nácvik vybraných činností před skutečnou jízdou tanku pod vodou. Využívá se také k výcviku potápěčů a k výcviku potápěčů záchranářů. Pracoviště je vybaveno bazénem o průměru 4 m a výškou vodního sloupce 4 m a tlakovou komorou. Cvičící vojáci metodicky procvičují činnost při zatopení vozidlového prostoru, nouzovém opuštění tanku a základní použití potápěčské výbavy.

2.1.3 Prostorová dispozice

Jednotlivá pracoviště speciálního výcvikového zařízení jsou dislokována v samostatné budově rozlehlého vojenského areálu, nacházejícího se na kopci na periferii města. Areál je ohrazený plotem, má vlastní síť komunikací, uvnitř se nachází další samostatné subjekty, včetně budovy SVZ. Umístění objektu v areálu je patrné z Obr. 1:



Obr. 1. Prostorové umístění SVZ

V okolí budovy se nachází rozlehlé parkoviště, sklady a sportovní areál. Budova SVZ s jednoduchým tvarem v podobě písmene E a rovnou střechou stojí z části na nezpevněném pískovém podloží. V samotném objektu, který je jednopodlažní, je dislokován další samostatný organizační celek. Ten využívá část kanceláří a hal v objektu.

Z hlediska fyzické bezpečnosti můžeme SVZ označit jako rozsáhlou budovu v komplexu ohraničeného vojenského areálu, která má určitou rozlohu a uvnitř moderní systémy, určené ke vzdělávání a výcviku vojáků.

Právě duševní vlastnictví těchto moderních systémů, které je ohodnoceno na stovky miliónů korun, vede k nutnosti analyzovat kvalitu zajištění ochrany majetku, kterou se zabývám ve své práci. Ve své práci nebudu provádět analýzu stávajícího zabezpečení a návrh modernizace zabezpečení určených oblastí z pohledu utajovaných informací podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. Zaměřím se na analýzu a modernizaci z pohledu ochrany jedinečného aktiva, jehož

nekorektní funkčnost z důvodu škody způsobené ztrátou či zničením majetku by měla vliv na provázanost výcviku jednotek v AČR a také by způsobila problémy při plnění závazků, spojených s připraveností vojáků při vysílání do mírových operací.

Objekt SVZ, nacházející se v rozlehlém vojenském areálu, má v podstatě uspořádání jako objekt v objektu se stejným stupněm zabezpečení, což pro samotné zařízení neskýtá dostatečný způsob ochrany. Jelikož není SVZ schopno si vlastními silami objekt zabezpečit, řídí se v rámci fyzické a režimové ochrany směrnicemi pro zabezpečení vojenského areálu a další ochrana je zajišťována technickými prostředky.

II. PRAKTICKÁ ČÁST

3 ANALÝZA SYSTÉMU FYZICKÉ BEZPEČNOSTI SVZ

Hlavní součástí bezpečnostní analýzy je vyhledání rizik. Cílem je identifikovat problémy, které mohou vzniknout jak v objektu, tak přímo v provozu nebo technice. Nejprve se zjišťuje situace v objektu a přilehlém okolí, podle výsledku se stanoví taktické řešení, technické řešení pro zabezpečení a způsob provedení mechanické či elektrické ochrany. [8]

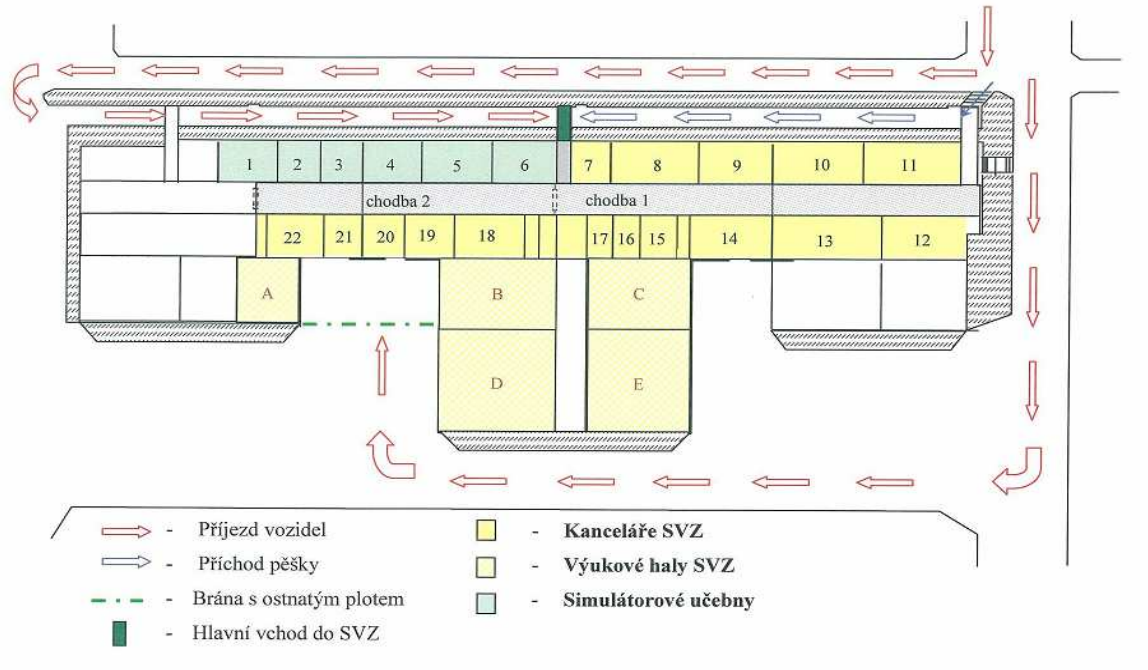
Stěžejním řešením zabezpečení každé organizace je její bezpečnostní politika. Jde o souhrn řídících a organizačních pokynů, pravidel, norem, nařízení, specifických bezpečnostních požadavků organizace, jejichž cílem je ochránit organizaci proti vloupání, rozkrádání, ale i jiným nekriminálním jevům ohrožujícím stabilní provoz organizace, jako jsou havárie, požáry, výpadky provozu, nedbalost, nepozornost pracovníků a podobně.

Přístup do objektů je řízený pravidly bezpečnostní politiky, kterou lze naplňovat pouze komplexními přístupy, jež jsou zahrnuty v kombinaci fyzické a technické ochrany.

U SVZ není bezpečnostní politika explicitně řešena, je pouze částečně zakomponována v provozním řádu zařízení v podobě bezpečnostních opatření.

Objekt SVZ lze zařadit dle RMO č. 6/2009, o ochraně vojenského objektu, do III. stupně ochrany. Minimální bezpečnostní opatření, související s tímto stupněm ochrany, jsou technické prostředky a fyzická ochrana, a to poskytovaná i prostřednictvím dodavatele.

V objektu SVZ je bezpečnost zajišťována fyzickou ochranou, režimovými opatřeními a technickými prostředky, a to poplachovým zabezpečovacím systémem (dále jen „PZS“) a elektronickou kontrolou vstupu (dále jen „EKV“).
Rozmístění prostorů SVZ a jeho ohraničení je patrné z následujícího obrázku (Obr. 2.):



Obr. 2. Rozmístění prostorů SVZ v objektu

3.1 Fyzická ochrana

Fyzická ochrana objektu SVZ je prováděna živou silou. Tvoří ji vojáci z povolání (dále jen VZP), kteří jsou k výkonu posádkové směny určeni a poučeni v souladu s vnitřní směrnicí velitele posádky, která vychází z předpisu Zákl-1.

