Bezpečnostní posouzení a návrh zabezpečení vybraného objektu

Bc. Tomáš Kallus

Diplomová práce
2022

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektroniky a měření

Akademický rok: 2021/2022

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Tomáš Kallus**
Osobní číslo:	**A20178**
Studijní program:	**N1032A020003 Bezpečnostní technologie, systémy a management**
Specializace:	**Bezpečnostní technologie**
Forma studia:	**Kombinovaná**
Téma práce:	**Bezpečnostní posouzení a návrh zabezpečení vybraného skladu**
Téma práce anglicky:	**Security Assessment and Security Proposal of a Selected Warehouse**

Zásady pro vypracování

1. Uveďte základní terminologii a základy řízení rizik.
2. Charakterizujte vybraný sklad.
3. Popište současný stav.
4. Proveďte bezpečnostní posouzení spolu s analýzou a vyhodnocením rizik.
5. Na základě výsledků bezpečnostního posouzení navrhněte konkrétní bezpečnostní opatření.

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

Seznam doporučené literatury:

1. KŘEČEK, Stanislav. *Příručka zabezpečovací techniky*. Vyd. 3. aktualiz. S.l.: Cricetus, 2006, 313 s. ISBN 8090293824(brož.).
2. LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management I.* Zlín: VeRBuM, 2011. ISBN 9788087500057.
3. KAFKA, Tomáš. *Průvodce pro interní audit a risk management*. Praha: C.H. Beck, 2009, xvii, 167 s. C.H. Beck pro praxi. ISBN 9788074001215.
4. NEUGEBAUER, Tomáš. *Vyhledání a vyhodnocení rizik v praxi. 2.*, aktualiz. a rozš. vyd. Praha: Wolters Kluwer, 2014, 111 s. ISBN 9788074784583.
5. LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management V.* Zlín: Radim Bačuvčík – VeRBuM, 2015. ISBN 978-80-87500-19-4.

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

Datum zadání diplomové práce: **3. prosince 2021**
Termín odevzdání diplomové práce: **23. května 2022**

doc. Mgr. Milan Adámek, Ph.D. v.r.
děkan

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

Ing. Milan Navrátil, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 7. února 2022

Prohlašuji, že

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

Prohlašuji,

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

Bc. Tomáš Kallus, v.r.

Ve Zlíně, dne 23.05.2022

…….

podpis studenta

ABSTRAKT

Hlavním cílem diplomové práce je bezpečnostní posouzení spedičního skladu a návrh jeho zabezpečení. V rámci teoretické části jsou popsány základní pojmy týkající se problematiky a popis bezpečnostních posouzení v oblasti bezpečnosti. Praktická část popisuje skutečný stav objektu skladu a kancelářské budovy, možné identifikace hrozeb, analýzu rizik a návrh bezpečnostních opatření.

Klíčová slova: analýza rizik, bezpečnost a ochrana zdravý při práci, požární ochrana, video surveillance system, kamerový system, poplachový a zabezpečovací tísňový systém, bezpečnostní opatření

ABSTRACT

The main goal of the diploma thesis is the security assessment of the forwarding warehouse and the design of its security. The theoretical part describes the basic concepts related to the issue and description of security assessment in the field of security. The practical part describes the actual state of the warehouse and office building, possible threat identification, risk analysis and design of security measures.

Keywords: Risk analysis, risk, threat, safety and health protection at work, fire protection, video monitoring system, camera system, alarm and security emergency system, security measures

Chtěl bych poděkovat své vedoucí diplomové práce Ing. Doře Kotkové, Ph.D za cenné rady a vedení při psaní mé práce. Dále bych rád poděkoval mým blízkým za jejich morální podporu při studiu.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Bezpečnost je v dnešní době velice důležitá pro každou organizaci. Dá se říct, že může ovlivnit i samotnou existenci organizace, a proto je důležité, aby nebyla podceňována oblast ochrany. Samotná bezpečnost je vnímána jako komplexní soubor různých bezpečnostních zaměření s cílem minimalizovat možné bezpečnostní incidenty a zajistit kontinuitu fungování organizace. Jedním ze způsobů k identifikaci a kvantifikaci rizik a odhalení zranitelností je bezpečnostní posouzení. Výsledkem takového posouzení je návrh opatření, jehož cílem je zvýšení bezpečnosti organizace.

Diplomová práce je zaměřena na fyzickou bezpečnost objektu skladu, odhalení slabých míst a návrh bezpečnostních opatření, a je rozdělena na dvě části.

V teoretické části, v první kapitole, bude obecně popsána terminologie se zaměřením na problematiku týkající se bezpečnosti objektu.

V praktické části bude stručně popsána společnost, podrobněji popsán objekt skladu a kancelářských prostor a blízké okolí. Bude popsán skutečný stav objektové a informační bezpečnosti, bude zmíněna i požární bezpečnost a bezpečnost a ochrana zdraví při práci. Dále bude realizována analýza a hodnocení rizik a návrh bezpečnostních opatření. V závěru praktické části bude návrh realizace bezpečnostních opatření.

Druhá kapitola práce obsahuje obecné informace o organizaci a stručný popis okolí.

Třetí kapitola je zaměřená na popis areálu, jednotlivých budov a jejich okolí. Současně uvádí zhodnocení aktuálních bezpečnostních opatření.

Kapitola čtvrtá popisuje aktuální stav objektů. Uvádí i stav bezpečnosti a ochrany zdraví při práci a požární ochrany.

Kapitola pátá je zaměřena na samotné posouzení rizik. Obsahuje identifikaci rizik, analýzu rizik pomocí vybrané metody a hodnocení rizik.

Kapitola šestá je zaměřena na zvládání rizik a návrh bezpečnostních opatření.

V sedmé kapitole je proveden návrh kamerového systému a poplachového zabezpečovacího systému včetně popisu jednotlivých komponentů a schémat.

Poslední osmá kapitola popisuje plán realizace bezpečnostních opatření.

I. TEORETICKÁ ČÁST

1 ZÁKLADNÍ POJMY

Základními pojmy rozumíme pojmy týkající se tématu diplomové práce. Jedná se například o bezpečnost, řízení rizik a podobně. Vše je níže v podkapitolách vysvětleno.

Obecné pojmy:

1. **Bezpečnost** – *„Bezpečnost je stav, kdy jsou na nejnižší možnou míru eliminovány (minimalizovány) hrozby pro objekt (zpravidla stát, organizaci) a jeho zájmy, přičemž tento objekt je efektivně vybaven k redukci, resp. eliminaci stávajících i potencionálních hrozeb a je ochoten při tomto procesu spolupracovat.“* [1]
2. **Bezpečnostní posouzení** – má za cíl odhalit slabiny a hrozby, jejich kategorizaci a konkretizaci. Zkušenost je taková, že bez vyhodnocování účinnosti opatření, návrhem opatření pro zlepšování bezpečnosti a procesních a technických kontrolních mechanismů, se neobejde žádné bezpečnostní opatření. Z pohledu aplikace normy ISO International Organization for Standardization, jsou nedílnou součástí bezpečnostního procesu.[1].
3. **Řízení rizik** – Řízení, ovlivňování, zvládání nebo minimalizace rizik je důležitou činností každé organizace. Jakákoliv organizace čelí různým hrozbám, které je nutné eliminovat a tím chránit organizaci před vzniklou škodou, popřípadě minimalizovat jejich dopad. Jedná se o nikdy nekončící činnost každého bezpečnostního managera.[2]
4. **Posuzování rizik** – Posuzování rizik zahrnuje tři důležité činnosti. Identifikace rizik, analýza rizik a hodnocení rizik. Jedná se o subproces řízení rizik.
5. **PZTS** – Poplachové zabezpečovací a tísňové systémy. V některých publikacích můžou být označeny anglickou zkratkou IaHAS, Intruder and Hold-up Alarm System. Jejím účelem je signalizace nebezpečí ve střeženém objektu. PZTS systémy jednak informují, ale mohou i indikovat jiný druh nebezpečí. Například přepadení obsluhy čerpací stanice, zaplavení objektu, únik plynu a podobně. Norma ČSN EN 50131-1 ED.2 uvádí podrobnější údaje. [1]
6. **VSS** – Video surveillance system, kamerové systémy, v minulosti označované jako CCTV, Closed-circuit television. Jedná se o systém analogových nebo dnes již převažujících IP kamer a záznamového zařízení. VSS je systém nepoplachový, nezabrání páchání trestné činnosti, ale lze zpětně odhalit pachatele. Současně může

působit preventivně a případného pachatele odradit. Dnešní moderní kamery obsahují různé aplikace jako je detekování pohybu, čtení poznávací značky auta, rozpoznávání obličeje a podobně. Lze je integrovat do systému PZTS. [2][3]

7. **BOZP** – Bezpečnost a ochrana zdraví při práci je soubor technických, výchovných nebo organizačních opatření, jejichž úkolem je eliminace potenciálních rizik na pracovišti. Opatření se vztahují jak na zaměstnavatele a zaměstnance, tak i na ostatní fyzické osoby jako zákazníky, klienty, externisty. BOZP musí trvale řešit každý zaměstnavatel s minimálně jedním zaměstnancem. Povinnosti zaměstnavatele a zaměstnance definuje zákoník práce č. 262/2006 Sb.
8. **Požární ochrana** – Požární ochrana je soubor technických prostředků, jejichž úkolem je eliminace potencionálních rizik spojených s požárem. Prostředky vycházejí z norem a platných předpisů v oboru požární bezpečnosti.

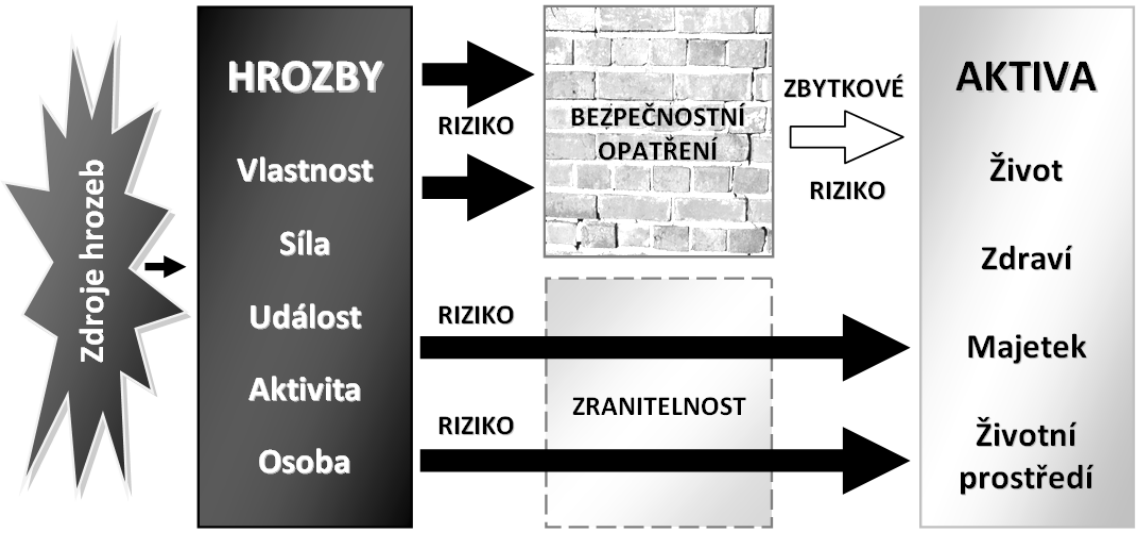
1.1 Řízení rizik

Základní pilíře řízení rizik jsou analýza rizik, hodnocení rizik a regulace rizik. V rámci své činnosti čelí organizace nebo podnik různým rizikům, jejichž následky mohou negativně ovlivnit činnost organizace či podniku. Následky těchto rizik pak mohou vést k ochromení, snížení hodnoty nebo dokonce k úplné likvidaci organizace nebo podniku. Jedním z úkolů každého manažera je působení těchto rizik předcházet, popřípadě snížit jejich dopad na nejmenší možnou míru. Řízení rizik je účinný nástroj pro identifikaci a kvantifikaci rizik a umožňuje rozhodnutí o způsobu zvládání rizik. [2]

1.1.1 Základní termíny v oblasti řízení rizik

Aktivum – Aktivem rozumíme vše, co má pro organizaci nebo podnik nějakou hodnotu, jež může být znehodnocena působením hrozby. Aktiva můžeme dělit na hmotná a nehmotná, současně může hrozba působit na organizaci či podnik jako celek, tedy aktivum může být i organizace samotná.[2][4]

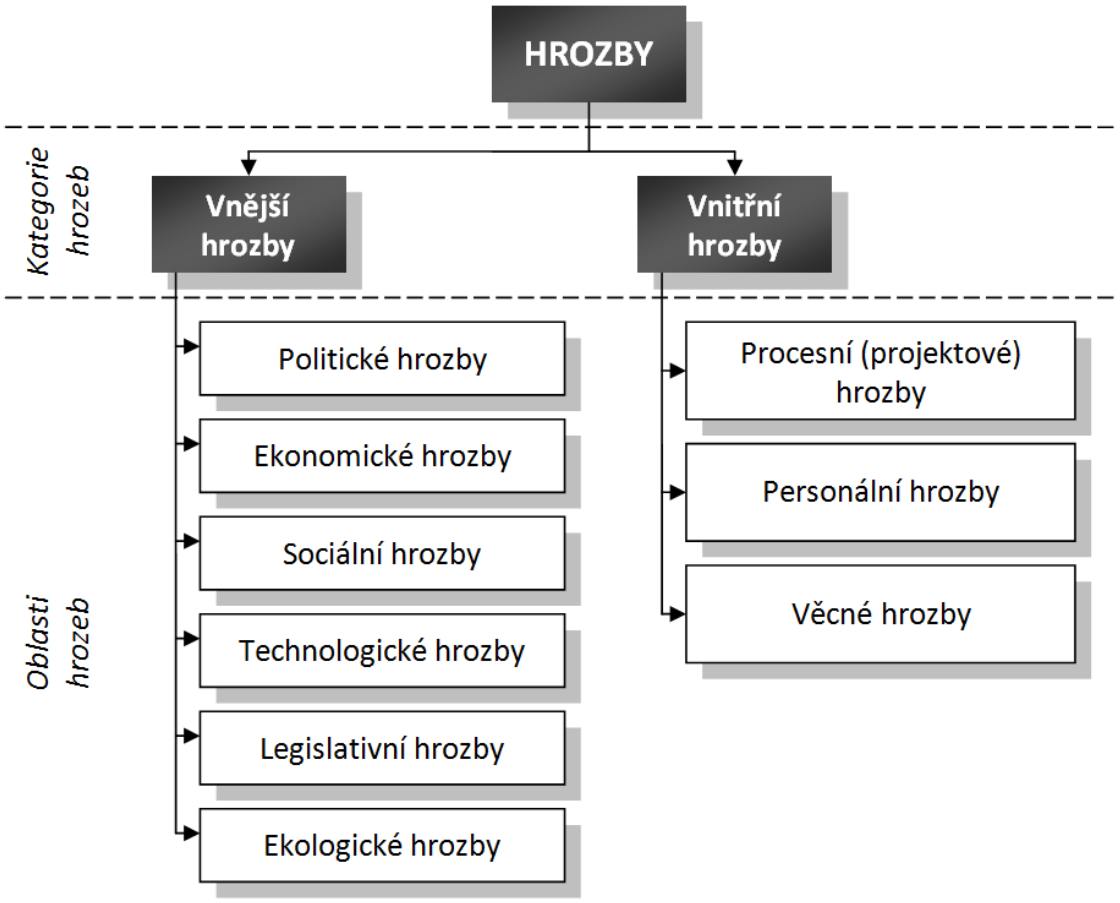
1. Hmotná aktiva – nemovitosti, finanční prostředky, zaměstnanci, majetek
2. Nehmotná aktiva – kvalita personálu, informace, autorská práva, know-how



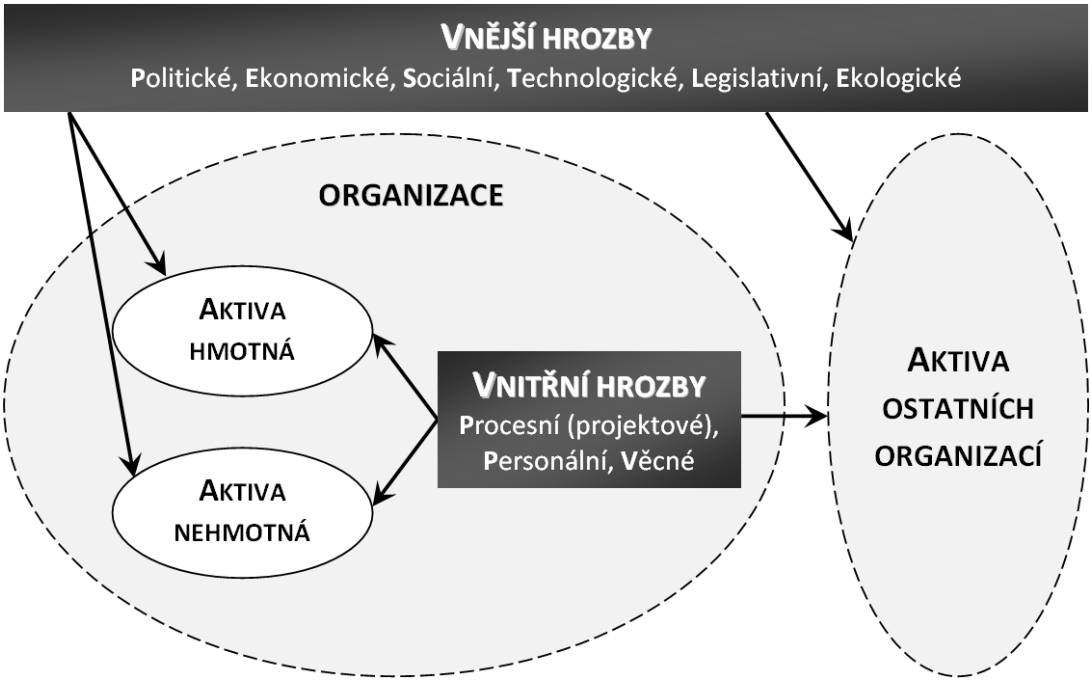
Obrázek 1. Vztah mezi základními termíny v oblasti řízení rizik. [2]

Hrozba – *„Vlastnost, síla, událost, aktivita nebo osoba, která působí buď přímo na aktivum nebo na bezpečnostní opatření s cílem získat přístup k aktivu.“*. [2] Z hlediska působení zdrojů hrozeb na organizaci můžeme dělit hrozby na vnější a vnitřní.

