

Bezpečnostní analýza vybraného areálu

Karel Polanecký

Bakalářská práce
2025



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav bezpečnostního inženýrství

Akademický rok: 2024/2025

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení: Karel Polanecký
Osobní číslo: A22141
Studijní program: B1032A020001 Bezpečnostní technologie, systémy a management
Forma studia: Kombinovaná
Téma práce: Bezpečnostní analýza vybraného areálu
Téma práce anglicky: Security Analysis of a Selected Area

Zásady pro vypracování

- Uvedte základní terminologii a základy řízení rizik.
- Charakterizujte vybraný areál.
- Popište současný stav.
- Provedte analýzu rizik a její vyhodnocení.
- Na základě výsledků analýzy rizik navrhnete bezpečnostní opatření.

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

Seznam doporučené literatury:

1. KYNCL, Jaromír. *Bezpečnost objektu ve světle moderních technologií*. Praha: Komora podniků komerční bezpečnosti ČR, 2014. ISBN 978-80-260-7115-0.
2. LUDĚK, Lukáš. *Bezpečnostní technologie, systémy a management II*. Zlín: VeRBuM, 2012. ISBN 978-80-87500-19-4. .
3. LUDĚK, Lukáš. *Teorie bezpečnosti I*. Zlín: VeRBuM, 2017. ISBN 978-80-87500-89-7
4. TICHÝ, Milík. *Ovládání rizika : analýza a management*. Praha: C.H. Beck, 2006. ISBN 80-7179-415-5.
5. UHLÁŘ, Jan. *Technická ochrana objektů*. 2. vydání. Praha: Policejní akademie České republiky, 2009. ISBN 978-80-7251-313-0.

Vedoucí bakalářské práce: **Ing. Dora Kotková, PhD.**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **23. listopadu 2024**
Termín odevzdání bakalářské práce: **2. června 2025**



doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan

Ing. Jan Valouch, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 23. listopadu 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 pracoval(a) samostatně a použitou literaturu jsem řádně citoval(a); v případě publikace výsledků budu uveden(a) jako spoluautor;
- odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

Ve Zlíně, dne

.....

podpis autora

ABSTRAKT

Bakalářská práce se zaměřuje na bezpečnostní analýzu vybraného areálu. V teoretické části je definována základní terminologie v oblasti bezpečnosti a popsána problematika řízení rizik. Praktická část zahrnuje analýzu současného stavu areálu, identifikaci potenciálních rizik a jejich hodnocení prostřednictvím metod **Checklist Analysis (CLA)** a **Failure Mode and Effects Analysis (FMEA)**. Na základě provedené analýzy jsou navržena konkrétní opatření zaměřená na zvýšení úrovně bezpečnosti. Práce si klade za cíl poskytnout ucelený pohled na bezpečnostní situaci areálu a navrhnout účinná opatření ke snížení rizik a ochraně osob i majetku.

Klíčová slova: bezpečnostní analýza, rizika, Checklist Analysis, FMEA, bezpečnostní opatření

ABSTRACT

This bachelor's thesis focuses on the security analysis of a selected site. The theoretical part defines key terminology in the field of security and describes risk management methods. The practical part includes an analysis of the current state of the site, identification of potential risks, and their evaluation using the **Checklist Analysis (CLA)** and **Failure Mode and Effects Analysis (FMEA)** methods. Based on the findings, specific measures to improve security are proposed. The thesis seeks to deliver a structured assessment of the site's security situation and to propose effective measures for reducing risks and ensuring the protection of people and property.

Keywords: security analysis, risks, Checklist Analysis, FMEA, security measures

Rád bych tímto vyjádřil poděkování své vedoucí bakalářské práce, paní Ing. Doře Kotkové, Ph.D., za odborné vedení, cenné rady, vstřícnost a čas, který mi během zpracování práce věnovala. Její připomínky k formální stránce textu výrazně pomohly k tomu, že práce nakonec vypadá úhledně a reprezentativně.

Mé upřímné díky patří také mé manželce Šárce za její trpělivost, pochopení a neocenitelnou podporu v průběhu celého studia — a za to, že i v těch náročnějších chvílích zachovala klid a úsměv.

OBSAH

ÚVOD.....	13
I TEORETICKÁ ČÁST	14
1 ZÁKLADNÍ TERMINOLOGIE.....	15
1.1 BEZPEČNOST	15
1.2 AKTIVUM	15
1.3 HROZBA	15
1.4 ZRANITELNOST.....	16
1.5 DEFINICE RIZIKA	17
1.6 BEZPEČNOSTNÍ OPATŘENÍ	17
1.7 ZBYTKOVÉ RIZIKO.....	17
1.8 PŘÍKLAD VZTAHŮ MEZI POJMY	18
1.9 ZÁVĚR KAPITOLY	18
2 TEORIE ZABEZPEČENÍ OBJEKTŮ.....	19
2.1 MECHANICKÉ ZÁBRANNÉ SYSTÉMY	19
2.1.1 Obvodová (perimetrická) ochrana.....	20
2.1.2 Plášťová ochrana	20
2.1.3 Předmětová ochrana	21
2.2 BEZPEČNOSTNÍ TECHNOLOGIE A SYSTÉMY	21
2.3 FYZICKÁ OSTRAHA	22
2.4 REŽIMOVÁ OPATŘENÍ	22
2.5 ZÁVĚR KAPITOLY	23
3 ŘÍZENÍ RIZIK	24
3.1 FÁZE PROCESU ŘÍZENÍ RIZIK	25
3.1.1 Stanovení kontextu.....	25
3.1.2 Identifikace rizik	25
3.1.3 Analýza rizik	26
3.1.4 Hodnocení rizik	26
3.1.5 Návrh opatření.....	26
3.1.6 Monitoring a přezkum.....	26
3.2 METODY PRO ANALÝZU RIZIK	27
3.2.1 FMEA (Failure Mode and Effects Analysis)	27
3.2.2 CLA (Checklist Analysis).....	27
3.2.3 HAZOP (Hazard and Operability Study).....	28
3.2.4 SWIFT (Structured What-If Technique).....	28
3.2.5 Stromové analýzy (FTA a ETA).....	29
3.3 VÝZNAM ŘÍZENÍ RIZIK PRO BEZPEČNOSTNÍ OPATŘENÍ	29
3.4 ZÁVĚR KAPITOLY	29

II	PRAKTICKÁ ČÁST	30
4	POPIS OKOLÍ A LOKALITY AREÁLU.....	31
4.1	POPIS AREÁLU	31
4.2	POPIS ADMINISTRATIVNÍ BUDOVY	33
4.3	ZÁVĚR KAPITOLY	38
5	SOUČASNÉ ZABEZPEČENÍ OBJEKTU.....	39
5.1.1	Perimetrická ochrana	40
5.1.2	Plášťová ochrana	42
5.1.3	Prostorová ochrana	43
5.1.4	Předmětová ochrana	45
5.1.5	Režimová opatření.....	45
5.1.6	Bezpečnostní dokumentace	47
5.2	ZÁVĚR KAPITOLY	48
6	ANALÝZA RIZIK.....	49
6.1	IDENTIFIKACE AKTIV V AREÁLU	49
6.2	IDENTIFIKACE HROZEB	51
6.2.1	Fyzické hrozby	51
6.2.2	Kybernetické hrozby	52
6.2.3	Přírodní hrozby	52
6.2.4	Provozní hrozby	53
6.2.5	Hrozby způsobené lidským faktorem.....	53
6.3	ANALÝZA RIZIK (CHECKLIST ANALYSIS - CLA).....	54
6.3.1	Perimetrická ochrana areálu	54
6.3.2	Prostorová ochrana areálu	57
6.3.3	Kontrolní seznam pro budovy	57
6.4	ANALÝZA RIZIK – FMEA	62
6.4.1	Faktory hodnocení jsou:	62
6.4.2	Proces analýzy se skládá z těchto kroků:	63
6.4.3	Provedení metody FMEA.....	66
6.5	VYHODNOCENÍ ANALÝZY FMEA	72
6.6	ZÁVĚR KAPITOLY	73
7	NÁVRH BEZPEČNOSTNÍCH OPATŘENÍ	74
7.1	TECHNICKÁ OPATŘENÍ.....	74
7.1.1	Instalace turniketu s čipovým přístupem.....	74
7.1.2	Doplňkové zábrany na perimetr (ostnatý drát, žiletková spirála)	76
7.1.3	Bezpečnostních dveře a zámky na rizikových vstupech	78
7.1.4	Zabezpečení prosklených vstupů a oken	78
7.1.5	Požární hlásiče.....	78
7.1.6	Instalace PTZ kamer s 360° výhledem.....	79
7.2	REŽIMOVÁ OPATŘENÍ	80
7.3	PREVENTIVNÍ OPATŘENÍ	82

7.4	ZHODNOCENÍ A PRIORITIZACE NAVRŽENÝCH OPATŘENÍ	82
7.5	PLÁN IMPLEMENTACE BEZPEČNOSTNÍCH OPATŘENÍ.....	83
7.6	KONTROLNÍ FMEA	84
7.7	ZÁVĚR KAPITOLY	85
8	ZÁVĚR.....	86
	SEZNAM POUŽITÉ LITERATURY.....	87
	SEZNAM OBRÁZKŮ	89
	SEZNAM TABULEK.....	90

ÚVOD

Bakalářská práce se zaměřuje na bezpečnostní analýzu vybraného areálu, která zahrnuje hodnocení současného stavu zabezpečení, identifikaci klíčových hrozeb, slabin, a návrh konkrétních opatření k jejich eliminaci. Bezpečnost hraje klíčovou roli nejen v každodenním životě lidí, ale i v rámci organizací, kde je jejím cílem chránit osoby, majetek a kritické procesy. Každý vážný bezpečnostní incident může způsobit nejen finanční ztráty, ale také narušit provozní činnost, důvěru zaměstnanců a veřejnosti nebo dokonce ohrozit život a zdraví osob. Z tohoto důvodu je bezpečnostní analýza nezbytným nástrojem, který umožňuje efektivně identifikovat rizika a navrhnout opatření ke zmírnění dopadů nejzávažnějších hrozeb. Práce je rozdělena do dvou hlavních částí: teoretické a praktické.

V teoretické části je nejprve vysvětlena základní terminologie a klíčové pojmy v oblasti bezpečnosti a řízení rizik. Tento přístup zajišťuje, že i čtenáři bez hlubší znalosti problematiky budou schopni pochopit odborné výrazy a koncepty použité v dalších částech. Dále je podrobně popsán proces řízení rizik, který se skládá z fází identifikace, analýzy, hodnocení a regulace rizik. Tato část slouží jako teoretický rámec, na němž je založena praktická analýza.

Praktická část práce zahrnuje důkladný popis a charakteristiku analyzovaného areálu, jeho funkce, prostorové uspořádání a organizační strukturu. Následně se zaměřuje na vyhodnocení současného stavu zabezpečení, přičemž hodnotí jednotlivé složky ochrany, jako jsou perimetrická, plášťová a prostorová. Dalším krokem je identifikace aktiv, hrozeb a slabin areálu. Následně jsou použity metody **Checklist Analysis (CLA)** a **Failure Mode and Effects Analysis (FMEA)** k provedení analýzy rizik. Tyto metody umožňují systematicky vyhodnotit identifikované hrozby, posoudit jejich závažnost a pravděpodobnost výskytu a navrhnout preventivní opatření.

V závěrečné části práce jsou navržena konkrétní bezpečnostní opatření, jejichž cílem je minimalizovat odhalená rizika a zajistit vyšší úroveň ochrany osob, majetku i samotných procesů probíhajících v areálu. Tyto návrhy vycházejí z vyhodnocení rizik a zohledňují specifika analyzovaného prostředí.

I. TEORETICKÁ ČÁST

1 ZÁKLADNÍ TERMINOLOGIE

Úspěšné řešení jakéhokoli problému vyžaduje jasné a přesné vymezení klíčových pojmů. Tato kapitola se věnuje základní terminologii, kde mezi klíčové pojmy patří aktivum, hrozba, zranitelnost a riziko.

1.1 Bezpečnost

Bezpečnost je stav, ve kterém je systém nebo organizace schopná odolávat známým, očekávaným i neočekávaným hrozbám, které by mohly ohrozit její stabilitu, strukturu nebo dosažení stanovených cílů. Tento pojem zahrnuje nejen ochranu před vnějším nebezpečím, ale také schopnost reagovat na interní problémy a zajištění ochrany hodnot, jako jsou lidé, majetek nebo informace. Bezpečnost je tedy dynamický proces, který zahrnuje nejen prevenci, ale i přípravu na možné rizikové situace a schopnost adaptace na změny. [1]

1.2 Aktivum

Aktivum představuje vše, co má pro daný subjekt hodnotu a co může být negativně ovlivněno hrozbami. Obecně lze aktiva rozdělit na hmotná (např. lidé, finance, majetek) a nehmotná (např. informace, organizační struktura nebo pracovní morálka). Aktivem může být i samotný subjekt, protože hrozby mohou ohrožovat jeho existenci jako celek. [1]

1.3 Hrozba

Hrozbou se rozumí jev, událost nebo subjekt, který může poškodit aktivum nebo jeho bezpečnostní opatření. Hrozba je aktivována tzv. zdrojem, kterým mohou být lidé, procesy či vnější faktory. Hrozby lze dělit podle úmyslu nebo podle zdroje. [1]

- **Podle úmyslu:**

Neúmyslné: Náhodné události, jako jsou přírodní katastrofy, technické poruchy nebo chyby způsobené lidskou nepozorností.

Úmyslné: Plánované činy, například krádeže, zneužití pravomocí nebo útoky

- **Podle zdroje:**

Vnitřní hrozby: pocházejí z organizace samotné (např. chyby zaměstnanců, selhání zařízení).

Vnější hrozby: přicházejí z okolí organizace například přírodní pohromy nebo kybernetické útoky. [1]

1.4 Zranitelnost

Zranitelnost lze definovat jako nedostatek, slabinu nebo stav aktiva, který umožňuje hrozbě negativně působit na toto aktivum. Jinými slovy zranitelnost představuje místo, kde je aktivum z hlediska bezpečnosti oslabené a může být vystaveno hrozbě. Tento koncept je klíčový při analýze rizik, protože ukazuje, kam je nutné zaměřit bezpečnostní opatření. Základním rysem zranitelnosti je její úroveň, která určuje, do jaké míry je aktivum ohroženo působením hrozby. Tato úroveň je určena dvěma klíčovými faktory: citlivostí a kritičností. [1]

- Citlivost

Vztahuje se k tomu, jak snadno může hrozba ovlivnit dané aktivum. Vyjadřuje míru náchylnosti aktiva vůči specifickým typům hrozeb. Například nezabezpečený počítačový systém je vysoce citlivý na kybernetické útoky, zatímco budova se starými a slabými zámky je citlivá na fyzické vloupání. [1]

- Kritičnost

Na druhé straně kritičnost vyjadřuje důležitost aktiva pro subjekt, který je předmětem analýzy. Jinými slovy, kritičnost ukazuje, jak zásadní je dané aktivum pro fungování subjektu a jaké dopady by mělo jeho poškození nebo ztráta. Například u nemocnice je kritickým aktivem vybavení pro intenzivní péči, protože jeho nefunkčnost by mohla ohrozit lidské životy. [1]

Tyto dva faktory se vzájemně ovlivňují a společně vytvářejí celkovou úroveň zranitelnosti. Aktivum, které je vysoce citlivé na určitou hrozbu a zároveň vysoce kritické, představuje prioritní oblast pro zavedení účinných bezpečnostních opatření. Naopak aktiva s nízkou citlivostí a nízkou kritičností mohou být považována za méně významná z hlediska bezpečnostních priorit. Porozumění zranitelnosti a jejím faktorům je nezbytné pro efektivní řízení rizik, protože pomáhá identifikovat, kde je potřeba zavést opatření, která minimalizují nebo eliminují možnosti negativního působení hrozeb. [1]

1.5 Definice rizika

Riziko je pojem, se kterým se setkáváme v každodenním životě. I když jeho význam bývá intuitivně pochopitelný, přesná definice může být obtížná. Tato složitost vyplývá z několika důvodů. Riziko je často vnímáno jako určitá forma nebezpečí, avšak nebezpečí je subjektivní a nelze jej snadno objektivně změřit. Navíc definice rizika závisí na konkrétním oboru a kontextu, ve kterém se používá. Proto existuje celá řada různých definic tohoto pojmu. Nejen v oblasti managementu a analýzy rizik je třeba přistupovat k pojmu riziko přesněji. To zahrnuje identifikaci nebezpečí, analýzu jeho možných scénářů a následné vyhodnocení rizika. Je zřejmé, že riziko a nebezpečí spolu úzce souvisí, ale nejsou totožné. Proto je důležité používat jednoznačné termíny, což je zvláště významné při aplikaci metod sloužících k analýze rizik. Zjednodušeně řečeno, riziko je pravděpodobnost, že dojde k události považované za nežádoucí, která vyplývá z konkrétní hrozby, a zároveň míra dopadu této události na analyzovaný subjekt. Dopad hrozby lze chápat jako rozsah škod nebo negativních důsledků, které se projeví v případě jejího naplnění. Tento dopad může být fyzický (například zranění, ztráta majetku), finanční (výrazné ekonomické ztráty), reputační (poškození dobrého jména organizace), nebo systémový (narušení procesů a struktur organizace). [2]

Vyhodnocení rizika proto spočívá nejen v analýze pravděpodobnosti výskytu hrozby, ale také v detailním posouzení jeho potenciálních dopadů. Tato kombinace umožňuje efektivnější řízení rizik a implementaci odpovídajících opatření ke zmírnění jejich dopadů. [2]

1.6 Bezpečnostní opatření

Bezpečnostní opatření jsou navrhována s cílem minimalizovat působení rizik. Snižují zranitelnost aktiva, eliminují zdroje hrozeb snižují pravděpodobnost jejich výskytu, nebo snižují dopad. Při návrhu opatření se zohledňují zejména efektivita a náklady. [2]

1.7 Zbytkové riziko

Zbytkové riziko je takové, které je pro organizaci nebo subjekt akceptovatelné a nevyžaduje zavedení opatření. Přijatelnost zbytkového rizika nesmí překročit referenční úroveň stanovenou zákony, normami nebo společenskými standardy. [2]

1.8 Příklad vztahů mezi pojmy

Pro lepší pochopení vzájemných vztahů mezi pojmy je níže uveden příklad vloupání do budovy:

- **Aktivum:** Majetek uvnitř budovy (např. technika, peníze).
- **Hrozba:** Vloupání do budovy.
- **Zdroj hrozby:** Pachatel, který využívá slabiny v zabezpečení objektu.
- **Zranitelnost:** Nedostatečné zabezpečení, jako například chybějící kamerový systém nebo slabé zámky případně oplocení pozemku.
- **Riziko:** Je to kvantitativní vyjádření, např. riziko vloupání 8/10, poškození cizí věci 5/10.
- **Bezpečnostní opatření:** Instalace kamerového systému, poplachových zabezpečovacích systémů, bezpečnostních dveří a pravidelné hlídky.
- **Zbytkové riziko:** I přes zavedená opatření může dojít k vloupání, například pokud pachatel překoná technická zabezpečení.

Kdyby nebyla zavedená žádná opatření, dopady vloupání by mohly být mnohem závažnější, například ztráta finančních prostředků, digitální techniky nebo citlivých informací. Zavedením bezpečnostních opatření se však vloupání stává přijatelným zbytkovým rizikem, protože jeho pravděpodobnost a dopad jsou minimalizovány.