SVZ je z hlediska fyzické ochrany zajištěno pravidelnými obchůzkami příslušníky posádkové směny a střeženo připojením poplachového zabezpečovacího systému na poplachové přijímací centrum, umístěného v prostoru operačního dozorčího[7], který zastřešuje činnost posádkové směny. Pokud shledá příslušník ostrahy při obchůzce narušení objektu, uvědomí telefonicky vyčleněné pracovníky SVZ o vzniklé události a ti pak dále řeší situaci prostřednictvím vojenské, popřípadě státní policie.

Tato bezpečnostní opatření jsou dostačující pro tento typ ochrany a objektu.

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

3.2 Režimová opatření

Tato opatření jsou administrativně organizační a prolínají se s fyzickou ochranou. Jsou platná pro všechny osoby, které se pohybují oprávněně v objektu.

Každá osoba, vstupující do vojenského areálu a následně na pracoviště SVZ, 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.

SVZ disponuje pro podporu režimové ochrany přístupovým systémem. Vstupní terminál není u hlavního vchodu instalován, pouze jsou v prostoru *chodby 2 (Obr. 2)* z obou stran umístěny elektronické snímače pro identifikaci osob.

Každý návštěvník (externí zaměstnanec, servisní pracovník, kontrola) vstupuje/vjíždí do prostorů SVZ na základě podané žádosti a povolení vedoucího pracovníka bez identifikačních médií, ale s doprovodem příslušníka SVZ. Žádost 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 SVZ se lze pohybovat pouze v pracovní době, v době mimopracovní na základě oznámení vedoucímu pracoviště.

Pracoviště SVZ je opatřeno PZS, na základě čehož první pracovník při příchodu do zaměstnání odstřeží objekt a poslední pracovník při odchodu z objektu jej zastřeží společným identifikačním kódem. Pomocí tohoto kroku je operační dozorčí informován o stavu zabezpečení na pracovišti.

V celém vojenském areálu, jakožto v prostorách SVZ, je zakázáno pořizování fotografií.

Z hlediska funkčnosti systému režimových opatření a bezpečnosti spatřuji závažné problémy především v nedostačující kontrole pohybu osob (cvičících jednotek, návštěvníků, technických pracovníků) na pracovišti a to především z důvodu možných krádeží a průmyslové špionáže (především zahraniční návštěvníci). Dalším problémem je

nekompatibilita přístupového systému SVZ a přístupového systému, který je umístěný u hlavního vchodu do vojenského areálu, což má za následek velké množství vstupních prvků do jednotlivých prostorů (klíče, karty).

3.3 Mechanické zábranné prostředky

Mechanické zábranné systémy se používají jako obvodová ochrana pro bezpečnost kolem chráněného objektu. Plášťová ochrana pro vstupní jednotky (okna a dveře), předmětová ochrana zabezpečuje prostory nebo úschovná místa. [9]

Obvodová ochrana je v objektu řešena mezi halami A a B (Obr. 2), kde jsou ostatní prostory areálu odděleny od nádvoří SVZ plotem o délce 29 m a výšce 2 m a vrcholovou ochranu tvoří žiletkový plot, uchycený na „V“ úchytu na horní straně plotu proti přelezení překážky. Oplocení je doplněno jednou dvoukřídlou bránou šířky 4 m, výšky 2 m a jednou jednokřídlovou brankou šířky 1 m a výšky 2 m s jednou řadou žiletkového plotu. Tento oplocený prostor se využívá jako jediný vjezd pro vozidla do objektu. Křídlo brány je osazeno kováním koule – klika. Stávající oplocení pro vjezd vozidel je dostačující, nedostatek vyplývá z použitého zámkového systému, kde by bylo vhodné použít bezpečnostní zámkový systém a jeho prvek v podobě cylindrické vložky bezpečnostního stupně 3, popřípadě doplnit zajištění pomocí bezpečnostního visacího zámku, který by měl být odolný proti přeřezání, přestřižení, vytržení a odvrtání třmenu a tělesa zámku. Také se jeví vhodným řešením oplocení celého objektu SVZ bezpečnostním plotem jako v případě prostoru mezi halami A a B.

Vstup do objektu je možný třemi vchody. Hlavní vstupní dveře jsou celokovové s prosklením, opatřeny běžným dveřním kováním s bezpečnostním zámkem. Zbývají dva vchody se shodným typem dveří a obyčejným dveřním systémem. Toto vybavení je nedostačující vzhledem k možnosti vloupání se pachatele rozbitím skleněné dveřní výplně nebo vypáčení či odvrtání zámku. Možným řešením problému je záměna stávajících dveří za bezpečnostní včetně zámkového systému a jeho prvku, jímž je bezpečnostní cylindrická vložka nebo lépe nahrazení klíčového systému systémem přístupovým.

Samotná budova SVZ a její střešní část je tvořena panelovými díly a povrch střechy je pokrytý plechem. Po celé střeše jsou zabudovány kopulové světlíky, které slouží k jejímu prosvětlení. Vlivem povětrnostních podmínek se ve střeše vytváří trhliny a místy zatéká

dovnitř, i přes světlíky. To může způsobovat falešné poplachy poplachového zabezpečovacího systému v místech, kde je prostor chráněný jeho detektory. Problém lze řešit stavebními opravami střešní pokrývky a světlíků.

Ve vnitřních prostorech objektu jsou na obou vstupech do *chodby 2* pracoviště se simulátory osazeny 2x bezpečnostní dveře šířky 1 m, certifikované NBÚ. Bezpečnostní dveře jsou zakotveny do vlastního certifikovaného rámu a opatřeny samozavírači. Výše uvedený prostor je zabezpečený dostatečně.

3.4 Poplachový zabezpečovací systém

Poplachový zabezpečovací systém sestává z několika funkčně propojených částí. Na určených místech a v určených prostorách jsou instalovány jednotlivé detektory, a to podle toho, zda slouží k plášťové, prostorové nebo předmětové ochraně. Ty identifikují poplachové podněty, kterými může být pohyb osoby ve střeženém prostoru, destrukce skla, otevření dveří, oken a pod. Informace, která vzniká na výstupu, je pak vyhodnocována ústřednou PZS. Ta zajistí zpracování informace a následnou aktivaci výstupních obvodů (lokální opticko – akustická signalizace, signalizace narušení v místě trvalé obsluhy, spuštění kamerového systému apod.). Poplachový výstup může být dále přenesen prostřednictvím telefonní linky nebo bezdrátového zařízení dálkového přenosu na monitorovací bezpečnostní systém policie nebo bezpečnostní agentury.

3.4.1 Ústředna PZS

Zabezpečovací ústředna Advisor CD 150 od firmy Aritech je srdcem PZS. Obsahuje 16 programovatelných výstupních smyček a ty jsou rozšiřitelné na max. 148 smyček, a to použitím vnitřního expandéru, externích klávesnic nebo externích expandérů.

K ústředně je možné připojit maximálně 16 externích zařízení (klávesnic a expandérů), která mohou být volně naprogramována na 18 různých typů: poplach, samoochrana, tíseň, požár, vstupní/výstupní smyčka, technická smyčka a další. Klávesnice má programovatelný výstup, který může být naprogramován na 30 různých typů: vnitřní siréna, spínač vnějšího osvětlení, spouštění telefonního komunikátoru, řízení paměti detektorů, apod.

