Bezpečnostní posouzení vybrané stanice technické kontroly

Pavel Král

Bakalářská práce
2023

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav bezpečnostního inženýrství

Akademický rok: 2022/2023

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Pavel Král**
Osobní číslo:	**A20555**
Studijní program:	**B1032A020001 Bezpečnostní technologie, systémy a management**
Forma studia:	**Prezenční**
Téma práce:	**Bezpečnostní posouzení vybrané stanice technické kontroly**
Téma práce anglicky:	**Safety Assessment of a Selected Technical Inspection Station**

Zásady pro vypracování

1. Uveďte základní terminologii a základy řízení rizik.
2. Charakterizujte vybranou stanici technické kontroly.
3. Popište současný stav.
4. Proveďte analýzu rizik a její vyhodnocení.
5. Na základě výsledků analýzy rizik navrhněte bezpečnostní opatření.

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

Seznam doporučené literatury:

1. SMEJKAL, Vladimír a Karel RAIS. Řízení rizik ve firmách a jiných organizacích. 4., aktualiz. a rozš. vyd. Praha: Grada, 2013. Expert (Grada). ISBN 9788024746449.
2. BUŘITA, Ladislav. Prognostické metody a jejich využití v resortu obrany. Obrana a strategie [online]. Obrana a strategie, 2003, 2003(1), 47-60 [cit. 2022-11-25]. ISSN 1802-7199. Dostupné z: https://www.obranaastrategie.cz/filemanager/files/6373.pdf.
3. BERNATÍK, Aleš. Analýza nebezpečí a rizik. VŠB Technická univerzita Ostrava [online]. Ostrava: Vysoká škola Báňská – Technická univerzita Ostrava, c2022, 2016 [cit. 2022-11-25]. Dostupné z: https://www.fbi.vsb.cz/export/sites/fbi/cs/.content/galerie-souboru/U3V/studijni-materialy/U3V_Analyza_nebezpeci_a_rizik.pdf.
4. Terminologická slovník – krizové řízení a plánování obrany státu. Ministerstvo vnitra České republiky [online]. Praha: Odbor bezpečnostní politiky a prevence kriminality, c2022, 8. června 2016 [cit. 2022-11-25]. Dostupné z: https://www.mvcr.cz/clanek/terminologicky-slovnik-krizove-rizeni-a-planovani-obrany-statu.aspx.
5. KOUDELKA, Ctirad. Rizika a jejich analýza. VŠB Technická univerzita Ostrava [online]. Ostrava: Vysoká škola Báňská – Technická univerzita Ostrava, c2022, 2006 [cit. 2022-11-25]. Dostupné z: http://fei1.vsb.cz/kat420/vyuka/Magisterske%20nav/prednasky/web/RIZIKA.pdf.

Vedoucí bakalářské práce: **Ing. Lukáš Kotek**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **13. prosince 2022**
Termín odevzdání bakalářské práce: **5. června 2023**

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

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

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

Ve Zlíně dne 13. prosince 2022

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně, dne 29.5.2023 Pavel Král, v.r.

ABSTRAKT

Bakalářská práce je zaměřena na bezpečnostní posouzení vybrané stanice technické kontroly. V teoretické části je uvedena základní terminologie a základy řízení rizik. V praktické části je zpracováno bezpečnostní posouzení vybrané stanice technické kontroly, které obsahuje popis současného stavu s vyznačením slabých míst, analýzu a vyhodnocení rizik. Výstupem bakalářské práce je návrh konkrétních bezpečnostních opatření na základě zjištěných rizik.

Klíčová slova: bezpečnost, analýza rizik, řízení rizik, kontrolní seznam, FMEA analýza

ABSTRACT

The bachelor thesis deals with the safety assessment of a selected technical inspection station. In the theoretical part the basic terminology and basics of risk management are presented. In the practical part, a safety assessment of the selected technical inspection station is presented, describing the current state of the station with determination of its weak points, the analysis, and the evaluation of risks. As a result, the bachelor thesis proposes specific safety measures based on the identified risks.

Keywords: security, risk analysis, risk management, check list, FMEA analysis

Děkuji svému vedoucímu práce panu Ing. Lukášovi Kotkovi a paní Ing. Doře Kotkové, Ph.D za velmi cenné rady a odborné vedení při vypracovávání mé bakalářské práce. Dále bych rád poděkoval své rodině, všem mým přátelům a spolužákům, kteří mě při studiu podporovali. Děkuji také provozovateli a zaměstnancům zkoumaného objektu, že mi vypracování této práce umožnili. Dále děkuji Veronice Brhláčové za pomoc při gramatické a stylistické kontrole.

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

OBSAH

ÚVOD

Bezpečnost je velmi aktuální téma, kterému se často nedostává patřičné pozornosti. Spousta firem i jedinců si riziko neuvědomuje nebo nepřipouští, dokud není příliš pozdě. Ve velkém množství případů lze tedy vypozorovat, že jsou bezpečnostní chyby zanedbávány a přehlíženy. Stále je ale prokazováno, že otázka bezpečnosti je čím dál tím důležitější. Je proto nezbytné, aby se brala naprosto vážně. V problematice, kterou se zabývá bakalářská práce, je bezpečnost chápána jako žádoucí stav organizace, kterého nelze dosáhnout. Lze se však tomuto stavu přiblížit a pomocí různých opatření minimalizovat faktory, které tento stav ohrožují. Vždy je tak hlavním cílem zjistit hrozby, které na organizaci působí, a následně snížit jejich působení. Toho lze dosáhnout například omezením jejich výskytu nebo snížením jejich dopadu.

Při výběru tématu bakalářské práce jsem měl jasnou představu, že bych rád zpracoval bezpečnostní posouzení objektu. Záměrem bylo především poukázat na různé přehlížené chyby v organizaci a tím rozšířit povědomí o dané problematice. Areál, který bude následně posuzován, byl navržen přímo jeho provozovatelem. Po vysvětlení obsahu práce ho téma zaujalo a souhlasil s provedením posouzení. Práce tedy vychází z reálného objektu a z dokumentů, které mi byly poskytnuty. Pro ochranu dané organizace je v práci anonymizována.

Bakalářská práce se tedy zabývá na bezpečnostní posouzení vybrané stanice technické kontroly, se zaměřením na fyzickou bezpečnost. Výstupem je návrh opatření, která sníží působení rizik na daný objekt. Práce je rozdělena na část teoretickou a praktickou.

Teoretická část je v první kapitole zaměřena na popis důležité terminologie, která se v dané oblasti často vyskytuje. Druhá kapitola teoretické části se zaměřuje na popis řízení rizik, jeho fází a účelu.

Praktická část nejdříve charakterizuje daný objekt, kde popisuje jednotlivé budovy, jejich účel a přilehlé okolí. V další kapitole je popsán aktuální stav zabezpečení objektu, který je popisován z hlediska samotného areálu i jednotlivých budov. Další podstatnou kapitolou praktické části je analýza rizik. Ta popisuje faktory ovlivňující hodnocení, samotnou analýzu rizik a následně její vyhodnocení. Poslední kapitola je zaměřena na návrhy opatření. Ty vycházejí z analýzy rizik a jejich přijetí by mohlo být zváženo posuzovanou organizací.

I. TEORETICKÁ ČÁST

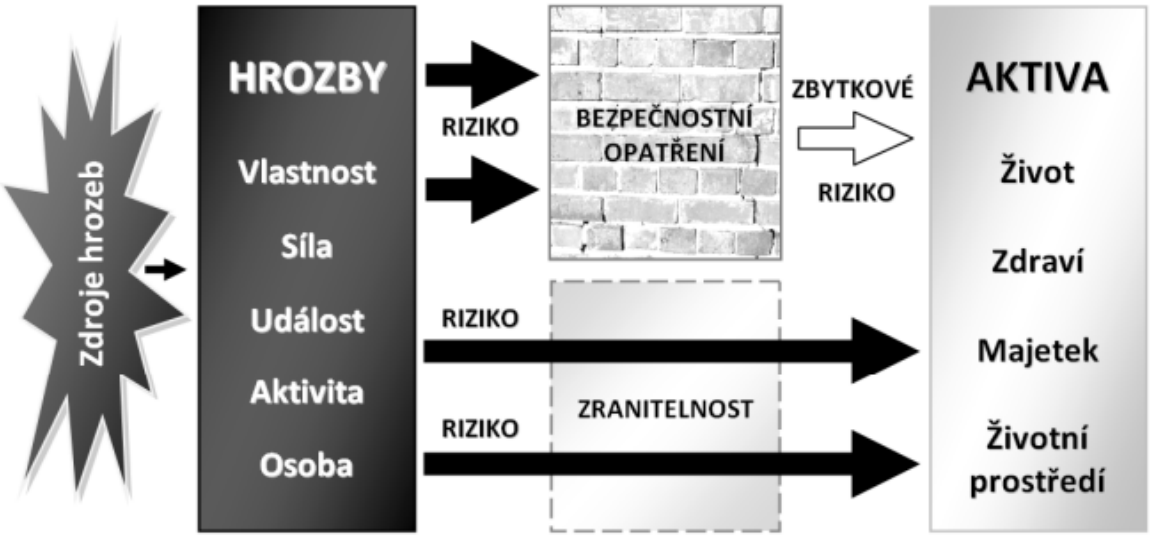
1 TERMINOLOGIE

Na začátku práce je potřeba stanovit základní termíny, které se běžně v bezpečnostním odvětví využívají, a je důležité je definovat pro účely bakalářské práce. Jedná se tak především o pojmy jako například aktivum, hrozba nebo riziko. Všechny jsou popsány v následujících podkapitolách.

1.1 Aktivum

„Označuje vše, co má pro organizaci či společnost hodnotu, která může být zmenšena působením hrozby.“ [1]

Může se tedy jednat o cokoliv, co považuje subjekt za hodnotné a co může být ohroženo. Aktiva lze rozdělit na dvě kategorie, hmotná a nehmotná. Hmotnými aktivy se primárně rozumí lidé, peníze, majetek nebo nemovitosti. Za nehmotná aktiva jsou považovány například citlivé informace a morálka. Aktivum se posuzuje z pohledu jeho hodnoty, ta může být určena například peněžně nebo i citově. [1] [2]

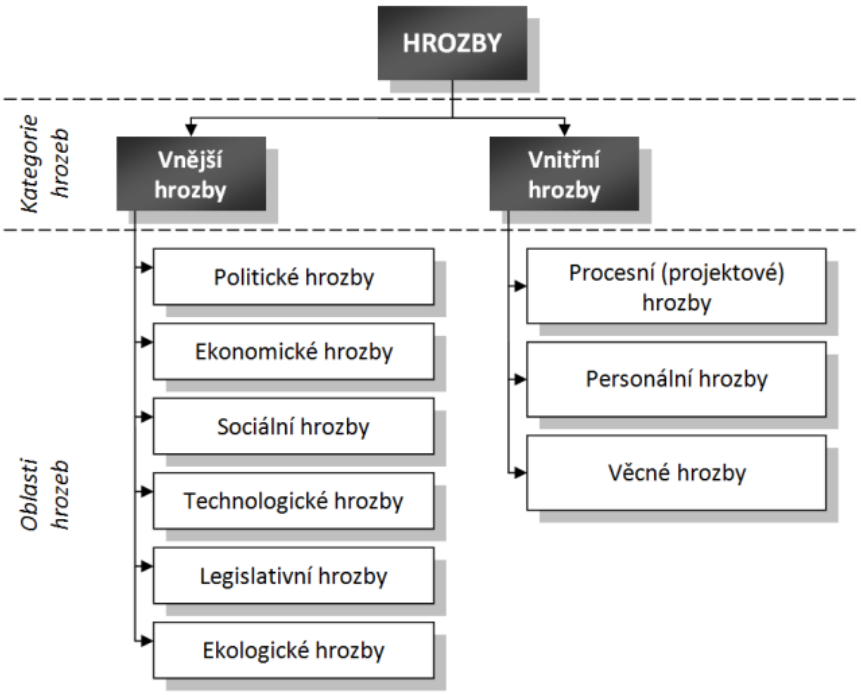


Obrázek 1. Vztah mezi jednotlivými termíny [3]

1.2 Hrozba

Jedná se o lidské nebo přírodní působení, které může způsobit poškození nebo zničení aktiva. Toto působení hrozby na konkrétní aktivum je označováno jako dopad hrozby. Hrozba se posuzuje na základě její nebezpečnosti, přístupu k aktivu a zájmu ovlivnit dané aktivum. Na základě způsobu vlivu se rozlišuje působení záměrné a náhodné. Za záměrné může být považována například kriminalita, jako je žhářství, krádež a podobně. Náhodné

je představováno především přírodními vlivy, které téměř nelze ovlivnit, jako například zemětřesení, silné bouřky a jiné. Hrozby se dále mohou dělit na vnitřní a vnější (viz Obrázek 2). Vnitřní hrozby působí zevnitř subjektu, může se tak jednat například o vlastní zaměstnance. Vnější hrozby mají zdroj mimo daný subjekt a může se tak jednat například o již zmíněné přírodní vlivy. [1] [2] [3]



Obrázek 2. Vnější a vnitřní hrozby [3]

1.3 Zranitelnost

Označuje se tak vlastnost aktiva, kterou může využít hrozba, aby poškodila dané aktivum. Dá se především chápat jakožto určitá citlivost, slabina či náchylnost. Jako příklad si lze uvést, že se jedná o hořlavost papíru; této zranitelnosti tak může využít hrozba ohně, a tak aktivum papír poškodit, či zničit. [1] [2]

1.4 Riziko

Tento pojem je odlišný podle toho, v jakém odvětví se zrovna používá. Není tak jednotná definice, která se užívá ve všech případech. V oblasti bezpečnosti se dá využít definice Ministerstva vnitra České republiky, která říká, že riziko je: *„Možnost, že s určitou pravděpodobností vznikne událost, kterou považujeme z bezpečnostního hlediska za nežádoucí. Riziko je vždy odvoditelné a odvozené z konkrétní hrozby. Míru rizika, tedy pravděpodobnost*

škodlivých následků vyplývajících z hrozby a ze zranitelnosti zájmu, je možno posoudit na základě analýzy rizik, která vychází i z posouzení naší připravenosti hrozbám čelit. Riziko také představuje účinek nejistoty na dosažení cílů nebo pravděpodobnost výskytu nežádoucí události s nežádoucími následky.“ [1]

Konkrétněji se v bezpečnosti riziko označuje jako působení hrozby na aktivum. Pro vyjádření rizika se tak využívá vztahu pravděpodobnosti výskytu hrozby a velikosti jejího dopadu na dané aktivum. [3]

1.5 Bezpečnostní opatření

Jedná se o opatření, které za použití fyzické ostrahy (dále jen FO), režimových opatření a systémů technické ochrany či jiných procesů a postupů snižuje riziko poškození aktiva. Například se tedy jedná o poplachové zabezpečovací a tísňové systémy (dále jen PZTS), mechanické zábranné systémy (dále jen MZS) a elektrické systémy kontroly vstupu (dále jen ESKV). Redukce rizik lze dosáhnout snížením zranitelnosti aktiva, regulací dopadu hrozby, snížením pravděpodobnosti výskytu hrozby či odstraněním příčiny vzniku hrozeb. [3]

1.6 Zbytkové riziko

Nikdy objekt nemůže úplně redukovat všechna rizika. Některá rizika jsou pro objekt příliš malá nebo by jejich regulace byla příliš nákladná. Navíc i po zavedení bezpečnostních opatření vždy zůstává určité nevyřešené či snížené riziko. Tato rizika se považují za zbytková a jsou akceptována subjektem. [1]

1.7 Řízení rizik

Je to nikdy nekončící, stále se opakující proces, u kterého je nutné jej buď pravidelně opakovat, anebo jej provést vždy, když dojde k nežádoucí události či významné změně v rámci subjektu. Cílem je zvládání a minimalizace rizik, čehož snaží dosáhnout pomocí zamezení působení hrozeb nebo zmírnění jejich dopadu. Zaměřuje se jak na známé a existující hrozby, tak i na předpokládané nebo očekávané hrozby. Výstupem je návrh vhodných regulačních opatření, která mají daného cíle dosáhnout. [3]

1.8 Soukromá bezpečnostní služba (dále jen SBS)

Jedná se o pojem, který lze jednoduše popsat jako činnost prováděnou za účelem zisku na základě smlouvy a v souladu se zákony, s cílem zajištění bezpečnosti osob a majetku soukromého subjektu. Mezi zákony, které činnost SBS upravují, se řadí především zákon 89/2012 Sb. občanský zákoník, zákon č. 141/1961 Sb. o trestním řízení soudním a zákon č. 40/2009 Sb. trestní zákoník. SBS vykonává svou činnost pomocí hlídací služby, která zajišťuje bezpečnost převážně fyzickou přítomností pracovníků SBS, která se označuje jako FO, nebo také pomocí technické služby, která je uplatňována především za využití detektorů a kamerových systémů. Dále se využívají také detektivní služby, které mají za cíl zajišťovat zákazníkovi požadované informace. [4]

1.9 Bezpečnostní posouzení

Jedná se o proces, při kterém jsou posuzovány aktiva, budovy a různé působící vlivy. Tyto body jsou analyzovány především z pohledu jejich vlivu na kvalitu zabezpečení. Mezi důležité faktory lze řadit vše, co by mohlo ovlivnit funkčnost bezpečnostního systému. Na základě posouzení se také určuje stupeň zabezpečení, třída prostředí a další aspekty, kterým je nutné podřídit budoucí návrh systému zabezpečení. [5]

1.10 Závěr kapitoly

V první kapitole byly stanoveny základní termíny, které se využívají v bakalářské práci, a vztahy mezi nimi. Jednalo se tak především o termíny jako je aktivum, hrozba, zranitelnost, riziko a jiné.

2 ŘÍZENÍ RIZIK

V této kapitole bude vysvětleno, jak probíhá řízení rizik a jaké má nejdůležitější části. Jedná se tak především o analýzu rizik, hodnocení rizik a následnou regulaci rizik.

Řízení rizik je proces, který je nutné neustále opakovat, případně jej provést kdykoliv, kdy je to nutné. Cílem tohoto procesu je zvládání a minimalizace rizik za použití různých metod pro zamezení působení hrozeb, případně opatření pro snížení dopadu hrozby. [3]

2.1 Analýza rizik

Jedná se o proces, který je naprosto nezbytný pro řízení rizik. Může se jednat o různá rizika působící na lidské zdraví a život, životní prostředí nebo také majetek. V závislosti na tom, na jaký typ rizika se aktuálně analýza zaměřuje, je potřeba využít různých metod a znalostí. Je třeba nejen brát v úvahu technický úhel pohledu, ale také využít další aspekty, jakými je například ekonomický, politický a psychologický stav. Jedná se tak o široký proces, který je vždy potřeba upravit na míru řešeným rizikům a konkrétním případům. [6]

Obsah a rozsah dané analýzy v rámci návrhu zabezpečení je určen v relevantních technických normách. Například v rámci PZTS se jedná o ČSN 50131-7, u kamerových systémů se jedná o ČSN 62674-4. V rámci elektronických systémů kontroly vstupu (dále jen ESKV) se jedná o ČSN 60839-11-2. [5]

2.1.1 Metody analýzy rizik

Při provádění analýzy rizik je nutné si stanovit, co vše se může stát a za jakých okolností. Dále je potřeba si uvědomit, jaké následky na analyzovaná aktiva by takové události měly. Jelikož se jedná o klíčový krok v celém systému řízení rizik, je důležité vybrat vhodnou metodu, kterou lze efektivně pro požadovaný úkon využít. Metody se obecně dělí na metody kvalitativní, kvantitativní a semikvantitativní. [7] [8]

Kvalitativní metody se využívají, když není k dispozici dostatek historických dat. Základem je tedy spoléhání na zkušenosti, úvahy a názory osob, které je provádí. Mělo by se tedy jednat především o odborníky a experty. Často se tak využívají zkušenosti a informace z minulosti k prognóze možných událostí a scénářů, které mohou v budoucnu nastat. Některé metody naopak vytyčují žádoucí stav v budoucnu. U tohoto stavu se zpětně analyzuje, jak by se daného cíle dalo dosáhnout a za použití jakých prostředků. Potenciální nevýhodou

kvalitativních metod je subjektivnost. Každý člověk, který danou metodu zpracuje a vyhodnotí, s velkou pravděpodobností získá odlišná data. [7]

Kvantitativní metody naopak využívají statistickou analýzu dat. Uplatňují se tak různá historická data z různých časových úseků. Ty se dále kombinují s vhodným matematickým modelem. Při použití těchto metod se tak předpokládá, že sledovaný proces udrží svůj vývojový trend i do budoucnosti. [7]

Semikvantitativní metody se dají považovat za kombinaci obou předchozích metod. Pracují se stupnicemi, které jsou kvalitativně vyjádřeny. Tyto stupnice mají ale také číselné vyjádření, které slouží pro více kvantitativní určení míry rizika. Jednotlivé úrovně je nutné rozdělit na rovnoměrné kvantitativní stupně. Ty jsou tedy vyjádřeny jak kvalitativně, tak kvantitativně. Při používání těchto metod, je nutné dobře stanovit používané vzorce, které budou zachovávat vytvořené stupnice. Při nesprávné aplikaci vzorce nebo stupnic může dojít k nevhodnému a zavádějícímu použití metody. Proto je třeba k těmto metodám přistupovat opatrně. [9] [10]

Pro potřeby analýzy rizik v rámci bezpečnosti je využíváno velké množství metod. Tyto metody jsou často různě upravovány tak, aby vyhovovaly konkrétnímu účelu. Běžně se využívají metody, jako jsou například revize bezpečnosti, kontrolní seznam, co se stane když…, analýza příčin a následků, předběžná analýza ohrožení nebo analýza stromu událostí. [8]

2.1.2 Kontrolní seznam

Jedná se o relativně jednoduchou a běžně využívanou metodu analýzy. Je především určena pro zjištění stavu sledovaného procesu a jeho odlišností a nedostatků od požadovaného stavu. Využití této metody není omezeno na konkrétní fázi života procesu a lze ji tedy využít jak při zjištění stavu, tak i pro navrhování a kontrolu. Pokud byl pro daný proces již kontrolní seznam vytvořen, je vhodné využívat stejného seznamu pro lepší relevantnost výsledků. Při tvorbě nového seznamu je nutno vycházet z relevantních norem a jiných předpisů. Dále by měl být tvořen zkušeným týmem. Tímto lze dosáhnout vyšší kvality vytvořeného kontrolního seznamu. Následně je nutné otázky postavit tak, aby se na ně dalo odpovědět buď ano, nebo ne. Odpověď ne by vždy měla být pro objekt špatně. [8]

Tabulka 1. Příklad kontrolního seznamu [Vlastní]

Otázka	ANO	NE	Poznámky
Je kamerový systém funkční?		NE	Staré kamery, časté výpadky
Je zamykací systém dveří funkční?	ANO		
Je zavedena kontrola vstupu?	ANO		Nutno přejít přes recepci

2.1.3 Analýza příčin a následků poruch (FMEA)

Je to metoda, která je složena z příčin poruch a dopadů, které mají nežádoucí vliv na sledovaný proces. Účelem této analýzy je identifikovat jednoduché poruchy, jež mohou způsobit havárii. Umožňuje vytvoření kvalitativního systému možných poruch, které je možné kvantifikovat pro lepší přehlednost. Při vypracovávání této analýzy je vhodné, když analytik své závěry konzultuje s jiným. Tím je dosaženo lepší objektivity. Běžně se vypracovává ve formě tabulky a zahrnuje také jednotlivá doporučení analytika pro zlepšení aktuálního stavu. [8]

2.2 Hodnocení rizik

Jde o fázi řízení rizik, kde jsou identifikovaná rizika hodnocena. Jedná se tak primárně o vyhodnocení potenciální velikosti a významu daného rizika. [3] V některých případech je tato část neúplně, nebo úplně zahrnuta v analýze rizik. Například u FMEA analýzy již dochází k číselnému vyjádření míry rizika. Naopak u kontrolního seznamu dochází pouze k identifikaci potenciálních hrozeb a zranitelností. Nedochází zde k žádnému konkrétnímu hodnocení.