1.9 Závěr kapitoly

Závěrem této kapitoly bylo objasnit základní pojmy, které jsou klíčové pro proces řízení rizik. Přestože existuje celá řada dalších termínů souvisejících s touto problematikou, uvedené pojmy patří mezi nejzásadnější a nejčastěji používané. Jejich přesné pochopení je nezbytným předpokladem pro efektivní analýzu a řízení rizik v praxi

2 TEORIE ZABEZPEČENÍ OBJEKTŮ

Bezpečnostní opatření v objektech či areálu lze obecně rozdělit do několika hlavních kategorií. Mechanické zábranné systémy zajišťují fyzickou odolnost proti neoprávněnému vniknutí, zatímco elektronická a monitorovací zařízení rychle a efektivně detekují pokusy o narušení. Důležitou roli hraje rovněž přenos informací a systém centrální ochrany, díky kterému lze z jednoho místa koordinovat případné zásahy a monitorovat stav celého objektu. [3]

2.1 Mechanické zábranné systémy

Zajišťují prvotní úroveň ochrany pro různé typy objektů a areálů. Jejich hlavní funkcí je ztížit nebo znemožnit neoprávněné vniknutí dovnitř a zároveň případnému útočníkovi prodloužit čas, který by k překonání zábran potřeboval. Díky tomu lze zvyšovat pravděpodobnost, že bude narušení včas detekováno, a zároveň zajistit dostatek času pro příjezd zásahové jednotky či bezpečnostní služby. Mechanické zábranné systémy se obvykle rozčleňují do následujících kategorií: **obvodová (perimetrická) ochrana, plášťová ochrana, prostorová ochrana a předmětová ochrana.** [3]

Tabulka 1 Bezpečnostní třídy dle ČSN EN 1627

Bezpečnostní třída (RC)	Čas napadení	Použité metody
RC 1	Neaplikuje se	Příležitostný zloděj využívá jednoduché fyzické násilí (kopání, narážení ramenem, vytrhávání), má k dispozici pouze malé jednoduché nářadí (např. šroubovák). Nemá žádné zvláštní znalosti a snaží se nevyvolat hluk.
RC 2	3 minuty	Příležitostný zloděj s malými znalostmi o úrovni ochrany MZS používá opět jednoduché nářadí (šroubováky, malé páčidlo) a fyzickou sílu. Čas i hluk se snaží omezit na minimum.
RC 3	5 minut	Zloděj již disponuje středně pokročilými znalostmi a používá páčidlo délky až 710 mm, ruční šroubováky, malé kladivo, důlčíky či mechanickou ruční vrtačku. Je schopný aplikovat zvýšenou fyzickou sílu s dlouhým páčidlem a částečně chápe funkci uzávěru.
RC 4	10 minut	Zkušený zloděj využívá širší škálu nářadí (zámečnické kladivo, sekáče, dláta, sekeru, přenosnou akumulátorovou vrtačku). Dokáže kombinovat různé způsoby napadení (vrtání, sekání, páčení) a neřeší nadměrný hluk.
RC 5	15 minut	Velmi zkušený zloděj používá i jednoruční elektrické nářadí (úhlová bruska s kotoučem do 125 mm, přímočará pila). Nepřikládá význam hluku a dokáže pracovat systematicky.

Bezpečnostní třída (RC)	Čas napadení	Použité metody
RC 6	20 minut	Nejzkušenější zloděj nasazuje dvouruční elektrické nářadí (např. úhlová bruska do 230 mm, výkonné pily). Hluk a doba potřebná k překonání zábrany nejsou pro něj podstatnou překážkou, má značné znalosti a je schopen rychle reagovat na nečekané komplikace.
poznámka:		Čas napadení je myšlen jako orientační doba aktivního, nepřetržitého útoku potřebného ke zdolání zábrany.

(zdroj: [4])

Mechanické zábranné systémy (MZS) se řídí normami ČSN EN 1627 až ČSN EN 1630, které je dělí do šesti bezpečnostních tříd (RC 1 až RC 6). U dveří se zpravidla setkáváme s třídami RC 2, RC 3 a RC 4. Každá třída přitom vyjadřuje, jakému nářadí a metodám dokáže MZS po určitou dobu odolat. [4][5]

2.1.1 Obvodová (perimetrická) ochrana

Obvodová ochrana, která vytyčuje hranice pozemku a zabraňuje snadnému vstupu nepovolaných osob, bývá zajištěna ploty (zhotovenými z pletiva, kovových panelů či betonových dílců) nebo zdmi (betonové, zděné) často doplněné nástavci (ostnatý či žiletkový drát, hroty), přičemž brány (posuvné, křídlové či rolovací) se opatřují spolehlivými zámky, elektronickým ovládáním, popř. závorami či turnikety; kromě mechanických bariér lze pro zvýšení bezpečnosti využít perimetrické detektory schopné vyhlásit poplach při narušení (např. rozřezání pletiva, přezení plotu). [6]

2.1.2 Plášťová ochrana

Plášťová ochrana, zaměřující se na dveře, okna, vrata a stěny, zahrnuje použití bezpečnostních dveří s vícenásobným uzamykacím mechanismem, zesílenou konstrukcí a odolnými závěsy proti vysazení; jejich zámky s cylindrickými vložkami vyšší bezpečnostní třídy znesnadňují neoprávněné otevření hrubou silou či planžetou. Okna a výlohy lze chránit mřížemi, pevnými roletami nebo bezpečnostní fólií, přičemž ve vysoce rizikových provozech (např. sklady cenného zboží) se často instalují speciální nerozbitná skla. V průmyslových areálech je zásadní odolnost vrat a garážových stání, které lze doplnit závorou či automatickým zámkem blokujícím násilné otevření. V případě vysokého ohrožení se používají betonové či ocelové panely v kritických místech a odolné výplně (dveřní výplně, parapety) zvyšující ochranu proti proražení nebo vybourání. [6][7]

2.1.3 Předmětová ochrana

Předmětová ochrana zajišťuje zabezpečení nejcennějších nebo nejzranitelnějších předmětů v budově, a to i v případě prolomení obvodové či plášťové ochrany. Trezory a sejfy, s ohledem na svou bezpečnostní třídu a správné ukotvení (např. k podlaze či ke zdi), se používají ke skladování hotovosti, cenností či citlivých dokumentů; jejich elektronické nebo mechanické zámky musejí vyhovovat normám vysoké bezpečnosti. Uzamykatelné skříně a boxy, často kovové, představují účinný doplněk k trezorům pro menší obnosy, elektronická zařízení nebo důležité záznamy. Speciální vitríny, vybavené pevnou konstrukcí a zabezpečením proti násilnému vniknutí, jsou pak nezbytné pro uchování a prezentaci drahých či unikátních exponátů, například v muzeích nebo galeriích předmětová ochrana slouží k zabezpečení nejcennějších nebo nejzranitelnějších předmětů uvnitř budovy, a to i v případě, že došlo k prolomení obvodové a plášťové ochrany. [6][7]

2.2 Bezpečnostní technologie a systémy

V návaznosti na mechanické zábranné systémy (MZS) dále jsou elektronická a technologická opatření, která umožňují rychlou detekci, vyhodnocení a hlášení potenciálního ohrožení. Tyto systémy poskytují nepřetržitý monitoring, automatizované řízení přístupu a okamžitou reakci na bezpečnostní incidenty, čímž významně zvyšují úroveň ochrany objektů. Jedním z nejdůležitějších prvků je dohledový videosystém (DV), který zajišťuje kontinuální sledování objektu, zaznamenávání pohybu osob a vozidel a možnost zpětné analýzy událostí. Kombinace viditelných i skrytých kamer pomáhá odradit potenciální pachatele a zajišťuje nepřetržitý dohled nad rizikovými místy. [6][7]

Dalším významným prvkem zabezpečení je poplachový zabezpečovací a tísňový systém (PZTS), který automaticky detekuje neoprávněný vstup, násilné vniknutí nebo jiné podezřelé aktivity. V případě narušení prostoru aktivuje zvukový i vizuální alarm a informuje ostrahu objektu. Z hlediska požární ochrany je klíčová elektrická požární signalizace (EPS), která detekuje přítomnost kouře, prudké teplotní změny nebo přímý plamen a v případě hrozby okamžitě spouští poplachový signál. Tento systém je napojen na centrální bezpečnostní ústřednu a může být propojen i s automatickým hasicím systémem, pokud objekt takovou ochranou disponuje. [6][7]

Řízení pohybu osob a kontrolu přístupu do objektu zajišťují elektronické systémy kontroly vstupu (ESKV). Tyto systémy využívají RFID čipy, biometrické údaje nebo přístupové kódy, čímž umožňují selektivní kontrolu vstupu pouze pro oprávněné osoby.

Veškeré typy ochrany mohou být dále doplněna dalšími prvky a spojena s dohledovým přijímacím a poplachovým centrem (DPPC), které monitoruje celý areál včetně jeho vnějších i vnitřních prostor. Tyto systémy dokážou detekovat pokusy o neoprávněný vstup, poškození zabezpečovacích prvků či jiné podezřelé aktivity. Jakmile je zaznamenána podezřelá aktivita, systém automaticky spouští poplach a informuje bezpečnostní službu. Moderní bezpečnostní technologie často fungují v kombinaci s fyzickou ostrahou, což umožňuje efektivní dohled nad areálem a rychlou reakci na bezpečnostní incidenty. Integrace všech prvků do jednoho centrálního systému zajišťuje komplexní řízení bezpečnosti, automatické vyhodnocení rizik a možnost vzdáleného dohledu nad celým objektem. [6][7]

2.3 Fyzická ostraha

Hlavním úkolem fyzické ostrahy je přímá kontrola a ochrana prostoru prostřednictvím přítomnosti vyškoleného bezpečnostního personálu. V rámci výkonu služby zajišťuje zejména kontrolu vstupů a výstupů osob a vozidel, monitoring poplachových zabezpečovacích a tísňových systémů, pochůzkovou činnost v definovaných intervalech a přímý zásah při zjištění narušení bezpečnosti. [6]

Fyzická ostraha může pracovat v nepřetržitém režimu (tzv. 24/7) na stálý fyzický dohled, vázaná na pracovní dobu (např. od 7:00 - 15:30) anebo nárazová. Její přítomnost má přímý preventivní účinek a slouží jako psychologická bariéra proti narušení. V rámci standardních činností bývá fyzická ostraha vybavena komunikační technikou, prostředky osobní ochrany a často rovněž technickým zařízením umožňujícím kontrolu vstupu či obchůzkový dohled (např. elektronické čipy, bodyguard systémy). [6]

Přítomnost fyzické ostrahy v objektech umožňuje okamžitou reakci na incidenty a posiluje celkovou bezpečnost. [6]

2.4 Režimová opatření

Je to forma ochrany, která stanovuje pravidla pro pohyb osob, manipulaci s materiálem, využívání technických prostředků v rámci střeženého objektu. Jejich cílem je vytvoření prostředí, které minimalizuje rizika vyplývající z lidského selhání, nepozornosti nebo zneužití pravomocí. [6]

Z hlediska praxe se mezi režimová opatření nejčastěji řadí:

- evidence a kontrola vstupujících osob
- vymezení přístupových práv
- stanovení pravidel pro manipulaci s klíči (klíčová služba)
- regulace vnášení a vynášení předmětů [6]

Režimová opatření jsou důležitá pro provoz a zároveň podporují účinnost ostatních prvků technické i fyzické ochrany. [6][7]

2.5 Závěr kapitoly

Tato kapitola poskytla přehled základních prvků technického a organizačního zabezpečení objektů, a to včetně mechanických zábran, elektronických systémů, fyzické ostrahy i režimových opatření. Vyplynula nutnost jejich vzájemné provázanosti a koordinace pro dosažení účinné ochrany. V následující kapitole bude navázáno popisem procesů řízení rizik, které jsou důležité pro identifikaci a vyhodnocení bezpečnostních hrozeb a návrhu vhodných opatření.

3 ŘÍZENÍ RIZIK

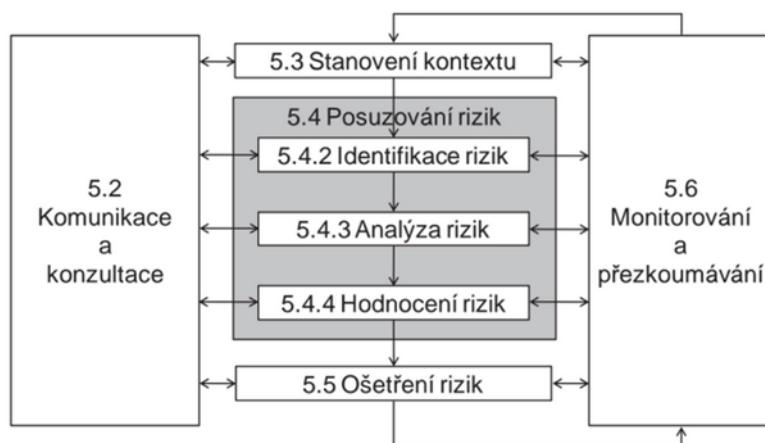
Řízení rizik představuje souhrn systematických procesů, které slouží k identifikaci, hodnocení a zmírňování rizik, jež by mohla negativně ovlivnit konkrétní subjekt, areál nebo organizaci. Jedná se o klíčovou součást moderního managementu a bezpečnostní strategie, která pomáhá předcházet událostem s potenciálně nepříznivými důsledky nebo minimalizovat jejich dopad. Řízení rizik tedy není jen jednorázovou činností, ale kontinuálním procesem, který se přizpůsobuje změnám v prostředí, technologiích nebo legislativě. V kontextu analýzy vybraného areálu je řízení rizik obzvláště důležité, neboť zahrnuje ochranu majetku, osob i citlivých informací. Areály, ať už průmyslové, obchodní, administrativní, nebo jiné, čelí různorodým hrozbám, která se mohou lišit podle jejich povahy a provozních podmínek. Identifikace těchto rizik a návrh adekvátních opatření umožňuje nejen zvýšit bezpečnost, ale také předejít finančním ztrátám, narušení provozu nebo ohrožení zdraví a života osob. [8]

Cílem řízení rizik je především minimalizovat pravděpodobnost výskytu nežádoucích událostí a zmírnit jejich případné dopady. Důležitou součástí je také zajištění kontinuity provozu, což je v areálech často klíčové pro udržení výroby, poskytování služeb nebo jiných činností. Kromě toho se řízení rizik zaměřuje na efektivní alokaci zdrojů – investice do bezpečnostních opatření musí být přiměřené reálným hrozbám a zároveň ekonomicky únosné. Dalším zásadním přínosem řízení rizik je podpora informovaného rozhodování. Díky systematickému přístupu k rizikům získává vedení organizace komplexní přehled o možných hrozbách a slabých místech. To jim umožňuje lépe plánovat, optimalizovat procesy a přijímat opatření, která nejen chrání areál, ale také přispívají k jeho efektivitě a konkurenceschopnosti. [8]

Tato kapitola je zaměřena na klíčové principy, procesy a nástroje řízení rizik, které budou dále aplikovány v praktické části práce. Důraz bude kladen na metody jako FMEA (Failure Mode and Effects Analysis) a CLA (Checklist Analysis), které pomohou strukturovaně a systematicky hodnotit identifikovaná rizika. Tyto metody poskytnou nezbytné podklady pro návrh účinných bezpečnostních opatření, která zajistí optimální ochranu daného areálu. [1] [8]

3.1 Fáze procesu řízení rizik

Řízení rizik obvykle zahrnuje několik základních fází, které na sebe logicky navazují. Jedná se např. o identifikaci rizik, analýzu rizik a hodnocení rizik. [9]



Obrázek 1 Proces managementu rizik

(zdroj: [2])

3.1.1 Stanovení kontextu

Před samotnou identifikací rizik je nutné vymezit kontext, v němž bude celý proces probíhat. Tato fáze zahrnuje analýzu vnitřního a vnějšího prostředí, včetně:

- **vnějších faktorů** – legislativa, bezpečnostní situace v lokalitě, požadavky zainteresovaných stran, vliv okolí,
- **vnitřních faktorů** – struktura organizace, aktuální bezpečnostní opatření, organizační kultura, rozpočet,
- **vymezení rozsahu a cílů** – co je předmětem analýzy (např. majetek, osoby), stanovení akceptovatelné míry rizika, definice hodnot, které mají být chráněny. [2]

Správné stanovení kontextu slouží k pochopení, jaké hrozby mohou ovlivnit daný areál a jaká opatření jsou v daných podmínkách realistická a efektivní. [2] [9]

3.1.2 Identifikace rizik

V této fázi se hledají a popisují potenciální rizika, jež mohou mít negativní dopad na vybraný areál. Prakticky může jít o analýzu interních i externích faktorů (např. stav infrastruktury, kriminální statistiky v lokalitě, provozní postupy). Patří sem i vytváření seznamů rizik

prostřednictvím metod, jako je brainstorming, kontrolní seznam (checklist) či konzultace s odborníky. [2] [9]

3.1.3 Analýza rizik

Nalezená rizika se v této fázi detailně zkoumají z hlediska jejich pravděpodobnosti a potenciálního dopadu na areál (například finanční ztráty, ohrožení zdraví osob, poškození infrastruktury). Lze zde využít kvalitativní i kvantitativní metody. Pro potřeby této práce jsou významné metody FMEA (Failure Mode and Effects Analysis) a CLA (Checklist Analysis), které umožňují systematické a podrobné posouzení možných scénářů a jejich následků. [2] [9]

3.1.4 Hodnocení rizik

Na základě výsledků analýzy se rizika hodnotí a třídí podle priority. Zohledňuje se zde, která rizika jsou pro fungování areálu kritická a jaké dopady by měla jejich realizace. Může jít o stanovení akceptovatelné úrovně rizika – tedy hranice, do které je organizace ochotna riziko tolerovat. [2] [9]

3.1.5 Návrh opatření

Pro rizika, která vyžadují zásah, se volí vhodné reakce:

1. **Prevence (eliminace rizika):** Úprava technologií, zabezpečení nebo procesů tak, aby ke vzniku rizika vůbec nedošlo.
2. **Zmírnění:** Zavedení opatření, která snižují pravděpodobnost nebo dopad konkrétního rizika (např. poplachové zabezpečovací systémy, školení zaměstnanců).
3. **Přenos:** Přenesení rizika na jiný subjekt, například formou pojištění či outsourcingu.
4. **Přijetí:** Pokud je riziko nízké nebo náklady na jeho řešení příliš vysoké, organizace jej může akceptovat jako zbytkové. [2] [9]

3.1.6 Monitoring a přezkum

Poslední krok zahrnuje průběžné sledování, zda zavedená opatření fungují a zda se neobjevují nová rizika nebo změny v těch stávajících. V případě potřeby se proces řízení rizik znovu aktualizuje a zpřesňuje. [2]

3.2 Metody pro analýzu rizik

Pro důkladné prozkoumání hrozeb a slabých míst ve vybraném areálu se využívá řada metod, které se liší svým zaměřením i rozsahem podrobnosti. Některé z nejčastěji používaných metod jsou uvedeny níže. Každá z nich poskytuje specifický úhel pohledu na rizika, a proto je vhodné je podle potřeby kombinovat, aby výsledná analýza byla co nejkomplexnější. [10]

3.2.1 FMEA (Failure Mode and Effects Analysis)

FMEA (Analýza příčin a následků poruch) je metoda zaměřená na identifikaci a hodnocení potenciálních způsobů selhání (tzv. failure modes), zkoumání jejich příčin a posuzování možných dopadů na zkoumaný systém, proces či produkt. [9]

1. **Identifikace možných selhání** – Např. která zařízení, komponenty nebo procesy mohou selhat a jakým způsobem.
2. **Stanovení příčin** – Zjištění, co by mohlo selhání způsobit (technický nedostatek, lidská chyba, nevhodný materiál).
3. **Hodnocení následků** – Určení závažnosti selhání z hlediska bezpečnosti, finančních ztrát či reputace.
4. **Odhad pravděpodobnosti výskytu** – Na základě historických dat, zkušeností nebo odhadů expertů.
5. **Určení detekovatelnosti** – Posouzení, jak rychle a snadno lze selhání rozpoznat, aby bylo možné včas zakročit. [9][10]

Součástí FMEA bývá i výpočet rizikového čísla (RPN – Risk Priority Number), které se odvozuje z pravděpodobnosti výskytu, závažnosti dopadů a schopnosti selhání včas odhalit. Díky tomu lze snadno určit, které selhání má nejvyšší prioritu a vyžaduje okamžitá preventivní opatření. [9][10]

3.2.2 CLA (Checklist Analysis)

CLA je metoda využívající kontrolní seznamy s předem definovanými položkami, které je nutné zhodnotit. Bývá efektivní zejména při rychlém odhalování zjevných nedostatků nebo opakujících se hrozeb. [9][10]

1. **Tvorba kontrolních seznamů** – Zpravidla na základě dřívějších zkušeností, norem, legislativy či odborné literatury.