Poplachové smyčky mohou být rozděleny do samostatného systému nebo do společné oblasti.

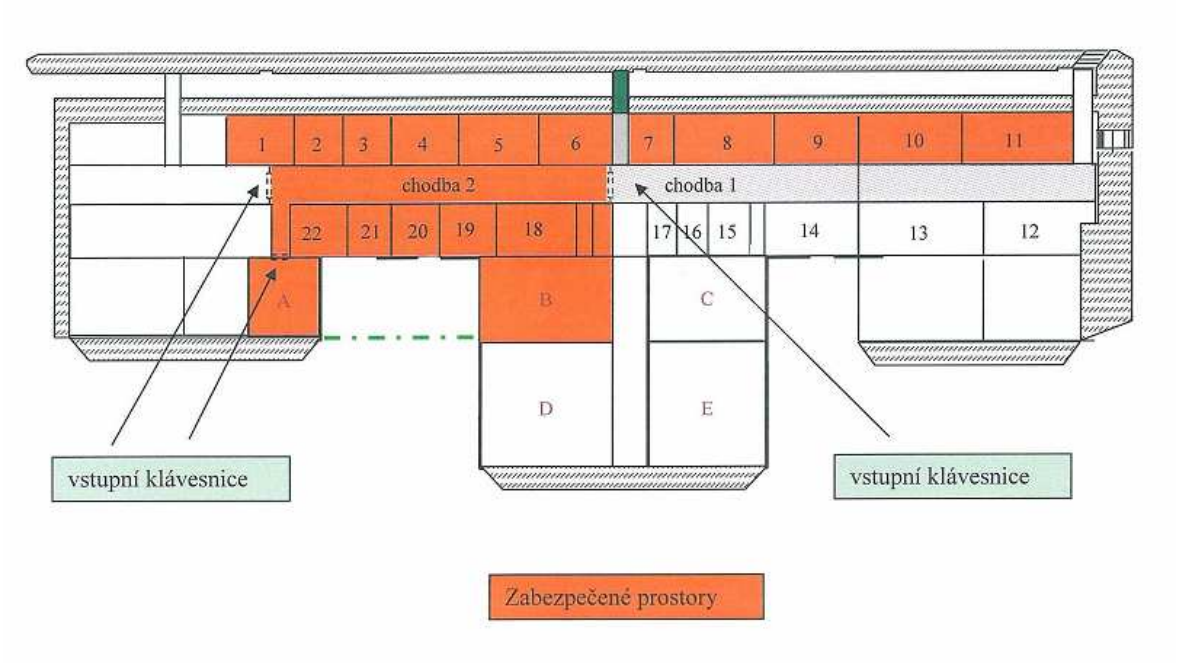
Technické parametry ústředny Advisor CD 150:

- až 50 výstupů,
- max. 16 externích zařízení (klávesnic, expandérů), připojených na 4 vodičové sběrnici,
- max. 100 uživatelských kódů, 4-6 místních,
- paměť 1000 událostí s časem a datem,
- možnost připojení tiskárny přes sériové rozhraní RS 232,
- paměťová karta pro uchování a přenos nastavení ústředny,
- 31 nezávislých časovačů,
- programovatelná volba poplachu i samoobsluhy v jedné smyčce (duální smyčky),
- napájecí napětí: primární 220/240 V / 66 VA, sekundární 18 V,
- napájení výstupních zařízení: 13,7 V VSS/1 A.

Ústředna je v objektu SVZ nainstalována v místnosti č. 18 v horní polovině stěny. Do tohoto místa je přivedeno samostatně jištěné a přepěťově chráněné napájecí vedení z hlavního rozvaděče NN, datová linka a napájecí vedení od koncentrátorů a klávesnic. Dále je do ústředny přivedeno vedení od detektorů, zapojených přímo na smyčkách ústředny. Koncentrátory jsou rozmístěny ve vybraných prostorách v jednotné výšce 2,2 m.

Vstupní klávesnice slouží pro 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.

V objektu SVZ je základní deska ústředny rozdělena do 8 zón a ovládána pomocí tří klávesnic. Klávesnice KL/1 a KL/3 jsou umístěny na *chodbě 2*, klávesnice KL/2 v hale A Obr. 3).



Obr. 3. Zabezpečené prostory SVZ

Ústřednový zdroj 1A je doplněn bezúdržbovým akumulátorem 12 V / 7 Ah. Pro napájení rozvodů je pod ústřednou umístěn přídavný zdroj se záložním akumulátorem 12 V / 40 A. Záložní zdroj zajišťuje po přerušení napájení ze základního zdroje ústředny provoz zařízení minimálně 16 hod. v pohotovostním stavu, z toho 15 min ve stavu poplachu, je-li výpadek signalizován v místě operačního dozorčího.

Přístup do místnosti č. 18 s ústřednou je řešen pomocí kódového zámku, dveře jsou opatřeny elektronickými zámky a samozavírači.

Signál z ústředny je vyveden optickou a akustickou signalizací na klávesnicích systému a hlasová zpráva je přenesena pomocí telefonního komunikátoru (Obr. 4) k operačnímu dozorčímu.

Obr. 4. Komunikátor

3.4.2 Prvky plášťové ochrany

Prvky plášťové ochrany slouží, jak už sám jejich název napovídá, k hlídání otevření, popř. destrukce prostupů pláště budovy (oken, dveří, vrat). [12]

Okna objektu SVZ jsou kastlová s běžným sklem bez přídavných mříží. Dveře pro vstup do budovy jsou běžné, prosklené bez mříží. Vstup do výukových hal je přes celokovová vrata.

Na vstupech do všech místností se vstupem z nechráněných prostor a na všech kovových oknech jsou umístěny magnetické kontakty DC 103. Závrtné magnetické kontakty MK 270 jsou umístěny na otevíratelných křídlech dřevěných oken. Na vratech hal jsou nainstalovány magnetické kontakty DC 108. Skla jsou chráněna duálními detektory tříštění skla FG 1025.

Duální detektor tříštění skla FG 1025

Duální detektor tříštění skla FG 1025 (Obr. 5) 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. FG 1025 se vyznačuje vysokou odolností vůči vysokofrekvenčnímu rušení. Jednotlivé detekce jsou indikovány LED diodami a poplachový signál přenášen přes výstupní relé.

Technické parametry detektoru tříštění skla:

- dosah rádius 7,6 m / otevřený prostor,
- frekvenční citlivost 4,1 – 16 kHz,
- amplitudová citlivost 74 dB / 5 kHz,
- napájecí napětí 10 – 14 V,
- odběr 25 mA / 12 V,
- provozní teplota -20 °C až +55 °C.

Obr. 5. FG 1025

V objektu SVZ je 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. Při eliminaci výše uvedeného jsou z hlediska ochrany prostoru detektory dostačující.

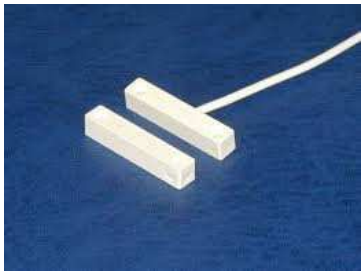
Magnetické kontakty

Magnetický kontakt je tvořen 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 DC 103 – příložný hranol (Obr. 6) a závrtného magnetického kontaktu MK 270 (Obr. 7) dojde k vyhlášení poplachu při vzájemné změně polohy spínače a ovládacího magnetu, tj. při otevření dveří nebo oken.

