

Hodnocení bezpečnostních rizik zabezpečení zvoleného objektu

Veronika Schenková



Univerzita Tomáše Bati ve Zlíně

Fakulta logistiky a krizového řízení

Ústav krizového řízení

Akademický rok: 2024/2025

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	Veronika Schenková
Osobní číslo:	L22690
Studijní program:	B1022A020002 Management rizik
Specializace:	Management rizik
Forma studia:	Kombinovaná
Téma práce:	Hodnocení bezpečnostních rizik zabezpečení zvoleného objektu

Zásady pro vypracování

1. Zpracujte teoretický vstup do řešené problematiky.
2. Zvolte vhodný objekt pro realizaci experimentální části a tento analyzujte z pohledu bezpečnostních rizik a požadavků fyzické bezpečnosti.
3. Vyhodnotte současná opatření fyzické bezpečnosti a navrhnete případná doplnění s cílem zvýšit úroveň zabezpečení zvoleného objektu.

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

Seznam doporučené literatury:

1. FENNELLY, Lawrence J. *Effective Physical Security. Fifth Edition*. Amsterdam: Elsevier, 2017. ISBN 978-0-12-804462-9.
2. FENNELLY, Lawrence J. a PERRY, Marianna A. *Physical Security: 150 Things You Should Know. Second Edition*. Amsterdam: Elsevier, 2016. ISBN 978-0-12-809487-7.
3. VALOUCH, Jan. *Projektování bezpečnostních systémů. Druhé vydání*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2019. ISBN 978-80-7454-858-1.
4. 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. Dostupné z: <https://www.nbu.cz/cs/pravni-predpisy/provade-ci-pravni-predpisy/1087-vyhlas-ka-c-5282005>.
5. Zákon č. 412/2005 Sb. ze dne 21. září 2005, o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. Online. In: *Sbírka zákonů České republiky*. 2005, částka 143. Dostupné z: <https://www.nbu.cz/cs/pravni-predpisy/zakon-c-412-2005/1122-uplne-zneni-zakona-c-412-2005>.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **Ing. Jakub Rak, Ph.D.**
Ústav ochrany obyvatelstva

Datum zadání bakalářské práce: **2. prosince 2024**
Termín odevzdání bakalářské práce: **2. května 2025**

L.S.

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

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

V Uherském Hradišti dne 2. prosince 2024

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že

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

Prohlašuji, že

- jsem na bakalářské práci pracovala samostatně a použitou literaturu jsem řádně citovala; v případě publikace výsledků budu uvedena jako spoluautor;
- odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne 2. 5. 2025

.....
podpis autora

ABSTRAKT

Tato bakalářská práce se zaměřuje na analýzu a návrh zlepšení fyzického zabezpečení vybraného objektu, ve kterém dochází k výuce, výcviku a práci s utajovanými informacemi. Cílem práce je zhodnotit současný stav ochrany objektu, identifikovat jeho slabá místa a navrhnout vhodná opatření ke zvýšení bezpečnosti. V teoretické části jsou popsány principy fyzické bezpečnosti, legislativní rámec, základní technické a organizační prostředky. Praktická část se věnuje analýze konkrétního objektu, využívá Ishikawa diagram pro grafické znázornění příčin a důsledků bezpečnostních rizik, a dále aplikuje kvalitativní metodu pro ohodnocení identifikovaných hrozeb. Výsledkem je návrh konkrétních opatření k zesílení ochrany objektu s důrazem na efektivitu, použitelnost a finanční přiměřenost.

Klíčová slova: analýza rizik, bezpečnostní rizika, fyzická bezpečnost, režimová opatření, vojenský objekt.

ABSTRACT

This bachelor's thesis focuses on the analysis and improvement proposal of physical security in a selected facility used for training, education, and handling classified information. The aim of the thesis is to evaluate the current level of security, identify vulnerabilities, and propose suitable measures to enhance protection. The theoretical part presents the principles of physical security, the legal framework, and key technical and organizational tools. The practical part analyzes the specific object, uses the Ishikawa diagram to visualize causes and consequences of security threats, and applies a qualitative risk assessment method to evaluate identified risks. The outcome is a set of tailored security recommendations focused on effectiveness, usability, and financial feasibility.

Keywords: military facility, physical security, risk analysis, security régime, security risks.

Chtěla bych poděkovat vedoucímu práce panu Ing. Jakubu Rakovi, Ph.D., za odborné vedení při zpracovávání bakalářské práce, cenné rady, vstřícný přístup a trpělivost. Zároveň děkuji pracovníkům firmy Trade FIDES, a.s. za poskytnutí důležitých informací a spolupráci, která významně přispěla k praktické části této práce.

OBSAH

ÚVOD.....	11
I TEORETICKÁ ČÁST	13
1 BEZPEČNOSTNÍ RIZIKA A FYZICKÁ BEZPEČNOST.....	14
1.1 BEZPEČNOST A JEJÍ DĚLENÍ.....	14
1.2 BEZPEČNOSTNÍ RIZIKO	15
2 PRÁVNÍ NORMY A NORMY V OBLASTI FYZICKÉ BEZPEČNOSTI V RESORTU MINISTERSTVA OBRANY.....	17
2.1 ZÁKON 412/2005 Sb., O OCHRANĚ UTAJOVANÝCH INFORMACÍ A O BEZPEČNOSTNÍ ZPŮSOBILOSTI.....	17
2.2 NAŘÍZENÍ VLÁDY Č. 440/2024 Sb., O KATALOGU OBLASTÍ UTAJOVANÝCH INFORMACÍ	18
2.3 VYHLÁŠKA Č. 300/2024 Sb. O PERSONÁLNÍ BEZPEČNOSTI A O BEZPEČNOSTNÍ ZPŮSOBILOSTI.....	19
2.4 VYHLÁŠKA Č. 275/2022 Sb. O ADMINISTRATIVNÍ BEZPEČNOSTI A O REGISTRECH UTAJOVANÝCH INFORMACÍ.....	19
2.5 VYHLÁŠKA Č. 528/2005, O FYZICKÉ BEZPEČNOSTI A CERTIFIKACI TECHNICKÝCH PROSTŘEDKŮ.....	20
2.6 NORMATIVNÍ VÝNOS Č. 42/2006, O FYZICKÉ BEZPEČNOSTI V REZORTU MINISTERSTVA OBRANY	21
2.7 TECHNICKÉ NORMY ČSN	21
3 OPATŘENÍ FYZICKÉ BEZPEČNOSTI	23
3.1 TYPY OCHRANY OBJEKTU	23
3.2 POPLACHOVÝ ZABEZPEČOVACÍ A TÍSŇOVÝ SYSTÉM	25
3.3 DOHLEDOVÝ VIDEOSYSTÉM	26
3.4 ELEKTRONICKÁ POŽÁRNÍ SIGNALIZACE.....	26
3.5 OSTRAHA	27
3.6 REŽIMOVÁ OPATŘENÍ	27
4 IDENTIFIKACE, ANALÝZA A HODNOCENÍ RIZIK.....	29
4.1 ISHIKAWA DIAGRAM.....	29
4.2 HODNOCENÍ RIZIK	31
4.3 DÍLČÍ ZÁVĚR	32
II PRAKTICKÁ ČÁST	34
5 CHARAKTERISTIKA VYBRANÉHO OBJEKTU	35
5.1 POPIS AREÁLU A HODNOCENÉHO OBJEKTU	35
5.2 PLÁŠŤOVÁ OCHRANA	37
5.2.1 Konstrukční prvky budovy.....	37

5.2.2	Mechanické zábranné prostředky pláště budovy.....	37
5.2.3	Elektronické zabezpečovací prvky pláště budovy.....	38
5.3	PROSTOROVÁ OCHRANA	39
5.3.1	Mechanické zábranné prostředky	39
5.3.2	Poplachový zabezpečovací a tísňový systém	40
5.3.3	Elektrická požární signalizace	41
5.3.4	Elektronická kontrola vstupu.....	41
5.4	PŘEDMĚTOVÁ OCHRANA.....	42
5.5	OSTRAHA.....	43
5.6	REŽIMOVÁ OPATŘENÍ	43
5.7	PERSONÁLNÍ BEZPEČNOST	45
5.8	PŘEHLED APLIKOVANÝCH SYSTÉMŮ	45
5.9	VYHODNOCENÍ SOUČASNÉHO STAVU ZABEZPEČENÍ OBJEKTU	47
6	ANALÝZA A IDENTIFIKACE BEZPEČNOSTNÍCH RIZIK OBJEKTU.....	49
6.1	ANALÝZA HROZEB POMOCÍ ISHIKAWA DIAGRAMU	49
6.2	KVALITATIVNÍ HODNOCENÍ RIZIK	50
6.3	ZÁVĚR ANALÝZY	52
7	NÁVRH OPATŘENÍ KE ZVÝŠENÍ ÚROVNĚ FYZICKÉ BEZPEČNOSTI.....	53
7.1	UMÍSTĚNÍ STÁLÉ OSTRAHY PŘÍMO DO OBJEKTU	53
7.2	NAVÝŠENÍ BEZPEČNOSTNÍCH PRVKŮ VE VYBRANÉ MÍSTNOSTI V 1. NP	55
7.3	DOPLNĚNÍ TURNIKETŮ KE VSTUPU DO 2. NP.....	57
7.4	FINANČNÍ PLÁN ZAVEDENÍ BEZPEČNOSTNÍCH PRVKŮ.....	58
	ZÁVĚR.....	61
	SEZNAM POUŽITÉ LITERATURY	63
	SEZNAM OBRÁZKŮ	67
	SEZNAM TABULEK.....	68
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	69
	SEZNAM PŘÍLOH.....	70

ÚVOD

Bezpečnost je jednou z nejdůležitějších hodnot v lidské společnosti. Vzhledem ke zhoršující se bezpečnostní situaci v Evropě i ve světě narůstá potřeba připravenosti ozbrojených sil a dalších bezpečnostních složek. S tím souvisí také zvyšující se nároky na bezpečnostní standardy vojenských objektů, kde probíhá výcvik, vzdělávání či práce s utajovanými informacemi. Efektivní ochrana těchto objektů je zásadní nejen pro fyzickou bezpečnost osob a majetku, ale i pro udržení důvěryhodnosti systému ochrany utajovaných informací.

Tato bakalářská práce se zabývá hodnocením úrovně fyzické bezpečnosti konkrétního výcvikového vojenského objektu, ve kterém dochází jak k výcviku příslušníků ozbrojených složek, tak k nakládání s utajovanými informacemi. Hlavním cílem práce je analyzovat současný stav zabezpečení tohoto objektu z hlediska fyzické bezpečnosti, identifikovat jeho slabá místa a navrhnout realistická opatření vedoucí k posílení bezpečnosti v souladu s platnými právními a technickými normami. Dílčími cíli jsou zpracování teoretického rámce fyzické bezpečnosti se zaměřením na ochranu utajovaných informací, dále popis a vyhodnocení stávajícího zabezpečení objektu, identifikace bezpečnostních rizik pomocí vhodných analytických nástrojů a návrh technických a organizačních opatření ke snížení nebo eliminaci těchto rizik.

V práci byly stanoveny výzkumné otázky:

- Které konkrétní oblasti současného zabezpečení objektu vykazují největší potenciál pro narušení fyzické bezpečnosti?
- Jaká organizační nebo technická opatření mohou přispět k efektivnímu snížení rizika narušení?
- Do jaké míry je možné zlepšit bezpečnostní úroveň objektu bez zásadních stavebních úprav nebo finančně náročných zásahů?

Pro získání odpovědí na tyto otázky byla použita kombinace následujících metod:

- Analýza současného stavu fyzické bezpečnosti na základě normativních požadavků a provozní dokumentace.
- Ishikawa diagram pro identifikaci příčin bezpečnostních incidentů.
- Kvalitativní hodnocení identifikovaných rizik.

Z důvodu bezpečnostních opatření vztahujících se k vojenskému objektu nejsou v této práci uvedeny žádné detailní fotografie, technické výkresy ani konkrétní označení reálných prostor. Použité plány budovy mají výhradně ilustrační charakter a slouží pouze pro orientační účely. Jedná se o reálný návrh na zvýšení opatření fyzické bezpečnosti, vycházející ze smyšleného objektu. Návrhová část vychází ze všeobecně známých bezpečnostních pravidel, odborných podkladů a zkušeností.

Práce je rozdělena do dvou hlavních částí. První, teoretická část, definuje základní pojmy, legislativní rámec a systém fyzické bezpečnosti. Druhá, praktická část, se zaměřuje na analýzu a návrh možných zlepšení na vybraném objektu.

I TEORETICKÁ ČÁST

1 BEZPEČNOSTNÍ RIZIKA A FYZICKÁ BEZPEČNOST

Bezpečnostní riziko je kombinace pravděpodobnosti, že se určitá hrozba uskuteční, a závažnosti následků, které by tuto událost způsobila. Hodnotí, jak je pravděpodobné, že hrozba způsobí škodu, a jak velký by byl její dopad (Fennelly, 2016).

Bezpečnost tvoří základní pilíř, který ovlivňuje naše jednání, životní podmínky i mezilidské vztahy. Znamená ochranu lidí, majetku a informací před různými hrozbami a nebezpečími, ať už pocházejí z přírodních událostí, kriminality nebo z technických selhání. S nárůstem rizik v moderním světě nabývá otázka bezpečnosti stále větší význam a stává se naléhavější, což vyžaduje pečlivé plánování a realizaci bezpečnostních opatření k účinné ochraně před potenciálními hrozbami. Fyzická bezpečnost je pro ochranu před riziky jakýmsi ochranným obalem, který ochraňuje cenné zdroje a zajišťuje jejich integritu. Skládá se z pečlivě navrženého bezpečnostního systému, který obsahuje přístupové kontrolní prvky, fyzické bariéry, alarmové systémy a monitorování. Definice zdůrazňuje význam fyzické bezpečnosti k efektivnímu řízení rizik (Fennelly, 2016).

Fyzická bezpečnost představuje soubor opatření zaměřených na zajištění nebo ztížení neoprávněného přístupu k utajovaným informacím (dále jen UI). Tato opatření se rovněž snaží tento každý pokus o přístup zaznamenat. Toho lze dosáhnout pomocí ostrahy, stanovení konkrétních pravidel a použití kombinací technických prostředků (Národní bezpečnostní úřad, 2025).

1.1 Bezpečnost a její dělení

Z teoretického hlediska je bezpečnost stav, kdy systém odolává známým i předvídatelným hrozbám zvenčí i zevnitř, aniž by utrpěl vážné poškození nebo selhal. To znamená, že si systém udrží svoji strukturu, stabilitu, spolehlivost a bude fungovat tak, jak má. Schopnost systému se přizpůsobit různým hrozbám a změnám je tedy podstatným prvkem bezpečnosti.

Z pohledu chráněného objektu můžeme rozlišovat:

- **Vnitřní bezpečnost** – zabývá se hrozbami uvnitř objektu,
- **Vnější bezpečnost** – zaměřuje se na hrozby přicházející zvenčí.