Tato fáze je nutná, jelikož pokus o eliminaci či snížení všech rizik by způsobil nepřiměřeně velké náklady. Je tedy potřeba vybrat rizika, jejichž kombinace různých faktorů je pro daný objekt nebo systém nejdůležitější. Vyhodnocuje se tak například jejich dopad, odhalitelnost nebo frekvence výskytu. Zároveň při vyhodnocování rizik je vhodné brát v úvahu možná opatření, která směřují ke snížení daných rizik. Díky tomu lze odhadnout cenovou efektivitu jednotlivých opatření s ohledem na rizika, která ovlivňují. Při výběru možných opatření je nutno brát v potaz, že náklady s nimi spojené by neměly být vyšší než potenciální ztráta. [3]

Identifikované riziko lze při hodnocení rozdělit do určitých skupin. Především se jedná o kritické, důležité nebo běžné riziko. K rizikům v každé z těchto skupin se pak musí přistupovat

rozdílně. U kritického rizika je nebezpečí tak vysoké, že by mohlo způsobit likvidační následky. Při následku důležitého rizika nedochází k bankrotu, ale vyřešení takového dopadu vyžaduje velké úsilí a finanční náklady. Ve skupině běžného rizika se potenciální škody dají vyřešit či nahradit běžnou činností. [2]

2.3 Regulování rizik

Po identifikaci a následném zhodnocení jednotlivých rizik je potřeba určit, jak bude s těmito riziky nakládáno dál. Jsou dva základní přístupy, kterými jsou redukce a retence rizik. Regulace rizika se dá dosáhnout množstvím různých metod, které cílí buď na snížení příčiny vzniku rizika, nebo na snížení důsledků rizika. [2]

2.3.1 Retence rizika

Jednou z nejčastěji využívaných metod je retence rizik. Jedná se o podstoupení nebo akceptaci daných rizik. Hlavním důvodem častého využívání v praxi je obrovské množství rizik, které na firmu nebo systém působí. Mnohá tato rizika nejsou natolik závažná, aby se musela řešit a jejich redukce by mohla mít nepřiměřené náklady. Zároveň vždy, i po zavedení opatření, zůstává určité zbytkové riziko, které musí být akceptováno. [2]

Obecně retence může být vědomá, nevědomá, dobrovolná nebo nedobrovolná. U vědomé je riziko známo, ale není s ním nijak nakládáno. Při nevědomé retence riziko známo není, a zůstává tak akceptováno bez znalosti jeho existence. V případě dobrovolné se jedná o nejpřijatelnější variantu přístupu, jelikož ostatní možnosti jsou z různých důvodů zamítnuty. Naopak u nedobrovolné se jedná o případy, kdy buď nelze s rizikem jinak nakládat, anebo je riziko nevědomé. [2]

2.3.2 Redukce rizika

Při výběru opatření pro redukci rizika je potřeba brát v úvahu několik kritérií. Opatření musí být účinná, přijatelná, efektivní a včasná. Tím, že je účinná, se rozumí, že musí riziko dostatečně snížit. Přijatelností se rozumí, že opatření je v souladu s právem, etikou a dalšími zásadami. Efektivita je poměr nákladů a potenciálního dopadu. Včasnou se rozumí, že je opatření přijaté dříve, než dojde k naplnění dopadu dané hrozby. Redukci rizik lze dělit podle toho, na jakou část je opatření zaměřeno. Jedná se tak o redukci příčiny vzniku rizika, nebo snížení důsledků rizika. [2]

Při odstraňování nebo redukci příčin vzniku rizika se jedná o metody, které mají působit především preventivně. Jejich hlavním cílem je zamezit vzniku rizika nebo alespoň snížit pravděpodobnost, že k němu dojde. Mezi tyto přístupy patří například bezpečnostní opatření a vyhnutí se riziku. [2]

Metody, které se zaměřují na snížení důsledků, naopak počítají s tím, že riziko nastane, a řeší, jakým způsobem minimalizovat daný dopad. Těmito způsoby lze například řešit rizika, kterým se nelze vyhnout. Především se jedná o diverzifikaci a pojištění. Diverzifikace je velmi běžný způsob pro snižování především podnikatelských rizik. Cílem je rozložení rizika na co možná největší základnu. Typicky se využívá například při investování. Pojištění je chápáno jako nahrazení potenciální velké škody způsobené rizikem za jistou malou ztrátu způsobenou platbou pojistného. [2]

Další důležitou částí je monitoring rizika. Jedná se o kontrolu potenciálních rizik, která je prováděna neustále a opakovaně. Cílem je zachytit případné změny stavu a předcházet nenadálým událostem. Kontroluje se tedy především případná změna míry rizika, případně výskyt nového rizika. [1]

2.4 Závěr kapitoly

V této druhé kapitole byly popsány základy řízení rizik a především jeho jednotlivé fáze. Nejdříve byla popsána analýza rizik a některé z jejich metod. Zvláště byly vypsány metody, které jsou následně využity v praktické části. Dále byly rozebrány fáze hodnocení rizik a jaká kritéria je v této fázi nutné brát v potaz. Na závěr bylo zmíněno regulování rizik a byly také popsány základní přístupy a metody nakládání s rizikem.

II. PRAKTICKÁ ČÁST

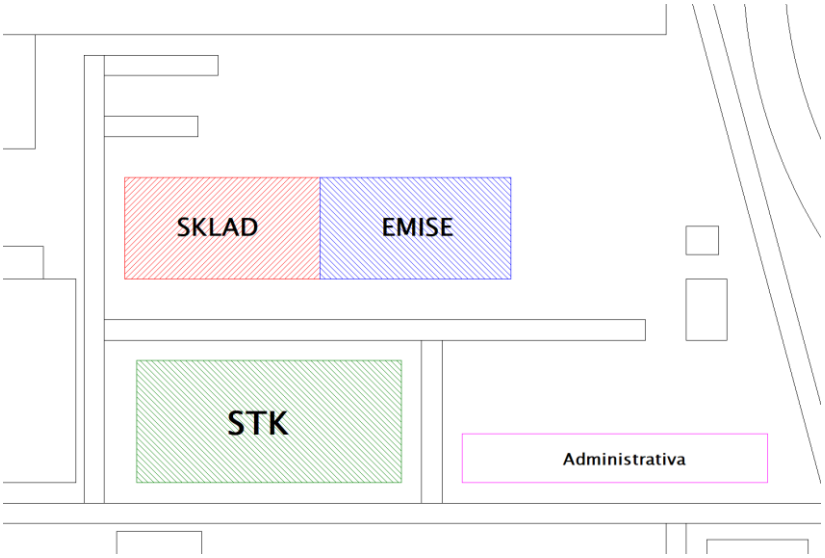
3 CHARAKTERISTIKA OBJEKTU

Tato kapitola má za cíl popsat areál objektu a jeho jednotlivé budovy a také zmínit rozdělení prostor jednotlivých budov a jejich přístupnost veřejnosti. Dále má za cíl určit úroveň kriminality v okolí objektu a přiblížit bezpečnostní incidenty, které se udály v minulosti. Poté bude popsáno množství zákazníků, kteří se v areálu normálně pohybují. Následně budou vypsány nejdůležitější aktiva, kterými se bude práce zabývat.

Pro potřeby této práce byl objekt anonymizován z důvodu povahy některých zkoumaných informací. Při vypracovávání jsme vycházeli z informací a podkladů, které byly k tomuto účelu poskytnuty.

3.1 Popis objektu

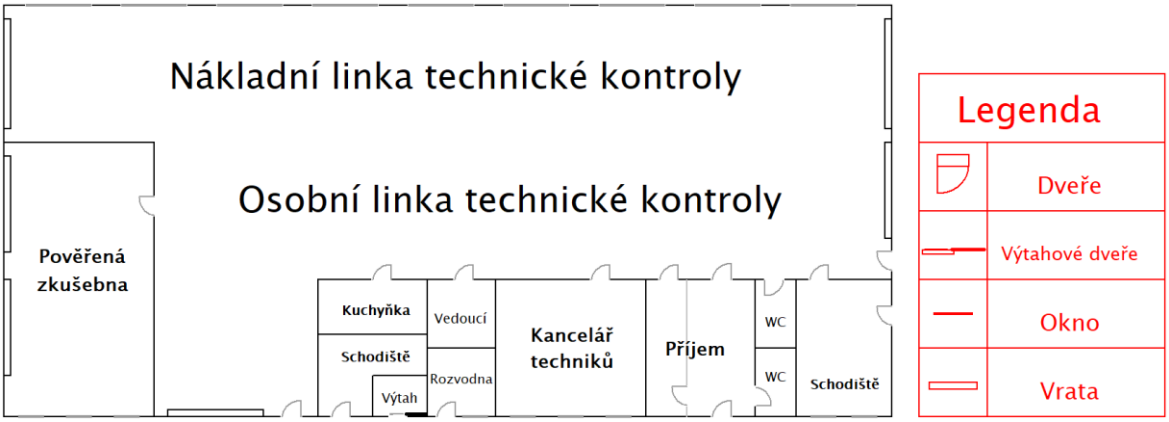
Pro bakalářskou práci byl vybrán areál stanice technické kontroly (dále jen STK), který se skládá ze tří budov. Jedná se o hlavní budovu STK, následně vedlejší stanici emisní kontroly a skladu a také budovu administrativy. Pro účely parkování jsou vymezena místa okolo hlavní budovy a vedle stanice emisní kontroly. Kolem areálu se nachází další budovy jak pro průmyslové užití, tak pro jiné účely. Nejedná se tedy o striktně uzavřený pozemek. Areál má jednoho hlavního vedoucího STK a svého zástupce. Následně pracoviště emisní kontroly má dva vedoucí, každý z nich má na zodpovědnost jednu pracovní linku v budově.



Obrázek 3. Rozložení areálu [vlastní]

3.1.1 Stanice technické kontroly

Hlavní budova je tedy samotné STK. Tato dvoupatrová stavba má dvě pracovní linky, jednu pro osobní automobily a druhou pro nákladní vozidla. V přízemí jsou kanceláře techniků, příjem a kancelář vedoucího. Dále se zde nachází malé zkušební emisní pracoviště s kapacitou dvou osobních automobilů. Jsou zde situovány i toalety a místnost s elektrickými rozvody. V prvním patře jsou umístěny pouze šatny, prostory pro zaměstnance a zároveň archív. Ke vstupu do druhého patra slouží schodiště umístěné u nouzového východu. Dále se pro přesun do druhého patra dá využít druhé schodiště nebo nákladní výtah. Tyto dva přístupy jsou dostupné z venkovní strany budovy, v běžném stavu jsou ale uzamčeny a nepřístupny. Pouze místnost příjmu a toalety jsou volně přístupné zákazníkům. Zbytek prostor je s omezeným pohybem osob a zákazníci se zde mohou pohybovat pouze se svolením a s doprovodem zaměstnanců. V budově a jejím okolí se obvykle nachází poměrně velké množství lidí. Je běžné, že technici při prohlídce automobilů či jiných vozidel mají zákazníky s sebou na kontrolní lince.

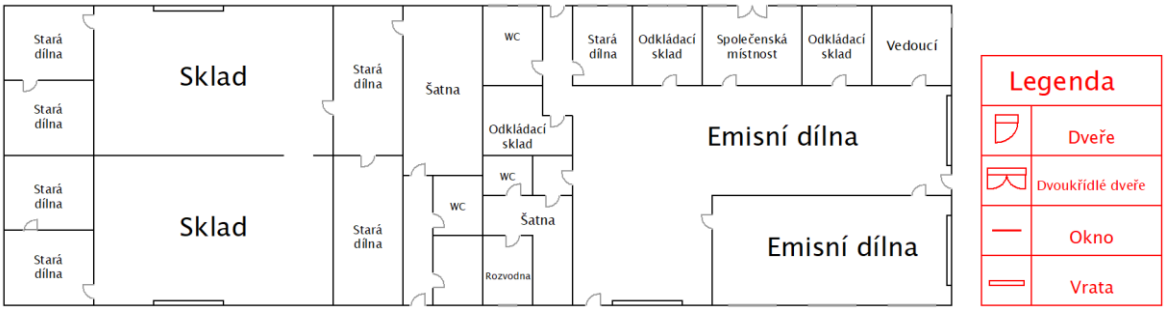


Obrázek 4. Rozložení přízemí budovy STK [vlastní]

3.1.2 Budova emisí a skladu

Vedlejší jednopatrová budova je rozdělena na dvě části, jedna je určena pro potřeby stanice emisní kontroly a druhá část je vyhrazena jako skladovací prostor. Tyto dvě části mají společnou stěnu, ta však není průchozí. Sektor určený pro měření emisí se skládá ze dvou pracovních ploch, jedna má vlastní místnost a pracovní prostor, druhá se nachází v hlavní hale budovy a zabírá pouze třetinu celkového místa v hlavních prostorách. Dále se zde nachází kancelář vedoucího a společenská místnost. V zadní části budovy je umístěna také šatna pro pracovníky, stará dílna a malý sklad. Celá budova má omezený pohyb osob, tedy běžně se uvnitř nezdržují žádní zákazníci ani jiné osoby vyjma pracovníků.

Druhá část budovy se skládá ze dvou hlavních skladních hal. Každá tato plocha má dvě malé dílny v zadní oblasti budovy. Dále se v budově nachází šatna, toalety a další dvě menší dílny. Většina dílen v budově je určena také pro skladní účely.



Obrázek 5. Rozložení budovy emisní kontroly [vlastní]

3.1.3 Budova administrativy

Jedná se o podlouhlou jednopatrovou stavbu. Uvnitř se nachází velké množství volných místností a bývalých kanceláří, je zde také umístěn sekretariát. Tato budova není veřejnosti přístupná. Využívá se pouze zaměstnanci jako jídelna, kromě toho se prostory již téměř nevyužívají. Nenachází se zde téměř žádná hodnotná aktiva. Význam budovy je pro stanici také velmi malý, jelikož je snaha budovu vyklidit a buď rekonstruovat a využívat pro jiné účely, nebo ji zbourat. Z těchto důvodů se po fyzické prohlídce a konzultaci jak s vedoucím práce, tak i vedoucím STK rozhodlo, že budova nebude nijak podrobně zpracovávána.

3.2 Kriminalita

Aby bylo možné co nejpřesněji posoudit výskyt různých hrozeb v analýze rizik, je vhodné si udělat představu o kriminalitě v okolí objektu. Za využití dostupných dat byla zpracována statistika kriminality v oblasti dané mapou kriminality. Byla vybrána nejmenší možná zóna, která obsahovala posuzovaný objekt. Pro tyto potřeby byla vybrána data z období od 1. 1. 2022 do 1. 1. 2023. Dále byly ze statistiky odebrány přestupky na úseku BESIP a silničního hospodářství, které nemají pro objekt relevanci. Za tento časový úsek bylo zaznamenáno dohromady 65 přestupků a 23 trestných činů. Z těchto čísel se u dvou přestupků a dvou trestných činů určilo, že se nestaly. U jednoho trestného činu bylo stanoveno, že se nejedná o trestný čin. Takto uzavřené přestupky a trestné činy tedy nebyly zahrnuty do tabulky. [11]

Tabulka 2. Kriminalita v okolí objektu [11]

Přestupky proti majetku	32
Přestupky proti veřejnému pořádku/ občanskému soužití	21
Přestupek ze zákona o pobytu cizinců	6
Přestupky na úseku ochrany před alkoholismem a toxikomanií	2
Ostatní přestupky	2
Trestné činy související s toxikomanií	5
Podvody	4
Jiné majetkové trestné činy	3
Krádeže	2
Krádeže vloupáním byt	2
Krádeže vloupáním prodejna	1
Krádež jiný objekt	1
Úmyslné ublížení na zdraví	1
Násilná loupež	1
Celkem	83

U přestupků byly nejčastější přestupky proti majetku. Těmi se rozumí především drobné krádeže a poškození majetku. V četnosti dále následovaly přestupky proti veřejnému pořádku a občanskému soužití. Toto jsou velmi obecné přestupky, u kterých se může jednat o lehké ublížení na zdraví, ale i o znevažování úřední osoby nebo rušení nočního klidu. Dále se jednalo o přestupky ze zákona o pobytu cizinců nebo přestupky na úseku ochrany před alkoholismem a toxikomanií. [11] [12]

V případě trestných činů byly nejčastější trestné činy související s toxikomanií. Následoval trestný čin podvodu a poté jiné majetkové trestné činy. Důležitým bodem byly také trestné činy krádeže. Ty se pro přehlednost rozdělily do daných podkategorií. Nakonec v úseku došlo i ke dvěma násilným trestným činům, z nichž u jednoho se jednalo o úmyslné ublížení na zdraví a u druhého šlo o násilnou loupež. [11]

Za dané období a při zkoumané lokalitě se nevyskytovalo nezvyklé množství trestných činů. Když však vezmeme v potaz, že byla analyzována pouze data z jednoho roku a nejmenší relevantní oblasti, je tak zřejmé, že hrozba krádeže nebo jiné násilné činnosti je reálná. Možnost, že tyto hrozby nastanou, není nijak vysoká. Je však potřeba tyto hrozby brát vážně.

3.3 Návštěvnost

Pro představu, jaké množství lidí se v průběhu týdne v objektu vyskytuje, je potřeba určit návštěvnost. Tato informace by mohla být užitečná, jelikož v časech, kdy je vysoký výskyt

lidí, je pravděpodobnější, že se mohou udát neočekávané incidenty. Podle zaměstnanců se na stanici pohybuje přibližně 130 až 200 zákazníků denně. Obrázky určující návštěvnost nezobrazují přesný počet osob, slouží pouze k ilustraci rozložení pohybu osob v průběhu dne.

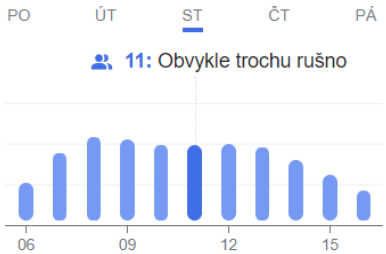
Pondělí a středa má pracovní dobu od 6:30 do 17 hodin. V úterý a ve čtvrtek je pracovní doba od 6:30 do 16 hodin a v pátek je pracovní doba pouze od 6:30 do 12 hodin.

Obrázek 6. Návštěvnost – pondělí [13]

Pondělí je velmi vytíženým dnem. Největší množství zákazníků se zde vyskytuje kolem 8 a 9 hodiny ranní. Jedná se za celý den přibližně o 180 zákazníků.

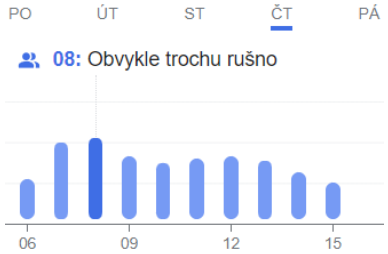
Obrázek 7. Návštěvnost – úterý [13]

Úterý je o poznání klidnějším dnem. Opět se zde pohybuje nejvíce zákazníků kolem 8 a 9 hodiny ranní. Nicméně zbytek dne je relativně klidným. Během dne se zde vyskytne přibližně 140 zákazníků.



Obrázek 8. Návštěvnost – středa [13]

Středa je dnem, kdy dochází k průměrnému vytížení. Lze si povšimnout, že je zde návštěvnost rozložena přes celý tento den. Jedná se o druhý nejvytíženější den s celkovým počtem zákazníků kolem 170.



Obrázek 9. Návštěvnost – čtvrtek [13]

Čtvrtek je poměrně klidným dnem. Můžeme zde vidět, že je návštěvnost největší kolem 7 a 8 hodiny ranní. V průběhu dne se zde vyskytne přibližně 150 zákazníků.

Obrázek 10. Návštěvnost – pátek [13]

Pátek je nejkratší pracovní den pro tento objekt. Můžeme pozorovat vytížení kolem 8 a 9 hodiny ranní. Kromě těchto časů je zde poměrně klid. V tento den se vystřídá asi 80 zákazníků.

Z vyplývajících dat je zřejmé, že nejvytíženějším dnem je pondělí a hned poté středa. V tyto dny lze tedy předpokládat nejvyšší výskyt osob v objektu. Zároveň lze vypozorovat, že nejvytíženějšími hodinami jsou 8 a 9 hodina ranní. Naopak za nejklidnější den lze považovat pátek.

3.4 Identifikace aktiv

V této podkapitole budou stručně popsána aktiva, která se vyskytují v objektu a mohou tak být ovlivněna působením hrozeb. Jedná se nejdříve o samotné zaměstnance a zákazníky, ti budou pro potřeby práce bráni v potaz pouze z pohledu napadení nebo jiného způsobu ublížení na zdraví, nikoliv z pohledu úrazů či jiných pracovních nehod. Dále zde spadají hmotná aktiva, jako jsou samotné budovy nebo vybavení objektu. Následně je potřeba brát v úvahu i potenciální ušlý zisk v případě, že se zastaví nebo omezí chod objektu. Mezi další aktiva patří například i data, se kterými organizace pracuje.

Písemná dokumentace – je aktivum, kterým se rozumí především různé papírové protokoly, které se vypracovávají v průběhu zkoušky a těsně po ní. Tato dokumentace sama o sobě

nemá příliš vysokou peněžní hodnotu. Obsahuje však osobní informace zákazníků, které by se neměly dostat do neoprávněných rukou.

Data – jedná se o všechny elektronické informace, se kterými stanice pracuje, které zpracovává a následně odesílá na Ministerstvo dopravy. Jejich hodnota je tak především v obsahu daných dat a v důležitosti jejich přístupnosti a bezpečnosti.

Zaměstnanci a zákazníci – jsou osoby pohybující se buď přímo v daném objektu, nebo v jeho přímé blízkosti. Ohrožení na zdraví těchto osob může mít pro objekt závažné důsledky. Jedná se také o riziko ztráty zaměstnance, kdy objekt musí vynaložit finanční prostředky pro nábor a proškolení nového člena.

Budova – v případě zkoumaného objektu se jedná o tři oddělené budovy. Budova STK je pro funkčnost objektu naprosto zásadní, a je tedy nejhodnotnějším aktivem. Samotná hodnota budovy je přibližně 7,2 milionů Kč. [14] V této částce ale není započítána hodnota újmy, kterou by její ztráta způsobila. Dá se tedy určit, že hodnota této budovy může být pro podnik likvidační. Budova emisní kontroly je také podstatnou součástí fungování tohoto objektu. Hodnota této budovy je vyčíslena přibližně na 1,8 milionů Kč. [14] V této částce opět není brán v potaz ušlý zisk, který by byl způsobený její ztrátou. V tomto případě by následek nebyl pro podnik likvidační, ale stále by se jednalo o podstatnou finanční ztrátu a ušlý zisk.

IT technika – jedná se o všechny počítače a jinou výpočetní techniku a příslušenství důležité pro chod objektu. Celková hodnota tohoto vybavení se pohybuje kolem 400 tisíc Kč. Je však nutné podotknout, že velké množství tohoto vybavení je již starší, a tak celková částka bude v realitě podstatně nižší. [14]

Technika – mezi tato aktiva spadá především technické vybavení objektu určené pro provádění technických zkoušek. Tato aktiva mají přibližnou hodnotu 5,5 milionů Kč. [14] Důležité je ale zmínit, že jsou pro funkčnost objektu naprosto nezbytné, takže je nutné počítat také s potenciálním ušlým ziskem při jejich ztrátě a poškození.

Hotovost – jedná se především o zisk objektu. Týdně je zisk v hotovosti odhadován na zhruba 700 tisíc Kč. Tato částka se však podstatně mění dle jednotlivých měsíců a jiných faktorů, které ovlivňují množství zákazníků. Mezi důležité faktory spadá také stále častější platba kartou.