2. **Posouzení každé položky** – Kontroluje se, zda je stav vyhovující, nebo zda existuje nutnost zásahu (např. chybějící požární hlásiče, zastaralé zámky nebo nedostatečné osvětlení).
3. **Vyhodnocení rizik** – Položky, které nevyhověly, se dále analyzují z hlediska závažnosti a pravděpodobnosti jejich negativního dopadu. [9][10]

Výhodou CLA je relativní rychlost, jednoduchost a srozumitelnost. Nevýhodou může být omezený rozsah – metoda obvykle zachytí pouze ty hrozby, které jsou v seznamu předem uvedeny. [9][10]

3.2.3 HAZOP (Hazard and Operability Study)

HAZOP je metoda původně vyvinutá v chemickém průmyslu, ale lze ji aplikovat i v jiných odvětvích či areálech, kde se pracuje s technickými nebo technologickými systémy. Jejím cílem je identifikovat a vyhodnotit potenciální nebezpečné odchylky od standardního provozu: [9]

1. **Systematické kladení otázek** (např. „Co se bude dít v případě výpadku proudu (blackoutu)“ nebo „Co když dojde k zastavení ventilace?“)
2. **Hodnocení následků** pro proces, personál nebo infrastrukturu.
3. **Doporučení opatření** k omezení pravděpodobnosti a následků rizikových situací. [9][10]

HAZOP je podrobná a strukturovaná metoda, která napomáhá odhalovat skryté možné scénáře selhání. [9][10]

3.2.4 SWIFT (Structured What-If Technique)

SWIFT je obdobou HAZOP, ale je univerzálnější a méně formalizovaná. Pracuje se s otázkami typu „Co když...?“ a účastníci týmově navrhnou možné scénáře, které by mohly vést k ohrožení areálu. Tato metoda se často používá jako doplněk k detailnějším analýzám, aby pokryla i ty hrozby, jež nejsou v běžných seznamech nebo se nemusí týkat jen technologií, ale i organizačních procesů či lidských faktorů. [9]

3.2.5 Stromové analýzy (FTA a ETA)

Mezi další užitečné techniky patří stromové analýzy.

1. **FTA (Fault Tree Analysis)** – Jde o metodu, která zobrazuje vztahy mezi různými příčinami potenciální události (tzv. top event). Vytváří se hierarchická struktura (strom poruch), jež pomáhá pochopit, jaké kombinace příčin mohou vést k nežádoucímu stavu.
2. **ETA (Event Tree Analysis)** – Naopak se zaměřuje na sled událostí po iniciujícím incidentu. Je vhodná zejména pro pochopení možných scénářů, které mohou nastat, pokud se riziko zrealizuje. [9][10]

Oba přístupy lze vzájemně kombinovat nebo použít společně s dalšími metodami, aby se komplexně zachytily příčiny i následné důsledky možných incidentů. [9][10]

Výše uvedené metody představují nejčastější přístupy, které lze aplikovat na různé typy areálů, provozů či procesů. V praxi se zpravidla volí kombinace více metod, a to na základě specifik daného prostředí, typu provozu či aktuálně zkoumaného systému. Pro některé organizace může být vhodné začít s jednoduchou CLA, aby rychle odhalily nejmarkantnější nedostatky, a poté přistoupit k detailnější FMEA či HAZOP, které doplní chybějící vhled. [9][10]

3.3 Význam řízení rizik pro bezpečnostní opatření

Závěry z procesu řízení rizik jsou podkladem pro návrh i optimalizaci bezpečnostních opatření. Zajišťují, že přijatá opatření odpovídají skutečným hrozbám a slabým místům v areálu, a zároveň podporují efektivní vynakládání finančních a lidských zdrojů. Prostřednictvím řízení rizik lze také odhalit dříve přehlížené vazby mezi různými hrozbami (např. kriminální, provozní nebo kybernetická rizika) a lépe je zkoordinovat. [9][10]

3.4 Závěr kapitoly

Řízení rizik je proces, který vyžaduje systematický a průběžný přístup. Jedině tak lze reagovat na měnící se prostředí, nové technologie a potenciální hrozby. Pečlivě vedené řízení rizik je nezbytnou podmínkou pro zajištění bezpečnosti osob, ochranu majetku a zajištění kontinuity provozu. V dalších částech práce se zaměříme na praktické využití metod FMEA a CLA, které umožní přenést teoretické zásady do konkrétních analýz rizik a návrhů opatření.

II. PRAKTICKÁ ČÁST

4 POPIS OKOLÍ A LOKALITY AREÁLU

V rámci praktické části je nejprve popsán stav areálu, na který navazuje analýza spolu s nastavením řízení rizik vybraného areálu nacházejícího se v lokalitě Brno-Jih. Tento průmyslový a logistický objekt je situován ve strategické oblasti s výbornou dostupností na hlavní dopravní tahy, včetně dálnic D1 a D2, což umožňuje efektivní propojení s centrem, ale i se zbytkem republiky, což je vhodné pro logistické a průmyslové aktivity. Areál se nachází v oblasti s rozvinutou průmyslovou infrastrukturou, kde se vedle něj nachází další komerční a výrobní objekty.

Okolí areálu je částečně tvořeno obytnou zástavbou, což může mít vliv na provozní a bezpečnostní opatření, zejména z hlediska regulace pohybu osob a vozidel. Na severní části tohoto areálu se nenachází nic pouze zahrádkářské kolonie. Tato zahrádkářská oblast vytváří potenciální riziko pro nepozorovaný pohyb osob směrem k areálu. Z této strany tak může docházet k nepozorovanému přiblížení nepovolaných osob, což snižuje efektivitu perimetrické ochrany a zvyšuje riziko vniknutí do areálu mimo hlavní kontrolované přístupové body.

Z důvodu ochrany citlivých údajů a bezpečnostních opatření je konkrétní identita areálu v rámci této bakalářské práce anonymizována.

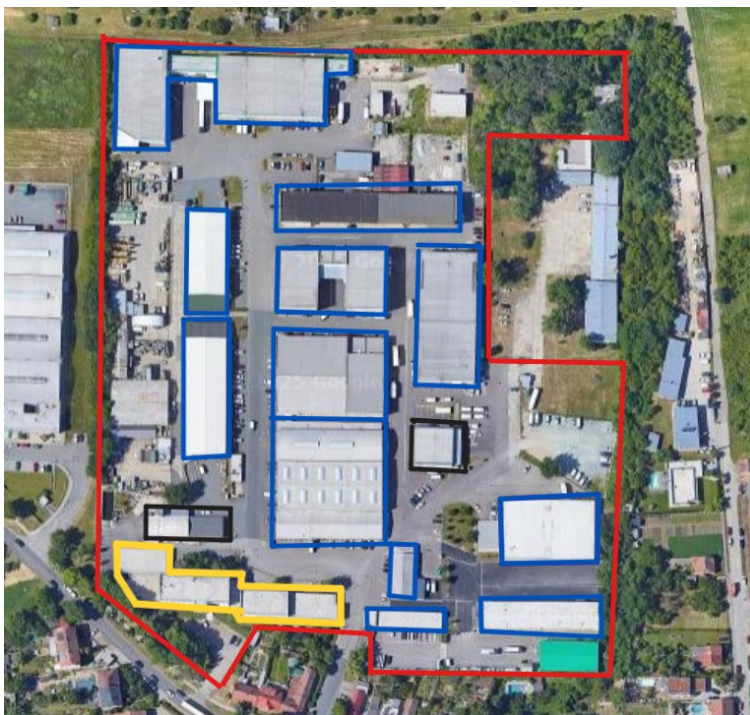
4.1 Popis areálu

Samotný areál tvoří několik rozsáhlých průmyslových a skladovacích hal doplněných o menší provozní budovy. Budovy o různých tvarů a rozměru zde mají různá využití projedeny/sklady např. lékařských materiálů, autodoplňků, tiskových materiálů a různého kancelářského vybavení, nebo je zde i autodílna pro opravy aut jedné ze společností.

Mezi jednotlivými objekty se nachází rozsáhlé zpevněné plochy, které slouží jako parkoviště a manipulační prostory pro nákladní dopravu. Uspořádání areálu vypovídá o tom, že zde probíhá logistický a výrobní provoz s častým pohybem zboží.

Dostupnost pro automobily je zajištěna jediným vstupem přes nákladní vrátnici umístěnou v jižní části areálu. Tato vrátnice je nepřetržitě střežena pracovníky bezpečnostní služby (SBS), kteří zde operují 24 hodin denně, 7 dní v týdnu, po celý rok. Díky tomu je zajištěn trvalý dohled a kontrola nad celým areálem. Pro pěší návštěvníky je k dispozici samostatný vstup přes administrativní budovu, kde se nachází další vrátnice. Tato vrátnice

je otevřena v pracovních dnech od 6:00 do 17:00 a slouží především pro zaměstnance a návštěvy.



Obrázek 1 Letecký snímek areálu

(zdroj: upraveno z [11])

Legenda k obrázku 2:

- **Modře zvýrazněné objekty:** průmyslové a skladovací haly s administrativní částí
- **Žlutě zvýrazněné objekty:** administrativní budova s kanceláři pronajímatele a dalších firem (včetně vstupní vrátnice pro pěší).
- **Černě označené budovy** – skladovací prostory
- **Červená linie:** hranice areálu definovaná oplocením.

Areál se nachází na okraji zastavěné oblasti a je částečně obklopen zelení i dalšími průmyslovými objekty. Díky své poloze je snadno dostupný jak pro zaměstnance, tak i pro nákladní dopravu. Jeho bezpečnostní opatření, včetně nepřetržité fyzické ostrahy a řízeného přístupu, zajišťují efektivní ochranu a kontrolu pohybu osob i vozidel.

Součástí areálu je také vlastní požární nádrž o objemu 100 m³, která slouží jako zdroj vody pro případ požáru. Z této nádrže jsou vyvedeny podzemní rozvody zakončené hydranty, které jsou strategicky rozmístěny po celém areálu tak, aby byly snadno dostupné pro jednotky hasičského záchranného sboru v případě zásahu. Umístění hydrantů bylo

voleno s ohledem na rychlý přístup ke všem důležitým objektům a technickým částem areálu, což přispívá k vyšší úrovni požární bezpečnosti celého komplexu. Tento systém představuje důležitý prvek požární ochrany, nezávislý na vnějších vodních zdrojích.

Na několika místech areálu se na fasádách budov nacházejí pevně instalované požární žebříky, které slouží k evakuačním a záchranným účelům v případě požáru. Je to pozitivní prvek z hlediska bezpečnosti osob a zásahu IZS. Na druhou stranu je však nutné upozornit, že tyto žebříky nejsou opatřeny žádnými ochrannými prvky, jako jsou zamykatelné kryty, výsuvné spodní části nebo přístupové zábrany. V důsledku toho mohou být snadno zneužitelné nepovolanými osobami k překonání výškových rozdílů, proniknutí do vyšších pater objektů nebo k usnadnění vloupání. Tento fakt představuje bezpečnostní slabinu, na kterou je vhodné při dalším posuzování rizik brát zřetel.

Celkově se jedná o rozsáhlý a dobře umístěný průmyslový areál, který je dobře dostupný a intenzivně využíván pro logistické účely.

4.2 Popis administrativní budovy

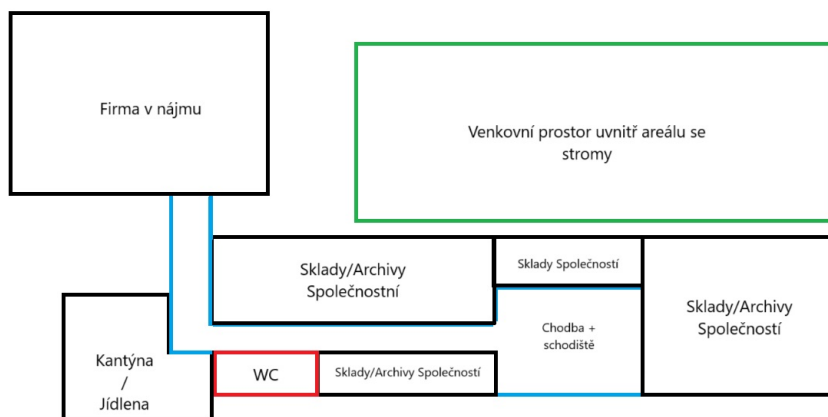


Obrázek 2 Administrativní budova s hl. vchodem

(zdroj: [12])

Administrativní budova představuje čtyřpodlažní objekt se suterénem, avšak bez výtahu. Jednotlivá patra jsou dispozičně uspořádána obdobně, s výjimkou suterénu a druhého patra, která mají specifické úpravy. Budova slouží primárně jako administrativní zázemí pro různé společnosti, včetně firmy, která spravuje celý areál.

Suterén – skladové prostory a spojovací chodba



Obrázek 3 Suterén

(zdroj: vlastní)

Suterén administrativní budovy je primárně skladovacím a archivním prostorem, který slouží různým společnostem sídlícím v objektu. Na rozdíl od vyšších podlaží zde nejsou kanceláře, ale spíše technické a provozní místnosti. Prostor je propojen dlouhou chodbou, která zajišťuje spojení mezi jednotlivými částmi budovy a přístup ke kantýně či venkovní části areálu.

Skladové a archivní prostory

Většinu suterénu tvoří sklady a archivy jednotlivých společností. Tyto prostory jsou využívány k uchovávání dokumentace, materiálů a vybavení.

Kantýna/Jídelna

V levé části suterénu se nachází kantýna/jídelna, která je přístupná z hlavní chodby. Tato jídelna slouží pro zaměstnance pracující v budově, ale i pro příchozí z venku ať už z areálu nebo z blízkých rodinných domků. Kantýna jako jedna z mála má svůj přístup jak z administrativní budovy, tak i z venku. Tento přístup je trvale monitorován kamerami.

Firma v nájmu

Na severní straně suterénu se nachází firma v nájmu, která má vlastní vymezený prostor oddělený od hlavních skladových sekcí. Přístup k této společnosti je jedině přes vrátnici v administrativní budově. Do firmy mají vstup pouze její zaměstnanci, kteří mají i vlastní zamykací dveře s mřížemi na dveřích. Nebýt společné vrátnice mohla by tato společnost fungovat nezávisle na admin. Budově.

Venkovní prostor Za hlavní částí administrativní budovy se nachází venkovní prostor se stromy, který tvoří částečně otevřenou zónu uvnitř areálu. Tento prostor může sloužit jako odpočinková zóna, případně jako průchod do dalších částí areálu.



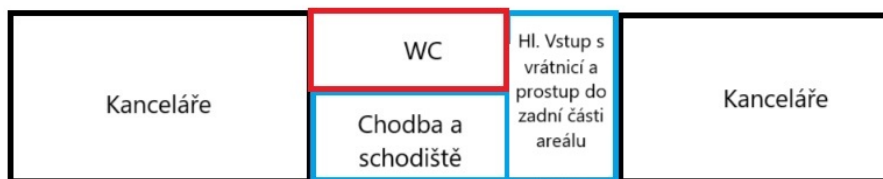
Obrázek 4 Venkovní prostory a suterén

(zdroj: vlastní)

Venkovní prostor zachycený na fotografii se nachází uvnitř areálu, kde slouží jako částečně odpočinková zóna. Tento prostor je situován v blízkosti administrativní budovy, na levé straně snímku, a zároveň poskytuje výhled na další firmu sídlící v areálu, která je viditelná v zadní části fotografie.

Na levé straně fotografie lze vidět okna s mřížemi, která patří k suterénním skladovým a archivním prostorům budovy. Zajímavým prvkem je fakt, že tyto mříže jsou umístěny na oknech z vnitřní části areálu, nikoliv z vnější, což může znamenat určité bezpečnostní riziko na které bude poukázáno v další části této práce.

1.patro – Hlavní vstup a kanceláře



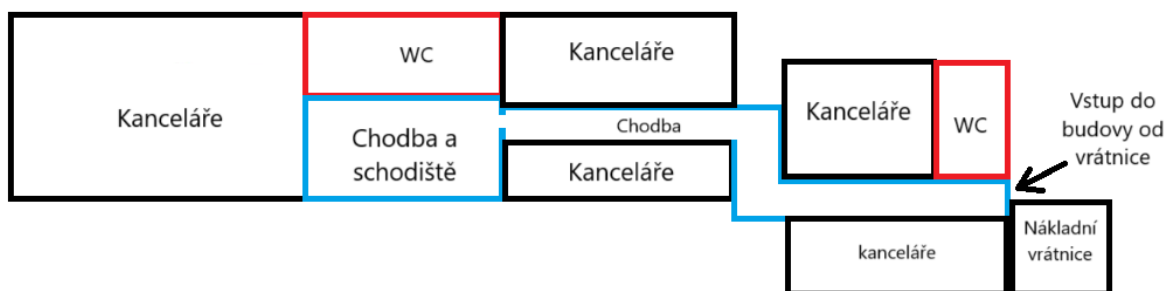
Obrázek 5 První patro

(zdroj: vlastní)

Toto podlaží zahrnuje kancelářské prostory, hlavní vstup s vrátnicí, sociální zázemí a centrální komunikační prostor v podobě chodby se schodištěm. Po obou stranách budovy se nacházejí kanceláře, které slouží různým nájemníkům. Tyto prostory jsou využívány především pro administrativní účely a jsou přístupné z centrální chodby. Každý nájemník si může zabezpečení kanceláře přizpůsobit dle vlastních požadavků. V pravé části přízemí se nachází hlavní vstup, který zahrnuje vrátnici s dohledem pracovníka SBS. Tento vstup zároveň slouží jako průchod do zadní části areálu.

V centrální části budovy se nachází chodba se schodištěm, která propojuje jednotlivá podlaží. Jelikož budova nemá výtah, je schodiště jediným způsobem, jak se dostat do vyšších pater a suterénu. Tato část je rovněž vybavena bezpečnostními prvky, jako jsou PIR detektory, tísňová tlačítka, hydranty a hasicí přístroje, což zajišťuje požární bezpečnost objektu.

2.patro – kanceláře a boční vchod



Obrázek 6 Druhé patro

(zdroj: vlastní)

Druhé patro administrativní budovy se liší od ostatních podlaží především rozšířenou chodbou, která propojuje hlavní část budovy s nákladní vrátnicí a přilehlými kancelářskými prostory. Tato úprava změnila půdorys budovy a umožňuje přímý přístup mezi administrativní částí a logistickým zázemím areálu.

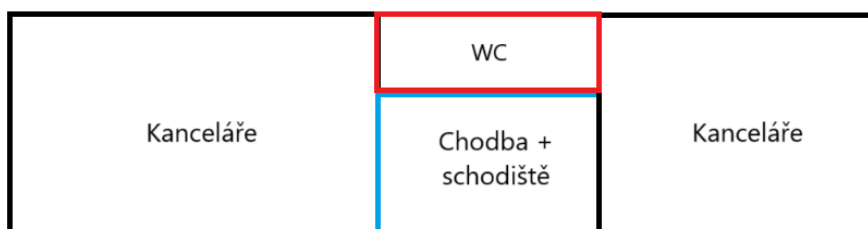
Kancelářské prostory

Podobně jako v přízemí a ostatních patrech se i zde nachází kanceláře různých nájemníků, rozdělené do několika částí. V hlavní části budovy jsou kanceláře umístěné po obou stranách centrální chodby. Další kanceláře se nacházejí v připojené části budovy, která vznikla rozšířením chodeb vedoucích až k vrátnici.

Hlavní chodba a schodiště

Centrální chodba a schodiště zůstávají v tomto patře podobné jako v nižších podlažích. Schodiště slouží jako hlavní komunikační prvek mezi patry, jelikož budova nemá výtah. Chodba propojuje jednotlivé kanceláře a zajišťuje přístup k sociálnímu zázemí.

3 a 4. patro – administrativní prostory



Obrázek 7 Třetí a čtvrté patro

(zdroj: vlastní)

Přízemí, třetí a čtvrté patro mají obdobné rozvržení, přičemž většinu plochy zabírají administrativní kanceláře různých nájemníků. Na chodbách těchto pater jsou rozmístěny PIR detektory napojené na bezpečnostní službu, stejně jako požární tlačítka, hydranty a hasicí přístroje, které zajišťují požární bezpečnost budovy.

Shrnutí

Administrativní budova je důležitým prvkem areálu, protože zde sídlí firma pronajímatele a také, kromě kancelářských prostor zahrnuje i skladové zázemí a propojení s dalšími částmi komplexu. Suterén je využíván primárně ke skladovacím účelům a propojuje budovu s kantýnou a dalšími firmami. Ve druhém patře se nachází unikátní chodba spojující objekt s nákladní vrátnicí, čímž se tato část liší od ostatních podlaží. Bezpečnost budovy je zajištěna standardními prvky včetně PIR detektorů, požárních tlačítek a hydrantů, zatímco provozní dohled je soustředěn do vrátnice v přízemí.