Z pohledu ochrany státu rozlišujeme:

- **Vnější bezpečnost státu** – zahrnuje ochranu jeho hranic, svrchovanosti a nezávislosti, a také ochranu jeho zástupců a občanů v zahraničí, zejména v krizových situacích. Zahrnuje rovněž mezinárodní vztahy a spolupráci, prostřednictvím kterých stát prosazuje své zájmy. Vnější bezpečnost je dosažena minimalizací vnějších hrozeb (vojenských, ekonomických, migračních atd.) a efektivní připravenosti státu těmto hrozbám čelit.
- **Vnitřní bezpečnost státu** – v širším pojetí znamená udržování základních funkcí státu, ochranu demokratických principů dodržování pořádku a zákonů a ochranu životů, zdraví, majetku a životního prostředí před vnitřními hrozbami. Toho se dosahuje prostřednictvím různých bezpečnostních mechanismů, zákonů a opatření, která podporují demokracii, ekonomický růst a bezpečnost občanů. Úspěšná vnitřní bezpečnost se vyznačuje minimalizací vnitřních hrozeb a efektivní připraveností státu při řešení současných i potenciálních rizik. Stát musí být vybaven a připraven tyto hrozby účinně eliminovat (Ščurek, 2021).

Podle Ústavního zákona č. 110/1998 Sb., o bezpečnosti České republiky, zajišťují bezpečnost České republiky (dále jen ČR) ozbrojené síly, ozbrojené bezpečnostní sbory, záchranné sbory a havarijní služby. Státní orgány, orgány územní samosprávy, právnické a fyzické osoby mají povinnost se podílet na zajišťování bezpečnosti ČR (Česko, 1998).

1.2 Bezpečnostní riziko

Riziko představuje pravděpodobnost, že dojde k události, kterou považujeme za nežádoucí z hlediska bezpečnosti. Toto riziko vychází z konkrétních hrozeb, které identifikujeme. Míru rizika, tedy pravděpodobnost negativních následků spojených s danou hrozbou a zranitelností, lze vyhodnocovat pomocí analýzy rizik. Ta mimo jiné zohledňuje naši schopnost a připravenost reagovat na potenciální hrozby, což je zásadní pro účinné plánování a realizaci ochranných opatření, které minimalizují pravděpodobnost vzniku nežádoucích událostí (Ministerstvo vnitra ČR, c 2025).

Každá organizace, firma nebo společnost se během své činnosti potýká s různými riziky, která mohou negativně ovlivnit jejich fungování a integritu. Bezpečnostní manažeři se proto snaží těmto rizikům vyhnout nebo předcházet, a tím minimalizovat jejich dopady

na co nejnížší úroveň. Odpovědným a správným řízením rizik lze předejít mnoha škodám a ztrátám, které by mohly mít nezvratné škodlivé důsledky pro organizaci (Smejkal a Rais, 2010).

Řízení rizik ve fyzické bezpečnosti je komplexní a náročný proces, který se liší od řízení rizik v jiných oblastech. Zatímco jiné oblasti se mohou zaměřovat na statistické modely a předpovídání pravděpodobností, řízení rizik ve fyzické bezpečnosti bere v úvahu zvláště chráněné zájmy jednotlivých subjektů, které se mohou značně lišit. Hodnocení rizik v této oblasti se proto zaměřuje na analýzu možných bezpečnostních incidentů, přičemž je nutné zohlednit motivaci a pohnutky potenciálních pachatelů, kteří se řídí cíleně a individuálními faktory. Tato individuální povaha protiprávních činností činí řízení rizik ve fyzické bezpečnosti je náročnější a vyžaduje komplexnější strategický přístup (Procházková, 2011).

2 PRÁVNÍ NORMY A NORMY V OBLASTI FYZICKÉ BEZPEČNOSTI V RESORTU MINISTERSTVA OBRANY

Ochrana a bezpečnost jsou řízeny zákony, vyhláškami a normami, které společně tvoří komplexní rámec pro ochranu lidí, majetku a citlivých informací. Tyto legislativní dokumenty zahrnují obecné normy pro zajištění standardů kvality a bezpečnosti, i specifické právní předpisy zaměřené na jednotlivé sektory jako je Ministerstvo obrany (dále jen MO) nebo jiné oblasti bezpečnosti. Cílem těchto pravidel je vytvořit bezpečné prostředí, které minimalizuje rizika a zajišťuje efektivní reakci na potenciální hrozby. Jsou základním kamenem pro vývoj a uplatnění bezpečnostních strategií a opatření na všech úrovních. Úředním orgánem ČR odpovědným za ochranu UI a zajištění bezpečnosti je Národní bezpečnostní úřad (dále jen NBÚ), v čele s bezpečnostním ředitelem.

2.1 Zákon 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti

Zákon zahrnuje ochranu UI a bezpečnostní způsobilost, stanovuje zásady pro jejich klasifikaci a podmínky přístupu k nim a další požadavky k jejich ochraně. NBÚ upravuje definici UI v novele tohoto zákona, protože původní verze podle úřadu nezahrnovala všechny možné formy UI. Nová definice zahrnuje také ústní, obrazovou nebo zvukovou formu UI, protože taková informace může existovat i bez záznamu na nosiči (Vláda posílá do sněmovny zpřesnění definice utajované informace, c 2021-2024).

Pro účely novely tohoto zákona s účinností od 1. ledna 2025, se rozumí „*utajovanou informací informace v jakékoliv podobě označená stupněm utajení podle tohoto zákona, jejíž vyrazení nebo zneužití může způsobit újmu zájmu České republiky nebo může být pro tento zájem nevýhodné, a kterou lze podřadit pod položku uvedenou v katalogu oblastí utajovaných informací.*“ (Česko, 2005a).

Újmou na zájem České republiky se v rámci tohoto zákona rozumí poškození nebo ohrožení zájmů státu. Tato újma se třídí podle míry závažnosti na tři kategorie: mimořádně vážná újma, vážná újma a prostá újma.

Podle výše újmy a dopadu na tento zájem, řadíme UI do 4 skupin. Toto zařazení určuje autor a je povinen informaci řádně označit.

Jak uvádí Zákon č. 412/2005 Sb.:

*„a) **Přísně tajné**, jestliže její vyjádření neoprávněné osobě nebo zneužití může způsobit mimořádně vážnou újmu zájmu České republiky,*

*b) **Tajné**, jestliže její vyjádření neoprávněné osobě nebo zneužití může způsobit vážnou újmu zájmu České republiky,*

*c) **Důvěrné**, jestliže její vyjádření neoprávněné osobě nebo zneužití může způsobit prostou újmu zájmu České republiky, nebo*

*d) **Vyhrazené**, jestliže její vyjádření neoprávněné osobě nebo zneužití může být nevýhodné pro zájem České republiky.“ (Česko, 2005a).*

Zákon stanovuje různé druhy zajištění ochrany UI, které jsou nezbytné pro garanci bezpečnosti a důvěrnosti těchto informací:

- **Personální bezpečnost** – výběr, ověřování a školení osob, které mají přístup k UI.
- **Průmyslová bezpečnost** – opatření k ověřování podmínek pro přístup podnikatelů k UI a zajištění správné manipulace s nimi.
- **Administrativní bezpečnost** – tvorba, evidence, zpracování, odesílání, přeprava, ukládání a archivace UI.
- **Fyzická bezpečnost** – nezbytná k zabránění neoprávněného přístupu k UI a zaznamenání pokusů o přístup.
- **Bezpečnost informačních a komunikačních systémů** – slouží k zajištění důvěrnosti, integrity a dostupnosti UI v těchto systémech.
- **Kryptografická ochrana** – opatření na ochranu UI pomocí kryptografických metod při jejich zpracování, přenosu nebo ukládání (Česko, 2005).

2.2 Nařízení vlády č. 440/2024 Sb., o katalogu oblastí utajovaných informací

Katalog rozděluje UI do 14 tematických oblastí (např. ochrana UI, obrana státu, mezinárodní vztahy, kybernetická bezpečnost, finance). Každá oblast dále obsahuje specifické typy UI s určením stupně utajení (Přísně tajné, Tajné, Důvěrné, Vyhrazené).

Nařízení nabylo účinnosti 1. ledna 2025. Toto nařízení tedy přináší modernizaci systému ochrany UI v ČR (Česko, 2024a).

2.3 Vyhláška č. 300/2024 Sb. o personální bezpečnosti a o bezpečnostní způsobilosti

Personální bezpečnost je důležitým prvkem ochrany UI. Zahrnuje nejen ověřování podmínek, které musí fyzická osoba splnit pro přístup k těmto informacím, ale také vzdělávání těchto osob. Odpovědná osoba je povinna zajistit, aby fyzické osoby s přístupem k UI byly pravidelně školeny v právních předpisech týkajících se ochrany UI, a to jednou za dvanáct měsíců. Tato osoba také vede záznamy o těchto školeních a je povinna je uchovávat po dobu jednoho roku. Metody a rozsah ověřování podmínek, které musí fyzická osoba splnit pro získání přístupu k takovým informacím, se liší podle různých stupňů utajení. Základní požadavky jsou dosažení plnoletosti, plná právní způsobilost a čistý trestní rejstřík. Pro stupeň utajení "Vyhrazené" ověřuje podmínky osoba, která je odpovědná za fyzickou osobu v rámci služebního, pracovněprávního, členského nebo obdobného vztahu, nebo jí určená osoba. Pokud taková osoba není určena, ověření provede odpovědná osoba nebo jí určená osoba toho, kdo umožní fyzické osobě přístup k UI stupně utajení "Vyhrazené". V ostatních případech provede ověření NBÚ na základě odůvodněné písemné žádosti (Národní bezpečnostní úřad, c 2025).

Výše zmíněná Vyhláška se zabývá personální bezpečností a bezpečnostní způsobilostí. Obsahuje vzory dokumentů, které jsou potřebné pro různé aspekty personální bezpečnosti, jako jsou prohlášení o svéprávnosti, žádosti o přístup k UI a další. Vyhláška také specifikuje, jaké informace musí být uvedeny ve zdůvodněných žádostech a jaké dokumenty musí být k těmto žádostem přiloženy. Dále definuje způsoby a formy podání žádostí, a to jak v listinné, tak v elektronické podobě. Stanovuje povinnost oznamovat změny v údajích, například změnu adresy, zaměstnavatele nebo nabytí nemovitého majetku. Vyhláška ruší předchozí právní předpisy týkající se personální bezpečnosti a bezpečnostní způsobilosti a nabývá účinnosti 1. ledna 2025 (Česko, 2024b).

2.4 Vyhláška č. 275/2022 Sb. o administrativní bezpečnosti a o registrech utajovaných informací

Administrativní bezpečnost tvoří nezbytnou součást systému ochrany informací. Jejím cílem je správné nakládání s utajovanými i běžnými dokumenty, a to v souladu s právními

předpisy a interními normami. Význam administrativní bezpečnosti spočívá v prevenci neoprávněného přístupu k citlivým informacím a ochranou před ztrátou nebo poškozením dokumentů.

Vyhláška č.275/2022 Sb., stanovuje druhy administrativních pomůcek, jejich náležitosti a požadavky na jejich vedení, včetně způsobu vyznačování náležitostí na utajovaných dokumentech. Vyhláška také upravuje podrobnosti k přepravě, přenášení, převzetí a zapůjčování těchto dokumentů a organizaci a činnost registrů UI. Definuje, jaké informace musí být uvedeny na utajovaných dokumentech, jak mají být evidovány a jaké jsou požadavky na jejich manipulaci a ukládání. Předpis rovněž stanovuje postupy pro jejich zničení a zajištění ochrany UI při personálních změnách nebo zániku organizace (Česko,2022).

2.5 Vyhláška č. 528/2005, o fyzické bezpečnosti a certifikaci technických prostředků

Tato vyhláška byla aktualizována v roce 2024 a podrobně popisuje pravidla pro fyzickou bezpečnost a proces certifikace technických zařízení. Hlavním cílem vyhlášky je ochrana UI. Vyhláška hodnotí bezpečnostní opatření a stanovuje minimální úroveň zabezpečení různých prostorů a technických zařízení. Je tudíž nezbytná pro správné sestavení a realizaci projektu v oblasti fyzické bezpečnosti.

Definuje důležité pojmy jako:

- **Objekt a jeho hranice** – budova nebo ohraničený prostor s chráněnými oblastmi, jehož hranici tvoří plášť budovy, oplocení nebo jiná viditelná bariéra.
- **Zabezpečená a jednací oblast** – vymezený a ohraničený prostor, zabezpečený podle stupně utajení uložené nebo projednávané informace.
- **Hrozba a riziko** – možnost úniku nebo zneužití UI při porušení ochrany a pravděpodobnost, že se hrozba uskuteční.
- **Technický prostředek** – prvek, který slouží ke ztížení, zaznamenání nebo oznámení narušení objektu nebo oblasti.
- **Úschovný objekt** – schránka k bezpečnému uložení chráněných aktiv.

Podrobně se věnuje tomu, jak se zabezpečují budovy a zabezpečené prostory v nich s využitím mechanických zábran, alarmů a kamerových systémů, přičemž se bere v potaz stupeň utajení chráněných aktiv. Stejně tak jsou popsány bezpečnostní postupy pro jednací prostory, včetně kontroly vstupu a používání technických prostředků. Vyhláška také definuje pravidla pro ochranu technických zařízení obsahujících citlivá data. Důraz je kladen na kontrolu přístupu, správné zacházení s klíči, identifikačními kartami a na to, kdo má právo k přístupu do chráněných oblastí. Vyhláška dále stanovuje metodiku pro pravidelnou kontrolu a hodnocení bezpečnostních opatření a rizik. Zabývá se náležitostmi žádosti o certifikaci technických prostředků, definuje platnost certifikátu a specifikuje potřebné náležitosti žádosti o uzavření smlouvy o zajištění bezpečnostních služeb (Česko, 2005b).

2.6 Normativní výnos č. 42/2006, o fyzické bezpečnosti v rezortu Ministerstva obrany

Tento výnos je založen na zákoně č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, a na dalších vyhláškách, jako jsou vyhláška č. 384/2024 Sb., o průmyslové bezpečnosti, vyhláška č. 300/2024 Sb., o personální bezpečnosti, a Rozkaze ministra obrany č. 14/2013, který se zabývá ochranou UI v MO. Výnos upřesňuje odpovědnost za svěřené prostory a další zařízení pro organizační celky umístěné ve vojenském areálu. Jsou stanoveni bezpečnostní manažeři pro rozsáhlé objekty a jednotlivé součásti, hranice objektu, odpovědnost za fyzickou bezpečnost na perimetru rozsáhlého objektu a způsob výkonu ostrahy. Opatření fyzické bezpečnosti jsou organizována vedoucím organizační celku (dále jen VOC) na základě určení kategorií a tříd zabezpečených a jednacích oblastí. Na základě hodnocení rizik a zranitelnosti UI se stanovuje míra rizika jako „malá“, „střední“ nebo „velká“. Projekt fyzické bezpečnosti schvaluje a realizuje VOC – velitel (Česko, 2006).

2.7 Technické normy ČSN

Ve spojení s vyhláškou č. 528/2005 Sb. jsou technické normy ČSN dokumentem, který specifikuje požadavky na různé typy úschovných objektů, zámků, zabezpečených oblastí, uzamykacích systémů a dalších bezpečnostních prvků, přičemž se odkazuje na konkrétní normy ČSN, které definují technické a bezpečnostní standardy.