Technické parametry magnetických kontaktů DC 103 / MK 270:

- výstup na centrálu,
- pracovní vzdálenost max. 31 mm (min. 15 mm) / max. 25 mm,
- 4 vodiče,
- polarizovaný kontakt (DC 103).



Obr. 6. DC 103

Obr. 7. MK 270

Závrtné magnetické kontakty MK 270 jsou v objektu SVZ použity na oknech a magnetické kontakty DC 103 na dveřích do místností.

DC 108

Hliníkový magnetický kontakt DC 108 (Obr. 8) je použitý na vratech hal. K vyhlášení poplachu dojde při vzájemné změně polohy spínače a ovládacího magnetu.

Technické parametry magnetického kontaktu:

- výstup na centrálu,
- 4 vodiče,
- pracovní vzdálenost max. 75 mm.

Obr. 8. DC 108

Všechny výše zmíněné magnetické kontakty jsou vysoce spolehlivým zabezpečením, pokud je dostatečně zajištěna přiléhavost (uzavření) oken a dveří.

V rámci plášťové ochrany by bylo vhodné použití bezpečnostních dveří na vstupech do objektu, které budou opatřeny bezpečnostními zámky. Doplňkovým opatřením ve prospěch režimových opatření a fyzické ochrany by nadále zůstalo k zabezpečení dveří použití pečetě, kterou má každý zaměstnanec k dispozici.

3.4.3 Prvky prostorové ochrany

Těžištěm prostorové ochrany jsou centrální body budovy, tj. schodišťové přístupy či výstupy, haly, spojovací chodby a vnitřní komunikační uzly. [8]

Světlíky chodeb a hal v objektu SVZ jsou chráněny PIR detektory Aritech EV 455 AM, prostory chodeb PIR detektory CX 50 AM, kanceláře a učebny PIR detektory EX 35 T, prostory hal PIR detektory CX 70 M. Ve strojovnách vzduchotechniky jsou osazeny duální detektory DX 40 PLUS.

ARITECH EV 455 AM

Nejrozšířenějšími detektory pohybu jsou pasivní infračervené (dále je „IR“) detektory, jejichž funkce spočívá v zachycení pohybu objektu, jehož teplota se liší od teploty střeženého okolí.

Mezi tuto skupinu patří i Aritech EV 455 (Obr. 9). Jde o prostorový detektor pohybu s velmi přesnou zrcadlovou optikou. Díky ní je IR záření, vycházející ze snímaného prostředí, rozděleno na detekční zóny a pomocí odrazu nebo lomu infračerveného paprsku přivedeno na senzor detektoru, který je citlivý na IR záření. Tím dojde k jeho rozžhavení a vzniku povrchového elektrického náboje, který elektronika zesílí a při dostatečné úrovni vyhodnotí jako poplach.

Technické parametry detektoru pohybu:

- napájecí napětí: 8 – 15 V, maximální špičky 2 V při 12 V,
- spotřeba proudu: 6 mA klidová, 18 mA poplachová,
- pokrytí prostoru: IR 1 záclona 25 m, prostorová 9 záclon do 15 m,

- dosah: 1 záclona 25 m,
- úhel pokrytí: 4° (dlouhý dosah),
- paměť poplachu, antimasking,
- rozsah pracovních teplot: -10 °C až +50 °C,
- vlhkost vzduchu 90 %.

Obr. 9. Aritech EV 455

Uvedený detektor je v prostorách SVZ umístěný na chodbách a v halách. Zde je k úplnému pokrytí prostoru použito více detektorů tak, aby byla pokryta celá střežená plocha. Vícenásobné použití detektoru je bezpečné, protože ty se vzájemně neovlivňují a tudíž je jejich aplikace v prostorách SVZ plně vyhovující.

EX – 35T

Dalším použitým infračerveným detektorem je EX – 35T (Obr. 10) s duálním senzorem a se schopností detekce s velmi dobrou odolností vůči vysokofrekvenčnímu rušení v pásmu 100 MHz až 1 GHz. Kombinací otočné čočky a víceohniskové optiky (možnost sledování na více vzdáleností) se zónou snížení rizika falešných poplachů způsobených zvířaty umožňuje výběr jednoho ze čtyř obrazů pomocí jediné čočky. Lze jej umisťovat do rohu i na stěnu.

Technické parametry infračerveného detektoru:

- dosah: vějíř 12 m / 85°, dlouhý dosah 17 m otočením čočky o 180°,
- montážní výška 1,2 – 2,4 m,
- detekční rychlost 0,3 – 1,5 m/s,

- délka trvání poplachu – 2,5 s,
- napájecí napětí: 9,5 až 14 V DC,
- odběr: max. 18 mA / 12 V při vypnuté LED,
- rozsah pracovních teplot: -20 °C až +50 °C,
- vlhkost vzduchu 90 %,
- paměť poplachu.

Obr. 10. EX – 35 T

Tento detektor je v objektu SVZ umístěn ve většině kanceláří a v učebnách, je velmi spolehlivý, tudíž dostačující pro potřeby objektu.

CX 50AM, CX 70M

Následující dva detektory doplňují pokrytí velkých prostorů.

Infračervený dvojitě stíněný detektor firmy OPTEX CX 50AM (Obr. 11) s vějířem snímání scény 15 m / 85° získá dosah 24 m otočením čočky o 180°. Detektor má vestavěný antimasking. Lze jej nainstalovat na zeď i do rohu.

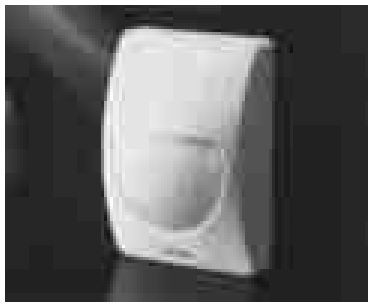
Detektor CX 70M (Obr. 12) se výborně uplatňuje při ochraně rozlehlých prostor. Infračervený dvojitě stíněný senzor, jehož dlouhý dosah 45 m se získá otočením čočky o 180°, má vějíř 21 m / 85°.

Technické parametry detektorů CX 50AM, CX 70M:

- montážní výška 1,5 – 3,6 m,
- LED dioda vypínatelná červená,
- napájecí napětí: 9,5 – 14 V DC,

- detekční rychlost 0,3 – 1,5 m/s,
- délka trvání poplachu – 2,5 s,
- napájecí napětí: 9,5 až 14 V DC,
- odběr: max. 42 mA / 12 V,
- rozsah pracovních teplot: -20 °C až +50 °C,
- vlhkost vzduchu 95 %,
- paměť poplachu.

Obr. 11. CX 50AM



Obr. 12. CX 70M

Výborných vlastností těchto detektorů je využito při zastřežení hal a chodeb v objektu SVZ. Jsou umístěny v rozích a doplňují tak IR detektor Aritech EV 455. Tato kombinace detektorů vyhovuje podmínkám pro zabezpečení rozsáhlých prostorů.

DX-40 PLUS

Do prostorů s obtížnými podmínkami a výrazným negativním vlivem okolního prostředí se využívají kombinované detektory, a to ve spojení PIR a ultrazvuk nebo PIR a mikrovlny

(dále jen „MW“). Dvojkombinace detektorů snižuje riziko vzniku poplachu vlivem změny prostředí.