1. Vnější hrozby – Pro organizaci neovlivnitelné hrozby. U této kategorie hrozeb lze tlumit jen důsledky jejich působení. Kategorie obsahuje hrozby ekonomické, sociální, technologické, legislativní, ekologické a politické. [2]
2. Vnitřní hrozby – Pro organizaci ovlivnitelné hrozby. Příčiny působení této kategorie hrozeb může organizace efektivně minimalizovat nebo úplně eliminovat. Kategorie je dále rozdělena na hrozby procesní, personální a věcné. [2]



Obrázek 2. Členění hrozeb do kategorií. [2]



Obrázek 3. Působení hrozby na aktiva [2]

Riziko – *„Vzniká vzájemným působením hrozby a aktiva a je vyjadřováno kombinací (resp. součinem) pravděpodobnosti výskytu mimořádné události a jejího dopadu na dané aktivum.“.* [2]

Riziko můžeme chápat jako určitou pravděpodobnost vzniku mimořádné události s nežádoucím dopadem na aktiva organizace. Riziko představuje součin pravděpodobnosti, že nastane mimořádná událost, a závažnosti jejího dopadu. Klasifikace rizik:

1. Předvídatelné, nepředvídatelné – Předvídatelná rizika vycházející např. z ochrany informací, těžko předvídatelná rizika jsou například z oblasti živelných událostí, (vznik tornáda).
2. Ovlivnitelné, neovlivnitelné – Živelné pohromy, např. povodeň, jsou neovlivnitelná rizika. Organizace může snížit dopady budováním protipovodňových opatření, ale vznik povodně neovlivní. Ovlivnitelné riziko je např. zabránit uzavření nevýhodné smlouvy využitím služeb externí odborné organizace.
3. Primární, sekundární – Sekundární riziko je vyvoláno při realizaci opatření ke zmírnění rizik primárních. [2][8]

Zranitelnost – *„Zranitelnost představuje nedostatek, slabinu nebo stav analyzovaného aktiva, které může hrozba využít pro usnadnění svého nežádoucího vlivu. Tato veličina je vlastností aktiva a vyjadřuje, jak citlivé je aktivum na působení dané hrozby.“* [2] [4]Základní charakteristika zranitelnosti je její úroveň, jež je stanovena podle dvou základních faktorů:

- Citlivost – jak náchylné je aktivum na poškození danou hrozbou.
- Kritičnost – jak významné je aktivum pro organizaci.

Bezpečnostní opatření – prostředky, postupy nebo procesy navržené pro minimalizaci působení rizik. Jejich účel je snížení zranitelnosti, závažnosti dopadu mimořádné události, eliminaci zdrojů hrozeb nebo snížení pravděpodobnosti výskytu mimořádné události. Bezpečnostní opatření chrání aktiva, při jejich realizaci je nutné zohlednit i hodnotu samotného aktiva. [2]

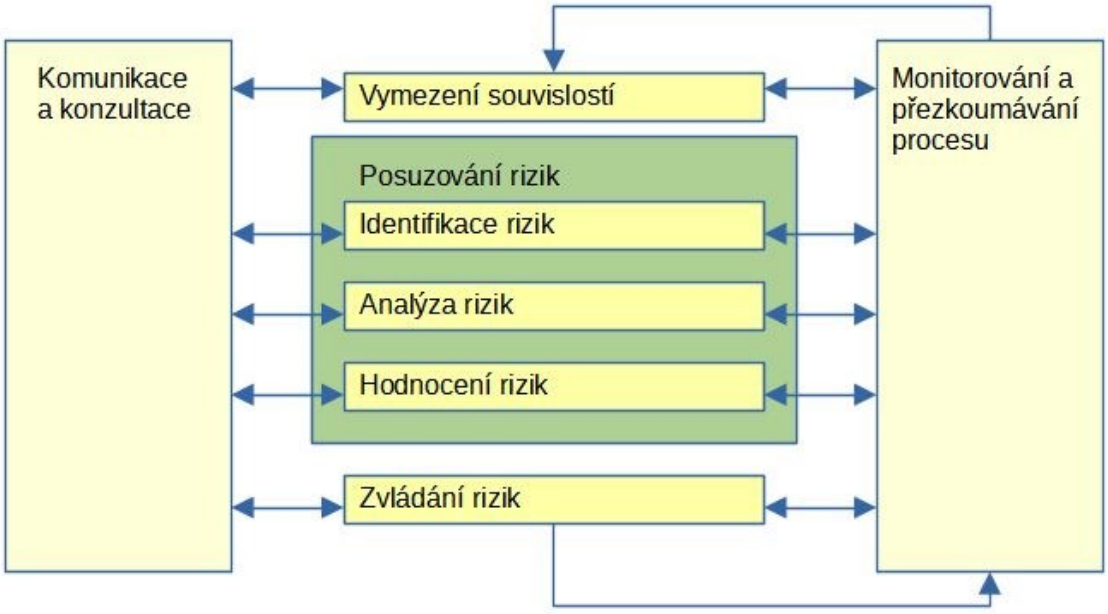
Zbytkové riziko – *„Zbytkové riziko takové riziko, které nebylo ošetřeno, nebo stále zůstává i po zavedení bezpečnostních opatření. Zbytkové riziko by mělo být natolik nízké, aby nebylo potřeba zavádět bezpečnostní opatření za účelem jeho snížení.“* [2]

Mimořádná událost – *„Mimořádnou událostí rozumíme nepříznivou (nežádoucí) odchylku od očekávaného (žádoucího) výsledku nebo stavu, resp. závažnou, časově obtížně předvídatelnou a prostorově ohraničenou událost způsobenou vlivem antropogenní činností, přírodních vlivů či procesů, která ohrožuje život, zdraví, majetek nebo životní prostředí.“* [2]

1.2 Proces řízení rizik

Proces řízení rizik musí být zakotven v kultuře společnosti, musí být součástí jejího řízení. Skládá se z pěti základních subprocesů:

- Komunikace a konzultace.
- Vymezení souvislostí.
- Posuzování rizik (zahrnuje identifikaci rizik, analýzu rizik a hodnocení rizik).
- Zvládání rizik.
- Monitorování a přezkoumávání procesu. [2]



Obrázek 4. Diagram procesu řízení rizik. [2]

1.2.1 Komunikace a konzultace

Subproces popisující komunikaci a konzultaci mezi interními a externími zainteresovanými stranami. Jedná se o nedílnou součást u procesu řízení rizik. Každá ze zainteresovaných stran si vytváří vlastní pohled a úsudek o rizicích podle toho, jak tato rizika vnímají. Vzhledem k rozdílným hodnotám, potřebám, předpokladům, zájmům a pojetí zainteresovaných stran je vnímání rizik odlišné a může se měnit. Očekávání, požadavky a vliv mohou významně ovlivnit rozhodnutí. Úsudky zainteresovaných stran je důležité zjistit, zaznamenat a vzít v úvahu v rozhodovacím procesu. Velice důležitou součástí je efektivní interní a externí komunikace a konzultace, pomocí kterých je zajištěno, že osoby odpovědné za implementaci procesu řízení rizik a zainteresované strany porozumějí základní principům a zdůvodnění, proč jsou jednotlivé činnosti požadovány a z nich vyplývající učiněná rozhodnutí. [2]

1.2.2 Vymezení souvislostí

Definice externích a interních faktorů v rámci vymezení souvislostí organizace, které budou následně zohledněný při řízení rizik.

- Vymezení externích souvislostí – Zahrnují očekávání externích zainteresovaných stran.
- Vymezení interních souvislostí – *„Interními souvislostmi chápeme vnitřní prostředí, ve kterém organizace usiluje o dosažení svých cílů. Proces řízení rizik by měl být v souladu s kulturou, procesy a strukturou organizace. Interními souvislostmi je cokoliv uvnitř organizace, co může ovlivňovat způsob, jakým bude organizace riziko řídit.“* [2]

1.2.3 Posuzování rizik

V rámci subprocesu posuzování rizik se provádí tři důležité činnosti. První činností je identifikace rizik. Identifikace rizik zahrnuje stanovení aktiv a identifikaci konkrétních hrozeb. Druhou činností je analýza rizik, která má za úkol lépe pochopit identifikovaná rizika a analýzu hrozeb a zranitelností. Hodnocení rizik je poslední činnost posuzování rizik, v níž jsou jednotlivá rizika vyhodnocena a je rozhodnuto, která rizika musí být přednostně zvládnuta.[2]

1.2.3.1 Identifikace rizik

Cílem je odhalit všechny možné hrozby působící na aktiva, jejich zdroj a možné následky. Neidentifikovaná hrozba nebude zahrnuta do následné analýzy a nebude proti ní zavedeno bezpečnostní opatření, proto je velice důležité identifikovat všechny hrozby. [2]

Stanovení aktiv

Aktivem rozumíme vše, co má pro organizaci nějakou hodnotu a co je nezbytné chránit. V rámci identifikace aktiv je vytvořen seznam všech aktiv, nacházející se v prostoru řízení rizik, stanovený v subprocesu vymezení souvislostí v předchozím kroku. Seznam obsahuje název aktiva a jeho umístění (např. vysokozdvižný vozík, umístění na vyhrazeném místě skladu), doplněné o hodnotu aktiva založeného na velikosti škody způsobené jeho zničením či ztrátou. Lze vycházet z pořizovací ceny, nebo může hodnotu charakterizovat výnosová stránka. Postavení na trhu, ochranná známka nebo kvalifikace a know-how patří mezi výnosové charakteristiky pro nepřímé dosahování zisků. Hodnota aktiva by měla odrážet závislost organizace a její samotné existence, popřípadě omezení její funkčnosti, v případě ztráty nebo poškození aktiva a následnou dobu potřebnou k jeho obnově.[2]

Identifikace hrozeb

Identifikace hrozeb spočívá ve vybírání těch hrozeb a jejich zdrojů, které můžou ohrozit minimálně jedno aktivum organizace. Pro výběr hrozeb může být využito již použitých seznamů, můžeme vycházet z vlastních zkušeností nebo třeba z dostupné literatury.

1.2.3.2 Analýza rizik

Jedná se o druhou činnost v rámci posuzování rizik. Součásti tohoto subprocesu jsou tři části:

- Analýza hrozeb a zranitelností.
- Stanovení pravděpodobnosti vzniku nežádoucí události.
- Stanovení, odhad, úrovně rizika.

Základem je lepší pochopení identifikovaných rizik. Analýza rizik poskytuje výstup pro hodnocení rizik, které vede k rozhodnutí, zda je nutné identifikovaná rizika zvládnout a současně určit nejvhodnější strategie pro zvládnutí zjištěných rizik. Analýza rizik pomocí analýzy zranitelnosti pomáhá identifikovat a kvantifikovat všechna slabá místa a v poslední části stanovit výsledné riziko.

Analýza hrozeb a zranitelností

Jde o první krok v analýze rizika. Hodnotí se každá hrozba vůči aktivu nebo skupině aktiv, které hrozba ohrožuje. Hrozba, která lze uplatnit na aktivum, je ohodnocena její úrovní vůči tomuto aktivu a také je ohodnocena úroveň zranitelnosti aktiva vůči této hrozbě. Pro stanovení úrovně hrozby bereme v potaz faktory jako motivace, přístup, nebezpečnost a podobně. U aktiva se vychází z faktorů jako kritičnost a citlivost. Je důležité zohlednit i již zavedená bezpečnostní opatření, která můžou snížit úroveň hrozby i zranitelnosti. Výstup analýzy hrozeb a zranitelností je seznam „hrozba – aktivum" s úrovní hrozby a zranitelnosti.

Stanovení pravděpodobnosti vzniku nežádoucí události a stanovení, odhad úrovně rizika

Druhý krok analyzuje hrozbu stanovením jejího dopadu a ve třetím kroku pak její pravděpodobnost. Zde je nutné také zohlednit možnost více dopadů jedné události a ovlivnění více aktiv. Analýzu rizik lze realizovat s různou úrovní podrobnosti vzhledem ke konkrétním rizikům, účelu analýzy a dostupných informací. Lze ji provést kvantitativním, semikvantitativním nebo kvalitativním způsobem, či jejich kombinací.

- Kvalitativní analýza – využívá slovního vyjádření hodnocení. Ve větší míře záleží na subjektivním odhadu hodnotitele. Může být využita v případech, kdy nejsou k dispozici číselná vyjádření nebo zdroje pro kvantitativní analýzu, anebo jako počáteční krok k identifikaci rizik, která potřebují podrobnější analýzu.
- Semikvantitativní analýza – využívá se pro podrobnější analýzu, kdy jsou ke kvalitativní stupnici přiřazeny číselné hodnoty.
- Kvantitativní analýza – Pro vyjádření používá číselné hodnoty a matematické operace. Hodnoty nám dávají větší přesnost než u kvalitativní analýzy. [2]

Tabulka 1. Příklad jednotlivých typů analýz. [2]

	Kvalitativní analýza	**Semikvantitativní analýza**	**Kvantitativní analýza**
Pravděpodobnost výskytu	Vysoká	4	83%
Závažnost dopadu	Střední	3,5	120.000,- Kč

1.2.3.3 Hodnocení rizik

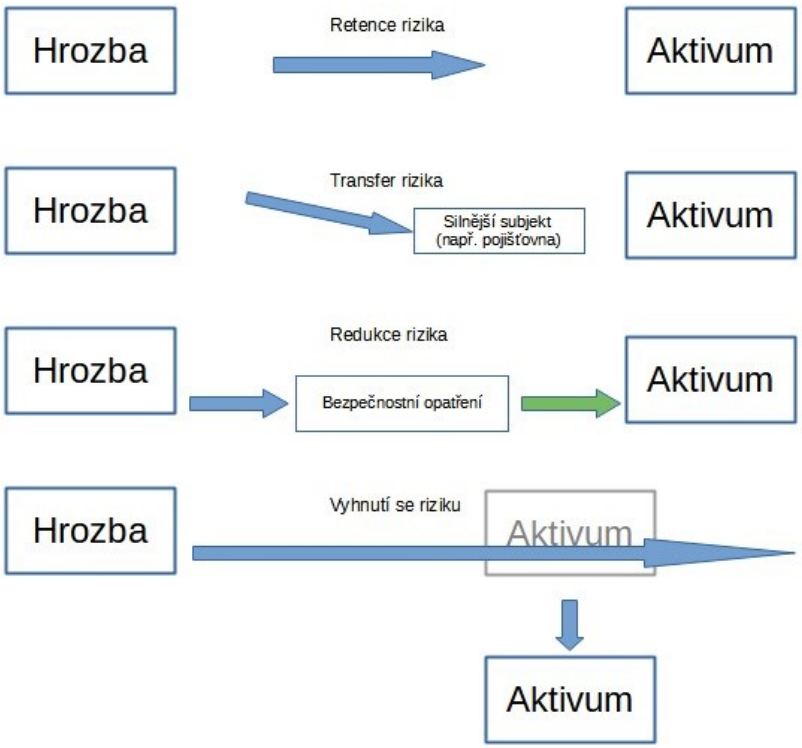
Poslední krok subprocesu posuzování rizik je hodnocení rizik. Účelem je pomoc při rozhodování o tom, která rizika musí být přednostně zvládnuta. Přitom se vychází z výsledku analýzy rizik. Součástí hodnocení rizik je komparace úrovní rizik identifikovaných během analýzy se stanovenými riziky při vymezení souvislostí, stanovení jejich přijatelnosti a jejich priorizaci. V případě nesplnění stanovených kritérií musí být riziko zvládnuto. V některých případech může organizace rozhodnout o provedení další analýzy nebo neřešit zvládání rizika.

1.2.4 Zvládání rizik

Jedná se o proces implementace jedné nebo více možností pro minimalizace rizik. Proces obsahuje čtyři části:

1. *„Výběr nejvhodnější možnosti zvládání rizik.*
2. *Implementace plánů zvládání rizik.*
3. *Zajištění realizovatelnosti vybraných bezpečnostních opatření.*
4. *Stanovení přijatelnosti zbytkového rizika.“[2]*

Jednotlivé části jsou opakovány cyklicky, dokud není riziko minimalizováno na přijatelnou úroveň, nebo zcela eliminováno. V případě, kdy riziko není přijatelné, je vhodné provést nové zvládání rizik včetně nového posouzení o jeho účinnosti. Výsledkem je zbytkové riziko na úrovni stanovených kritérií pro hodnocení rizik.



Obrázek 5. Možnosti zvládání rizik. [2]

1.2.4.1 Retence rizika

Jedná se o nejběžnější metodu zvládání rizik. Každá organizace čelí různému množství rizik, ale ve většině případů nezavádí žádné bezpečnostní opatření pro jejich zvládnutí. Retence může být vědomá v případě, kdy je riziko identifikované, či nevědomá v případě, kdy si organizace neuvědomuje hrozbu a tedy ani její možné důsledky.[2]

1.2.4.2 Transfer rizika

Transferem rizika je myšleno přesun rizika na jiný subjekt. Příčina nežádoucí události není transferem odstraněna, zaměřuje se pouze na tlumení dopadů. Nejběžnější příklad transferu rizika je uzavření pojistky. Existuje celá řada druhů pojistek a pojistit se dá prakticky cokoliv, od zdraví po majetek. Další způsob je uzavření dlouhodobé smlouvy s předem danou cenou za komoditu, čímž se organizace vyhne působení inflace, leasingové smlouvy.[2]

1.2.4.3 Redukce rizika

Redukce rizika může být provedena dvěma způsoby:

- **Proaktivní** – implementace preventivních opatření, snaha o předvídání a předcházení nežádoucím událostem.
- **Reaktivní** – reakce na již vzniklou nežádoucí událost a minimalizace závažnosti dopadu.

V obou případech mohou být rizika minimalizována jak na straně aktiva, tak i na straně hrozby.[2]

1.2.4.4 Vyhnutí se riziku

Jedná se o způsob zvládání rizik neprovedením akce. Jestliže jsou pravděpodobnost výskytu a současně i závažnost dopadu hrozby příliš vysoké a není tedy možné úroveň rizika akceptovat. [2]

1.2.5 Monitorování a přezkoumávání procesu

Nedílnou součástí procesu zvládání řízení rizik je i monitorování a přezkoumávání procesu. Mělo by zahrnovat všechna hlediska procesu řízení pro další možnosti jeho zdokonalení díky poučení se z událostí, změn, nových trendů a technologií a dalších možností. Kontrola rizik musí být efektivní již ve fázi návrhu, v realizaci i při odhalování nových objevujících se rizik. Monitorování a přezkoumávání může probíhat jak u pravidelných, jednorázových kontrol nebo formou stálého dozoru. Veškeré výsledky provedených kontrol je nezbytné zaznamenat a předat je všem zainteresovaným stranám.[2]

1.3 Metody analýzy rizik

Existuje několik metod pro analýzu rizik a je důležité vybrat tu nejvhodnější. Každá z metod má jiný druh výsledku, jsou různě náročné jak na velikost týmu, tak i z časového hlediska, a v neposlední řadě i z ekonomického hlediska. Rozdíly jsou také ve velikosti a složitosti procesu. Tabulka č. 2 uvádí několik nejpoužívanějších metod.[2]

Tabulka 2. Neužívanější metody analýzy rizik.[2]

Český název metody	Anglický název metody	zkratka
Indexové metody	Relative Ranking	RR
Revize bezpečnosti	Safety Review	SR
Kontrolní seznam	Checklist Analysis	CL

Předběžná analýza ohrožení	Preliminary Hazard Analysis	PHA
Analýza "Co se stane když ..."	What-If Analysis	WI
Co se stane když / kontrolní seznam	What-If / Check Analysis	WI/CL
Analýza nebezpečnosti a provozovatelnosti	Hazard and Operability Analysis	HAZOP
Analýza příčin a následků poruch	Failure Modes and Effects Analysis	FMEA
Analýza stromem poruch	Fault Tree Analysis	PTA
Analýza stromem událostí	Event Tree Analysis	ETA
Analýza příčin a následků	Cause - Consequence Analysis	CCA
Analýza lidského faktoru	Human Reliability Analysis	HRA

1.3.1 Kontrolní seznam

Jedná se o jednoduchou metodu odpovědí na předem připravený seznam otázek. Seznam obsahuje jasně formulované otázky, na něž existují jen dvě odpovědi, „ano“ a „ne“. Otázky jsou směrovány na možné nedostatky nebo na provozní postupy, splnění předpisů apod. Seznam může být již převzatý z jiných analýz doplněný o další otázky uzpůsobené konkrétnímu předmětu zájmu, nebo může být vytvořen seznam nový. Při vytváření nového seznamu využívá analytik norem a příslušných předpisů. [2][6]

Tabulka 3. Ukázka tabulky kontrolního seznamu [Vlastní]

Otázka	Odpověď	
	ANO	NE

1.3.2 Metoda PNH

Jednodušší nástroj pro hodnocení rizik. Metoda spočívá v postupném bodování jednotlivých kroků. Jedná se o tři kroky:

1. Pravděpodobnost vzniku (P).

2. Závažnost následků (N).
3. Názor hodnotitelů (H). [6]

Pravděpodobnost vzniku – odhad hodnotitele s jakou pravděpodobností by mohlo nastat hrozba.

Závažnost následků – odhad závažnosti následků hrozby

Názor hodnotitelů – zohledňuje několik faktorů, ke kterým patří například počet ohrožených jedinců, délka ohrožení, míra závažnosti, technický stav technologických celků, zajištění první pomoci apod.

Principem metody je ohodnocení jednotlivých hrozeb hodnotitelem. Stupnice hodnocení je stanovena hodnotitelem, kdy může být například v intervalu 1–5 nebo 1–10 (méně častá). Pro každý krok hodnocení hrozby je použita stejná stupnice. Součinem hodnocení jednotlivých kroků získáme samotné ohodnocení rizika (R).

$$R = P \times N \times H$$

Hodnota „R“ ukazuje míru rizika, na základě které bude riziko zařazeno do odpovídající kategorie stupně rizika. Tabulka č.4 ukazuje příklad kategorizace rizik při stanoveném hodnocení jednotlivých kroků 1–5.

Tabulka 4. Příklad hodnocení rizik [6][7][8]

Stupeň rizika	R	Míra rizika
I.	>100	Nepřijatelné riziko
II.	51–100	Nežádoucí riziko
III.	11–50	Mírné riziko
IV.	3–10	Akceptovatelné riziko
V.	<3	Bezvýznamné riziko

Nepřijatelné riziko – riziko s existenčními důsledky.

Nežádoucí riziko – riziko, pro které je nutné zavedení bezpečnostních opatření v co možná nejkratší době.

Mírné riziko – nutnost bezpečnostního opatření k pokrytí rizika. Kompetentní osobou stanovená lhůta pro zavedení bezpečnostního opatření.

Akceptovatelné riziko – riziko, pro které není nezbytně nutné zavádět bezpečnostní opatření, rozhoduje kompetentní osoba.

Bezvýznamné riziko – není nutné žádné opatření. [8]

1.4 Dílčí závěr

V rámci první kapitoly byly popsány základní pojmy související s problematikou bezpečnostního posouzení a řízení rizik. Byl popsán proces řízení rizik a jednotlivé jeho subprocesy.

PRAKTICKÁ ČÁST

2 OBECNÉ INFORMACE

Předmětem diplomové práce je bezpečnostní posouzení spedičního skladu. Sklad se nachází v pronajatém objektu v Brně, kam se organizace přestěhovala v loňském roce. Vlastník skladu je organizace, která má aktuálně 8 zaměstnanců a tři majitele.

Vzhledem k popisu zabezpečení firmy a poukázání na možné slabiny nebudou název společnosti ani její bližší poloha uvedeny. Důležité a potřebné informace nezbytné k provedení bezpečnostního posouzení, včetně přiložených fotografií, jsou autentické a vycházejí z podkladů poskytnutých majitelem společnosti. Současně jsem osobně provedl obhlídku objektu.

Obrázek 6. Spediční sklad [Vlastní]

Společnost se zabývá logistikou a sklad zboží je služba pro zákazníky. Zákazník určuje, jaké zboží je ve skladě uskladněno. Pro zákazníka nabízí společnost dopravu zboží do skladu, naskladnění, skladování, vyskladnění a dopravu k cílovému zákazníkovi.

2.1 Stručný popis okolí

Samotný sklad je součástí většího areálu, kde sídlí několik dalších společností. V okolí skladu se nachází příjezdová komunikace a ze dvou stran sklad sousedí se společností pro výkup železného odpadu. Část sousedící se skladem železného odpadu má vlastní oplocení. Zhruba 50 metrů od objektu skladu je vícepodlažní kancelářská budova.

2.2 Závěr

Kapitola stručně popisuje obecné informace o společnosti a předmětu podnikání, dále popisuje základní náhled na areál, ve kterém působí.

3 POPIS AREÁLU

Společnost působí v pronajaté hale ve větším areálu, kde působí několik dalších společností. Součástí pronájmu je pronájem kancelářských prostor ve vícepodlažní budově vzdálené zhruba 50 metrů od samotného skladu, kde má společnost pronajaté dvě kanceláře, sociální zařízení a kuchyňku. V objektu se nacházejí další nevyužité kanceláře. Současně je v budově i jiný nájemce, ale má vlastní vchod a je od ostatních prostor kancelářské budovy oddělen.

Obrázek 7. Náhled dispozice budov v areálu. Upraveno z [10]

Celý areál je oplocený, se vstupní pojezdovou bránou na dálkové ovládání. Obvodový plot je drátěný, z části tvoří hranici areálu budovy.

3.1 Perimetr areálu

Areál samotný se nachází v průmyslové zóně, jejíž součástí je několik dalších areálů, z nichž dva přímo sousedí s popisovaným areálem. Přední strana areálu sousedí s příjezdovou komunikací a je oddělena vstupní branou a drátěným plotem. Jednotlivé areály jsou odděleny také drátěným plotem a místy supluje plot budova postavená na hranici pozemku areálu. Drátěný plot je vysoký 2 metry, brána má výšku 1,8 metru. Kancelářská budova je jedna z budov postavených na hranici pozemku. Část, sousedící s vedlejším areálem, nemá žádné vstupní ani výstupní otvory. Budova skladu je pozičně ve středu areálu a ze dvou stran sousedí s areálem výkupu železného šrotu, který má vlastní oplocení.

Obrázek 8. Zadní část budovy skladu. [Vlastní]

Plot výkupny železného šrotu je vysoký 2 metry ze zadní strany, z přední strany je plot celokovový s výškou 1,8 metru. Celkový obvod areálu je zhruba 200 metrů, z čehož je až na výjimky plot tvořen drátěným pletivem. Při prohlídce areálu a okolí skladu nebyly nalezeny žádné bezpečnostní kamery.

Obrázek 9. Oplocení mezi budovou skladu a výkupnou železného šrotu. [Vlastní]

3.2 Režimové opatření

Společnost využívá pouze část z areálu a nemůže přímo ovlivnit zabezpečení areálu jako celku. Ten je přístupný v pracovní dny od 7:00 do 18:00. Mimo tento čas je areál uzavřený. Hlavní brána je nastavená na automatické uzavření v 18:00. Každý nájemce má k bráně dálkový ovladač a má umožněn přístup do areálu i mimo provozní dobu. Areál není vybaven žádným systémem kontroly vstupu.

3.3 Fyzická ostraha

Během provozní doby ani mimo ni není v areálu zajištěna fyzická ostraha.

3.4 Technická ochrana

Technická ochrana areálu není zajištěna. Samotná budova spedičního skladu je vybavena systémem EPS (Elektrická požární signalizace), kancelářská budova je vybavena systémem PZTS (Poplachové zabezpečovací a tísňové systémy), která je momentálně v nefunkčním stavu.

3.5 Dílčí závěr

Kapitola detailněji seznamuje s aktuálním stavem a charakteristikou areálu a spedičního skladu s kancelářskou budovou. Dále zmiňuje aktuální stav režimových opatření, fyzické ostrahy, technické ochrany a perimetrické ochrany.

4 POPIS OBJEKTU

Kapitola je zaměřená na detailnější popis objektu spedičního skladu s kancelářskou budovou.

4.1 Spediční sklad

Vlastní budova skladu je postavená z železné konstrukce obložené izolačním panelem. Budova má dvoje sekvenční vrata vysoká 3,8 metru s vestavěnými dveřmi, z nichž jsou využívána pouze jedna vrata. Dveře ve vratech jsou zabezpečeny cylindrickou vložkou. Třída bezpečnosti použité cylindrické vložky není známa. Okna skladu jsou ve výšce 3,40 metru. Budova je 20 metrů široká a 44 metrů dlouhá, výška haly je 8 metrů a byla postavena v roce 2019. V rámci technické ochrany je vybavena systémem EPS, nemá instalovaný systém PZTS ani VSS (Video surveillance systems).

Větší část vybavení haly je tvořena regálovým systémem pro uskladnění zboží. Regály jsou vysoké 6 metrů a dovolují uložit dvě patra zboží na paletách. Stojky regálů jsou ukotveny do betonové podlahy, čímž je zvýšena jejich stabilita a pevnost.

Obrázek 10. Regálový systém skladu. [Vlastní]

Obrázek 11. Skladová ulička. [Vlastní]

Obrázek 12. Volná plocha skladu. [Vlastní]

Dále je sklad vybaven vysokozdvižným vozíkem pro manipulaci se zbožím, nízkozdvižným paletovým vozíkem, počítačem pro zpracování skladové dokumentace, tiskárnou, zařízením pro barelovou vodu vybaveným ohřevem i chlazením vody, kancelářskými židlemi, stolem a skříní na oděvy.

Charakteristika skladovaného zboží je sortiment surovin pro gumárenský, stavební a kosmetický průmysl.

4.2 Kancelářská budova

V kancelářské budově má společnost pronajaty dvě kanceláře. Hlavní kancelář je vybavena kancelářským nábytkem pro dvě pracovní místa, dvěma počítači a serverem, dvěma tiskárnami a síťovým switchem. Vedlejší kancelář je vybavena kancelářským nábytkem pro jedno pracovní místo, počítačem a tiskárnou. Síťový router a NAS server je umístněný v serverové místnosti, obě zařízení jsou zálohované a chráněné záložním zdrojem UPS, který zařízení chrání proti krátkodobému výpadku elektrické energie a současně proti přepětí nebo podpětí v síti.

Obrázek 13. Kancelářská budova. [Vlastní]

Obrázek 14. Kancelář. [Vlastní]

4.3 Bezpečnost a ochrana zdraví při práci

V oblasti BOZP disponuje organizace směrnicí „Vstupní a periodické školení bezpečnosti a ochrany zdraví při práci“ a „Místní bezpečnostní předpis pro používání služebních vozidel, Školení řidičů firemních vozidel“. Oba dokumenty byly vypracovány 25.01.2022 a mají uvedenou účinnost od 31.01.2022 do 31.01.2023. Směrnice byly vypracovány externí společností, která hned v úvodu dokumentu zmiňuje, že jsou publikace duševním majetkem

organizace, jež směrnice vypracovala, a jsou chráněny autorským právem. Vzhledem k faktu nemožnosti dokument kopírovat, popíšu zde důležité pasáže směrnic.

4.3.1 Vstupní periodické školení bezpečnosti a ochrany zdraví při práci

1. První část směrnice popisuje aktuální platné zákony, vyhlášky a nařízení vztahující se k BOZP.
    a. Zákon č.262/2006 Sb. Zákoník práce.
    b. Zákon č. 309/2006 Sb. Zákon upravující další požadavky bezpečnosti a ochrany zdraví při práci.
    c. Zákon č. 258/200 Sb. O ochraně veřejného zdraví a o změně některých souvisejících zákonů.
    d. Zákon č. 373/2011 Sb. Pracovně lékařské služby
    e. Vyhláška č.432/2003 Sb. Stanovující podmínky pro zařazování prací do kategorií.
    f. Vyhláška č. 125/1993 Sb. Stanovující podmínky a sazby zákonného pojištění odpovědnosti zaměstnavatele za škodu při pracovním úrazu nebo nemoci z povolání.
    g. Nařízení vlády č. 361/2007 Sb. Stanovující podmínky ochrany zdraví zaměstnanců při práci.
    h. Nařízení vlády č. 378/2001 Sb. Stanovující bližší požadavky na bezpečný provoz a používání strojů, technických zařízení, přístrojů a nářadí.
    i. Nařízení vlády č. 101/2005 Sb. O podrobnějších požadavcích na pracoviště a pracovní prostředí.
    j. Nařízení vlády č. 375/2017 Sb. Popisující vhled, umístění a provedení bezpečnostních značek a značení.
    k. Nařízení vlády č. 201/2010 Sb. Ve znění NV č. 170/2014 Sb. Stanovující způsob evidence hlášení a zaslání záznamu o úrazu.
    l. Nařízení vlády č. 390/2021 Sb. Popisující bližší podmínky poskytování osobních ochranných pracovních prostředků, mycích, čistících a dezinfekčních prostředků.

m. Vyhláška č. 50/1978 Sb. O odborné způsobilosti v elektrotechnice.

2. Druhá část popisuje základní zásady bezpečnosti a hygieny práce a požární předpisy. Součástí je vymezení práv a povinností zaměstnanců.

    a. Práva zaměstnanců – Právo na zajištění bezpečnosti a ochrany zdraví při práci a na informování o rizicích jejich práce. V případě dojmu o ohrožení zaměstnance mají právo práci odmítnout.

    b. Povinnosti zaměstnanců – dbát o svou vlastní bezpečnost, podílet se na vytváření zdravého pracovního prostředí, dodržovat právní a ostatní předpisy a pokyny zaměstnavatele k zajištění BOZP, Oznamovat zjištěné nedostatky svému nadřízenému, bezodkladně oznámit pracovní úraz nadřízenému, dodržovat stanovené pracovní postupy, podrobit se testu na přítomnost omamných látek a alkoholu, používat osobní ochranné pracovní pomůcky a další.

3. Třetí část popisuje zásady bezpečného chování na pracovišti, rozdělené do několika podkapitol popisující například zákaz používání omamných látek a alkoholu, dodržování hygienických zásad a předpisů a podobně. Informace, návody a postupy, se kterými musí být zaměstnanec seznámen před zahájením jeho práce. Kontrola pracovišť, odborná způsobilost, zdravotní způsobilost, první pomoc, pracovně lékařské služby, prevence rizik, kategorizace prací, nakládání s odpady, trestní a hmotná odpovědnost. Současně je zde uvedeno, že zdvihací zařízení, elektrické zařízení, plynové zařízení a tlakové zařízení smí obsluhovat jen zdravotně a odborně způsobilí zaměstnanec.

V jednotlivých bodech jsou pak uvedeny i práva a povinnosti zaměstnavatele. Školení BOZP je prováděno vždy jednou ročně pro každého zaměstnance, V rámci tohoto školení jsou zaměstnanci seznámení s obsahem směrnice, příslušným ustanovením zákoníku práce a na něj navazujícími zákony, s vyhláškami, technickými normami, interními dokumenty zaměstnavatele, návody k obsluze a dalšími dokumenty.

Přílohy obsahují vzor směrnice o vstupním školením zaměstnance při jeho přijetí. Je rozděleno do dvou částí. První část školení je zaměřena na bezpečnost a ochranu zdraví při práci, druhá část je zaměřena na požární ochranu. Dále vzor obsahuje místo pro vyplnění zařazení zaměstnance do pracovní kategorie dle vyhlášky 423/2003 Sb. a jméno, funkce a podpis školícího pracovníka.

Periodické školení o bezpečnosti a ochraně zdraví při práci je v rozsahu 90 minut se závěrečným přezkoušením. Součástí je přehledná osnova čítající 16 bodů vyplývajících ze směrnice. Z prezenční listiny vyplývá, že všichni zaměstnanci mají pro tento rok školení BOZP splněno. Školení probíhalo 31.01. 2022 za účasti všech zaměstnanců.

Periodické školení vedoucích pracovníků má vlastní osnovu ve stejném rozsahu jako pro zaměstnance. Školení vedoucích zaměstnanců proběhlo ve stejný den za účasti dvou vedoucích, kteří jsou současně zodpovědní za oblast BOZP v organizaci.

4.3.2 Místní bezpečnostní předpis pro používání služebních vozidel, školení řidičů firemních vozidel

V úvodu dokumentu jsou vymezeny související předpisy, definice a pojmy, účel a platnost. Účelem dokumentu je upravení podmínek pro provoz služebních vozidel tak, aby se zabránilo vzniku pracovních úrazů zaměstnanců. Zákony a předpisy uvedené v dokumentu:

- Zákon č.262/2006 Sb. zákoník práce.
- Zákon č.309/2006 Sb. upravující další požadavky bezpečnosti a ochrany zdraví při práci.
- Zákon č. 480/2008 Sb. o provozu na pozemních komunikacích.
- Zákon č. 168/1999 Sb. o pojištění odpovědnosti za škodu způsobenou provozem vozidla.
- Zákon č. 56/2001 Sb. o podmínkách provozu na pozemních komunikacích.

Dokument popisuje povinnosti a odpovědnost zaměstnavatele i zaměstnanců. Zákoník práce udává zaměstnavateli povinnost zajistit zaměstnancům, kteří používají služební vozidlo, školení o právních a ostatních předpisech k zajištění BOZP. Současně udává povinnost zaměstnanců tyto předpisy dodržovat. Školení řidičů je prováděno jednou ročně a je součástí opakovaného školení zaměstnanců o BOZP. Druhá část dokumentu obsahuje přehlednou osnovu školení zahrnující šest bodů se závěrečným testem. Školení probíhalo 31.1. 2022 za účasti šesti zaměstnanců.

Zaměstnanci mají v rámci BOZP přiděleny následující osobní ochranné pracovní prostředky:

- Pracovní rukavice.
- Zpevněnou pracovní obuv.

- Helmy.
- Reflexní vesty.
- Mycí, čistící a dezinfekční prostředky.

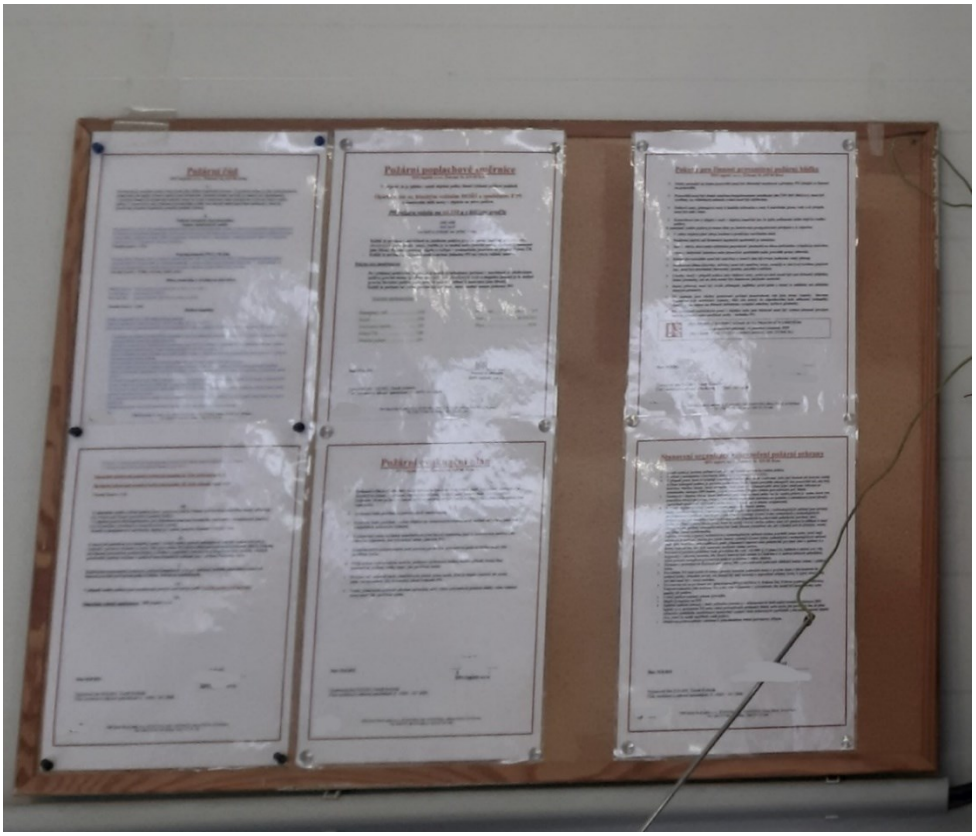
4.4 Požární ochrana

Organizace má vypracovaný dokument Požární ochrana, školení. Dokument byl vypracovaný stejnou společností jako dokumentace BOZP a byl vytvořen dne 25.01.2022 s účinností od 31.01.2022 do 31.01.2023. Téma školení má dvě verze. První verze je určená pro zaměstnance a je rozdělena do osmi tematických bodů s dobou trvání 40 minut. Druhá verze je určena pro vedoucí zaměstnance a má shodně osm tematických bodů s dobou trvání 80 minut. Součástí dokumentu jsou prezenční listiny, jedna pro školení zaměstnanců a druhá pro školení vedoucích zaměstnanců.

Z prezenčních listin vyplývá, že se první verze školení požární ochrany zúčastnilo šest zaměstnanců. Druhé verze školení, pro vedoucí pracovníky, se zúčastnili dva vedoucí zaměstnanci, kteří jsou odpovědní za oblast požární ochrany v organizaci. Školení proběhlo 31.01.2022, tedy shodně s termínem školení BOZP.

Druhá verze školení obsahuje test čítající 20 uzavřených otázek. Každá otázka má výběr ze tří možných odpovědí, kdy správná je vždy pouze jedna odpověď.

Dokument obsahuje také osnovu a tematický test pro preventivní požární hlídku a preventistu.



Obrázek 15. Požární směrnice ve skladu. [Vlastní]

Obrázek 16. Hasící přístroje. [Vlastní]

Obrázek 17. *Požární hydrant. [Vlastní]*

Obrázek 18. Únikový východ ze skladu. [Vlastní]

4.5 Zhodnocení stavu objektu

Objekt skladu je moderní budova, má zřízený systém EPS (Elektrická požární signalizace), ale nemá žádný systém technického zabezpečení. Kancelářská budova má systém zabezpečení PZTS nefunkční. Stav objektů je bez známek jakéhokoliv poškození.

Obrázek 19. Nefunkční klávesnice systému PZTS. [Vlastní]

4.6 Dílčí závěr

Kapitola popisuje aktuální stav budovy skladu a kancelářské budovy. Déle je zmíněna problematika z oblasti požární bezpečnosti a bezpečnosti a ochrany zdraví při práci.

5 POSOUZENÍ RIZIK

Součástí subprocesu posuzování rizik jsou tři důležité činnosti. Identifikace rizik, analýza rizik a hodnocení rizik.

5.1 Vymezení souvislostí

Definice externích a interních faktorů.

Zainteresované strany:

- Zákazník – externí zainteresovaná strana.

Očekávání zákazníka:

- Zajištění přepravy zboží na sklad.
- Bezpečná manipulace se skladovaným zbožím při naskladnění i vyskladnění.
- Zajištění bezpečného uskladnění zboží.
- Zabezpečení evidence skladových zásob.
- Zabezpečení přepravy a včasné doručení zboží ze skladu k odběrateli.

Odpovědné osoby v organizaci:

- Odpovědné osoby za BOZP – odpovědné osoby jsou dva majitelé. Oba mají platné proškolení pro BOZP vedoucího zaměstnance.
- Odpovědné osoby za PO – odpovědné osoby jsou dva majitelé. Oba mají platné proškolení pro PO vedoucího zaměstnance.

5.2 Identifikace rizik

V rámci identifikací rizik jsou definována aktiva a odhaleny všechny možné hrozby působící na tato aktiva.

5.2.1 Stanovení aktiv

Aktivem rozumíme vše, co má pro organizaci nebo podnik nějakou hodnotu, jež může být znehodnocena působením hrozby. [2]

- Uskladněný materiál.
- Regálový systém.

- Počítače, tiskárny.
- Data.
- Vysokozdvižný vozík.
- Nízkozdvižný vozík.
- Zaměstnanci.
- Know-how.
- Informační systém.
- Kontinuita.
- Dobré jméno společnosti.

Odhad hodnoty aktiv:

Tabulka 5. Odhad hodnoty hmotných aktiv. [Vlastní]

Aktivum	Hodnota
Uskladněný materiál	35 000 000 Kč
Regálový systém	130 000 Kč
Počítače tiskárny	100 000 Kč
Vysokozdvižný vozík	300 000 Kč
Nízkozdvižný vozík	10 000 Kč
Informační systém	20 000 Kč

5.2.2 Identifikace hrozeb

„Vlastnost, síla, událost, aktivita nebo osoba, která působí buď přímo na aktivum nebo na bezpečnostní opatření s cílem získat přístup k aktivu.“. [2] Z hlediska působení zdrojů hrozeb na organizaci můžeme dělit hrozby na vnější a vnitřní. Pro identifikaci hrozeb byla zvolena metoda kontrolního seznamu.

Tabulka 6. Kontrolní seznam.[Vlasní]

Otázka	ANO	NE
1. Obvodová ochrana areálu		
Je zajištěno oplocení celého areálu firmy?	Ano	
Je plot vždy nejméně 2 m vysoký?		Ne
Je plot v dobrém technickém stavu?	Ano	
Je zajištěný trvalý monitoring vstupu do areálu?		Ne
Je zřízen režim pro kontrolu vstupu osob, vozidel a nákladů do areálu?		Ne
2. Plášťová ochrana objektu		
Jsou vchodové dveře v dobrém technickém stavu?	Ano	
Je zabezpečena provozovna a sklad proti vstupu nepovolených osob mimo pracovní dobu?	Ano	
Je zabezpečena kancelářská budova a sklad proti vstupu nepovolených osob v pracovní době?	Ano	
Jsou zabezpečeny uskladněné produkty proti znehodnocení nežádoucí osobou při jejím případném vniknutí do objektu?		Ne
Je zabezpečeno vybavení skladu a kanceláří proti znehodnocení nežádoucí osobou při jejím případném vniknutí do objektu?		Ne
Je prostor skladu trvale monitorován?		Ne
Je prostor skladu a kanceláří vybaven systémem PZTS?		Ne
Vlastní pronajímatel klíč od objektu skladu a kanceláří	Ano	
3. Požární ochrana		
Je zpracován dokument o Požární ochraně?	Ano	
Jsou pravidelně prováděny revizní zkoušky u elektrotechnických zařízení?	Ano	
Jsou zpracovány požadované dokumenty k této oblasti?	Ano	
Jsou tyto dokumenty pravidelně aktualizovány?	Ano	

Odpovídají tyto dokumenty současným požadavkům?	Ano	
Dochází k pravidelným školením o požární ochraně?	Ano	
Dochází k pravidelným kontrolám dodržování podmínek požární bezpečnosti?		Ne
Jsou tyto kontroly a navrhovaná opatření zapsána v Požární knize?		Ne
Dochází k pravidelné revizi hasicích přístrojů?	Ano	
Vlastní provozovna agregát pro případ nefunkčnosti elektrické sítě?		Ne
Jsou cesty a prostory únikových cest trvale průchodné?	Ano	
Je sklad a kancelářská budova vybavena hromosvodem?	Ano	
Má budova skladu instalovaný systém EPS?	Ano	
4. BOZP		
Jsou zpracovány požadované dokumenty k této oblasti?	Ano	
Jsou tyto dokumenty pravidelně aktualizovány?	Ano	
Odpovídají tyto dokumenty současným požadavkům?	Ano	
Používají zaměstnanci příslušné OOPP (Osobní ochranné pracovní prostředky)?	Ano	
Je vedena evidence OOPP?		Ne
Jsou zavedeny kontroly dodržování OOPP?	Ano	
Dochází k pravidelnému školení a kontroly znalostí z BOZP?	Ano	
Dokumentace Hodnocení rizik je pravidelně aktualizována?	Ano	
Jsou nášlapné plochy schodů zabezpečeny proti uklouznutí?	Ano	
5. Informační bezpečnost		
Jsou notebooky chráněny proti virům?	Ano	
Jsou notebooky chráněny heslem proti případnému zneužití?	Ano	
Jsou notebooky dostatečně chráněn při denním přenášení z/do provozovny?	Ano	

Jsou notebooky chráněny proti krádeži dat v případě jeho krádeže?		Ne
Jsou data na serveru chráněna?	Ano	
Jsou data serveru zálohována?	Ano	
Jsou data v PC zálohována?		Ne
Jsou hesla k PC/Notebooku pravidelně měněna?		Ne
Jsou stanovena pravidla pro složitost a délku hesla k PC/Notebooku?		Ne
Jsou chráněna PC proti virům?	Ano	
5. Kontinuita		
Je činnost chráněna proti výpadku elektrické energie na déle jak 30 minut?		Ne
Je organizace chráněna proti výpadku konektivity?	Ano	
Má organizace vypracovaný plán v případě nečekané výpovědi z nájmu?		Ne

Na základě výsledku kontrolního seznamu a osobní obhlídky areálu jsou stanoveny následující hrozby.

Vnitřní hrozby:

- Krádež zboží zaměstnancem.
- Pracovní úraz zaměstnance.
- Poškození majetku zaměstnance.
- Požár – Způsoben technickou závadou, nedbalostí, popřípadě úmyslně.
- Ztráta dat v PC/notebooku z nedbalosti.
- Ztráta dat v PC/notebooku v případě jeho poškození.
- Chyba v evidenci skladovaného zboží.
- Poškození image.
- Technická závada na vybavení skladu, kanceláří.

- Nedodání zboží.
- Zpoždění dodávky.
- Chyba při nakládce zboží.

Vnější hrozby:

- Přerušení dodávky elektrické energie.
- Možnost překonání vstupu do spedičního skladu i kancelářské budovy.
- Krádež majetku, vybavení nebo skladovaného zboží cizí osobou.
- Vandalismus.
- Úmyslné znehodnocení skladovaného zboží cizí osobou.
- Krádež dat z odcizeného notebooku.
- Ztráta nebo manipulace s daty v PC/notebooku v případě odhalení hesla uživatele.
- Povodně vlivem vytrvalého deště.
- Tornádo.
- Výpověď z nájmu.
- Výpadek konektivity.

5.3 Analýza rizik

Vzhledem k množství různých metod, které lze pro zpracování bezpečnostního posouzení použít, je důležité vybrat správnou metodu. Pro bezpečnostní posouzení spedičního skladu jsem zvolil metodu kontrolního seznamu pro účel identifikace hrozeb v kombinaci s metodou PNH pro stanovení výsledného rizika.

5.3.1 Metoda PNH

Stanovení výsledného rizika bude probíhat na základě určení pravděpodobnosti jeho vzniku a následků. Pro každou zjištěnou hrozbu bude provedeno hodnocení rizika zvlášť. Po stanovení výsledného rizika bude rozhodnuto, která rizika budou přenesena na jiné subjekty, která je možné akceptovat, a pro která bude zavedeno bezpečnostní opatření. [8][9]

Jako stupnici pro ohodnocení jednotlivých rizik jsem zvolil 1 až 5 a hodnocení bude provedeno kvantitativní formou ve spolupráci s majitelem spedičního skladu.

Tři složky hodnocení:

1. Pravděpodobnost vzniku (P) – Odhad pravděpodobnosti vzniku hodnocené hrozby. Zvolená stupnice odpovídá úrovni pravděpodobnosti vzniku.
2. Míra následků (N) – Hodnocení je stanoveno stejnou stupnicí, tedy 1 až 5.
3. Názor hodnotitelů (H) – Ohodnocení zohledňuje míru závažnosti ohrožení aktiva, ale i časovou osu jeho působení na aktivum. Dále zahrnuje stav objektů, zařízení, pracovní prostředí a podmínky, zajištění první pomoci a další vlivy.

Tabulka 7. „P“ – Pravděpodobnost vzniku a existence nebezpečí.[9]

Nahodilá	1
Nepravděpodobná	2
Pravděpodobná	3
Velmi pravděpodobná	4
Jistá či trvalá	5

Tabulka 8. „N“ – Možné následky na zdraví, majetek a finance.[9]

Bez poškození zdraví, majetku či financí	1
Lehké poškození zdraví, majetku či financí	2
Vážné poškození zdraví, majetku či financí	3
Těžké poškození zdraví, majetku či financí	4
Smrtelný úraz, zničení majetku či kritický dopad na finance	5

Tabulka 9. „H“ – Vliv na míru nebezpečí akce.[9]

Zanedbatelný vliv na míru nebezpečí a ohrožení	1
Malý vliv na míru nebezpečí a ohrožení	2

Větší, nezanedbatelný vliv na míru ohrožení a nebezpečí	3
Velký a významný vliv na míru ohrožení a nebezpečí	4
Více významných a nepříznivých vlivů na závažnost a následky ohrožení a nebezpečí	5

Tabulka č. 10 uvádí úroveň hodnocení rizik seřazené sestupně dle míry rizika.

Tabulka 10. Určení stupně rizika. [6][7][8]

Rizikový stupeň	R	Míra rizika
I.	> 100	Nepřijatelné riziko
II.	51–100	Nežádoucí riziko
III.	11–50	Mírné riziko
IV.	3–10	Akceptované riziko
V.	<3	Bezvýznamné riziko

Vlastní hodnocení zjištěných rizik je uvedené v tabulce č. 11. Tabulka obsahuje seznam zjištěných hrozeb. Sloupce P, N, H obsahují hodnocení konkrétního hrozby dle výše uvedených kritérií. Poslední sloupec R obsahuje celkovou míru rizika získanou součinem všech tří hodnot.

Tabulka 11. Seznam zjištěných hrozeb a jejich hodnocení. [Vlastní].

Hrozba	P	N	H	R
Krádež zboží zaměstnancem.	1	3	2	6
Pracovní úraz zaměstnance.	2	3	2	12
Poškození majetku zaměstnancem.	3	1	2	6
Požár – způsoben technickou závadou.	3	4	4	48
Požár – způsoben nedbalostí	1	4	4	16
Požár – způsoben úmyslně.	1	4	4	16
Krádež dat z odcizeného notebooku.	4	3	3	36

Ztráta dat v PC/notebooku z nedbalosti.	3	3	3	27
Ztráta dat v PC/Notebooku v případě jeho poškození, závady.	3	2	2	12
Chyba v evidenci skladovaného zboží.	2	2	2	8
Poškození image.	2	2	3	12
Technická závada na vybavení skladu, kanceláří.	3	2	2	12
Nedodání zboží.	2	2	2	8
Zpoždění dodávky.	2	2	2	8
Přerušení dodávky elektrické energie.	2	2	2	8
Možnost překonání vstupu do spedičního skladu a kancelářské budovy.	2	3	3	18
Krádež majetku, vybavení nebo skladovaného zboží cizí osobou.	2	3	4	24
Vandalismus.	1	3	3	9
Úmyslné znehodnocení skladovaného zboží cizí osobou.	2	3	3	18
Ztráta dat nebo manipulace s daty v PC/Notebooku v případě odhalení hesla.	2	2	3	12
Povodně vlivem vytrvalého nebo intenzivního deště.	1	3	3	9
Tornádo.	1	5	5	25
Chyba při nakládce zboží.	2	2	2	8
Výpadek konektivity.	2	3	2	12
Výpověď z nájmu.	2	3	3	18

5.4 Hodnocení rizik

Každé riziko bylo vyhodnoceno mou osobou společně s majitelem skladu. Tabulka č. 12 uvádí výsledek hodnocení seřazené podle míry rizika R sestupně.

Tabulka 12. Hodnocení rizik, uspořádáno podle míry rizika. [Vlastní]

Hrozba	P	N	H	R
Požár – způsoben technickou závadou.	3	4	4	48
Krádež dat z odcizeného notebooku.	4	3	3	36
Ztráta dat v PC/notebooku z nedbalosti.	3	3	3	27
Tornádo.	1	5	5	25
Krádež majetku, vybavení nebo skladovaného zboží cizí osobou.	2	3	4	24
Možnost překonání vstupu do spedičního skladu a kancelářské budovy.	2	3	3	18
Úmyslné znehodnocení skladovaného zboží cizí osobou.	2	3	3	18
Výpověď z nájmu.	2	3	3	18
Požár – způsoben nedbalostí	1	4	4	16
Požár – způsoben úmyslně.	1	4	4	16
Pracovní úraz zaměstnance.	2	3	2	12
Ztráta dat v PC/Notebooku v případě jeho poškození, závady.	3	2	2	12
Poškození image.	2	2	3	12
Technická závada na vybavení skladu, kanceláří.	3	2	2	12
Ztráta dat nebo manipulace s daty v PC/Notebooku v případě odhalení hesla.	2	2	3	12
Výpadek konektivity.	2	3	2	12
Vandalismus.	1	3	3	9
Povodně vlivem vytrvalého nebo intenzivního deště.	1	3	3	9
Chyba v evidenci skladovaného zboží.	2	2	2	8
Nedodání zboží.	2	2	2	8
Zpoždění dodávky.	2	2	2	8
Přerušení dodávky elektrické energie.	2	2	2	8

Chyba při nakládce zboží.	2	2	2	8
Krádež zboží zaměstnancem.	1	3	2	6
Poškození majetku organizace zaměstnancem.	3	1	2	6

Nejzávažnější hrozba, vyplývající z hodnocení rizik, je požár, následovaný ztrátou dat z notebooku nebo počítače z nedbalosti, dále tornádem, krádeží majetku nebo skladovaného zboží cizí osobou. Naopak nejmenší riziko je krádež zboží zaměstnancem a poškození majetku společnosti zaměstnance.

Tabulka 13. Hodnocení rizik, uspořádáno podle pravděpodobnosti vzniku. [Vlastní]

Hrozba	P	N	H	R
Krádež dat z odcizeného notebooku.	4	3	3	36
Poškození majetku organizace zaměstnancem.	3	1	2	6
Požár – způsoben technickou závadou.	3	4	4	48
Ztráta dat v PC/notebooku z nedbalosti.	3	3	3	27
Ztráta dat v PC/Notebooku v případě jeho poškození, závady.	3	2	2	12
Technická závada na vybavení skladu, kanceláří.	3	2	2	12
Pracovní úraz zaměstnance.	2	3	2	12
Chyba v evidenci skladovaného zboží.	2	2	2	8
Poškození image.	2	2	3	12
Nedodání zboží.	2	2	2	8
Zpoždění dodávky.	2	2	2	8
Přerušení dodávky elektrické energie.	2	2	2	8
Možnost překonání vstupu do spedičního skladu a kancelářské budovy.	2	3	3	18
Krádež majetku, vybavení nebo skladovaného zboží cizí osobou.	2	3	4	24
Úmyslné znehodnocení skladovaného zboží cizí osobou.	2	3	3	18

Ztráta dat nebo manipulace s daty v PC/Notebooku v případě odhalení hesla.	2	2	3	12
Chyba při nakládce zboží.	2	2	2	8
Výpadek konektivity.	2	3	2	12
Výpověď z nájmu.	2	3	3	18
Krádež zboží zaměstnancem.	1	3	2	6
Požár – způsoben nedbalostí.	1	4	4	16
Požár – způsoben úmyslně.	1	4	4	16
Vandalismus.	1	3	3	9
Povodně vlivem vytrvalého nebo intenzivního deště.	1	3	3	9
Tornádo.	1	5	5	25

Z hodnocení podle pravděpodobnosti vyplývá jako nejzávažnější požár následovaný ztrátou dat z nedbalosti nebo závadou na zařízení, technickou závadou na vybavení skladu a poškození majetku zaměstnancem. Naopak nejnižší riziko vzniku má tornádo, vandalismus, povodně vlivem vytrvalého deště a krádež zboží zaměstnancem.

Tabulka 14. Hodnocení rizik, uspořádané podle možných následků. [Vlastní]

Hrozba	P	N	H	R
Tornádo.	1	5	5	25
Požár – způsoben technickou závadou.	3	4	4	48
Požár – způsoben nedbalostí.	1	4	4	16
Požár – způsoben úmyslně.	1	4	4	16
Krádež zboží zaměstnancem.	1	3	2	6
Pracovní úraz zaměstnance.	2	3	2	12
Krádež dat z odcizeného notebooku.	4	3	3	36
Ztráta dat v PC/notebooku z nedbalosti.	3	3	3	27

Možnost překonání vstupu do spedičního skladu a kancelářské budovy.	2	3	3	18
Krádež majetku, vybavení nebo skladovaného zboží cizí osobou.	2	3	4	24
Vandalismus.	1	3	3	9
Úmyslné znehodnocení skladovaného zboží cizí osobou.	2	3	3	18
Povodně vlivem vytrvalého nebo intenzivního deště.	1	3	3	9
Výpadek konektivity.	2	3	2	12
Výpověď z nájmu.	2	3	3	18
Ztráta dat v PC/Notebooku v případě jeho poškození, závady.	3	2	2	12
Chyba v evidenci skladovaného zboží.	2	2	2	8
Poškození image.	2	2	3	12
Technická závada na vybavení skladu, kanceláří.	3	2	2	12
Nedodání zboží.	2	2	2	8
Zpoždění dodávky.	2	2	2	8
Přerušení dodávky elektrické energie.	2	2	2	8
Ztráta dat nebo manipulace s daty v PC/Notebooku v případě odhalení hesla.	2	2	3	12
Chyba při nakládce zboží.	2	2	2	8
Poškození majetku organizace zaměstnancem.	3	1	2	6

Z pohledu možných následků na zdraví, majetek a finance vychází jako nejzávažnější hrozba tornádo a požár. Hrozba s minimálními následky je poškození majetku zaměstnancem.

Tabulka 15. Hodnocení rizik, uspořádané podle vlivu na míru nebezpečí akce. [Vlastní]

Hrozba	P	N	H	R
Tornádo.	1	5	5	25
Požár – způsoben technickou závadou.	3	4	4	48
Požár – způsoben nedbalostí	1	4	4	16
Požár – způsoben úmyslně.	1	4	4	16
Krádež majetku, vybavení nebo skladovaného zboží cizí osobou.	2	3	4	24
Krádež dat z odcizeného notebooku.	4	3	3	36
Ztráta dat v PC/notebooku z nedbalosti.	3	3	3	27
Poškození image.	2	2	3	12
Možnost překonání vstupu do spedičního skladu a kancelářské budovy.	2	3	3	18
Vandalismus.	1	3	3	9
Úmyslné znehodnocení skladovaného zboží cizí osobou.	2	3	3	18
Ztráta dat nebo manipulace s daty v PC/Notebooku v případě odhalení hesla.	2	2	3	12
Povodně vlivem vytrvalého nebo intenzivního deště.	1	3	3	9
Výpověď z nájmu.	2	3	3	18
Krádež zboží zaměstnancem.	1	3	2	6
Pracovní úraz zaměstnance.	2	3	2	12
Poškození majetku organizace zaměstnancem.	3	1	2	6
Ztráta dat v PC/Notebooku v případě jeho poškození, závady.	3	2	2	12
Chyba v evidenci skladovaného zboží.	2	2	2	8
Technická závada na vybavení skladu, kanceláří.	3	2	2	12
Nedodání zboží.	2	2	2	8
Zpoždění dodávky.	2	2	2	8

Přerušení dodávky elektrické energie.	2	2	2	8
Chyba při nakládce zboží.	2	2	2	8
Výpadek konektivity.	2	3	2	12

Poslední pohled na hodnocení rizik uspořádaný podle vlivu na míru nebezpečí akce ukazuje jako nejzávažnější hrozby tornádo, požár a krádež majetku, nebo skladovaného zboží cizí osobou. Hrozeb s nejnižším vlivem na míru nebezpečí podniku řadíme ztrátu dat vlivem poškození zařízení, technickou závadu na vybavení skladu, kanceláří, pracovní úraz zaměstnance, chyba v evidenci skladovaného zboží, nedodání zboží, zpoždění dodávky zboží, přerušení dodávky elektrické energie, krádež zboží zaměstnancem, výpadek konektivity, chyba při nakládce zboží a poškození majetku zaměstnancem.

5.5 Vyhodnocení rizik

Rizika jsou rozdělena do pěti kategorií podle tabulky číslo 10.

5.5.1 Kategorie I. a II. nepřijatelné a nežádoucí riziko

Dvě kategorie s hodnocením míry rizika vyšším jak 51 neobsahují žádné odhalené hrozby.

5.5.2 Kategorie III. Mírné riziko

Kategorie s hodnocením míry rizika 11–50, 16 hrozeb.

- Požár – způsoben technickou závadou, nedbalostí, popřípadě úmyslně.
- Krádež dat z odcizeného notebooku.
- Ztráta dat v PC/notebooku z nedbalosti.
- Tornádo.
- Krádež majetku, vybavení nebo skladovaného zboží cizí osobou.
- Možnost překonání vstupu do spedičního skladu a kancelářské budovy.
- Úmyslné znehodnocení skladovaného zboží cizí osobou.
- Výpověď z nájmu.
- Pracovní úraz zaměstnance.

- Ztráta dat v PC/Notebooku v případě jeho poškození, závady.
- Poškození image.
- Technická závada na vybavení skladu, kanceláří.
- Ztráta dat nebo manipulace s daty v PC/Notebooku v případě odhalení hesla.
- Výpadek konektivity.

5.5.3 Kategorie IV. Akceptované riziko

Kategorie s hodnocením míry rizika 3–10, 9 hrozeb

- Vandalismus.
- Povodně vlivem vytrvalého nebo intenzivního deště.
- Chyba v evidenci skladovaného zboží.
- Nedodání zboží.
- Zpoždění dodávky.
- Přerušení dodávky elektrické energie.
- Chyba při nakládce zboží.
- Krádež zboží zaměstnancem.
- Poškození majetku zaměstnancem.

5.5.4 Kategorie V. bezvýznamné riziko

Kategorie s hodnocením míry rizika méně jak tři, neobsahují žádné odhalené hrozby.

5.5.5 Vyhodnocení hrozeb, které nebudou řešeny

Z výsledku analýzy vyplývá seznam hrozeb s hodnocením 1 alespoň v jedné katrogii, které nebudou řešeny nápravným opatřením.

Tabulka 16. Hrozby, které nebudou řešeny v rámci nápravných opatření. [Vlastní]

Hrozba	P	N	H	R
Krádež zboží zaměstnancem.	1	3	2	6
Požár – způsoben nedbalostí	1	4	4	16

Požár – způsoben úmyslně.	1	4	4	16
Vandalismus.	1	3	3	9
Povodně vlivem vytrvalého nebo intenzivního deště.	1	3	3	9
Tornádo.	1	5	5	25
Poškození majetku zaměstnancem.	3	1	2	6

5.6 Dílčí závěr

Pátá kapitola je zaměřena na analýzu rizik. Identifikuje aktiva organizace a z nich vyplívající hrozby, které jsou dále hodnoceny metodou PNH. Závěr kapitoly zkoumá ohodnocené hrozby z různých pohledů.

6 ZVLÁDÁNÍ RIZIK

Na základě hodnocení rizik budou navržena bezpečnostní opatření odpovídající závažnostem zkoumaného rizika. Bezpečnostní opatření pro zvládnutí musí maximálně ošetřit konkrétní riziko a minimalizovat dopad náhlé události.

6.1 Bezpečnostní opatření

Vzhledem k výsledku analýzy rizik budou řešena jen rizika kategorie III a IV.

1. Pracovní úraz zaměstnance – Pravděpodobnost hrozby je nízká. Pro zvládnutí rizika je navrhováno zavedení kontrolního mechanismu. Celkové hodnocení míry rizika je 12.
2. Požár způsobený technickou závadou– Pravděpodobnost vzniku je střední, ale následky mohou být vysoké. Celkové hodnocení míry rizika 48. Budova skladu je vybavena systémem EPS, ve skladu jsou rozmístěny hasící přístroje a organizace splňuje bezpečnostní standard v oblasti požární ochrany. Organizace splňuje podmínky dovolující pojištění proti požáru, a tedy přenesení rizika na pojišťovnu. Pro snížení rizika je doporučeno pravidelně kontrolovat dodržování požárních předpisů, zapisovat výsledky kontrol do požární knihy a zavést sankce při jejich porušení. V případě požáru mimo pracovní dobu, je doporučeno instalovat samočinný požární systém.
3. Krádež dat z odcizeného notebooku – Doporučení pro zvládnutí rizika odcizení dat z kradeného notebooku je šifrovat pevný disk notebooku. Pro šifrování dat notebooku lze využít programu BitLocker, který je součástí systém Windows 10 professional. Všechny počítače organizace jsou vybaveny tímto systémem, není tedy nutná žádná investice do nákupu šifrovacího software.
4. Ztráta dat v PC/notebooku z nedbalosti – Doporučení přemístit důležitá data na sdílený disk serveru, který je pravidelně zálohován.
5. Ztráta dat v PC/notebooku v případě jeho poškození, závady – Doporučení ukládat data na sdílený disk serveru, který je pravidelně zálohován. Případně zálohování PC nebo notebooků, které nemají přístup k síťovému disku. Pro zálohování lze využít síťové úložiště Synology, obsahující několik integrovaných aplikací pro zálohování PC, notebooků a serverů. Například aplikace Synology cloud station

server a jeho klient instalovaný na zálohovaném počítači s názvem Cloud station backup.

6. Chyba v evidenci skladovaného zboží – Chybu v evidenci odhalí každoroční inventura. Doporučení provádět namátkovou kontrolu stavu skladových zásob i v průběhu roku.
7. Poškození image – Doporučení provádět pravidelně pohovor se zaměstnanci doplněný o dotazník spokojenosti zaměstnance. Současně použít dotazník spokojenosti i pro zákazníky pro získání zpětné vazby.
8. Technická závada na vybavení skladu, kanceláří – Riziko zvládnuto formou pravidelných revizí elektrických zařízení.
9. Nedodání zboží zákazníkovi – Riziko zvládnuto jeho přenesením na přepravce. Nedodání zboží zákazníkovy může nastat v případě nehody, nebo technické závady u přepravce. Za přepravu je zodpovědný přepravce. Organizace samotná má přepravu pojištěnou také. Při vyšší ceně zboží a po dohodě se zákazníkem je zboží připojištěno. Případ nefunkčnosti vysokozdvižného vozíku není zahrnut, jelikož je možné zapůjčit jiný přímo v areálu. V případě delší nefunkčnosti vozíku spolupracuje organizace s firmou, která vozík opraví a po dobu opravy zapůjčí jiný.
10. Zpoždění dodávky zboží k zákazníkovi – Riziko zvládnuto jeho přenesením na přepravce. Mimo přepravce má organizace vlastní pojištění přepravy.
11. Přerušení dodávky elektrické energie – Doporučení nákupu elektrocentrály pro pokrytí výpadku elektrické energie.
12. Možnost překonání vstupu do spedičního skladu a kancelářské budovy – Doporučení realizace systému PZTS a VSS (v budově skladu), následně přenést zbytkové riziko na pojišťovnu.
13. Krádež majetku nebo vybavení, skladovaného zboží cizí osobou – Doporučení realizace systému PZTS a VSS, následně přenést zbytkové riziko na pojišťovnu.
14. Úmyslné znehodnocení skladovaného zboží cizí osobou – Doporučení realizace systému PZTS a VSS, současně přenesení rizika na třetí subjekt, pojišťovnu.
15. Ztráta dat nebo manipulace s daty v PC/Notebooku v případě odhalení hesla – Doporučení stanovení pravidel pro složitost hesla na použití velkých a malých znaků,

číslic a speciálních znaků. Nastavení maximálního stáří hesla na 4 měsíce a minimální délku hesla na 12 znaků.

16. Chyba při nakládce – Doporučení realizace systému VSS pro možné odhalení chybného vyskladnění.
17. Výpadek konektivity – Riziko zvládnuto druhým poskytovatelem internetu.
18. Výpověď z nájmu – Doporučení změny výpovědní lhůty na 6 měsíců v nájemní smlouvě.

6.2 Dílčí závěr

Výsledkem hodnocení rizik je zjištění dvou důležitých bezpečnostních opatření, a to systému PZTS, systému VSS a pojištění, návrh systémů PZTS a VSS bude zpracován v následující kapitole.

7 NÁVRH POPLACHOVÉHO ZABEZPEČOVACÍHO A TÍSŇOVÉHO SYSTÉMU A KAMEROVÉHO SYSTÉMU

V rámci bezpečnostního opatření bude navržen systém PZTS a VSS.

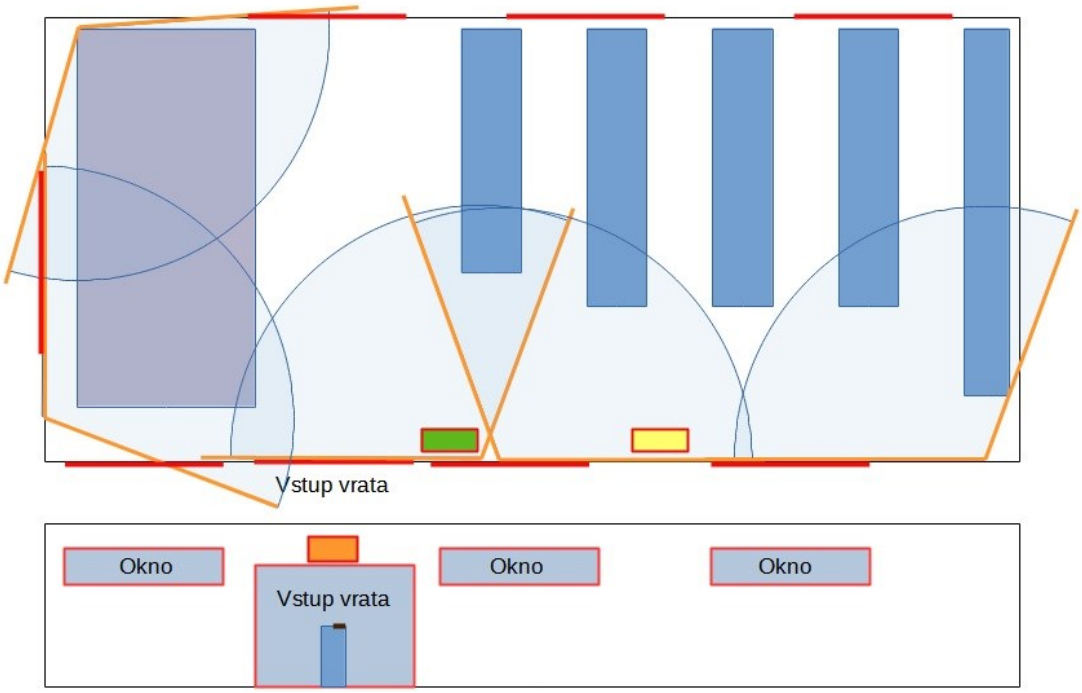
7.1 Návrh PZTS v budově skladu

Pro realizaci systému PZTS bude použit systém Jablotron, který již společnost vlastní. Tento systém byl používán v předchozích letech v budově, kde sklad sídlil původně. Jelikož nové prostory nejsou vybaveny systémem PZTS, využije se starší, již vlastněný sytém. Systém bude doplněn o nové komponenty.

Systém se skládá z následujících komponent:

1. 1 ks základní jednotka JA-101K.
2. 1ks přístupový modul JA-112E.
3. 5 ks bezdrátových PIR detektorů JA-150P.
4. 1 ks magnetický bezdrátový detektor JA-150M.
5. 1 ks vnitřní siréna JA-110A.
6. 1 ks vnější siréna JA-111A-Base-RB.
7. 50m instalační kabel CC-01.

Návrh rozmístění jednotlivých komponent ukazuje obrázek č. 20.



Obrázek 20. Rozmístění jednotlivých komponent systému PZTS. [Vlastní]

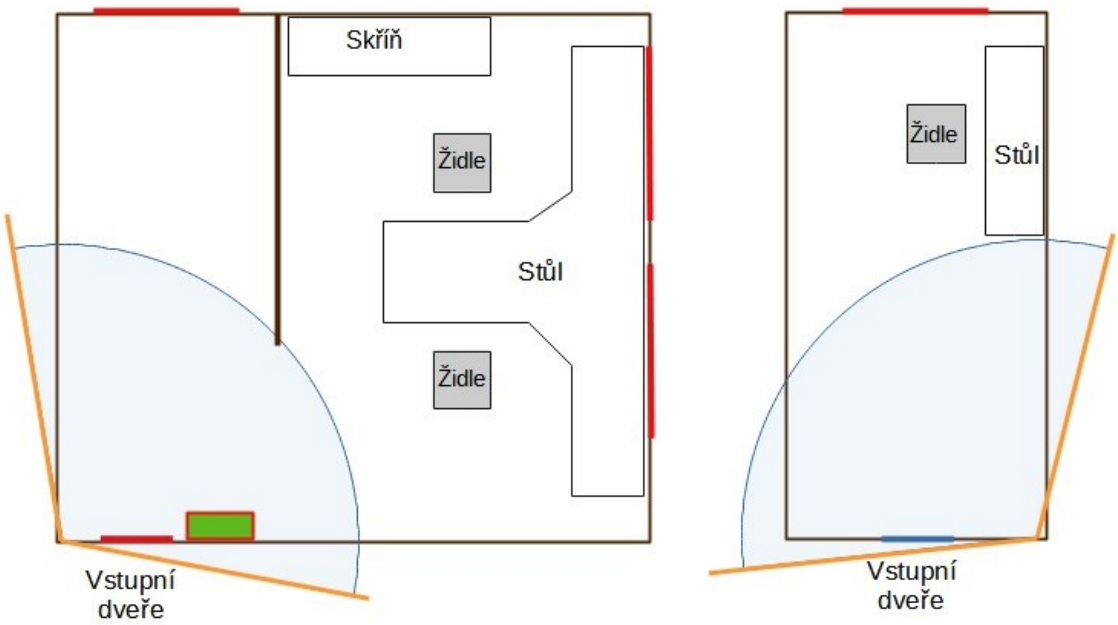
Tabulka 17. Legenda. [Vlastní]

	Volná skladovací plocha
	Regálový systém
	Ústředna JA-101k
	Přístupový modul JA-112E
	Magnetický bezdrátový detektor
	PIR detektor JA-150P
	Vnější siréna

Umístění jednotlivých komponent vychází z dispozic skladu a vstupních otvorů. Vstupní dveře v sektorových vratech budou chráněny magnetickým bezdrátovým detektorem JA-150M se zpožděním. Okna do objektu jsou ve výšce 3,40 metru a není nutné je chránit magnetickým detektorem. Současně i detektor chránící vnitřní prostor před vraty bude taktéž nastaven na zpoždění a to vždy 10 vteřin. Čas 10 vteřin je dostatečně dlouhý na odblokování systému PZTS. Vnitřní siréna bude umístěna v místě nad přístupovým modulem. Samotná základní jednotka bude umístěna ve výšce 4 metrů vedle nosníku. Počet jednotlivých detektorů lze do budoucna rozšířit a pokrýt celý vnitřní prostor skladu. Odhadovaná cena instalace systému je v rozmezí 5000,- až 7000,- Kč.

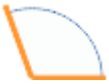
7.2 Návrh PZTS v kancelářské budově

Kancelářská budova má instalovaný systém PZTS, ale aktuálně není funkční. V případě nemožnosti opravy tohoto instalovaného systému bude navržený nový, který bude chránit pouze kanceláře. Chodby a vstup do budovy jsou společné prostory. I když je v budově momentálně pouze jeden nájemce, může nastat situace, kdy budou pronajaty i ostatní volné kanceláře. Z tohoto důvodu by nebylo vhodné, aby instalovaný systém PZTS chránil společné prostory.



Obrázek 21. Schéma systému PZTS. [Vlastní]

Tabulka 18. Legenda. [Vlastní]

	Přístupový modul JA-112E
	PIR detektor JA-150P

Obě kanceláře jsou v prvním patře budovy a považuji za dostatečné chránit pouze vstup do kanceláří. Detektory budou připojeny k stávající řídící jednotce umístěné ve skladu.

7.3 Realizace kamerového systému VSS

Úkolem kamerového VSS systému je chránit majetek a současně plnit funkci prevence nebo odstrašení případného pachatele před páchaním trestné činnosti. Jedná se ale o systém nepoplachový, nezabrání samotné protiprávní činnosti, ale zpětně lze odhalit pachatele vzniklé škody a současně ukázat, jak ke škodě došlo. V dnešní době je systém VSS cenově dostupný a nejedná se tak o velké investiční záměry.

7.3.1 Seznam komponent a jejich popis

Kamerový systém je složený z několika komponent. Navrhovaný systém počítá v první fázi s dvěma kamerami Hikvision DS-2CD1043G0-I. Napájení kamer bude realizováno pomocí technologie PoE ze síťového switche. Jako záznamové zařízení bude použit síťový disk NAS Synology DS115j vybavený 2TB pevným diskem. Tento NAS síťový disk obsahuje aplikaci pro záznam dvou kamer zdarma. Pro použití více kamer je nutné dokoupit licenci.

Základní funkce kamery DS-2CD1043G0-I:

- 1/3“ CMOS čip.
- 4mm objektiv s úhlem záběru 77° horizontálně a 42° vertikálně.
- IR přísvit pro noční režim s dosahem až 30 metrů.
- DWDR – digitální komprese protisvětla.
- Komprese videa H.265+, H.265, H.264+, H.264, MJPEG.
- BLC – nastavení zóny.
- Dva nezávislé streamy.

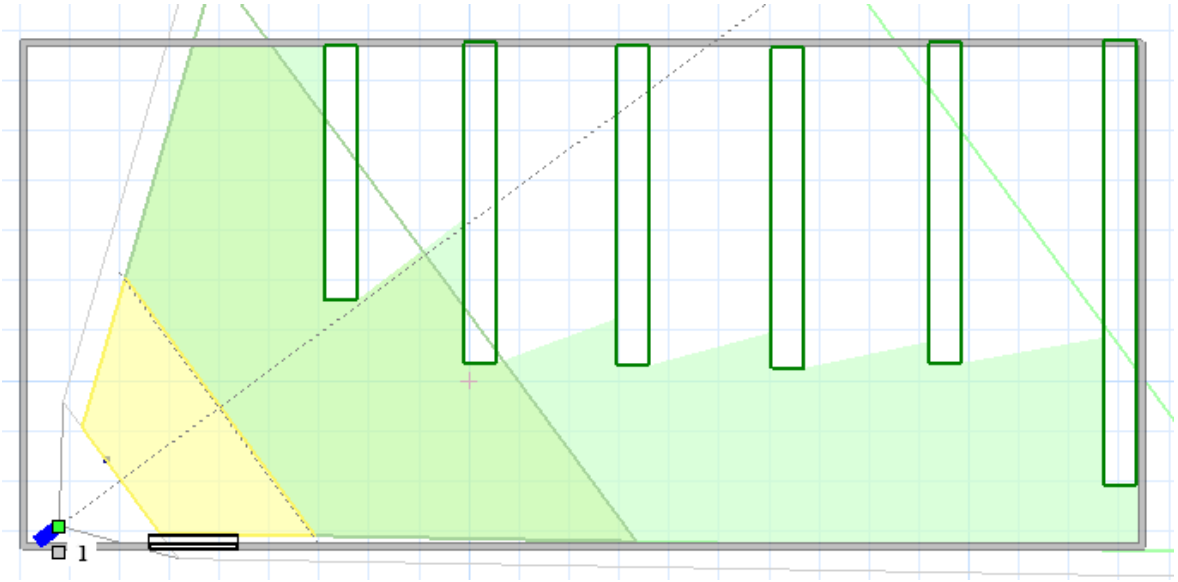
- Alarmové funkce detekce pohybu, temper alarm, neoprávněný přístup.
- IP67 krytí.
- Provozní teplota -30 až 50 °C.
- Hmotnost 280 g.
- Napájení 0,2A – 0,13A maximálně 7. [11]

Obrázek 22. Kamera Hikvision DS-2CD1043G0-I.[11]

Síťový switch TP-Link TL-SG1008P:

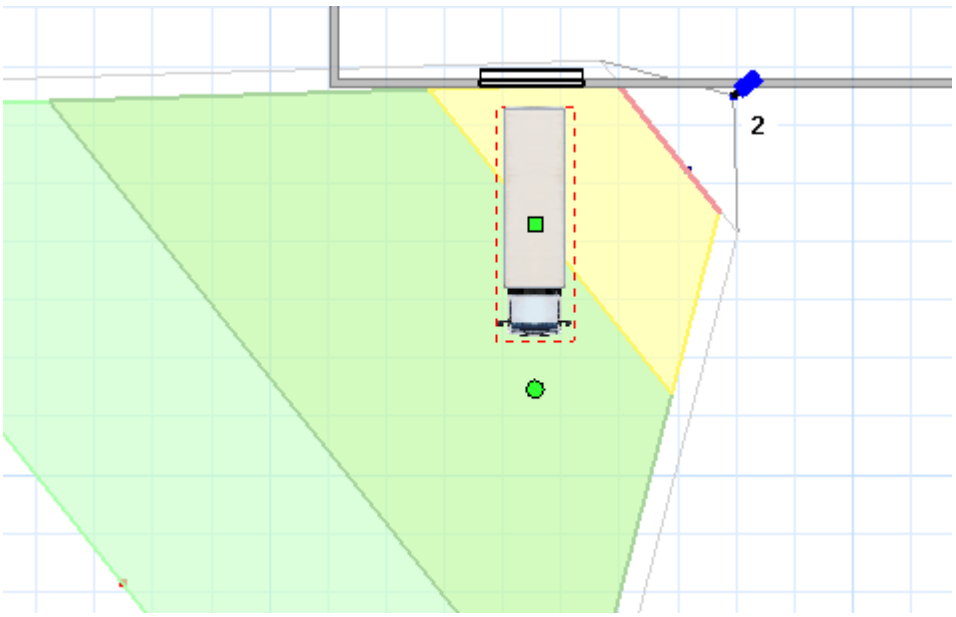
- Rychlost 10/100/1000 Mbps.
- 4x port PoE pro přenos dat i napájení.
- Celkový výkon až 55 W.[12]

Pro návrh kamerového systému byl použit SW IP Video Systém Design Tool. Výsledkem je jak umístění kamer, tak i výpočet potřebného místa na záznamovém zařízení a šířky pásma pro přenos dat z kamer do záznamového zařízení. Obrázek číslo 23 zobrazuje půdorys skladu i s regálovým systémem a výseč viditelnosti kamery č. 1. Obrázek č. 24 pak zobrazuje kameru č. 2, která je nasměrovaná na prostor před vraty skladu. [13]



Obrázek 23. Umístnění kamery číslo 1. [13]

Kamera č. 1 je umístněná ve výšce tří metrů a zabírá vnitřní prostor před vraty a regály, částečně i volnou skladovací plochu. Do budoucna by bylo vhodné doplnit systém o další kameru umístněnou v protějším rohu.



Obrázek 24. Umístnění kamery číslo 2. [13]

Tabulka 19. Výpočet potřebného místa pro záznam. [Vlastní]

Název	Protokol	Kvalita	Snímků za vteřinu	Délka záznamu (dní)	Šířka pásma	Velikost na disku
Kamera DS-2CD1043G0-I	H.265	Vysoká	20	7	5,5 Mbps	422 GB
Kamera DS-2CD1043G0-I	H.265	Vysoká	20	7	5,5 Mbps	422 GB
Požadovaná velikost na záznamovém zařízení celkem						844 GB

Kalkulace ukazuje velikost 844 GB datového prostoru pro záznam dvou kamer s historií 7 dní. Síťové zařízení NAS obsahuje disk s kapacitou 1,8 TB, což je plně dostačující i s mírnou rezervou s ohledem na fakt, že zařízení není určené jen pro záznam kamer, ale i pro zálohu dat ze serveru. Tato záloha má aktuálně velikost 60 GB, ale lze očekávat její postupný nárůst.

Orientační kalkulace potřebných komponent systému VSS je dle internetových cen.

Tabulka 20. Kalkulace VSS. [Vlastn]

Název	počet	cena celkem
Kamera DS-2CD1043G0-I	2x	5 768 Kč
Síťový switch TL-SG1008P	1x	1 350 Kč
Kabeláž 30m	30m	300 Kč
Celkem:		7 418 Kč

Ceny uvedené v kalkulaci jsou bez DPH a vychází z cen z internetu. V kalkulaci není zahrnuto záznamové zařízení, jelikož společnost již zařízení vlastní. Síťový disk NAS pro ukládání záznamu z kamer je přístupný pouze z vnitřní sítě. Přístup k záznamům bude dostupný pro administrátora a majitele organizace. Majitel má vlastní účet pro sledování záznamu a má i heslo k účtu administrátora, který ale nepoužívá. Záznam z kamer lze zpřístupnit i z internetu a sledovat záznamy kdekoliv, ale aktuálně proto nebyl požadavek od majitele. Celková historie záznamu je navržená na 7 dní a jedna kamera by tak měla vyžadovat 422GB místa na disku. Přístup k záznamu je možný pouze z vnitřní sítě organizace, přístup z vnější sítě internet nebyl požadován, nic méně jej lze kdykoliv povolit.

7.4 Dílčí závěr

V kapitole byl popsán návrh systému PZTS a VSS. U systému VSS byla uvedena i zběžná kalkulace systému. Pro systém PZTS byl použit již vlastněný demontovaný systém a je tedy uvedena pouze odhadovaná cena za instalaci.

8 REALIZACE

Z kapitoly 6 vyplývají následující nová opatření:

- Zřízení systému PZTS.
- Zřízení systému VSS.
- Aktivovat šifrování dat u notebooků.
- Přenesení citlivých dat z notebooků a PC na sdílenou složku serveru.
- Aktivovat zálohování vybraných notebooků a PC.
- Provádět náhodné kontroly stavu skladu.
- Nákup elektrocentrály.
- Stanovit pravidla pro složitost hesla.
- Prodloužit dobu výpovědní lhůty na 6 měsíců.
- Pojištění.

8.1 Rozhodnutí o realizaci jednotlivých bezpečnostních opatření

V rámci komunikace s majitelem o jednotlivých návrzích bezpečnostních opatření bylo aktuálně rozhodnuto o následujícím:

Tabulka 21. Rozhodnutí o zavedení bezpečnostního opatření. [Vlastní]

Navržené bezpečnostní opatření	Stav
Zřízení systému PZTS.	Částečně odsouhlaseno
Zřízení systému VSS.	Částečně odsouhlaseno
Aktivovat šifrování dat u notebooků.	Nebylo rozhodnuto
Přenesení citlivých dat z notebooků a PC na sdílenou složku serveru.	Nebylo rozhodnuto
Aktivovat zálohování vybraných notebooků a PC.	Nebylo rozhodnuto
Provádět náhodné kontroly stavu skladu.	Nebylo rozhodnuto
Nákup elektrocentrály.	Nebylo rozhodnuto

Stanovit pravidla pro složitost hesla.	Nebylo rozhodnuto
Prodloužit dobu výpovědní lhůty na 6 měsíců.	Nebylo rozhodnuto

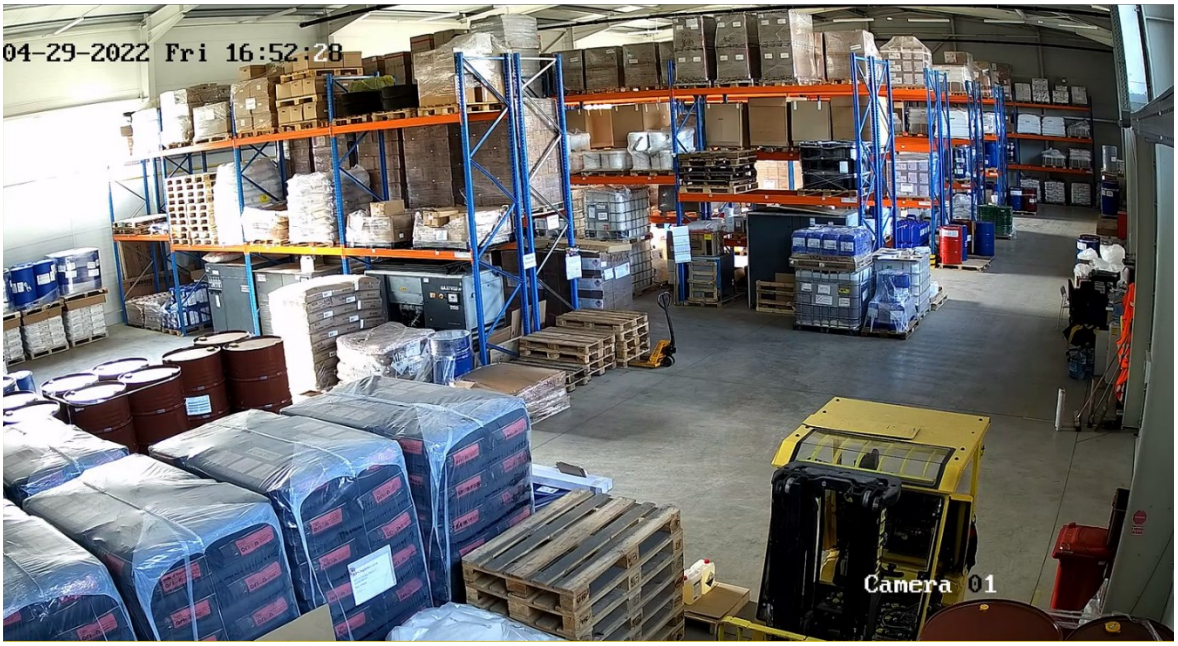
U realizace systému VSS bylo rozhodnuto o instalaci pouze jedné vnitřní kamery DS-2CD1043G0-I. U systému PZTS bylo rozhodnuto o jeho instalaci pouze v budově skladu. Rozšíření systému i v kancelářské budově ještě nebylo odsouhlaseno.

Plánovaný termín instalace systému PZTS je červenec 2022.

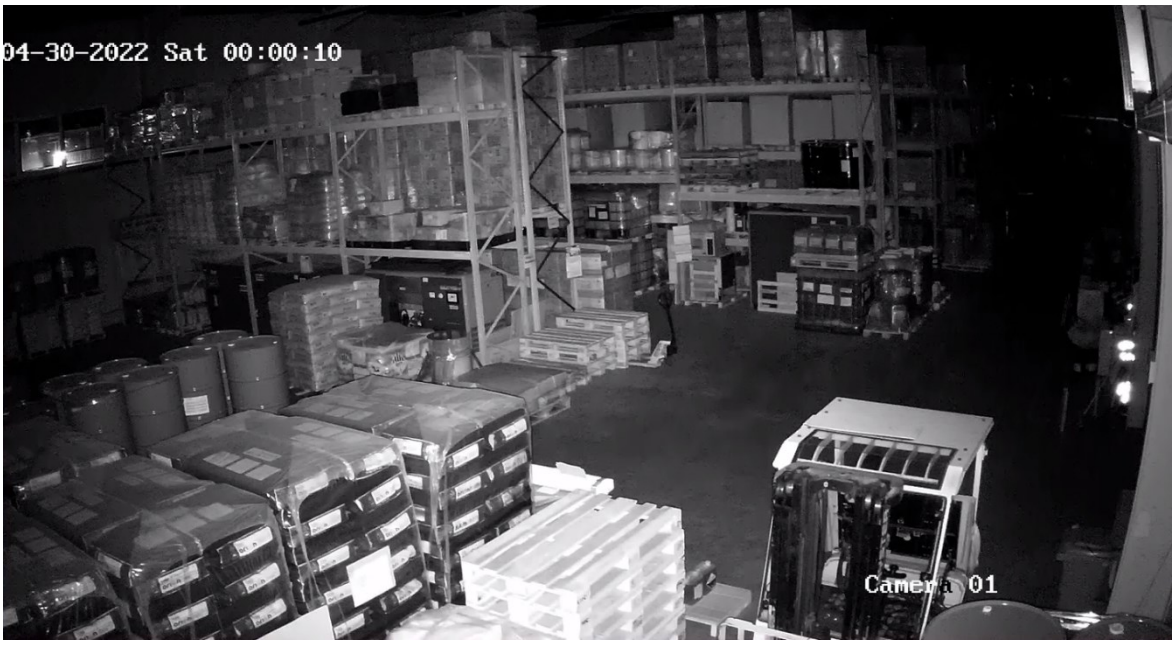
8.2 Již realizováno

Systém VSS byl již realizován podle návrhu z kapitoly 7, a je plně funkční. Níže je uvedeno několik fotografií z realizace systému VSS.

Obrázek 25. Uchycení bezpečnostní kamery. [Vlastní]



Obrázek 26. Záběr z bezpečnostní kamery opatřený časovým razítkem. [Vlastní]



Obrázek 27. Záběr bezpečnostní kamery v nočním režimu. [Vlastní]

9 NÁSLEDNÁ ANALÝZA RIZIK

Proces analýzy rizik se stále opakuje, ať už v nějakém intervalu, při zjištění nových skutečností z oblasti bezpečnosti nebo například po bezpečnostním incidentu, kdy je nutné na incident reagovat nápravným opatřením a odhalením příčiny. V případě následné analýzy rizik se vychází z původní analýzy rizik. Následné hodnocení rizik je provedeno s vědomím, že byla zavedena všechna navrhovaná opatření a zkoumá, zda zafungovala.

Tabulka 22. Následné hodnocení rizik. [Vlastní]

Hrozba	P	N	H	R
Krádež zboží zaměstnancem.	1	3	2	6
Pracovní úraz zaměstnance.	2	3	2	12
Poškození majetku zaměstnancem.	3	1	2	6
Požár – způsoben technickou závadou.	3	3	3	27
Požár – způsoben nedbalostí	1	3	3	9
Požár – způsoben úmyslně.	1	3	3	9
Krádež dat z odcizeného notebooku.	1	1	1	1
Ztráta dat v PC/notebooku z nedbalosti.	1	2	1	2
Ztráta dat v PC/Notebooku v případě jeho poškození, závady.	1	2	1	2
Chyba v evidenci skladovaného zboží.	2	2	2	8
Poškození image.	2	2	2	8
Technická závada na vybavení skladu, kanceláří.	3	2	2	12
Nedodání zboží.	2	2	2	8
Zpoždění dodávky.	2	2	2	8
Přerušení dodávky elektrické energie.	2	2	1	4
Možnost překonání vstupu do spedičního skladu a kancelářské budovy.	2	3	3	18
Krádež majetku, vybavení nebo skladovaného zboží cizí osobou.	2	3	3	18
Vandalismus.	1	3	3	9

Úmyslné znehodnocení skladovaného zboží cizí osobou.	1	3	3	9
Ztráta dat nebo manipulace s daty v PC/Notebooku v případě odhalení hesla.	1	2	3	6
Povodně vlivem vytrvalého nebo intenzivního deště.	1	3	3	9
Tornádo.	1	5	5	25
Chyba při nakládce zboží.	2	2	2	8
Výpadek konektivity.	2	3	2	12
Výpověď z nájmu.	2	2	2	8

9.1 Následné vyhodnocení rizik

Tabulka 23. Následné hodnocení rizik, uspořádáno podle míry rizika. [Vlastní]

Hrozba	P	N	H	R
Požár – způsoben technickou závadou.	3	3	3	27
Tornádo.	1	5	5	25
Možnost překonání vstupu do spedičního skladu a kancelářské budovy.	2	3	3	18
Krádež majetku, vybavení nebo skladovaného zboží cizí osobou.	2	3	3	18
Pracovní úraz zaměstnance.	2	3	2	12
Technická závada na vybavení skladu, kanceláří.	3	2	2	12
Výpadek konektivity.	2	3	2	12
Požár – způsoben nedbalostí	1	3	3	9
Požár – způsoben úmyslně.	1	3	3	9
Vandalismus.	1	3	3	9
Úmyslné znehodnocení skladovaného zboží cizí osobou.	1	3	3	9
Povodně vlivem vytrvalého nebo intenzivního deště.	1	3	3	9
Chyba v evidenci skladovaného zboží.	2	2	2	8
Poškození image.	2	2	2	8

Nedodání zboží.	2	2	2	8
Zpoždění dodávky.	2	2	2	8
Chyba při nakládce zboží.	2	2	2	8
Výpověď z nájmu.	2	2	2	8
Krádež zboží zaměstnancem.	1	3	2	6
Poškození majetku zaměstnancem.	3	1	2	6
Ztráta dat nebo manipulace s daty v PC/Notebooku v případě odhalení hesla.	1	2	3	6
Přerušení dodávky elektrické energie.	2	2	1	4
Ztráta dat v PC/notebooku z nedbalosti.	1	2	1	2
Ztráta dat v PC/Notebooku v případě jeho poškození, závady.	1	2	1	2
Krádež dat z odcizeného notebooku.	1	1	1	1

Hrozba s největším rozdílem původního a následného hodnocení je krádež dat z notebooku, které bylo sníženo z 36 na 1. Druhá nejvýraznější změna byla u ztráty dat v PC/notebooku v případě jeho poškození nebo závady z původních 27 na 2 míry rizika. Původní nezávažnější hrozba byla snížena ze 48 na 27.

Tabulka 24. Následné hodnocení rizik, uspořádané podle možných následků. [Vlastní]

Hrozba	P	N	H	R
Požár – způsoben technickou závadou.	3	3	3	27
Technická závada na vybavení skladu, kanceláří.	3	2	2	12
Poškození majetku zaměstnancem.	3	1	2	6
Možnost překonání vstupu do spedičního skladu a kancelářské budovy.	2	3	3	18
Krádež majetku, vybavení nebo skladovaného zboží cizí osobou.	2	3	3	18
Pracovní úraz zaměstnance.	2	3	2	12
Výpadek konektivity.	2	3	2	12
Chyba v evidenci skladovaného zboží.	2	2	2	8

Poškození image.	2	2	2	8
Nedodání zboží.	2	2	2	8
Zpoždění dodávky.	2	2	2	8
Chyba při nakládce zboží.	2	2	2	8
Výpověď z nájmu.	2	2	2	8
Přerušení dodávky elektrické energie.	2	2	1	4
Tornádo.	1	5	5	25
Požár – způsoben nedbalostí	1	3	3	9
Požár – způsoben úmyslně.	1	3	3	9
Vandalismus.	1	3	3	9
Úmyslné znehodnocení skladovaného zboží cizí osobou.	1	3	3	9
Povodně vlivem vytrvalého nebo intenzivního deště.	1	3	3	9
Krádež zboží zaměstnancem.	1	3	2	6
Ztráta dat nebo manipulace s daty v PC/Notebooku v případě odhalení hesla.	1	2	3	6
Ztráta dat v PC/notebooku z nedbalosti.	1	2	1	2
Ztráta dat v PC/Notebooku v případě jeho poškození, závady.	1	2	1	2
Krádež dat z odcizeného notebooku.	1	1	1	1

V případě uspořádání podle pravděpodobnosti je změna výrazná, hned 15 hrozeb bylo ohodnoceno pravděpodobností 1. Naopak hodnotu 4 nemá žádná hrozba. Původní hrozba krádeže dat z odcizeného notebooku byla snížena z hodnoty 4 na 1.

Tabulka 25. Následné hodnocení rizik, uspořádané podle možných následků. [Vlastní]

Hrozba	P	N	H	R
Tornádo.	1	5	5	25
Požár – způsoben technickou závadou.	3	3	3	27
Možnost překonání vstupu do spedičního skladu a kancelářské budovy.	2	3	3	18

Krádež majetku, vybavení nebo skladovaného zboží cizí osobou.	2	3	3	18
Pracovní úraz zaměstnance.	2	3	2	12
Výpadek konektivity.	2	3	2	12
Požár – způsoben nedbalostí	1	3	3	9
Požár – způsoben úmyslně.	1	3	3	9
Vandalismus.	1	3	3	9
Úmyslné znehodnocení skladovaného zboží cizí osobou.	1	3	3	9
Povodně vlivem vytrvalého nebo intenzivního deště.	1	3	3	9
Krádež zboží zaměstnancem.	1	3	2	6
Technická závada na vybavení skladu, kanceláří.	3	2	2	12
Chyba v evidenci skladovaného zboží.	2	2	2	8
Poškození image.	2	2	2	8
Nedodání zboží.	2	2	2	8
Zpoždění dodávky.	2	2	2	8
Chyba při nakládce zboží.	2	2	2	8
Výpověď z nájmu.	2	2	2	8
Přerušení dodávky elektrické energie.	2	2	1	4
Ztráta dat nebo manipulace s daty v PC/Notebooku v případě odhalení hesla.	1	2	3	6
Ztráta dat v PC/notebooku z nedbalosti.	1	2	1	2
Ztráta dat v PC/Notebooku v případě jeho poškození, závady.	1	2	1	2
Poškození majetku zaměstnancem.	3	1	2	6
Krádež dat z odcizeného notebooku.	1	1	1	1

V případě uspořádání hodnocení podle možných následků zůstává na prvním místě tornádo následované požárem. U požáru byla míra rizika snížena o 21 bodů na 27.

Tabulka 26. Následné hodnocení rizik, uspořádané podle vlivu nebezpečí akce. [Vlastní]

Hrozba	P	N	H	R
Tornádo.	1	5	5	25
Požár – způsoben technickou závadou.	3	3	3	27
Možnost překonání vstupu do spedičního skladu a kancelářské budovy.	2	3	3	18
Krádež majetku, vybavení nebo skladovaného zboží cizí osobou.	2	3	3	18
Požár – způsoben nedbalostí	1	3	3	9
Požár – způsoben úmyslně.	1	3	3	9
Vandalismus.	1	3	3	9
Úmyslné znehodnocení skladovaného zboží cizí osobou.	1	3	3	9
Povodně vlivem vytrvalého nebo intenzivního deště.	1	3	3	9
Ztráta dat nebo manipulace s daty v PC/Notebooku v případě odhalení hesla.	1	2	3	6
Pracovní úraz zaměstnance.	2	3	2	12
Výpadek konektivity.	2	3	2	12
Krádež zboží zaměstnancem.	1	3	2	6
Technická závada na vybavení skladu, kanceláří.	3	2	2	12
Chyba v evidenci skladovaného zboží.	2	2	2	8
Poškození image.	2	2	2	8
Nedodání zboží.	2	2	2	8
Zpoždění dodávky.	2	2	2	8
Chyba při nakládce zboží.	2	2	2	8
Výpověď z nájmu.	2	2	2	8
Poškození majetku zaměstnancem.	3	1	2	6
Přerušení dodávky elektrické energie.	2	2	1	4
Ztráta dat v PC/notebooku z nedbalosti.	1	2	1	2

Ztráta dat v PC/Notebooku v případě jeho poškození, závady.	1	2	1	2
Krádež dat z odcizeného notebooku.	1	1	1	1

Poslední pohled na následné hodnocení rizik podle vlivu na míru nebezpeční podniku ukazuje podobné výsledky jako předchozí. Opět je jako nejzávažnější hrozba tornádo následované požárem.

9.2 Následné vyhodnocení rizik

9.2.1 Kategorie I. a II. Nepřijatelné a nežádoucí riziko

Dvě kategorie s hodnocením míry rizika vyšším jak 51 neobsahují žádné odhalené hrozby.

9.2.2 Kategorie III. Mírné riziko

Kategorie s hodnocením míry rizika 11–50, 7 hrozeb z původních šestnácti.

- Požár – způsoben technickou závadou.
- Tornádo.
- Možnost překonání vstupu do spedičního skladu a kancelářské budovy.
- Krádež majetku, vybavení nebo skladovaného zboží cizí osobou.
- Pracovní úraz zaměstnance.
- Technická závada na vybavení skladu, kanceláří.
- Výpadek konektivity.

9.2.3 Kategorie IV. Akceptovatelné riziko

Kategorie s hodnocením míry rizika 3–10, 15 hrozeb z původních devíti.

- Požár – způsoben nedbalostí.
- Požár – způsoben úmyslně.
- Vandalismus.
- Úmyslné znehodnocení skladovaného zboží cizí osobou.
- Povodně vlivem vytrvalého nebo intenzivního deště.

- Chyba v evidenci skladovaného zboží.
- Poškození image.
- Nedodání zboží.
- Zpoždění dodávky.
- Chyba při nakládce zboží.
- Výpověď z nájmu.
- Krádež zboží zaměstnancem.
- Poškození majetku zaměstnancem.
- Ztráta dat nebo manipulace s daty v PC/Notebooku v případě odhalení hesla.
- Přerušení dodávky elektrické energie.

9.2.4 Kategorie V. Bezvýznamné riziko

Kategorie s hodnocením míry rizika méně jak tři, obsahuje 3 hrozby.

- Ztráta dat v PC/notebooku z nedbalosti.
- Ztráta dat v PC/Notebooku v případě jeho poškození, závady.
- Krádež dat z odcizeného notebooku.

9.3 Dílčí závěr

Kapitola 9 provádí následné hypotetické hodnocení rizik v případě, že by byla zavedena všechna navrhovaná bezpečnostní opatření. Z následné analýzy rizik vyplývá, že navrhované bezpečnostní opatření zafungovalo a v některých případech výrazně.

ZÁVĚR

Provedení bezpečnostního posouzení pomáhá k odhalení nejen slabých míst v bezpečnosti. Je důležité věnovat pozornost výsledku posouzení, dbát na navrhované bezpečnostní opatření a zavádět je do praxe. V rámci procesu řízení rizik je velice důležité v následném přezkoumání zhodnotit, zda bezpečnostní opatření zafungovala.

Cílem diplomové práce bylo bezpečnostní posouzení logistického skladu. Na základě informací získaných z obhlídky objektu a od majitele, byla vypracována analýza rizik a navržena bezpečnostní opatření.

V teoretické části byly popsány jednotlivé pojmy použité v diplomové práci, metody použité pro analýzu rizik, kdy bylo použito metody kontrolního seznamu a metody PNH. V praktické části byla popsána společnost, samotný objekt zájmu a jeho okolí.

Kapitola 2 popisuje obecné informace o organizaci a stručný popis okolí, který je doplněný podrobnějším popisem areálu v kapitole 3 a popisem objektu skladu s kancelářskou budovou v kapitole 4.

Posouzení rizik popisuje kapitola 5, jež uvádí identifikaci rizik, stanovení aktiv a identifikaci hrozeb formou kontrolního seznamu. Současně kapitola uvádí odhalené hrozby, jejich analýzu formou metody PNH a jejich hodnocení. Na hodnocení rizik je pak nahlíženo z pohledu pravděpodobnosti vzniku události, možných následků na zdraví či majetek, míry nebezpečnosti pro podnik a míry rizika.

Kapitola 6 je zaměřena na zvládání rizik a návrh bezpečnostních opatření, což je v kapitole 7 rozšířeno návrhem systému VSS a PZTS. V nejbližší době bude částečně realizován systém PZTS, který bude instalovaný v budově skladu. O instalaci systému v kancelářské budově ještě nebylo rozhodnuto.

Společnost dbá na bezpečnost jako celek. Majitelé mají snahu rizikům předcházet a bezpečnost je po ně důležitá. I přesto se rozhodli některé hrozby ignorovat. Již v průběhu identifikace rizik bylo rozhodnuto o instalaci systému VSS zatím pouze s jednou vnitřní kamerou. Realizace již proběhla a v kapitole 8 jsou vloženy snímky z instalované kamery. Systém VSS je plně funkční.

Kapitola 9 je zaměřena na hypotetickou analýzu rizik, která vychází z původní analýzy a následné nové hodnocení rizik bylo provedeno s vědomím, že byla zavedena všechna navrhovaná opatření a zkoumá, zda zafungovala.

Závěrem je třeba uvést, že proces řízení rizik je cyklus, který by měl být opakován periodicky, dále při zjištění nových skutečností z oblasti bezpečnosti a vybavení, popřípadě při náhlé události, kdy je nutné tuto událost zohlednit.

SEZNAM POUŽITÉ LITERATURY

[1] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management V*. Zlín: Radim Bačuvčík - VeRBuM, 2015. ISBN 978-80-87500-67-5.

[2] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management II*. Zlín: Radim Bačuvčík - VeRBuM, 2012. ISBN 978-80-87500-19-4.

[3] LOVEČEK, Tomáš a Peter NAGY. *Bezpečnostné systémy: kamerové bezpečnostné systémy*. Žilina: Žilinská univerzita, 2008, 283 s. Vysokoškolské učebnice. ISBN 9788080708931.

[4] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 4., aktualiz. a rozš. vyd. Praha: Grada, 2013. Expert (Grada). ISBN 978-80-247-4644-9.

[5] LAUCKÝ, Vladimír a Rudolf DRGA. *SPECIÁLNÍ TECHNOLOGIE KOMERČNÍ BEZPEČNOSTI*. Univerzita Tomáše Bati ve Zlíně, 2012. ISBN 978-80-7454-146-9

[6] BUREŠOVÁ, Soňa. *Bezpečnostní audit ve vybraném potravinářském podniku*. Univerzita Tomáše Bati ve Zlíně, 2019. Diplomová práce. Univerzita Tomáše Bati ve Zlíně. Vedoucí práce Ing. Lapková Dora PhD.

[7] Rizika a jejich analýza. *VŠB* [online]. b.r. [cit. 2019-05-05]. Dostupné z: http://fei1.vsb.cz/kat420/vyuka/Magisterske%20nav/prednasky/web/RIZIKA.pdf

[8] ŠEFČÍK, Vladimír. *Analýza rizik*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009. ISBN 978-80-7318-696-8.

[9] KOUDELKA, Ctirad. *RIZIKA A JEJICH ANALÝZA* [online]. 2006, 2006, , 17 [cit. 2020-10-27]. Dostupné z: http://fei1.vsb.cz/kat420/vyuka/Magisterske%20nav/prednasky/web/RIZIKA.pdf

[10] Mapy Google. *Mapy Google* [online]. [cit. 2022-04-27]. Dostupné z: maps.google.com

[11] DS-2CD1043G0-I. *Https://www.hikvision.com/* [online]. 2022 [cit. 2022-05-18]. Dostupné z: https://www.hikvision.com/mena-en/products/IP-Products/Network-Cameras/Value-Series/DS-2CD1043G0-I/

[12] TP-LINK TL-SG1008P. *Https://www.czc.cz/* [online]. 2022 [cit. 2022-05-18]. Dostupné z: https://www.czc.cz/tp-link-tl-sg1008p/125837/produkt

[13] JVSG: CCTV Design Software. *Https://www.jvsg.com/* [online]. 2022 [cit. 2022-05-18]. Dostupné z: https://www.jvsg.com/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

PZTS Poplachový a zabezpečovací tísňový systém

VSS Video surveillance system

OOPP Osobní ochranné pracovní prostředky

NAS Network Attached Storage

PC Personal computer

PoE Power over ethernet

EPS Elektronická požární signalizace

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: POŽÁRNÍ ŘÁD

Požární řád

I.

Provozovna je součástí areálu a hala slouží jako sklad a logistické centrum. V prostoru skladu je jak volná plocha ke skladování, tak regály určené k paletovému skladování. Součástí skladovací haly je zázemí pro zaměstnance. V prostoru činnosti je skladován materiál, který by svými vlastnostmi nebo množstvím zvyšoval riziko vzniku požáru. V prostorech, kde je činnost provozována se dále nevyskytují žádné specifické podmínky, které by ohrožovaly případné zasahující jednotky požární ochrany.

II.

Požárně technická charakteristika:

Izolace elektrických vodičů

Při teplotě cca 110°C lze očekávat měknutí několika druhů materiálů vesměs hořlavých, eventuálně samozhášivých. Při hoření lze očekávat ukapávání a vývin toxických plynů. Převážná část izolace je z polyetylénu vyráběného jako vysokotlaký s teplotou hoření 400°C a teplotou vznícení 440°C, nízkotlaký s teplotou hoření 360°C a s teplotou vznícení 417°C. V prašném stavu je výbušný.

Vhodné hasivo : CO_2

Polyvinylchlorid /PVC/, PE folie

Hoření 320°C, žhnutí 240 °C, hotové výrobky hoření 360 °C, vznícení od 400°C. Polyuretanová měkká pěna - vznícení 480 °C, hoření 440 °C. Ostatní materiály molitan a silon mají obdobné vlastnosti. U všech plastů lze očekávat odkapávání, ve větším množství tok jako kapalina, plyny hoření silně toxické.

Vhodné hasivo : Těžká, střední, lehká pěna

Dřevo, materiály a výrobky na bázi dřeva

Měkké dřevo: bod vznícení se pohybuje od 260 °C do 300 °C
Tvrdé dřevo: bod vznícení 295 °C
Dřevotřísky: jsou kombinací dřevěných pilin a pojidla

Vhodné hasivo : voda

Hořlavé kapaliny

Hořlavé kapaliny II. a III. třídy nebezpečnosti:
Teplota vzplanutí u třídy II. cca 21 - 55 °C, u třídy III. 55 - 100 °C.
Nadýchání a styk s pokožkou může vyvolat alergické reakce, narkotické účinky, dráždí pokožku, oči, sliznice.

- V případě, že dojde k rozlití hořlavé kapaliny, musí se odstranit sorbčním materiálem a uložit na určeném místě; havarijní jímka musí být udržována čistá
- Jakákoliv manipulace s hořlavými kapalinami musí být prováděna za přímého dozoru příslušného pracovníka
- Sklad je nutné zajistit proti vstupu nepovolaných osob jeho uzamčením.
- Barvy a ředidla se musí ukládat do regálu podle druhu a skladovat dle bezpečnostních listů; příjem a výdej se řídí provozním řádem skladu.
- Plné a prázdné přepravní obaly se musí skladovat odděleně a místa viditelně označit.
- Všechny obaly musí být označeny nápisem upozorňujícím na obsah s udáním třídy nebezpečnosti kapaliny.
- Obaly s hořlavými kapalinami musí být uloženy otvorem nahoru, musí být náležitě utěsněny a zajištěny proti úniku.
- Pro hořlavé kapaliny I. a II. třídy nebezpečnosti se nesmí používat přepravní obaly z plastů a pryže, pokud použití těchto obalů není upraveno výrobcem a označeno trvale na obalu.
- Při otevírání obalů s hořlavými kapalinami I. a II třídy nebezpečnosti se nesmí používat nářadí, které může způsobit mechanickou jiskru.
- Při skladování poškozených obalů hrozí nebezpečí vytečení hořlavé kapaliny, proto se poškozené obaly se nesmí skladovat.
- Skladovací prostor musí být dostatečně větraný, chráněný před slunečním zářením.

- Podlaha ve skladu musí být nepropustná a odolná vůči skladovaným hořlavým kapalinám.
- V zimních měsících nesmí teplota klesnout pod 10 °C.

Maximální skladované množství hořlavých kapaliny II. třídy nebezpečnosti: 7t

Maximální skladované množství hořlavých kapaliny III. třídy nebezpečnosti: 220t

Vhodné hasivo : CO_2

III.

- K zamezení vzniku a šíření požáru jsou v prostoru, kde je činnost provozována umístěny hasicí přístroje; (viz. Pokyny pro činnost preventivní požární hlídky)
- V objektu jsou kvůli bezpečnosti a pro případnou evakuaci rozmístěny výstražné a bezpečnostní značky; (viz. Rozmístění výstražných a bezpečnostních značek)
- Kouřit a manipulovat s otevřeným ohněm je v celém prostoru činnosti ZAKÁZÁNO.

IV.

O stanovení podmínek pro bezpečný pobyt a pohyb osob a způsob zabezpečení volných únikových cest a východů v prostoru činnosti se stará vždy preventista PO nebo velitel preventivních požárních hlídek. Pokyny pro činnost preventivní požární hlídky a přehled o umístění výstražných a bezpečnostních značek, věcných prostředků požární ochrany a požárně bezpečnostních zařízení jsou v příloze Požárního řádu.

V.

Zajišťování stanovených podmínek požární bezpečnosti, a to pro zahájení, průběh, přerušení a ukončení činnosti provádí preventivní požární hlídka složená ze zaměstnanců.

VI.

V případě vzniku požáru jsou zaměstnanci povinni postupovat podle Požární poplachové směrnice

VII.

Odpovědný vedoucí zaměstnanec:

Dne: 25.8.2021

.....

Statutární zástupce

Vypracoval dne 25.8.2021,
Číslo osvědčení o odborné způsobilosti:

Požární evakuační plán

- **Evakuaci vyhlásí a bude řídit velitel preventivních požárních hlídek popř. jím určený zástupce a to, dovolí-li to situace, z prostoru zasaženého objektu. Jestliže tento prostor bude pro organizaci evakuace vlivem požáru k tomuto účelu nepoužitelná, určí velitel preventivních požárních hlídek jiný z prostorů.**
- **Evakuace bude probíhat za pomoci všech zaměstnanců.**
- **Evakuace bude probíhat v celém objektu po vyznačených evakuačních cestách směrem k jednomu z nejbližších únikových východů.**
- **Evakuované osoby se budou soustřeďovat před hlavní objektem, jímž je provozovna součástí, ale takovým způsobem, aby byl možný zásah jednotek PO.**
- **Kontrolu počtu evakuovaných osob provede první člen preventivní požární hlídky-popř. jím pověřená osoba.**
- **První pomoc evakuovaným osobám poskytne záchranná služba, kterou přivolá druhý člen preventivní požární hlídky-popř. jím pověřená osoba.**
- **Evakuovaný materiál bude soustřeďován taktéž mimo areál, jímž je objekt součástí ale pouze takovým způsobem, aby byl možný zásah jednotek PO.**
- **Osoba, která bude provádět střežení materiálu, určí velitel preventivní požární hlídky nebo vedoucí firmy-popř. jím pověřená osoba.**

Dne: 25.8.2021

.....

Statutární zástupce

Vypracoval dne 25.8.2021,

Číslo osvědčení o odborné způsobilosti

Požární poplachové směrnice

V případě, že je zjištěn v místě objektu požár, ihned vyhlaste požární poplach

Opakujícím se, hlasitým voláním HOŘÍ a spuštěním EPS
a upozorněte další osoby v objektu na místo požáru.

Při požáru volejte na tel.150 a v hlášení uveďte

-kdo volá
-kde hoří
-co hoří a vyčkejte na zpětný dotaz

- **Každý je povinen v souvislosti se zdoláním požáru provést nutná opatření pro záchranu ohrožených osob, uhasit požár, jestliže je to možné nebo provést nutná opatření k zamezení jeho šíření. Opustit ohrožený objekt a vyčkat v evakuačním prostoru na příjezd Policie ČR.**
- **Každý je povinen poskytnout osobní pomoc jednotce PO na výzvu velitele zásahu.**

Pokyny pro zaměstnance

- **Po vyhlášení požárního poplachu je každý zaměstnanec povinen v souvislosti se zdoláváním požáru provést nutná opatření pro záchranu ohrožených osob a majetku (pokud je to možné provést likvidaci požáru nebo provést nutná opatření k zamezení jeho šíření).**
- **Každý je povinen na výzvu velitele zásahu poskytnout osobní pomoc jednotce PO.**

Důležitá telefonní čísla

Emergency call 112
Hasiči 150
Záchranná služba 155
Policie ČR 158
Městská policie 156

El. Proud 800 225 577
Voda 543 212 537
Plyn 1239

Dne: 25.8.2021

.....
Statutární zástupce

Vypracoval dne 25.8.2021,
Číslo osvědčení o odborné způsobilosti:

Pokyny pro činnost preventivní požární hlídky

- **Osoby pracující na tomto pracovišti musí být důkladně seznámeni s předpisy PO týkající se činnosti na pracovišti.**
- **Pracoviště musí být řádně označeno bezpečnostními tabulkami (dle ČSN ISO 3864) a ty musí být vyvěšeny na viditelných místech, a také musí být udržovány.**
- **Únikové cesty, přístupové cesty k hasícím zařízením a cesty k uzávěrům plynu, vody a el. proudu musí být stále volné.**
- **Kontrolovat zda si nějaká z osob v objektu nepočíná tak, že jejím počínáním může dojít ke vzniku požáru.**

K zamezení vzniku požáru je nutno dbát na dodržování protipožárních předpisů a to zejména:

- **V celém objektu platí zákaz kouření a používání otevřeného ohně.**
- **Používání jiných než firemních tepelných spotřebičů je zakázáno.**
- **Sušení oděvů, obuvi nebo odkládání jakýchkoliv předmětů na tělesa ústředního vytápění je zakázáno.**
- **Opravy elektrické instalace nebo plynových spotřebičů může provádět pouze odborník.**
- **Elektrické rozvaděče musí být uzavřeny a musí k nim být trvale zachován volný přístup.**
- **Osvětlovací tělesa (žárovky, zářivky) musí být opatřeny kryty, nesmějí se zakrývat textilem, papírem atp., musí být pravidelně zbavovány prachu, pavučin a nečistot.**
- **Chodby slouží v případě požáru jako únikové cesty, proto na nich nesmí být (ani dočasně) ukládány žádné předměty, ani na nich nesmí být skladován jakýkoliv materiál.**
- **Hasicí přístroje musí být trvale přístupné, zajištěny proti pádu a nesmí se zakládat ani obkládat různými předměty.**
- **Při odchodu jsou všichni pracovníci povinni zkontrolovat, zda jsou stroje vypnuty hlavním vypínačem a el. spotřebiče vypnuty. Dále zda nebyly do odpadkového koše odhozeny nedopalky cigaret, a zda nejsou na tělesech ústředního vytápění odloženy hořlavé předměty.**
- **Pro provádění svářečských prací v objektu nebo jeho blízkosti musí být vydáno písemné povolení ředitele podniku nebo pověřené osoby – technika PO.**

PRO PRVOTNÍ HASEBNÍ ZÁSAH JE NA PRACOVIŠTI UMÍSTĚNO
- .....ks hasících přístrojů; viz protokol o kontrole PHP
(dle § 2 odst. 5 vyhl. 246/2001 o požární prevenci; vyhl. 23/2008 Sb.)

Dne: 25.8.2021

.....
Statutární zástupce

Vypracoval dne 25.8.2021,
Číslo osvědčení o odborné způsobilosti:

Rozmístění výstražných a bezpečnostních značek

NA PRACOVIŠTI JSOU ROZMÍSTĚNY ZNAČKY:

Výstražné a bezpečnostní značky:

Seznam členů preventivní požární hlídky ČPH

Členové preventivní požární hlídky Jméno Příjmení	Číslo člena
[redacted]	1
[redacted]	2
[redacted]	3

Seznam protipožárních bezpečnostních Zařízení PBZ

Typ:	počet	umístění	Kontrolu zajišťuje
Hasicí přístroje			
Hydranty			
Nouzové osvětlení s vlastním zdrojem			
Protipožární dveře			
EPS			
Panikové kování s klikou			
Požární hlásič			

Dne: 25.8.2021

.....
Statutární zástupce

Vypracoval dne 25.8.2021, [redacted]
Číslo osvědčení o odborné způsobilosti: [redacted]

Stanovení organizace zabezpečení požární ochrany

- Každá osoba je povinna počínat si tak, aby její činnost nevedla ke vzniku požáru.
- Kouření a manipulace s otevřeným ohněm je v objektu ZAKÁZÁNO.
- V případě prací, které si vyžadují použití otevřeného ohně, popř. svařování, nebo jiné činnosti při kterých vzniká zvýšené nebezpečí požáru, je povinna osoba, která bude činnost provádět zabezpečit toto pracoviště tak, aby byly dodrženy všechny zásady, které znemožní vznik požáru a o činnosti ještě před jejím zahájením informovat statutárního zástupce RPS logistic s.r.o. a preventistu PO nebo velitele preventivních pož. hlídek.
- Nastane-li v objektu vlivem např. nedbalosti osob situace, která může vést ke vzniku požáru je osoba, která tuto nenadálou situaci zpozoruje, povinna informovat neprodleně zaměstnance podniku a zaměstnanci musí závadu neprodleně operativně odstranit a udělat kroky k tomu, aby se situace neopakovala.
- V Celém objektu je zákaz kouření a manipulace s otevřeným ohněm.
- Osoby pověřené obsluhou, kontrolou, údržbou a opravami technických a technologických zařízení jsou povinny mít odbornou kvalifikaci, kterou pro jejich činnost vyžadují výrobci těchto technických a technologických zařízení popř. tuto kvalifikaci mít rozšířenou podle případných legislativních požadavků pro daný obor.
- Osoby pověřené k prováděním prací, které by mohly vést ke vzniku požáru musí mít platnou kvalifikaci k dané činnosti a jsou povinny zabezpečit místo kde bude činnost prováděna tak, jak vyžadují právní předpisy, normy atd. řešící danou problematiku.
- Údržbu, kontroly a opravy technických a technologických zařízení mohou provádět pouze osoby, které mají odbornou kvalifikaci, kterou pro jejich činnost vyžadují výrobci těchto technických a technologických zařízení popř. tuto kvalifikaci mít rozšířenou podle případných legislativních požadavků pro daný obor a počínat si u těchto činností tak, aby bylo zamezeno možnosti vzniku požáru.
- Preventivní požární prohlídka bude prováděna dle vyhl. 246/2001 § 13 písm.1 b), každých 6 měsíců a to vždy nejpozději v takovém termínu, aby časový interval šesti měsíců byl dodržen a to osobou odborně způsobilou, která provede komplexní preventivní požární prohlídku v celém objektu.
- Záznamy o provedených školeních preventisty PO a preventivních požárních hlídkách budou vedeny v požární knize.
- Preventista PO musí každé tři měsíce provést kontrolu požárních úseků a provést zápis o této kontrole do požární knihy; případné závady zde musejí být také zmíněny a neprodlené učiněny kroky k jejich odstranění, což také musí být v knize zmíněno.
- Provozovna má za povinnost mít zpracovanou DOKUMENTACI: Požární řád, Požární poplachové směrnice, Požární evakuační plán textovou část a mít tyto dokumenty v provozovně, aby mohli být kontrolovány nebo použity při požáru.
- Cvičný požární poplach nebude prováděn.
- Objekt je napojen na EPS.
- Zajištění požární ochrany v době sníženého provozu a v mimopracovní době zajistí statutární zástupce RPS logistic s.r.o. preventista PO nebo velitel preventivních požárních hlídek nebo osoba jím pověřená tím, že před odchodem posledního zaměstnance zkontrolují vypnutí všech elektrických spotřebičů a zda nejsou patrné nějaké vlivy, které by mohli zapříčinit vznik požáru.
- Ohlašovna požáru nebude vzhledem k jednoduchému řešení provozovny zřízena.

Dne: 25.8.2021

.....

Statutární zástupce

Vypracoval dne 25.8.2021,

Číslo osvědčení o odborné způsobilosti

Datum	ZJIŠTĚNÉ ZÁVADY	Zapsal
25.8.21	Byla vydána dokumentace PO, ta je aktuální a platná.	
31.1.22	Byla provedena preventivní požární prohlídka prostor. Bez závad. Proběhlo školení PO vedoucího. Dokumentace je aktuální a platná. ✓	