- Úschovné objekty musí splňovat požadavky bezpečnostních tříd podle normy ČSN EN 1143-1.
- Zámky úschovných objektů musí odpovídat třídám podle normy ČSN EN 1300.
- Okna, dveře a další uzávěry zabezpečených oblastí musí splňovat požadavky bezpečnostních tříd podle normy ČSN EN 1627.
- Systém kontroly vstupu musí splňovat požadavky bezpečnostních tříd podle normy ČSN EN 60839-11-1.
- Poplachové zabezpečovací a tísňové systémy musí být v souladu s normou ČSN EN 50131-1 ED. 2.

Tyto normy zajišťují, že všechny uvedené bezpečnostní prvky a systémy dosahují požadované úrovně ochrany a spolehlivosti (Česko, 2005c).

3 OPATŘENÍ FYZICKÉ BEZPEČNOSTI

S rostoucími hrozbami a riziky, které mohou ohrozit fyzickou integritu budov, zařízení a dalších cenných aktiv, je nezbytné implementovat i efektivní ochranná opatření. Tato kapitola se zaměřuje na různé typy ochrany objektů, které jsou využívány k minimalizaci rizik a zajištění bezpečnosti. Opatření fyzické bezpečnosti zahrnují skupinu pravidel, technických prostředků a postupů. Ty mají za cíl chránit osoby, majetek a citlivé informace před různými riziky a hrozbami. Můžeme sem zařadit mechanické zábranné systémy, elektronická zařízení, pravidla a postupy organizace, bezpečnostní standardy, fyzickou ostrahu a personální bezpečnost z hlediska přístupu k UI. Všechna tato opatření se navzájem doplňují a jejich kombinace a efektivita závisí na specifických potřebách a rizicích daného objektu a organizace. Je to proces navržený tak, aby minimalizoval rizika včetně jejich negativních dopadů.

3.1 Typy ochrany objektu

Tento systém rozlišuje čtyři typy ochrany, které představují různé úrovně zabezpečení. Liší se podle toho, kterou část objektu sledují. Jsou schopny detekovat jakékoli narušení normálního stavu.

Ochrana perimetru – perimetrická ochrana, známá také jako obvodová, se soustředí na zabezpečení hranic pozemku a samotného chráněného objektu. Jasně tyto hranice vyznačuje a dává najevo, že vstup je zakázán. Fyzické překážky by měly být umístěny podél celého obvodu hranice chráněného prostoru, pokud to povaha terénu dovoluje. Obvykle zahrnuje ploty, vysoké zdi, branky nebo přírodní překážky, jako jsou živé ploty nebo vodní toky. Pro zvýšení účinnosti zabezpečení mohou být kolem těchto překážek instalovány elektronické a technické ochranné prvky, jako jsou kamery a alarmy. Tyto prvky musí být vyrobeny z odolných materiálů, aby odolaly přírodním vlivům. Nevýhodou tohoto typu ochrany je častý výskyt planých poplachů způsobených pohybem zvířete vně nebo uvnitř pozemku (Lukáš, 2011).

Hlavní části obvodové ochrany jsou mechanické zábranné systémy (dále jen MZS) a poplachové zabezpečovací a tísňové systémy (dále jen PZTS) a dohledové videosystémy (dále jen DVS). Efektivitu těchto typů ochrany lze zvýšit například použitím vrcholových zábran, jako jsou ostnaté nebo žiletkové dráty. Dále je možné využít překážky proti podhrabání, například v podobě betonových desek nebo ocelových roštů. K regulaci

průjezdu vozidel a pohybu osob se osvědčují také závory a turnikety (Perimetrická ochrana, 2020).

Ploty a zdi neslouží jen k ohraničení chráněného okolí objektu. Brání nepovolenému vstupu, a také zabráňují nežádoucímu pozorování zvenčí.

Ke zdokonalení ochrany nám může sloužit osvětlení perimetru, které výrazně zvyšuje bezpečnost daného hlídaného objektu a může být využito různými způsoby. Stálé osvětlení poskytuje nepřetržité světlo po celou noc, což odrazuje potenciální narušitele a zvyšuje viditelnost pro bezpečnostní kamery a ostrahu. Osvětlení na pohyb se aktivuje pouze při detekci pohybu, což šetří energii a zároveň upozorňuje na přítomnost osoby v blízkosti perimetru. Tento typ osvětlení může být obzvláště účinný v kombinaci s alarmy nebo kamerovými systémy. Kombinované osvětlení spojuje stálé osvětlení s osvětlením na pohyb, čímž poskytuje základní úroveň osvětlení po celou noc a zvýšenou intenzitu světla při detekci pohybu. Použití různých typů osvětlení může výrazně zvýšit bezpečnost perimetru a odradit potenciální narušitele (Introduction to Physical Security Student Guide, 2017).

Osvětlení je jedním z nejúčinnějších a nejlevnějších způsobů, jak předcházet trestné činnosti. Výzkumy ukazují, že existuje silná souvislost mezi úrovní osvětlení a mírou kriminality nebo strachem z ní (Fennelly, Perry 2016).

Ochrana plášťová – efektivní plášťová ochrana je výsledkem pečlivého plánování a integrace různých technologií a materiálů, které společně vytvářejí neprostupnou bariéru proti možným hrozbám. Tento druh ochrany, jak název napovídá, se aplikuje na vnější části budovy. Kombinace bezpečnostních opatření, která jsou zde použita, brání nezákonnému vstupu do objektu. Mezi tyto prvky patří okna, dveře, zámkové systémy, střechy, mříže a bezpečnostní fólie (Lukáš, 2011).



Obrázek 1 Pyramida bezpečnosti

(zdroj: ROSTEX, b. r.)

Ochrana prostorová – je bezpečnostní opatření zaměřené na detekci a prevenci neoprávněného pohybu uvnitř chráněného prostoru. Tento typ ochrany využívá různé technologie, jako jsou pyroelektrické senzory, ultrazvukové senzory, infračervené závary a mikrovlnné detektory, které monitorují pohyb a aktivitu v dané oblasti. Prostorová ochrana je často využívána v kombinaci s perimetrickou a plášťovou ochranou, aby poskytla víceúrovňový bezpečnostní systém, který chrání jak vnější, tak vnitřní části objektu (Prostorová ochrana, b.r.).

Ochrana předmětová – soustředí se na ochranu konkrétních věcí nebo citlivých informací před neautorizovaným přístupem, krádeží nebo poškozením. Tento typ ochrany většinou doplňuje výše uvedené typy ochrany. Patří sem trezory, skříně na zbraně, kartotéky i obyčejný šuplík. Podle druhu chráněného předmětu či stupně utajení UI volíme typ schránky. Ke zlepšení úrovně zabezpečení, můžeme prvky předmětové ochrany vylepšit instalací přídatných elektronických komponentů. Ty mohou detekovat jakýkoli pokus o jejich odnesení nebo manipulaci s nimi. Tento systém napojený na PZTS okamžitě hlásí jakékoli podezřelé aktivity, čímž zvyšuje úroveň zabezpečení (Janovský, 2022).

3.2 Poplachový zabezpečovací a tísňový systém

Poplachový a tísňový zabezpečovací systém je standardní součástí elektronického zabezpečení objektů. Je navržen tak, aby spolehlivě detekoval neoprávněné vniknutí, porušení obvodového pláště nebo pokus o násilné otevření vstupů. Celý systém tvoří navzájem propojené prvky fungující v reálném čase, detektory zaznamenávají narušení, ústředna provádí jejich vyhodnocení a podle nastavení spouští reakci. Systém může být propojen s DVS, což umožňuje vizuální ověření události. Podle umístění a funkce se komponenty dělí na prvky plášťové ochrany, zabezpečující vstupy a stavební otvory, a prvky prostorové ochrany, monitorující pohyb v interiéru budovy.

Důležité je také členění PZTS do zón a podsystémů, což je podstatné pro návrh a implementaci těchto systémů. Základní informace o zajištění ostrahy a režimových opatření jsou stěžejní pro návrh rozmístění prvků PZTS, včetně výběru vhodných komponent, konfigurace a způsobu ovládání. Technické prostředky v souvislosti s ochranou UI zahrnují bezpečnostní prvky, které zabraňují, ztěžují, oznamují nebo zaznamenávají narušení zabezpečení objektu, zabezpečené oblasti nebo jednacích oblastí, a také zařízení určená k ničení UI (Valouch, 2019).

3.3 Dohledový videosystém

Dohledové videosystémy představují jeden z nejrozšířenějších prvků ochrany objektů a areálů. Hlavním účelem těchto systémů je monitorování, detekce, zaznamenávání událostí, identifikace osob a podpora vyšetřování trestných činů či přestupků. Moderní videosystémy umožňují online sledování prostoru a současné ukládání obrazového materiálu na pevné disky pro následné vyhodnocení. Technická struktura zahrnuje kamery, hardware (např. záznamová zařízení, servery) a software pro správu a analýzu dat. Systémy lze dále rozšířit o mikrofony, reproduktory či další senzory dle specifických požadavků ochrany. Kamery mohou působit i preventivně, neboť jejich samotná přítomnost snižuje pravděpodobnost protiprávního jednání. Vlastní návrh a instalace systému závisí na charakteru chráněného objektu, jeho rozloze a bezpečnostních prioritách. Z technologického hlediska se DVS dělí na tři základní typy: analogové, digitální a hybridní. Výběr konkrétního řešení závisí na požadavcích na kvalitu obrazu, možnosti integrace a rozsahu systému (Valouch, 2019, Lukáš, 2011).

V rámci fyzické ochrany vojenských objektů představují DVS nástroj pro zajištění nepřetržitého monitorování perimetru i vnitřních zón. Na rozdíl od civilních instalací je jejich provoz ve vojenském prostředí vázán na přísnější technické a bezpečnostní požadavky, včetně vyšší odolnosti vůči klimatickým vlivům, zajištění provozu za podmínek výpadku energie a zvýšené úrovně zabezpečení přenášených a uchovávaných dat. Kamery jsou strategicky rozmístěny pro pokrytí přístupových cest, kontrolních stanovišť, muničních skladů a dalších klíčových prvků infrastruktury. Integrace kamerového systému s dalšími prvky, např. PZTS, senzory pohybu nebo přístupovým systémem umožňuje vytvářet komplexní bezpečnostní architekturu, která je schopna reagovat v reálném čase a podle předem definovaných scénářů.

3.4 Elektronická požární signalizace

Elektronická požární signalizace (dále jen EPS) představuje automatizovaný systém, jehož primárním účelem je včasné rozpoznání vznikajícího požáru, rychlé vyhlášení poplachu a aktivace opatření směřujících k omezení šíření požáru. V prostředí vojenských objektů, kde se často nachází hořlavé materiály, výbušniny či zbraně, hraje EPS zásadní roli v prevenci katastrofických škod. Systém je navržen tak, aby zajišťoval bezpečnost osob, chránil kritickou infrastrukturu a minimalizoval narušení operační činnosti. EPS se skládá z řídicí ústředny, automatických detektorů (např. kouřových, teplotních, plamenných),

ručních tlačítkových hlásičů a signalizačních prvků (sirény, majáky). Hlásiče jsou rozmístěny v zájmových částech objektu a trvale komunikují s ústřednou prostřednictvím monitorovaných smyček. Systém nepřetržitě sleduje svůj provozní stav a v případě jakékoli závady okamžitě informuje obsluhu. Aktivace poplachu může spustit další bezpečnostní mechanismy, jako je automatické uzavření protipožárních dveří, odpojení elektrických rozvodů, spuštění evakuačních signálů nebo aktivaci hašení (TZB-info, c 2001-2025).

3.5 Ostraha

Ostraha představuje fyzickou přítomnost strážců, kteří zajišťují bezpečnost a ochranu osob, majetku nebo objektů. Tyto osoby mohou být zaměstnanci státních složek, jako je policie, armáda, nebo pracovníci soukromých bezpečnostních agentur. Jejich hlavním úkolem je prevence a reakce na bezpečnostní incidenty, poškození, vandalismus nebo zneužití. Příslušníci ostrahy provádějí pravidelné obchůzky, monitorují okolí, kontrolují přístup a sledují bezpečnostní kamery. V případě incidentu okamžitě zasahují a informují příslušné odpovědné osoby (Ostraha majetku a osob – koncese krok za krokem, c 1997-2025).

Ostraha je nepřetržitě zajišťována u objektů, které obsahují zabezpečené oblasti kategorie „Důvěrné“ a vyšší. Pro oblasti kategorie „Důvěrné“ je vyžadována přítomnost alespoň jedné osoby, která může rychle reagovat na poplachové hlášení technických prostředků. U oblastí kategorie „Tajné“ musí být přítomna alespoň jedna osoba u objektu a další osoba, která je schopna rychlého zásahu na základě poplachového hlášení technických prostředků. Pro oblasti kategorie „Přísně tajné“ je vyžadována přítomnost alespoň dvou osob (Valouch, 2019).

3.6 Režimová opatření

Režimová opatření patří spolu s ostrahou a technickými prostředky do opatření fyzické bezpečnosti. Určují pravidla pro vstup/výstup osob a vjezd/výjezd vozidel do objektu, přístup do zabezpečených a jednacích oblastí, kontrola těchto oprávnění a manipulaci s klíči a identifikačními prostředky. Zahrnují také dohled nad technickými prostředky, kontrolu pohybu osob a regulaci vynášení UI. Rozsah využití režimových opatření a technických prostředků pro zabezpečení technického zařízení určuje odpovědná osoba nebo jí pověřený zástupce na základě hodnocení rizik.

Zahrnuje zejména:

- **Vstup/vjezd** – oprávnění ke vstupu do zabezpečených oblastí uděluje odpovědná osoba nebo její pověřený zástupce. Osoby s tímto oprávněním musí splňovat podmínky pro přístup k UI. Ti, kteří oprávnění nemají, mohou vstupovat pouze s doprovodem oprávněné osoby, pokud je to nezbytné a neohrozí to ochranu UI. Na vstupu do objektů se provádí kontrola a evidence návštěv. V případě objektů kategorie Přísně tajné se navíc kontroluje přítomnost nebezpečné látky nebo předmětů za pomoci rentgenu.
- **Klíče a identifikace** – manipulace s nimi zahrnuje jejich označování, přidělování, úschovu a evidenci. Klíče a identifikační prostředky k zabezpečeným oblastem (dále jen ZO) a úschovným objektům (dále jen ÚO) musí být označeny a odpovědná osoba stanoví pro manipulaci s nimi pevná pravidla. V době nepřítomnosti osoby s povolením samostatného vstupu, musí být ZO a ÚO uzamčeny. Ztrátu klíčů a identifikačních prostředků je nutné okamžitě nahlásit odpovědné osobě, která zajistí nápravu (Česko, 2005b).

Dodržování režimových opatření stanovených odpovědnou osobou je podstatné pro ochranu UI v souladu se zákonem. Minimalizuje se riziko neoprávněného přístupu nebo vyzrazení citlivých informací, což je důležité pro ochranu zájmů České republiky.

4 IDENTIFIKACE, ANALÝZA A HODNOCENÍ RIZIK

Metody analýz rizik jsou důležitým nástrojem pro identifikaci a hodnocení nejistot, které mohou ovlivnit různé oblasti lidské činnosti. Využívají se v mnoha disciplínách, od řízení projektů a financí až po bezpečnostní analýzy a inženýrství. Obecně lze metody rozdělit na kvalitativní a kvantitativní přístupy, přičemž každý z nich má své specifické výhody i omezení. Zatímco kvalitativní metody se zaměřují na expertní posouzení a subjektivní hodnocení rizik, kvantitativní přístupy pracují s číselnými daty a matematickými modely. V praxi se často kombinují různé metody, aby bylo dosaženo co nejpresnějších a nejrelevantnějších výsledků.