Představitelem kombinovaných detektorů PIR – MW je duální detektor DX-40 PLUS (Obr. 13). Detektor snímá velmi ostře díky kulové čočce, která je mechanicky pevná především na okrajích a tudíž infračervené paprsky dopadají přesně do středu senzoru a tím nedochází k "deformaci" informace. Následně jsou vyhodnoceny všechny vstupní signály a detektor dokáže eliminovat falešné poplachy způsobené drobnými pohyby např. záclon, nebo vibracemi. Lze jej nainstalovat do rohu, na zeď i na držák. Jeho ochranu před zakrytím nebo zasprejováním tvoří funkce antimasking.

Technické parametry duálního detektoru:

- montážní výška 1,5 – 3,6 m,
- pracovní kmitočet MW části – 9 900/10 525 GHz,
- napájecí napětí: 9 – 18 V DC,
- detekční rychlost 0,3 – 1,5 m/s,
- dosah: vějíř – 12 x 12 m, 85°,
- délka trvání poplachu – 2 s,
- nastavitelná citlivost, paměť poplachu,
- odběr: 17 mA (normál), max. 40 mA / 12 V,
- rozsah pracovních teplot: -10 °C až +50 °C,
- vlhkost vzduchu 95 %.

Obr. 13. DX-40 PLUS

Vlastností detektoru je v prostorách SVZ využito v místnostech se vzduchotechnikou, což poskytuje dostačující ochranu uvedeného prostoru.

3.5 Přístupový systém

Přístupový systém umožňuje spolehlivé sledování, evidenci a řízení průchodů osob prostřednictvím specializovaných snímačů průchodu a přístupových mechanizmů, instalovaných v rámci systému jako celku. Základními stavebními prvky systému jsou speciální elektronické snímače, instalované v místech, kde je třeba monitorovat, evidovat a případně též řídit přístup osob v souladu s jejich oprávněním a bezpečnostní politikou.

Na základě načtení vnitřního kódu karty příslušným terminálem je bez ohledu na práva držitele karty vždy proveden záznam o této události do systému s potřebnými parametry (místo, čas atd.). Poté je na základě v systému uložených údajů ověřováno oprávnění držitele karty k povolení průchodu nebo vstupu do snímačem monitorované zóny.

Nejjednodušší schéma přístupového systému je znázorněno na Obr. 14., kde:

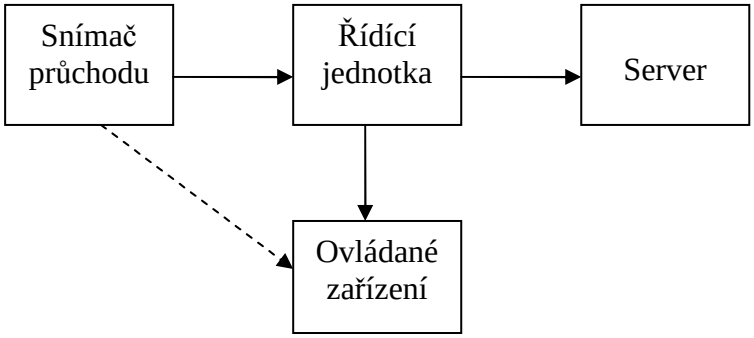
Snímač průchodu - systém snímání průchodu - skládá se z elektronických snímačů - terminálů, jejichž minimální funkcí je snímat průchod a řídit přístup, např. otevírat oblasti.

Řídící jednotka - slouží k přijetí kódu ze snímače průchodu, autentizaci osoby, porovnání s právy osob v paměti, otevření ovládaného zařízení a komunikaci se serverem.

Ovládané zařízení - je zařízení otevírající (příp. uzavírající) přístup do objektů.

Server - zařízení pro správu, monitorování a evidenci přístupových systémů.

Přístupový systém tvoří také technickou podporu pro režimovou ochranu.



Obr. 14. Principiální schéma přístupového systému

3.5.1 Systém Granta

Systém Granta je přístupový systém, schopný zpracovávat signály ze čtyř až 250-ti čtecích míst. Systémová charakteristika je jednoduchá.

Stručný systémový přehled :

- 256 čteček / 30 000 držitelů karet,
- 64 časových dělení,
- tříletý kalendář,
- denní záznamy,
- PIN kontrola a management, systémové monitorování,
- časový záznam zpráv,
- kontrola stavu,
- uživatelsky konfigurovatelné zobrazení údajů.

Systém Granta umožňuje osm přístupových míst a do sítě je připojen přes rozhraní RS 485. Pro čtení identifikačních karet systém používá bezkontaktní čtecí hlavy pro vnitřní i venkovní použití s dosahem 5 – 30 cm. Hlavice jsou zabudovány před ovládanými dveřmi. Elektrické zámky a uvolňovací tlačítka jsou připojena k řídící jednotce.

Speciální výcvikové zařízení je vybaveno elektronickou kontrolou vstupu GRANTA, které je součástí celkového řešení bezpečnosti. Přístupová část je řešena prostřednictvím bezkontaktních karet a příslušných čtecích hlav.

Řídící jednotka a zálohový napájecí zdroj jsou umístěny v místnosti č. 18. Zde je nainstalován také přídavný zdroj pro napájení kódových a elektrických zámků se záložním akumulátorem 12 V / 7 Ah. Použité čtecí hlavy, zajišťující čtení bezkontaktní karty a její vyhodnocení, jsou rozmístěny jednostranně u vstupních dveří na *chodbu 2* a oboustranně na vstupu do haly A. Pro odchod jsou na vnitřní straně dveří hlavní *chodby 2* umístěna odchodová tlačítka, ovládající elektronické zámky. Celý systém je zálohovaný na 5 – 6 hodin.

Při zvážení výše provedené analýzy zabezpečení objektu SVZ lze konstatovat, že ústřednová část poplachového zabezpečovacího systému a řídící část přístupového systému již z dnešního pohledu bezpečnostně, hardwarově ani softwarově neodpovídají nastoleným trendům v zajištění bezpečnosti objektu. V současné době se také ustupuje od používání ovládacích klávesnic a tento prostředek se nahrazuje systémem bezkontaktního čtení a následné identifikace.

Výčet konkrétních nedostatků fyzické bezpečnosti SVZ v návaznosti na předcházející analýzu:

1. Režimová ochrana:
   - nedostačující kontrola pohybu osob na pracovišti - krádeže, špionáž,
   - nekompatibilita přístupového systému SVZ a přístupového systému u hlavního vchodu do areálu - velké množství vstupních prvků do jednotlivých prostorů jak areálu, tak SVZ.
2. Mechanické zábranné prostředky:
   - oplocení - nedostatečné z pohledu zámkového systému - vloupání,
   - střecha a světlíky - zatékání - falešné poplachy PZS,
   - vstupní dveře - nevyhovující skleněná výplň a zámkový systém - vloupání,
3. Poplachový zabezpečovací systém:
   - ústřednová část - bezpečnostně, hardwarově ani softwarově nevyhovující,
   - ovládací klávesnice - hardwarově ani softwarově nevyhovující.
4. Přístupový systém:
   - bezpečnostně, hardwarově ani softwarově nevyhovující.

Naproti tomu vývoj v oblasti koncových prvků není natolik dynamický, aby bylo nutné koncové prvky zaměnit nebo modifikovat.