4.3 Závěr kapitoly

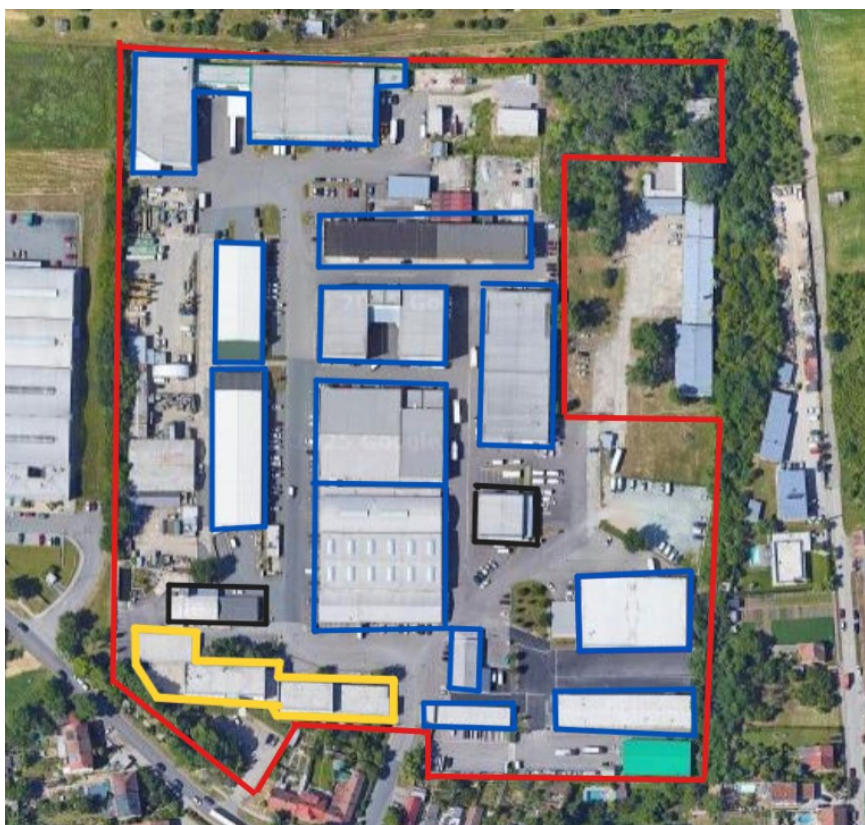
V této kapitole byl poskytnut podrobný popis vybraného areálu, jeho okolí a vnitřního uspořádání. Pro lepší přehlednost byly jednotlivé budovy rozděleny podle jejich funkce. Popsána byla také administrativní budova včetně dispozičního řešení jednotlivých podlaží. Z důvodu ochrany citlivých údajů byla zachována anonymita areálu a jeho konkrétní identita není v textu uvedena.

V rámci této práce bude bezpečnostní analýza zaměřena především na hlavní administrativní budovu, v níž sídlí společnost provozující areál. Dále bude zohledněna bezpečnost perimetru areálu a pohyb osob ve společných venkovních prostorách. Ostatní objekty v areálu nejsou předmětem detailního hodnocení. Toto vymezení umožňuje soustředit pozornost na klíčové oblasti z hlediska řízení a kontroly přístupu.

5 SOUČASNÉ ZABEZPEČENÍ OBJEKTU

Pátá kapitola se zaměřuje na aktuální zabezpečení, včetně ochranných prvků, režimových opatření a technických zabezpečovacích systémů. Popisuje jednotlivé úrovně ochrany, od perimetrické a plášťové ochrany až po prostorovou a režimovou bezpečnost, které společně zajišťují kontrolovaný přístup a dohled nad celým objektem.

V areálu se nachází několik typů budov s různým využitím a odlišnou úrovní zabezpečení. Každý objekt má své specifické prvky ochrany, přičemž obecně platí, že základní zabezpečení zajišťuje pronajímatel, zatímco nájemníci mají možnost si své prostory chránit dle vlastních potřeb.



Obrázek 8 Vyznačené budovy

(zdroj: upraveno z [11])

I. Modře označené budovy – průmyslové a skladovací haly s administrativní částí

Tyto budovy slouží převážně k průmyslovým a skladovacím účelům, přičemž jejich administrativní části zajišťují zázemí pro kanceláře. Základní zabezpečení těchto objektů zahrnuje:

- **PIR detektory**, které nájemníci aktivují a deaktivují prostřednictvím klávesnice. Všechny PIR detektory jsou napojeny na ústřednu v nákladní vrátnici, kde je nepřetržitý dohled pracovníků bezpečnostní služby (SBS).
- **Kouřové hlásiče a hasicí přístroje** umístěné pouze v administrativních částech těchto budov jako součást požární ochrany.
- **Kamerový systém**, který je instalován na budovách a monitoruje venkovní prostory areálu.

Každý nájemník má možnost doplnit si další bezpečnostní prvky dle vlastních potřeb, například přídavné alarmy, přístupové systémy nebo další kamerové pokrytí v rámci svého prostoru.

II. Černě označené budovy – objekty bez základního zabezpečení od pronajímatele

V těchto objektech není instalováno žádné zabezpečení ze strany pronajímatele, pouze hasicí přístroje. Veškeré ochranné systémy, včetně poplachového zabezpečovacího a tísňového systému (PZTS), si zde zajišťují přímo nájemníci. Zabezpečení se tak může výrazně lišit podle individuálních potřeb jednotlivých subjektů.

III. Žlutě označená budova – administrativní budova s kanceláři pronajímatele a dalších firem

Tato budova slouží jako administrativní zázemí a sídlí zde firma, která areál vlastní a spravuje. Nachází se zde také vrátnice, kde je přítomen pracovník SBS v pracovní dny od 6:00 do 17:00. Budova disponuje vyšší úrovní požární ochrany díky požárními tlačítkům, hydrantům a hasicím přístrojům. A ze zabezpečení je každé patro opatřeno PIR detektory na chodbách.

5.1.1 Perimetrická ochrana

Na obrázku 8. je červeně vyznačená perimetrická ochrana. Areál je téměř celý oplocen, přičemž oplocení tvoří kombinaci různých materiálů v závislosti na umístění. Východní a západní strana je oplocena kovovým svařovaným plotem s betonovým základem. Tento plot poskytuje vyšší mechanickou odolnost oproti běžným pleteným plotům a zamezuje

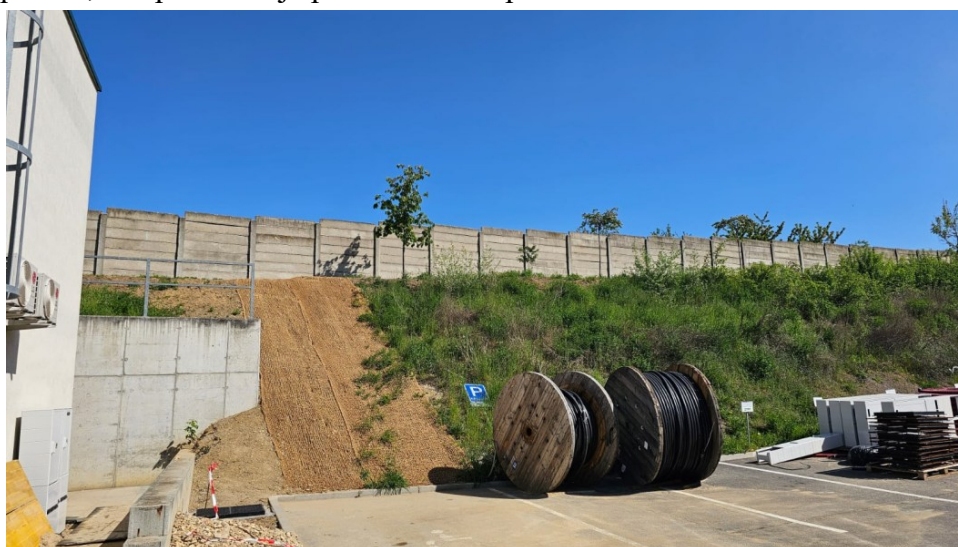
podhrabání. Nicméně, není opatřen detekčními senzory, což může představovat bezpečnostní slabinu.



Obrázek 9 Východní část plotu

(zdroj: vlastní)

Severní strana je chráněna plným betonovým plotem, který zajišťuje vysokou úroveň fyzické bariéry v rámci perimetru areálu. Tento plot poskytuje lepší soukromí a odolnost proti vniknutí, ale zároveň může snižovat přirozenou viditelnost, což může komplikovat dohled nad touto částí areálu. Stejně tak bez dalších doplňkových bezpečnostních systémů, jako jsou ostnaté dráty, nakloněné zábrany nebo detekční prvky, lze betonový plot poměrně snadno přelézt, což představuje potenciální bezpečnostní hrozbu.



Obrázek 10 Severní část plotu

(zdroj: vlastní)

Jižní část areálu má specifické uspořádání z hlediska oplocení a přístupu. Před administrativní budovou se nachází parkoviště, které není nijak fyzicky odděleno od areálu, což znamená, že k budově lze volně přistoupit bez nutnosti překonání jakékoliv bariéry. Tento prostor je využíván jak zaměstnanci areálu, tak návštěvníky. Nicméně, v těsné blízkosti administrativní budovy již oplocení existuje, a to zejména pro oddělení areálu od sousedících zahrad rodinných domků. Tento plot plní především funkci vymezení hranic.



Obrázek 11 Plot na jižní straně

(zdroj:[12])

Hlavní nákladní vrátnice, která se rovněž nachází na jižní straně, slouží jako hlavní vstup do uzavřené části areálu. Odtud je již perimetrická ochrana plně zajištěna oplocením, které navazuje na ostatní části areálu.

5.1.2 Plášťová ochrana

Plášťová ochrana administrativní budovy je zajištěna kombinací základních mechanických zábranných systémů (dále jen MZS) a technických prostředků. Mechanické prvky, jako jsou standardní uzamykatelné dveře a okenní výplně, poskytují základní fyzickou bariéru proti neoprávněnému vniknutí. Významnou roli však hraje především dohledový video systém (dále jen DV), který zajišťuje nepřetržitý vizuální monitoring klíčových částí budovy i jejího okolí. Budova je pod trvalým dohledem, přičemž záznamy a živé přenosy z kamer jsou dostupné jak majiteli areálu, tak bezpečnostní službě (SBS). Tato služba zajišťuje nepřetržitý bezpečnostní dohled a kontrolu pohybu osob a vozidel jak v rámci administrativní části, tak celého perimetru areálu.

Dohledový video systém

Dohledový video systém je instalován strategicky tak, aby pokrýval celý areál, včetně vzdálenějších koutů, kde by mohlo dojít k neoprávněnému pohybu osob. Kamery jsou

umístěny především u všech vstupů do areálu, včetně hlavního vstupu, nákladní vrátnice a vstupu do kantýny z venkovní strany. Na většině budov, odkud monitorují venkovní prostory a komunikační trasy v areálu a na perimetru areálu, kde pokrývají rizikové oblasti, včetně oplocení a přístupových cest.

Kamery jsou vybaveny IR přísvitem, což umožňuje zlepšenou viditelnost v horších světelných podmínkách nebo během nočního provozu. Záznamy lze sledovat v reálném čase a zároveň jsou uchovávány po určitou dobu pro případnou analýzu bezpečnostních incidentů.

Mechanické zábranné systémy (MZS)

Kromě kamerového dohledu je plášťová ochrana zajištěna také mechanickými bezpečnostními prvky, které zahrnují: Uzamykatelné vstupy do všech administrativních a průmyslových budov. Mříže na oknech skladovacích prostor v suterénu pouze jen z vnitřní strany areálu, které snižují riziko vniknutí.

5.1.3 Prostorová ochrana

Prostorová ochrana areálu se skládá z kombinace požárních a bezpečnostních prvků, které zajišťují ochranu osob i majetku uvnitř budov. Důraz je kladen na požární bezpečnost, označení únikových cest a rozmístění bezpečnostních prvků napříč areálem.

Požární ochrana

Součástí požární ochrany jsou v budovách umístěny hasicí přístroje a hydranty, které jsou rozmístěny na strategických místech administrativní budovy i průmyslových hal. Součástí systému jsou rovněž požární tlačítka, která umožňují okamžité spuštění poplachu v případě požáru. Požární evakuační plán je vyvěšen v hlavních komunikačních prostorech a únikové východy jsou jasně označeny tak, aby v případě nutnosti umožnily rychlou a bezpečnou evakuaci osob z objektu.



Obrázek 12 Požární hydrant a tlačítko

(zdroj: vlastní)

Požární bezpečnost je v areálu nastavena dle platných předpisů, přičemž administrativní budova disponuje vyšší úrovní požární ochrany v rámci celého komplexu.

Bezpečnostní opatření v budovách

Každá budova v areálu disponuje mechanickými zábranami, které zajišťují její bezpečnost. Sklady a archivy v suterénních prostorech obsahují mříže na oknech a dveřích, aby bylo ztíženo neoprávněné vniknutí.



Obrázek 13 Archiv a sklady

(zdroj: vlastní)

Administrativní budova je přístupná přes hlavní vstup a nákladní vrátnici. Veškerý přístup do areálu je monitorován kamerovým systémem, který sleduje pohyb osob i vozidel.

Některé budovy, především skladové a průmyslové haly, jsou chráněny pouze základním zabezpečením v podobě PIR detektorů, které jsou napojeny na ústřednu PZTS a celá ústředna zároveň připojena na DPPC. Ostatní nájemci si mohou zabezpečení upravit dle vlastních potřeb, například pomocí přístupových systémů nebo poplachových zařízení.

5.1.4 Předmětová ochrana

Předmětová ochrana v areálu se zaměřuje na zabezpečení důležitých prostor a vybavení proti krádeži nebo neoprávněnému přístupu. V kancelářích administrativní budovy mají zaměstnanci možnost uzamykat důležité dokumenty a cennosti do zamykatelných skříní případně do vlastních trezorů.

Administrativní budova neobsahuje centrální trezor, jednotlivé společnosti si zabezpečení hodnotných předmětů řeší individuálně.

5.1.5 Režimová opatření

V rámci režimových opatření je v areálu zajištěna kontrola vstupů a pohybu osob prostřednictvím dvou vrátnic, systému evidence a kamerového dohledu. Součástí těchto opatření je také provoz klíčové služby, pravidelné fyzické kontroly a další bezpečnostní mechanismy, které jsou popsány dále.

Přístupové body do areálu.

Areál disponuje dvěma vrátnicemi, které zajišťují kontrolovaný přístup osob i vozidel:

- Administrativní vrátnice je umístěna v přízemí administrativní budovy a slouží jako hlavní vstup pro pěší návštěvníky a zaměstnance. V pracovní dny je tato vrátnice přístupná od 6:00 do 17:00. přičemž každý návštěvník by se měl při vstupu nahlásit na vrátnici, kde je ověřen pracovníkem bezpečnostní služby (SBS).
- Nákladní vrátnice se nachází v jižní části areálu a představuje hlavní kontrolovaný vstup do areálu. Je nepřetržitě střežena SBS a slouží jak pro vstup osob mimo pracovní dobu, tak především pro vjezd schválených vozidel a dodavatelů. Každé nákladní vozidlo by mělo být při vjezdu evidováno a kontrolováno. Vjezd do areálu je zajištěn přes nákladní vrátnici

opatřenou posuvnou branou a závorou, která je ovládána pracovníkem SBS. Po pracovní době je vstup do administrativní budovy umožněn výhradně přes tuto nákladní vrátnici a pouze na základě povolení, čímž se snižuje riziko neoprávněného pohybu osob v budově.

Ostatní vstupy do průmyslových hal a skladovacích prostor nejsou centrálně řízeny jejich správou a režim vstupu si zajišťují jednotliví nájemci dle vlastních provozních pravidel. Každý nájemce tak odpovídá za kontrolu přístupu do svého prostoru a za zamezení vstupu nepovolaných osob. Osoby bez oprávnění nesmí vstupovat do jiných částí areálu. Celý areál je pod nepřetržitým dohledem kamerového systému, který sleduje hlavní vstupy, vjezdy a důležité body v rámci společných prostor. Bezpečnostní opatření zahrnují rovněž kontrolu pohybu osob a majetku.

Fyzická ostraha

Součástí režimových opatření je také pravidelná obchůzka bezpečnostní služby (SBS). Každou hodinu provádí jeden z vrátných fyzickou kontrolu areálu, přičemž prochází kolem oplocení, kontroluje neporušenost pletiva, dveří a oken na budovách a sleduje případné známky narušení. Pro zajištění pravidelnosti obchůzek se strážný musí při každém kontrolním bodě prokazovat načtením identifikačního čipu, který zaznamenává jeho přítomnost na daném místě. Tímto je i dosaženo toho, že strážní mají zároveň vytyčenou trasu, kterou musí projít a nevynechají tak žádné zákoutí.



Obrázek 14 Identifikační čip na budově

(zdroj: vlastní)

Druhý pracovník na vrátnici tak sleduje pohyb kolegy v reálném čase, což zajišťuje nejen důslednost kontrol, ale i bezpečnost samotného strážného při obchůzkách. Tento systém je provozován v nepřetržitém režimu 24/7, což znamená, že i v nočních hodinách je areál pravidelně monitorován a kontrolován.

Součástí nákladní vrátnice je kromě dohledového stanoviště také hlavní klíčový depozit a tzv. klíčová služba, která zajišťuje správu, evidenci a výdej klíčů k vybraným částem areálu. Tento systém umožňuje bezpečnostní službě rychlý a organizovaný přístup do konkrétních prostor v případě mimořádných událostí, jako je požár, havárie vody nebo technická závada, a může být využit i při běžných provozních či servisních činnostech. Přístup do citlivých míst, jako jsou technické místnosti nebo archivy, je přísně omezen pouze na autorizované osoby, čímž je minimalizováno riziko neoprávněného vstupu a narušení bezpečnosti klíčových částí objektu.

Kombinace fyzických kontrol, kamerového systému a elektronického sledování obchůzek vytváří komplexní bezpečnostní mechanismus, který pomáhá předcházet narušením a udržuje areál v bezpečném provozu.

5.1.6 Bezpečnostní dokumentace

Pro zajištění bezpečnosti areálu je vedena bezpečnostní dokumentace, která zahrnuje dokumenty vztahující se k požární ochraně (PO) a bezpečnosti a ochraně zdraví při práci (BOZP). Tyto dokumenty stanovují povinnosti, odpovědnosti a pravidla pro zajištění bezpečného provozu areálu a jeho jednotlivých částí.

V oblasti požární ochrany je zajištěna pravidelná kontrola požárních opatření. Osobou odpovědnou za PO je majitel areálu, který odpovídá za revize požárních zařízení. Každý nájemce je zároveň odpovědný za požární bezpečnost ve svých prostorách a musí dodržovat stanovená opatření. Externí technik provádí pravidelné kontroly požárního zabezpečení minimálně 1x ročně.

V rámci BOZP se každý nájemce stará o bezpečnost svých zaměstnanců nezávisle, avšak vlastník areálu zajišťuje dodržování základních bezpečnostních předpisů ve společných prostorech a školení vlastních zaměstnanců.

Součástí dokumentace jsou také evakuační plány a krizová opatření, která jsou vyvěšena ve společných prostorech a určují postupy pro případ mimořádných situací.

5.2 Závěr kapitoly

Cílem této kapitoly bylo zhodnotit současné zabezpečení areálu a popsat jednotlivé prvky, které přispívají k jeho ochraně. Byla rozebrána perimetrická ochrana, plášťová ochrana, prostorová ochrana, režimová opatření i bezpečnostní dokumentace.

Jednotlivé prvky zabezpečení jsou navrženy tak, aby zajišťovaly kontrolovaný pohyb osob, ochranu majetku a minimalizaci rizik. Efektivita těchto opatření však bude analyzována v následující kapitole, kde budou identifikovány případné bezpečnostní slabiny a navržena možná zlepšení pro zvýšení.

6 ANALÝZA RIZIK

Před samotnou analýzou rizik je nezbytné nejprve určit všechna aktiva, která je třeba chránit, a identifikovat možné hrozby, které by je mohly ohrozit. Teprve poté lze přistoupit k samotnému vyhodnocení rizik. V tomto případě bude analýza provedena s využitím metod Checklist a FMEA, v souladu s tím, co bylo popsáno v teoretické části.

6.1 Identifikace aktiv v areálu

Tato kapitola se zaměřuje na přehled aktiv nacházejících se v areálu a jejich rozdělení dle charakteru na hmotná a nehmotná. Identifikace vychází z teoretického základu uvedeného v předchozí části práce. Součástí je i orientační odhad hodnoty jednotlivých kategorií pro potřeby další analýzy rizik.