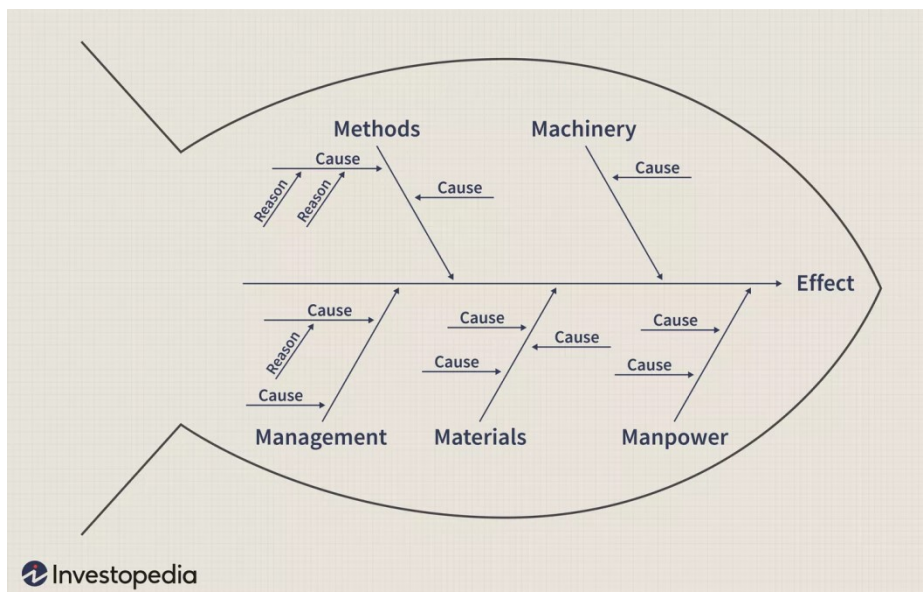
V této bakalářské práci bude využita kombinace Ishikawa diagramu a kvalitativního hodnocení rizik jako nástrojů pro identifikaci a analýzu příčin možných bezpečnostních rizik. Cílem práce pak bude hodnocení rizik zabezpečení zvoleného objektu, přičemž Ishikawa diagram umožní systematicky rozčlenit faktory ovlivňující úroveň fyzické bezpečnosti a identifikovat oblasti, které mohou představovat hrozbu. Na základě těchto výsledků bude provedeno kvalitativní hodnocení rizik, které podrobněji zhodnotí zejména oblasti s největším rizikem a možné scénáře vzniku rizikových událostí a jejich důsledky. Výstupy obou analýz poslouží jako podklad pro návrh opatření ke zvýšení bezpečnosti objektu.

4.1 Ishikawa diagram

Známý také jako diagram rybí kosti nebo diagram příčin a následků, slouží k vizualizaci příčin vedoucích k určité události. Diagram je založen na jednoduché kauzalitě, každý problém má svou příčinu nebo kombinaci příčin. V 60. letech 20. století ho vyvinul univerzitní profesor Kaoru Ishikawa, původně pro kontrolu kvality v loděařském průmyslu. Graf připomíná rybí kostru – hlavní páteř vede k problému, zatímco žebra představují jednotlivé příčiny. Analýza obvykle zahrnuje šest M: pracovní sílu, stroje, metody, materiály, měření a okolní podmínky (matku přírodu). Jeho hlavním přínosem je systematická identifikace faktorů ovlivňujících výsledek, což managementu pomáhá zaměřit se na hlavní problémy a navrhnout vhodná opatření. Je flexibilní a jeho strukturu lze přizpůsobit konkrétním potřebám. Nevýhodou je, že neposkytuje informace o závažnosti jednotlivých problémů, což může vést k nesprávnému stanovení priorit. Navíc je interpretace diagramu subjektivní, což může vést k rozdílným názorům mezi manažery (Ishikawa Diagram, 2023).

Díky své všestrannosti se Ishikawa diagram používá nejen při hledání příčin nekvality v oblasti výroby, ale také při identifikaci rizik a řešení problémů. Tento přístup pomáhá identifikovat nejen zjevné příčiny, ale i skryté faktory, které mohou přispívat k problému. Díky tomu je možné navrhnout efektivní opatření k jejich odstranění a zlepšení procesů. V kontextu ochrany utajovaných informací může metoda 6M pomoci identifikovat a analyzovat různé aspekty, které ovlivňují bezpečnostní rizika.

- **Metody** – zahrnuje výrobní a podpůrné procesy nezbytné k vytvoření výstupu nebo dodání služby. Je důležité zvážit, zda procesy neobsahují příliš mnoho kroků, které nepřispívají k efektivitě systému.
- **Materiál** – týká se prvků, surovin a spotřebního materiálu. Je nutné zajistit, aby materiály splňovaly nutné specifikace, byly správně označeny a skladovány.
- **Měření** – vyhodnocení, kontrola a fyzikální měření, včetně automatických i manuálních metod.
- **Stroje** – nástroje a zařízení potřebné k produkci výstupu nebo dodání služby. Je důležité posoudit, zda současné stroje splňují požadavky a zda jsou efektivně řízeny pro maximální využití jejich schopností.
- **Matka příroda** – zohledňuje jak ovladatelné, tak nepředvídatelné podmínky prostředí, které mohou ovlivnit procesy. Tento parametr pomáhá organizaci uvažovat o vlivech vnějších i vnitřních faktorů na jejich procesy.
- **Pracovní síla** – osoby nebo pracovní síla, kontroluje odbornost personálu a zajišťuje, že jejich dovednosti odpovídají požadovaným standardům (Morales, 2022).



Obrázek 2 Ishikawa diagram

(zdroj: Investopedia, 2023)

4.2 Hodnocení rizik

Hodnocení rizik je nezbytnou součástí řízení projektů, která umožňuje identifikovat, analyzovat a řídit potenciální rizika, která mohou ovlivnit jeho úspěch. Kvalitativní hodnocení rizik umožňuje stanovit jejich priority na základě závažnosti a pravděpodobnosti výskytu. Zahrnuje hodnocení dopadu rizika na projekt a jeho pravděpodobnosti pomocí škály, například od velmi nízkého po velmi vysoký. Výsledky kvalitativního hodnocení rizik umožňují efektivní alokaci zdrojů a opatření k jejich zmírnění, což přispívá k celkovému zlepšení bezpečnosti objektu (Qualitative risk assessment, c 2025).

V resortu MO ČR je postup při řízení rizik upraven rozkazem ministra obrany č. 20/2015. Tento dokument navazuje na zákon č. 320/2001 Sb., o finanční kontrole a také vychází z mezinárodní normy ČSN ISO 31000, která se zabývá řízením rizik. Jeho cílem je zavést jednotný a srozumitelný způsob, jak s riziky pracovat a jak je včas rozpoznat, vyhodnotit jejich závažnost a přijmout opatření, která pomohou předejít problémům nebo zmírnit jejich dopad. Takový přístup má přispět k lepšímu plnění úkolů v rámci celého resortu obrany.

Proces řízení rizik probíhá ve třech fázích: identifikace a hodnocení rizik, jejich zvládání a následné monitorování. Nejprve se identifikují aktiva a hrozby, hodnotí se zranitelnost a pravděpodobnost jejich dopadu. Rizika jsou rozdělena podle závažnosti

na nízká, střední, vysoká a kritická. Ve fázi zvládnání rizik se přijímají konkrétní opatření, například snížení, přenesení nebo akceptace rizika. Následně se rizika průběžně sledují a vyhodnocuje se účinnost přijatých opatření. Systém stojí na jasně definovaných rolích, například gestor systému řízení rizik, hodnotitel rizik, manažer cíle nebo vlastník aktiva (Česko, 2015).

V oblasti fyzické bezpečnosti se často používá jednodušší třístupňová škála rizik (nízké, střední a vysoké). Tento přístup je přehledný a praktický zejména v provozních situacích, kde je potřeba rychle reagovat a rozhodovat. Přestože se tento způsob může na první pohled lišit od podrobnějších metod používaných v rámci celého rezortu obrany, oba přístupy se dají dobře propojit. Nejzávažnější rizika ve fyzické bezpečnosti odpovídají nejvyšší úrovni závažnosti v obecnějším systému. Díky tomu lze obě škály sladit a používat vedle sebe – například podle toho, v jakém prostředí nebo kontextu se rizika hodnotí. Pro lepší přehled uvádí následující tabulka srovnání mezi oběma přístupy.

Tabulka 1 Porovnání úrovně rizika

Fyzická bezpečnost	Systém MO	Poznámka
Nízké riziko	Nízké riziko	Běžně přijatelné, není nutné zásadní opatření
Střední riziko	Střední riziko	Vyžaduje sledování, možná preventivní opatření
Vysoké riziko	Vysoké + kritické riziko	Vyžaduje zásah; „kritické“ riziko je nejzávažnější forma

(zdroj: vlastní zpracování)

4.3 Dílčí závěr

Přestože teoretická část práce shrnuje základní principy, legislativní požadavky a doporučené přístupy k fyzické ochraně objektů, samotná existence těchto opatření ještě nezaručuje jejich bezchybnou funkčnost v praxi. Technické prostředky mohou být zastaralé, lidský faktor zůstává zranitelným článkem a některá pravidla mohou být obtížně kontrolovatelná nebo dodržována jen formálně. Praktická část se proto zaměřuje na podrobný popis současného stavu zabezpečení konkrétního objektu, přičemž

cílem je odhalit oblasti, které by mohly být potenciálně oslabeny a navrhnout způsoby, jak zvýšit jejich spolehlivost a účinnost.

Například:

- **Lidský faktor** – riziko opakovaného porušování režimových pravidel (např. manipulace s UI a klíči, sdílení přístupových karet).
- **Kontrolní činnosti** – absence pravidelného vyhodnocování funkčnosti bezpečnostních systémů nebo nepravidelné školení zaměstnanců v oblasti bezpečnosti.
- **Nespolehlivost systémů** – využívání starších verzí ústřední PZTS, které již nesplňují moderní standardy vzdálené správy a diagnostiky.
- **Ostraha** – nedůsledná kontrolní činnost při obchůzkách, ztrátě pozornosti a podcenění skutečné hrozby.

II PRAKTICKÁ ČÁST

5 CHARAKTERISTIKA VYBRANÉHO OBJEKTU

Objekty důležité pro obranu státu zahrnují pozemky a stavby s politickým, vojenským nebo ekonomickým významem pro obranu ČR. Patří sem vojenské újezdy a objekty, nemovitosti ve správě MO, stavby k ochraně obyvatel a další strategická zařízení určená vládou. V případě ohrožení státu mohou být některé další objekty prohlášeny za strategické. Přístup do těchto objektů může být omezen či zakázán z důvodu bezpečnosti nebo veřejného zájmu. Vojenské objekty slouží MO, Armádě České republiky (dále jen AČR) a Hradní stráži pro výcvik, ubytování, skladování vojenského materiálu a další účely. Spravuje je MO a musí být ve vlastnictví státu (Česko, 1999).

Ochrana těchto kritických objektů a bezpečnostní rizika s nimi spojená, jsou nezbytnou nutností pro bezpečnost a stabilitu státu. Tato praktická část práce se zaměří na hodnocení rizik stávajícího zabezpečení vybraného objektu a případné navržení vhodnější úrovně ochrany. Bezpečnostní opatření v armádních objektech zahrnují fyzickou ochranu, kybernetickou bezpečnost, monitorovací systémy a kontroly přístupu.

Cílem této práce je poskytnout hodnocení bezpečnostních rizik, navrhnout efektivní opatření pro ochranu citlivých informací a v případě potřeby navrhnout vhodnější řešení bezpečnosti objektu. Bezpečnostní rizika mohou vzniknout nejen v samotném objektu, při denních činnostech v rámci porušení režimových pravidel, ale také závadou na prvcích fyzických bariér či zabezpečovacího systému. Všechna tato vnější a vnitřní rizika a mnohdy jejich kombinace, vyžadují komplexní přístup k jejich identifikaci a řešení.

5.1 Popis areálu a hodnocení objektu

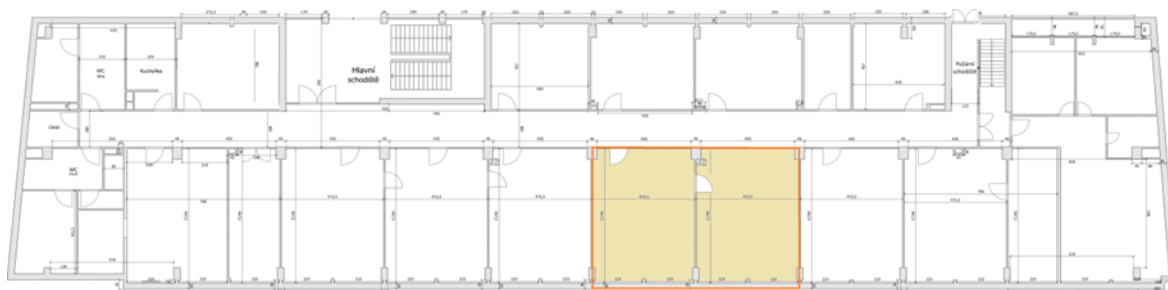
Hodnocený objekt je dislokován v rozsáhlém vojenském areálu na okraji města. V těsné blízkosti areálu se nachází průmyslová zóna s několika výrobními halami, kde probíhá nepřetržitý provoz. Areál má dva vstupy/vjezdy, které slouží k regulovanému přístupu osob a vozidel. Každý z nich je vybaven odpovídajícími bezpečnostními prvky a kontrolními stanovišti, která zajišťují dohled nad pohybem v areálu a minimalizují riziko neoprávněného vniknutí. Areálem prochází páteřní komunikace, pro zajištění plynulého pohybu vozidel a osob. K jednotlivým objektům vedou menší cesty, které umožňují snadný přístup jak pro vozidla, tak i pro chodce. S ohledem na citlivost celého prostoru areálu je nezbytné zajistit víceúrovňovou ochranu, přičemž jedním z nejdůležitějších prvků zabezpečení je perimetrická ochrana.

Perimetrická ochrana je řešena po celém obvodu areálu, kombinací 3 metry vysokého betonového a 2,2 metru vysokého plotu z pletiva, přičemž oba typy jsou vybaveny ostnatým drátem na vrcholu a podhrabovými deskami. Tato kombinace zvyšuje ochranné schopnosti plotu, jejich stabilitu a odrazuje před neoprávněným vniknutím. V této práci nebude dále ochrana perimetru řešena, jelikož se jedná o fyzickou ochranu rozsáhlého objektu, a ta je v gesci velitele dané vojenské posádky.

Hodnocený objekt je výcvikové centrum AČR koncipovaný jako dvoupodlažní budova. V prvním nadzemním podlaží (dále jen 1. NP) se nacházejí kanceláře určené pro stálý personál, které poskytují dostatek prostoru pro administrativní činnosti a zajišťují pohodlné pracovní prostředí. Druhé nadzemní podlaží (dále jen 2. NP) budovy je vybaveno učebnami a tréninkovými místnostmi, které jsou navrženy tak, aby splňovaly specifické potřeby výcviku a vzdělávání. Centrum slouží k výcviku nejen příslušníkům AČR, ale i koaličním partnerům a složkám Integrovaného záchranného systému. K přípravě a výcviku jednotek, velitelů a štábů na různých úrovních velení a také přípravu osob odpovědných za krizové řízení.

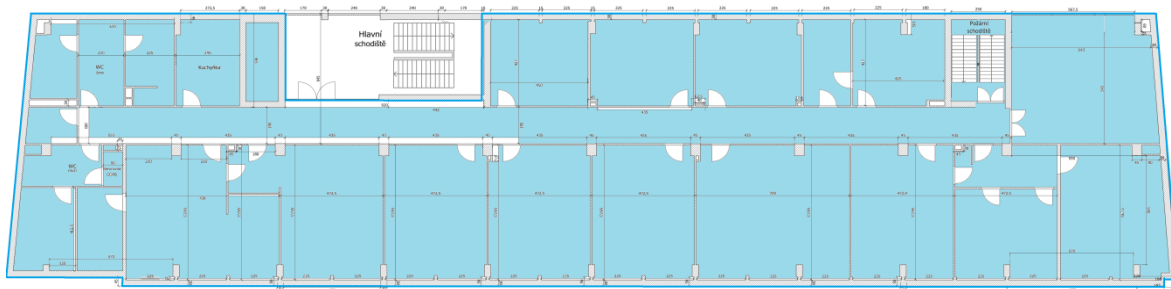
S ohledem na charakter vykonávaných činností, zpracovávaných informací je celé 2. NP objektu zařazeno do režimu stupně utajení „Tajné“ a v prvním patře, dvě místnosti do režimu stupně utajení „Vyhrazené“, ve smyslu zákona č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti. Tato skutečnost zásadně ovlivňuje požadavky na fyzickou ochranu, režimová opatření i personální bezpečnost uvnitř objektu.

Rozdělení objektu podle podlaží, včetně umístění sledovaných místností a zabezpečených zón, je znázorněno na půdorysu prvního a druhého podlaží (Obrázek č. 2 a č. 3).



Obrázek 3 1. nadzemní podlaží – umístění zabezpečených prostor

(zdroj: vlastní zpracování)



Obrázek 4 2. nadzemní podlaží – umístění zabezpečených prostor

(zdroj: vlastní zpracování)

5.2 Plášťová ochrana

Plášťová ochrana budovy představuje druhou úroveň fyzického zabezpečení objektu a jejím hlavním cílem je zabránit neoprávněnému vstupu přímo do prostor budovy. Tato ochrana navazuje na perimetrickou a tvoří podstatnou překážku mezi vnějším prostředím a vnitřními citlivými prostory.

5.2.1 Konstrukční prvky budovy

Budova výcvikového centra je dvoupodlažní objekt zděné konstrukce, který byl v minulosti modernizován s ohledem na současné požadavky provozu. Objekt nemá žádné podzemní podlaží ani sklepní prostory. Střecha je sedlová, nepochůzná a přístupná pouze pro servisní účely, čímž je minimalizována možnost jejího zneužití k neoprávněnému přístupu. Mezi jednotlivými podlažími se nachází hlavní schodiště a jedno požární. Hlavní schodiště slouží pro běžný pohyb osob v rámci objektu a zároveň tvoří jeden z hlavních vstupních bodů do zabezpečené zóny v 2. NP. Požární schodiště je určeno primárně pro nouzovou evakuaci a splňuje příslušné požární bezpečnostní požadavky.

5.2.2 Mechanické zábranné prostředky pláště budovy

V rámci plášťové ochrany jsou tyto prostředky aplikovány především na vstupních a okenních otvorech, které představují pravděpodobná průchodná místa. Vstup do budovy je zajištěn prostřednictvím hlavního vchodu, který tvoří automatické posuvné dveře ovládané přístupovým systémem se čtečkou čipových karet. V pracovní době jsou dveře aktivní pro vstup oprávněných osob, mimo pracovní dobu je vstup zabezpečen pomocí integrovaného zámkového mechanismu a napojením na PZTS. Budova také disponuje požárním vstupem vybaveným dveřmi s panikovým kováním (tzv. panikovým madlem),

kteřé splňují bezpečnostní normy a umožňují rychlý únik v případě nouze. Tyto dveře jsou z vnější strany trvale uzamčeny a nelze je otevřít zvenčí, čímž je zamezen neoprávněnému vstupu. Aktivují se pouze v případě nouze, kdy umožňují únik směrem ven. V případě neoprávněného otevření dveří mimo stav nouze nebo požár je tato událost automaticky zaznamenána systémem PZTS.

Okna budovy jsou plastová, osazená izolačním dvojsklem, které zajišťuje základní úroveň ochrany proti mechanickému poškození. Všechna okna ve 2. NP a dvě okna v patře prvním jsou, vzhledem k požadavkům na fyzickou bezpečnost dle vyhlášky č. 528/2005 Sb., doplněna pevnými kovovými mřížemi. Průlezné otvory, tedy okna, mohou být ponechány bez mechanické zábrany pouze tehdy, pokud se jejich spodní okraj nachází alespoň 5,5 metru nad terénem a zároveň k nim nelze jednoduše proniknout, například pomocí hromosvodů, okapů, terénních nerovností či jiných stavebních prvků. Protože okna v obou nadzemních podlažích tyto podmínky nesplňují a existuje reálné riziko průniku zvenčí, je jejich zabezpečení mřížemi nezbytné. Tím je zajištěno, že objekt splňuje požadavky na fyzickou ochranu podle platných právních předpisů a že jsou dostatečně chráněny prostory, kde se nacházejí UI.

5.2.3 Elektronické zabezpečovací prvky pláště budovy

Elektronické zabezpečovací prvky pláště představují aktivní složku ochrany, která doplňuje MZP a umožňuje včasné rozpoznání pokusu o neoprávněný vstup do budovy. Jejich hlavním cílem je detekovat narušení vnějšího obvodu objektu a předat informaci k dalšímu vyhodnocení a zásahu.

Součástí plášťové ochrany jsou magnetické kontakty, ty jsou instalovány na rámy oken a slouží k detekci pokusu o jejich otevření. Skládají se ze dvou částí, jazýčkového kontaktu, který je umístěn na rámu okna a permanentního magnetu, jenž je připevněn na jejich křídle. V případě oddálení obou částí kontaktu při otevření chráněného prvku je vyslán signál do ústředny systému. Tento nenápadný, ale účinný prvek zajišťuje včasnou detekci pokusu o neoprávněný vstup. Magnetické kontakty jsou umístěny pouze v 2. NP.

Duální detektory tříštění skla jsou umístěny v blízkosti okenních výplní a reagují na specifické frekvence a vibrace, které vznikají při rozbití skla. Pracují na principu detekce akustického signálu nebo změny tlaku vzduchu. Každý z těchto signálů je zpracováván odděleným snímačem, přičemž jeden zachycuje zvuk a druhý změny tlaku v prostoru. Aby byl poplach skutečně vyhlášen, musí být charakteristický impuls

rozbíjeného skla zaznamenán oběma snímači současně. Tím se výrazně snižuje pravděpodobnost falešných poplachů způsobených náhodným hlukem v okolí. Detektory tříštění skla slouží jako doplněk magnetických kontaktů a zvyšují účinnost plášťové ochrany. Těmito detektory jsou zabezpečena všechna okna 2. NP.

5.3 Prostorová ochrana

Prostorová ochrana představuje vnitřní bezpečnostní vrstvu objektu. Jejím hlavním úkolem je zabránit neoprávněnému pohybu osob uvnitř budovy, chránit citlivé prostory a zajistit včasnou detekci a signalizaci jakéhokoliv narušení. V rámci objektu jsou prostory členěny podle míry citlivosti a přístupových oprávnění. Vyšší úroveň prostorové ochrany je aplikována zejména ve 2. NP, které tvoří jednotnou chráněnou zónu ve stupni utajení „Tajné“. Tato zóna začíná již hlavním vstupem do patra a zahrnuje všechny výukové a tréninkové prostory. Vzhledem k citlivosti zde vykonávaných činností zde platí přísnější režim přístupu a podrobnější přehled nad pohybem osob. Naopak v 1. NP, kde se nacházejí místnosti určené pro práci s informacemi stupně utajení „Vyhrazené“, prostorová ochrana z hlediska fyzické bezpečnosti aktuálně řešena není. Tyto prostory jsou zabezpečeny pouze pomocí plášťových, MZP a režimových opatření.

Přístup do těchto prostor je řízen režimovými opatřeními a technologickými prostředky, které lze dále rozdělit na MZP a elektronické zabezpečovací systémy.

5.3.1 Mechanické zábranné prostředky

Mechanické zábranné prostředky představují bariéru, jejímž úkolem je zamezit nebo ztížit neoprávněný vstup do chráněných prostor. To i v případě, kdy dojde k selhání elektronických systémů. V rámci prostorové ochrany tvoří tyto prostředky první vrstvu fyzického zabezpečení uvnitř objektu, zejména na vstupu do režimově chráněných prostor. V objektu jsou aplikovány na vstupech do vybraných místností v 1. NP a dále na přístupech do chráněné zóny ve 2. NP.

V prvním patře jsou většinou instalovány standardní plně dřevěné interiérové dveře. Výjimku tvoří dvě zmíněné místnosti režimového pracoviště, které jsou osazeny bezpečnostními dveřmi splňujícími požadovanou úroveň mechanické ochrany. Tyto dveře jsou vybaveny bezpečnostním kováním a certifikovanou cylindrickou vložkou, zajišťující odolnost proti běžným způsobům překonání (např. odvrtání nebo rozlomení).

Druhé nadzemní podlaží tvoří samostatnou chráněnou zónu ve stupni utajení „Tajné“. Vstup do této zóny je veden přes hlavní schodiště prostřednictvím dvoukřídlých bezpečnostních dveří s elektronickým zámekem, které oddělují režimový prostor od zbytku budovy. Druhý vstup zajišťují bezpečnostní dveře opatřené panikovým kováním, vedoucí na požární schodiště. Všechny tyto dveře jsou instalovány do zesílených zárubní a vybaveny bezpečnostním kováním a cylindrickou vložkou odpovídající požadavkům na fyzickou bezpečnost pro daný stupeň utajení.

Zatímco MZP tvoří pasivní fyzickou překážku proti neoprávněnému vniknutí, elektronické systémy představují aktivní prvek detekce a včasného varování. V další části je proto popsán poplachový zabezpečovací a tísňový systém, který doplňuje fyzickou ochranu objektu o technologické prvky schopné reagovat v reálném čase.

5.3.2 Poplachový zabezpečovací a tísňový systém

PZTS tvoří nedílnou součást elektronické prostorové ochrany objektu. Jeho hlavním úkolem je včasné rozpoznání neoprávněného pohybu, narušení pláště budovy nebo pokusu o násilné vniknutí. Systém se skládá z několika vzájemně propojených prvků, které spolupracují v reálném čase. Detektory zachycují narušení, ústředna vyhodnocuje situaci a podle nastavených parametrů aktivuje výstupní reakci. V případě incidentu dochází ke spuštění poplachu, předání informace obsluze nebo přenosu na pult centrální ochrany (dále jen PCO). Systém může být rovněž napojen na DVS pro vizuální ověření situace. V rámci systému PZTS lze jednotlivé prvky rozdělit podle jejich umístění a funkce na prvky plášťové ochrany, které chrání vstupy do budovy, a prvky prostorové ochrany, které monitorují pohyb uvnitř jednotlivých místností a zón.

Magnetické kontakty jsou instalovány na rámech dveří a slouží k detekci jejich otevření. Skládají se ze dvou částí – jazýčkového kontaktu, který je umístěn na zárubni dveří, a permanentního magnetu, jenž je připevněn na křídle dveří. Pokud dojde k jejich oddálení otevřením, kontakt vyše signál ústředně. Tento jednoduchý a spolehlivý prvek umožňuje včas zaznamenat pokus o vstup do chráněného prostoru.

Vnitřní prostory objektu jsou střeženy pomocí duálních detektorů pohybu, které kombinují infračervený a mikrovlnný senzor. Tato kombinace zajišťuje vyšší spolehlivost detekce a zároveň pomáhá minimalizovat falešné poplachy, které by mohly vznikat např. vlivem změn teploty nebo drobných pohybů v okolí. Detektory jsou schopny rozpoznat skutečný pohyb osoby v prostoru na základě změny tepelného obrazu i pohybu

objektu v elektromagnetickém poli. Pro zvýšení bezpečnosti jsou navíc vybaveny ochranou proti sabotáži, která spustí poplach v případě, že by se někdo pokusil jejich funkci narušit, například zakrytím nebo zaslepením.

V rámci 2. NP, které je zařazeno do stupně utajení „Tajné“, je každý prostor vybaven vlastním detektorem, včetně všech výukových a tréninkových místností. Detektor je instalován také na hlavní chodbě, přičemž jeho umístění, počet detektorů a jejich nasměrování je navrženo tak, aby bylo možné spolehlivě pokrýt celý prostor a včas detekovat pohyb osob mimo stanovený režim.

5.3.3 Elektrická požární signalizace

Důležitou součástí technologického zabezpečení objektu je rovněž EPS, která slouží k včasné detekci požáru a automatickému vyhlášení poplachu. Systém je instalován v celé budově a pomocí detektorů, nepřetržitě sleduje výskyt kouře nebo změny teploty, které by mohly signalizovat vznik požáru. Ovládání a kontrola nad EPS je zajištěna prostřednictvím tabla umístěného přímo v objektu. Systém je také vyvedený ke stálému operačnímu dozoru (dále jen SOD), což je osoba zodpovědná za nepřetržitý dohled a rychlou reakci v případě mimořádné události. V případě požárního poplachu systém automaticky aktivuje evakuační režim, otevření únikových cest a přenáší informaci o události na stanovené místo obsluhy. EPS je provozně oddělena od PZTS, avšak v rámci celkového zabezpečení tvoří jejich kombinace důležitý celek pro ochranu osob i majetku.

5.3.4 Elektronická kontrola vstupu

Systém elektronické kontroly vstupu (dále EKV) je dalším prvkem elektronického zabezpečení, který slouží k řízení, kontrole a evidenci vstupu osob do určených částí objektu. Jeho hlavním účelem je umožnit přístup pouze oprávněným osobám na základě předem definovaných pravidel a přístupových práv. Ve většině případů je identifikace osob prováděna prostřednictvím bezkontaktních identifikačních karet, které uživatelé přikládají ke čtecím zařízením umístěným u vstupních bodů. Systém následně ověří oprávnění osoby na základě zadaných přístupových práv a rozhodne o povolení nebo zamítnutí vstupu. Kromě řízení přístupu může být systém využíván také k evidenci docházky, případně zaznamenávání důvodů odchodu či příchodu. Tím se zvyšuje nejen bezpečnost, ale i přehled o pohybu osob v rámci objektu.

V rámci objektu je přístupový systém využit na dvou místech. První přístupová čtečka je umístěna u hlavního vstupu do budovy a slouží pouze pro vstup. Odchod z budovy je řešen automatickými dveřmi.

Další čtečky jsou instalovány u dveří do chráněného 2. NP, které tvoří samostatnou zabezpečenou oblast. V tomto případě je systém obousměrný. Čtečky jsou osazeny z obou stran dveří a řízení přístupu je aktivní jak pro příchod, tak pro odchod. Díky tomu je zároveň možné vést přehled o počtu přítomných osob v této oblasti, což zvyšuje úroveň kontroly nad pohybem. Čtečky jsou napojeny na elektrický zámek, který umožňuje otevření dveří pouze po úspěšné identifikaci oprávněné osoby. Celý přístupový systém je napájen ze záložního zdroje, který zajišťuje jeho funkčnost i při výpadku elektrické energie. Pro případ celkového výpadku nebo mimořádné události (např. požár) jsou dveře do patra opatřeny panikovým kováním, které umožňuje jejich rychlé otevření směrem ven bez použití karty. Toto řešení odpovídá požadavkům na bezpečný únik osob z budovy.

Pro komplexní správu zabezpečení a přístupu do objektu je využíván systém ASSET, který propojuje softwarové a hardwarové prvky do jednoho funkčního celku. Umožňuje řídit PZTS, EKV a v případě potřeby také další technologie, například EPS, DVS nebo další senzory a prvky. Součástí řešení je také systém LATIS, který slouží jako grafická nadstavba pro přehledné zobrazení a vzdálené řízení bezpečnostních technologií. LATIS umožňuje sledovat stav připojených systémů, zaznamenávat události a v případě potřeby reagovat na poplachové signály. V hodnoceném objektu není systém DVS implementován, ale rozhraní systému ASSET a LATIS umožňuje jeho budoucí integraci. Obsluhu těchto systémů a správu přístupových práv má na starosti odpovědná osoba, zpravidla bezpečnostní manažer objektu, nebo jím pověřená osoba. Ta je proškolená k práci se systémem a odpovídá za jeho nastavení a zajištění provozu.

5.4 Předmětová ochrana

Předmětová ochrana je v hodnoceném objektu zajištěna prostřednictvím certifikovaných trezorů určených pro bezpečné ukládání utajovaných dokumentů a komponent informačních systémů. V současnosti jsou v provozu čtyři trezory různého typu bezpečnostní třídy, a to pro stupeň utajení „Tajné“ (3 trezory) a „Důvěrné“ (1 trezor). Trezory typu „Tajné“ jsou umístěny v určených místnostech 2. NP, trezor nižšího stupně utajení je umístěn v 1. NP, v zabezpečené oblasti „Vyhrazené“. Tím je zajištěna ochrana citlivých informací v souladu s platnými právními normami.

5.5 Ostraha

Ostrahu areálu zajišťuje kombinace příslušníků AČR a civilních zaměstnanců dodavatelské organizace. Pracovníci externí firmy mají na starosti kontrolu vstupních a vjezdových bodů do kasáren, kontrolují povolení ke vstupu osob a vjezdu vozidel. Vydávají jednorázová povolení a provádí jejich evidenci do knihy návštěv. Prostřednictvím nepravidelných obchůzek provádí fyzickou kontrolu perimetru. Po dobu obchůzky jsou vybaveni prostředky pro spojení, telefonem nebo radiostancí. Vojáci z povolání, kteří vykonávají službu stálého operačního dozorcího (osoba odpovědná za dohled nad bezpečností a provozem objektu, která je přítomna 24/7), mají nad činností těchto pracovníků přímou pravomoc a odpovědnost. PZTS hodnoceného objektu je vyveden právě k operačnímu dozorcímu, který má oprávnění k jeho vyhodnocení i případnému zásahu.

Vzhledem k dislokaci stanoviště SOD mimo stanovený objekt se však reakční doba v případě poplachu pohybuje na hranici stanoveného limitu dle vyhlášky. V případě jiného zatížení tak může dojít k prodloužení zásahu, což představuje slabinu současného nastavení.

5.6 Režimová opatření

Vstup do vojenského areálu je povolen pouze oprávněným osobám. Identifikace zaměstnanců je zajištěna prostřednictvím bezkontaktních čipových karet, které slouží ke vstupu jak do areálu, tak do samotného hodnoceného objektu. Vstup probíhá přes vstupní turnikety u hlavního vchodu a jsou monitorovány a evidovány přístupovým systémem. Fyzickou kontrolu vstupu zajišťuje stálá ostraha u hlavní brány, která ověřuje totožnost příchozích a dohlíží na dodržování režimových pravidel. Do hodnoceného objektu, osoby s oprávněním vstupu, vstupují přes čtečku EKV, instalovanou na hlavním vstupu do budovy. Do 2. nadzemního podlaží, které je určeno pro činnosti ve stupni utajení „Tajné“, mají přístup pouze osoby s odpovídajícím osvědčením fyzické osoby. Pro 1. NP platí mírnější režim, avšak přístup do vybraných místností se stupněm utajení „Vyhrazené“ kde je samostatný vstup povolený jen odpovědným osobám. Osoby bez přiděleného oprávnění mohou vstupovat pouze za doprovodu pověřeného pracovníka.

V případě návštěvy (externí technik, servis, kontrola) je nezbytné schválení vstupu vedoucím zaměstnancem. Návštěva se do objektu dostává pouze s doprovodem oprávněné osoby a na základě předem evidované žádosti, která obsahuje identifikační údaje, účel návštěvy a dobu pobytu v objektu. U zahraničních návštěv se postupuje podle

zprísňeného režimu. Veškerá návštěva i vjezd vozidel jsou zaznamenávány a kontrolovány rovněž pracovníky ostrahy, kteří mají k dispozici seznam schválených vstupů.

Pohyb osob je omezen na prostory, ke kterým mají přidělená oprávnění. Mimo pracovní dobu je vstup do objektu možný pouze po předchozím oznámení nadřízené osobě. První příchozí zaměstnanec objekt odstřeží prostřednictvím přístupového systému, poslední odcházející jej opět zabezpečí. Tento postup je elektronicky zaznamenán a navázán na stálý dohled SOD.

Režim manipulace s klíči od zabezpečených oblastí je stanoven tak, aby byla zajištěna jejich ochrana a kontrola použití. Schránku s klíči od těchto prostor si vyzvedává výhradně oprávněná osoba na stanovišti SOD, které se nachází v jiném objektu, a to pouze na nezbytně nutnou dobu. Po ukončení pracovní doby je povinností zaměstnance klíče neprodleně vrátit zpět. Klíče od zabezpečených prostor nesmí být vynášeny mimo areál, a proto jsou po celou dobu uloženy a evidovány právě na stanovišti stálé služby. Schránky na klíče jsou uloženy v elektronické úložně klíčů, jejichž připojení do systému LATIS umožňuje provádět pravidelný audit prováděných úkonů. Tento postup zajišťuje, že přístup k utajovaným prostorům je jednoznačně dohledatelný a řízený v souladu s požadavky na fyzickou ochranu.

V rámci režimových opatření jsou stanovena jasná pravidla pro používání a manipulaci s technickými prostředky v prostorách objektu. Všichni cvičící, návštěvníci i příslušníci stálého stavu jsou povinni při vstupu do 2. NP, uložit všechna záznamová zařízení. Zejména mobilní telefony, chytré hodinky, USB nosiče a další elektroniku, do uzamykatelných schránek, které jsou umístěny u vstupu do této chráněné zóny. Toto opatření má zabránit možnosti neoprávněného pořízení či přenosu citlivých informací.

V celém areálu je dále striktně zakázáno pořizovat jakékoli audiovizuální záznamy. Vytváření audiovizuálních záznamů je možné pouze se souhlasem odpovědné osoby, a to výhradně pro tiskové a informační účely. Platí také zákaz používání soukromých mobilních telefonů ve vybraných místnostech, kde může docházet k manipulaci s UI, a omezení používání přenosných datových nosičů a připojování zařízení k síti. Připojení nového zařízení podléhá schválení a musí být provedeno v souladu s vnitřními pravidly kybernetické bezpečnosti.

5.7 Personální bezpečnost

V hodnoceném objektu jsou uplatňována základní opatření personální bezpečnosti v souladu s požadavky zákona č. 412/2005 Sb. a vyhlášky č. 300/2024 Sb. Přístup k UI je umožněn pouze osobám, kterým bylo vydáno osvědčení fyzické osoby nebo oznámení a byly poučeny. Všichni zaměstnanci pracující s UI jsou pravidelně školeni v oblasti ochrany UI a režimových opatřeních, a to minimálně jednou ročně.

Vedoucí objektu nebo jím pověřená osoba odpovídá za vedení dokumentace o školeních, přidělování přístupových oprávnění a ověřování podmínek personální způsobilosti. V případě ztráty čipové karty je přístup k chráněným oblastem neprodleně zablokován prostřednictvím systému EKV. Při nástupu nových zaměstnanců nebo v případě změny pracovního zařazení je prováděna vstupní poučení včetně podpisu prohlášení o mlčenlivosti. Osoby, které mají jednorázový přístup do chráněných prostor (např. technici), musí být vždy doprovázeny oprávněnou osobou.

5.8 Přehled aplikovaných systémů

Pro lepší přehled o stávajícím zabezpečení objektu a rozdělení jednotlivých ochranných opatření byla sestavena souhrnná tabulka. Ta zachycuje základní bezpečnostní prvky aplikované v rámci areálu i samotného objektu, včetně jejich rozmístění a aktuálního stavu z hlediska požadavků na fyzickou ochranu. Tento přehled zároveň slouží jako výchozí bod pro další analýzu a návrh možných zlepšení v následujících kapitolách.

Tabulka 2 Přehled zajištění fyzické bezpečnosti objektu

Checklist			
Typ ochrany	I. NP	II. NP	Poznámka
Perimetrická ochrana areálu			
Vjezdová a vstupní brána	ANO	ANO	Externí pracovníci ostrahy
Obvodový plot	ANO	ANO	Externí pracovníci ostrahy – pravidelné obchůzky
Kontrola vstupu osob do areálu	ANO	ANO	Externí pracovníci ostrahy

Checklist			
Typ ochrany	I. NP	II. NP	Poznámka
Plášťová ochrana			
Magnetické kontakty na oknech	NE	ANO	Návrh na doplnění v I. NP– záloha ZO
Mříže na oknech	ANO	ANO	
Bezpečnostní dveře vstup do budovy	NE	NE	Dveře posuvné elektronické, doplněny o EKV
Panikové kování	NE	ANO	
Prostorová ochrana			
Duální detektory pohybu	NE	ANO	Návrh na doplnění v I. NP– záloha ZO
Magnety a detektory tříštění skla	NE	ANO	Návrh na doplnění v I. NP– záloha ZO
Mechanické zábranné prostředky			
Bezpečnostní dveře do ZO	ANO	ANO	
Bezpečnostní kování do ZO	ANO	ANO	
Bezpečnostní kování do ZO	ANO	ANO	
Elektronické systémy			
Poplachový zabezpečovací systém (PZTS)	NE	ANO	Vyvedena k SOD
Elektronická požární signalizace (EPS)	ANO	ANO	Vyvedena k SOD
Elektronická kontrola vstupu (EKV)	NE	ANO	
Přístupový software ASSET a LATIS	NE	ANO	
Režimová opatření			
Identifikační karty	NE	ANO	
Evidence návštěv	NE	ANO	

Checklist			
Typ ochrany	I. NP	II. NP	Poznámka
Pravidla pohybu osob	ANO	ANO	
Manipulace s klíči a UI	ANO	ANO	
Ostraha			
Stálý operační dozorcí	ANO	ANO	V areálu
Externí pracovníci ostrahy	ANO	ANO	V areálu
Reakční doba a obchůzky	ANO	ANO	Reakční doba na hranici 5 minut, návrh na ostrahu v objektu

(zdroj: vlastní zpracování)

5.9 Vyhodnocení současného stavu zabezpečení objektu

Na základě provedené charakteristiky objektu a následného kontrolního checklistu jednotlivých druhů zajištění fyzické bezpečnosti lze konstatovat, že většina základních požadavků na fyzickou ochranu objektu je v současnosti naplněna. Zabezpečení odpovídá právním i interním normám pro práci s UI, zejména ve 2. NP, které je zařazeno do stupně utajení „Tajné“. V přízemí jsou vybrané místnosti zařazeny do stupně utajení „Vyhrazené“.

Checklist ukazuje, že perimetrická ochrana areálu je komplexní, kombinující prvky fyzického i režimového zabezpečení. Plášťová ochrana budovy je řešena standardními konstrukčními prvky doplněnými o elektronická a mechanická opatření. Prostorová ochrana je aktivně využívána pouze ve 2. NP. Elektronické zabezpečovací systémy (PZTS, EPS, EKV) jsou aplikovány ve funkčním rozsahu. V rámci režimových opatření a personální bezpečnosti jsou nastavena pravidla, která odpovídají charakteru chráněného prostoru a současným požadavkům na provoz.

Zjištěný stav však rovněž poukazuje na určité rozdíly mezi jednotlivými podlažími, které mohou v budoucnu představovat potenciální slabiny, např. v oblasti prostorové ochrany přízemí nebo omezené možnosti přímého dohledu v blízkosti objektu. Reakční doba ostrahy, kterou zabezpečuje SOD, naplňuje požadavky vyhlášky, ale je na hranici 5 minut od signalizace narušení. V případě řešení jiné mimořádné události, by se mohlo stát, že dojde k prodlení. Toto vyhodnocení slouží jako výchozí podklad pro následující

analýzu rizik a identifikaci hrozeb, jejichž důsledky mohou mít dopad na celkovou bezpečnost objektu i ochranu zpracovávaných informací.

6 ANALÝZA A IDENTIFIKACE BEZPEČNOSTNÍCH RIZIK OBJEKTU

Analýza bezpečnostních rizik představuje zásadní krok při posouzení úrovně ochrany objektu a odhalení slabých míst, která mohou vést k narušení bezpečnosti. Cílem této kapitoly je systematicky identifikovat možné příčiny a důsledky bezpečnostních incidentů, a to jak z pohledu technického, tak i organizačního. K vizuálnímu znázornění a rozboru příčinových vztahů byla využita metoda Ishikawa diagramu.

Identifikovaná rizika byla následně podrobena kvalitativnímu hodnocení, které umožňuje stanovit jejich relativní význam na základě kombinace pravděpodobnosti výskytu a závažnosti dopadu. Výsledné skóre umožňuje určit jeho míru a navrhnout odpovídající opatření ke zmírnění nebo eliminaci konkrétních slabin v systému zabezpečení.

6.1 Analýza hrozeb pomocí Ishikawa diagramu

V rámci této části práce je analyzován současný stav fyzického zabezpečení objektu, zejména v oblastech, které mohou představovat pravděpodobné slabiny nebo významná bezpečnostní rizika s ohledem na charakter objektu a platné požadavky. Identifikované hrozby vycházejí z kombinace provozních zkušeností, platných právních předpisů a požadavků na ochranu UI. Vizuální znázornění hlavních příčin a jejich následků je uvedeno v níže uvedeném Ishikawa diagramu, který slouží jako analytický základ pro návrhovou část, jejímž cílem je formulovat konkrétní a cílená opatření ke zmírnění identifikovaných rizik.

Na základě vytvořeného diagramu příčin a následků narušení bezpečnosti (Příloha 1) byly identifikovány hlavní oblasti, které mohou vést k ohrožení fyzické bezpečnosti nebo úniku UI. Tyto oblasti zahrnují technická selhání, lidský faktor, nedostatky v režimových opatřeních, slabiny v prostorové nebo plášťové ochraně a také rizika způsobená nevhodně řešenou ostrahu.

Z pohledu technické infrastruktury můžeme jako hrozby považovat poruchy nebo výpadky systémů PZTS, EKV a EPS, stejně jako selhání záložních zdrojů napájení. K těmto slabinám může přispět také nedostatečná frekvence funkčních zkoušek nebo špatně nastavená údržba. Dále byly identifikovány případy nefunkčních či chybně

nasměrovaných detektorů nebo překrytí čidel, což může vést k falešným nebo naopak nevyhlášeným poplachům.

V oblasti lidského faktoru může docházet k úmyslnému obcházení systému (např. sdílení přístupových údajů), nedodržení režimu (např. nezastřežení systému, špatná manipulace s klíči, přístup bez oprávnění), nebo neprovádění pravidelných školení zaměstnanců. Závažné dopady může mít i vědomé či nevědomé porušení pravidel manipulace s UI, ať už jde o tisk, skartaci nebo používání nepovolených zařízení.

Z hlediska fyzických opatření se jako slabiny ukázaly například možnosti vniknutí střechními okny nebo rozbitím okenních výplní, záměrné zablokování dveří, nedostatečný přehled o osobách v chráněných zónách či neexistence standardních operačních postupů (dále jen SOP) při incidentu.

V neposlední řadě byla identifikována i slabá místa v oblasti ostrahy. Ať už se jedná o možné nedodržování času obchůzek, pomalou reakci na incidenty, laxní přístup a předem definování poplachů jako „falešné“, které může vést k podcenění skutečných událostí.

6.2 Kvalitativní hodnocení rizik

Následující tabulka shrnuje ohodnocení jednotlivých rizik identifikovaných jako zásadní pro bezpečnost hodnoceného objektu. Tato kategorizace slouží jako výchozí podklad pro návrhovou část, kde budou navržena konkrétní opatření k jejich snížení.

Tabulka 3 Hodnocení míry rizika na základě identifikovaných hrozeb

Hrozba	Pravděpodobnost	Závažnost	Zhodnocení míry rizika
Neoprávněný vstup do objektu	Střední	Vysoká	Vysoké – vyžadující opatření
Nedostatečná evidence a kontrola vstupu do 2. NP	Vysoká	Střední	Vysoké – vyžadující opatření
Chybějící dohled nad zabezpečením mimo pracovní dobu	Střední	Vysoká	Vysoké – vyžadující opatření
Nesprávná manipulace s klíči	Střední	Střední	Střední – vyžadující zlepšení kontroly

Hrozba	Pravděpodobnost	Závažnost	Zhodnocení míry rizika
Nežádoucí chování zaměstnanců a návštěv	Střední	Střední	Střední – vyžadující zlepšení kontroly
Nedodržování režimových pravidel	Střední	Střední	Střední – nutná kontrola dodržování
Porušení plášťové ochrany	Nízká	Střední	Nízké – současný stav považován za vyhovující
Selhání technických prostředků (čidla, ústředna)	Nízká	Střední	Nízké – vyžaduje pravidelné zkoušky
Nedostatečný zásah v případě poplachu	Střední	Vysoká	Vysoké – vyžadující opatření

(zdroj: vlastní zpracování)

Na základě provedeného vlastního hodnocení, kombinace pravděpodobnosti a dopadu. Byly identifikovány bezpečnostní hrozby, které si s ohledem na míru závažnosti a pravděpodobnosti výskytu zasluhují zvláštní pozornost. Tyto hrozby byly označeny jako hrozby vysoké závažnosti a jsou dále rozpracovány formou návrhu konkrétních opatření, která by měla přispět ke zlepšení úrovně fyzické bezpečnosti objektu, efektivnější kontrole vstupu a pohybu osob a ochraně UI.

Nejzávažnější hrozby byly identifikovány v oblastech neoprávněného vstupu do objektu, nedostatečné kontroly pohybu ve 2. NP a nedostatečného zásahu při poplachu. V těchto případech je pravděpodobnost incidentu kombinována s vysokou závažností dopadu, což vyžaduje návrh cílených a efektivních opatření ke zmírnění těchto hrozeb.

Střední úroveň byla přiřazena hrozbám souvisejícím s režimovými opatřeními a lidským faktorem – zejména při manipulaci s klíči, nedodržování interních pravidel či nežádoucím chování osob. Tyto oblasti vyžadují důslednou vnitřní kontrolu a pravidelné proškolení zaměstnanců, aby bylo minimalizováno selhání režimových opatření.

Naopak hrozby spojené s porušením plášťové ochrany nebo technickým selháním byly označeny jako nízké. Současný stav těchto oblastí je považován za vyhovující,

avšak i zde je nutné zajišťovat pravidelné funkční zkoušky, preventivní údržbu a fyzické kontroly pohledem na neporušenost bezpečnostních prvků.

6.3 Závěr analýzy

Na základě kvalitativního hodnocení byla stanovena míra rizika u jednotlivých hrozeb. Hrozby označeny jako vysoce závažné, jsou dále rozpracovány formou návrhu konkrétních opatření, která by měla přispět ke zlepšení úrovně fyzické bezpečnosti objektu, efektivnější kontrole vstupu, pohybu osob a ochraně UI.

7 NÁVRH OPATŘENÍ KE ZVÝŠENÍ ÚROVNĚ FYZICKÉ BEZPEČNOSTI

Analýza bezpečnostních rizik, podpořená metodou Ishikawa diagramu a kvalitativním hodnocením, odhalila několik oblastí, které vykazují zvýšenou míru ohrožení bezpečnosti hodnoceného objektu.

Mezi nejvýznamnější hrozby patří:

- nedostatečná kontrola nad vstupem do objektu a do zabezpečených prostor,
- absence přímé ostrahy v blízkosti objektu,
- omezené možnosti kontroly pohybu osob ve 2. NP,
- nedostatečné nebo ne vždy důsledně uplatňovaná režimová opatření.

Na základě těchto zjištění jsou v následujících podkapitolách navržena konkrétní opatření, která by měla vést ke zdokonalení úrovně ochrany objektu a ke snížení nebezpečí narušení.

7.1 Umístění stálé ostrahy přímo do objektu

Současný způsob zajištění výkonu ostrahy v rámci areálu je postaven na kombinaci činnosti zaměstnanců smluvního poskytovatele a služby SOD, který dohlíží na režimová pracoviště i celkový chod areálu. Ačkoli je deklarovaná reakční doba v souladu s vyhláškou č. 528/2005 Sb. (max. 5 minut), reálně je tento limit plněn s minimální rezervou. V případě paralelního incidentu nebo složitější situace může být zásah zpožděn, což zvyšuje riziko selhání bezpečnostních opatření.

Z provedené analýzy je patrné, že absence přímé fyzické přítomnosti ostrahy přímo u hodnoceného objektu představuje slabé místo, zejména z pohledu okamžité reakce, přehledem nad vstupem osob, vizuální kontroly po pracovní době i posílení režimových opatření. Tyto nedostatky jsou navíc umocněny zvyšujícím se počtem výcvikových aktivit, které vyplývají od zhoršující se bezpečnostní situace v Evropě.

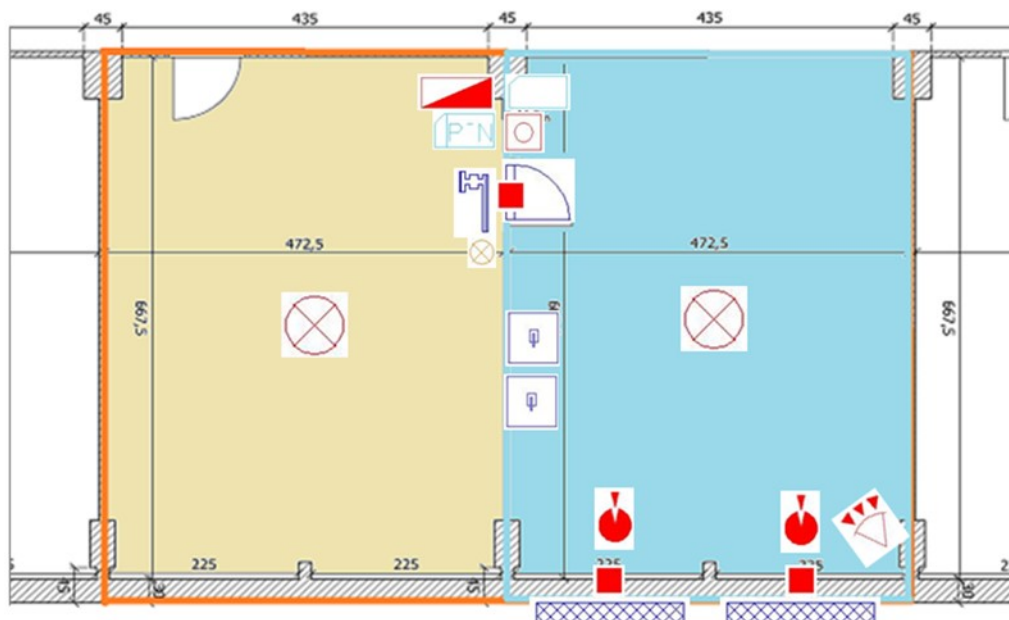
Navrhuje se proto zřízení samostatného stanoviště ostrahy přímo v objektu formou služby dvou vojáků z povolání ve 24hodinových směnách, 7 dní v týdnu. Ostrahu budou vykonávat příslušníci výcvikového střediska. Toto řešení představuje efektivní a hospodárné řešení, které eliminuje potřebu smluvních partnerů. Začlenění vojáků

z povolání do střežení umožňuje optimální využití dostupného personálu, přičemž tito příslušníci jsou již vycvičeni, mají bezpečnostní prověrku a znají vnitřní režim objektu. Zapojením profesionálních vojáků v rámci ostrahy zvyšuje operační připravenost a posiluje celkovou bezpečnost objektu. Umístění ostrahy v objektu (Obrázek č. 5).

Toto opatření by umožnilo:

- Nepřetržitý přehled nad vstupem do objektu, zejména do 2. NP, kde je uplatněna vyšší míra zabezpečení. Ošetřením v režimových pravidlech a směrnicích pro výkon ostrahy, zajistit dohled jedním pracovníkem ostrahy nad příchodem a odchodem cvičících. Tímto se eliminuje neoprávněný přístup do této zóny.
- Dohled nad manipulací s klíči od zabezpečených oblastí. Z hlediska snížení nákladů je navrženo ukládat schránky s klíči přímo u ostrahy způsobem, který umožňuje kontrolu jejich použití. A to zápisem do knihy výdeje schránek s klíči. Možnost ukládání klíčů přímo v objektu, významně usnadní zaměstnancům každodenní provoz. Tímto k nim bude zajištěn neustálý přístup, bez nutnosti docházet na stanoviště SOD, což zefektivní práci a zároveň zvýší pohotovost při řešení mimořádných situací.
- Toto opatření by umožnilo vyvedení PZTS, EPS a EKV na stanoviště ostrahy. Zobrazení pomocí systémů ASSET a LATIS zajistí okamžitou reakci na případné incidenty, poplachové nebo nouzové situace.
- Efektivní reakci v případě mimořádných událostí, například náhlého vstupu neoprávněné osoby nebo včasné zjištění otevřených oken mimo pracovní dobu.
- Vyhodnocování planých poplachů přímo na místě, čímž se zamezí zbytečné aktivaci SOD a zároveň se eliminuje riziko, že v důsledku opakovaných falešných hlášení dojde k podcenění skutečného narušení.

- Zefektivnění ochrany záložních prostředků (dokumenty, duplikátů klíčů), v případě mimořádné události, ztrátě nebo poškození hlavního klíče. Nebo v případě poškození střechy a hrozby zničení UI vodou. V případě odstávky prvků PZTS v 2. NP poslouží k dočasnému ukládání informací.



Obrázek 6 Návrh nové ZO v 1. NP

(zdroj: vlastní)

Legenda prvků:

	Úschovný objekt (trezor)		Tísňový hlásič tlačítkový
	Bezpečnostní dveře		Signalizace optická
	Bezpečnostní uzamykací systém s kováním v provedení knoflík-klika		PIR vějíř
	Ovládání klávesnice EZS		Čidlo rozbití skla
	Terminál bezkontaktní PIN		Magnetické čidlo otevření



Terminál bezkontaktní



Bezpečnostní mříž pevná



Požární signalizace

7.3 Doplnění turniketů ke vstupu do 2. NP

2. NP objektu je vymezeno jako zabezpečená oblast ve stupni utajení „Tajné“. Přístup do této zóny je aktuálně řízen přes bezpečnostní dveře, opatřeny systémem EKV, který vyžaduje identifikaci čipovou kartou při příchodu i odchodu, na základě zadaných práv. Vzhledem k tomu, že zde probíhá výuka a výcvik s vyšší frekvencí pohybu osob, dochází v určitých momentech ke kumulaci osob u vstupu a tím i ke zpomalení plynulosti průchodu. Což může vést k jednání v rozporu s režimovými pravidly, a ne všichni cvičící užijí systém EKV. V mnoha případech dochází k přidržení dveří a cvičící volně prochází. Instalace dvojice turniketů u vstupu by přispěla k plynulejšímu a efektivnějšímu pohybu osob, a to při zachování všech bezpečnostních požadavků. Turnikety zajistí, že do chráněné zóny vstupují pouze osoby s oprávněním, přičemž každý průchod bude elektronicky zaznamenán. Díky obousměrnému snímání bude zachována evidence aktuálního počtu přítomných osob v zabezpečené oblasti, což přispívá nejen k bezpečnostní kontrole, ale také k evakuačním a krizovým postupům.

Navržené řešení tak přispívá k/ke:

- Zrychlení, plynulosti a zefektivnění vstupu. Možnost průchodu více než jedné osoby zároveň za použití EKV.
- Vyšší míře kontroly a evidence přítomnosti osob.
- Minimalizaci rizika neautorizovaného průchodu, znemožnění průchodu více osob na jedno načtení přes EKV.

Navržená opatření reagují na nejzásadnější zjištěná rizika a slabiny systému fyzické bezpečnosti, která byla identifikována v předchozí analýze. Zaměřují se na posílení ochrany v oblasti vstupu do objektu, zpřísnění přístupového režimu do zabezpečených zón a optimalizaci pohybu osob uvnitř budovy. Zřízení stanoviště ostrahy přímo v hodnoceném objektu umožní nejen rychlejší reakci v případě incidentu. Ale i lepší kontrolu nad vstupem do objektu, kontrolu při manipulaci s klíči a celkovým

bezpečnostním režimem. Rozšíření zabezpečení ZO v 1. NP a její navýšení na stupeň utajení „Tajné“. Přispívá k rozšíření kapacity pro bezpečné ukládání dokumentů a duplikátů klíčů od 2. NP. Zavedení turniketového systému zajistí plynulejší průchod a přehled o pohybu osob v režimové části objektu. Uvedené návrhy jsou navrženy s ohledem na reálné provozní potřeby a organizační možnosti objektu. Předpokládá se jejich proveditelnost z technického i ekonomického hlediska, přičemž jejich realizace by měla přinést znatelné posílení celkové bezpečnostní úrovně pracoviště a zároveň zjednodušit vnitřní provoz a zvýšit komfort zaměstnanců. Efektivita navržených technických a organizačních opatření je však podmíněna i důsledným dodržováním stanovených režimových pravidel a pravidelným školením všech osob s přístupem do objektu. Tato školení jsou standardně prováděna jednou ročně, avšak je nezbytné realizovat je i mimořádně. Zejména v případech, kdy dojde k porušení ochrany UI, nesprávné manipulace s ní nebo nedodržování režimových opatření.