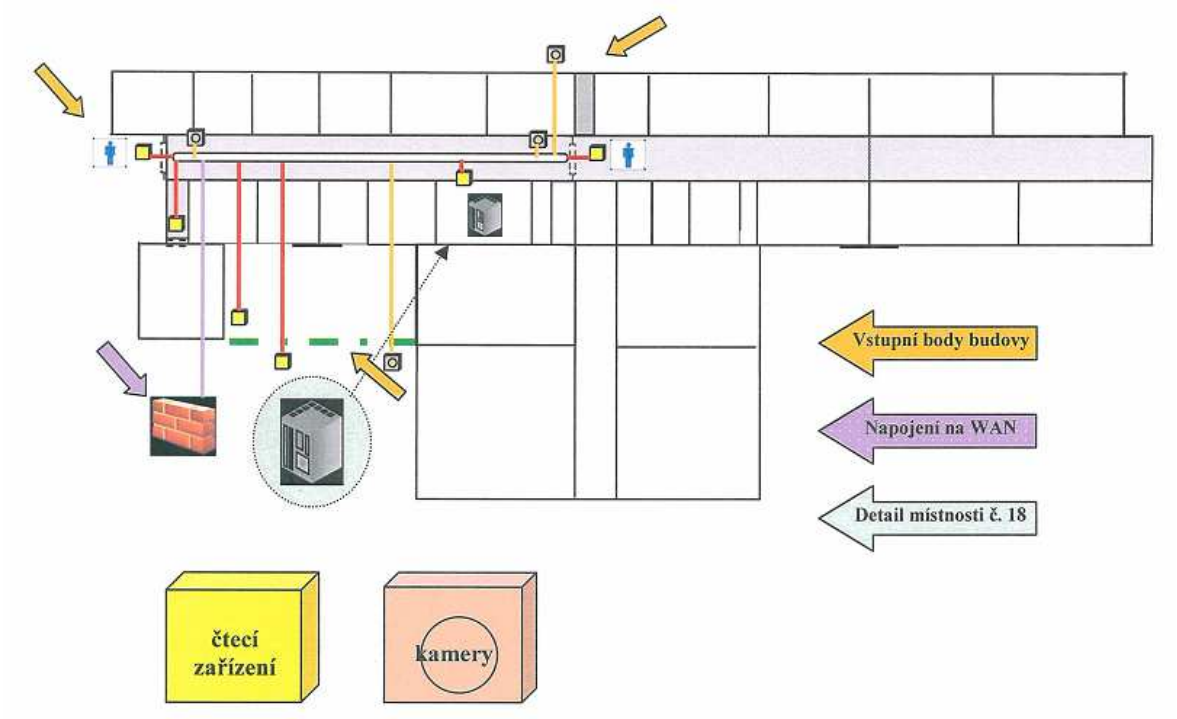
4 NÁVRH OPATŘENÍ KE ZLEPŠENÍ FYZICKÉ BEZPEČNOSTI SVZ

Hlavními prostředky zabezpečení speciálního vojenského zařízení jsou poplachový zabezpečovací systém a přístupový systém. Části těchto systémů jsou již zastaralé a nevyhovující, což navozuje myšlenku na jejich modernizaci.

Za účelem obnovy stávajícího systému se jako vhodné řešení jeví nahrazení řídících částí PZS a vstupního systému. Součástí modernizace by měla být výměna stávajících ovládacích klávesnic systému PZS za bezkontaktní čtecí body u vybraných místností.

Ústřední místnost s ústřednami PZS a vstupního systému, tj. místnost č. 18, by bylo nutné pro zvýšení bezpečnosti zajistit kontrolou vstupu v kombinaci prvků „karta + PIN kód“ a všechny jednotky propojit do místní sítě LAN a zajistit napojení na síť WAN. Jako účelové se jeví doplnění o přehledové kamery systému CCTV.

Na Obr. 15 je navržené řešení v rámci objektu znázorněno.



Obr. 15. Návrh řešení modernizace zabezpečení objektu SVZ

Možným komplexním technickým řešením modernizace SVZ je využití integrovaného bezpečnostního systému Xtralis 3000.

Tento systém sestává z několika základních částí, kde se každá orientuje na jednu z částí integrovaného zabezpečovacího systému. Jsou jimi poplachový zabezpečovací systém spolu s přístupovým systémem a kamerový dohledový systém. V komplexu pak části působí jako jeden celistvý systém, který je možné plně programovat a přizpůsobovat požadavkům uživatele.

Všechna zařízení systému S3000 jsou vzájemně propojena prostřednictvím datové sítě na bázi protokolu TCP/IP.

Lze vytvořit systém s teoreticky neomezeným počtem zařízení, který je limitován pouze volným adresným prostorem v datové síti. Pro uložení dat je využit otevřený databázový systém PostgreSQL, do kterého se ukládají všechna systémová data, tedy například údaje o přístupových kartách, bezpečnostních kódech, otiscích prstů a podobně. Díky velikosti této databáze lze ukládat statisíce údajů.

Prostřednictvím univerzálních vstupně/výstupních IP modulů mohou být do systému připojeny již instalované klasické zabezpečovací prvky přes svá rozhraní. Tím jsou sníženy náklady na instalaci tohoto systému.

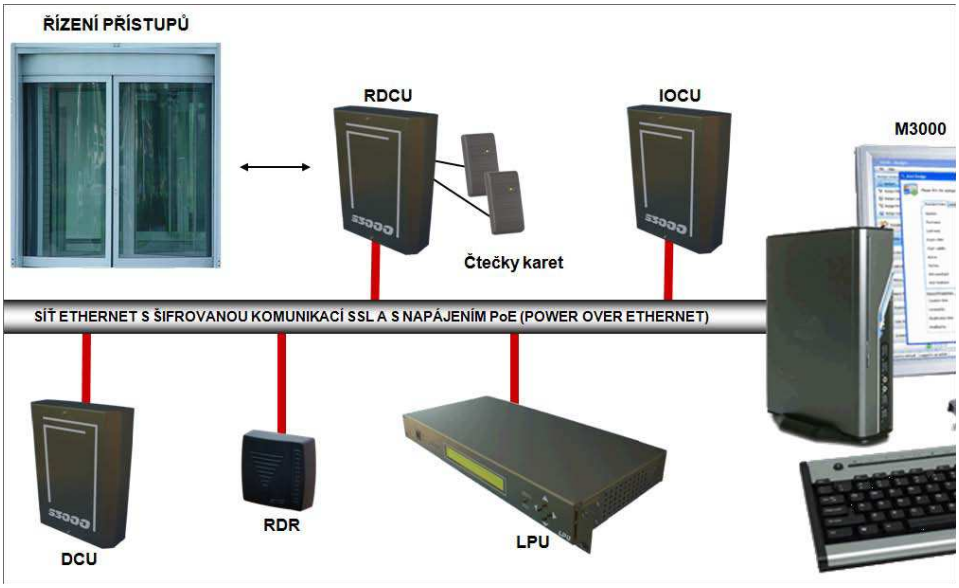
Xtralis 3000 se skládá z následujících částí:

- S3000 je PZS s přístupovým systémem (poplachový a zabezpečovací systém),
- V3000 je kamerový dohledový systém CCTV,
- M3000 je řídicí software, jenž ovládá všechny prvky Xtralis 3000. [13]

4.1 Prvky přístupového systému Xtralis 3000

Přístupový systém S3000 (Obr. 16) se skládá z níže uvedených prvků:

- Centrální ústředna LPU (Local Processing Unit),
- Dveřní IP jednotka DCU (Door Control Unit),
- Nástěnná IP čtečka RDR (Read Door Reader),
- Univerzální IP modul IOCU (Input/Output Control Unit),
- Dveřní IP jednotka RDCU (Reader Door Control Unit) s připojením 2 čteček karet přes rozhraní Wiegand.