Kontrolní nálepky – jde o ceninu, se kterou objekt nakládá. Hodnota samotných nálepek je zanedbatelná i přes velké množství, které se v objektu nachází.

Automobily – firma má dle inventury dvě vozidla, které se mohou nacházet u objektu. Tyto automobily mají přibližnou hodnotu 800 tisíc Kč. Je ale nutné si uvědomit, že se jedná o ceny z roku 2013 a 2018. [14] Tím pádem aktuální cena bude podstatně nižší. Zároveň se v objektu běžně vyskytují vozidla zaměstnanců a zákazníků. A to v některých případech i přes noční hodiny.

Osobní věci – do těchto aktiv spadá především majetek zaměstnanců. Většinou se jedná o oblečení, drobnou elektroniku, hotovost a případně šperky. Hodnota těchto předmětů je pro objekt zanedbatelná.

Ostatní majetek – v této skupině aktiv se vyskytují především malé přenosné přístroje, firemní telefony a další vybavení prostor. Hodnota těchto aktiv je přibližně 250 tisíc Kč. Opět je nutné upozornit, že se často jedná o starší zařízení, jejichž hodnota je aktuálně podstatně nižší. [14]

Dodávky elektřiny a vody, přívod topení a internetu – dodávky elektřiny a přívod internetu jsou pro chod objektu zásadní nutností. Proto při přerušení těchto služeb dochází k vysokému ušlému zisku. Dodávky vody a přívod topení nejsou pro objekt takto zásadní. Každopádně mohou ovlivňovat kvalitu poskytovaných služeb, a tím také působit na zisk.

Reputace – jedná se o nehmotné aktivum. Jde o důležitý faktor z pohledu úspěchu a růstu firmy. Tato stanice má obecně dobrou reputaci a její udržení je v jejím zájmu.

Závěrem lze říci, že v objektu se vyskytuje velká rozmanitost aktiv, která je nutno chránit. Ovlivnění všech zmíněných aktiv způsobuje finanční ztrátu objektu, ať už přímou nebo nepřímou, případně formou ušlého zisku. Patří zde tedy relativně snadno vyčíslitelná aktiva jako například budova a vybavení. Ale také ty, jejichž finanční hodnota je nejednoznačná a ne zcela předvídatelná. Ve vyšším odhadu se u vyčíslitelných aktiv jedná o hodnotu přibližně 16,6 milionů Kč.

4 ANALÝZA SOUČASNÉHO STAVU ZABEZEPČENÍ

V této kapitole je uvedena analýza současného stavu zabezpečení, která byla provedena pomocí připraveného kontrolního seznamu a fyzické obhlídky objektu. Kontrolní seznam byl pro přehlednost rozdělen na dvě části, jedna pro každou zkoumanou budovu. Zjištěné závěry jsou popsány v podkapitolách níže. Po domluvě s provozovatelem není řešena požární ochrana a bezpečnost a ochrana zdraví při práci. Proto se analýza zaměřuje především na prvky PZTS a MZS, zmiňují se tady ale i další nedostatky, které je vhodné mít na paměti pro případné budoucí použití.

4.1 Kontrolní seznam

Zde je k nahlédnutí využívaný kontrolní seznam. Každý objekt byl pro přehlednost rozdělen podle úrovně ochranných opatření na ochranu perimetrickou/plášťovou, prostorovou, režimové opatření a fyzickou ostrahu. Předmětová ochrana není samostatně řešena, jelikož byla zahrnuta v režimových opatřeních z důvodu nízkého využívání.

Tabulka 3. Kontrolní seznam pro STK [vlastní]

STK			
Perimetr – plášť	**ANO**	**NE**	**Poznámky**
Jsou z venkovní strany nouzové východy uzamčeny?		NE	Ne všechny
Je zavedena kontrola vstupu?	ANO		Potřeba projít přes příjem
Jsou z venkovní strany okna uzamčena?	ANO		Okna ve špatném stavu
Je vstup na střechu nepřístupný?		NE	Žebřík z venkovní strany
Jsou zabezpečeny střešní vstupy?		NE	
Jsou zabezpečeny ventilace/průduchy?	ANO		
Jsou zabezpečeny hlavní vstupy?	ANO		PIR detektory (kromě příjmu) + IR brány

Jsou zabezpečeny skleněné výplně?	ANO		PIR detektory + IR brány
Je perimetr oplocen?		NE	Nelze (nachází se zde další budovy)
Prostor	**ANO**	**NE**	**Poznámky**
Jsou monitorovány hlavní prostory?		NE	
Má objekt prostory pouze pro zaměstnance?	ANO		
Je zabezpečen přechod mezi veřejnými a omezenými prostory?	ANO		Ale z linky se už dá dostat kamkoliv
Jsou zabezpečeny prostory pro zaměstnance?	ANO		Možnost zamčení dveří + PIR detektory
Jsou kamerami monitorovány prostory pro zaměstnance?		NE	
Režim	**ANO**	**NE**	**Poznámky**
Jsou v objektu nastavena režimová opatření?	ANO		
Jsou zaměstnanci objektu rozeznatelní?	ANO		
Je nastavena otevírací doba?	ANO		
Je ústředna PZTS vhodně umístěna?	ANO		
Existuje směrnice pro zadržení narušitele?		NE	
Je v objektu zakázáno kouření?	ANO		
Je hotovost v trezoru v době mimo pracovní dobu?	ANO		
Je hotovost ukládána na bezpečné místo v průběhu dne?	ANO		

Jsou vždy pod dozorem doklady od automobilů?	ANO		
Je zavedena klíčová služba?	ANO		Klíče u vedoucího STK
Fyzická ostraha	**ANO**	**NE**	**Poznámky**
Je objekt napojen na SBS?	ANO		Pomocí dohledového přijímacího a poplachového centra
Probíhá přes den fyzická kontrola pracovníkem FO?		NE	
Probíhá přes den monitoring kamerového systému a stavu zabezpečení?	ANO		Monitoring ano, zabezpečení kromě kamer je přes den vypnuto
Probíhá přes noc fyzická kontrola pracovníkem?		NE	
Probíhá přes noc monitoring kamerového systému a stavu zabezpečení?		NE	SBS nemá vzdálený přístup ke kamerám
Existuje napojení na výjezdovou skupinu SBS?	ANO		
Dochází ke sledování kamer přímo v objektu?	ANO		Napojení kamer na SBS nefunkční!
Probíhá kontrola objektu před zastřežením zaměstnancem STK?	ANO		

Tabulka 4. Kontrolní seznam pro stanici emisní kontroly [vlastní]

Stanice emisní kontroly			
Perimetr – plášť	**ANO**	**NE**	**Poznámky**
Jsou z venkovní strany nouzové východy uzamčeny?		NE	

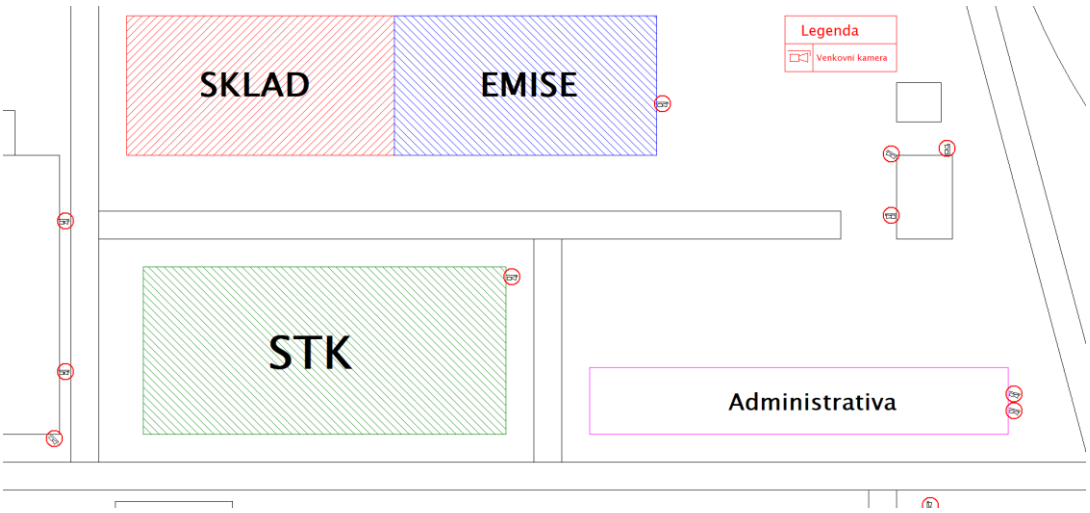
Je zavedena kontrola vstupu?		NE	
Jsou z venkovní strany okna uzamčena?	ANO		
Je vstup na střechu nepřístupný?	ANO		
Jsou zabezpečeny střešní vstupy?	ANO		
Jsou zabezpečeny ventilace/průduchy?	ANO		
Jsou zabezpečeny hlavní vstupy?	ANO		PIR detektory
Jsou zabezpečeny skleněné výplně?	ANO		PIR detektory + IR brány (ne všechny)
Je perimetr oplocen?		NE	Nelze (nachází se zde další budovy)
Prostor	**ANO**	**NE**	**Poznámky**
Jsou monitorovány hlavní prostory?		NE	Kamery nefunkční
Má objekt prostory pouze pro zaměstnance?	ANO		
Je zabezpečen přechod mezi veřejnými a omezenými prostory?		NE	V prostorách emisí a skladu se kromě zaměstnanců téměř nikdo nepohybuje
Jsou zabezpečeny prostory pro zaměstnance?	ANO		IR brána
Jsou kamerami monitorovány prostory pro zaměstnance?		NE	
Režim	**ANO**	**NE**	**Poznámky**
Jsou v objektu nastavena režimová opatření?	ANO		
Jsou zaměstnanci objektu rozeznatelní?	ANO		

Je nastavena otevírací doba?	ANO		
Je ústředna PZTS vhodně umístěna?	ANO		
Existuje směrnice pro zadržení narušitele?		NE	
Je hotovost v trezoru v době mimo pracovní dobu?	ANO		
Je hotovost ukládána na bezpečné místo v průběhu dne?		NE	Hotovost volně ležící na stolech
Jsou vždy pod dozorem doklady od automobilů?		NE	Volně ležící na stole
Je zavedena klíčová služba?	ANO		Klíče u vedoucího stanice
Fyzická ostraha	**ANO**	**NE**	**Poznámky**
Je objekt napojen na SBS?	ANO		Pomocí dohledového příjímacího a poplachového centra
Probíhá přes den fyzická kontrola pracovníkem FO?		NE	
Probíhá přes den monitoring kamerového systému a stavu zabezpečení?	ANO		Monitoring ano, zabezpečení kromě kamer je přes den vypnuto
Probíhá přes noc fyzická kontrola pracovníkem?		NE	
Probíhá přes noc monitoring kamerového systému a stavu zabezpečení?		NE	SBS nemá vzdálený přístup ke kamerám
Existuje napojení na výjezdovou skupinu SBS?	ANO		

Dochází ke sledování kamer přímo v objektu?	ANO		Napojení kamer na SBS nefunkční!
Probíhá kontrola objektu před zastřežením zaměstnancem STK?	ANO		

4.2 Areál objektu

Okolí budov je monitorováno kamerovým systémem, k těmto kamerám má přístup sekretářka a někteří další zaměstnanci hlavně z důvodu přehlednosti o množství čekajících zákazníků. Napojení kamerového systému na SBS je již několik měsíců zcela nefunkční, takže v noci jsou kamery nepřístupné. Kamerový systém poskytuje možnost záznamu. V době naší přítomnosti fungovalo však jen 7 z 10 kamer a bylo nám sděleno, že to je zcela normální a že nefunkční kamery se „střídají“. Oplocení se zde téměř nevyskytuje, a je tak irelevantní.



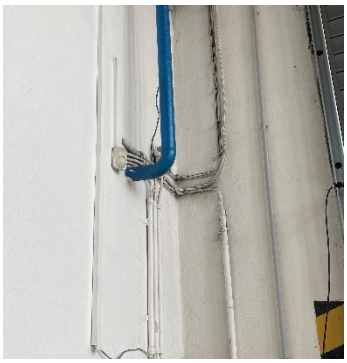
Obrázek 11. Rozmístění venkovních kamer v areálu [vlastní]

4.3 Budova STK

Budova je z venkovních dvou stran zabezpečena IR bariérami a je ze všech stran pod dohledem venkovních kamer. Jedná se o strany, kde jsou kanceláře a příjem a z druhé strany prosklená část linky. Vjezd na linku a nouzový východ z venkovní strany je vidět kamerou. Výjezd z nákladní linky, vjezd do prostoru malé emisní dílny a také žebřík vedoucí na střechu není z venkovní strany nijak zabezpečen (viz Obrázek 12), je pouze pod dohledem kamer.

Obrázek 12. Žebřík vedoucí na střechu [vlastní]

Ve vnitřních prostorách budovy jsou v pracovní ploše linky rozmístěny tři PIR detektory, dva u výjezdu z linek a jeden u vjezdu na linky. Tyto detektory zároveň pokrývají prosklenou část linky.



Obrázek 14. PIR detektor u výjezdu nákladní linky [vlastní]

Obrázek 13. PIR detektor u vjezdu na linky [vlastní]

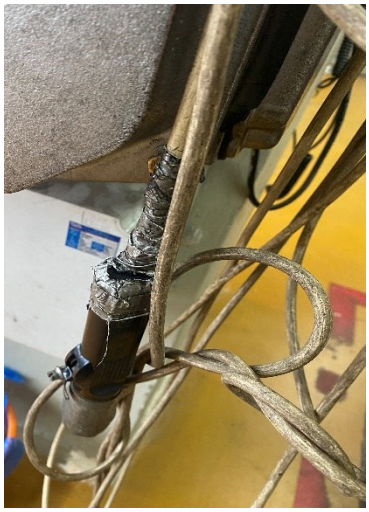
Následně je další PIR detektor umístěn v příjmové části, tento pokrývá pracovní plochu příjmu a okna, nepokrývá však vstup do čekárny před příjmem. Další PIR detektor se nachází u nouzového východu ze strany vjezdu na linky, který pokrývá zároveň i schodiště do druhého patra. Tento nouzový východ zároveň slouží jako vchod pro zaměstnance a nachází se u něj klávesnice pro zastřežení a odstřežení budovy. Dílna malé emisní zkušebny je zabezpečena využitím dvou PIR detektorů, které pokrývají celou dílnu. Ani místnost kanceláře techniků, ani místnost elektrické rozvodny či vstupy na druhé schodiště a výtah nejsou nijak zabezpečeny, a spoléhají se tak na IR bránu z venkovní strany. Druhé patro také nemá žádné bezpečnostní prvky.

Obrázek 15. IR bariéra vně STK [vlastní]

Okna jsou v relativně špatném stavu, nejdou však z venkovní strany otevřít. Nouzové východy jsou jednak již zmíněné prosklené dveře u schodiště, jednak jsou u výjezdu z osobní linky. Nouzové východy se nedají z venkovní strany otevřít, ale jelikož je zakázáno na lince kouřit, může být problematické využívání těchto dveří kuřáky, kteří je občas nechají pootevřené. Ventilační systém se nedá využít pro vniknutí do budovy.

Prostory jsou situovány tak, že zákazníci se z čekárny na linku dostanou pouze se svolením a za přítomnosti některého ze zaměstnanců. Na lince se však pohybuje množství zákazníků, kteří se více či méně účastní testování jejich vozidel, někdy pouze postávají bokem. Prostory pouze pro zaměstnance jsou tak označeny, většinou jsou však z linky volně přístupné. Nejsou tak samy nijak zabezpečeny, kromě možnosti zamčení dveří, tato možnost se však využívá pouze u některých místností, a to pouze v určitou dobu. V kanceláři vedoucího se nachází trezor. Kancelář vedoucího nemá okna a není nijak speciálně zabezpečena. Přístup do prostor pro zaměstnance včetně kanceláří je tak omezen primárně samotným přístupem na linku.

Linky, prostory kanceláří ani jiné prostory pro zaměstnance nejsou monitorovány kamerovým systémem, všechny kamery na lince jsou určeny pouze k funkčnosti STK. Dále se nachází ve vnitřních prostorách staré, již nefunkční kamery, které mohou sloužit jako atrapy. V budově se nenachází žádný požární hlásič, ať už hlásič kouře nebo plamene, a to ani v kuchyňce pro zaměstnance. Následně je porušená izolace některé volně přístupné kabeláže, která obecně není v nejlepším stavu.

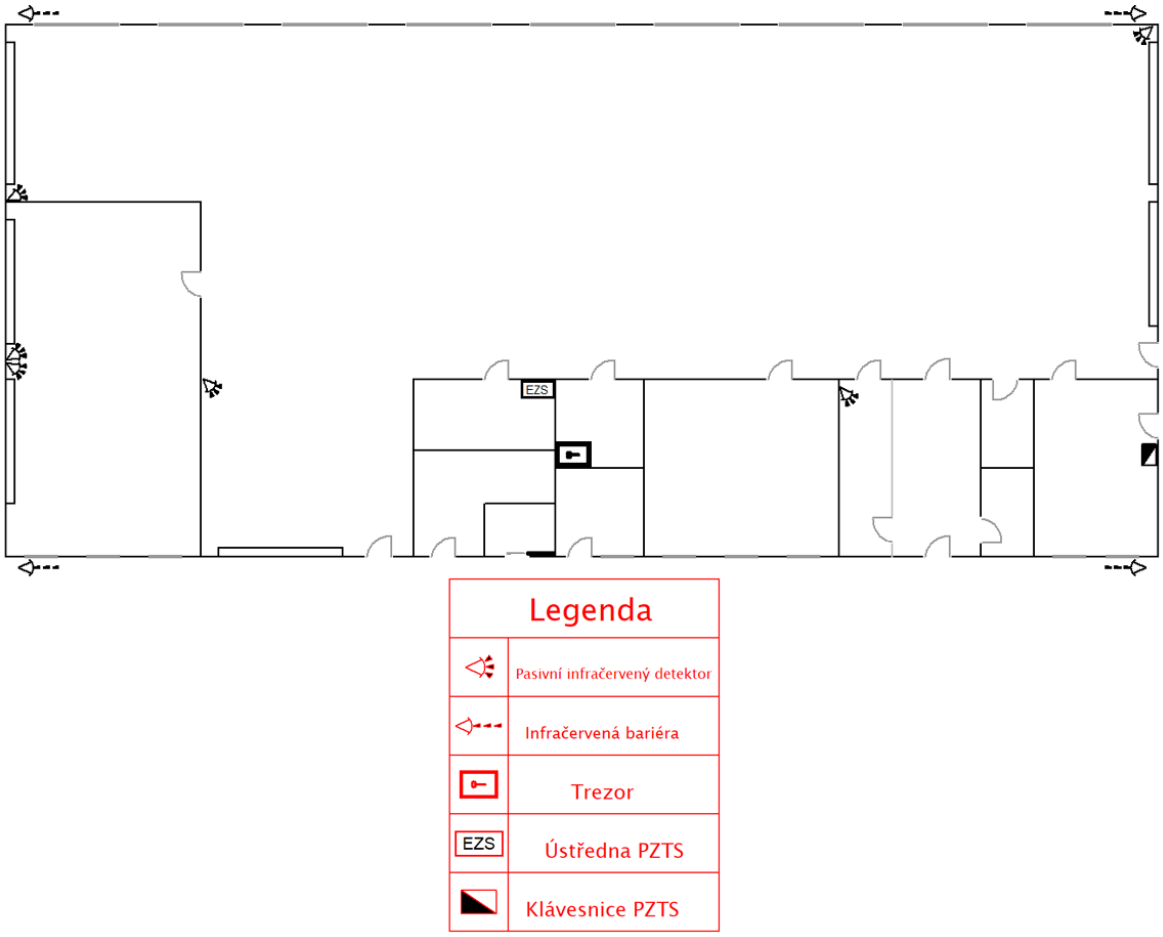


Obrázek 16. Porušená izolace kabeláže [vlastní]

Režim objektu je nastaven tak, že klíče ke všemu má pouze vedoucí a jeho zástupce. Ostatní mají klíče pouze od vchodu pro zaměstnance. V objektu je také zakázáno kouřit. Zaměstnanci nosí pracovní oblečení, díky kterému jsou jednoznačně rozeznatelní od zákazníků. Označení nouzových východů je přítomno přímo na dveřích, ale nesměřuje k nim žádný ukazatel. Jelikož se STK zodpovídá Ministerstvu dopravy, musí budova splňovat příslušné normy z pohledu detektorů plynu, množství a rozmístění hasících přístrojů a dalších povinných ochran v tomto typu objektu. Tyto normy splňuje, ale nachází se zde několik rizikových pochybení. Budova nemá evakuační plán ani zpracovanou dokumentaci k požární bezpečnosti a pokud ano, tak ji žádný ze zaměstnanců nezná a neví, kde se nachází. Proto tedy zaměstnanci neznají shromaždiště budovy ani jiné postupy při požáru této konkrétní budovy. Zaměstnanci podstupují povinné školení v rámci obecné požární ochrany. Budova má otevírací dobu nastavenou tak, že pracovní dny jsou pondělí až pátek. Ústředna PZTS budovy STK je umístěná v kuchyňce, která je přístupná z linky, a je zabezpečena proti neoprávněnému otevření. V případě agresivního či násilného zákazníka si zaměstnanci musejí poradit sami svépomocí, žádná vnitřní směrnice pro tento případ není zavedena.

Obrázek 17. Ústředna budovy STK [vlastní]

Monitoring budovy probíhá pouze v budově, a to z důvodu přehledu o množství zákazníků. Kamerový systém tak nikdo aktivně nesleduje a využívá se až následná možnost záznamu. V nočních hodinách nebo přes víkend ke kamerám nemá nikdo přístup. Dříve byly kamery napojeny na SBS zabezpečující tento objekt, toto propojení však již několik měsíců nefunguje. Aktuální stav bezpečnostních prvků není pravidelně kontrolován. V případě vzniku poplachu v budově je upozorněna SBS, která nejdříve kontaktuje vedoucího, jestli se nejedná o planý poplach. Pokud tomu tak není, následně vysílá na místo pracovníky fyzické ostrahy na kontrolu objektu.



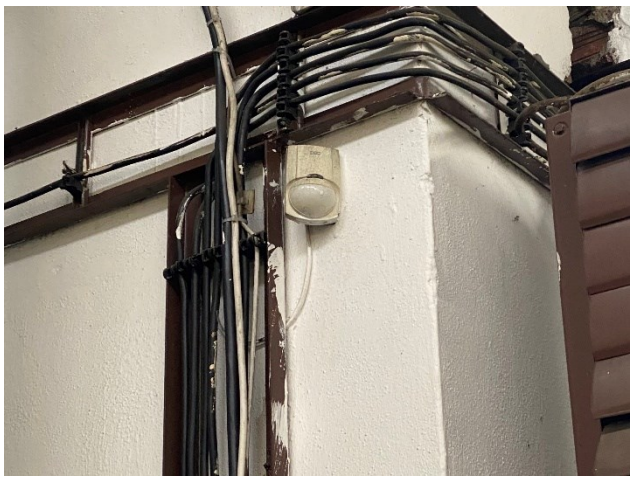
Obrázek 18. Rozmístění bezpečnostních prvků budovy STK [vlastní]

4.4 Budova emisní kontroly a skladu

Budova je z jedné strany zabezpečena IR bariérou, jedná se o stranu blíže k budově STK s bočním vstupem, zbytek budovy je pouze v zorném poli venkovních kamer. Kamery však nemají zorné pole na stranu budovy, která se nachází nejdál od budovy STK.

Obrázek 19. IR bariéra vně budovy emisní kontroly [vlastní]

Vjezd na stanici a vstupy do budovy jsou zabezpečeny PIR detektory rozmístěnými ve vnitřních prostorách. Dva PIR detektory jsou umístěny u vjezdů na stanici, které pokrývají hlavní vstupy a vjezdy společně s prostory obou pracovních ploch.



Obrázek 20. PIR detektor u vjezdu na stanici [vlastní]

Další PIR detektor zabezpečuje boční vstup, který je určen také jako vchod pro zaměstnance. U bočního vstupu se zároveň nachází klávesnice pro zastřežení a odstřežení budovy. Dále se PIR detektor nachází v prostorách malé elektrické rozvodny, který je umístěn tak, že pokrývá vstup i okno místnosti. V této místnosti se také vyskytuje ústředna PZTS pro tuto budovu, která je zabezpečena proti neoprávněnému otevření. Okna v této části budovy nelze z venkovní strany otevřít.

Obrázek 21. Ústředna budovy emisní kontroly a PIR detektor [vlastní]

Následně jsou v prostorách skladu rozmístěny dva PIR detektory. První je umístěn u hlavního vstupu společně s klávesnicí pro zastřežení a odstřežení této části budovy (viz Obrázek 23).

Obrázek 22. PIR detektor u vstupu do skladu [vlastní]

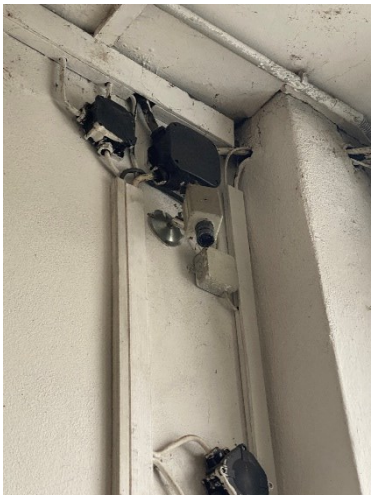
Obrázek 23. Klávesnice PZTS u vstupu do skladu [vlastní]

Další se nachází v prostorách skladu, který je blíže ke stanici STK. Zbytek místností a prostor není nijak zabezpečen ani z venkovní strany budovy. Na střechu budovy se nelze nijak dostat ani z vnitřní, ani z venkovní strany. Vstupní dveře do skladovací části nelze z venkovní strany otevřít bez klíče.

Až na výjimky do prostor emisní kontroly zákazníci nechodí, a tak se zde nachází většinově pouze zaměstnanci. Vstupní dveře však nejsou zamčeny ani nijak zabezpečeny, takže umožnují volný vstup na stanici. Boční vstup nelze z venkovní strany bez klíče otevřít. Okna

situována na straně blíže k STK jsou zabezpečena zmiňovanou IR bariérou. Střešní okna ani okna na jiných stranách budovy nejsou nijak zabezpečena s výjimkou kamerového systému, který však nevidí na stranu budovy nacházející se nejdál od budovy STK. Ventilační systém se nedá využít pro vniknutí do budovy.

Prostory jsou rozděleny na část emisní kontroly a na skladní část. Budova jako celek není nijak monitorována. V prostorách určených pro emisní kontrolu se nacházejí kamery. Ty však nefungují a nikdo k nim nemá přístup.



Obrázek 24. Nefunkční kamera v budově emisní kontroly [vlastní]

Kancelář vedoucího je z hlavních prostor volně přístupná a není nijak zabezpečená, okno v této kanceláři také není nijak chráněno s výjimkou kamer z venkovní strany. V kanceláři se však nachází zabudovaný trezor na peněžní hotovost, ten měl v průběhu naší přítomnosti v zámku zastrčený klíč.

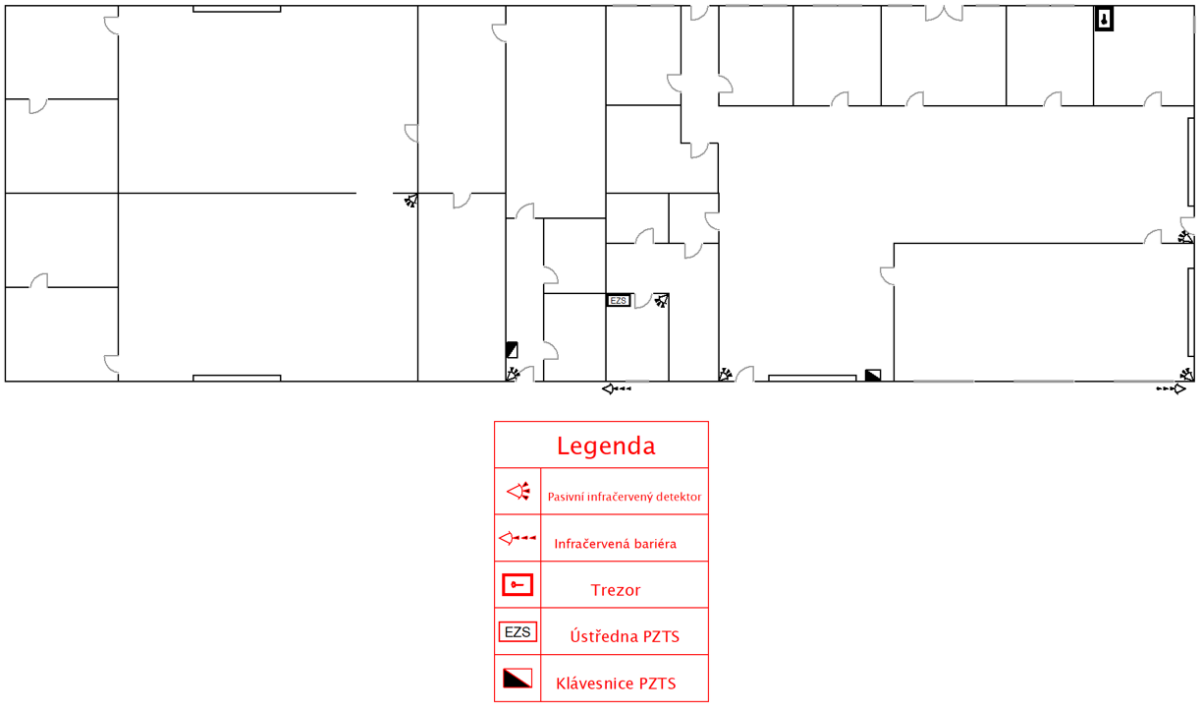
Obrázek 25. Trezor v kanceláři vedoucího budovy emisní kontroly [vlastní]

Obecně při procházení budovy emisní kontroly bylo na stolech ponecháno různé množství peněžní hotovosti společně s doklady od automobilů. Další prostory pro zaměstnance včetně šatny jsou volně přístupné z hlavní haly. Následně se nikde v budově nenachází žádný požární hlásič, ať už detektor kouře nebo plamene.

Režim objektu je nastaven tak, že klíče od hlavního a bočního vchodu mají všichni zaměstnanci pracující v budově. Klíče od skladu má skladník a vedoucí STK. Oba vedoucí emisní kontroly jsou jediné dvě osoby, které mají přístup k zabudovanému trezoru. Zaměstnanci nosí pracovní oblečení, díky nimž jsou jednoznačně rozeznatelní od zákazníků.

Jelikož emise spadají pod STK, zodpovídá se také Ministerstvu dopravy, a musí tedy budova také splňovat příslušné normy z pohledu detektorů plynu, množství a rozmístění hasicích přístrojů a dalších povinných ochran v tomto typu objektu. Tyto normy splňuje, ale nachází se zde několik rizikových pochybení. Budova nemá evakuační plán ani zpracovanou dokumentaci k požární bezpečnosti. Proto tedy zaměstnanci neznají shromaždiště budovy ani jiné postupy při požáru této konkrétní budovy. Zaměstnanci také podstupují povinné školení v rámci obecné požární bezpečnosti. Budova má otevírací dobu nastavenou tak, že pracovní dny jsou pondělí až pátek. V případě agresivního či násilného zákazníka si zaměstnanci musejí poradit sami svépomocí, žádná vnitřní směrnice pro tento případ není zavedena.

Okolí budovy je monitorováno stejně jako v případě budovy STK ze stejného místa, přes noční hodiny nebo přes víkend ke kamerám nemá nikdo přístup. Kamery nacházející se uvnitř budovy nikdo nesleduje, proto ani nikdo neví, jestli vůbec fungují a kdo k nim má přístup. Zaměstnanci fyzické ostrahy budovu kontrolují až při vyvolaném poplachu a telefonickém ověření vedoucímu STK, jestli se nejedná o planý poplach. Aktuální stav bezpečnostních prvků zde také nikdo pravidelně nekontroluje.



Obrázek 26. Rozmístění bezpečnostních prvků budovy emisní kontroly [vlastní]

4.5 Závěrečné posouzení

Obecně je znatelné, že areál spoléhá na kamerový systém se záznamem, u kterého nefunguje vzdálené propojení na SBS, což značně komplikuje ověřování planých poplachů a může vyústit i ve zbytečné výjezdy pracovníků SBS. Tento kamerový systém také nevidí na vzdálenou stranu budovy emisní kontroly a skladu.

Samotná budova STK je poměrně dobře zabezpečena. Všechny prosklené plochy a jiné vstupní otvory jsou chráněny buď PIR detektory, IR bránami či zámky. I samotný přístup na hlavní linku je adekvátně vyřešen, a to nutností odemčení klíči nebo otevřením dveří zaměstnancem. Největším rizikem je pohyb poměrně vysokého počtu zákazníků na lince. A to z důvodu volného přístupu do většiny místností právě z této linky. Dále je problémem snadný přístup do druhého patra. Ve druhém patře se však místnosti zamykají s výjimkou šaten pro zaměstnance.

Budova emisní kontroly se spoléhá primárně na to, že se v ní téměř nikdo nevyskytuje. Proto se ponechávají odemčené vstupní dveře, díky nimž se lze snadno dostat na linku, ze které je volný přístup do většiny ostatních místností. Většina vstupních a prosklených otvorů je zabezpečena PIR detektory, až na výjimku okna v kanceláři vedoucího a okna na vzdálené straně budovy, což je značně rizikové. Uvnitř se také nacházejí staré a nefunkční kamery.

Rizikové, vzhledem k malé kontrole pohybu osob v prostorách, je také ponechávání hotovosti a jiných dokumentů na stolech.

5 ANALÝZA RIZIK

Pro potřeby této práce byla zvolena metoda FMEA, která byla upravena pro potřeby analýzy rizik vybraného objektu. Jsou zde tedy v rámci této analýzy určeny pojmy jako hrozba, příčina a dopad. V této kapitole jsou rozebrány jednotlivá kritéria, která jsou nutná pro správné vyhodnocení analýzy. Byly dále popsány hodnotící body a jejich rozdělení do jednotlivých úrovní a ohodnocení. Některé ze stupňů mají více číselných hodnocení. Je to takto zavedeno z důvodu, kdy dochází například ke zlepšení po zavedení opatření. Toto opatření ale pak není dost zásadní, aby daný faktor snížila o celý stupeň (například ze středního na nízký). Dále je popsáno číslo RPN a vysvětlena použitá klasifikace daného čísla. Následně je uvedena provedená analýza rizik, která měla za cíl určit závažnost daných hrozeb a míru rizika. Na závěr kapitoly je popsáno vyhodnocení zjištěných rizik.

5.1 Hrozba, příčina a dopad

V analýze byla jednotlivá aktiva rozdělena dle konkrétních hrozeb, které na daná aktiva mohou působit. Obecně byly brány v potaz především hrozby jako ztráta, odcizení, poškození, napadení, zničení, vloupání apod. Každá z hrozeb má své možné příčiny. Především se jednalo o příčiny z pohledu úmyslu osoby, která danou příčinu způsobuje. Následně tyto příčiny byly rozděleny do možných dopadů, které mohou dané hrozby způsobit. S ohledem na povahu zkoumaného objektu se tak jednalo například o finanční dopady, úniky informací apod.

5.2 Význam, výskyt a odhalitelnost

Význam je brán z pohledu vyhodnocení úrovně dopadu dané hrozby. Proto bylo toto kritérium rozděleno do pěti úrovní z pohledu jeho důležitosti. Každá tato úroveň má své slovní vyjádření a odpovídající číselné hodnocení. Úrovně byly s ohledem na povahu analýzy rozděleny především z pohledu vlivu hrozby na chod objektu a celkového rozsahu finančního poškození. Proto do nejnižšího stupně spadají hrozby, které chod objektu neovlivní a jejichž způsobené finanční poškození je zanedbatelné. Naopak do nejvyššího stupně náleží hrozby, které nenávratně poškodí chod objektu a finanční ztráta je tak velká, že může způsobit likvidaci podniku.

Tabulka 5. Klasifikace významu [vlastní]

Klasifikace významu		Hodnocení
Zanedbatelný	Podstata hrozby je taková, že neovlivní chod objektu, a finančně je poškození zanedbatelné.	1
Nízký	Hrozba naruší chod objektu, avšak lze tuto hrozbu rychle eliminovat, a finanční poškození je nízkého rozsahu.	2 3
Střední	Hrozba poškodí chod objektu a finanční poškození je znatelné.	4 5 6
Vysoký	Hrozba značně poškodí chod objektu a finanční poškození je vysoké.	7 8
Velmi vysoký	Hrozba nenávratně poškodí chod objektu, finanční poškození je likvidační.	9 10

Výskyt lze chápat jako frekvenci, se kterou se daná hrozba objevuje, případně jak často lze očekávat, že se objeví. Jedná se tedy o určitou pravděpodobnost výskytu hrozby. Výskyt byl rozdělen do pěti úrovní z pohledu četnosti výskytu hrozby. U nepravděpodobného výskytu se tedy vznik hrozby téměř vylučuje, naopak u velmi vysokého výskytu je vznik hrozby až jistý.

Tabulka 6. Klasifikace výskytu [vlastní]

Klasifikace výskytu		Hodnocení
Nepravděpodobný	Vznik hrozby je skoro vyloučen.	1
Nepatrný	Vznik hrozby je velmi ojedinělý.	2 3
Malý	Hrozba občas nastane.	4 5

		6
Vysoký	Hrozba se vyskytuje často.	7 8
Velmi vysoký	Hrozba téměř jistě nastane.	9 10

Odhalitelnost lze chápat jako skutečnost, že se hrozba včasně odhalí. Pro případ použité analýzy se jedná konkrétně o pravděpodobnost, s jakou zabezpečení hrozbu včas odhalí, případně jestli si některý z pracovníků dané skutečnosti může včas všimnout. Opět byla odhalitelnost rozdělena do pěti úrovní z pohledu pravděpodobnosti odhalení. Jako vysokou odhalitelnost lze klasifikovat situaci, kdy má zabezpečení vysokou pravděpodobnost, že možnou hrozbu odhalí. Naopak nepravděpodobnou odhalitelností se rozumí stav, kdy zabezpečení nemůže odhalit případnou hrozbu.

Tabulka 7. Klasifikace odhalitelnosti [vlastní]

Klasifikace odhalitelnosti		Hodnocení
Vysoká	Zabezpečení objektu nebo zaměstnanci s vysokou pravděpodobností odhalí možnou hrozbu.	1
Pravděpodobná	Zabezpečení objektu nebo zaměstnanci by měli odhalit možnou hrozbu.	2 3
Malá	Zabezpečení objektu nebo zaměstnanci mohou možnou hrozbu odhalit.	4 5 6
Velmi malá	Zabezpečení objektu nebo zaměstnanci pravděpodobně hrozbu neodhalí.	7 8
Nepravděpodobná	Zabezpečení objektu nebo zaměstnanci téměř nemohou hrozbu odhalit.	9 10

5.3 RPN

Jedná se o matematicky vypočítanou míru rizika, se kterou metoda FMEA pracuje. Toto číslo je součinem hodnocení významu, výskytu a odhalitelnosti. Jelikož hodnoty jednotlivých kritérií dosahují hodnot 1 až 10, tak se velikost míry rizik může pohybovat v rozmezí 1 až 1000. Z tohoto důvodu je nutné zavést vhodné stupnice pro vyhodnocení závažnosti jednotlivých rizik. Bylo tedy zavedeno pět úrovní míry rizika. U mírného rizika se nepředpokládá, že by riziko způsobovalo zásadní problém pro objekt. Naopak u rizika, které se nachází v hodnotách spadajících do stupně velmi vysoké, je naprosto nezbytné se jím začít zabývat, jelikož toto riziko ohrožuje samotnou existenci objektu.

Tabulka 8. Hlavní klasifikace míry rizika [vlastní]

Hlavní klasifikace míry rizika	
Slovní hodnocení	**Číselný rozsah**
Mírné	0–199
Nízké	200–399
Střední	400–599
Vysoké	600–799
Velmi vysoké	800–1000

5.4 FMEA

Tato metoda byla připravena a vyhodnocena na základě fyzické obhlídky objektu a dříve vyhodnoceného kontrolního seznamu. Z důvodu požadavků provozovatele je zaměřena na hodnocení především hmotného majetku z pohledu fyzické bezpečnosti. Proto zde nejsou zahrnuty hrozby týkající se požární ochrany nebo hrozby spadající pod bezpečnost a ochranu zdraví při práci. Hodnocení jednotlivých faktorů bylo konzultováno s příslušnými zaměstnanci objektu tak, aby se docílilo co nejrealističtějšího ohodnocení. Tato analýza byla vypracována pro obě zkoumané budovy. Společné služby, případně aktiva nacházející se kolem objektů, byla zahrnuta v analýze budovy STK.

Název FMEA							FMEA-Stav			Datum poslední změny			
Budova STK							Dokonončená			30.04.2023			
Aktiva	**Hrozby**	**Příčiny**	**Dopad**	**Význam**	**Výskyt**	**Odhalitelnost**	**RPN**	**Současná opatření/ současný stav**	**Doporučená opatření**	**Význam**	**Výskyt**	**Odhalitelnost**	**RPN**
Písemná Dokumentace	Ztráta	Nedbalost	Finanční ztráta	2	2	2	8	Archivace a elektrický přepis	Vhodné ukládání dokumentace před archivací	2	1	2	4
			Opakování zkoušky	2	2	2	8	Archivace a elektrický přepis	Vhodné ukládání dokumentace před archivací	2	1	2	4
		Zlý úmysl	Finanční ztráta	2	1	3	6	Archivace a elektrický přepis	Vhodné ukládání dokumentace před archivací	2	1	3	6
			Opakování zkoušky	2	1	3	6	Archivace a elektrický přepis	Vhodné ukládání dokumentace před archivací	2	1	3	6
	Poškození	Nedbalost	Finanční ztráta	1	2	1	2	Archivace a elektrický přepis	Vhodné ukládání dokumentace před archivací	1	1	1	1
		Zlý úmysl	Finanční ztráta	1	1	2	2	Archivace a elektrický přepis	Vhodné ukládání dokumentace před archivací	1	1	2	2
	Odcizení	Vlastní obohacení	Únik informací	3	1	2	6	Archivace a elektrický přepis	Vhodné ukládání dokumentace před archivací	3	1	2	6
			Finanční ztráta	2	1	2	4	Archivace a elektrický přepis	Vhodné ukládání dokumentace před archivací	2	1	2	4
		Příležitost	Únik informací	3	2	2	12	Archivace a elektrický přepis	Vhodné ukládání dokumentace před archivací + zajištění nouzových východů	3	1	2	6
			Finanční ztráta	2	2	2	8	Archivace a elektrický přepis	Vhodné ukládání dokumentace před archivací + zajištění nouzových východů	2	1	2	4
		Zlý úmysl	Únik informací	3	1	2	6	Archivace a elektrický přepis	Vhodné ukládání dokumentace před archivací + zajištění nouzových východů	3	1	2	6
			Finanční ztráta	2	1	2	4	Archivace a elektrický přepis	Vhodné ukládání dokumentace před archivací + zajištění nouzových východů	2	1	2	4

Písemná Dokumentace	Neoprávněné užití	Vlastní obohacení	Únik informací	3	1	5	15	Archivace a elektrický přepis	Vhodné ukládání dokumentace před archivací + zajištění nouzových východů	3	1	4	12
			Finanční ztráta	3	1	5	15	Archivace a elektrický přepis	Vhodné ukládání dokumentace před archivací + zajištění nouzových východů	3	1	4	12
		Příležitost	Únik informací	3	1	5	15	Archivace a elektrický přepis	Vhodné ukládání dokumentace před archivací + zajištění nouzových východů	3	1	4	12
			Finanční ztráta	3	1	5	15	Archivace a elektrický přepis	Vhodné ukládání dokumentace před archivací + zajištění nouzových východů	3	1	4	12
Data	Ztráta	Nedbalost	Finanční ztráta	3	2	3	18	Archivace u ministerstva		3	2	3	18
			Opakování zkoušky	2	2	3	12	Archivace u ministerstva		2	2	3	12
		Zlý úmysl	Finanční ztráta	3	1	4	12	Archivace u ministerstva		3	1	4	12
			Opakování zkoušky	2	1	4	8	Archivace u ministerstva		2	1	4	8
	Poškození	Nedbalost	Finanční ztráta	3	2	5	30	Archivace u ministerstva		3	2	5	30
		Zlý úmysl	Finanční ztráta	3	1	5	15	Archivace u ministerstva		3	1	5	15
	Oddizení	Vlastní obohacení	Únik informací	5	1	2	10	Archivace u ministerstva a kontrola přístupu k datům		5	1	2	10
			Finanční ztráta	4	1	2	8	Archivace u ministerstva a kontrola přístupu k datům		4	1	2	8
		Příležitost	Únik informací	5	2	3	30	Archivace u ministerstva a kontrola přístupu k datům		5	2	3	30
			Finanční ztráta	4	2	3	24	Archivace u ministerstva a kontrola přístupu k datům		4	2	3	24
		Zlý úmysl	Únik informací	5	1	2	10	Archivace u ministerstva a kontrola přístupu k datům		5	1	2	10
			Finanční ztráta	4	1	2	8	Archivace u ministerstva a kontrola přístupu k datům		4	1	2	8
	Neoprávněné užití	Vlastní obohacení	Únik informací	5	1	2	10	Archivace u ministerstva a kontrola přístupu k datům		5	1	2	10
			Finanční ztráta	4	1	2	8	Archivace u ministerstva a kontrola přístupu k datům		4	1	2	8
		Příležitost	Únik informací	5	2	2	20	Archivace u ministerstva a kontrola přístupu k datům		5	2	2	20
			Finanční ztráta	4	2	2	16	Archivace u ministerstva a kontrola přístupu k datům		4	2	2	16
	Kybernetický útok	Nevědomost	Únik informací	5	3	8	120	Absence bezpečnostního školení o kybernetické bezpečnosti	Bezpečnostní školení o kybernetické bezpečnosti	5	2	7	70

Data	Kybernetický útok	Nevědomost	Poškození dat	5	3	6	90	Absence bezpečnostního školení o kybernetické bezpečnosti	Bezpečnostní školení o kybernetické bezpečnosti	5	2	4	40
		Nedostatečná ochrana	Únik informací	5	1	2	10	Zabezpečení ministerstva + základní kybernetická ochrana		5	1	2	10
			Poškození dat	5	1	2	10	Zabezpečení ministerstva + základní kybernetická ochrana		5	1	2	10
Zaměstanci	Napadení	Loupežné přepadení budovy	Újma na životě	8	1	2	16	Chybějící směrnice	Zavedení postupů jak se chovat při napadení + Školení + tísňové tlačítko	7	1	1	7
			Zranění	5	3	2	30	Chybějící směrnice	Zavedení postupů jak se chovat při napadení + Školení + tísňové tlačítko	4	2	1	8
			Pracovní neschopnost	6	2	2	24	Chybějící směrnice	Zavedení postupů jak se chovat při napadení + Školení + tísňové tlačítko	6	2	1	12
		Zákazník	Újma na životě	8	1	4	32	Chybějící směrnice	Zavedení postupů jak se chovat při napadení + Školení	7	1	3	21
			Zranění	5	3	4	60	Chybějící směrnice	Zavedení postupů jak se chovat při napadení + Školení	4	2	3	24
			Pracovní neschopnost	6	2	4	48	Chybějící směrnice	Zavedení postupů jak se chovat při napadení + Školení	6	2	3	36
		Zaměstnanec	Újma na životě	8	1	4	32	Chybějící směrnice	Zavedení postupů jak se chovat při napadení + Školení	7	1	3	21
			Zranění	5	4	4	80	Chybějící směrnice	Zavedení postupů jak se chovat při napadení + Školení	4	3	3	36
			Pracovní neschopnost	6	3	4	72	Chybějící směrnice	Zavedení postupů jak se chovat při napadení + Školení	6	2	3	36
			Ztráta zaměstance	6	3	4	72	Chybějící směrnice	Zavedení postupů jak se chovat při napadení + Školení	6	2	3	36
Zákazníci	Napadení	Loupežné přepadení budovy	Újma na životě	8	1	2	16	Chybějící směrnice	Zavedení postupů jak se chovat při napadení + Školení + tísňové tlačítko	7	1	1	7
			Zranění	7	3	2	42	Chybějící směrnice	Zavedení postupů jak se chovat při napadení + Školení + tísňové tlačítko	6	2	1	12

Zákazníci	Napadení	Loupežné přepadení budovy	Ztáta zákazníka	6	2	2	24	Chybějící směrnice	Zavedení postupů jak se chovat při napadení + Školení + tísňové tlačítko	6	2	1	12
		Zákazník	Újma na životě	8	1	4	32	Chybějící směrnice	Zavedení postupů jak se chovat při napadení + Školení	7	1	3	21
			Zranění	7	2	4	56	Chybějící směrnice	Zavedení postupů jak se chovat při napadení + Školení	6	2	3	36
			Ztáta zákazníka	6	2	4	48	Chybějící směrnice	Zavedení postupů jak se chovat při napadení + Školení	6	2	3	36
		Zaměstnanec	Újma na životě	8	1	4	32	Chybějící směrnice	Zavedení postupů jak se chovat při napadení + Školení	7	1	3	21
			Zranění	7	3	4	84	Chybějící směrnice	Zavedení postupů jak se chovat při napadení + Školení	6	2	3	36
			Ztáta zákazníka	7	2	4	56	Chybějící směrnice	Zavedení postupů jak se chovat při napadení + Školení	6	2	3	36
Budova	Poškození	Vandalismus	Finanční ztráta	4	4	8	128	Kamerový systém se záznamem a IR brány	Napojení kamer na SBS, pravidelná kontrola budovy	4	4	6	96
		Žhářství	Finanční ztráta	7	1	6	42	Kamerový systém se záznamem, IR brány a požární hlásiče	Napojení kamer na SBS, pravidelná kontrola budovy	7	1	5	35
		Pomsta	Finanční ztráta	4	1	7	28	Kamerový systém se záznamem a IR brány	Napojení kamer na SBS, pravidelná kontrola budovy	4	1	6	24
	Zničení	Žhářství	Likvidace podniku	10	1	3	30	Požární hlásiče	Napojení kamer na SBS, pravidelná kontrola budovy	10	1	2	20
			Ušlý zisk	9	1	3	27	Požární hlásiče	Napojení kamer na SBS, pravidelná kontrola budovy	9	1	2	18
			Finanční ztráta	9	1	3	27	Požární hlásiče	Napojení kamer na SBS, pravidelná kontrola budovy	9	1	2	18
		Přírodní vlivy	Likvidace podniku	10	1	4	40			10	1	4	40
			Ušlý zisk	9	1	4	36			9	1	4	36
			Finanční ztráta	9	1	4	36			9	1	4	36

IT technika	Zničení	Vloupání	Finanční ztráta	6	3	2	36	MZS, PZTS, kamerový systém se záznamem	Napojení kamer na SBS, posílení PZTS	6	2	2	24
			Ztráta dat	5	3	2	30	MZS, PZTS, kamerový systém se záznamem	Napojení kamer na SBS, posílení PZTS	5	2	2	20
			Ušlý zisk	6	3	2	36	MZS, PZTS, kamerový systém se záznamem	Napojení kamer na SBS, posílení PZTS	6	2	2	24
		Nedbalost	Finanční ztráta	6	3	4	72		Školení o správném zacházení	6	2	4	48
			Ztráta dat	5	3	4	60		Školení o správném zacházení	5	2	4	40
			Ušlý zisk	6	3	4	72		Školení o správném zacházení	6	2	4	48
	Poškození	Vloupání	Finanční ztráta	5	3	2	30	MZS, PZTS, kamerový systém se záznamem	Napojení kamer na SBS, posílení PZTS	5	2	2	20
			Ztráta dat	5	3	2	30	MZS, PZTS, kamerový systém se záznamem	Napojení kamer na SBS, posílení PZTS	5	2	2	20
			Ušlý zisk	6	3	2	36	MZS, PZTS, kamerový systém se záznamem	Napojení kamer na SBS, posílení PZTS	6	2	2	24
		Nedbalost	Finanční ztráta	4	4	4	64		Školení o správném zacházení	4	3	4	48
			Ztráta dat	5	4	4	80		Školení o správném zacházení	5	3	4	60
			Ušlý zisk	6	4	4	96		Školení o správném zacházení	6	3	4	72
		Sabotáž	Finanční ztráta	4	2	4	32		Zamezení fyzického přístupu k zařízení	4	2	4	32
			Ztráta dat	5	2	4	40		Zamezení fyzického přístupu k zařízení	5	2	4	40
			Ušlý zisk	6	2	4	48		Zamezení fyzického přístupu k zařízení	6	2	4	48
		Opotřebení	Finanční ztráta	4	2	4	32		Průběžná kontrola stavu	4	2	3	24
			Ztráta dat	5	2	4	40		Průběžná kontrola stavu	5	2	3	30
			Ušlý zisk	6	2	4	48		Průběžná kontrola stavu	6	2	3	36
	Odcizení	Vloupání	Finanční ztráta	6	3	2	36	MZS, PZTS, kamerový systém se záznamem	Napojení kamer na SBS, posílení PZTS	6	2	2	24
			Ztráta dat	5	3	2	30	MZS, PZTS, kamerový systém se záznamem	Napojení kamer na SBS, posílení PZTS	5	2	2	20
			Ušlý zisk	6	3	2	36	MZS, PZTS, kamerový systém se záznamem	Napojení kamer na SBS, posílení PZTS	6	2	2	24
		Vlastní obohacení	Finanční ztráta	6	3	7	126	Režim (prostory pouze pro zaměstance)	Zamezení fyzického přístupu k zařízení	6	2	6	72
			Ztráta dat	5	3	7	105	Režim (prostory pouze pro zaměstance)	Zamezení fyzického přístupu k zařízení	5	2	6	60
			Ušlý zisk	6	3	7	126	Režim (prostory pouze pro zaměstance)	Zamezení fyzického přístupu k zařízení	6	2	6	72

IT technika	Odcizení	Zlý úmysl	Finanční ztráta	6	2	6	72	Režim (prostory pouze pro zaměstance)	Zamezení fyzického přístupu k zařízení	6	2	6	72
			Ztráta dat	5	2	6	60	Režim (prostory pouze pro zaměstance)	Zamezení fyzického přístupu k zařízení	5	2	6	60
			Ušlý zisk	6	2	6	72	Režim (prostory pouze pro zaměstance)	Zamezení fyzického přístupu k zařízení	6	2	6	72
	Neoprávněné užití	Vlastní obohacení	Únik informací	6	2	2	24	Kontrola přístupu		6	2	2	24
			Únik citlivých informací	7	2	2	28	Kontrola přístupu		7	2	2	28
			Finanční ztráta	5	2	2	20	Kontrola přístupu		5	2	2	20
	Kybernetický útok	Nevědomost	Únik informací	6	3	6	108	Absence bezpečnostního školení o kybernetické bezpečnosti	Bezpečnostní školení o kybernetické bezpečnosti	6	2	4	48
			Únik citlivých informací	7	3	6	126	Absence bezpečnostního školení o kybernetické bezpečnosti	Bezpečnostní školení o kybernetické bezpečnosti	7	2	4	56
			Finanční ztráta	5	3	6	90	Absence bezpečnostního školení o kybernetické bezpečnosti	Bezpečnostní školení o kybernetické bezpečnosti	5	2	4	40
			Ztráta dat	5	3	6	90	Absence bezpečnostního školení o kybernetické bezpečnosti	Bezpečnostní školení o kybernetické bezpečnosti	5	2	4	40
Technika	Poškození	Nedbalost	Finanční ztráta	6	4	2	48	Školení o správném zacházení		6	4	2	48
			Ušlý zisk	7	4	2	56	Školení o správném zacházení		7	4	2	56
		Sabotáž	Finanční ztráta	6	2	2	24	Přítomnost pracovníků		6	2	2	24
			Ušlý zisk	7	2	2	28	Přítomnost pracovníků		7	2	2	28
		Zlý úmysl	Finanční ztráta	6	3	2	36	Přítomnost pracovníků		6	3	2	36
			Ušlý zisk	7	3	2	42	Přítomnost pracovníků		7	3	2	42
		Opotřebení	Finanční ztráta	6	4	2	48	Revize		6	4	2	48
			Ušlý zisk	7	4	2	56	Revize		7	4	2	56
	Zničení	Nedbalost	Finanční ztráta	7	3	2	42	Školení o správném zacházení		7	3	2	42
			Ušlý zisk	8	3	2	48	Školení o správném zacházení		8	3	2	48
		Sabotáž	Finanční ztráta	7	2	2	28	Přítomnost pracovníků		7	2	2	28
			Ušlý zisk	8	2	2	32	Přítomnost pracovníků		8	2	2	32
		Zlý úmysl	Finanční ztráta	7	3	2	42	Přítomnost pracovníků		7	3	2	42
			Ušlý zisk	8	3	2	48	Přítomnost pracovníků		8	3	2	48
	Odcizení	Vlastní obohacení	Finanční ztráta	7	1	2	14	MZS, PZTS, kamerový systém se záznamem	Napojení kamer na SBS, posílení PZTS	7	1	2	14
			Ušlý zisk	8	1	2	16	MZS, PZTS, kamerový systém se záznamem	Napojení kamer na SBS, posílení PZTS	8	1	2	16
		Zlý úmysl	Finanční ztráta	7	1	2	14	MZS, PZTS, kamerový systém se záznamem	Napojení kamer na SBS, posílení PZTS	7	1	2	14
			Ušlý zisk	8	1	2	16	MZS, PZTS, kamerový systém se záznamem	Napojení kamer na SBS, posílení PZTS	8	1	2	16
Hotovost	Odcizení zaměstnancem	Vlastní obohacení	Finanční ztráta	7	2	4	56	Denní uzávěrka	Instalace kamery u kasy (v příjmu)	7	2	3	42
			Ztráta zaměstance	6	2	4	48	Denní uzávěrka	Instalace kamery u kasy (v příjmu)	6	2	3	36

Hotovost	Odcizení zaměstnancem	Příležitost	Finanční ztráta	7	2	4	56	Denní uzávěrka	Instalace kamery u kasy (v příjmu)	7	2	3	42
			Ztráta zaměstance	6	2	4	48	Denní uzávěrka	Instalace kamery u kasy (v příjmu)	6	2	3	36
	Odcizení bývalým zaměstancem	Vlastní obohacení	Finanční ztráta	7	2	3	42	Denní uzávěrka + odevzdání klíčů/čipů při odchodu	Instalace kamery u kasy (v příjmu)	7	2	2	28
		Příležitost	Finanční ztráta	7	2	3	42	Denní uzávěrka + odevzdání klíčů/čipů při odchodu	Instalace kamery u kasy (v příjmu)	7	2	2	28
		Pomsta	Finanční ztráta	7	2	3	42	Denní uzávěrka + odevzdání klíčů/čipů při odchodu	Instalace kamery u kasy (v příjmu)	7	2	2	28
	Odcizení zákazníkem	Vlastní obohacení	Finanční ztráta	7	2	2	28	Režim (prostory pouze pro zaměstance) + denní uzávěrka	Instalace kamery u kasy (v příjmu)	7	2	2	28
		Příležitost	Finanční ztráta	7	2	2	28	Režim (prostory pouze pro zaměstance) + denní uzávěrka	Instalace kamery u kasy (v příjmu)	7	2	2	28
		Pomsta	Finanční ztráta	7	2	2	28	Režim (prostory pouze pro zaměstance) + denní uzávěrka	Instalace kamery u kasy (v příjmu)	7	2	2	28
	Odcizení neznámou osobou	Vlastní obohacení	Finanční ztráta	7	2	2	28	Režim (prostory pouze pro zaměstance) + denní uzávěrka	Instalace kamery u kasy (v příjmu)	7	2	2	28
		Příležitost	Finanční ztráta	7	2	2	28	Režim (prostory pouze pro zaměstance) + denní uzávěrka	Instalace kamery u kasy (v příjmu)	7	2	2	28
	Přepadení	Vlastní obohacení	Finanční ztráta	7	1	4	28	Rozsáhlost objektu (někdo by si toho asi všiml)	Instalace kamery u kasy (v příjmu) + tísňové tlačítko	7	1	2	14
	Vloupání	Vlastní obohacení	Finanční ztráta	7	2	2	28	MZS, PZTS, kamerový systém se záznamem	Napojení kamer na SBS, posílení PZTS	7	2	2	28
		Příležitost	Finanční ztráta	7	2	2	28	MZS, PZTS, kamerový systém se záznamem	Napojení kamer na SBS, posílení PZTS	7	2	2	28
	Podvod	Falšené bankovky	Finanční ztráta	2	3	8	48	Kontrola pouze 5000 bankovek	Kontrola více druhů bankovek	2	3	3	18
Kontrolní nálepky	Poškození	Nedbalost	Finanční ztráta	1	9	1	9	Evidence cenin + MZS		1	9	1	9
	Odcizení	Vlastní obohacení	Finanční ztráta	1	2	2	4	Evidence cenin + MZS		1	2	2	4
		Příležitost	Finanční ztráta	1	2	2	4	Evidence cenin + MZS		1	2	2	4
	Přepadení	Vlastní obohacení	Finanční ztráta	1	1	2	2	Evidence cenin + MZS		1	1	2	2
	Vloupání	Vlastní obohacení	Finanční ztráta	1	1	2	2	Evidence cenin + MZS		1	1	2	2
		Příležitost	Finanční ztráta	1	1	2	2	Evidence cenin + MZS		1	1	2	2
	Zneužití	Korupce	Finanční ztráta	1	2	2	4	Evidence cenin + MZS		1	2	2	4
Automobily	Zničení	Žhářství	Finanční ztráta	4	2	7	56	Kamerový systém se záznamem + oplocení	Napojení kamer na SBS, pravidelná kontrola budovy	4	2	6	48
		Zlý úmysl	Finanční ztráta	4	2	8	64	Kamerový systém se záznamem + oplocení	Napojení kamer na SBS, pravidelná kontrola budovy	4	2	6	48
	Poškození	Nedbalost	Finanční ztráta	3	4	4	48	Kamerový systém se záznamem + oplocení	Napojení kamer na SBS, pravidelná kontrola budovy	3	3	4	36

Automobily		Zlý úmysl	Finanční ztráta	3	3	6	54	Kamerový systém se záznamem + oplocení	Napojení kamer na SBS, pravidelná kontrola budovy	3	3	5	45
		Vandalismus	Finanční ztráta	3	3	6	54	Kamerový systém se záznamem + oplocení	Napojení kamer na SBS, pravidelná kontrola budovy	3	3	5	45
		Žhářství	Finanční ztráta	3	2	7	42	Kamerový systém se záznamem + oplocení	Napojení kamer na SBS, pravidelná kontrola budovy	3	2	6	36
	Odcizení	Vloupání	Finanční ztráta	4	2	4	32	Kamerový systém se záznamem + oplocení	Napojení kamer na SBS, pravidelná kontrola budovy	4	2	4	32
		Krádež klíčů	Finanční ztráta	4	3	5	60	Kamerový systém se záznamem + oplocení	Vhodné ukládání klíčů	4	3	5	60
		Příležitost	Finanční ztráta	4	2	5	40	Kamerový systém se záznamem + oplocení	Vhodné ukládání klíčů	4	2	5	40
Osobní věci	Odcizení	Vlastní obohacení	Finanční ztráta	2	5	6	60	MZS	Posílení MZS	2	4	6	48
		Příležitost	Finanční ztráta	2	5	6	60	MZS	Posílení MZS	2	4	6	48
		Pomsta	Finanční ztráta	2	4	6	48	MZS	Posílení MZS	2	4	6	48
Ostatní majetek	Zničení	Nedbalost	Finanční ztráta	3	2	2	12		Finanční postih	2	2	2	8
		Zlý úmysl	Finanční ztráta	3	2	2	12	MZS		3	2	2	12
	Poškození	Nedbalost	Finanční ztráta	2	3	2	12		Finanční postih	2	2	2	8
		Zlý úmysl	Finanční ztráta	2	3	2	12	MZS		2	3	2	12
	Odcizení	Příležitost	Finanční ztráta	3	3	3	27	MZS	Posílení MZS	3	2	3	18
		Vlastní obohacení	Finanční ztráta	3	3	3	27	MZS	Posílení MZS	3	2	3	18
		Zlý úmysl	Finanční ztráta	3	2	3	18	MZS	Posílení MZS	3	2	3	18
Elektrický proud	Výpadek	Zkrat	Ušlý zisk	8	2	1	16	Záložní zdroj serveru	Záložní generátor	4	2	1	8
		Sabotáž	Ušlý zisk	8	1	1	8	Záložní zdroj serveru	Záložní generátor	4	1	1	4
		Přerušení dodávky	Ušlý zisk	8	4	1	32	Záložní zdroj serveru	Záložní generátor	4	4	1	16
		Přírodní vlivy	Ušlý zisk	8	3	1	24	Záložní zdroj serveru	Záložní generátor	4	3	1	12
Reputace	Korupce	Vlastní obohacení	Finanční ztráta	3	2	6	36	Finanční postih + ztráta zaměstnání zaměstnance		3	2	6	36
			Ušlý zisk	4	2	6	48	Finanční postih + ztráta zaměstnání zaměstnance		4	2	6	48
		Příležitost	Finanční ztráta	3	2	6	36	Finanční postih + ztráta zaměstnání zaměstnance		3	2	6	36
			Ušlý zisk	4	2	6	48	Finanční postih + ztráta zaměstnání zaměstnance		4	2	6	48
	Kvalita služeb	Neprofesionálnost	Ušlý zisk	4	2	3	24	Pravidelné školení		4	2	3	24
			Ztráta zákazníka	5	2	3	30	Pravidelné školení		5	2	3	30
		Nekvalifikovanost	Ušlý zisk	4	2	3	24	Pravidelné školení		4	2	3	24
			Ztráta zákazníka	5	2	3	30	Pravidelné školení		5	2	3	30

Reputace	Chování zaměstanců	Nespokojenost	Ušlý zisk	5	2	3	30	Kniha stížností		5	2	3	30
			Ztráta zákazníka	6	2	3	36	Kniha stížností		6	2	3	36
		Neprofesionálnost	Ušlý zisk	5	2	3	30	Kniha stížností		5	2	3	30
			Ztráta zákazníka	6	2	3	36	Kniha stížností		6	2	3	36
	Pomluva	Pomsta	Ušlý zisk	3	4	4	48			3	4	4	48
			Ztráta zákazníka	3	4	4	48			3	4	4	48
		Konkurence	Ušlý zisk	3	4	4	48			3	4	4	48
			Ztráta zákazníka	3	4	4	48			3	4	4	48
Dodávka vody	Výpadek	Přerušení dodávky	Finanční ztráta	3	2	2	12		Smluvní ustanovení pokut za přerušení dodávek	2	2	2	8
		Přírodní vlivy	Finanční ztráta	2	2	2	8		Smluvní ustanovení pokut za přerušení dodávek	2	2	2	8
Internet	Výpadek	Poškození	Finanční ztráta	3	3	5	45	Offline režim pro dlouhodobý výpadek		3	3	5	45
			Ušlý zisk	6	3	5	90	Offline režim pro dlouhodobý výpadek		6	3	5	90
		Nedbalost	Finanční ztráta	3	2	4	24	Offline režim pro dlouhodobý výpadek		3	2	4	24
			Ušlý zisk	6	2	4	48	Offline režim pro dlouhodobý výpadek		6	2	4	48
		Přerušení dodávky	Ušlý zisk	6	7	1	42	Offline režim pro dlouhodobý výpadek	Smluvní ustanovení pokut za přerušení dodávek	5	7	1	35
		Přírodní vlivy	Finanční ztráta	4	4	1	16	Offline režim pro dlouhodobý výpadek		4	4	1	16
			Ušlý zisk	6	4	1	24	Offline režim pro dlouhodobý výpadek		6	4	1	24
	Zpomalení	Nevhodný tarif	Ušlý zisk	3	8	4	96		Vhodnější tarif	3	4	4	48
		Soukromé účely	Ušlý zisk	3	6	4	72		SW blokace stránek	3	4	4	48
Topení	Výpadek	Přerušení dodávky	Finanční ztráta	3	2	3	18	Externí řešení	Smluvní ustanovení pokut za přerušení dodávek	2	2	3	12
		Poškození	Finanční ztráta	3	2	3	18	Externí řešení	Smluvní ustanovení pokut za přerušení dodávek	2	2	3	12

Obrázek 27. FMEA budovy STK [vlastní]

Název FMEA							FMEA-Stav			Datum poslední změny			
Budova emisní kontroly							Dokončená			30.04.2023			
Aktiva	**Hrozby**	**Příčiny**	**Dopad**	**Význam**	**Výskyt**	**Odhalitelnost**	**RPN**	**Současná opatření/ současný stav**	**Doporučená opatření**	**Význam**	**Výskyt**	**Odhalitelnost**	**RPN**
Písemná Dokumentace	Ztráta	Nedbalost	Finanční ztráta	2	3	3	18	Archivace a elektrický přepis	Vhodné ukládání dokumentace před archivací	2	2	2	8
			Opakování zkoušky	2	3	3	18	Archivace a elektrický přepis	Vhodné ukládání dokumentace před archivací	2	2	2	8
		Zlý úmysl	Finanční ztráta	2	1	3	6	Archivace a elektrický přepis	Vhodné ukládání dokumentace před archivací	2	1	3	6
			Opakování zkoušky	2	1	3	6	Archivace a elektrický přepis	Vhodné ukládání dokumentace před archivací	2	1	3	6
	Poškození	Nedbalost	Finanční ztráta	1	2	2	4	Archivace a elektrický přepis	Vhodné ukládání dokumentace před archivací	1	1	2	2
		Zlý úmysl	Finanční ztráta	1	1	3	3	Archivace a elektrický přepis	Vhodné ukládání dokumentace před archivací	1	1	2	2
	Odcizení	Vlastní obohacení	Únik informací	3	2	3	18	Archivace a elektrický přepis	Vhodné ukládání dokumentace před archivací	3	2	3	18
			Finanční ztráta	2	2	3	12	Archivace a elektrický přepis	Vhodné ukládání dokumentace před archivací	2	2	3	12
		Příležitost	Únik informací	3	2	3	18	Archivace a elektrický přepis	Vhodné ukládání dokumentace před archivací + zajištění nouzových východů	3	2	2	12
			Finanční ztráta	2	2	3	12	Archivace a elektrický přepis	Vhodné ukládání dokumentace před archivací + zajištění nouzových východů	2	2	2	8
		Zlý úmysl	Únik informací	3	1	3	9	Archivace a elektrický přepis	Vhodné ukládání dokumentace před archivací + zajištění nouzových východů	3	1	2	6
			Finanční ztráta	2	1	3	6	Archivace a elektrický přepis	Vhodné ukládání dokumentace před archivací + zajištění nouzových východů	2	1	2	4

Písemná Dokumentace	Neoprávněné užití	Vlastní obohacení	Únik informací	3	1	5	15	Archivace a elektrický přepis	Vhodné ukládání dokumentace před archivací + zajištění nouzových východů	3	1	4	12
			Finanční ztráta	3	1	5	15	Archivace a elektrický přepis	Vhodné ukládání dokumentace před archivací + zajištění nouzových východů	3	1	4	12
		Příležitost	Únik informací	3	1	5	15	Archivace a elektrický přepis	Vhodné ukládání dokumentace před archivací + zajištění nouzových východů	3	1	4	12
			Finanční ztráta	3	1	5	15	Archivace a elektrický přepis	Vhodné ukládání dokumentace před archivací + zajištění nouzových východů	3	1	4	12
Zaměstanci	Napadení	Loupežné přepadení budovy	Újma na životě	8	1	2	16	Chybějící směrnice	Zavedení postupů jak se chovat při napadení + Školení + tísňové tlačítko	7	1	1	7
			Zranění	5	3	2	30	Chybějící směrnice	Zavedení postupů jak se chovat při napadení + Školení + tísňové tlačítko	4	2	1	8
			Pracovní neschopnost	6	2	2	24	Chybějící směrnice	Zavedení postupů jak se chovat při napadení + Školení + tísňové tlačítko	6	2	1	12
		Zákazník	Újma na životě	8	1	5	40	Chybějící směrnice	Zavedení postupů jak se chovat při napadení + Školení	7	1	3	21
			Zranění	5	3	5	75	Chybějící směrnice	Zavedení postupů jak se chovat při napadení + Školení	4	2	3	24
			Pracovní neschopnost	6	2	5	60	Chybějící směrnice	Zavedení postupů jak se chovat při napadení + Školení	6	2	3	36
		Zaměstnanec	Újma na životě	8	1	5	40	Chybějící směrnice	Zavedení postupů jak se chovat při napadení + Školení	7	1	3	21
			Zranění	5	4	5	100	Chybějící směrnice	Zavedení postupů jak se chovat při napadení + Školení	4	3	3	36
			Pracovní neschopnost	6	3	5	90	Chybějící směrnice	Zavedení postupů jak se chovat při napadení + Školení	6	2	3	36
			Ztráta zaměstance	6	3	5	90	Chybějící směrnice	Zavedení postupů jak se chovat při napadení + Školení	6	2	3	36

Zákazníci	Napadení	Loupežné přepadení budovy	Újma na životě	8	1	2	16	Chybějící směrnice	Zavedení postupů jak se chovat při napadení + Školení + tísňové tlačítko	7	1	1	7
			Zranění	7	3	2	42	Chybějící směrnice	Zavedení postupů jak se chovat při napadení + Školení + tísňové tlačítko	6	2	1	12
			Ztáta zákazníka	6	2	2	24	Chybějící směrnice	Zavedení postupů jak se chovat při napadení + Školení + tísňové tlačítko	6	2	1	12
		Zákazník	Újma na životě	8	1	5	40	Chybějící směrnice	Zavedení postupů jak se chovat při napadení + Školení	7	1	3	21
			Zranění	7	3	5	105	Chybějící směrnice	Zavedení postupů jak se chovat při napadení + Školení	6	2	3	36
			Ztáta zákazníka	6	2	5	60	Chybějící směrnice	Zavedení postupů jak se chovat při napadení + Školení	6	2	3	36
		Zaměstnanec	Újma na životě	8	1	5	40	Chybějící směrnice	Zavedení postupů jak se chovat při napadení + Školení	7	1	3	21
			Zranění	7	3	5	105	Chybějící směrnice	Zavedení postupů jak se chovat při napadení + Školení	6	2	3	36
			Ztáta zákazníka	7	2	5	70	Chybějící směrnice	Zavedení postupů jak se chovat při napadení + Školení	6	2	3	36
Budova	Poškození	Vandalismus	Finanční ztráta	4	4	8	128	Kamerový systém se záznamem a IR brány	Napojení kamer na SBS, pravidelná kontrola budovy	4	4	6	96
		Žhářství	Finanční ztráta	6	1	6	36	Kamerový systém se záznamem, IR brány a požární hlásiče	Napojení kamer na SBS, pravidelná kontrola budovy	7	1	5	35
		Pomsta	Finanční ztráta	4	1	7	28	Kamerový systém se záznamem a IR brány	Napojení kamer na SBS, pravidelná kontrola budovy	4	1	6	24
	Zničení	Žhářství	Omezení funkčnosti podniku	8	1	3	24	Požární hlásiče	Napojení kamer na SBS, pravidelná kontrola budovy	8	1	2	16
			Ušlý zisk	8	1	3	24	Požární hlásiče	Napojení kamer na SBS, pravidelná kontrola budovy	8	1	2	16
			Finanční ztráta	7	1	3	21	Požární hlásiče	Napojení kamer na SBS, pravidelná kontrola budovy	7	1	2	14

Budova	Zničení	Přírodní vlivy	Omezení funkčnosti podniku	8	1	4	32			8	1	4	32
			Ušlý zisk	8	1	4	32			8	1	4	32
			Finanční ztráta	7	1	4	28			7	1	4	28
IT technika	Zničení	Vloupání	Finanční ztráta	6	3	3	54	MZS, PZTS, kamerový systém se záznamem	Napojení kamer na SBS, posílení PZTS	6	2	2	24
			Ztráta dat	5	3	3	45	MZS, PZTS, kamerový systém se záznamem	Napojení kamer na SBS, posílení PZTS	5	2	2	20
			Ušlý zisk	6	3	3	54	MZS, PZTS, kamerový systém se záznamem	Napojení kamer na SBS, posílení PZTS	6	2	2	24
		Nedbalost	Finanční ztráta	6	3	4	72		Školení o správném zacházení	6	2	4	48
			Ztráta dat	5	3	4	60		Školení o správném zacházení	5	2	4	40
			Ušlý zisk	6	3	4	72		Školení o správném zacházení	6	2	4	48
	Poškození	Vloupání	Finanční ztráta	5	3	3	45	MZS, PZTS, kamerový systém se záznamem	Napojení kamer na SBS, posílení PZTS	5	2	2	20
			Ztráta dat	5	3	3	45	MZS, PZTS, kamerový systém se záznamem	Napojení kamer na SBS, posílení PZTS	5	2	2	20
			Ušlý zisk	6	3	3	54	MZS, PZTS, kamerový systém se záznamem	Napojení kamer na SBS, posílení PZTS	6	2	2	24
		Nedbalost	Finanční ztráta	4	4	4	64		Školení o správném zacházení	4	3	4	48
			Ztráta dat	5	4	4	80		Školení o správném zacházení	5	3	4	60
			Ušlý zisk	6	4	4	96		Školení o správném zacházení	6	3	4	72
		Sabotáž	Finanční ztráta	4	2	4	32		Zamezení fyzického přístupu k zařízení	4	2	3	24
			Ztráta dat	5	2	4	40		Zamezení fyzického přístupu k zařízení	5	2	3	30
			Ušlý zisk	6	2	4	48		Zamezení fyzického přístupu k zařízení	6	2	3	36
		Opotřebení	Finanční ztráta	4	2	4	32		Průběžná kontrola stavu	4	2	3	24
			Ztráta dat	5	2	4	40		Průběžná kontrola stavu	5	2	3	30
			Ušlý zisk	6	2	4	48		Průběžná kontrola stavu	6	2	3	36
	Odcizení	Vloupání	Finanční ztráta	6	3	3	54	MZS, PZTS, kamerový systém se záznamem	Napojení kamer na SBS, posílení PZTS	6	2	2	24
			Ztráta dat	5	3	3	45	MZS, PZTS, kamerový systém se záznamem	Napojení kamer na SBS, posílení PZTS	5	2	2	20
			Ušlý zisk	6	3	3	54	MZS, PZTS, kamerový systém se záznamem	Napojení kamer na SBS, posílení PZTS	6	2	2	24

IT technika	Odcizení	Vlastní obohacení	Finanční ztráta	6	3	7	126	Režim (prostory pouze pro zaměstance)	Zamezení fyzického přístupu k zařízení	6	2	6	72
			Ztráta dat	5	3	7	105	Režim (prostory pouze pro zaměstance)	Zamezení fyzického přístupu k zařízení	5	2	6	60
			Ušlý zisk	6	3	7	126	Režim (prostory pouze pro zaměstance)	Zamezení fyzického přístupu k zařízení	6	2	6	72
		Zlý úmysl	Finanční ztráta	6	2	6	72	Režim (prostory pouze pro zaměstance)	Zamezení fyzického přístupu k zařízení	6	2	5	60
			Ztráta dat	5	2	6	60	Režim (prostory pouze pro zaměstance)	Zamezení fyzického přístupu k zařízení	5	2	5	50
			Ušlý zisk	6	2	6	72	Režim (prostory pouze pro zaměstance)	Zamezení fyzického přístupu k zařízení	6	2	5	60
	Neoprávněné užití	Vlastní obohacení	Únik informací	6	2	2	24	Kontrola přístupu		6	2	2	24
			Únik citlivých informací	7	2	2	28	Kontrola přístupu		7	2	2	28
			Finanční ztráta	5	2	2	20	Kontrola přístupu		5	2	2	20
	Kybernetický útok	Nevědomost	Únik informací	6	3	6	108	Absence bezpečnostního školení o kybernetické bezpečnosti	Bezpečnostní školení o kybernetické bezpečnosti	6	2	4	48
			Únik citlivých informací	7	3	6	126	Absence bezpečnostního školení o kybernetické bezpečnosti	Bezpečnostní školení o kybernetické bezpečnosti	7	2	4	56
			Finanční ztráta	5	3	6	90	Absence bezpečnostního školení o kybernetické bezpečnosti	Bezpečnostní školení o kybernetické bezpečnosti	5	2	4	40
			Ztráta dat	5	3	6	90	Absence bezpečnostního školení o kybernetické bezpečnosti	Bezpečnostní školení o kybernetické bezpečnosti	5	2	4	40
Technika	Poškození	Nedbalost	Finanční ztráta	6	4	2	48	Školení o správném zacházení		6	4	2	48
			Ušlý zisk	7	4	2	56	Školení o správném zacházení		7	4	2	56
		Sabotáž	Finanční ztráta	6	2	2	24	Přítomnost pracovníků		6	2	2	24
			Ušlý zisk	7	2	2	28	Přítomnost pracovníků		7	2	2	28
		Zlý úmysl	Finanční ztráta	6	3	2	36	Přítomnost pracovníků		6	3	2	36
			Ušlý zisk	7	3	2	42	Přítomnost pracovníků		7	3	2	42
		Opotřebení	Finanční ztráta	6	4	2	48	Revize	Častější revize	6	3	2	36
			Ušlý zisk	7	4	2	56	Revize	Častější revize	7	3	2	42
	Zničení	Nedbalost	Finanční ztráta	7	3	2	42	Školení o správném zacházení		7	3	2	42
			Ušlý zisk	8	3	2	48	Školení o správném zacházení		8	3	2	48
		Sabotáž	Finanční ztráta	7	2	2	28	Přítomnost pracovníků		7	2	2	28
			Ušlý zisk	8	2	2	32	Přítomnost pracovníků		8	2	2	32
		Zlý úmysl	Finanční ztráta	7	3	2	42	Přítomnost pracovníků		7	3	2	42
			Ušlý zisk	8	3	2	48	Přítomnost pracovníků		8	3	2	48
	Odcizení	Vlastní obohacení	Finanční ztráta	7	1	2	14	MZS, PZTS, kamerový systém se záznamem	Napojení kamer na SBS, posílení PZTS	7	1	2	14
			Ušlý zisk	8	1	2	16	MZS, PZTS, kamerový systém se záznamem	Napojení kamer na SBS, posílení PZTS	8	1	2	16

Technika	Odcizení	Zlý úmysl	Finanční ztráta	7	1	2	14	MZS, PZTS, kamerový systém se záznamem	Napojení kamer na SBS, posílení PZTS	7	1	2	14
			Ušlý zisk	8	1	2	16	MZS, PZTS, kamerový systém se záznamem	Napojení kamer na SBS, posílení PZTS	8	1	2	16
Hotovost	Odcizení zaměstnancem	Vlastní obohacení	Finanční ztráta	5	2	5	50	Denní uzávěrka	Průběžné ukládání do trezoru/bezpečnostní schránky	5	2	3	30
			Ztráta zaměstance	5	2	5	50	Denní uzávěrka	Průběžné ukládání do trezoru/bezpečnostní schránky	5	2	3	30
		Příležitost	Finanční ztráta	5	2	5	50	Denní uzávěrka	Průběžné ukládání do trezoru/bezpečnostní schránky	5	2	3	30
			Ztráta zaměstance	5	2	5	50	Denní uzávěrka	Průběžné ukládání do trezoru/bezpečnostní schránky	5	2	3	30
	Odcizení bývalým zaměstancem	Vlastní obohacení	Finanční ztráta	5	2	4	40	Denní uzávěrka + odevzdání klíčů/čipů při odchodu	Průběžné ukládání do trezoru/bezpečnostní schránky + zabezpečení nouzových východů	5	2	2	20
		Příležitost	Finanční ztráta	5	2	4	40	Denní uzávěrka + odevzdání klíčů/čipů při odchodu	Průběžné ukládání do trezoru/bezpečnostní schránky + zabezpečení nouzových východů	5	2	2	20
		Pomsta	Finanční ztráta	5	2	4	40	Denní uzávěrka + odevzdání klíčů/čipů při odchodu	Průběžné ukládání do trezoru/bezpečnostní schránky + zabezpečení nouzových východů	5	2	2	20
	Odcizení zákazníkem	Vlastní obohacení	Finanční ztráta	5	3	4	60	Režim (prostory pouze pro zaměstance) + denní uzávěrka	Průběžné ukládání do trezoru/bezpečnostní schránky + zabezpečení nouzových východů	5	2	2	20
		Příležitost	Finanční ztráta	5	3	4	60	Režim (prostory pouze pro zaměstance) + denní uzávěrka	Průběžné ukládání do trezoru/bezpečnostní schránky + zabezpečení nouzových východů	5	2	2	20
		Pomsta	Finanční ztráta	5	3	4	60	Režim (prostory pouze pro zaměstance) + denní uzávěrka	Průběžné ukládání do trezoru/bezpečnostní schránky + zabezpečení nouzových východů	5	2	2	20
	Odcizení neznámou osobou	Vlastní obohacení	Finanční ztráta	5	2	3	30	Režim (prostory pouze pro zaměstance) + denní uzávěrka	Průběžné ukládání do trezoru/bezpečnostní schránky + zabezpečení nouzových východů	5	2	2	20

Hotovost	Odcizení neznámou osobou	Příležitost	Finanční ztráta	5	2	3	30	Režim (prostory pouze pro zaměstance) + denní uzávěrka	Průběžné ukládání do trezoru/bezpečnostní schránky + zabezpečení nouzových východů	5	2	2	20
	Přepadení	Vlastní obohacení	Finanční ztráta	5	1	4	20	Rozsáhlost objektu (někdo by si toho asi všiml)	Tísňové tlačítko	5	1	2	10
	Vloupání	Vlastní obohacení	Finanční ztráta	5	2	4	40	MZS, PZTS, kamerový systém se záznamem	Napojení kamer na SBS, posílení PZTS	5	2	3	30
		Příležitost	Finanční ztráta	5	2	4	40	MZS, PZTS, kamerový systém se záznamem	Napojení kamer na SBS, posílení PZTS	5	2	3	30
	Podvod	Falšené bankovky	Finanční ztráta	2	3	8	48	Kontrola pouze 5000 bankovek	Kontrola více druhů bankovek	2	3	3	18
Osobní věci	Odcizení	Vlastní obohacení	Finanční ztráta	2	5	6	60	MZS	Posílení MZS	2	3	4	24
		Příležitost	Finanční ztráta	2	5	6	60	MZS	Posílení MZS	2	3	4	24
		Pomsta	Finanční ztráta	2	4	6	48	MZS	Posílení MZS	2	3	4	24
Ostatní majetek	Zničení	Nedbalost	Finanční ztráta	3	2	3	18		Finanční postih	2	2	2	8
		Zlý úmysl	Finanční ztráta	3	2	3	18	MZS		3	2	3	18
	Poškození	Nedbalost	Finanční ztráta	2	3	3	18		Finanční postih	2	2	2	8
		Zlý úmysl	Finanční ztráta	2	3	3	18	MZS		2	3	3	18
	Odcizení	Příležitost	Finanční ztráta	3	3	3	27	MZS	Posílení MZS	3	2	2	12
		Vlastní obohacení	Finanční ztráta	3	3	3	27	MZS	Posílení MZS	3	2	2	12
		Zlý úmysl	Finanční ztráta	3	2	3	18	MZS	Posílení MZS	3	2	2	12

Obrázek 28. FMEA budovy emisní kontroly [vlastní]

5.5 Vyhodnocení analýzy

V případě zkoumaného objektu se všechna analyzovaná rizika pohybovala v rozmezí mírné úrovně škály. Z důvodu zájmu provozovatele rizika řešit bylo tedy nutné zavedení druhého škálování, které mělo za cíl rozdělit daný stupeň na další čtyři úrovně. Tyto úrovně lépe reprezentují rozdíly mezi jednotlivými mírami rizika. V potaz byly brány rizika I. úrovně, jejichž význam je pro objekt zanedbatelný. Naopak u rizik IV. stupně je stále důležité se danými riziky zabývat.

Tabulka 9. Zmenšená klasifikace míry rizika [vlastní]

Zmenšená klasifikace míry rizika		
Hodnocení	**Číselný rozsah**	**Barevné označení**
I.	0–49	
II.	50–99	
III.	100–149	
IV.	150–199	

5.6 Vyhodnocení budovy STK

Při vyhodnocování jsou zmíněny jednotlivé úrovně rizika, které se v analýze vyskytují. Následně byla tato rizika jednoduše pospána a shrnuta. Jelikož všechna analyzovaná rizika vycházela v nejnižším stupni škály analýzy, byla klasifikována za využití zmenšené škály pro tuto konkrétní úroveň tak, jak bylo popsáno výše.

5.6.1 Míra rizika IV.

Po zpracování analýzy pro tuto budovu je zřejmé, že se zde nevyskytují žádná rizika z kategorie IV. To je velice dobré znamení pro objekt, jelikož se zde nevyskytují žádná rizika, která je naprosto nezbytné řešit.

5.6.2 Míra rizika III.

Do III. míry rizik spadá pro tuto část analýzy celkem sedm rizik. Tato rizika je vhodné zpracovat a věnovat jim pozornost. Mohou totiž stále způsobovat nežádoucí následky, které by mohly ovlivnit chod a výdělečnost objektu. Je tak vhodné navrhnout adekvátní opatření, která dokážou jejich celkovou míru rizika snížit.

Nejvyšší hodnota RPN = 128 byla zjištěna u hrozby poškození s příčinou vandalismu u samotné budovy. Dopadem tohoto rizika by byla finanční ztráta. Samotná ztráta není příliš vysoká, jelikož budova je už postarší, každopádně stále je vzniklá škoda pro objekt znatelná. Zároveň výskyt byl zhodnocen tak, že hrozba občas nastane. Takové ohodnocení bylo založeno na zkušenosti z minulosti, poněvadž se párkrát stalo, že někdo budovu zvenčí poškodil, případně rozbil okna apod. Nejdůležitějším parametrem je v tomto případě odhalitelnost. Ta je velmi nízká, jelikož pachatele, který do areálu pronikne, nemá objekt ve většině případů jak detekovat.

Další skupinu obsáhly hrozby odcizení IT techniky. V těchto případech je především problematické, že velké množství počítačů jsou velmi malé pracovní stanice. Tyto stanice lze velmi snadno ukrást v nestřeženém okamžiku, a tím pádem se jedná o příčinu vlastního obohacení. To může mít za následky ztrátu dat, finanční ztrátu a ušlý zisk. V tomto případě způsobuje vysokou míru rizika kombinace faktorů významnosti a problematické odhalitelnosti. Tato aktiva jsou pro objekt významná, jelikož jsou nutná k jeho správnému chodu. Do této skupiny spadají dvě rizika úrovně RPN = 126. Jedná se o rizika finanční ztráty a ušlého zisku způsobené odcizením IT techniky. Řadí se zde i jedno riziko ztráty dat způsobené odcizením IT techniky s hodnotou RPN = 105.

Poslední hrozby, které spadají do tohoto stupně míry rizika, jsou kybernetické útoky směřující na IT techniku a data. Dějí se především v případech, kdy dopad způsobí únik informací a citlivých informací. Tento dopad je v tomto případě způsoben nevědomostí pracovníků, jelikož neprobíhá žádné školení zaměstnanců v oblasti kybernetické bezpečnosti. Nelze se tedy spoléhat, že případná hrozba bude včas detekována. V případě dat by mohl neopatrný krok zaměstnance poskytnout případnému pachateli přístupové údaje k serverům Ministerstva dopravy, kde se nacházejí soukromé informace nejen zákazníků zkoumaného STK. Jedná se o riziko úniku citlivých informací způsobené kybernetickým útokem na IT techniku s hodnotou RPN = 126, dále únik informací způsobený kybernetickým útokem na data s hodnotou RPN = 120. Nakonec zde patří únik informací způsobený kybernetickým útokem na IT techniku s hodnotou RPN = 105.

5.6.3 Míra rizika II.

Do II. stupně míry rizika se v této části analýzy řadí celkem 33 rizik. Tato rizika, neznamenají pro objekt příliš velké nebezpečí. Je ale vhodné o nich vědět a sledovat jejich vývoj,

jelikož mohou způsobit nežádoucí dopady na sledovaný objekt. Proto je žádoucí alespoň některá z těchto rizik regulovat.

Do hlavní skupiny rizik v tomto stupni spadají rizika působící na IT techniku z pohledu jejího poškození, zničení nebo odcizení. V rámci poškození a zničení se jedná především o příčinu nedbalosti způsobenou nesprávným zacházením. U hrozby odcizení je hlavní příčinou zlý úmysl, který sice není pravděpodobný, ale byl by složitě odhalitelný a zároveň je zde opět problém jednoduchosti přístupu a rozměrů těchto zařízení. V této skupině se nachází celkem devět rizik. Jedná se o riziko ušlého zisku u poškození z nedbalosti s hodnocením RPN = 96. Dále o riziko ztráty dat způsobené poškozením z nedbalosti s hodnotou RPN = 80. Následně dvě rizika finanční ztráty a ušlého zisku způsobené zničením z nedbalosti s hodnotami RPN = 72. Poté dvě rizika ušlého zisku a finanční ztráty způsobené odcizením s hodnotami RPN = 72. Dále jde o riziko finanční ztráty způsobené poškozením z nedbalosti s hodnotou RPN = 64. Následně riziko ztráty dat způsobené zničením z nedbalosti a riziko ztráty dat způsobené odcizením s hodnotami RPN = 60.

Další rizika, která se nacházejí v této úrovni, jsou ta, která působí na funkčnost a stabilitu internetové služby. Jedná se o hrozby výpadku a zpomalení internetu. Výpadek je především brán v případě poškození kabeláže, routeru nebo chyby ze strany poskytovatele. Hlavním dopadem je v tomto případě ušlý zisk, který je způsoben tím, že se dlouho čeká, zda internet bude znovu zapnut. Zároveň i po přechodu na offline režim nedokáže objekt vykonávat všechny své funkce. Toto riziko má hodnotu RPN = 90. U zpomalení internetu je příčina především použití nevhodného tarifu objektu, jehož rychlost omezuje pracovníky při efektivitě práce, a byla mu přidělena hodnota RPN = 96. Druhou příčinou je využívání internetu pro soukromé účely zaměstnanci a vyhodnocení odpovídá hodnotě RPN = 72. Dopadem této hrozby je snížení efektivity práce, a tím způsobení ušlého zisku.

Mezi jiná rizika spadající do tohoto stupně patří rizika působící na IT techniku a data způsobená kybernetickým útokem s příčinou nevědomosti. Jedná se případy, kdy dopady způsobí finanční ztráty a ztráty dat. U rizika působící na IT techniku s příčinami finanční ztráty a ztráty dat způsobených nevědomostí jsou hodnoty RPN = 90. V případě rizika poškození dat způsobeny nevědomostí je hodnota RPN = 90.

Dále se v objektu vyskytují také rizika působící na zaměstnance a zákazníky. Jedná se o hrozbu napadení způsobené jiným zaměstnancem nebo zákazníkem. Taková hrozba může mít za následek zranění zaměstnance a zákazníka, pracovní neschopnost nebo ztrátu

zaměstnance z důvodu jeho propuštění. Tato rizika se řadí do II. stupně především kvůli důležitosti významu pro objekt. Ohrožení zdraví má vysokou důležitost u všech objektů a pokud způsobí pracovní neschopnost zaměstnance, může se stát, že bude nutné přijmout pracovníka, který práci na určitý čas zastoupí. Ztráta zaměstnance je problematická, jelikož přijmutí a zaškolení nového pracovníka je jak časově, tak finančně náročné. Výskyt těchto rizik není nijak častý, ale zároveň není vyloučený, jelikož se v některých stanicích takové incidenty občas stávají. Zároveň je problém, že STK nemá žádné směrnice, případně školení o chování při napadení. Riziko zranění zaměstnance jiným zaměstnancem bylo vyhodnoceno hodnotou RPN = 80. Dále rizika pracovní neschopnosti a ztráty zaměstnance způsobené jiným zaměstnancem mají obě hodnotu RPN = 72. U zranění zaměstnance způsobeného zákazníkem je hodnota RPN = 60. V případě zranění zákazníka způsobeného zaměstnancem byla hodnota RPN = 84. Nakonec hodnoty RPN obou rizik zranění zákazníka způsobeného jiným zákazníkem a ztráta zákazníka způsobená napadením zaměstnancem jsou rovny 56.

Další jsou rizika působící na automobily nacházející se v areálu objektu. Hrozby, které se zde vyskytují, jsou zničení, poškození a odcizení automobilů. Zničení je bráno s příčinou žhářství nebo zlého úmyslu především po zavíracích hodinách. U příčiny vandalismu a zlého úmyslu u hrozby poškození je také předpokládáno provedení až v době, kdy se v areálu nikdo nevyskytuje. Hlavním problémem obou těchto příčin je, že objekt nemá téměř žádné prostředky, jak případného pachatele detekovat, a SBS je bez možnosti kontrolovat stav pomocí přítomného kamerového systému. Další hrozbou je odcizení způsobené krádeží klíčů během provozu objektu. Dopadem všech těchto možných rizik je především finanční ztráta způsobená na vozidle. Riziko finanční ztráty zničením automobilu ze zlého úmyslu má hodnotu RPN = 64. U rizika finanční ztráty zničení způsobeným žhářstvím je hodnota RPN = 56. V případě rizik finanční ztráty způsobené poškozením ze zlého úmyslu a vandalismu jsou hodnoty RPN = 54. Nakonec riziko finanční ztráty způsobené odcizením automobilu kvůli krádeži klíčů má hodnotu RPN = 60.

Mezi další rizika spadají ta, která působí na osobní věci zaměstnanců. Hrozbou, která zde působí, je odcizení daného majetku s příčinou vlastního obohacení a příležitostí. V těchto případech je dopadem finanční ztráta. Hlavním problémem je občasný výskyt a problematická odhalitelnost v kombinaci s nezamykáním šatny pro zaměstnance. V tomto případě se jedná o dvě zjištěná rizika finanční ztráty způsobené odcizením z důvodu vlastního obohacení a příležitosti. Obě tato rizika mají hodnotu RPN = 60.

Následně je nutno zmínit rizika působící na techniku stanice. Především se jedná o hrozbu poškození techniky s příčinou nedbalosti a opotřebení. U takových rizik je znatelná především velká významnost těchto aktiv. Při projevu tohoto poškození se velmi omezí provoz objektu, a tak dochází ke značnému ušlému zisku. Tato dvě rizika mají hodnotu RPN = 56.

Poslední skupinou jsou dvě rizika působící na hotovost, která se nachází v objektu. Jedná se o hrozbu odcizení zaměstnancem s příčinou vlastního obohacení a příležitosti. U obou rizik je hodnota RPN = 56. V této úrovni se nacházejí především pro potenciálně vysoký finanční význam a relativně jednoduchý přístup ke kase, kde se peníze ukládají.

5.6.4 Míra rizika I.

Do I. míry rizik spadá pro tuto část analýzy celkem 151 rizik. Jedná se tak o většinu zkoumaných rizik. Tato rizika nepředstavují pro objekt téměř žádnou významnou hrozbu, a proto s nimi není dále pracováno. Je však dobré vědět o jejich existenci a monitorovat jejich vývoj do budoucna.

5.7 Vyhodnocení budovy emisní kontroly

Při vyhodnocení druhé části analýzy jsou opět zmíněny jednotlivé stupně míry rizika podle zmenšené škály vysvětlené výše. Jednotlivá rizika tak byla stručně klasifikována a shrnuta.

5.7.1 Míra rizika IV.

I pro tuto druhou budovu je zřejmé, že obecně se zde nevyskytují žádná rizika, která by spadala do IV. stupně míry rizika. Opět se jedná o velice dobrou zprávu, jelikož ani zde se nevyskytují žádná rizika, kterým je nutno věnovat neodkladnou pozornost.

5.7.2 Míra rizika III.

Do III. stupně míry rizik je v případě analýzy této budovy zahrnuto devět rizik, tudíž o něco více než u předchozí budovy. Lze si ale povšimnout, že se jedná o podobná rizika jako u předešlé budovy. Tato rizika je opět vhodné sledovat a ideálně je regulovat. Je tak vhodné navrhnout adekvátní opatření pro jejich snížení.

Riziko s nejvyšší hodnotou RPN je pouze jedno, které působí na budovu s hodnotou 128. Jedná se o hrozbu poškození budovy způsobené vandalismem. Dopadem takové hrozby je především finanční ztráta. Hlavním důvodem vysokého čísla RPN je velice malá schopnost objektu tuto hrozbu odhalit.

Dále zde spadají rizika ohrožující IT techniku z pohledu jejího odcizení. Příčinou této hrozby je především vlastní obohacení. V tomto objektu je o to více znatelný problém, který se týká jednoduchosti, se kterou lze tyto počítače odcizit. Jelikož se jedná o objekt, kde se nevyskytuje příliš mnoho lidí, je zde velmi reálná hrozba, že někdo v nestřežený okamžik vnikne dovnitř, stanici odpojí a odcizí. Nefunkčnost vnitřních kamer a jejich namíření do země je také faktorem snižující bezpečnosti těchto aktiv. Hlavním důvodem vysoké hodnoty RPN je tedy opět problematická odhalitelnost v kombinaci s významem těchto zařízení pro chod objektu. V tomto případě se jedná o dvě rizika finanční ztráty a ušlého zisku způsobených odcizením z důvodu vlastního obohacení s hodnotou RPN = 126. Navíc zde existuje i riziko ztráty dat způsobené odcizením s hodnotou RPN = 105.

Další dvě důležitá rizika jsou opět rizika působící na IT techniku, které jsou tentokrát způsobené hrozbou kybernetického útoku. Tato hrozba má příčinu nevědomosti zaměstnanců, na kterou má vliv absence jakéhokoliv školení z oblasti kybernetické bezpečnosti. V případě úniku citlivých informací je hodnota RPN = 126. A úniku informací je hodnota RPN = 108. Důvodem vysokého čísla RPN je opět kombinace důležitosti chráněného aktiva s kombinací malé pravděpodobnosti odhalitelnosti, která je způsobena již zmíněnou absencí školení.

Poslední skupina, která byla klasifikována do střední míry rizik, obsahuje tři rizika spojená s hrozbou napadení zákazníků a zaměstnanců. Příčinou projevu těchto hrozeb je především napadení zákazníkem nebo jiným zaměstnancem. Ve všech případech v této skupině je dopadem zranění zaměstnance nebo zákazníka. Zařazení do této úrovně RPN je především způsobeno významem zdraví těchto osob s kombinací problematické odhalitelnosti, jelikož je zde nutno spoléhat na to, že si incidentu někdo včas všimne. Je také běžné, že například v prostoru skladu se pohybuje pouze jediný pracovník. Rizika zranění zákazníka způsobeného jiným zákazníkem nebo zaměstnancem byla vyhodnocena na hodnotu RPN = 105. Poté riziko napadení zaměstnance jiným zaměstnancem má hodnotu RPN = 100.

5.7.3 Míra rizika II.

V případě analýzy pro tuto budovu se do II. míry rizika řadí celkem 33 rizik. Tato rizika opět nepředstavují příliš velké ohrožení objektu. Přesto je vhodné tato rizika stanovit a monitorovat jejich stav.

Velkou skupinou jsou rizika působící na IT techniku, především z pohledu zničení, poškození a kybernetického útoku. U hrozby zničení a poškození je nejvýznamnější příčinou nedbalost, která může být způsobena například špatným zacházením se zařízeními. Hlavní

dopady jsou finanční ztráta, ztráta dat a ušlý zisk. Nejpodstatnějším dopadem je v tomto případě ušlý zisk, jelikož tato zařízení jsou nutná ke správnému chodu objektu. Z pohledu kybernetického útoku se jedná o podobný případ, který byl popsán výše, rozdílné zasazení je způsobeno nižším významem způsobených dopadů, kterými v tomto případě jsou finanční ztráta a ztráta dat. Rizika finanční ztráty a ušlého zisku způsobených zničením z nedbalosti mají hodnotu RPN = 72. Dále riziko ztráty dat způsobené zničením z nedbalosti má hodnotu RPN = 60. Následně rizika finanční ztráty i ušlého zisku způsobených zničením s příčinou vloupání mají hodnotu RPN = 54. Poté riziko ušlého zisku způsobené poškozením z nedbalosti má hodnotu RPN = 96. Riziko ztráty dat poškozením z nedbalosti bylo vyhodnoceno na hodnotu RPN = 80. Dále finanční ztráta způsobená poškozením z nedbalosti má hodnotu RPN = 64. Poté je zde riziko ušlého zisku poškozením způsobeného vloupáním s hodnotou RPN = 54. Hodnoty RPN = 90 dosahují rizika finanční ztráty a ztráty dat způsobených kybernetickým útokem kvůli nevědomosti zaměstnanců.

Další skupinou, která se v této úrovni vyskytuje, je pět rizik působících na IT techniku. V tomto případě se jedná ale především o hrozbu odcizení. Hlavní příčinou je zde zlý úmysl a vloupání. Umístění v tomto stupni RPN je způsobeno především velkým významem možných dopadů, které by se projevily především finanční ztrátou, ušlým ziskem a ztrátou uložených dat. Hodnot RPN = 72 dosahují rizika finanční ztráty a ušlého zisku způsobené odcizením ze zlého úmyslu. Dále riziko ztráty dat způsobené odcizením ze zlého úmyslu dosahuje hodnoty RPN = 60. Následně rizika finanční ztráty a ušlého zisku způsobených odcizením vloupáním mají hodnotu RPN = 54.

Mezi další rizika spadají ta, která ohrožují zaměstnance a zákazníky objektu. Hlavní hrozbou pro zmíněná aktiva je napadení, které může být způsobeno zákazníkem nebo jiným zaměstnancem. Hlavními dopady jsou pracovní neschopnost, ztráta zaměstnance, ztráta zákazníka nebo zranění. Podstatným problémem je, že z důvodu relativně malé koncentrace osob je menší šance, že si někdo takového incidentu stihne včas všimnout. Dalším faktorem je neznalost, jak se v takovém případě zachovat. V případě rizik pracovní neschopnosti a ztráty zaměstnance způsobené napadením jiným zaměstnancem je hodnota RPN = 90. U rizika zranění zaměstnance způsobené napadením zákazníkem je hodnota RPN = 75. Dále v případě způsobení pracovní neschopnosti zaměstnance způsobené napadením zákazníkem je hodnota RPN = 60. Poté u rizika ztráty zákazníka z důvodu napadení zaměstnancem je hodnota RPN = 70. Nakonec riziko ztráty zákazníka způsobená napadením jiným zákazníkem je hodnota RPN = 60.

Rizika působící na hotovost v objektu jsou další významnou skupinou, která se řadí do této úrovně. Jedná se především o působení hrozeb odcizení zaměstnancem a zákazníkem. Hlavními příčinami těchto hrozeb je především vlastní obohacení, příležitost a případně pomsta. Je nutno podotknout, že kromě hlavního dopadu finanční ztráty je zde také dopad ztráty zaměstnance z důvodu jeho propuštění. V tomto objektu se nenachází tak vysoká finanční hotovost jako v budově STK, ale je zde větší problém s detekcí takového incidentu, a navíc je velkým problémem ponechávání hotovosti na stolech. Nízká odhalitelnost je způsobena především povahou objektu i relativně nízkým výskytem osob. Tři rizika finanční ztráty, která jsou způsobena odcizením zákazníkem s příčinami vlastního obohacení, příležitosti a pomsty, mají hodnoty RPN = 60. Další rizika finanční ztráty a ztráta zaměstnance způsobené odcizením zaměstnancem z důvodu vlastního obohacení mají hodnotu RPN = 50. Stejné hodnoty RPN dosahují také rizika finanční ztráty a ztráta zaměstnance způsobené odcizením zaměstnance z důvodu příležitosti.

Následně je nutné zde zařadit také rizika ovlivňující osobní majetek zaměstnanců. Hlavní hrozbou je zde odcizení, jenž je zapříčiněno vlastním obohacením a příležitostí. V těchto případech je dopadem finanční ztráta. Problematický je občasný výskyt a nepravděpodobná odhalitelnost v kombinaci s nízkým pohybem osob a nezamykání prostoru šaten zaměstnanců. V tomto případě se jedná o dvě zjištěná rizika finanční ztráty způsobené odcizením s příčinou vlastního obohacení a příležitosti s hodnotami RPN = 60.

Poslední skupinou je skupina dvou rizik působících na techniku nacházející se uvnitř budovy. Hrozbou je především poškození, které může být způsobeno nedbalostí nebo opotřebením. Tato technika je nutná pro chod emisní kontroly, a proto její poškození má větší význam. Dopadem takového poškození by byl především ušlý zisk způsobený omezením funkčnosti dílny. Jedná se tedy o rizika ušlého zisku způsobený poškozením techniky s příčinami nedbalosti a opotřebením s hodnotou RPN = 56.

5.7.4 Míra rizika I.

V případě druhé části analýzy do I. míry rizik spadá celkem 80 rizik. To je podstatná část zkoumaných rizik. Tato rizika však nepředstavují pro objekt téměř žádnou významnou hrozbu, a proto s nimi není dále pracováno. Je však vhodné s danými riziky počítat a monitorovat jejich vývoj.

5.8 Závěr

V této kapitole byla určena použitá analýza rizik s popisem hodnotících faktorů a jejich klasifikace. Poté je užita také klasifikace míry rizika, se kterou analýza pracuje. Dále je zde samotná analýza a její následné vyhodnocení a zdůvodnění zmenšení škály pro hodnotu RPN. V rámci vyhodnocení jsou popsána jednotlivá zjištěná rizika a stručně shrnuty faktory, které jejich hodnocení nejvíce ovlivnily.

6 NÁVRHY OPATŘENÍ

Pro bezpečnostní posouzení bylo využito metody kontrolního seznamu a analýzy FMEA. Z obou těchto částí je zřetelné, že celková bezpečnost objektu je velmi dobrá. Všechna zkoumaná rizika vycházejí v nejnižší míře RPN. V objektu se ale i tak nacházejí nedostatky. Ty jsou na základě požadavků provozovatele řešeny dále v rámci obou návrhů opatření.

V této kapitole budou shrnuty návrhy opatření, které vyplynuly z vypracované analýzy rizik. Jedná se o opatření, která mají za cíl snížit celkové hodnocení RPN u rizik, která byla zařazena do II. a III. stupně. První návrh se bude zabývat pouze riziky spadajících do III. stupně RPN a bude tedy obsahovat odpovídající opatření. Druhý návrh následně doplňuje první návrh o další opatření s cílem snížení i těch rizik, která byla klasifikována do II. stupně RPN. Z důvodu zájmu provozovatele o realizování opatření byly při výběru opatření brány v potaz požadavky provozovatele. Daná opatření tak byla omezena z cenového hlediska i z hlediska přijatelnosti zaměstnanci. Z tohoto důvodu se mezi opatřeními nenachází například zavedení systému ESKV či rozsáhlejší kamerový systém ve vnitřních prostorách budov.

Seznam opatření vyplývajících z analýzy rizik:

- Oprava kamerového systému a jeho napojení a vzdálená kontrola budovy.
- Uzavírání počítačů do skříněk tak, aby je nebylo možné jednoduše odpojit a odnést.
- Zavedení školení o kybernetické bezpečnosti.
- Zavedení postupů, jak se chovat při napadení, a následné školení těchto postupů.
- Zavedení školení o správném zacházení s IT zařízeními a zavedení hmotné odpovědnosti.
- Vylepšení stávajícího tarifu internetu s rychlejším připojením.
- Zvážení zavedení softwarového blokování nežádoucích stránek.
- Posílení MZS v oblasti úschovných skříněk pro zaměstnance v obou budovách a zamykání prostor šaten.
- Zvážení instalace kamery, monitorující přístup ke kase v příjmu budovy STK.
- Zavedení postupného ukládání hotovosti do trezoru, případně pořízení bezpečnostní schránky nebo pokladny do budovy emisní kontroly.
- Zajištění nouzových dveří a zamykání vstupů.
- Posílení PZTS u budovy emisní kontroly.

V případě navýšení rozpočtu lze jako opatření zavést systém ESKV. Tento systém by dokázal snížit některá rizika, která jsou řešena jinými opatřeními. V tomto případě by systém ESKV měl být zaveden u následujících vstupů:

- Hlavní vstupy do budov.
- Vedlejší vstupy do budov.
- Vstupy do kanceláří.
- Vstupy do šaten.
- Vstup do archivních prostor.

Tento systém by mohl řešit problémy s jednodušším přístupem do budov a některých místností. Dále by poskytoval evidenci osob, které se v daném prostoru vyskytují, a byla by tak zvýšena odhalitelnost a snížen výskyt u některých rizik.

6.1 Varianta návrhu snižující rizika ve středním stupni RPN

První varianta má za cíl snížení rizik, která jsou pro objekt nejproblematičtější. Aplikují se zde pouze opatření, která v analýze rizik vykazovala snížení míry rizika minimálně do nižšího stupně. Neboli opatření, která snížila rizika ze stupně III. minimálně na stupeň II.

6.1.1 Oprava kamerového systému a jeho napojení, vzdálená kontrola budovy

Prvním navrhovaným opatřením je oprava kamerového systému a napojení na smluvenou SBS. Objekt má poměrně rozsáhlý kamerový systém s dobrým pokrytím areálu a zároveň má i nasmlouvaný dohled u SBS. Proto je vhodné provést důslednou kontrolu systému, vyměnit nefunkční kamery a zjistit přesnou příčinu vzniklé chyby v napojení a odstranit ji. Opětovným zpřístupněním vzdáleného přístupu je umožněno rychleji identifikovat případný výskyt hrozby nebo přítomnost narušitele v areálu. Takové rychlé jednání není při aktuálním stavu systému možné. Zároveň lze pomocí vzdálené kontroly eliminovat některé plané a falešné poplachy, které by jinak mohly vyústit v bezdůvodný výjezd pracovníků SBS. Je také vhodné umožnit vzdálený přístup přímo provozovateli objektu. Při této příležitosti je zároveň výhodné rozšířit smlouvu s SBS o pravidelnou kontrolu areálu pomocí kamerového systému, tím lze zamezit neočekávaným událostem, na které by se v jiném případě nemuselo stihnout včas přijít. Cena tohoto konkrétního opatření je složitá na vyčíslení, jelikož není zcela jasné, kde se konkrétní problém nachází a jakým způsobem se bude dát odstranit.

6.1.2 Zamezení fyzického přístupu k IT technice

Dalším opatřením spadajícím do tohoto návrhu je instalace zamykatelných skříněk, do kterých lze uzavřít počítače a jinou podobnou techniku. Tím by se mělo zamezit riziko volného přístupu k těmto přístrojům. Toto opatření by nijak neovlivnilo efektivitu práce nebo komfort zaměstnanců a poskytovalo by větší ochranu IT techniky před mechanickým poškozením nebo odcizením. Výhodou je, že zaměstnanci přístup k samotným počítačům nepotřebují, jelikož k práci potřebují pouze myš, monitor a přístup k internetu, případně propojení s tiskárnou. Pro potřeby stanice by se cena tohoto kroku pohybovala v nízkých desetitisících Kč.

6.1.3 Školení v oblasti kybernetické bezpečnosti

Jako další součást návrhu je zajištění školení pro zaměstnance v oblasti kybernetické bezpečnosti. Toto opatření je čistě zaměřeno na edukaci pracovníků. Z důvodu povahy práce zaměstnanců a propojenosti systému je důležité vzdělávat pracovníky o rizicích spojených s online prostředím. Především by se mělo jednat o školení zaměřené na rozpoznávání falešných e-mailů a jiné online komunikace. Dále by také mělo obsahovat základní zásady, kterými by se zaměstnanci měli v kyberprostoru řídit. Například se může jednat o zásadu nepřihlašování se přes podezřelé odkazy z e-mailů, nestahovat podezřelý software apod. Mělo by také obsahovat zákaz přihlašování se do soukromých emailů na firemních zařízeních. Toto opatření lze dále rozvinout opatřením v druhém návrhu, které se zaměřuje na blokaci nežádoucích stránek a softwaru. Cena takových školení se pohybuje v nízkých desetitisících Kč.

6.1.4 Zavedení postupů, jak se chovat při napadení, a následné školení

Následujícím opatřením je zavedení správných postupů chování při napadení a při vyskytnutí vypjaté situace. Mělo by se především jednat o soubor zásad, kterými by pracovník měl zvládat předvídat možnou eskalaci situace a naučit se základní způsoby, jak vyostření situace předcházet. Může se tak jednat především o školení metod v oblasti komunikace s agresorem. Případně také způsoby, jak se zachovat, pokud se incident začíná eskalovat v prostředí, kde se nenachází žádný další spolupracovník. Náklady na zpracování těchto zásad a následné školení zaměstnanců v této problematice se může pohybovat v nižších desetitisících Kč.

6.1.5 Shrnutí prvního návrhu

Výše zmíněná opatření snižují všechna zjištěná rizika ze střední míry. Celková cena všech těchto opatření se může pohybovat kolem 80 tisíc Kč. Samozřejmě daná cena se může lišit využitím vlastních zdrojů nebo již případně nasmlouvaných firem.

Opatření, které zabezpečuje nejvíce z těchto rizik, je fyzické zabezpečení IT zařízení z pohledu jejich přístupnosti. Toto opatření snižuje míru u šesti středně závažných rizik. Následuje opatření zaměřené na školení o kybernetické bezpečnosti, které snižuje pět rizik.

Dále je nutné stanovit, že tato opatření snižují rizika také v nízkém stupni míry rizika. Konkrétně opatření zavádějící postupy, jak se chovat při napadení, snižuje čtrnáct těchto rizik. Následně opatření navrhující opravu kamerového systému snižuje deset rizik z této kategorie.

6.2 Varianta návrhu snižující rizika v nízkém stupni RPN

Druhá varianta má za cíl doplnění první varianty. Dále je cílem snížení i těch rizik, která pro objekt nemají takový význam, ale i tak je vhodné je regulovat. Aplikují se zde opět pouze opatření, která v analýze rizik vykazovala snížení míry rizika minimálně o jeden stupeň. Neboli opatření, která snížila rizika ze stupně II. do stupně I.

6.2.1 Školení v oblasti zacházení s IT technikou a zavedení hmotné odpovědnosti

V rámci návrhu by mělo být obsaženo základní školení o zacházení s IT zařízeními. Toto školení by mělo obsahovat zásady chování k danému zařízení a postupy směřující k vyřešení případného problému se zařízením. Mělo by se tedy jednat především o školení z pohledu mechanického zacházení a osobnímu přístupu k zařízením. Tento krok lze realizovat i formou základního poučení zaměstnanců, které může provést například příslušný pracovník firmy v oblasti IT. Po tomto školení je nutné zavést hmotnou odpovědnost a každý zaměstnanec, který se nebude školením řídit, bude zodpovídat za vzniklé škody. Tím lze také udržet náklady v řádu maximálně několika tisíc Kč.

6.2.2 Posílení rychlosti internetu v objektu

Mezi další opatření spadá také posílení rychlosti internetu v objektu. Jedná se o relativně malou částku, díky které by se měl odstranit poměrně častý problém s rychlostí připojení. Jedná se o důležitý bod návrhu, jelikož je objekt na funkčnosti internetového připojení značně závislý. Cenově se tato položka pohybuje v řádu vyšších stovek Kč.

6.2.3 Softwarové blokování nežádoucích stránek

Jakožto další opatření je vhodné zvážení zavedení softwarového blokování některých stránek na firemních zařízeních. Toto opatření rozvíjí dříve zmíněné opatření navrhující školení o kybernetické bezpečnosti. Hlavním účelem je zamezení zpomalení internetu sledováním filmů nebo stahováním různých souborů. Toto opatření může provést i firemní pracovník pro oblast IT, který má k potřebnému softwaru přístup, a je teda pouze nutné uvést toto opatření v platnost, případně vymezit konkrétní rozsah takového omezení.

6.2.4 Posílení MZS v oblasti zabezpečení skřínek a zamykání prostorů šaten

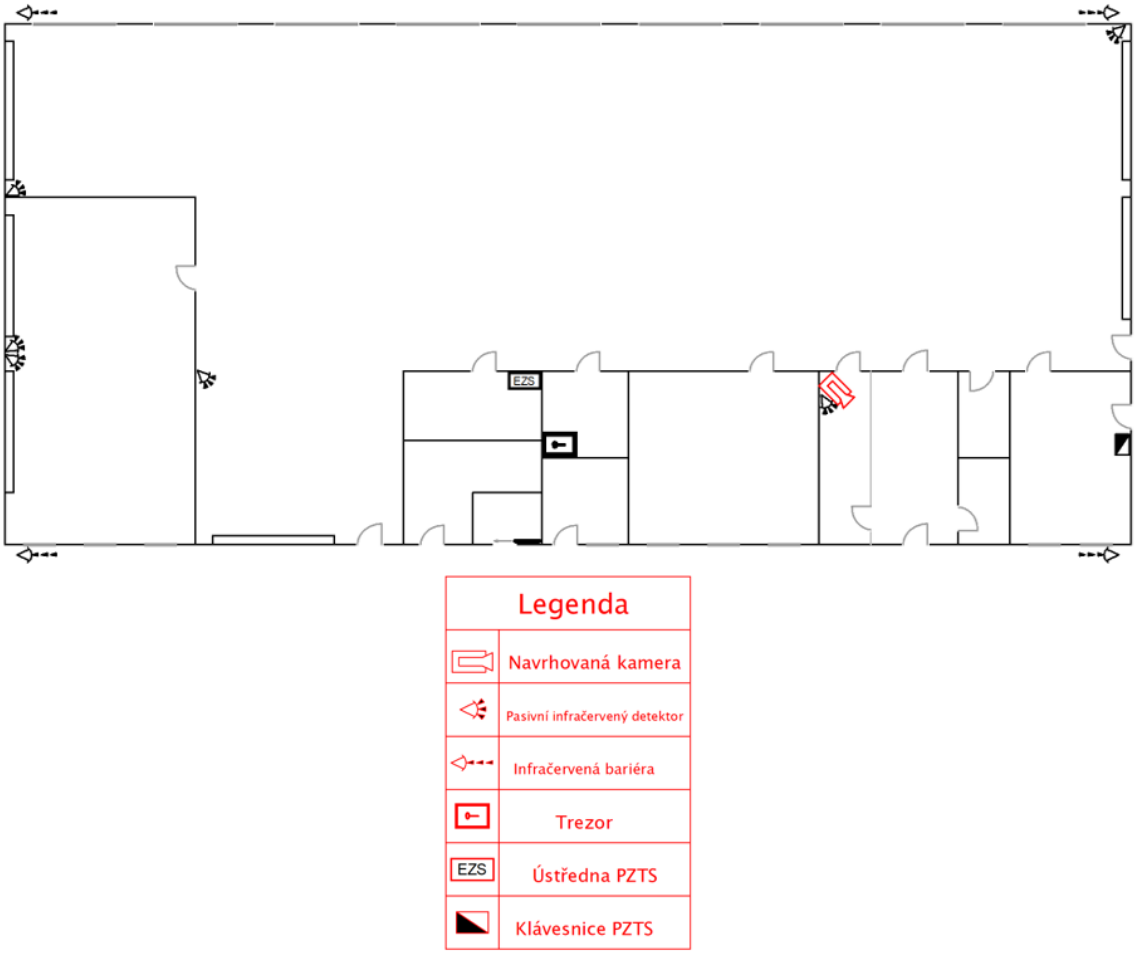
Mezi další navrhovaná opatření spadá použití odolnějších zámků na šatních skříních s osobními věcmi zaměstnanců. Použitím kvalitnějších zámků lze snížit pravděpodobnost jejich prolomení. Navíc je nutné využívat možnosti zamykání místností šaten. Tato část návrhu by stála přibližně 5000 Kč.

6.2.5 Instalace kamery do místnosti příjmu v budově STK

Opatření, které je dále nutno zvážit, je instalace kamery do prostor příjmu budovy STK. Pomocí této kamery by bylo možné efektivně sledovat přístup pracovníků do kasy s hotovostí. Je tak ideálním preventivním prvkem, který odradí případného pachatele od odcizení hotovosti přímo z dané kasy. Pro tyto potřeby je dostačující relativně malá kamera, která nepotřebuje velký dosah. Jedna z možných kamer, které lze v tomto případě použít, je DS-2CD2126G2-ISU(4MM) od firmy HIKVISION. Samozřejmě je možné použít i jinou kameru, která bude vyhovovat danému využití a bude kompatibilní s již fungujícím systémem.

Obrázek 29. Navrhovaná kamera [15]

Z důvodu přehlednosti je na obrázku umístění kamery zvětšeno a vyznačeno červenou barvou.



Obrázek 30. Umístění navrhované kamery [vlastní]

Parametry navrhnuté kamery:

- 1/2,8“ CMOS čip Progressive Scan.
- Objektiv 4 mm s úhlem záběru 86° horizontálně, 47° vertikálně a 102° diagonálně.
- Rozlišení Full HD.
- Možnost IR přísvitu s dosahem 30 m.
- WDR kompenzace protisvětla (120 dB).
- 3 nezávislé streamy.
- Alarmové funkce (tamper, detekce odpojení ze sítě, konflikt IP adres, neoprávněný přístup, plný HDD, chyba HDD).
- SMART funkce (zachycení tváře, detekce pohybu, překročení linie, detekce vystoupení z oblasti, filtr falešných poplachů).

- Rozměry 121 x 92 mm.
- Váha 585 g.
- Napájení 0,45 A a 5,4 W nebo 0,2 A–0,1 A a 6,5 W [15].
- Cena přibližně 5000 Kč.

6.2.6 Pořízení pokladny a průběžné ukládání hotovosti v budově emisní kontroly

Následným opatřením je pořízení pokladny do budovy emisní kontroly. Tato pokladna bude sloužit pro průběžné ukládání hotovosti v průběhu pracovní doby. Na večerní hodinu bude tato hotovost uložena do již přítomného trezoru. Pro tyto potřeby je dostačující relativně malá přenosná pokladna. Ta umožní zaměstnancům jednoduchý a komfortní způsob, jak udržovat hotovost v bezpečí, a eliminuje potřeby volně peníze odkládat z pouhé pohodlnosti. Pokladna, která vyhovuje těmto kritériím, je například příruční pokladna Cash SR 5 od výrobce Rottner Tresor. [16] Cena této konkrétní pokladny je přibližně 800 Kč. Následně je nutné průběžně kontrolovat dodržování postupného ukládání hotovosti a případné nedodržování by mělo být finančně sankciováno.

Obrázek 31. Navrhovaná příruční pokladna [16]

6.2.7 Zajištění nouzových dveří budovy emisní kontroly a zamykání dalších vstupů

V tomto opatření je pouze řešeno nedodržování režimových opatření objektu. Konkrétně se jedná o neuzamykání některých bočních vchodů v budově emisní kontroly. Pro případ, že tyto vchody mají sloužit také jako nouzové východy, je navrhnuta výměna zámků na těchto dveřích. Měl by být vybrán adekvátní panikový zámek, který odpovídá příslušným normám.

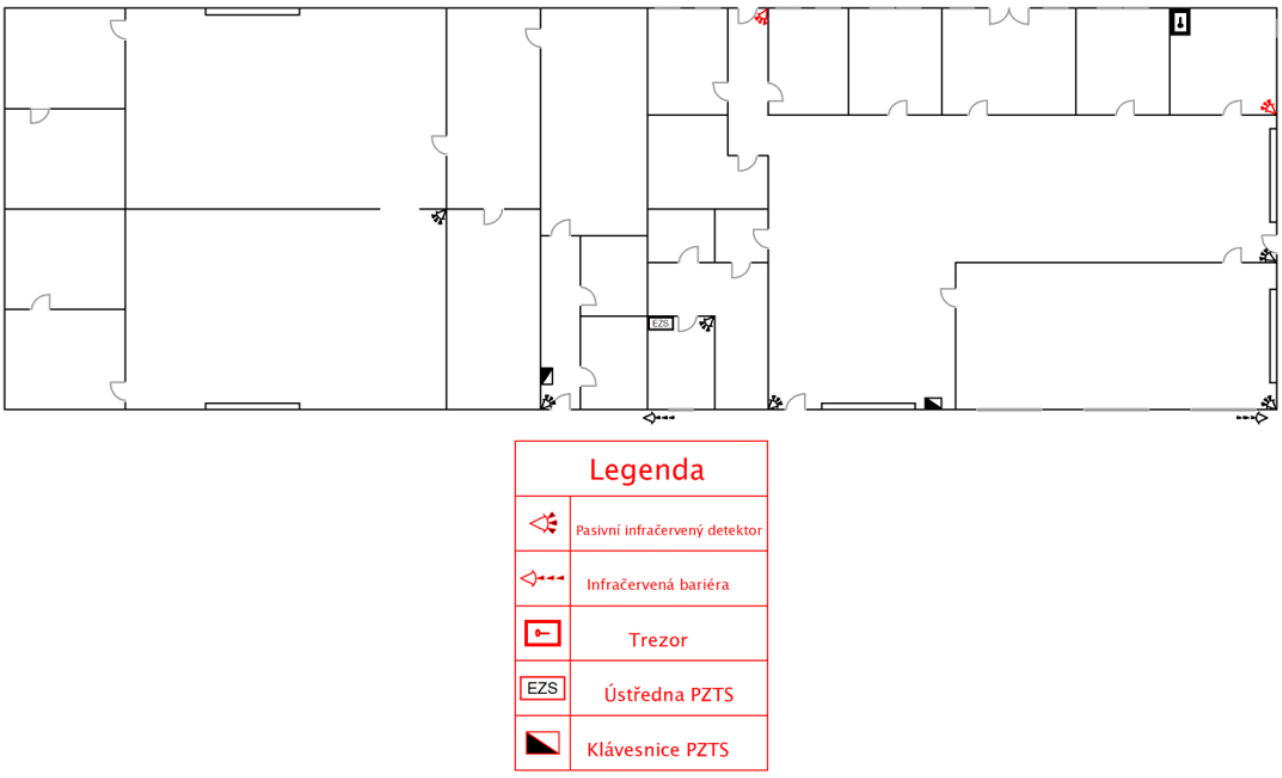
6.2.8 Posílení PZTS budovy emisní kontroly

Jakožto poslední opatření v rámci tohoto návrhu je posílení PZTS zmíněné budovy, které má za cíl zvýšit pravděpodobnost detekce narušitele mimo pracovní dobu. Tohoto posílení lze docílit několika způsoby. Bylo však vybráno přidání dvou PIR detektorů. Jeden je navržen k zadnímu východu budovy. Umístění druhého je navrhováno do kanceláře vedoucího,

Obrázek 32. Navrhovaný PIR detektor [17]

kde se nachází také trezor. V rámci zajištění kompatibility aktuálního zabezpečení je pro tyto potřeby vybrán digitální PIR detektor LC-100IP od výrobce DSC.

Z důvodu přehlednosti je na obrázku umístění PIR detektorů vyznačeno červenou barvou.



Obrázek 33. Umístění navrhovaných PIR detektorů [vlastní]

Parametry navrženého PIR detektoru:

- Typ snímače – čtyřnásobný PIR.
- Dosah – vějíř, 15x20 m.
- Stupeň zabezpečení 2.
- Montážní výška 2,4 m.
- Funkce – tamper kontakt a PET imunita.
- Napájení 9,6 až 16 V s odběrem 8 až 10 mA [17].
- Cena přibližně 300 Kč za kus.

6.2.9 Shrnutí druhého návrhu

Výše zmíněná opatření jsou přidána k opatřením z předchozího návrhu. Tato opatření snižují zjištěná rizika z nízké míry, které lze ovlivnit. Celková cena všech těchto nově zmíněných opatření je přibližně 27 tisíc Kč. Samozřejmě daná cena se může lišit využitím vlastních zdrojů nebo úpravou doporučených opatření.

Opatření, které snižuje nejvíce rizik z nízkého stupně míry rizika, je návrh školení o zacházení s IT technikou. Toto opatření snižuje jedenáct rizik dané kategorie. Následují opatření jsou zaměřena na pořízení pokladny a zajištění nouzových východů u budovy emisní kontroly. Tato opatření byla navrhována společně, a proto každé přispívá ke snížení sedmi rizik.

6.3 Závěr

V rámci této kapitoly byla popsána jednotlivá navržená opatření. Tato opatření byla rozdělena do dvou návrhů z pohledu rizik, která mají snižovat. V rámci prvního návrhu byla navržena opatření, která redukují rizika ve III. stupni RPN. Tato opatření by tak měla být pro objekt nejpodstatnější. U druhého návrhu je doplněn první návrh tak, ať snižuje rizika také ve II. stupni. Opatření, která se zde nacházejí, nejsou pro objekt tak důležité, ale je vhodné jejich zavedení minimálně zvážit.

ZÁVĚR

Při provádění bezpečnostního posouzení je důležité identifikovat a správně vyhodnotit všechna rizika. Jen tehdy lze určit, jaká rizika je nutné snížit a která nepředstavují pro objekt citelnou hrozbu. Je tedy žádoucí použití metod, které jsou vhodné pro identifikaci slabých míst, potenciálních rizik a které vhodně poslouží pro jejich vyhodnocení.

Cílem bakalářské práce bylo provedení bezpečnostního posouzení. Následným výstupem práce je navržení opatření, která budou vycházet z provedeného posouzení. Tyto návrhy tedy snižují míry rizik, která se v objektu vyskytují a byla analýzou rizik vyhodnocena jako důležitá.

Teoretická část práce v první kapitole popisuje základní terminologické pojmy, které jsou pro tuto bakalářskou práci nezbytné. Jsou tak popsány pojmy jako aktivum, hrozba, riziko a bezpečnostní opatření. Druhá kapitola teoretické části se zabývá přiblížením procesu řízení rizik a jeho hlavních fází. Součástí této kapitoly je také stručný popis typů metod, se kterými se lze v oblasti řízení rizik setkat. Především jsou popsány metody použité v praktické části práce. Jedná se tak o metodu kontrolního seznamu a FMEA.

Praktická část je nejdříve zaměřena na popis objektu jako celku i jeho jednotlivých částí. Je zde také jednoduše popsána kriminalita v okolí objektu a jeho návštěvnost. Tento popis je doplněn o nákresy, které mají pomoci lepší charakterizaci jednotlivých budov a jejich vzájemnému rozpoložení. Dále jsou identifikována aktiva objektu a je vyhodnocena jejich přibližná cena, která je stanovena na 16,6 milionů Kč.

Následující kapitola zkoumá aktuální stav zabezpečení objektu. Tento stav byl zjišťován fyzickou ohlídkou objektu, rozhovory se zaměstnanci a využitím kontrolního seznamu. Tato kapitola je doplněna fotografiemi, které byly pořízeny při obhlídce objektu. V závěru kapitoly je provedeno vyhodnocení zjištěných nedostatků.

Pátou kapitolou je samotné provedení analýzy rizik. Tato analýza byla provedena za využití metody FMEA, která byla pro tyto účely upravena. V kapitole jsou také vysvětleny jednotlivé hodnotící faktory a jejich klasifikace do jednotlivých škál. Vyhodnocení analýzy je popsáno z pohledu jednotlivých zjištěných stupňů rizik u každé z budov. Celkem je zjištěno 313 rizik. Z toho žádná rizika nespadají do stupně IV. 16 rizik patří do stupně III. a 66 rizik odpovídá stupni II. Zbylých 231 rizik je zařazeno do stupně I.

Poslední kapitola popisuje konkrétní návrhy bezpečnostních opatření. V úvodu kapitoly jsou jednoduše shrnuta všechna opatření, která vycházejí z předchozí analýzy. Tato opatření byla následně rozdělena do dvou návrhů. Cílem prvního návrhu bylo snížení nejzávažnějších rizik, která byla v objektu zjištěna. První návrh obsahuje pět opatření, jejichž zavedení by stálo přibližně 80 tisíc Kč. Účelem druhého návrhu bylo doplnění prvního návrhu o opatření, která sníží navíc i druhou nejvyšší skupinu rizik. V druhém návrhu je obsaženo osm opatření s přibližnou cenou 27 tisíc Kč.

Tato bakalářská práce byla předložena posuzovanému objektu. Ten ji využívá pro seznámení se s jednotlivými riziky a závěry práce budou využity pro zavedení některých navrhovaných opatření po projednání s vyšším vedením.

Závěrem je nutno zmínit, že problematika bezpečnostního posouzení v oblasti řízení rizik je náročné a komplexní téma. Práce však obsahuje velké množství informací takovým způsobem, aby co nejlépe obsáhla všechny možné hrozby, které daný objekt mohou ohrozit. Byla limitována především poskytnutými podklady a skutečností, že se v průběhu času mohou vyskytovat nové hrozby. Tato práce může také sloužit jako vhodný podklad při vypracovávání dalších bezpečnostních posouzení podobných objektů. Je také důležité podotknout, že řízení rizik je opakující se proces, takže je nutné bezpečnostní posouzení provádět opakovaně. Mělo by být také provedeno v případě, že se ve sledované oblasti vyskytnou nové technologie, skutečnosti nebo jiné okolnosti, které mohou bezpečnost organizace ovlivnit.

SEZNAM POUŽITÉ LITERATURY

[1] Terminologický slovník – krizové řízení a plánování obrany státu. *Ministerstvo vnitra České republiky* [online]. Praha: Odbor bezpečnostní politiky a prevence kriminality, c2022, 8. června 2016 [cit. 2022-11-25]. Dostupné z: https://www.mvcr.cz/clanek/terminologicky-slovnik-krizove-rizeni-a-planovani-obrany-statu.aspx.

[2] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích.* 4., aktualiz. a rozš. vyd. Praha: Grada, 2013. Expert (Grada). ISBN 9788024746449.

[3] KOTKOVÁ, Dora. *Krizové plánování a řízení, Řízení rizik.* Zlín, 2022. Přednáška pro studenty oboru BTSM. [cit. 2022-11-29].

[4] IVANKA, Ján. *Systemizace bezpečnostního průmyslu.* Digitální knihovna UTB [online]. Zlín: UTB, 2014 [cit. 2022-11-27]. Dostupné z: https://digilib.k.utb.cz/bitstream/handle/10563/27488/Systemizace_bezpecnostniho_prumyslu.pdf?sequence=1&isAllowed=y.

[5] VALOUCH, Jan. *Projektování integrovaných systémů* [online]. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013 [cit. 2023-05-15]. ISBN 978-80-7454-296-1. Dostupné z: https://digilib.k.utb.cz/bitstream/handle/10563/25814/Skripta%20-%20Valouch.pdf?sequence=1&isAllowed=n.

[6] KOUDELKA, Ctirad. *Rizika a jejich analýza.* VŠB Technická univerzita Ostrava [online]. Ostrava: Vysoká škola Báňská – Technická univerzita Ostrava, c2022, 2006 [cit. 2022-11-25]. Dostupné z: http://fei1.vsb.cz/kat420/vyuka/Magisterske%20nav/prednasky/web/RIZIKA.pdf.

[7] BUŘITA, Ladislav. *Prognostické metody a jejich využití v resortu obrany.* Obrana a strategie [online]. Obrana a strategie, 2003, 2003(1), 47-60 [cit. 2022-11-25]. ISSN 1802-7199. Dostupné z: doi:10.3849/1802-7199.

[8] BERNATÍK, Aleš. *Analýza nebezpečí a rizik.* VŠB Technická univerzita Ostrava [online]. Ostrava: Vysoká škola Báňská – Technická univerzita Ostrava, c2022, 2016 [cit. 2022-11-25]. Dostupné z: https://www.fbi.vsb.cz/export/sites/fbi/cs/.content/galerie-souboru/U3V/studijni-materialy/U3V_Analyza_nebezpeci_a_rizik.pdf.

[9] ČSN EN IEC 31010. *Management rizik – Techniky posuzování rizik.* 2nd ed. Praha: Česká agentura pro standardizaci, 2020, 116 s.

[10] Analýza rizik. *Guard7* [online]. Pardubice, 2022, 27. 6. 2022 [cit. 2023-05-15]. Dostupné z: https://www.guard7.cz/analyza-rizik/.

[11] Mapa kriminality. *Policie České republiky* [online]. Praha, c2023 [cit. 2023-05-15]. Dostupné z: https://kriminalita.policie.cz.

[12] ČESKÁ REPUBLIKA. *Zákon o některých přestupcích.* In: Sbírka zákonů. Praha: Ministerstvo vnitra, 2016, ročník 2016, částka 98, číslo 251. Dostupné také z: https://www.zakonyprolidi.cz/cs/2016-251.

[13] Návštěvnost STK XY. *Google* [online]. [cit. 2022-12-15]. Dostupné z: https://www.google.com/.

[14] Inventura majetku: Stav majetku střediska XY. XY, 2022.

[15] DS-2CD2126G2-ISU(4MM). In: *HIKVISION* [online]. Tišice, c2023 [cit. 2023-05-15]. Dostupné z: https://www.kamery-hikvision.cz/dome-kamery/8727-ds-2cd2126g2-isu4mm-2mpix-ip-dome-acusense-kamera-ir-30m-audio-alarm-ip67-ik10-mikrofon-6941264039211.html.

[16] Příruční pokladna Cash SR5. In: *Trezor.cz* [online]. Brno, c2023 [cit. 2023-05-15]. Dostupné z: https://www.trezor.cz/trezory/prirucni-pokladna-cash-box-sr-5-detail.html.

[17] LC-100-PI. In: *KELCOM* [online]. Hradec Králové, c1991-2023 [cit. 2023-05-15]. Dostupné z: https://www.kelcom.cz/dsc-lc-100-pi-205.html.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ESKV Elektronické systémy kontroly vstupu

FMEA Analýza příčin a následků poruch

FO Fyzická ostraha

IR Infračervené

IT Informační technologie

MZS Mechanické zábranné systémy

PIR Pohybový detektor

PZTS Poplachové zabezpečovací a tísňové systémy

RPN Rizikové číslo

SBS Soukromá bezpečnostní služba

STK Stanice technické kontroly

SEZNAM OBRÁZKŮ

SEZNAM TABULEK