7.4 Finanční plán zavedení bezpečnostních prvků

Na základě návrhové části byly identifikovány konkrétní prvky a opatření, jejichž zavedení povede ke zvýšení úrovně fyzické bezpečnosti hodnoceného objektu. Pro ilustraci finanční náročnosti byla vypracována orientační kalkulace, která vychází z reálných cenových podkladů. Ceny technických prostředků byly poskytnuty společností Trade FIDES, a.s., která se specializuje na návrh a realizaci bezpečnostních systémů a dlouhodobě spolupracuje s AČR.

Kalkulace představuje pouze návrhový rozpočet a může se lišit v závislosti na rozsah realizace nebo technickém řešení napojení jednotlivých prvků. Přesto může sloužit jako užitečný přehled nákladů potřebných k dosažení vyšší míry zabezpečení objektu a ke splnění navržených opatření.

Tabulka 4 Návrh rozpočtu

P. č.	Název prvku	Typ	Ks	Cena za jednotku	Celková cena	Poznámka
1	Akustický detektor tříštění skla	AD-800AM	1	2 941 Kč	2 941 Kč	

P. č.	Název prvku	Typ	Ks	Cena za jednotku	Celková cena	Poznámka
2	Magnetický kontakt čtyřdrátový	MAS 303	3	357 Kč	1 071 Kč	
3	Duální detektor	Prestige AMDT	1	1 650 Kč	1 650 Kč	Detektor pohybu
4	Klávesnice pro ovládání systému	KMU 4	1	4 100 Kč	3 870 Kč	Ovládání ústředn ASSET
5	Tísňové tlačítko	ART 476	1	673 Kč	673 Kč	
6	Čtečka bezkontaktních karet	ARC 301	1	1 540 Kč	1 540 Kč	Karta + PIN
7	Čtečka bezkontaktních karet	ARC 301	1	1 320 Kč	1 320 Kč	Karta
8	El. zámek dveří	BEFO 1221	1	2 900 Kč	2 900 Kč	Momentový kolík
9	LED signalizace	LED 310	1	310 Kč	310 Kč	
10	Ústředna PZTS		1	26 500 Kč	26 500 Kč	
11	Záložní zdroj	PWR 533	1	7 600 Kč	7 600 Kč	
12	Ostatní komponenty				3 500 Kč	Modul, opakovač
13	Systém ASSET	HW, SW licence			56 500 Kč	

P. č.	Název prvku	Typ	Ks	Cena za jednotku	Celková cena	Poznámka
14	Systém LATIS	SW, licence			28 000 Kč	
15	Kabeláž, ostatní materiál				36 000 Kč	
16	Turniket	Speedgate DNG	2	100000	200 000 Kč	
17	Práce				93 000 Kč	
18	Doprava				14 000 Kč	
19	celkem				481 375 Kč	

(zdroj: vlastní zpracování)

Navržená opatření představují sice vyšší investici, ale jsou plně odůvodněna vzhledem k identifikovaným hrozbám. Náklady spojené s vyvedením systému PZTS a EPS na stanoviště ostrahy, pomohou k výraznému zkrácení doby reakce na poplachy a zlepší dohled nad objektem. Zavedení fyzické přítomnosti ostrahy v budově navíc umožní přímou kontrolu přístupů a režimových pravidel.

Technická opatření, jako doplnění detekčních prvků nebo turniketů, reagují na konkrétní slabiny. Vzhledem k tomu, že ostrahu zajistí vlastní personál, odpadá potřeba externí služby, což návrh činí ekonomicky udržitelným. Celkové náklady tak odpovídají závažnosti rizik a přinášejí přiměřené zvýšení úrovně zabezpečení objektu.

ZÁVĚR

Cílem této bakalářské práce bylo provést komplexní analýzu fyzické bezpečnosti vybraného vojenského objektu, identifikovat případné slabiny a navrhnout efektivní opatření ke zvýšení úrovně jeho ochrany. V teoretické části byly představeny základní pojmy související s fyzickou bezpečností, příslušná legislativa a prostředky ochrany využívané v praxi. Praktická část následně aplikovala tyto poznatky na konkrétní objekt. Pomocí nástrojů, jako je Ishikawa diagram a kvalitativní metoda hodnocení rizik, byly určeny hlavní problematické oblasti, které mohou ohrozit bezpečnost objektu či vést k úniku UI.

Na základě zjištěných skutečností byly formulovány konkrétní návrhy ke zlepšení. Například zavedení stálé ostrahy přímo do budovy, doplnění prostorové ochrany v prvním podlaží, vyvedení bezpečnostních systémů k ostraze, posílení kontrolních prvků přístupového systému formou turniketů na vstupu do druhého patra. Součástí návrhů je také důraz na personální a režimová opatření, zejména na průběžné školení zaměstnanců a cvičících. Přestože navrhovaná opatření představují jistou finanční zátěž, odpovídají vysokým nárokům kladeným na práci s utajovanými informacemi a zajištění bezpečnosti v dynamicky se měnícím bezpečnostním prostředí. V tomto ohledu lze investice vnímat jako nezbytné a dlouhodobě přínosné.

Navržené úpravy nejen zvyšují úroveň ochrany samotného objektu, ale také přispívají k větší komfortnosti provozu a zajištění kontinuity činnosti bez zbytečných rizik a komplikací. Výsledky práce tak mohou sloužit jako podklad pro reálnou modernizaci zabezpečení a zároveň jako metodický rámec pro posouzení dalších objektů s obdobným využitím.

SEZNAM POUŽITÉ LITERATURY

ČESKO, 1998. Ústavní zákon č. 110/1998 Sb. ze dne 29. května 1998, o bezpečnosti České republiky. In: *Zákony pro lidi* [online]. [cit. 2025-02-24]. Dostupné z: <https://www.zakonyprolidi.cz/cs/1998-110>

ČESKO, 2005a. Zákon 412/2005 Sb. ze dne 21. září 2005, o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. Online. In: *Sbírka zákonů České republiky*. 2005, částka 143. [cit. 2025-02-23]. Dostupné z: <https://www.nbu.cz/cs/pravni-predpisy/1089-zakon-c-4122005/>.

ČESKO, 1999. Zákon 222/1999 Sb. ze dne 12. října 1999, o zajišťování obrany České republiky. Online. In: *Sbírka zákonů České republiky*. 1999, částka 76. [cit. 2025-02-23]. Dostupné z: <https://www.zakonyprolidi.cz/cs/1999-222/zneni-20250306>.

ČESKO, 2024a. Nařízení vlády č. 440/2024 Sb. ze dne 18. prosince 2024, ve znění pozdějších předpisů. Online. [cit. 2025-02-23]. Dostupné z: <https://www.nbu.cz/cs/pravni-predpisy/provade-ci-pravni-predpisy/1080-narizeni-vlady-c-5222005/>.

ČESKO, 2015. Ministerstvo obrany ČR, 2015. *Řízení rizik v rezortu Ministerstva obrany: rozkaz ministra obrany č. 20/2015, ve znění pozdějších předpisů*. In: Ministerstvo obrany. [online]. [cit. 2025-02-23] Dostupné z: https://www.mocr.army.cz/assets/informacni-servis/zpravodajstvi/rmo_20_2015_rizeni_rizik.pdf

ČESKO, 2023. Normativní výnos Ministerstva obrany ze dne 14. srpna 2023, *Fyzická bezpečnost v rezortu Ministerstva obrany*. In: *Věstník MO*. 2023, částka 12.

ČESKO, 2002. Vyhláška č. 275/2002 Sb. ze dne 14. září 2002, o administrativní bezpečnosti a o registrech utajovaných informací, ve znění pozdějších předpisů. Online. [cit. 2025-02-23]. Dostupné z: <https://www.nbu.cz/cs/pravni-predpisy/provade-ci-pravni-predpisy/1087-vyhlas-ka-c-2752002/>.

ČESKO, 2024b. Vyhláška č. 300/2024 Sb. ze dne 7. října 2024, o personální bezpečnosti a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. Online. [cit. 2025-02-23]. Dostupné z: <https://www.nbu.cz/cs/pravni-predpisy/provade-ci-pravni-predpisy/1087-vyhlas-ka-c-3002024/>.

ČESKO, 2005b. Vyhláška č. 528/2005 Sb. ze dne 14. prosince 2005, o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů. Online. [cit. 2025-02-23]. Dostupné z: <https://www.nbu.cz/cs/pravni-predpisy/provade-ci-pravni-predpisy/1087-vyhlaska-c-5282005>

ČESKO, 2005c. Příloha č. 1 k vyhlášce č. 528/2005 Sb., 2005. In: Národní bezpečnostní úřad [online]. [cit. 2025-02-23]. Dostupné z: <https://www.nbu.cz/cs/pravni-predpisy/provade-ci-pravni-predpisy/1087-vyhlaska-c-5282005/>

FENNELLY, Lawrence J., 2016. *Effective Physical Security*. 5th edition. Amsterdam: Elsevier. ISBN 978-0-12-804462-9.

FENNELLY, Lawrence J. a PERRY, Marianna A. *Physical Security: 150 Things You Should Know*. 2nd Edition. Amsterdam: Elsevier, 2016. ISBN 978-0-12-809487-7.

Introduction to Physical Security Student Guide, 2017. In: <https://www.cdse.edu/> [online]. [cit. 2025-02-25]. Dostupné z: <https://www.cdse.edu/Portals/124/Documents/student-guides/PY011-guide.pdf>.

Ishikawa Diagram, 2023. Investopedia [online]. [cit. 2025-02-27]. Dostupné z: <https://www.investopedia.com/terms/i/ishikawa-diagram.asp>.

JANOVSKÝ, Dušan, 2022. *Předmětová ochrana objektů* [online]. Zlín [cit. 2025-02-26]. Dostupné z: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://digilib.k.utb.cz/bitstream/handle/10563/51179/janovsk%C3%BD_2022_dp.pdf?sequence=-1&isAllowed=y. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně.

LUKÁŠ, Luděk, 2011-. *Bezpečnostní technologie, systémy a management: [teorie a praxe ochrany majetku a fyzické bezpečnosti]*. Zlín: VeRBuM. ISBN 9788087500057. MINISTERSTVO VNITRA ČESKÉ REPUBLIKY, c 2025. Pojmy. Online. Ministerstvo vnitra České republiky. [cit. 2025-02-12]. Dostupné z: <https://mv.gov.cz/clanek/riziko.aspx>.

MORALES, Jane, 2022. *6M Fishbone Analysis: Diagram Definition, Explanation, and Template*. In: MindOnMap [online]. [cit. 2025-03-02]. Dostupné z: <https://www.mindonmap.com/cs/blog/6m-method/>.

Národní bezpečnostní úřad [online], 2025. [cit. 2025-02-23]. Dostupné z: <https://www.nbu.cz/cs/ochrana-utajovanych-informaci/fyzicka-bezpecnost-technicke-prostredky-a-dalsi-prvky-fyzicke-bezpecnosti-a-jejich-certifikace/1014-informace/>.

Obecně k personální bezpečnosti, c 2025. In: Národní bezpečnostní úřad [online]. [cit. 2025-02-27]. Dostupné z: <https://www.nbu.cz/cs/ochrana-utajovanych-informaci/personalni-bezpecnost-oznameni-pro-v-osvedceni-d-t-pt-certifikaty/1043-obecne-k-personalni-bezpecnosti/>.

Ostraha majetku a osob – koncese krok za krokem, c 1997-2025. In: BusinessInfo.cz [online]. [cit. 2025-03-02]. Dostupné z: <https://www.businessinfo.cz/navody/ostraha-majetku-a-osob/>.

Perimetrická ochrana. Z čeho se skládá a kdy je vhodná?, 2020. *Securitas* [online]. [cit. 2025-02-24]. Dostupné z: <https://www.securitas.cz/novinky--blog/blog/perimetricka-ochrana-z-ceho-se-sklada-a-kdy-je-vhodna/>.

PROCHÁZKOVÁ, Dana, 2011. *Analýza a řízení rizik*. Praha: České vysoké učení technické v Praze. ISBN 978-80-01-04841-2.

Prostorová ochrana, b. r. In: <https://www.prumyslovkaliberec.cz/> [online]. [cit. 2025-02-25]. Dostupné z: https://www.pslib.cz/jiri.kubin/ELZ/03_20Perimetricka_20plastova_20prostorova_20predmetova_20ochrana.pdf.

Pyramida bezpečnosti, b. r. In: ROSTEX [online]. [cit. 2025-03-20]. Dostupné z: <https://www.rostex.cz/pyramida-bezpecnosti.html>

Qualitative risk assessment, c 2025. In: *Project Management Institute* [online]. [cit. 2025-03-25]. Dostupné z: <https://www.pmi.org/learning/library/qualitative-risk-assessment-cheaper-faster-3188>

SMEJKAL, Vladimír a RAIS, Karel, 2010. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, 2010. ISBN 978-80-247-3051-6.

ŠČUREK, Radomír, 2021. Základy bezpečnostní politiky. In: www.fbi.vsb.cz [online]. [cit. 2025-02-23]. Dostupné z: <https://www.fbi.vsb.cz/060/cs/studium/studijni-materialy/>.

TZB-info.cz. Elektrická požární signalizace [online]. Praha: TZB-info.cz, [cit. 2025-04-29]. Dostupné z: <https://www.tzb-info.cz/elektricka-pozarni-signalizace>

VALOUCH, Jan, 2019. *Projektování bezpečnostních systémů*. Druhé. Zlín: Univerzita Tomáše Bati ve Zlíně. ISBN ISBN 978-80-7454-858-1.

Vláda posílá do sněmovny zpřesnění definice utajované informace, c 2021-2024. Online. *Advokátní deník*. [cit. 2025-02-22]. Dostupné z: <https://advokatnidenik.cz/2023/08/24/vlada-posila-do-snemovny-zpresneni-definice-utajovane-informace/>.

SEZNAM OBRÁZKŮ

Obrázek 1 Pyramida bezpečnosti.....	24
Obrázek 2 Ishikawa diagram	31
Obrázek 3 1. nadzemní podlaží – umístění zabezpečených prostor	36
Obrázek 4 2. nadzemní podlaží – umístění zabezpečených prostor	37
Obrázek 5 Umístění ostrahy v objektu	55
Obrázek 6 Návrh nové ZO v 1. NP	56

SEZNAM TABULEK

Tabulka 1 Porovnání úrovně rizika	32
Tabulka 2 Přehled zajištění fyzické bezpečnosti objektu	45
Tabulka 3 Hodnocení míry rizika na základě identifikovaných hrozeb	50
Tabulka 4 Návrh rozpočtu.....	58

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AČR Armáda České republiky

ČR Česká republika

ČSN Česká státní norma

DVS Dohledový videosystém

EPS Elektronický požární systém

MO Ministerstvo obrany

MZS Mechanické zábranné systémy

NBÚ Národní bezpečnostní úřad

NP Nadzemní podlaží

PCO Pult centrální ochrany

PZTS Poplachové zabezpečovací a tísňové systémy

SOD Stálý operační dozorčí

SOP Standartní operační postup

UI Utajovaná informace

ÚO Úschovný objekt

VOC Vedoucí organizačního celku

ZO Zabezpečená oblast

SEZNAM PŘÍLOH

Příloha 1 Ishikawa diagram bezpečnostních hrozeb objektu

PŘÍLOHA P 1: ISHIKAWA DIAGRAM BEZPEČNOSTNÍCH HROZEB OBJEKTU