Obr. 16. Systém řízení přístupů spolu s řídícím softwarem [13]

4.1.1 Centrální ústředna

Centrální řídicí ústředna (Obr. 17) je srdcem systému S3000. Softwarově ji řídí grafické rozhraní M3000. Ústředna má za úkol řídit a analyzovat data od podřízených jednotek, kontrolovat a ovládat dveřní jednotky a vést záznamy historie událostí. Základní nastavení a testování se zobrazuje na LCD displeji.

Pro připojení k síti Ethernet využívá LPU dva vstupy.

Ústřednu je možné kromě napájení ze sítě ještě připojit na druhý zdroj, kterým může být záložní dobíjecí baterie nebo další elektrická síť.

Obr. 17. Centrální ústředna LPU [13]

4.1.2 Dveřní IP jednotka

Dveřní jednotka DCU je umísťována u dveří společně s nástěnnou IP čtečkou. Funkcí DCU je vyhodnotit stav dveřního kontaktu, odemknout a zamknout dveřní zámek, závoru nebo ovládat turnikety. V případě výpadku napájení je činnost jednotky zajištěna vestavěnou baterií. Pro komunikaci používá šifrovanou komunikaci SSL[8] (Secure Sockets Layer). S ostatními prvky S3000 komunikuje bez potíží.

4.1.3 Nástěnná IP čtečka karet

Nástěnná IP čtečka karet (Obr. 18) má nenáročné požadavky na kabeláž (kabely kategorií CAT5 a CAT6). Používá automatické přidělování IP adres podle protokolu DHCP[9] (Dynamic Host Configuration Protocol). Ostatní komunikační vlastnosti jsou totožné jako u dveřní IP jednotky.

Obr. 18. Nástěnná IP čtečka RDR [13]

4.1.4 Univerzální IP modul (I/O modul)

Jedná o univerzální vstupně/výstupní (Input/Output – I/O) IP modul s 16 vstupy a 8 výstupy. Slouží pro připojení stávajících koncových prvků PZS do systému Xtralis. Ostatní komunikační vlastnosti jsou totožné jako u dveřní IP jednotky.

---

[8] SSL – Secure Sockets Layer – je v informatice protokol, podle kterého probíhá elektronická komunikace a který poskytuje zabezpečení komunikace šifrováním a autentizaci komunikujících stran

[9] DHCP - Dynamic Host Configuration Protocol – je v informatice protokol, pomocí něhož se automaticky přidělují IP adresy počítačům v síti

4.2 Řídící software M3000

Řídicí software M3000 je grafickým rozhraním pro ovládání celého systému Xtralis 3000. Používá zabezpečenou komunikaci SSL na všech úrovních. Je schopný obsluhovat vysoký počet uživatelů a držitelů identifikačních karet.

M3000 používá otevřenou databázi SQL, proto se snadno importují a exportují data z jiných databází. Také zaznamenává rozsáhlé zprávy o poplachu i o stavech celého systému a jeho prvků.

4.3 Využití prvků systému Xtralis 3000

Navržené řešení je znázorněno na Obr. 15. Tento návrh se dá označit za modernizaci zabezpečovacích prvků.

Vstupní ovládací klávesnice, umístěné u vstupů (vjezdu) do vybraných prostorů, lze nahradit bezkontaktními IP čtečkami (Xtralis RDR), popřípadě zachovat stávající čtečky, které se k systému propojí prostřednictvím modulů RDCU (jeden modul = jedny oboustranné dveře).

U vstupů (*chodba*, *chodba 2*, hlavní vstup do budovy, vstup do haly A, vstup přes bránu mezi halami A a B – viz. Obr. 15) je možno nainstalovat přehledové kamerové body. Kamery se nasměrují do oblasti vstupu a čtecího bodu a při každém platném/neplatném průchodu bude do systémové databáze uložen snímek zachycující osobu, která se o průchod do budovy pokusila. Tyto kamery nejsou primárně použity jako klasický záznamový systém CCTV, ale pouze přehledově ukládají snímky, popřípadě umožňují přímé sledování osob. Řízení přístupů je řešeno nainstalováním řídící jednotky Xtralis LPU (rovněž místnost č. 18).

Koncové prvky PZS by mohly zůstat zachovány vzhledem k vlastnostem popsaným v částech kapitoly 3.4. Do systému se implementují prostřednictvím vstupně / výstupních modulů Xtralis IOCU.

Celý zabezpečovací systém se napojí na firewall, který zajistí propojení do sítě WAN a díky tomu je možné, aby byly všechny prvky, události, apod. přístupné odkudkoli v rámci sítě internet.

Jelikož místnost č. 18 obsahuje všechny hlavní řídící moduly, je třeba vstup do místnosti doplnit kombinovaným zařízením, a to v kombinaci klávesnice a bezkontaktní čtečky karet. Každá osoba, vstupující do místnosti, se identifikuje jedinečnou dvojicí PIN kód + karta. Místnost, jakožto i všechny ostatní místnosti a jednotlivé podsystémy jsou automaticky střeženy. Toto střežení lze vhodně nastavit například následovně:

- podsystémy, kde nebude identifikován pohyb osob, se automaticky zastřeží v 17:00 hod. (pro případ, že dojde k zapomenutí zastřežit oblast)
- celá budova se v případě, že v ní nebude identifikován pohyb osob, zastřeží v 18:00 hod.
- po příchodu osob a mávnutí kartou u přístupových bodů se automaticky odstřeží prostory, které mají být danému uživateli k dispozici
- při odchodu „mávne“ uživatel třikrát kartou u přístupového bodu a dojde k automatickému střežení míst, která daný uživatel opustil a kde již není identifikován žádný další pohyb

Dalším návrhem, tentokrát z pohledu prováděného výcviku a velkého množství návštěv v objektu SVZ, je opatření zvolených místností (učeben) čtečkami přístupového systému. Pro takové rozšíření je nutné u každých jednotlivých dveří instalovat čtečku bezkontaktních karet, modul pro ovládání dveří a zámků a zvolený elektrický zámek pro otevírání a umožnění přístupů. Jako vhodné se též jeví připojení přehledových kamer ve vybraných místnostech. Tímto způsobem se dá dohledat pohyb osob po místnostech (např. v případě krádeže) a řídící výcviku by měli přehled o počtu vycvičených osob u jednotlivých simulátorů a jejich pohybu.

Pro potřebu další evidence zůstávají návštěvníci v evidenčním softwaru po určitou dobu. Dojde-li opakovaně k návštěvě již dříve zaevidované osoby, urychlí se tak proces opětovného vydání identifikačního prvku.

Neméně důležitou inovací v zajištění ochrany objektu je ta, že se každému zaměstnanci přidělí, na rozdíl od stávajícího stavu, jedinečný kód opravňující ke vstupu do prostorů SVZ. Nastolí se tím přehlednější systém v ovládání přístupových bodů.

4.4 Shrnutí

Eliminace hrozeb, vycházející ze selhání lidského faktoru či z nedostatečného systémového opatření, není účinná pouze stanovením legislativního rámce. Není v silách žádné organizace při dodržení všech uvedených ustanovení ani při volbě nejvhodnějšího bezpečnostního opatření vyhnout se riziku. Avšak uvědoměním si slabých a silných stránek (Tab. 5.) bezpečnostních systémů v návaznosti na lidské možnosti, lze rizika minimalizovat vhodnou kombinací opatření ve věcech ostrahy objektů.