- **Hmotná aktiva**

- **Zaměstnanci**
- **Návštěvníci**
- **Vozidla**
 - Firemní vozidla
 - Nákladní vozidla
 - Vozidla zaměstnanců
- **Venkovní areál**
 - Parkoviště
 - Osvětlení areálu
 - Oplocení a vstupní brány
 - Zelené plochy a stromy
 - Požární nádrž
- **Budovy**
 - Kanceláře
 - Nábytek
 - Dokumentace v tištěné podobě

- Elektronická zařízení (PC, tiskárny,)
- Finanční hotovost
- **Energetická infrastruktura**
 - Rozvodna elektrické energie
 - Kotle a plynové rozvody
 - Hlavní uzávěry energií (plyn, voda, elektřina)
 - Klimatizace
- **Technické zázemí**
 - Serverovna
 - Požární systémy
 - Vodovodní a kanalizační systémy
- **Sociální a odpočinkové zázemí**
 - Odpočinkové zóny (lavičky venku pod stromy)
 - Sociální zařízení
- **Nehmotná aktiva**
 - Interní databáze a informační systémy, Zálohy dat a cloudové úložiště, Internetové Stránky, Emaily zaměstnanců
 - Bankovní účty

Tabulka 2 Odhad hodnoty hmotných aktiv

Segment	Cenový odhad (Kč)
Administrativní budova	100 000 000
Sklady a haly	800 000 000
Dopravní technika	4 600 000
Vybavení kanceláří	4 100 000
Bezpečnostní systémy	3 250 000
IT infrastruktura	4 500 000
Sociální zázemí	3 200 000

(zdroj: vlastní)

K identifikaci aktiv je třeba uvést, že tato analýza se zaměřuje výhradně na hmotná a nehmotná aktiva identifikovatelná v rámci areálu a administrativní budovy. Posouzení kontinuity provozu, závislostí na dodavatelských řetězcích či provozní návaznosti není předmětem tohoto zpracování.

Dále je nutné upozornit, že skladovací haly a přilehlé prostory jsou pronajímány jednotlivým nájemcům, kteří si zajišťují bezpečnostní opatření samostatně. Tyto části areálu nejsou v kompetenci provozovatele, a proto nejsou zahrnuty do identifikace ani do dalšího hodnocení rizik.

6.2 Identifikace hrozeb

Tato podkapitola popisuje a kategorizuje potenciální hrozby, které mohou ohrozit aktiva.

Při analýze rizik areálu je nezbytné zohlednit všechny reálné hrozby, které mohou negativně ovlivnit bezpečnost, provoz nebo hodnotu majetku. Tyto hrozby mohou mít různorodý charakter a zahrnují fyzické, kybernetické, přírodní a provozní rizikové faktory. Následující kapitola podrobně popisuje jednotlivé typy hrozeb a poskytuje konkrétní příklady jejich výskytu v prostředí průmyslového areálu.

6.2.1 Fyzické hrozby

Fyzické a kriminální hrozby představují významné riziko pro osoby, majetek a infrastrukturu areálu. Mohou být způsobeny jak lidským faktorem, tak technickým selháním nebo vnějšími vlivy.

- **Příklady fyzických a kriminálních hrozeb v areálu:**

- **Požár:** Může vzniknout v důsledku technické závady, lidské chyby nebo úmyslného jednání, například žhárství či nevhodné manipulace s hořlavými materiály.
- **Krádeže a vandalismus:** Nedostatečné zabezpečení objektu může usnadnit odcizení vybavení, výrobního materiálu nebo narušení provozu formou úmyslného poškození zařízení.
- **Úrazy zaměstnanců:** Pády, nehody

Preventivní opatření zahrnují moderní zabezpečovací systémy (kamerové systémy, přístupové systémy), pravidelnou údržbu technologií, školení zaměstnanců v oblasti bezpečnosti a důsledné dodržování bezpečnostních směrnic.

6.2.2 Kybernetické hrozby

Moderní průmyslové areály jsou stále více závislé na digitální infrastruktuře, což přináší rizika spojená s kybernetickou bezpečností. Kybernetické útoky mohou narušit provoz, vést k odcizení citlivých informací nebo ohrožit fyzickou bezpečnost prostřednictvím napadení chytrých zařízení či řídicích systémů.

- **Příklady kybernetických hrozeb v areálu:**

- **Útoky na IT infrastrukturu:** Neoprávněný přístup k databázím, systémům řízení budov, bezpečnostním kamerám nebo výrobním linkám může vést k narušení provozu.
- **Ransomware útoky:** Škodlivý software blokující přístup k systémům nebo datům s požadavkem na výkupné může paralyzovat výrobu a způsobit významné finanční ztráty.
- **Phishingové útoky:** Zaměřené na získání přístupových údajů zaměstnanců nebo dodavatelů, což může vést k neoprávněnému přístupu do kritických systémů.

Prevence kybernetických hrozeb zahrnuje pravidelnou aktualizaci softwaru, použití bezpečných hesel, víceúrovňovou autentizaci, důkladné školení zaměstnanců o hrozbách (např. phishing) a segmentaci sítě, aby bylo možné izolovat napadené systémy.

6.2.3 Přírodní hrozby

Přírodní hrozby jsou nepředvídatelné události způsobené vnějšími vlivy, které mohou poškodit infrastrukturu areálu, narušit provoz nebo ohrožit bezpečnost zaměstnanců.

- **Příklady přírodních hrozeb v areálu:**

- **Extrémní počasí:** Silné bouřky, vichřice, přívalové deště a kroupy mohou poškodit budovy, dopravní infrastrukturu a výrobní zařízení.
- **Povodně a záplavy:** Areál je cca 100 m od povodňové oblasti. Tzn. tento problém se ho netýká.
- **Extrémní teploty:** Dlouhodobé období mrazů nebo vlny veder mohou zvýšit riziko požárů či poruch zařízení.

Řešení přírodních hrozeb zahrnuje pevné konstrukční prvky, pravidelnou údržbu budov, plány pro nepříznivé podmínky a mít zjednané dobré pojištění, které tyto události pokryje.

6.2.4 Provozní hrozby

Provozní hrozby zahrnují selhání technických zařízení, chyby v řízení provozu nebo lidské pochybení, které mohou vést k přerušení výroby, ohrožení bezpečnosti nebo ekonomickým ztrátám.

- **Příklady provozních hrozeb v areálu:**
 - **Blackout nebo výpadek elektřiny:** Přerušení dodávky elektřiny může, výpadek zabezpečovacích systémů nebo nefunkčnost IT infrastruktury (servery, síťové prvky, počítače; blackout může způsobit ztrátu dat, poškození zařízení nebo výpadek komunikace.)
 - **Poškození vodovodního a kanalizačního systému:** Prasknutí potrubí nebo ucpání odpadních cest může způsobit znečištění pracovního prostředí a výpadky v provozu.

Řešení provozních hrozeb zahrnuje pravidelnou kontrolu a údržbu technologií, implementaci záložních zdrojů energie (generátory, UPS), školení zaměstnanců a vytvoření krizových plánů pro mimořádné situace.

6.2.5 Hrozby způsobené lidským faktorem

Lidský faktor představuje jednu z největších bezpečnostních hrozeb v průmyslovém areálu. Může jít o úmyslné nebo neúmyslné jednání, které způsobí materiální škody, finanční ztráty nebo ohrozí bezpečnost osob.

- **Porušení bezpečnostních předpisů:** Nedodržování pracovních postupů a předpisů může vést k nehodám a úrazům.
- **Užívání návykových látek na pracovišti:** Konzumace alkoholu nebo drog může vést k ohrožení provozu i ostatních zaměstnanců.
- **Únik citlivých informací:** Interní data, například obchodní strategie nebo výrobní postupy, mohou být zneužita konkurencí nebo neoprávněnými osobami.

Preventivní opatření zahrnují přísnou kontrolu přístupu k citlivým oblastem, důsledné školení zaměstnanců, zavedení interních bezpečnostních směrnic a pravidelné prověrky bezpečnostních opatření.

6.3 Analýza rizik (Checklist Analysis - CLA)

Cílem této podkapitoly je identifikovat potenciální slabiny, které by mohly být využity k narušení bezpečnosti areálu. Sestavení Checklistu probíhalo systematicky podle jednotlivých úrovní ochrany, počínaje perimetrickou ochranou až po ochranu jednotlivých objektů a zařízení. Vyhodnocení jednotlivých otázek bylo provedeno na základě dostupných informací a analýzy současného zabezpečení.

6.3.1 Perimetrická ochrana areálu

Tabulka 3 Checklist perimetrické ochrany

Perimetrická ochrana		
Mechanické zábranné systémy		
Otázka	Ano	Ne
Má areál oplocení po celém obvodu?	✓	
Je oplocení v dobrém technickém stavu?	✓	
Je výška plotu dostatečná (150–200 cm)?	✓	
Je oplocení z pletiva?	✓	
Je oplocení kombinované (Pletivo + beton)	✓	
Je při instalaci perimetrických prvků zachována dostatečná vzdálenost od vegetace a terénních nerovností ovlivňujících jejich funkci?	✓	
Jsou součástí perimetrické ochrany vstupní brány?	✓	
Má oplocení doplňkové zábrany (ostnatý drát, otočné válce)?		✓
Existuje dostatečná ochrana proti vniknutí vozidel (zátarasy, bariéry)?		✓
Elektronické systémy		
Je ochrana zajištěna po celém perimetru objektu (IR bariéry, detekční kabely)?		✓
Zahrnuje perimetrická ochrana elektronický systém kontroly vstupu (ESKV)?		✓
Jsou v rámci perimetrické ochrany instalovány prvky PZTS		✓
Je v rámci perimetrické ochrany instalován kamerový systém	✓	
Fyzická ostraha		
Je perimetr hlídán fyzickou ostrahou?	✓	

Probíhá pravidelná kontrola perimetru ze strany fyzické ostrahy?	✓	
Režimová opatření		
Je zavedena kontrola vstupu do perimetru objektu?	✓	
Jsou vozidla na parkovišti dodatečně chráněna?		✓
Provádí se pravidelně kontrola bezpečnostních prvků perimetru?	✓	
Jsou všechny vstupní brány uzamčeny?		✓

(zdroj: vlastní)

Zhodnocení stavu perimetrické ochrany areálu:

Na základě provedené analýzy a odpovědí v checklistu lze konstatovat, že perimetrická ochrana základní úroveň zabezpečení splňuje, avšak obsahuje několik významných slabin, které mohou být potenciálním rizikem pro bezpečnost areálu.

Pozitivní aspekty perimetrické ochrany:

- ✓ Areál je oplocen po celém obvodu, což zajišťuje základní fyzickou bariéru proti neoprávněnému vstupu.
- ✓ Oplocení je kombinované (pletivo + beton), což poskytuje vyšší mechanickou odolnost než pouze pletivový plot.
- ✓ Výška oplocení splňuje standardy (150–200 cm) a ztěžuje neoprávněný vstup.
- ✓ Vstupní brány jsou součástí perimetrické ochrany a umožňují regulovaný přístup do areálu.
- ✓ Fyzická ostraha provádí pravidelné kontroly perimetru, což zvyšuje celkovou úroveň zabezpečení.
- ✓ Je instalován kamerový systém v rámci perimetrické ochrany, což zlepšuje dohled a monitoring nad vstupy.

Identifikované slabiny a bezpečnostní nedostatky:

✗ Oplocení nemá doplňkové zábrany, jako je ostnatý drát nebo otočné válce, což zvyšuje riziko přelezení obzvláště na severní části pozemku.



Obrázek 15 severní část plotu

(zdroj: vlastní)

✗ Chybí ochrana proti vniknutí vozidel (např. zátarasy, pevné bariéry), což může usnadnit násilné vniknutí vozidlem.

✗ Neexistuje elektronická detekce narušení perimetru, jako jsou IR bariéry nebo detekční kabely, což znamená, že neoprávněný vstup není automaticky detekován v odlehlých oblastech areálu.

✗ Perimetrická ochrana neobsahuje elektronický systém kontroly vstupu (ESKV), což znamená, že přístup je regulován pouze fyzickou kontrolou, která nemusí být vždy na místě.

✗ Není zajištěna zvláštní ochrana aut na parkovišti, což může vést k potenciálním krádežím nebo vandalismu.

6.3.2 Prostorová ochrana areálu

Tabulka 4 Checklist prostorové ochrany areálu.

Prostorová ochrana areálu		
Otázka	Ano	Ne
Je v areálu zajištěno dostatečné osvětlení?	✓	
Jsou v areálu hlídkové trasy pro ostrahu?	✓	
Je kamerový systém napojen na DPPC?	✓	
Jsou kamery vybaveny funkcí nočního vidění pro záznam ve zhoršených světelných podmínkách?	✓	

(zdroj: vlastní)

6.3.3 Kontrolní seznam pro budovy

Tabulka 5 Checklist plášťové ochrany

Plášťová ochrana		
Mechanické zábranné systémy		
Otázka	Ano	Ne
Mají všechny budovy instalovány bezpečnostní dveře?		✓
Nachází se na hlavních dveřích speciální zámky?		✓
Jsou všechny vchody, okna a nouzové východy řádně uzavíratelné?	✓	
Jsou okna chráněna proti neoprávněnému vniknutí (fólie, mříže, rolety)?		✓
Jsou pravidelně kontrolovány zámky a závory u vchodů?	✓	
Jsou dveře opatřeny panikovým kováním?	✓	
Elektronické systémy		
Jsou přístupové body do budov kontrolovány (kamery, SKV, ostraha)?	✓	
Jsou pravidelně kontrolovány a udržovány venkovní kamery a alarmy?	✓	
Je monitorování zajištěno po celém obvodu objektu?	✓	
Režimová opatření		
Jsou osoby u hlavního vstupu kontrolovány?		✓
Je omezený režim vstupu?	✓	
Je nastavený režim pro příchozí návštěvníky?		✓
Je určena odpovědná osoba za kontrolu vstupu do budovy?	✓	
Má plášť budov ochranu proti vandalismu (anti graffiti nátěr, osvětlení)?		✓
Jsou vnější prostory budov dobře osvětleny?	✓	

Plášťová ochrana		
Otázka	Ano	Ne
Režimová opatření		
Existuje systém pro hlášení podezřelých aktivit v okolí budov?	✓	
Jsou jasně označeny nouzové východy a únikové cesty z budov?	✓	

(zdroj: vlastní)

Pozitivní aspekty plášťové ochrany:

- ✓ Všechna okna, vchody a nouzové východy jsou řádně uzavíratelné, což minimalizuje možnosti neoprávněného přístupu.
- ✓ Pravidelně se provádí kontrola zámků a závor u vstupů, čímž se předchází jejich poškození nebo zneužití.
- ✓ Dveře jsou opatřeny panikovým kováním, což zajišťuje bezpečný únik osob v případě nouzové situace.
- ✓ Budovy jsou monitorovány kamerovým systémem, přičemž přístupové body jsou pod kontrolou bezpečnostních prvků, jako jsou alarmy a fyzická ostraha.
- ✓ Plášť budov je dobře osvětlen, což snižuje pravděpodobnost vandalismu nebo neoprávněného vniknutí.
- ✓ Nouzové východy a únikové cesty jsou jasně označeny, což usnadňuje evakuaci v krizových situacích.

Identifikované slabiny a bezpečnostní nedostatky:

- ✗ Budovy nejsou vybaveny bezpečnostními dveřmi, což zvyšuje riziko násilného vniknutí nebo poškození vstupů.
- ✗ Hlavní vstupy nejsou opatřeny speciálními bezpečnostními zámkami, což znamená, že jejich překonání může být snadnější než u standardně zabezpečených objektů.
- ✗ Okna nejsou chráněna proti neoprávněnému vniknutí (např. bezpečnostní fólie, mříže, rolety), což může představovat zranitelné místo pro násilné vniknutí, zejména v méně monitorovaných částech areálu.

✗ Plášť budov nemá ochranu proti vandalismu (např. antigrffiti nátěry nebo speciální povrchy), což může vést k estetickému poškození budov, ale i ke zhoršení celkové bezpečnostní úrovně.



Obrázek 16 hl. rozvodna

(zdroj: vlastní)

Tabulka 6 Checklist prostorové ochrany budov

Prostorová ochrana budov		
Požární ochrana		
Otázka	Ano	Ne
Jsou v budovách funkční a pravidelně kontrolované hasicí přístroje?	✓	
Jsou v budovách instalovány požární hlásiče a hlásiče kouře?		✓
Jsou v budovách požární uzávěry (dveře, klapky) v dobrém stavu?	✓	
Jsou v budovách pravidelně prováděny požární cvičení?		✓
Je v budovách umístěna aktuální požární dokumentace?	✓	
Je požární zabezpečení budovy funkční?	✓	
Mechanické zábranné systémy		
Jsou zabezpečeny technické místnosti a serverovny?		✓
Jsou únikové cesty volné a nezatarasené?	✓	
Jsou únikové východy správně označené a osvětlené?	✓	
Jsou dveře únikových východů snadno otevíratelné zevnitř?	✓	

Elektronické systémy		
Jsou vnitřní prostory budov pokryty kamerovým systémem s dostatečným rozlišením?		✓
Jsou v budovách instalovány detektory pohybu (PIR detektory)?	✓	
Je bezpečnostní systém napojen na dohledové a poplachové přijímací centrum (DPPC) nebo jiný dohledový systém?	✓	
Jsou kamery vybaveny funkcí nočního vidění pro záznam ve zhoršených světelných podmínkách?	✓	
Jsou dveře do důležitých prostor (serverovny, archivy) vybaveny kontrolou přístupu (karty, kódy)?		✓
Jsou v budovách instalovány paniková tlačítka pro přivolání pomoci v nouzových situacích?		✓
Jsou v budovách systémy pro detekci a potlačení požáru v kritických prostorech (serverovny)?		✓
Existuje systém pro pravidelné testování a údržbu všech bezpečnostních systémů?	✓	
Režimová opatření		
Je v budově zajištěna kontrola přístupových karet a vstupních kódů?		✓
Existuje plán evakuace pro případ nouze?	✓	
Je zajištěna pravidelná údržba a kontrola bezpečnostních systémů?	✓	
Je zajištěna klíčová služba pro případ nouze?	✓	
Fyzická ostraha		
Je v areálu fyzická ostraha?	✓	
Pracuje FO v režimu 24/7?	✓	
Jsou v areálu hlídkové trasy pro ostrahu?	✓	
Kyberbezpečnost		
Jsou servery a databáze chráněny proti neoprávněnému přístupu?	✓	
Je prováděno pravidelné zálohování dat?	✓	
Jsou pravidelně aktualizovány firmwary bezpečnostních systémů?	✓	
Bezpečnost a ochrana zdraví při práci		
Je zajištěno pravidelné školení zaměstnanců v oblasti BOZP?	✓	
Předmětová ochrana		
Je v budově centrální trezor		✓
Je součástí společnosti trezor na dokumenty, finanční prostředky a jiné listiny?	✓	

(zdroj: vlastní)

Pozitivní aspekty prostorové ochrany:

- ✓ V budovách jsou funkční a pravidelně kontrolované hasicí přístroje, což zajišťuje základní požární ochranu.
- ✓ Požární uzávěry (dveře, klapky) jsou v dobrém stavu, což přispívá k efektivnímu oddělení požárních úseků.
- ✓ V budovách je umístěna aktuální požární dokumentace, která je dostupná pro příslušné osoby.
- ✓ Únikové cesty jsou volné a správně označené, což umožňuje bezpečnou evakuaci.
- ✓ Existuje plán evakuace pro případ nouze, což zajišťuje připravenost na bezpečnostní incidenty.
- ✓ Fyzická ostraha má definované hlídkové trasy, čímž je zajištěna pravidelná kontrola objektu.
- ✓ Kyberbezpečnost je do určité míry řešena – servery jsou chráněny proti neoprávněnému přístupu a je prováděno pravidelné zálohování dat.
- ✓ Firmware bezpečnostních systémů jsou pravidelně aktualizovány, což minimalizuje zranitelnost vůči kybernetickým hrozbám.

Identifikované slabiny a bezpečnostní nedostatky:

- ✗ V budovách nejsou instalovány požární hlásiče a detektory kouře, což zvyšuje riziko opožděné detekce požáru.
- ✗ Technické místnosti a serverovny nejsou adekvátně zabezpečeny, což může vést k neoprávněnému přístupu nebo ohrožení citlivých dat.
- ✗ Vnitřní prostory nejsou dostatečně pokryty kamerovým systémem, což může znamenat slepá místa v monitorování budovy.
- ✗ V budovách chybí paniková tlačítka pro přivolání pomoci, což může zpomalit reakci v případě nouzové situace.
- ✗ Nejsou implementovány systémy pro detekci a potlačení požáru v kritických prostorech (např. serverovnách), což představuje riziko ztráty dat při požáru.

Pomocí metody Checklist Analysis (CLA) byla identifikována klíčová slabá místa v zabezpečení areálu, zejména v oblasti mechanické ochrany vstupů, absence vnitřního kamerového systému a požárních hlásičů. V následující podkapitole budou tyto zjištěné nedostatky dále analyzovány pomocí metody FMEA, která umožní detailnější vyhodnocení jejich dopadu a návrh opatření ke zvýšení bezpečnosti.

6.4 Analýza RIZIK – FMEA

Na základě předchozí analýzy CLA byla identifikována klíčová slabá místa v zabezpečení areálu, zejména nedostatečná mechanická ochrana vstupů, absence kamerového systému uvnitř budovy a chybějící prvky požární ochrany. V této kapitole bude provedena detailní analýza rizik pomocí metody FMEA výsledkem bude návrh konkrétních opatření ke zvýšení bezpečnosti areálu na základě prioritizace rizik.

Analýza FMEA (Failure Mode and Effects Analysis) je metoda sloužící k identifikaci možných hrozeb, jejich příčin a následků. Jejím hlavním cílem je předcházet a minimalizovat rizika, která by mohla vést k poruchám, škodám nebo ztrátám. FMEA pracuje na principu identifikace potenciálních selhání (failure modes), přičemž pro každé z nich analyzuje příčiny a dopady na systém, proces či organizaci. Každé hrozbě je přiřazena číselná hodnota podle tří kritérií: význam, výskyt a odhalitelnost. Z těchto hodnot se následně vypočítává rizikové prioritní číslo (Risk Priority Number, RPN), které pomáhá určit nejkritičtější vady vyžadující prioritní řešení. [13]

6.4.1 Faktory hodnocení jsou:

- a) **Význam (Severity)** – Určuje závažnost následků selhání. Hodnotí se na škále od 1 do 10, kde 1 představuje minimální vliv a 10 značí maximální, až katastrofální dopad na zaměstnance, podnik či zákazníky.
- b) **Výskyt (Occurrence)** – Vyjadřuje pravděpodobnost výskytu selhání. Hodnota se pohybuje od 1 do 10, kde 1 znamená velmi nepravděpodobný výskyt a 10 označuje vysokou pravděpodobnost opakovaného výskytu.
- c) **Odhalitelnost (Detectability)** – Měří pravděpodobnost, že selhání bude odhaleno dříve, než způsobí škodu. Hodnotí se rovněž na stupnici od 1 do 10, kde 1 znamená, že problém lze snadno identifikovat, zatímco 10 znamená, že jeho detekce je velmi obtížná. [13]

6.4.2 Proces analýzy se skládá z těchto kroků:

- a) **Výpočet RPN** – Rizikové prioritní číslo je určeno součinem hodnot významu, výskytu a odhalitelnosti ($RPN = S \times O \times D$). Vyšší hodnota RPN znamená vyšší prioritu pro řešení dané vady.
- b) **Identifikace kritických vad** – Po výpočtu RPN jsou vady s nejvyššími hodnotami považovány za nejzávažnější a vyžadují okamžitou pozornost.
- c) **Návrh opatření** – Pro kritické vady jsou navržena opatření ke snížení rizika, například změna procesů, zavedení dodatečných kontrolních mechanismů, zlepšení zabezpečení objektu či školení zaměstnanců.
- d) **Implementace opatření a opětovné hodnocení** – Po provedení navržených opatření se hodnoty významu, výskytu a odhalitelnosti přehodnocují, aby bylo možné určit, zda došlo ke snížení celkového rizika. [13]

Před použitím metody FMEA je nezbytné stanovit hodnoticí tabulky, které přesně určují význam jednotlivých kritérií. Jedním z faktorů při hodnocení rizika je jeho význam, který určuje, jak závažné důsledky může mít pro budovy/areál. Rozlišujeme dvě hlavní kategorie dopadů: majetkovou škodu a ohrožení zdraví či života osob v objektu.

Tabulka 7 Význam

Význam		
Hodnota S	Význam pro areál	Popis
1	Velmi nízký	Majetková škoda do 50 000 Kč / žádné zranění
2	Nízký	Majetková škoda do 250 000 Kč / drobné poranění
3		Majetková škoda do 1 000 000 Kč / mírný stres zaměstnanců
4	Střední	Majetková škoda do 3 000 000 Kč / lehké zranění
5		Majetková škoda do 7 000 000 Kč / středně těžké zranění
6		Majetková škoda do 15 000 000 Kč / středně těžké zranění
7	Vysoký	Majetková škoda do 50 000 000 Kč / těžké zranění
8		Majetková škoda do 100 000 000 Kč / ohrožení života jednotlivce
9	Velmi vysoký	Majetková škoda do 500 000 000 Kč / ohrožení života více osob
10	Kritický	Likvidace objektu nebo ztráta života

(zdroj: vlastní)

Dalším z kritérií při hodnocení rizika je výskyt hrozby, který určuje pravděpodobnost, s jakou může dané selhání nastat. Čím častěji se hrozba vyskytuje, tím vyšší je jeho celková závažnost. Tato hodnota je důležitá pro stanovení celkové úrovně ohrožení a pomáhá určit, která rizika vyžadují nejvyšší prioritu při prevenci a zmírňování dopadů.

Tabulka 8 Výskyt

Hodnota O	Třída	Pravděpodobnost výskytu [%]
1	Velmi nízký	0 až 5
2	Nízký	6 až 15
3		16 až 25
4	Střední	26 až 35
5		36 až 45
6		46 až 55
7	Vysoký	56 až 65
8		66 až 75
9	Velmi vysoký	76 až 85
10	Kritický	86 až 100

(zdroj: vlastní)

Poslední tabulka se zaměřuje na odladitelnost rizika, tedy na pravděpodobnost, že bude včas rozpoznáno a lze mu zabránit dříve, než způsobí škody. Zatímco předchozí dvě tabulky hodnotily význam hrozeb a výskyt, tedy pravděpodobnost jeho naplnění. Tato část analýzy se soustředí na to, jak snadno lze hrozbu identifikovat. Hodnoty uvedené v tabulce tak vyjadřují pravděpodobnost její detekce a slouží jako důležitý faktor pro stanovení celkové míry ohrožení.

Tabulka 9 Odhalitelnost

Odhalitelnost			
Hodnota D	Třída	Popis	pravděpodobnost [%]
1	Velmi nízká	Porucha bude téměř vždy detekována kontrolou nebo při montáži	86 až 100
2	Nízká	Porucha má nízkou pravděpodobnost uniknout detekci	76 až 85
3		Porucha má nižší pravděpodobnost uniknout detekci	66 až 75

Hodnota D	Třída	Popis	pravděpodobnost [%]
4	Střední	Porucha má střední pravděpodobnost, že nebude detekována	56 až 65
5		Porucha je často přehlédnuta během kontroly	46 až 55
6		Porucha je obtížně detekovatelná běžnými kontrolními mechanismy	36 až 45
7	Vysoká	Porucha má zvýšenou pravděpodobnost uniknout detekci	26 až 35
8		Porucha je velmi obtížně detekovatelná	16 až 25
9	Velmi vysoká	Porucha je téměř jistě neodhalitelná běžnými kontrolními mechanismy	6 až 15
10		Porucha je prakticky neodhalitelná	0 až 5

(zdroj: vlastní)

Na základě výsledků analýzy jsou rizika rozdělena do kategorií podle jejich přijatelnosti. Tato kategorizace pomáhá určit, zda je riziko přijatelné, vyžaduje preventivní opatření, nebo je natolik kritické, že je nutné jej okamžitě řešit.

Tabulka 10 Přijatelnost RPN

Úroveň rizika	Rozsah RPN	Popis
Minimální riziko	1 až 200	Riziko je téměř zanedbatelné, nevyžaduje zásah.
Nízké riziko	201 až 400	Riziko je nízké, doporučuje se sledování a drobné úpravy.
Střední riziko	401 až 700	Střední riziko vyžaduje preventivní opatření ke snížení dopadu.
Vysoké riziko	701 až 900	Vysoké riziko vyžaduje okamžitá nápravná opatření.
Kritické riziko	901 až 1000	Kritické riziko musí být neprodleně eliminováno nebo výrazně omezeno.

(zdroj: vlastní)

6.4.3 Provedení metody FMEA

Tabulka 11 Provedení FMEA

Aktivum	Možná Hrozba	Možné následky hrozby	Možné příčiny	Význam (S)	Výskyt (O)	Odhaditelnost (D)	RPN	Stávající opatření pro prevenci	Doporučená opatření	Termín nápravy + kdo opravu provede
	Perimetrická ochrana									
Majetek	Krádež	Ztráta majetku	Přelézání plotu, chybí ostnatý drát, hroty proti přelézání	8	5	6	240	Fyzické kontroly	Instalace doplňkových zábran	01.07.2025 Údržba
Brána	Poškození brány	Poškození infrastruktury, ohrožení osob v blízkosti.	Absence zátarasů	5	2	2	20	Kamery na vstupech	Betonové bloky + hydraulické závory	01.09.2025 Bezpečnostní firma
Oplocení	Vandalismus oplocení	Možné zvýšení krádeží nebo vandalismu	Nedostatečná doplňková ochrana	7	4	5	140	Noční hlídky	Svatované pletivo + senzorické kabely	01.09.2025 Bezpečnostní firma
Vstupní dveře	Vandalismus	Narušení bezpečnosti nebo majetku.	Chybí ESKV	7	5	6	210	Fyzická kontrola	Implementace RFID systému	01.09.2025 Bezpečnostní firma
Vozidla	Krádež vozidel	Poškození majetku	Chybí dodatečné osvětlení, Žádná kontrola vjezdu/výjezdu	6	4	6	144	Základní osvětlení	Instalace perimetrické ochrany (ploty brány) na přední parkoviště	01.09.2025 Bezpečnostní firma
Vozidla	Vandalismus vozidel	Poškození majetku	Chybí dodatečné osvětlení, Žádná kontrola vjezdu	4	3	5	60	Základní osvětlení	Instalace pohybových senzorů	01.09.2025 – Údržba
Vozidla	Neúmyslné poškození vozidel	Poškození majetku	Nepozornost	2	3	3	18	Základní osvětlení	Instalace pohybových senzorů	01.09.2025 – Údržba
	Plášťová ochrana									
Okna	Vandalismus	Možný přístup nepovolených osob do objektu. Poškození majetku	Rozbití oken - Chybí bezpečnostní fólie	7	5	6	210	Ruční kontrola	Instalace laminovaných skel	01.08.2025 Bezpečnostní firma
Okna	Neúmyslné poškození	Poškození majetku	Rozbití oken - Chybí bezpečnostní fólie	3	4	2	24	Ruční kontrola	Instalace laminovaných skel	01.08.2025 Bezpečnostní firma
Dveřní zámky	Vandalismus	Možný přístup nepovolených osob do objektu. Poškození majetku	Standardní zámky	7	5	4	140	Denní kontroly	Bezpečnostní zámky	01.08.2025 Bezpečnostní firma
Osvětlení areálu umístěné na fasádě	Vandalismus	Zvýšení vandalismu nebo krádeží během nočních hodin.	Chybí dodatečné osvětlení	5	5	4	100	Základní osvětlení	Instalace záložního napájení a pohybových senzorů	01.08.2025 Bezpečnostní firma

Aktivum	Možná Hrozba	Možné následky vady	Možné příčiny	Význam (S)	Výskyt (O)	Odhalitelnost (D)	RPN	Stávající opatření pro prevenci	Doporučená opatření	Termín nápravy + kdo opravu provede
	Plášťová ochrana									
Budova	Vandalismus	Poškození fasád budov nebo infrastruktury, snížení estetické hodnoty	Absence antigrafitů nátěrů	6	4	5	120	Pravidelné čištění	Nanášení speciálních povrchů	01.07.2025 Údržba
Vstupní dveře	Vandalismus	Neoprávněný vstup do budovy, riziko krádeže nebo ohrožení	Skleněné dveře bez ochranné folie	8	4	5	160	Základní dveře	Instalace bezpečnostních dveří	01.07.2025 Bezpečnostní firma
Vstupní dveře	Neúmyslné poškození	Neoprávněný vstup do budovy, riziko krádeže nebo ohrožení	Skleněné dveře bez ochranné folie	4	3	3	36	Základní dveře	Instalace bezpečnostních dveří	01.07.2025 Bezpečnostní firma
	Prostorová ochrana									
<i>Tato opatření se týká i jednotlivých budov a porostoru areálu</i>										
Kancelářské vybavení	krádež	chybějící vybavení , poškození majetku	Chybějící zámky nebo kryty na žebříčích	6	4	5	120	Občasná vizuální kontrola	Instalace zamykacích krytů	01.08.2025 Bezpečnostní firma
Vybavení	Požár	Ztráta a poškození majetku.	Chybějící kouřové hlásiče	9	4	8	288	Hasicí přístroje	Instalace multisenzorových detektorů	01.08.2025 Požární technik
IT Infrastruktura	Požár v technických místnostech	Ztráta technologií a dat při požáru.	Chybí požární hlásiče	7	3	7	147	Ruční hlásiče	Instalace automatických hlásičů	01.08.2025 Požární technik
IT Infrastruktura	Požár v serverovně	Poškození majetku, narušení provozu	Chybí hasicí systém	7	3	7	147	Ruční hasicí zařízení	Instalace hasicího systému	01.08.2025 Požární technik
Serverovna	Přehřátí nebo porucha serverů	Ztráta dat, přerušení provozu	Selhání klimatizace nebo UPS	7	3	5	105	Zálohované napájení a chlazení	Monitoring teploty, automatická notifikace poruch	01.07.2025 IT oddělení
Servery / počítače	Vloupání se do serveroven	Neoprávněný přístup k datům, poškození majetku	Chybí bezpečnostní dveře, chybějící dvoufaktorové ověřování	6	4	6	144	Základní uzamykání	Implementace RFID čteček	01.09.2025 Bezpečnostní firma
Elektronická zařízení	Krádež	Ztráta a poškození majetku.	Slepa místa v monitorování uvnitř budov, nedostatečná kontrola osob	7	5	6	210	Externí kamery	Instalace kamer unitř objektů, Instalace ESKV	01.09.2025 Bezpečnostní firma

Aktivum	Možná Hrozba	Možné následky vady	Možné příčiny	Význam (S)	Výskyt (O)	Odhaltelnost (D)	RPN	Stávající opatření pro prevenci	Doporučená opatření	Termín nápravy + kdo opravu provede
	Prostorová ochrana	<i>Tato opatření se týká i jednotlivých budov a porostoru areálu</i>								
Elektronická zařízení	Neúmyslné poškození majetku	Ztráta a poškození majetku.	Slepá místa v monitorování uvnitř budov, nedostatečná kontrola osob	3	1	6	18	Externí kamery	Instalace kamer unitř objektů, Instalace ESKV	01.09.2025 Bezpečnostní firma
Kanceláře	Neúmyslné Poškození majetku	Finanční ztráta	Nedostatek dohledu	5	3	5	75	Uzamykání kanceláří	Instalace kamer na chodbách	01.09.2025 Bezpečnostní firma
Sociální zázemí (WC)	Vandalismus na toaletách	Poškození zařízení	Nedostatečné zabezpečení vstupu do budovy	6	4	6	144	SBS na vřátnici	Instalace turniketu s přístupem na čip/kartu	01.09.2025 Bezpečnostní firma
Vozidla	Krádež vozidel	poškození majetku	Nedostatečná perimetrická ochrana	5	2	5	50	Oplocení	Instalace bezpečnostních kamer	01.09.2025 Bezpečnostní firma
Vozidla	vandalismus vozidel	poškození majetku	Nedostatečná perimetrická ochrana	5	3	5	60	Oplocení	Instalace bezpečnostních kamer	01.09.2025 Bezpečnostní firma
Vozidla	Neúmyslné poškození vozidel	poškození majetku	Nepozornost	5	2	2	20	Parkovací karty	Instalace bezpečnostních kamer	01.09.2025 Bezpečnostní firma
Protipožární nádrží	Znečištění vody (chemické, biologické, mechanické)	Neúčinnost při hašení požáru, možné zdravotní následky	Otevřený přístup, nedostatečná filtrace	6	3	6	108	Pravidelné testování	Instalace ochranné sítě a filtračního systému	01.06.2025 Údržba
Rozvodna elektrické energie	Porucha nebo zkrat	Přerušení provozu, riziko požáru	Nedostatečná údržba, přetížení	8	4	4	128	Pravidelné kontroly	Záložní napájení	01.10.2025 Energetika
Dokumentace	Ztráta	Únik citlivých informací, ztráta důvěry	Nepozornost, Špatné zabezpečení skříní	3	3	4	36	Uzamykatelné kartotéky	Zavedení digitalizace	01.07.2026 IT oddělení
Dokumentace	Krádež	Únik citlivých informací, ztráta důvěry	Špatné zabezpečení skříní	6	3	4	72	Uzamykatelné kartotéky	Zavedení digitalizace	01.07.2026 IT oddělení

Aktivum	Možná Hrozba	Možné následky vady	Možné příčiny	Význam (S)	Výskyt (O)	Odhalitelnost (D)	RPN	Stávající opatření pro prevenci	Doporučená opatření	Termín nápravy + kdo opravu provede
	Prostorová ochrana									
<i>Tato opatření se týkají jednotlivých budov a porostoru areálu</i>										
Zaměstnanci	Fyzické napadení	Dopad na život a zdraví, absence zaměstnance, psychická újma	Narušitel v areálu, konflikt mezi osobami	9	2	5	90	SBS na vřátnici	Instalace dodatečných kamer v rizikových zónách, zavedení ESKV pro kontrolu vstupů	01.08.2025 Bezpečnostní firma
Zaměstnanci / návštěvy	Úraz	Dopad na život a zdraví, absence zaměstnance, právní odpovědnost	Kluký povrch, chybějící protiskluzová úprava na vřátních schodech, uklouznutím na namrzlém/mokrém povrchu z důvodu chybějící protiskluzové úpravy	8	3	2	48	žádné	Instalace protiskluzové dlažby / pásků	01.06.2025 Údržba
Zaměstnanci / návštěvy	Úraz	Dopad na život a zdraví, absence zaměstnance, právní odpovědnost	Namrzlém/mokrém povrchu z důvodu chybějící protiskluzové úpravy	8	5	3	120	Posypový materiál	Instalace protiskluzové dlažby / pásků	01.06.2025 Údržba
Zaměstnanci / návštěvy	Úraz	Dopad na život a zdraví, absence zaměstnance	Nevyznačené komunikace, nepozornost řidiče v pohybujícím se vozidle	9	5	5	225	Rychlostní omezení	Vyznačení zón, reflexní prvky pro pohyb v areálu	01.07.2025 Bezpečnostní firma
Zaměstnanci / návštěvy	Úraz	Dopad na život a zdraví, absence zaměstnance	Neodborná manipulace - zavalení osob materiálem při manipulaci, špatná stabilita nákladu,	9	3	5	135	Vysokozdvížené vozíky pouze pro školené osoby	Vyznačení zón, reflexní prvky pro pohyb v areálu	01.07.2025 Bezpečnostní firma
Zaměstnanci	Úraz	Dopad na život a zdraví, absence zaměstnance, právní odpovědnost	Chybějící zámky nebo kryty na požárních žebřících	9	2	3	54	Občasná vizuální kontrola	Instalace zamykacích krytů	01.08.2025 Bezpečnostní firma
Finanční hotovost	Krádež	Přímá finanční škoda,	Nedostatečné zabezpečení pokladny	7	3	4	84	Uzamykatelný trezor	Kamerový dohled v místnosti s trezorem	01.07.2025 Bezpečnostní firma
Finanční hotovost	Ztráta	Přímá finanční škoda	Nepozornost	3	3	3	27	Uzamykatelný trezor	Kamerový dohled v místnosti s trezorem	01.07.2025 Bezpečnostní firma
Klimatizace	Selhání systému	Zhoršené pracovní podmínky, přehřátí techniky	Porucha zařízení, zanedbaná údržba	4	4	4	64	Servisní smlouvy	Monitoring teplot	01.07.2026 IT oddělení

Aktivum	Možná Hrozba	Možné následky vady	Možné příčiny	Význam (S)	Výskyt (O)	Odhaltitelnost (D)	RPN	Stávající opatření pro prevenci	Doporučená opatření	Termín nápravy + kdo opravu provede
	Kybernetická ochrana									
IT Infrastruktura	Únik dat	Ztráta důvěry, právní důsledky, narušení provozu	Slabá hesla, absence aktualizací	7	3	6	126	Antiviry, přístupová práva	Dvoufaktorová autentizace, pravidelné audity	01.07.2025 IT oddělení
IT Infrastruktura	Kybernetický útok	Ztráta citlivých dat, narušení provozu organizace, finanční ztráty	Zastaralý firewall	9	3	6	162	Základní antivirový software	Modernizace firewallu, Pravidelné aktualizace + školení personálu	01.07.2025 IT oddělení
Bankovní účty	Neoprávněný přístup	Finanční ztráty	phishing	9	3	5	135	Dvoufaktorová autentizace	Pravidelné školení, kontrola transakcí	01.07.2025 IT oddělení
Data	Poškození integrity dat	Trvalá ztráta důležitých informací	Chybné zálohování	6	3	4	72	Automatizované zálohování	Pravidlo 3-2-1, šifrování záloh	01.07.2025 IT oddělení
Data	Krádež dat	Trvalá ztráta důležitých informací	Chybné zálohování	8	2	3	48	Automatizované zálohování	Pravidlo 3-2-1, šifrování záloh	01.07.2025 IT oddělení
Data	Znepřístupnění dat	Trvalá ztráta důležitých informací	Ransomware	7	5	5	175	Automatizované zálohování	šifrování záloh, Pravidelné testy obnovy dat	01.07.2025 IT oddělení
Zálohy dat	kompromitace záloh	Trvalá ztráta důležitých informací	Chybné zálohování	8	2	4	48	Automatizované zálohování	Šifrování záloh, přístupová práva, logování, oddělení záloh od produkční sítě	01.07.2025 IT oddělení
Zálohy dat	krádež záloh	Trvalá ztráta důležitých informací	Chybné zálohování	8	3	3	72	Automatizované zálohování	Fyzické zabezpečení médií,	01.07.2025 IT oddělení
Zálohy dat	Znepřístupnění záloh	Trvalá ztráta důležitých informací	Chybné zálohování	8	2	2	32	Automatizované zálohování	Šifrování záloh, Pravidelné testy obnovy dat	01.07.2025 IT oddělení
Emaily zaměstnanců	Neoprávněný přístup	Únik informací, phishing útoky	Neopatrnost uživatelů, slabá hesla, phishing	9	3	4	108	Antispam a antivirové filtry	Školení uživatelů, pravidelná výměna hesel	01.07.2025 IT oddělení

Aktivum	Možná Hrozba	Možné následky vady	Možné příčiny	Význam (S)	Výskyt (O)	Odhaltitelnost (D)	RPN	Stávající opatření pro prevenci	Doporučená opatření	Termín nápravy + kdo opravu provede
	Environmentální ochrana									
Budovy / areál	Silný vítr / tornádo	Likvidace budov nebo infrastruktury	Nedostatečná odolnost konstrukce	10	1	7	70	pojištění		
Budovy /areál	Kroupy	Poškození sítěch a venkovních zařízení (např. kamerový systém).	Standardní krytina	8	4	5	160	pojištění		
Zeleň v areálu (stromy)	Vandalismus zaměřený na zeleň	Finanční ztráta, estetická újma	Nedostatečný dohled, volný přístup k zeleni	5	3	6	90	žádné	Rozšíření kamerového systému,	01.09.2025 Bezpečnostní firma
Energetická infrastruktura	Výpadek	Narušení provozu organizace, ztráta dat kvůli výpadkům systémů.	Přetížení sítě	6	4	6	144	Záložní UPS	Diesलगenerator	01.10.2025 Energetika + IT oddělení
Budovy /areál	Požár	Likvidace budov nebo infrastruktury	Blesk	8	4	4	128	pojištění	Revize hromosvodu	01.09.2025 Revizní technik
Budovy /areál	Záplavy	Poškození infrastruktury, ztráta provozuschopnosti.	Blízkost vodních toků	6	1	3	18	Areál nad záplavovou zónou		
	Doplňková ochrana									
Elektrické pojistkové skříně	Neúmyslné poškození, úmyslné	Poškození majetku, výpadek systému	Zapomenutý otevřený zámek nebo neuzamčení	7	3	5	105	Vizuální kontrola	Instalace zámků s klíčem + kontrolní štitky	01.09.2025 – Údržba
Elektrické rozvodné skříně	přetížení	Výpadek systému, poškození technologií, riziko požáru	Nezajištěné plechové skříně	6	4	6	144	Vizuální kontrola	Instalace zámků s klíčem	01.09.2025 – Údržba
Plynové rozvody v areálu	Neúmyslné poškození, úmyslné	Poškození majetku omezení provozu	Chybějící detekce úniku plynu	8	3	6	144	Ruční kontroly	Instalace automatických senzorů	01.07.2025 + Požární technik

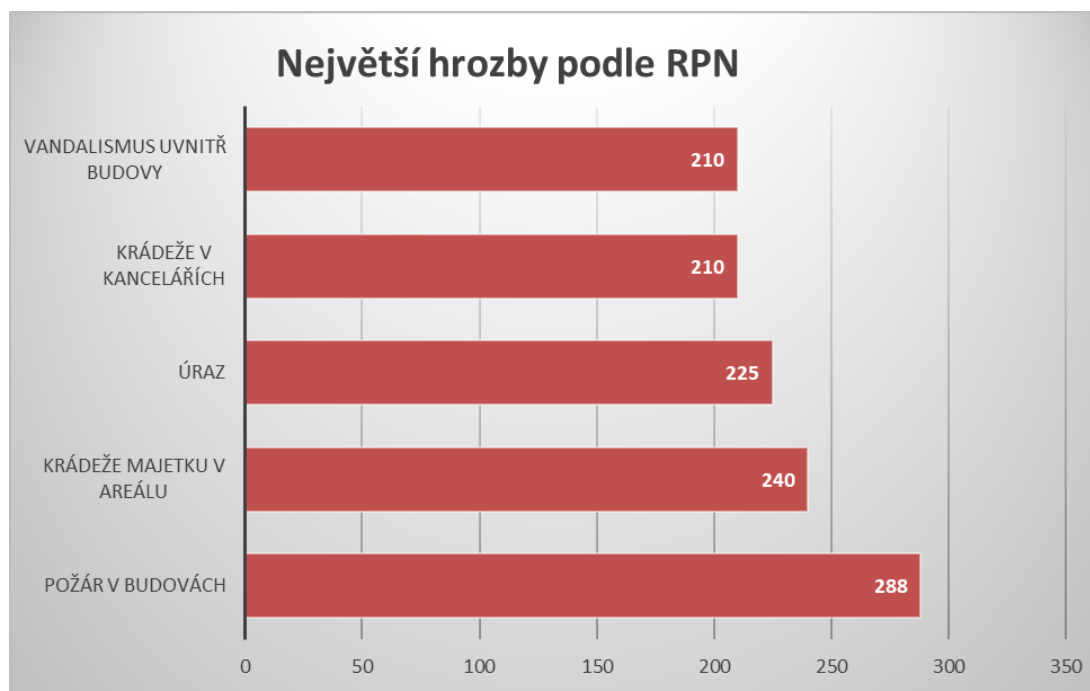
(zdroj: vlastní)

6.5 Vyhodnocení analýzy FMEA

Z výsledků provedené analýzy FMEA vyplynulo, že v rámci hodnocených hrozeb nebylo identifikováno žádné riziko, které by dle klasifikace RPN spadalo do kategorie vysoké riziko (RPN 651–850) nebo kritické riziko (RPN 851–1000). To znamená, že žádné z analyzovaných selhání v současném nastavení a při stávajících opatřeních nepředstavuje bezprostřední hrozbu, která by vyžadovala okamžitý zásah nebo neodkladná nápravná opatření.

Celkem bylo identifikováno 59 rizik, přičemž všechna spadají do kategorií minimálního (RPN v rozmezí 1–200) nebo nízkého rizika (RPN v rozmezí 201–400). Tato rizika, i když nejsou bezprostředně vysoká, mohou při kombinaci nepříznivých faktorů (např. výpadek kontroly, selhání lidského faktoru nebo technické poruchy) vést k dopadům na bezpečnost, provozní kontinuitu nebo majetkové ztráty.

Pro další návrh opatření jsou proto zpracována pouze ta rizika, jejichž hodnota RPN přesahuje hranici 200, a tedy spadají do kategorie nízkého rizika.



Obrázek 17 Největší hrozby

(zdroj: vlastní)

Z tohoto důvodu bude další část hodnocení a návrhů opatření zaměřena právě na tyto hrozby. Cílem bude jejich rozbor, přehodnocení účinnosti současných preventivních opatření a případné navržení konkrétních kroků ke snížení jejich RPN do bezpečnějších hodnot, ideálně pod hranici 100, která by byla považována za přijatelnou.

6.6 Závěr kapitoly

V rámci analýzy FMEA byla identifikována skupina rizik, jejichž hodnota RPN přesahuje hranici 200. Tato rizika sice nespádají do kritické zóny, ale vzhledem ke kombinaci závažnosti, pravděpodobnosti výskytu a nízké odhalitelnosti představují možné ohrožení provozu areálu. Rizika spojená například s nedostatečnou kontrolou vstupů, požární bezpečností, neodhaleným narušením perimetru nebo vandalismem ukazují na oblasti, které by mohly být při zhoršení podmínek nebo selhání stávajících opatření problematické. Z tohoto důvodu byla stanovena hranice $RPN > 100$ jako mez, nad kterou budou rizika dále podrobněji rozebrána. Pro každé z těchto rizik bude navržena konkrétní nápravná opatření, jejichž cílem je snížit hodnotu RPN pod doporučenou mez.

Následující část práce se zaměří na analýzu těchto vybraných hrozeb a zhodnocení účinnosti navrhovaných opatření z pohledu technického provedení, organizačních zásahů a ekonomické efektivity.

7 NÁVRH BEZPEČNOSTNÍCH OPATŘENÍ

V této kapitole se práce bude zabývat návrhem konkrétních bezpečnostních opatření, která reagují na zjištěná rizika vyplývající z předchozí analýzy FMEA. Cílem je navrhnout taková technická a režimová opatření, která povedou ke snížení hodnoty RPN (Risk Priority Number), a tím i celkové míry ohrožení osob, majetku a provozní spolehlivosti areálu.

Opatření jsou zaměřena na rizika, jejichž RPN překročila stanovenou mez (v tomto případě hodnotu 200), a tedy jsou považována za prioritní. Přestože se v rámci analýzy neobjevila rizika s hodnotou RPN natolik vysokou, aby byla zařazena do kritické nebo vysoké kategorie, identifikované hrozby ve střední zóně rizikovosti stále představují potenciálně závažné scénáře, které je vhodné řešit s předstihem. Navrhovaná opatření nejsou řešena izolovaně, ale s ohledem na celkový kontext zabezpečení objektu. Jsou navržena tak, aby vzájemně doplňovala stávající systémy, zohledňovala dané prostředí a zároveň byla reálně proveditelná z hlediska technického i ekonomického.

V následujících podkapitolách budou tato opatření zpracována s důrazem na jejich přímou návaznost na konkrétní rizika identifikovaná v rámci analýzy.

7.1 Technická opatření

V rámci analýzy byla na základě výsledků FMEA identifikována celá řada situací, které je možné efektivně řešit právě pomocí technických prostředků. Jedná se především o oblasti, kde selhání nebo absence technického vybavení může vést k nežádoucím událostem, jako je neoprávněný vstup, zpožděná detekce požáru, nebo fyzické poškození majetku.

Mezi navržená technická opatření patří zejména: turnikety, ostnaté dráty a ocelové hroty proti přelezu, bezpečnostních dveře a zámky, bezpečnostní folie na okna a kouřové hlásiče.

7.1.1 Instalace turniketu s čipovým přístupem

Toto opatření reaguje na hrozbu vandalizmu a krádeží způsobených nekontrolovaným pohybem osob v objektu. Turniket je navržen pro vstup do administrativní části areálu, jako kontrola vstupu do budovy. Zařízení s individuálním přístupem na čip nebo kartu zajišťuje kontrolu pohybu osob a zabrání vstupu nepovolaným. Nejčastějšími negativními jevy by mohli být poškození sociálního zázemí (rozbité sanitární zařízení, ucpané odpady, poničené

dveře¹⁾ případně krádeže v neuzamčených kancelářích, kde hrozí ztráta osobních věcí zaměstnanců či kancelárního vybavení. Celkové škody mohou v některých případech dosáhnout řádu tisíců až desítek tisíc korun ročně.

Zavedení turniketového systému navíc snižuje závislost na fyzické přítomnosti pracovníků bezpečnostní služby (SBS) na vrátnici v administrativní budově. V případě dlouhodobého provozu lze uvažovat o částečné náhradě jednoho pracovníka, což může znamenat roční úsporu přes 240 000 Kč. Dalším přínosem je odstranění potřeby dotazování se návštěvníků, které bylo podle zpětné vazby opakovaně vnímáno návštěvníky jako nepříjemné²⁾.

V souvislosti s instalací turniketů je však nutné zároveň upravit režim návštěv – např. jejich vyzvedávání oprávněnou osobou u turniketu nebo využití recepčního panelu s přivoláním odpovědného zaměstnance.

Orientační investice na instalaci 2–4 turniketů včetně čteček, kabeláže a softwaru pro správu přístupů se pohybuje v rozmezí 120 000 až 180 000 Kč bez DPH. Díky snížení nákladů na ostrahu lze očekávat návratnost investice v horizontu 1,5 až 2 let.

Turnikety tripod Tristar

- Řízený průchod po autorizaci (např. pomocí čtečky RFI)
- Automatické otáčení ramen, mechanické nebo elektromechanické provedení



Obrázek 18 Turniket

(zdroj: [14])

¹⁾ V minulosti došlo k případům, kdy sociální zařízení poškodily nepovolané osoby z okolí areálu.

²⁾ Od vedení jsou zprávy o stížnostech z minulosti

- Možnost nastavení jednosměrného nebo obousměrného provozu
- **Orientační cena:** 24 000 až 38 000 Kč bez DPH (v závislosti na typu ovládání a příslušenství) [14]

7.1.2 Doplnkové zábrany na perimetr (ostnatý drát, žiletková spirála)

Přestože je oplocení základním bezpečnostním prvkem, jeho samotná přítomnost často nestačí k odrazení pachatele, zejména v méně frekventovaných a hůře osvětlených částech. Pachatelé často využívají snadno překonatelné úseky oplocení, čímž zvyšují riziko krádeže nebo vandalismu. Z tohoto důvodu je doporučeno doplnit oplocení o ostnatý drát nebo žiletkové spirály typu Concertina, které ztíží přelezení plotu nebo jej znemožňují úplně. Navíc tyto zábrany působí preventivně i psychologicky – odradí neoprávněné osoby již při prvním pohledu na perimetr.

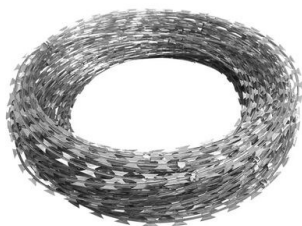
Ostnatý drát / žiletková spirála Concertina

- **Popis:** Kovová spirála osazená ostrými body sloužící k ochraně vrchní hrany plotu. Umožňuje natažení v délce až 10–15 m, výška cca 45–90 cm. Dostupná i v nerezovém provedení.
- **Orientační cena:** Ostnatý drát: 50 až 80 Kč/m, Žiletková spirála: 90 až 120 Kč/m
- **Dostupnost:** Běžně dostupné u specializovaných dodavatelů oplocení

Varianta A – Ostnatý drát: $1\,200\text{ m} \times 60\text{ Kč} = 72\,000\text{ Kč}$ bez DPH

Varianta B – Žiletková spirála: $1\,200\text{ m} \times 110\text{ Kč} = 132\,000\text{ Kč}$ bez DPH

Doplnkové zábrany tohoto typu jsou finančně dostupné, jednoduché na instalaci i údržbu. Celkové náklady se pohybují mezi 70 000 až 140 000 Kč bez DPH, přičemž návratnost investice může být dosažena již při jediném zmařeném pokusu o vniknutí.



Obrázek 19 Žiletkový drát

(zdroj:[15])

Hroty proti přelezu

Představují ochranný prvek, který se instaluje na horní hranu stávajícího oplocení, zdi nebo vrat. Jde o nenápadné, ale velmi účinné opatření, které ztěžuje nebo znemožňuje neoprávněné přelezení. Oproti žiletkové spirále nebo ostnatému drátu působí i vizuálně méně agresivně a mohly by být výhodné zejména v reprezentativnějších nebo veřejnosti viditelných částech perimetru.

- **Orientační cena:** cca 90–200 Kč za 50cm díl, tedy přibližně 180–400 Kč/m
- **Dostupnost:** běžně dostupné např. Alza, Hornbach apod.
- **Výhody:** nenápadný vzhled, účinnost, jednoduchá instalace na různé typy oplocení
- **Celkové náklady při pokrytí celého perimetru (1 200 m):**
- Při průměrné ceně 250 Kč/m: $1\,200\text{ m} \times 250\text{ Kč} = \text{cca } 300\,000\text{ Kč bez DPH}$

Z ekonomického hlediska jde o nejnákladnější variantu perimetrického opatření. Oproti tomu ostnatý drát by stál přibližně 72 000 Kč a žiletková spirála kolem 132 000 Kč. Obě tyto varianty sice působí agresivněji, ale poskytují vysokou účinnost za podstatně nižší pořizovací náklady.

Vzhledem k výrazně vyšší ceně hrotů proti přelezu a jejich zaměření na estetiku se jeví jako vhodné instalovat je pouze ve vybraných částech areálu, kde je kladen důraz na vzhled – například u vrátnice a administrativní budovy.



Obrázek 20 Hroty proti přelezu

(zdroj:[16])

7.1.3 Bezpečnostních dveře a zámky na rizikových vstupech

V několika částech areálu byly identifikovány vstupy, které nejsou dostatečně chráněny proti neoprávněnému vstupu, a to jak z pohledu mechanické odolnosti samotných dveří, tak i z hlediska jejich uzamykacích mechanismů. Proto se navrhuje výměna stávajících dveří za certifikované bezpečnostní dveře odpovídající minimálně třídě odolnosti RC3, které poskytují zvýšenou ochranu proti násilnému otevření, vypáčení nebo vyražení. Důležitou součástí těchto dveří je také bezpečnostní kování a vícebodový zámkový systém, který zajistí pevné uchycení dveří v rámu a znemožňuje jejich překonání běžnými nástroji.

V České republice je dostupná pestrá nabídka dodavatelů a technických řešení. Výběr by měl vycházet z konkrétních potřeb, vizuálních požadavků a finančního rámce.

7.1.4 Zabezpečení prosklených vstupů a oken

Skleněné části objektu, jako jsou vstupní dveře s prosklenou výplní nebo nízko položená okna, mohou být snadno zneužity k násilnému vstupu. Z tohoto důvodu je vhodným opatřením použití bezpečnostní fólie, která zvyšuje odolnost skla proti rozbití a průrazu. Alternativně lze použít vrstvená bezpečnostní skla s vyšší odolností. Tato řešení nemění vzhled ani propustnost světla, a přitom výrazně posilují ochranu exponovaných částí objektu.

Na českém trhu je k dispozici široký výběr vhodných výrobků i dodavatelů. Volba konkrétního řešení by měla odpovídat provozním podmínkám, požadované úrovni zabezpečení, vzhledu a finančním možnostem.

7.1.5 Požární hlásiče

V některých částech areálu byly prostory bez základního požárního zabezpečení. Pro zvýšení úrovně bezpečnosti a včasnou detekci požáru se doporučuje instalace požárních hlásičů – zejména optických a teplotních hlásičů. Na trhu je k dispozici široká nabídka těchto zařízení od běžných výrobců, jako jsou Jablotron, Paradox, Bosch, Siemens a další, které splňují

normy požární bezpečnosti a jsou vhodné pro instalaci v administrativních, provozních i technických prostorách.



Obrázek 21 Detektor kouře

(Zdroj: [17])

Cenové rozpětí základních detektorů se pohybuje od 700 – 1500kč. Při výběru vhodného typu je důležité zohlednit, zda má být detektor samostatný (s vestavěnou sirénou) nebo napojený na stávající EPS systém. [17]

7.1.6 Instalace PTZ kamer s 360° výhledem

Pro lepší dohled nad děním uvnitř areálu, budov a málo frekventovaných částech, se doporučuje instalace otočných PTZ kamer s funkcí 360° sledování. Cílem je reagovat na hrozbu krádeže uvnitř objektu, přičemž kamery zároveň umožňují i rychlé vizuální ověření případného požáru v budovách a tím přispívají k včasné reakci na tuto hrozbu.

Doporučený model: TP-Link Tapo C520WS s 360° pokrytím



Obrázek 22 kamera

(Zdroj: [18])

Rozlišení: 2K QHD (2560 × 1440 px) – ostrý a detailní obraz

Barevné noční vidění

Detekce pohybu s AI: rozpoznání osob, vozidel i domácích zvířat

Obousměrný zvuk: mikrofón a reproduktor pro přímou komunikaci

Orientační cena: cca 1899 Kč [18]

Přínos:

Tato kamera umožňuje sledovat velké plochy s minimálním počtem zařízení a zároveň díky pokročilé detekci snižuje počet planých poplachů. Vhodná pro sledování vstupních prostor, parkovišť i odlehlých částí areálu. Možné připojení k mobilní aplikaci pro vzdálený přístup. Kromě preventivní funkce proti krádežím přispívá také k rychlému vyhodnocení požárních událostí, což napomáhá včasné reakci a zajištění adekvátního zásahu.

7.2 Režimová opatření

Tato opatření představují součást bezpečnostního rámce areálu. Na rozdíl od technických prostředků se tato opatření zaměřují na vnitřní pravidla, řízení přístupu, pracovní návyky a celkový systém kontroly a dohled. Jejich účinnost je závislá nejen na správném nastavení, ale také na důsledném dodržování ze strany zaměstnanců a vedení.

Cílem této skupiny opatření je zlepšit kontrolu nad pohybem osob a materiálu, omezit možnost lidského selhání a nastavit pravidla, která minimalizují riziko vzniku bezpečnostních incidentů. Tato opatření často nevyžadují nákladné investice, ale jejich přínos spočívá v systematičnosti, důslednosti a prevenci.

Na základě zjištěných rizik jsou navržena následující režimová opatření:

- **Zavedení bezpečnostních zón při manipulaci s materiálem.**

Na základě identifikovaného rizika zavalení osob při manipulaci s materiálem budou v areálu vymezeny bezpečnostní zóny určené pro nakládku a vykládku materiálu, Budou sloužit k oddělení manipulační techniky (např. vysokozdvíhových vozíků) od běžného pohybu osob.

- **Stanovení pravidel pro pohyb návštěvníků**

Návštěvy budou umožněny pouze po předchozí registraci, v doprovodu odpovědného zaměstnance a s jednorázovým přístupovým oprávněním. Každému

návštěvníkovi bude při vstupu na vrátnici vydána návštěvnická karta. Pro zvýšení bezpečnosti budou v areálu vyznačeny pěší trasy, které omezí pohyb osob v rizikových zónách se zvýšeným provozem manipulační techniky (např. vysokozdvizných vozíků). Tím se sníží pravděpodobnost kolize a úrazu.

- **Povinnost nošení reflexních vest pro návštěvníky**

Z důvodu zvýšeného rizika střetu osob s provozní technikou bude zavedena povinnost nošení reflexních vest pro všechny pěší návštěvníky během jejich pohybu v areálu. Reflexní vesta bude vydávána na vrátnici současně s návštěvnickou kartou a vrácena při odchodu. Toto opatření významně zvyšuje viditelnost osob, zejména za zhoršených světelných podmínek, a snižuje riziko úrazu.



Obrázek 23 Vesta

(Zdroj:[19])

Orientační náklady na pořízení přibližně 50 kusů reflexních vest činí cca 5 000 Kč (počítáno s průměrnou cenou 100 Kč/ks). [19]

- **Doporučení na zefektivnění fyzické ostrahy**

Areál má podlouhlý půdorys o délce cca 400 metrů, což je vzdálenost, kterou průměrný člověk urazí za 5 až 7 minut běžnou chůzí. Při pravidelných obchůzkách nebo urgentních situacích může být tato vzdálenost časově neefektivní. Doporučuje se proto zvážit pořízení malého elektrického vozíku (např. typu golfového), který umožní ostraze rychlejší a efektivnější pohyb po celém perimetru, zejména ve večerních hodinách nebo při kontrole odlehlých částí. Investice do tohoto prostředku může navíc přispět ke snížení fyzické zátěže ostrahy a zvýšit schopnost rychlé reakce např. pokud pachatel překoná oplocení v odlehlé části areálu.

7.3 Preventivní opatření

Preventivní opatření a školení mají dlouhodobý dopad a jsou zvlášť důležitá tam, kde hrozby vyplývají z lidského faktoru – tedy z nepozornosti, neznalosti nebo nedbalosti. Na základě provedené analýzy FMEA a zjištěných slabin jsou navržena následující opatření:

- **Zavedení úvodního školení pro nové pracovníky a externí osoby**

Každý nový zaměstnanec nebo externí technik, který se bude v areálu pohybovat, projde základním instruktážním školením o pohybu v objektu a o odpovědnosti za škody způsobené nedodržením pravidel.

7.4 Zhodnocení a prioritizace navržených opatření

Navržená bezpečnostní opatření byla zformulována na základě výsledků analýzy FMEA, která identifikovala hrozby a rizika v zabezpečení areálu a přiřadila jim hodnotu rizikového prioritního čísla (RPN). Smyslem této části je zhodnotit přínos jednotlivých opatření, porovnat jejich náročnost a určit pořadí jejich zavádění s ohledem na efektivitu a dostupné zdroje.

Pro hodnocení byla použita tři kritéria:

- **Účinnost:** míra, do jaké opatření sníží identifikovanou hrozbu (tedy jak výrazně snižuje hodnotu RPN).
- **Náročnost:** finanční i provozní náklady, technická proveditelnost.
- **Časová realizovatelnost:** možnost implementace v krátkém časovém horizontu (během několika týdnů až měsíců).

Na základě těchto kritérií byla navržená opatření rozčleněna do prioritních úrovní:

- **Priorita 1 – Okamžitě realizovatelná a vysoce účinná opatření**

Ochrana prosklených částí vstupů (bezpečnostní fólie nebo vrstvené sklo)

Doplnění požárních hlásičů v kritických místech

- **Priorita 2 – Technická opatření s vyšší investiční náročností**

Instalace turniketu s čipovým přístupem na vstupu do administrativní budovy

Výměna vstupních dveří za bezpečnostní modely s vícebodovým zámekem

Posílení mechanické ochrany plotu (ostnatý drát, hroty proti přelezu)

Instalace vnitřních kamer s 360° záběrem

- **Priorita 3 – Doplňková a dlouhodobá opatření**

Vyznačení manipulačních zón pro nakládku a vykládku

Povinnost nošení reflexních vest v provozních zónách

Oddělení pohybu techniky a osob pomocí značení

Tohle pomůže při plánování investic a postupném zavádění změn bez nutnosti přerušení provozu areálu. Cílem je nejen zvýšit bezpečnost, ale zároveň optimalizovat náklady a minimalizovat negativní dopady na běžný provoz.

7.5 Plán implementace bezpečnostních opatření

Aby bylo dosaženo skutečného efektu navržených opatření, bude nezbytné připravit realistický plán jejich zavádění. Ten musí zohlednit naléhavost jednotlivých rizik, časové možnosti provozu a také ekonomickou náročnost implementace.

Plán implementace je rozdělen do tří etap podle časového horizontu:

1. Fáze – Okamžitě realizovatelná opatření (zahájení do 3 měsíců)

Opatření, která jsou technicky a organizačně méně náročná, lze realizovat rychle a s nižšími náklady. Jejich zavedení má okamžitý dopad na eliminaci některých provozních rizik.

- Vymezení manipulačních zón a pěších tras – Vizuální označení zón pro nakládku a vykládku materiálu a vyhrazené trasy pro bezpečný pohyb osob v areálu.
- Značení rizikových míst a vstupů – Např. označení technických místností, vstupních bran a slabě osvětlených částí pro zvýšení ostražitosti.
- Doplnění optických a teplotních požárních hlásičů – Instalace autonomních detektorů v místech, kde dosud chybí detekce požáru.

2. Fáze – Technicky středně náročná opatření (realizace do 6 měsíců)

Jedná se o opatření technického charakteru, která vyžadují schválení investic, dodávku a odbornou instalaci.

- Doplnění oplocení o mechanické zábrany (ostnatý drát, hroty)
- Instalace bezpečnostních folií na okna

3. Fáze – Investičně a časově náročnější opatření (realizace ve výhledu nad 6 měsíců)

Opatření vyžadující plánování, koordinaci více dodavatelů nebo zásahy do infrastruktury.

- Instalace turniketu s RFID přístupem do hlavního vstupu
- Instalace vnitřních kamer s 360° záběrem
- Instalace bezpečnostních dveří

Implementace by měla být řízena dle priority, přičemž prioritou bude vždy bezpečnost osob a ochrana majetku.

7.6 Kontrolní FMEA

Po návrhu bezpečnostních opatření byla provedena kontrolní analýza FMEA, jejímž cílem bylo ověřit, jakým způsobem navržená řešení přispívají ke snížení identifikovaných rizik. Analýza pracuje se stejnými hrozbami jako původní FMEA a hodnotí nově upravené hodnoty výskytu, významu a odhalitelnosti po zavedení konkrétních opatření. Výsledky této aktualizované analýzy jsou uvedeny v následující tabulce.

Tabulka 12 Kontrolní FMEA po provedení opatření

Aktivum	Možná Hrozba	RPN před zavedením opatření	zavedené opatření	Význam (S)	Výskyt (O)	Odhalitelnost (D)	RPN po zavedení opatření
Vstupní dveře	Vandalismus	200	Instalace bezpečnostních dveří	8	4	3	96
Elektronická zařízení	Krádeže	210	Instalace PTZ kamer s 360° výhledem	7	3	3	63
Okna	Vandalismus	210	Instalace laminovaných skel	7	3	4	84
Vstupní dveře	Vandalismus	210	Implementace RFID systému	7	5	2	70
Zaměstnanci / návštěvy	Úraz	225	Vyznačení zón, reflexní prvky pro pohyb v areálu	9	3	3	81
Majetek	Krádež	240	Instalace ostnatého drátu, hroty proti přelezení	8	4	3	96
Vybavení	Požár	288	Instalace multisenzorových detektorů	9	4	2	72

(zdroj: Vlastní)

Kontrolní analýza FMEA byla provedena s cílem ověřit účinnost navržených a plánovaných bezpečnostních opatření v rámci areálu. Z porovnání hodnot RPN před a po implementaci vyplývá:

- Ve všech případech došlo ke snížení hodnoty RPN, což znamená, že bezpečnostní opatření mají prokazatelný pozitivní dopad.
- Největší pokles byl zaznamenán u hrozby „Pozdní detekce požáru“, kde díky instalaci optických a teplotních požárních hlásičů došlo k výraznému zlepšení odhalitelnosti a tím i snížení RPN z 288 na 72. K tomuto zlepšení přispěla také instalace kamerového systému, který napomáhá k rychlému vizuálnímu ověření požárních poplachů.
- Významně klesly i hodnoty u hrozeb spojených s neoprávněným vstupem (např. přelezení plotu, vstup do budovy), kde byla zavedena technická řešení jako bezpečnostní dveře, Ochranné folie, RFID systém či doplňkové zábrany.

Tato kontrolní FMEA tak potvrzuje, že přijatá opatření vedou k efektivnímu snížení identifikovaných rizik, a napomáhá stanovit prioritu pro případná budoucí doplnění či úpravy systému zabezpečení.

7.7 Závěr kapitoly

Navržená bezpečnostní opatření přímo reagují na konkrétní rizika identifikovaná v rámci metody FMEA a představují praktické kroky ke snížení jejich dopadu i pravděpodobnosti výskytu. Cílem bylo vytvořit ucelený systém, který bude vyváženě kombinovat efektivitu, dostupnost a proveditelnost v reálném provozu analyzovaného areálu.

Opatření byla rozdělena do tří hlavních oblastí:

- **technická**, která posilují fyzické a elektronické zabezpečení objektu,
- **režimová**, která nastavují pravidla, dohled a odpovědnosti,
- **preventivní**, zaměřená na školení a budování bezpečnostního povědomí.

Tato struktura umožňuje systematické a prioritní zavádění opatření bez výrazných zásahů do chodu organizace. Kontrolní FMEA následně potvrdila, že při správné implementaci navržených kroků dojde k výraznému poklesu rizikových prioritních čísel (RPN) a tím i ke zlepšení celkové bezpečnostní úrovně objektu.

8 ZÁVĚR

Tato práce si kladla za cíl provést bezpečnostní analýzu vybraného areálu a na základě identifikovaných rizik navrhnout odpovídající opatření, která povedou ke snížení pravděpodobnosti výskytu hrozeb a ke zmírnění jejich dopadu. Obsah práce je členěn do dvou hlavních oblastí: teoretické a praktické části.

V teoretické části byla pozornost věnována základním principům řízení rizik, zejména pak procesu identifikace hrozeb, analýzy rizik a hodnocení. Popsány byly také metody Check List Analysis a FMEA, které sloužily jako hlavní nástroje pro praktickou část. Důraz byl kladen na praktické využití těchto metod při odhalování slabých míst v bezpečnostním systému.

Praktická část se zabývala podrobným rozбором vybraného areálu, včetně popisu jeho struktury a současného stavu zabezpečení. Byly identifikovány jednotlivé prvky, které vyžadují zvýšenou pozornost z hlediska bezpečnosti. Pomocí metody Check List byla zhodnocena úroveň mechanické, technické i organizační ochrany. Následně byla provedena rozsáhlá FMEA analýza, která přinesla celkem 59 posouzených hrozeb.

Po vyhodnocení hodnot RPN bylo zjištěno, že žádné z analyzovaných rizik nedosahuje kritických nebo vysokých hodnot, které by vyžadovaly okamžitá zásadní opatření. Bylo rozhodnuto zaměřit se na ta rizika, jejichž hodnota RPN spadá do rozmezí 200 až 300 tzn. nižšího rizika. Z tohoto důvodu bylo rozhodnuto zaměřit se právě na tuto skupinu a provést jejich detailnější analýzu. Vybráno bylo celkem 7 prioritních případů, pro které byla navržena konkrétní technická, organizační nebo režimová opatření vedoucí ke snížení jejich rizikového potenciálu.

Výstupem práce je návrh bezpečnostních opatření, která zahrnují instalaci turniketu s čipovým přístupem, doplnění perimetrických ochranných prvků, výměnu nevyhovujících dveří, modernizaci požární ochrany a také zlepšení režimových pravidel uvnitř areálu.

Závěrem lze konstatovat, že areál sice nevykazuje kritická selhání, ale i tak existují oblasti, jejichž zlepšení povede k výraznému posílení celkové bezpečnosti. Návrh opatření je koncipován jako realistický a postupně implementovatelný, a jeho realizace přispěje k vyšší odolnosti objektu vůči vnějším i vnitřním hrozbám.

SEZNAM POUŽITÉ LITERATURY

- [1] SMEJKAL, Vladimír a RAIS, Karel. *Řízení rizik ve firmách a jiných organizacích*. 4. vydání. Praha: Grada Publishing, 2013. ISBN 978-80-247-4644-9.
- [2] KORECKÝ, Michal a TRKOVSKÝ, Václav. *Management rizik projektů*. Praha: Grada Publishing a.s, 2011. ISBN 978-80-247-3221-3.
- [3] KYNCL, Jaromír. *Bezpečnost objektu ve světle moderních technologií*. Praha: Komora podniků komerční bezpečnosti ČR, 2014. ISBN 978-80-260-7115-0.
- [4] *Bezpečnostní třídy*. Online. Klicovecentrum.cz. 2012. Dostupné z: https://www.klicovecentrum.cz/bezpecnostni-tridy-vyznate-se-v-nich/?srsltid=AfmBOor5skEuwks0AJKVw9wrcTKEkTUzcv39mfx_lWsabPsZkA2r4eUn. [cit. 2025-01-12].
- [5] *Bezpečnostní třídy*. Online. Bezpecnostni-dvere-mrize-kavan.cz. 2012. Dostupné z: <https://www.bezpecnostni-dvere-mrize-kavan.cz/2023/08/19/co-je-to-bezpecnostni-trida/>. [cit. 2025-01-12].
- [6] UHLÁŘ, Jan. *Technická ochrana objektů*. 2. vydání. Praha: Policejní akademie České republiky, 2009. ISBN 978-80-7251-313-0.
- [7] LUDĚK, Lukáš. *Teorie bezpečnosti I*. Zlín: VeRBuM, 2017. ISBN 978-80-87500-89-7
- [8] TICHÝ, Milík. *Ovládání rizika : analýza a management*. Praha: C.H. Beck, 2006. ISBN 80-7179-415-5.
- [9] LUDĚK, Lukáš. *Bezpečnostní technologie, systémy a management II*. Zlín: VeRBuM, 2012. ISBN 978-80-87500-19-4.
- [10] ROUDNÝ, Radim a LINHART, Petr. *Krizový management III.: teorie a praxe rizika*. Pardubice: Univerzita Pardubice, 2006. ISBN 80-7194-924-8.
- [11] *Google maps*. Online. 2025. Dostupné z: <https://www.google.com/maps/>. [cit. 2025-02-12].
- [12] *Budova*. Online. 2023. Dostupné z: <https://mapy.cz/>. [cit. 2025-02-13].
- [13] *FMEA*. Online. Lean6sigma.cz. 2025. Dostupné z: <https://lean6sigma.cz/fmea/>. [cit. 2025-04-13].

- [14] Turniket. Online. Asparking.cz. 2025. Dostupné z: https://www.asparking.cz/cz/vyrobky/turnikety-a-speedgate/tripody#item_detail_7. [cit. 2025-03-22].
- [15] *Žiletkový drát*. Online. Wwww.levne-pletivo.cz. 2025. Dostupné z: https://www.levne-pletivo.cz/ziletkovy-ostnaty-drat-concertina-prumer-980-mm/?gad_source=1&gclid=Cj0KCQjwv_m-BhC4ARIsAIqNeBu2B5YWJaHMFZY7ItlbDI6byjMC3OYGvswzbiIwbaBltlAktl3m6lcaAn-FEALw_wcB. [cit. 2025-03-22].
- [16] *Hroty proti přelezu*. Online. Wwww.levne-pletivo.cz. 2025. Dostupné z: <https://www.levne-pletivo.cz/hroty-proti-prelezu/>. [cit. 2025-03-22].
- [17] *Detektor kouře*. Online. Wwww.jabloshop.cz/. 2025. Dostupné z: <https://www.jabloshop.cz/sd-503st-kombinovany-detektor-koure-a-teplot-autonomni>. [cit. 2025-05-27].
- [18] *Kamera*. Online. Alza.cz. 2025. Dostupné z: <https://www.alza.cz/tp-link-tapo-c520ws-d8009690.htm>. [cit. 2025-05-27].
- [19] *Výstražná vesta*. Online. Heureka.cz. 2025. Dostupné z: <https://www.heureka.cz/?h%5Bfraz%5D=vesta+v%C3%BDstra%C5%BEn%C3%A1+%C5%BElut%C3%A1>. [cit. 2025-05-27].

SEZNAM OBRÁZKŮ

Obrázek 1 Letecký snímek areálu.....	32
Obrázek 2 Administrativní budova s hl. vchodem	33
Obrázek 3 Suterén.....	34
Obrázek 4 Venkovní prostory a suterén	35
Obrázek 5 První patro	36
Obrázek 6 Druhé patro.....	36
Obrázek 7 Třetí a čtvrté patro	37
Obrázek 8 Vyznačené budovy	39
Obrázek 9 Východní část plotu.....	41
Obrázek 10 Severní část plotu	41
Obrázek 11 Plot na jižní straně	42
Obrázek 12 Požární hydrant a tlačítko.....	44
Obrázek 13 Archiv a sklady.....	44
Obrázek 14 Identifikační čip na budově	46
Obrázek 15 severní část plotu.....	56
Obrázek 16 hl. rozvodna	59
Obrázek 17 Největší hrozby	72
Obrázek 18 Turniket	75
Obrázek 19 Žiletkový drát	76
Obrázek 20 Hroty proti přeletu	77
Obrázek 21 Detektor kouře.....	79
Obrázek 22 kamera	79
Obrázek 23 Vesta.....	81

SEZNAM TABULEK

Tabulka 1 Bezpečnostní třídy dle ČSN EN 1627	19
Tabulka 2 Odhad hodnoty hmotných aktiv	50
Tabulka 3 Checklist perimetrické ochrany	54
Tabulka 4 Checklist prostorové ochrany areálu.....	57
Tabulka 5 Checklist plášťové ochrany.....	57
Tabulka 6 Checklist prostorové ochrany budov	59
Tabulka 7 Význam	63
Tabulka 8 Výskyt.....	64
Tabulka 9 Odhalitelnost	64
Tabulka 10 Přijatelnost RPN.....	65
Tabulka 11 Provedení FMEA	66
Tabulka 12 Kontrolní FMEA po provedení opatření.....	84

Seznam použitých symbolů a zkratek

CLA	Checklist Analysis
FMEA	Failure Mode and Effects Analysis
SBS	Soukromá bezpečnostní služba
RC	Resistivity class (Třída odolnosti)
MZS	Mechanické zábranné systémy
PZTS	Poplachové zabezpečovací a tísňové systémy
IZS	Integrovaný záchranný sbor
DV	dohledový videosystém
EPS	Elektrická požární signalizace
ESKV	Elektronický systém kontroly vstupu
DPPC	Dohledové a Poplachové Přijímací Centrum
ČR	Česká republika