Tab. 5. Shrnutí výsledků

SHRNUTÍ VÝSLEDKŮ	**Silné stránky**	**Slabé stránky**
Současný stav	• fyzická ochrana • detektory PZS	• režimová opatření • mechanické zábranné prostředky • technický stav objektu • ústřednová část PZS • přístupový systém
Budoucí Stav	• integrovaný bezpečnostní systém • kamerový dohledový systém • systém monitorování pohybu osob • zvýšení kvality zabezpečení	• finanční prostředky • omezení provozu a bezpečnosti při modernizaci • přeškolení zaměstnanců

ZÁVĚR

Cílem této bakalářské práce bylo navrhnout možnosti a způsoby zlepšení fyzické bezpečnosti specifického výcvikového zařízení. Objekt, ve kterém se SVZ nachází, má původně jiné určení, než je u ostatních budov areálu (původně byl projektován jako garáže, remízy a učebny speciální bojové techniky). S tím souvisí i rozdílné požadavky na fyzickou bezpečnost objektu.

V této práci jsem se zaměřila na základní analýzu systému fyzické bezpečnosti objektu, který je předmětem mých návrhů. Důraz jsem kladla na fyzickou ochranu, režimová opatření, technické systémy a také jejich prvky.

Návrhy na zvýšení fyzické bezpečnosti SVZ byly koncipovány s důrazem na reálné technické řešení. Navržená opatření mohou výrazně zvýšit úroveň zabezpečení SVZ. Jsem si vědoma toho, že návrhy na doplnění SVZ technickými prostředky nemohou být finálním řešením, a že je nutné na věc pohlížet jako na neustálý proces modernizace. Moje návrhy mohou být využity jako podklad pro zpracování základních požadavků modernizace zabezpečení objektu SVZ (v podobě Uživatelského požadavku akviziční potřeby i jako výchozí podklad pro zahájení projektových prací). Na modernizaci technického řešení, zvyšujícího užitnou hodnotu SVZ i cestou zvyšování kvality fyzické bezpečnosti SVZ, bych se chtěla podílet i v budoucnosti.

ZÁVĚR V ANGLIČTINĚ

The aim of this bachelor work was to suggest options and ways to improve physical security of the specific training equipment. The building where STE is situated, has another original function than the other buildings in this area (it was originally designed as a garage, classrooms, and draws special combat techniques). This fact means different requirements for physical security of the building.

In this work I focused on fundamental system analysis of the physical security of the building, which is the subject of my proposals. I highlightet the physical protection regime measures, and technical systems and their components.

Proposals to increase the physical security of STE have been designed with an emphasis on real technical solutions. The proposed measures can significantly increase the security level STE. I am aware that proposals to supplement the STE technical resources can not be the final solution, and that the matter should be viewed as a continuous process of modernization. My proposals may be used as a basis for the processing of basic security requirements of modernization object STE (in the form of User requirement acquisition needs as a precursor for initiation of project work). In the future I would like to participate in the modernization of technical solutions which increase the usefulness of the STE and by increasing the quality of the physical security of STE.

SEZNAM POUŽITÉ LITERATURY

[1] Ministerstvo obrany ČR [online]. [cit. 2011-01-24]. Dostupné z WWW: <http://www.army.cz/>

[2] ČT 24 [online]. 21.7.2010 [cit. 2011-02-03]. Dostupné z WWW: <http://www.ct24.cz/domaci/96337-generalni-stab-kam-vnikli-zlodeji-nehlidala-vojenska-policie/>

[3] Národní bezpečnostní úřad [online]. 2010 [cit. 2011-01-24]. Dostupné z WWW: <http://www.nbu.cz/cs/ochrana-utajovanych-informaci/fyzicka-bezpecnost/informace/>

[4] Národní bezpečnostní úřad [online]. 2010 [cit. 2011-03-24]. Dostupné z WWW: <http:// www.nbu.cz/cs/pravni-predpisy/zakon-c-4122005/uplne-zneni-zakona/>

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

[6] Rozkaz ministryně obrany č. 6/2009, o ochraně vojenského objektu

[7] ČANDÍK, Marek. *Objektová bezpečnost II.* 1. vydání, UTB Zlín, 2004. 100 s. ISBN 80-7318-217-3

[8] ČERNÝ, Josef., IVANKA, Ján., a kol. *Systemizace bezpečnostního průmyslu I.* 2. vydání, UTB Zlín, 2006. 135 s. ISBN 80-7318-402-8

[9] UHLÁŘ, Jan. *Technická ochrana objektů I. díl, Mechanické zábranné systémy II.* 1. vydání, Praha: PA ČR, 2004. 180 s. ISBN 80-7251-172-6

[10] LAUCKÝ, Vladimír. *Řízení technologických procesů v průmyslu komerční bezpečnosti*. 2. vydání, UTB Zlín, 2006. 101 s. ISBN 80-7318-432-X

[11] KINDL, Jiří. *Projektování bezpečnostních systémů*. Zlín: UTB, 2007. 134 s. ISBN 978-80-7318-554-1

[12] KŘEČEK, S. a kol. *Příručka zabezpečovací techniky*. 3. vydání, Blatná: Cricetus, 2006. 313 s. ISBN 80-902938-2-4

[13] Xtralis S3000, V3000 a M3000: Integrovaný bezpečnostní systém [prezentace]. Vyškov: JIMI CZ, a. s. 26. 4.2011

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AČR	Armáda České republiky.
apod.	A podobně.
BVP-2	Bojového vozidla pěchoty.
CCTV	Closed circuit television.
ČR	Česká republika.
ČSN EN 50 131-1	Česká norma pro poplachové zabezpečovací a tísňové systémy (všeobecné požadavky).
ČSN P ENV 1627	Česká norma pro mechanické zábranné systémy (okna, dveře, uzávěry, odolnost proti násilnému vniknutí, požadavky a klasifikace).
ČSN EN 50 133-1	Česká norma pro systémy kontroly a řízení vstupu (všeobecné požadavky).
DC	Stejnosměrný proud.
DCU	Door Control Unit.
DHCP	Dynamic Host Configuration Protocol.
I/O	Input/Output.
IOCU	Input/Output Control Unit.
IP	Internet Protocol.
IR	Infrared.
LAN	Local Area Network.
LED	Light-Emitting Diode.
LOS	Light Observation System .
LPU	Local Processing Unit.
Mi-17	Vrtulník Mi-17.
Mi-24	Vrtulník Mi-24.
MILES	Multiple Integrated Laser Engagement System.

MO	Ministerstvo obrany.
MW	Microwave.
MZS	Mechanické zábranné systémy.
NBÚ	Národní bezpečnostní úřad
PIN	Personal Identification Number.
PIR	Pasiv infrared.
PPC	Poplachové přijímací centrum.
PZS	Poplachový zabezpečovací systém.
RDCU	Reader Door Control Unit.
RDR	Read Door Reader.
RMO	Rozkaz ministra obrany.
SSL	Secure Sockets Layer.
SQL	Structured Query Language.
SVZ	Speciální výcvikové zařízení.
SWOT	Strengths, Weaknesses, Opportunities, Threats.
TCP	Transmission Control Protocol.
T-72M	Modernizovaný tank T-72.
T-72M4Cz	Modernizovaný tank T-72 podnikem ČR.
VZP	Voják z povolání.
WAN	Wide Area Network.
Zákl-1	Základní řád ozbrojených sil České Republiky.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK