Posouzení rizik ve vybrané organizaci

Lucie Podborská

Bakalářská práce
2017

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav krizového řízení
akademický rok: 2016/2017

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

Jméno a příjmení:	**Lucie Podborská**
Osobní číslo:	**L14355**
Studijní program:	**B3909 Procesní inženýrství**
Studijní obor:	**Ovládání rizik**
Forma studia:	**kombinovaná**

Téma práce: **Posouzení rizik ve vybrané organizaci**

Zásady pro vypracování:

1. **Teoretické vymezení pojmů souvisejících s danou problematikou.**
2. **Stručné představení organizace.**
3. **Analýza a charakteristika bezpečnostních rizik ve vybrané organizaci.**
4. **Návrh opatření vedoucích k eliminaci rizik.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

[1] SMEJKAL, Vladimír a Karel RAIS. Řízení rizik ve firmách a jiných organizacích. 4., aktualiz. a rozš. vyd. Praha: Grada, 2013, 483 s. Expert. ISBN 978-80-247-4644-9.

[2] HNILICA, Jiří a Jiří FOTR. Aplikovaná analýza rizika ve finančním managementu a investičním rozhodování. Praha: Grada, 2009, 262 s. Expert. ISBN 978-80-247-2560-4.

[3] ŠEFČÍK, Vladimír. Analýza rizik. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009, 98 s. ISBN 978-80-7318-696-8.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **prof. Ing. Jiří Dvořák, DrSc.**
Ústav krizového řízení

Datum zadání bakalářské práce: **3. února 2017**

Termín odevzdání bakalářské práce: **15. května 2017**

V Uherském Hradišti dne 20. února 2017

doc. RNDr. Jiří Dostál, CSc.
děkan

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta logistiky a krizového řízení

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

PROHLÁŠENÍ AUTORA
BAKALÁŘSKÉ PRÁCE

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

V Uherském Hradišti 15.5.2017

.....
podpis studenta

1) zákon č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, § 47b Zveřejňování závěrečných prací:

(1) Vysoká škola nevýdělečně zveřejňuje bakalářské, diplomové, disertační a rigorózní práce, u kterých proběhla obhajoba, včetně posudků oponentů a výsledku obhajoby prostřednictvím databáze kvalifikačních prací, kterou spravuje. Způsob zveřejnění stanoví vnitřní předpis vysoké školy. Vysoká škola disertační práce nezveřejňuje, byla-li již zveřejněna jiným způsobem.

(2) Bakalářské, diplomové, disertační a rigorózní práce odevzdané uchazečem k obhajobě musí být též nejméně pět pracovních dnů před konáním obhajoby zveřejněny k nahlížení veřejnosti v místě určeném vnitřním předpisem vysoké školy nebo není-li tak určeno, v místě pracoviště vysoké školy, kde se má konat obhajoba práce. Každý si může ze zveřejněné práce pořizovat na své náklady výpisy, opisy nebo rozmnoženiny.
(3) Platí, že odevzdáním práce autor souhlasí se zveřejněním své práce podle tohoto zákona, bez ohledu na výsledek obhajoby.

(4) Vysoká škola může odložit zveřejnění bakalářské, diplomové, disertační a rigorózní práce nebo jejich části, a to po dobu trvání překážky pro zveřejnění, nejdéle však na dobu 3 let. Informace o odložení zveřejnění musí být spolu s odůvodněním zveřejněna na stejném místě, kde jsou zveřejňovány bakalářské, diplomové, disertační a rigorózní práce, jíž se týká odklad zveřejnění podle věty první, jeden výtisk práce k uchování ministerstvu.
2) zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, § 35 odst. 3:
(3) Do práva autorského také nezasahuje škola nebo školské či vzdělávací zařízení, užije-li nikoli za účelem přímého nebo nepřímého hospodářského nebo obchodního prospěchu k výuce nebo k vlastní vnitřní potřebě dílo vytvořené žákem nebo studentem ke splnění školních nebo studijních povinností vyplývajících z jeho právního vztahu ke škole nebo školskému či vzdělávacího zařízení (školní dílo).
3) zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, § 60 Školní dílo:
(1) Škola nebo školské či vzdělávací zařízení mají za obvyklých podmínek právo na uzavření licenční smlouvy o užití školního díla (§ 35 odst. 3). Odpírá-li autor takového díla udělit svolení bez vážného důvodu, mohou se tyto osoby domáhat nahrazení chybějícího projevu jeho vůle u soudu. Ustanovení § 35 odst. 3 zůstává nedotčeno.
(2) Není-li sjednáno jinak, může autor školního díla své dílo užít či poskytnout jinému licenci, není-li to v rozporu s oprávněnými zájmy školy nebo školského či vzdělávacího zařízení.
(3) Škola nebo školské či vzdělávací zařízení jsou oprávněny požadovat, aby jim autor školního díla z výdělku jím dosaženého v souvislosti s užitím díla či poskytnutím licence podle odstavce 2 přiměřeně přispěl na úhradu nákladů, které na vytvoření díla vynaložily, a to podle okolností až do jejich skutečné výše; přitom se přihlédne k výši výdělku dosaženého školou nebo školským či vzdělávacím zařízením z užití školního díla podle odstavce 1.

ABSTRAKT

Bakalářská práce je zaměřena na posouzení bezpečnostních rizik v organizaci ABC. Práce se dělí na dvě části – teoretickou a praktickou. Teoretická část se věnuje charakteristice pojmů souvisejících s danou problematikou (riziko, bezpečnost a ochrana zdraví při práci, organizace a analýza rizik).

Praktická část se zabývá stručným uvedením organizace, analýzou současné situace organizace a jejími bezpečnostními riziky. Závěr práce je věnován vyhodnocení analýzy rizik a návrhy opatření ke snížení citovaných rizik.

Klíčová slova: riziko, bezpečnost, organizace, analýza rizik.

ABSTRACT

The bachelor thesis is focused on the evaluation of security risks in the ABC organization. The thesis is divided into two parts - theoretical and practical. The theoretical part focuses on characteristics related to the given subject (risk, safety and health at work, organization and risk analysis).

The practical part deals with the brief introduction of the organization, the analysis of the current situation of the organization and its security risks. The conclusion of the work consists of the evaluation of risk analysis and proposals how to reduce founded risks.

Keywords: risk, safety, organization, risk analysis.

Děkuji mému vedoucímu bakalářské práce panu prof. Ing. Jiřímu Dvořákovi, DrSc. za obětavý přístup a cenné rady, které mi poskytl po celou dobu zpracování této práce.
Dále bych ráda poděkovala Ing. Josefu Slezákovi, který mi ochotně pomáhal a poskytl mi kvalitní konzultace, informace a materiály k tvorbě bakalářské práce.

V neposlední řadě patří velký dík mému příteli, který byl mou velkou oporou.

Motto:
Kdo je připraven, není překvapen.

OBSAH

ÚVOD

Bezpečnostní riziko je v současné době velmi probíraným tématem, které se neustále s postupem nových technologií vyvíjí. Nové technologie nám sice umožní se cítit bezpečněji než dříve, ale i to nese své stinné stránky. S vývojem nových nápadů přichází i vývoj nových rizik, které nás mohou ohrozit. Právě proto by lidstvo nemělo otálet a mělo by být stále ve střehu a naučit se více s těmito riziky pracovat. Ke zdárnému zvládnutí těchto rizik a jejich eliminaci slouží v organizacích preventivní opatření. Vyhledání a následné vyhodnocení rizik se zjištěním příčin vzniku rizika tvoří základ pro stanovení vhodné prevence rizik.

Organizaci může ohrozit řada rizik, včetně osob pracující v ní. Z důvodu širokého rozpětí z hlediska kategorií rizik, je bakalářská práce zaměřena na rizika bezpečnostní.

Cílem bakalářské práce bude na základě průzkumu v organizaci analyzovat a charakterizovat bezpečnostní rizika a současně určit preventivní opatření ke snížení rizik. Na základě získaných poznatků a jejich vyhodnocení budou předkládány mé návrhy na zlepšení.

V teoretické části bude kladen důraz na vymezení pojmů souvisejících s danou problematikou. Tato část bude zahrnovat z pohledu teorie vysvětlení rizika, bezpečnostního rizika, nebezpečí, bezpečnosti a ochrany zdraví při práci, organizace, veřejné správy a analýzy rizik, jejíž součástí budou metody pro stanovení rizik.

Praktická část bude zaměřena přímo na vybranou organizaci, která bude stručně představena a charakterizována, dále bude věnována samotné analýze současných opatření a bezpečnostních rizik v organizaci. Po zpracování a vyhodnocení zvolených metod budou navržena má preventivní opatření vedoucích ke snížení a eliminaci bezpečnostních rizik.

Ke zjištění bezpečnostních rizik v organizaci bude využito možnosti vlastního průzkumu se souhlasem vedení organizace. Hodnocení rizik bude probíhat prostřednictvím brainstormingu, metody What – if, a následných rozhovorů s vybranými zaměstnanci organizace. Bezpečnostní rizika, která budou definována a ohodnocena prostřednictvím skórovací metody budou znázorněna na mapě rizik.

I. TEORETICKÁ ČÁST

1 ÚVOD DO PROBLEMATIKY

1.1 Riziko

Tento pojem souvisel s lodní dopravou a byl objeven již v 17. století. Slovo *risico* pochází z italštiny. Určovalo úskalí, se kterým se plavci potýkali a chtěli se mu tak vyvarovat. Později se tak vyjadřovalo „vystavení nepříznivým okolnostem“. Pod tímto výrazem můžeme nalézt vysvětlení jednající o odvaze či nebezpečí. V současnosti již víme, že nebezpečí představuje něco poněkud jiného a v teorii rizika se pojí s hrozbou. [7]

Riziko je chápáno jako určitý druh nebezpečí (např. riziko ochoření, porucha výrobního stroje aj.), tzn., že se zaměřujeme na negativní stránku rizika.

Setkáváme se s řadou definic pro tento termín:

- *pravděpodobnost vzniku ztráty,*
- *přítomnost události, která ohrozí dosažení cílů,*
- *nebezpečí negativních odchylek od stanovených úrovní cílů* [3, s. 12]

V knize „Risk management in organizations: an integrated case study approach“ autorka Margaret Woods uvádí, že všechna rizika mají na nás a náš systém velký dopad a mnohá rizika jsou klasifikována jako závažná. [13]

Riziko má dva rozměry:

- *pravděpodobnost vzniku nebezpečné situace ohrožení,*
- *závažnost možného důsledku.* [9, s. 6]

Rizikové situace

Jsou to situace, jež jsou prostorově a časově závislé na okolnostech, ve kterých se vyskytuje jak zdroj nebezpečí, tak příjemce nebezpečí, případně příjemci rizika. Riziková situace je někdy nazývána jako *riziková expozice* (exposure to risk) či *hazardová expozice* (hazard exposure).

Rizikový faktor

V anglickém překladu *risk factor, risk driver*. Zpravidla jím rozumíme jev (stacionární nebo nestacionární), který může ve vyšetřovaném případě být zdrojem nebezpečí. Lze sem zařadit i absenci neurčitého jevu (např. zabezpečovací systém) či nečinnost. [10]

1.1.1 Zdroje rizika

Existuje několik zdrojů rizik, která musí organizace vzít do úvahy ještě před tím, než udělá rozhodnutí. Pro organizaci je klíčové znát její případná rizika, jelikož je může identifikovat, analyzovat a učinit odezvu. Zdrojem rizika je jakýkoliv faktor, který má schopnost určitým způsobem ovlivnit projekt či samotný výkon firmy. Ve výsledku to znamená, že definice cílů projektu a kritéria výkonu mají základní vliv na úroveň rizika projektu. [5]

1.1.2 Identifikace rizika

Identifikace rizik má za úkol nalézt rizikové faktory, jež mají (negativní či pozitivní) vliv na výsledky firmy (hospodářské, investiční). Tento proces se skládá z několika bodů. Hlavním bodem je vhodné rozložení objektu analýzy rizika, vlastní uskutečnění procesu identifikace, použití metody a nástroje podporující identifikaci, dále informační zdroje a subjekty mající podíl na identifikaci. Na samotné identifikaci by se měli podílet pracovníci firmy. Doporučuje se spolupráce s externími specialisty. Důležitou roli během identifikace rizik sehrává management firmy, zejména na vrcholové úrovni řízení (generální ředitel a výkonní ředitelé), dále jsou to orgány společnosti (představenstvo a dozorčí rada). Identifikace rizik se řadí mezi důležitou a časově náročnou fázi analýzy rizik. Je potřeba zkušenosti, systematičnosti, tvůrčího přístupu (mít schopnost předvídat takové situace, které nejsou známé), týmové práce a v prvé řadě zaměřit se na budoucnost.

Nejvýznamnější nástroje pro identifikaci rizik:

- **kontrolní seznamy** poskytující vyčerpávající přehled potenciálních rizikových faktorů firmy,
- **pohovory s experty a skupinové diskuze** (např. brainstorming),
- **nástroje strategické analýzy** (např. What – if),
- **kognitivní (myšlenkové) mapy**. [3]

U jednotlivého identifikovaného zdroje rizika dále posoudíme, jaká škoda může být způsobena a jak k ní může dojít. Jedná se o to určit zejména:

a) kdo nebo co může být vystaveno nebezpečí,
b) jaké mohou být následky,
c) jaký je způsob iniciace ohrožení,
d) jaké faktory či další zdroje nebezpečí mohou přispívat k iniciaci a ke zvýšení škody.

Účelem identifikace rizik je:

- identifikovat a podchytit nejdůležitější účastníky při řízení rizika a poskytnout základy pro následné řízení,
- stabilizovat přípravné fáze zajištěním všech nezbytných informací pro provedení analýzy rizika,
- identifikovat komponenty projektu či služby,
- identifikovat neodmyslitelná rizika projektu nebo služby. [6]

1.1.3 Klasifikace rizik

Rizika lze hodnotit z mnoha úhlů. Mezi základní způsoby patří:

- podnikatelské a čisté,
- systematické a nesystematické,
- vnitřní a vnější,
- primární a sekundární,
- rizika ve fázi přípravy a realizace projektu.

Dále můžeme rizika členit dle jejich věcné náplně. Mezi tyto řadíme např. rizika *technologická* (havárie strojního zařízení), *výrobní*, jež mají často charakter omezenosti (tzn. nedostatek surovin, energií, pracovníků) a *bezpečnostní* (mechanické prostředky, požární signalizace). Některá rizika spadají pod rizika *ovlivnitelná* (riziko, které lze nějakým způsobem eliminovat) a *neovlivnitelná* (u těchto rizik nelze příčině zabránit, např. povodeň, zemětřesení). [3]

V textu níže si uvedeme stručnou charakteristiku rizik vnitřních a vnějších. Bezpečnostní rizika budou definována v samotné kapitole, a to z důvodu, že se těmito riziky budu zabývat v praktické části a jsou velmi významná pro vybranou organizaci.

Vnitřní rizika

Pojmem vnitřní riziko se rozumí riziko, jež se vztahuje na faktory uvnitř organizace. Mohou to být např. rizika výzkumně – vývojová či rizika selhání pracovníků aj.

Vnější rizika

Vnější riziko se vztahuje k okolí organizace. Zdrojem jsou externí faktory, které se člení na *makroekonomické* (ekonomické, sociální makrookolí) a *mikroekonomické* (patří sem konkurence, odběratelé, dodavatelé aj.). [3]

1.2 Bezpečnostní rizika

Bezpečnostními riziky označujeme rizika spojená s bezpečností osob, majetku a informací. Mezi tyto skupiny rizik patří:

- personální bezpečnost – škoda na majetku, zdraví a života osob, ochrana osobních údajů,
- fyzická bezpečnost – poničení majetku, vniknutí do objektů či systémů,
- informační rizika – napadení sítě či informačního systému, zneužití dat. [23]

1.2.1 Personální bezpečnost

Personální bezpečnost slouží k zajištění ochrany utajovaných informací. K tomu, aby fyzická osoba (dále jen „FO“) získala přístupy k utajovaným informacím, je třeba jejího ověření. Toto ověření zahrnuje výchovu těchto osob. Za proškolení FO ručí odpovědná osoba, která má za povinnost jednou ročně provádět školení v oblasti ochrany utajovaných informací a vést o těchto proškoleních přehledy. Utajované informace se rozlišují dle stupňů utajení, k nimž má mít FO přístup. [25]

Dle provedených průzkumů bylo zjištěno, že téměř 80 % zaměstnanců způsobilo bezpečnostní incidenty přímo ve své organizaci. Z tohoto hlediska je tedy důležité, aby byli voleni vhodní kandidáti, kteří budou respektovat a dbát pokynů svých zaměstnavatelů. [15]

1.2.2 Fyzická bezpečnost

Fyzickou bezpečnost upravuje zákon č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti. Tvoří ji systém opatření, jež mají zamezit neoprávněné osobě přístupu k utajovaným informacím, případně přístup či pokus o něj zaznamenat. Pro ochranu utajovaných informací se vymezují objekty, zabezpečené oblasti a jednací oblasti. Objektem se rozumí budova či ohraničený prostor, ve kterém se vyskytuje zabezpečená oblast. V této oblasti jsou ukládány utajované informace, které se uchovávají v zabezpečeném trezoru nebo jiné uzamykatelné schránce. Zabezpečené oblasti se dělí na:

- přísně tajné,
- tajné,
- důvěrné,
- vyhrazené.

Dále se využívají certifikované nebo necertifikované technické prostředky. Certifikací technických prostředků se má na mysli:

- přístroj elektrické požární signalizace,
- specifické televizní systémy,
- elektronický zabezpečovací systém,
- přístroj, který je schopen vypátrat nebezpečné látky či předměty,
- přístroj, jež má zamezit odposlechu. [24]

Přístroj elektrické požární signalizace a elektronický zabezpečovací systém podrobněji popíši v textu níže, jelikož se jedná o nejvíce využívané a známé prostředky ochrany.

Elektronická požární signalizace

Elektronická požární signalizace (dále jen „EPS“) patří podle vyhlášky o požární prevenci mezi vyhrazená požárně bezpečnostní zařízení. Jejím hlavním úkolem je včas identifikovat požár v jeho prvotním stádiu. Mezi další důležité úkoly EPS patří také akusticky a opticky varovat osazenstvo v prostorech, které mohou být ohroženy požárem. Nesmí se zapomenout ani na možnost ovládat zařízení, která brání šíření požáru nebo vydávání signálů pro ovládání technologických zařízení v případě požáru apod. [20]

Pro jeho naplnění platí tyto technické předpisy:

- ČSN EN 54 Elektrická požární signalizace – soubor norem,
- ČSN 34 2300 Předpisy pro vnitřní rozvody vedení elektronických komunikací,
- ČSN 34 2710 Elektrická požární signalizace – projektování, montáž, užívání, provoz, kontrola, servis, údržba,
- ČSN 73 0875 Požární bezpečnost staveb – stanovení podmínek pro navrhování elektrické požární signalizace v rámci požárně bezpečnostní ho řešení. [26]

Na obrázku *(Obr. 1.)* můžeme vidět různé druhy protipožární signalizace.

Obr. 1. Typy protipožárních signalizací. [17]

Elektronický zabezpečovací systém

Úkolem elektronického zabezpečovacího systému (dále jen „EZS“) je poskytnout informace majiteli objektu (obchodu, bytu, chaty, kanceláře) v případě neoprávněného vniknutí cizí osoby. Další funkcí EZS je zajištění zabezpečení peněz, obrazů, klenotů či jiných významných cenností. Elektronický zabezpečovací systém se skládá z ústředny, která vyhodnocuje stav detektorů a je ovládána prostřednictvím klávesnice. Jestliže detektor shledá pohyb, vyšle signál do ústředny a spustí se alarm. Na stav narušení objektu může systém upozornit akustickou či optickou signalizací. Mnoho organizací, firem a obchodů zajišťuje ochranu objektu fyzickou ostrahou (bezpečnostní agentura nebo zaměstnanec organizace), která má za cíl objekt střežit (ve většině případů 24 hodin) a v případě vniknutí zavolat Policii ČR. [22]

Mezi prvky elektronického zabezpečovacího systému řadíme:

- čidlo EZS,
- ústřednu EZS,

- přenosové zařízení,
- signalizační zařízení,
- doplňková zařízení,
- ovládací zařízení,
- napájecí zdroj.

Zabezpečovací systém tvoří čtyři základní druhy ochrany:

- klasická ochrana (zámky, ploty, mříže),
- režimová ochrana (soubor administrativně organizačních opatření a postupů),
- fyzická ochrana (strážní, hlídači, policisté),
- technická ochrana (elektronický zabezpečovací systém). [12]

Obr. 2. Zabezpečovací prvky EZS. [18]

1.2.3 Informační rizika

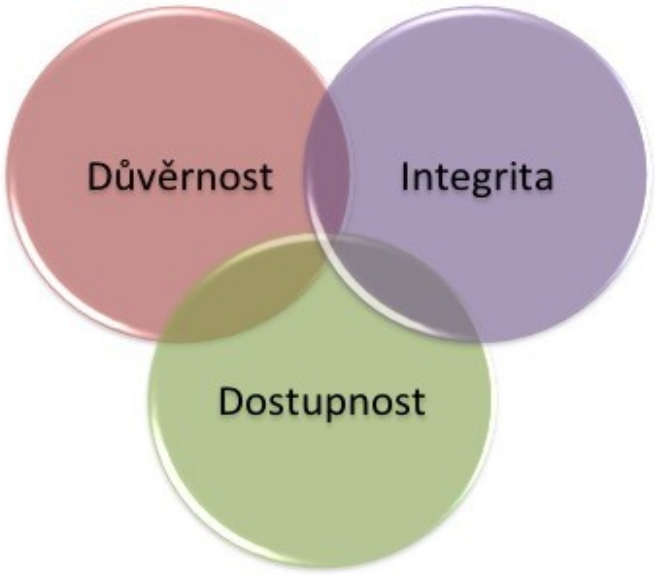
Informační bezpečnost zařazuje ochranu veškerých informací bez rozdílu nosiče. V současnosti je propojována s informacemi komunikovanými skrze informační technologie. Informační bezpečnost vznikla za účelem ochrany informací, kterých FO a PO využívá během své činnosti. Jelikož se ve většině případů jedná o informace

s nezanedbatelnou hodnotou (např. osobní záznamy, bankovní účty, výrobek či výzkum), je třeba tyto informace chránit tak aby:

- k nim měly přístup jen oprávněné osoby,
- nedocházelo k paděláním,
- bylo patrné, kdo je vyrobil, změnil či odstranil,
- nebyly vyneseny,
- byly přístupny v případě potřeb. [16]

Systém řízení bezpečnostních informací dělíme na tři základní principy, které je potřeba brát v úvahu. Jsou jimi:

- důvěrnost,
- dostupnost,
- integrita. [29]



Obr. 3 Tři základní principy bezpečnostních informací. [29]

1.3 Nebezpečí

Důležitým pojmem v rizikovém inženýrství je nebezpečí, které je reálnou hrozbou daného objektu či procesu. Stroje, materiály, zařízení a pracovní činnosti se vyznačují tím, že mohou zapříčinit neočekávaný negativní důsledek, např. škoda na majetku. [9]

Jedná se o:

- *nebezpečí nebo nebezpečné činnosti,*
- *podstatnou, ale skrytou vlastnost nebo schopnost něčeho (materiálu, stroje), která může zapříčinit vznik škody,*
- *zdroj možného ohrožení nebo škoda.* [9, s. 8]

Pojmem nebezpečí se dá taktéž vyjádřit vlastnost látky či fyzikálního jevu, který působí nepříznivě na zdraví člověka či životní prostředí. Vlastnost je to vrozená a daný subjekt se jí nemůže zbavit. Projeví se však pouze tehdy, je-li člověk jejímu vlivu vystaven.

Dalším pojmem úzce spjatým s termínem je zdroj nebezpečí. Zdrojem nebezpečí může být cokoliv, co může v daném prostoru za určitých podmínek vyvolat nebezpečí, tedy různá zařízení, materiály (např. mechanická či chemická). [28]

Nebezpečí má dva základní rysy:

- *vztahuje se k budoucnosti* (neboť uvažujeme o tom, jaká nebezpečí hrozí),
- *je neurčité* (nepříznivá událost, o níž víme, že nastane určitě, není nebezpečím nýbrž skutečností, s níž se musíme aktivně či pasivně vypořádat). [10]

1.3.1 Scénář nebezpečí

Scénář nebezpečí líčí promítnutí nebezpečí do prostoru a času. Jedná se o popis dějů, které podmiňují výskyt nepříznivé příhody, dále okolností, v nichž takové děje probíhají, a skutečností, jež je provázejí. Vytvoření takového scénáře není jednoduché. K problémům se tedy musí přistupovat z několika hledisek a je třeba vytvoření určitých metodických postupů. Při zjišťování nebezpečí a scénářů nebezpečí se prosazuje zejména inženýrský důvtip, zkušenost a jistá velkorysost v chápání souvislostí. [9]

1.3.2 Škoda

Škoda (damage) sděluje ztrátu vzniklou realizací scénáře nebezpečí. Často škodu vyjadřujeme penězi, ale také se popisuje počtem zmařených lidských životů, počtem vadných nebo zničených výrobků, objemem kontaminované zeminy aj. Jedná se o časově závislou veličinu, neboť hodnota objektu se mění a mění se tak i cena následků. [9]

1.3.3 Nejistota a neurčitost

Informace, se kterými běžně přicházíme do styku, a které používáme v analýzách rizik, nemají stejnou významnost a stejnou spolehlivost. Přesto se dají odstupňovat. Za výchozí bod se dá považovat jistota, kdy veškeré skutečnosti jsou jednoznačné, a výsledek činnosti, o níž se rozhodovalo, se nemůže od předpokladu nijak odchýlit. Pokud se jistota ztratí, musíme se vyrovnat s nejistotou a neurčitostí. [10]

1.4 Bezpečnost a ochrana zdraví při práci

Lze říci, že každá činnost, kterou člověk vykonává, má v sobě určité riziko. Zkrátka neexistuje život bez rizika. Riziko je potřeba přijmout a nějakým způsobem se s ním vypořádat. I přes velké technologické zlepšení nejsme schopni riziko zcela eliminovat. V dnešní době jej ale chceme mít pod kontrolou a mít je v jisté míře kontrolované.

Během pracovní činnosti může dojít ke vzniku rizika. Abychom těmto rizikům předcházeli, je třeba, aby byla předem stanovena nějaká pravidla. Pracovník by si měl být vědom, že svým chováním neohrožuje pouze sebe, ale i své okolí. K tomu slouží školení na pracovištích. Pracovníci si tak uvědomí, co je může čekat v případě, že nedodrží jistá pravidla a povinnosti.

Dle zákoníku práce (zákon č. 262/2006 Sb.) zaměstnavatel odpovídá za své zaměstnance. Jestliže se zaměstnanec během pracovní době poraní, jde o pracovní úraz – a za škodu vzniklou pracovním úrazem odpovídá zaměstnavatel, u něhož byl zaměstnanec v době úrazu v pracovním poměru. V případě, že se zjistí, že k pracovnímu úrazu došlo proto, že zaměstnanec porušil předpisy k zajištění bezpečnosti a ochrany zdraví při práci, může se zaměstnavatel své odpovědnosti zprostit. Z tohoto důvodu je školení zaměstnanců velmi důležité. [21]

1.4.1 Školení zaměstnanců

Školení zaměstnanců v oblasti bezpečnosti a ochrany zdraví při práci (dále jen „BOZP“) patří k základním povinnostem zaměstnavatele. Toto školení není po obsahové stránce upraveno žádným obecně závazným předpisem. Směrnice Evropské unie klade důraz

na prevenci rizik a na přijímání opatření k prevenci rizik. Tato legislativa je začleněna i do českého právního systému. Zaměstnavatel by tak měl sám vyhledávat rizika, prošetřovat jejich původ, zdroje a přijímat opatření k jejich odstranění nebo snížení. Zaměstnavatel tedy ví nejlépe, jaká rizika hrozí a je na něm, jakým obsahem školení BOZP naplní. Zákon nestanovuje, jak často má školení probíhat (taktéž není určena obsahová náplň) a jak má vypadat ověřování znalostí zaměstnanců z oblasti BOZP. [21]

Čím začít při zajišťování školení?

Při zabezpečení školení je zapotřebí především zpracování podrobného seznamu prací a činností, které zaměstnanci v rámci plnění pracovních úkolů provozují. Seznam prací je pomůckou při výběru přesných požadavků vyplývajících z právních a ostatních předpisů k zajištění bezpečnosti a ochrany zdraví při práci. Je tedy vodítkem k formulování konkrétních zásad a informací, které se stanou obsahem školení zaměstnanců. Podrobnější přehled o pracích, činnostech a pracovních podmínkách, ve kterých zaměstnanci uvedené práce vykonávají, je důležitý pro zaměstnavatele i při zpracování záznamů o zhodnocených rizicích a při tvorbě vlastního seznamu osobních ochranných pracovních prostředků poskytovaných zaměstnancům. [1]

Zdroje vzdělávání:

- *právní předpisy k zajištění BOZP,*
- *ostatní předpisy k zajištění BOZP (např. české technické normy),*
- *výsledky hodnocení rizik a opatření na ochranu před jejich působením,*
- *dokumentace o strojích, technických zařízeních a technologiích,*
- *výsledky prověrek BOZP,*
- *opatření nežádoucích událostí na pracovištích.*

Druhy školení:

- *vstupní obecné školení při nástupu do práce,*
- *vstupní školení na pracovišti (probíhá v den nástupu do práce, jak požaduje zvláštní právní předpis).* [1, s. 55]

Zaměstnavatel je povinen proškolit zaměstnance ještě před přidělením práce, kterou mají vykonávat. Toto školení by mělo proběhnout v den nástupu do zaměstnání. Vstupní obecné školení obvykle provádí osoba odborně způsobilá k prevenci rizik (v oblasti BOZP), vstupní školení na pracovišti posléze provádí příslušný vedoucí zaměstnanec. [1]

1.4.2 Povinnosti zaměstnavatele

Zaměstnavatel je povinen v oblasti BOZP provádět:

- prověrku BOZP na všech pracovištích (1x za rok),
- revize a provozuschopnost strojů a zařízení (dle harmonogramu),
- školení zaměstnanců,
- řízení rizik,
- záznamy o pracovních úrazech.

Do dalších kompetencí, které spadají mezi povinnosti zaměstnavatele v oblasti BOZP, patří:

- budování podmínek pro bezpečnou, zdraví neohrožující práci,
- hledání případných rizik možného ohrožení, informovování zaměstnanců,
- vykonávání opatření pro ochranu před riziky,
- zajištění první pomoci. [19]

1.4.3 Povinnosti zaměstnance

K tomu, aby zaměstnanec vykonával bezpečnou práci a vyhnul se případným úrazům či jiným pochybením, je třeba, aby dbal určitých povinností, mezi které se řadí například:

- ctění bezpečnostních předpisů,
- užívání osobních ochranných pracovních prostředků a ochranných zařízení,
- podrobování se školení či zkouškám,
- nepožívat alkohol a jiné návykové látky,
- dbání zákazu kouření,
- hlášení nedostatků nebo jiných závad. [19]

1.5 Organizace a veřejná správa

V této kapitole budou stručně charakterizovány pojmy organizace a veřejná správa, jelikož tyto pojmy spolu úzce souvisejí a zároveň jsou důležitým teoretickým východiskem této bakalářské práce.

Organizace

Organizací chápeme určité sociální uspořádání stvořené proto, aby řízeným způsobem jednání dosáhlo kolektivních záměrů. Sociálním uspořádáním vyjadřujeme skutečnost, že organizaci představuje určitý počet členů, jež přichází do styku s ostatními členy, což má za důsledek společné ovlivňování a efektivnější práci. K dosažení cílů je využíváno technologií, informací či nástrojů řízení. [2]

Organizace je charakterizována těmito znaky:

- *vymezení vůči okolnímu prostředí,*
- *vymezení organizační struktury,*
- *dělba práce v rámci organizační struktury,*
- *respektování pravomocí a odpovědností plynoucích z organizační struktury,*
- *spolupráce a koordinace činností na společném cíli.* [2, s. 23]

Veřejná správa

Veřejná správa je vykonávána ve veřejném zájmu a zabezpečuje výkon veřejných činností vymezených zákony. Poskytuje veřejné služby pro občany. Organizačními jednotkami jsou úřady jakožto přímí nositelé veřejné správy. V současné době se veřejná správa dělí na státní správu a samosprávu. [11]

1.6 Analýza rizik

Analýza rizika se řadí mezi základní prvek rizikového inženýrství, je nezbytnou podmínkou rozhodování o riziku a základním procesem v managementu rizika. [10]

Lze ji zpravidla chápat jako proces definování případných hrozeb, pravděpodobnosti jejich uskutečnění a dopadu na aktiva. [7]

Analýza rizik zpravidla zahrnuje:

- identifikaci aktiv – definování posuzovaného subjektu a charakteristika aktiv, které vlastní,

- stanovení hodnoty aktiv – určení hodnoty aktiv a jejich význam pro subjekt, ohodnocení možného dopadu jejich ztráty,
- identifikaci hrozeb a slabin (zranitelnosti) – určení druhů událostí a akcí, které mohou ovlivnit negativně hodnotu aktiv,
- stanovení závažnosti hrozeb a míry zranitelnosti – stanovení pravděpodobnosti výskytu hrozby a míra zranitelnosti subjektu vůči dané hrozbě. [7]

1.6.1 Obecný postup analýzy rizik

Riziko obvykle neexistuje izolovaně, ale většinou se jedná o kombinace rizik, které představují hrozbu pro daný subjekt. Vzhledem k počtu rizik je potřeba určit priority z pohledu dopadu a pravděpodobnosti jejich výskytu a soustředit se na klíčové rizikové okruhy. V procesu analýzy rizik se konají některé obecné činnosti. Jednotlivé postupy za sebou následují v níže uvedené posloupnosti.

Stanovení hranice analýzy rizik

Během stanovení hranice analýzy rizik se vychází z plánů managementu, eventuálně z úvodní studie, jestliže byla zpracována. Aktiva, která mají kvůli probíhajícímu procesu snižování rizik vztah k cílům managementu, budou zařazena do analýzy a budou spočívat uvnitř hranice analýzy. Zbylé aktiva budou spočívat mimo hranici analýzy rizik. V rámci hranice budou ležet jednotlivá aktiva, ze kterých je subjekt strukturován, neboť jsou z hlediska aktuálního záměru důležitá.

Identifikace aktiv

Identifikace se skládá z vytvoření soupisu veškerých aktiv ležících uvnitř hranice analýzy rizik. Během rozhodování o zahrnutí daného aktiva na soupis se předloží název aktiva a jeho umístění. [7]

Stanovení hodnoty a seskupování aktiv

Posuzování hodnoty aktiva je založeno na velikosti škody zapříčiněné zničením či ztrátou aktiva. Zpravidla se při stanovení hodnoty aktiv vychází z jeho nákladových charakteristik, mohou být ale charakteristiky výnosové. Vzhledem k tomu, že aktiv je obvykle velké množství, snižuje se jejich počet tak, že se provede seskupení aktiv podle různých hledisek, aby se vytvořily skupiny aktiv podobných vlastností. Seskupovat se mohou aktiva podobné kvality, ceny, účelu apod. Takto vytvořená skupina aktiv pak dále vystupuje jako jedno aktivum. Poté se musí zabezpečit, aby protiopatření, navržená v etapě zvládání rizik pro skupinu aktiv, byla aplikována na všechna aktiva, která jsou do této skupiny sdružena. Z tohoto hlediska je třeba identifikovat vlastníka každého daného aktiva.

Identifikace hrozeb

V této části se zaměřujeme na identifikaci hrozeb, které mohou být klíčové pro analýzu rizik. Tato část zahrnuje výběr potenciálních hrozeb jednoho z aktiv subjektu. Můžeme vyjít ze seznamu hrozeb, z vlastní praxe nebo z provedených průzkumů. Hrozby se mohou odvíjet taktéž od subjektu, jeho statusu či jeho postavení na trhu.

Analýza hrozeb a zranitelnosti

Jakoukoliv hrozbu klasifikujeme vůči každému aktivu či skupině aktiv. U těch aktiv, na něž se hrozba může vztahovat, se určí úroveň hrozby vůči tomuto aktivu a stanoví se také úroveň její zranitelnosti vůči hrozbě. Jestliže se stanovuje úroveň hrozby, je vycházeno z faktorů, jako je nebezpečnost, motivace a přístup. Při určení úrovně zranitelnosti se vychází z faktorů jako je citlivost a kritičnost. Během této analýzy věnujeme pozornost i na již provedená protiopatření vedoucí ke snížení úrovně zranitelnosti, případně na vyskytující se hrozby.

Pravděpodobnost jevu

Pravděpodobnost jevu nastane v situaci, kdy nejsme schopni s určitostí říci, zda se zkoumaný jev dostaví. Tento případ nesměřuje vždy ke stejnému účinku. Pakliže chceme počítat s pravděpodobností, je nevyhnutelné zaměřit se na otázku, zda zkoumaný

jev je či není náhodný. Dále je vhodné určit, jaké jsou jeho pravděpodobnostní charakteristiky. [7]

Měření rizika

Je třeba si uvědomit, že ne v každé situaci můžeme nalézt stejné riziko. V určitých situacích je větší, v některých menší. Jeho výše vychází z hodnoty aktiva, úrovně hrozby a zranitelnosti aktiva. V tomto kroku se pracuje s veličinami, které ne vždy jdou s určitostí změřit a určit jejich velikost. V tomto případě nastoupí kvalifikovaný specialista, který se vyjádří na základě své dlouholeté praxe (zpravidla stupnicí 1 až 10). Jevy s vysokou pravděpodobností ztráty bereme jako rizikovější než ty, které se potýkají s pravděpodobností menší. [7]

1.6.2 Metody analýzy rizik

Metody analýzy rizik dělíme do dvou kategorií, které se od sebe odlišují způsobem vyjádření veličin, s nimiž se v analýze pracuje. Jedná se o kvantitativní a kvalitativní metody vyjádření veličin. V případě řešení je možné použít jednu z výše uvedených metod nebo využít jejich kombinaci.

Kvalitativní metody

Tyto metody zkoumají to, jak srovnat relativní významy rizik, kterým daný subjekt čelí. Předpokládá se, že údaje z kvalitativní analýzy jsou hodnotnější než z kvantitativní analýzy. Kvalitativní analýza je doporučována pro vývoj začínajícího ohodnocení rizika.

Kvantitativní metody

Úkolem této analýzy je stanovit absolutní rozsah hodnot společně s rozdělením pravděpodobnosti pro výstup firmy či plánovaného projektu.

Management zvolí, jakou analýzu rizik je třeba stanovit a měl by zvážit následující:

- dosažitelnost zdrojů pro analýzu – lidských, výpočetních a času,
- praxi osob, jež provádějí analýzu,

- velikost a složitost projektu,
- dostupnost informací,
- smysl analýzy. [10]

WHAT – IF analýza

Tato metoda je ideální volbou ve chvíli, kdy chceme identifikovat rizika, která se zkoumají v širším detailu dalšími metodami. Pro identifikaci rizik jsou kladeny otázky, doplňkem pak může být brainstorming. Účastní se jí skupina lidí, jež mají zkušenosti a kladou si mezi sebou vzájemně otázky, které mají vést na možné dopady. Tato metoda není vnitřně strukturována jako ostatní techniky. Její výhodou je flexibilita a její přizpůsobení konkrétnímu účelu. Hlavním cílem je nalézt problém či nebezpečné stavy v procesu. Výstupem je uvedení případných rizik či problémů, včetně doporučení a postupů, jak jim předejít. [4]

BRAINSTORMING

Doslovně přeloženo „bouře mozků“ – jedná se o skupinovou techniku, která se zaměřuje na generování co nejvíce nápadů na dané téma. Očekává se, že když se sejde více lidí, vyvstane více nápadů/názorů, než by vymyslel jedinec. Důležitá je důvěra ve skupině lidí, příjemná atmosféra a také to, že každý nápad je vítán, nikoliv kritizován. [8]

SKÓROVACÍ METODA S MAPOU RIZIK

Cílem této metody je ohodnotit rizika pro každý rizikový faktor. Metoda hodnotí jak možnost výskytu rizikového faktoru, tak i jeho dopad prostřednictvím desetibodové stupnice. Je vhodné, aby každý člen/hodnotitel týmu stanovil svůj odhad hodnoty nezávisle na ostatních členech. Výsledný odhad se vypočítá jako aritmetický průměr odhadů jednotlivých členů/hodnotitelů. Závěrem je sestavená mapa rizik (dvojrozměrná matice) ve tvaru bodového grafu. Návrhy na snížení rizika jsou zpracovány pro rizika v kvadrantu kritických rizik a pro kvadrant významných rizik. [24]

2 DÍLČÍ ZÁVĚR TEORETICKÉ ČÁSTI

V teoretické části byly vysvětleny základní pojmy související s tématem bakalářské práce, a to zejména definice rizika – zdroje rizika, identifikace rizika, typy rizik a přijatelnost rizika. Okrajově bylo charakterizováno nebezpečí (scénář nebezpečí, škoda, nejistota a neurčitost).

Součástí úvodní kapitoly byla taktéž terminologie zabývající se bezpečností a ochranou zdraví při práci. Stručně bylo nastíněno, jak by měl vypadat průběh školení zaměstnanců, a v neposlední řadě byly vymezeny povinnosti jak zaměstnavatele, tak i zaměstnance. Školení zaměstnanců je velmi důležitým krokem, díky němuž jsou mnohá rizika eliminována.

Závěr teoretické části byl věnován analýze rizik, kde byl popisován objektivní postup a metody analýzy rizik, z čehož některé zmíněné budou aplikovány v praktické části. Posledním bodem byla stručná definice organizace a veřejné správy.

II. PRAKTICKÁ ČÁST

3 METODIKA PRAKTICKÉ ČÁSTI

Cílem praktické části je stručné definování organizace ABC, ve které bude analýza rizik implementována. Úvod obsahuje charakteristiku organizace, historii, současnost a její organizační strukturu. Práce bude soustředěna na detašované pracoviště organizace, které bude taktéž stručně charakterizováno.

Další část bakalářské práce se zaměřuje na uvedení bezpečnostních rizik. Cílem bude uvést rizika, která mohou mít na dané pracoviště zásadní vliv.

Po úvodním seznámení s pracovištěm a jeho případnými riziky je práce zaměřena na samotnou analýzu rizik a navržení opatření ke snížení rizik.

3.1 Použité metody analýzy

Stávající situace v organizaci byla zjištěna vlastním průzkumem a konzultacemi s technikem BOZP. Po těchto zjištění budou aplikovány metody analýzy rizik: What – if, brainstorming, a skórovací metoda s mapou rizik. Charakteristika těchto zvolených metod byla zmíněna v teoretické části bakalářské práce.

3.2 Vyhodnocení a závěr

Závěrem praktické části je celkové zhodnocení zjištěných výsledků analýzy rizik a jejich následné doporučení pro jejich eliminaci včetně doporučení. Praktická část je zakončena závěrem, který se věnuje výslednému shrnutí problematiky daného tématu a přínosu práce.

4 PŘEDSTAVENÍ ORGANIZACE ABC

Pro vypracování praktické části bakalářské práce jsem zvolila organizaci, ve které jsem v současné době zaměstnána. Informace, které jsem využila pro potřebu zpracování této části, jsem vykonávala s písemným souhlasem vedení organizace s tím, že organizace bude uvedena pod smýšleným názvem ABC.

Organizace ABC se řadí mezi největší finančně správní instituci, která spravuje agendu cca 8,5 milionu klientů, z toho 2,9 milionu důchodců. Vyplácí více než 3,5 milionu důchodů a měsíčně přes 200 tisíc dávek nemocenského pojištění. Jedna třetina veškerých příjmů míří do státního rozpočtu. Jedná se o peníze, které organizace získává na pojistném a sociálním zabezpečení a příspěvcích na státní politiku zaměstnanosti.

Mimo to organizace ABC vykonává působnost v oblasti lékařské posudkové služby (přiznání invalidity, zda se jedná o osobu zdravotně znevýhodněnou a další). Rovněž provádí úkoly vyplývající z mezistátních úmluv o sociálním zabezpečení. [14]

4.1 Historie

Organizace ABC byla zřízena s účinností od 1. září 1990, zákonem ČNR č. X/1990 Sb. a zákonem ČNR č. X/1998 Sb. se sídlem v hlavním městě. Jedná se o největší budovu této organizace, která prošla řadou oprav a změn. [14]

Ve své bakalářské práci se zaměřuji na detašované pracoviště uvedené organizace, které vzniklo v letech 1995.

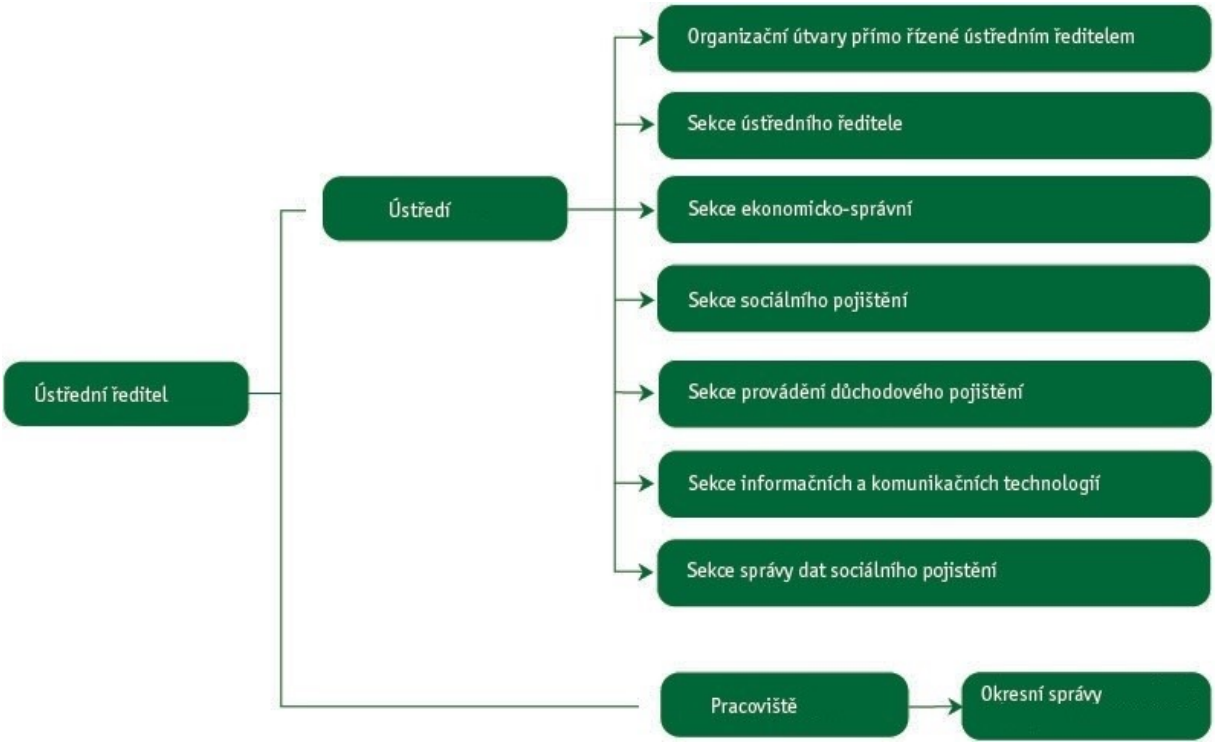
4.2 Současnost

Od dob vzniku této organizace se mnohé změnilo. Pro usnadnění a komfort klienta zřídila organizace ABC na svém webu sekci *e-podání*. Tato služba dává možnost elektronickou cestou zasílat vybrané předepsané tiskopisy – evidenční listy důchodového pojištění, přehled výše pojistného, potvrzení o studiu aj. Služba využívá elektronické formuláře. Vyplněné údaje se posléze převedou do datových vět. Dále se organizace ABC může pyšnit další užitečnou internetovou službou, jež má zpřístupnit občanovi informace ohledně započtené doby důchodu. Jedná se o aplikaci, díky které může občan z pohodlí domova nahlédnout

do svého osobního konta, kde si vyčte vlastní životní kariéru od dob studií. Celkově by se tedy dalo shrnout, že hlavním cílem celé organizace je mít co nejvíce spokojených klientů a usnadnit jim cestu za jejich požadavky. [14]

4.3 Organizační struktura

Struktura organizace ABC se skládá z ústředí, z pracovišť (např. Praha, Brno, České Budějovice) a okresních správ (Uherské Hradiště, Brno-venkov, Ostrava). V popředí všech organizačních jednotek jsou ředitelé, kromě pražské pobočky, v jejichž čele jsou vedoucí. Dále se organizační struktura větví na sekce *(Obr. 4.*). [14]



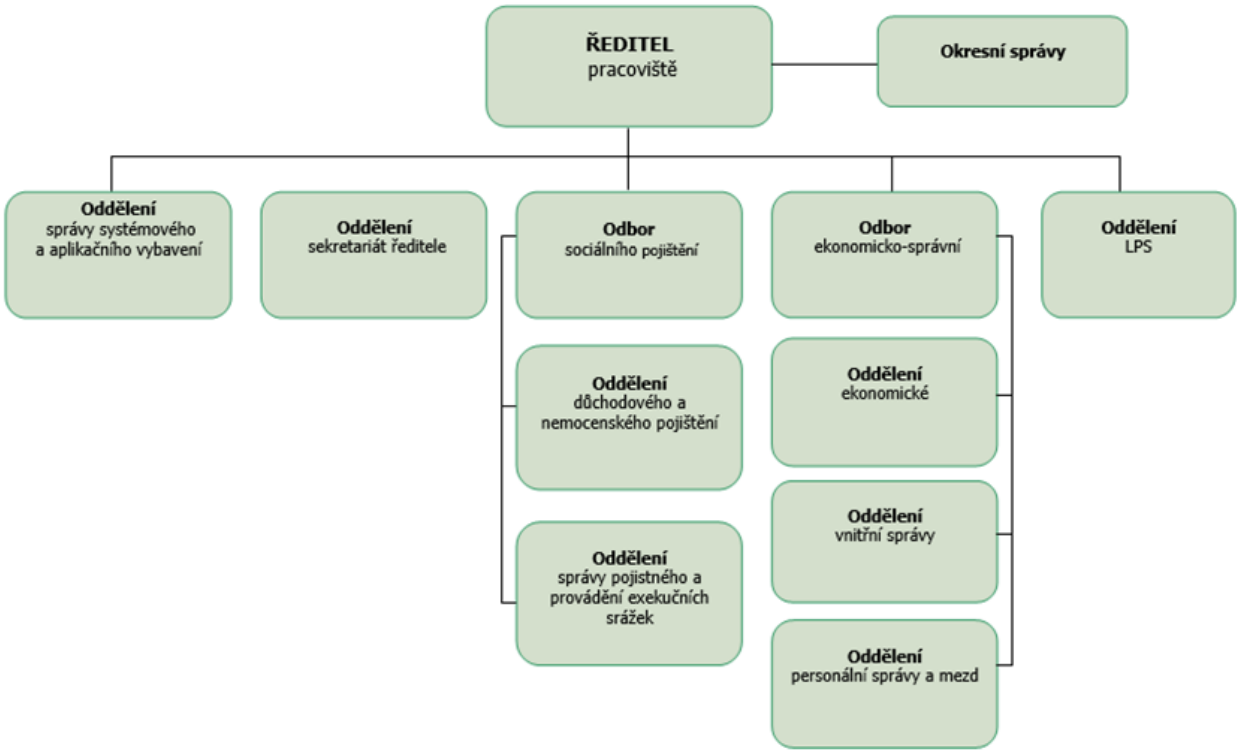
Obr. 4. Organizační uspořádání ABC. [14]

Detašované pracoviště

Jak již bylo zmíněno v kapitole výše, detašované pracoviště (dále jen „pracoviště“) vykonává zejména metodickou a kontrolní činnost (důchodové, sociální, nemocenské pojištění a provádění exekučních srážek), komplexní ekonomické, personální a technicko – provozní

zabezpečení své činnosti a činnosti okresních správ. Pracoviště nepřichází do přímého kontaktu s veřejností. [32]

Pracoviště se nachází v samotném centru města. Jedná se o starší objekt, který prošel od svého vzniku mnohými rekonstrukcemi. Poslední změnou byla výměna starších a nekvalitních oken a hlavních vchodových dveří. Objekt má 5 nadzemních podlaží a jedno podzemní. Při vstupu u hlavního vchodu se nachází vrátnice a naproti ní je instalován docházkový systém. Je zde zbudován výtah, který, jak je již obecně známo, je využíván pouze pro přepravu osob, neslouží tedy pro evakuaci osob v případě vzniku požáru. V každém patře se nachází 5 kanceláří o různých výměrách, toalety, sprcha a kuchyňka, v 1. nadzemním podlaží je zasedací místnost. V podzemním podlaží se nachází spisovna celého objektu. Zde zaměstnanci archivují dokumentace až po dobu 5 let. V kuchyňkách není zřízen plynový vařič a to proto, aby se zamezilo případnému požáru. Zaměstnanci si tak své jídlo či nápoje, mohou ohřívat v mikrovlnných troubách. U těchto spotřebičů jsou prováděny roční kontroly. Aktuálně má organizace 58 zaměstnanců, z toho většinu tvoří ženy. Organizační struktura je velmi obdobná jako na ústředí. Je rozdělena dle jednotlivé úrovně řízení.



Obr. 5. Organizační struktura pracoviště. [32]

5 ANALÝZA SOUČASNÝCH OPATŘENÍ A BEZPEČNOSTNÍCH RIZIK V ORGANIZACI ABC

Organizace se snaží zajistit opatření směřující k zajištění ochrany objektů a osob, majetku a chráněných zájmů, zajištění ochrany zaměstnanců i ostatních osob oprávněných ke vstupu do objektu, a to vše v souladu s právním řádem a platnými vnitřními směrnicemi. V podkapitolách budou uvedeny opatření, která vedou ke snížení bezpečnostních rizik zmíněného pracoviště. Opatření pro případ zdolávání mimořádných událostí jsou upravena ve vnitřních organizačních směrnicích ředitele pracoviště, které se zabývají problematikou ochrany budov, krizového řízení a požární ochrany.

5.1 Uvedení bezpečnostních rizik

V dnešní době se většina organizací zabývá především modernizací a digitalizací svých pracovišť. Bezpečnostní rizika jsou stále jednou z velkých hrozeb, které mohou společnosti velmi ohrozit. Právě z tohoto důvodu jsem se rozhodla vypracovat bakalářskou práci na toto téma. Chci se hlavně zaměřit na pracoviště, ve kterém vykonávám svůj pracovní poměr, protože mi velmi záleží na bezproblémovém a bezpečném chodu celého pracoviště. Věřím, že výstup z mé práce bude přínosný pro celou organizaci a pomůže předejít analyzovaným rizikům.

Při hodnocení rizika jako možnosti, že se určitá hrozba vyskytne na pracovišti, jsou zvažována následující bezpečnostní rizika:

- zneužití identity fyzické osoby,
- poškození technického vybavení,
- selhání programového vybavení,
- kybernetický útok z vnější či vnitřní komunikační sítě,
- škodlivý kód (např. viry, trojské koně),
- narušení fyzické bezpečnosti,
- přerušení dodávek elektrické energie, vody a tepla,
- požár.

Jednotlivá bezpečnostní rizika budou analyzována a charakterizována v samostatné kapitole.

5.2 Popis stávající situace v organizaci

Jak již bylo zmíněno v kapitole popisující pracoviště, hlavní vstup do objektu je z hlavní ulice a slouží zejména zaměstnancům a návštěvám. Tento vstup je zajištěn fyzickou ostrahou objektu. Vstupní dveře jsou protipožární. Druhá vstupní cesta vede přes vnitroblok. Slouží pro parkování vozidel zaměstnanců objektu, eventuálně návštěvám (dodavatelé, údržba) a to především v pracovní hodiny. Tento příjezdový přístup je jištěn závorou, kterou obsluhuje fyzická ostraha objektu. Vnitroblok je zajištěn kamerovým systémem, tzn. každý pohyb v tomto vnitrobloku je sledován a zaznamenáván. V případě, že si zaměstnanec musí z vážných důvodů vzít s sebou do práce nezletilé dítě, vykonává tak na vlastní nebezpečí. Zaměstnanec je povinen po celou dobu jeho pobytu v objektu dodržovat nad dítětem osobní dozor. Dítě by mohlo svým jednáním a chováním způsobit škodu sobě, ostatním osobám či zaměstnavateli. V případě škody způsobené dítětem odpovídá v plném rozsahu zaměstnanec.

V budově se aktuálně nacházejí v každém patře hasicí přístroje, které se v případě vzniklého požáru použijí. Aktuálně se v budově nachází 6 hasicích přístrojů (v přízemním patře se nachází 2x, přímo na chodbě a u ostrahy objektu). Dalším důležitým bodem je evakuační a požární plán budovy. Tyto plány visí v každém patře naproti schodišti. V případě nenadálé události jsou tedy na velmi přehledném místě. Chodby jsou označeny evakuačními šipkami, které mají za cíl zaměstnanec navést k rychlému a bezpečnému úniku z objektu. Schodiště budovy je zabezpečeno reflexními páskami nacházejícími se vždy na začátku schodu a na jeho konci.

Objekt má v současné době tato bezpečnostní opatření, která zajišťují bezpečnost pracoviště:

- fyzickou ostrahu objektu,
- technické prostředky,
- „Help me“ systém,
- osobní alarm,
- zabezpečení prostřednictvím IT technologií,
- místní rozhlas,
- nouzový východ,
- pravidelné školení zaměstnanců.

5.2.1 Fyzická ostraha objektu

Fyzická ostraha objektu je zajišťována vyškolenými pracovníky bezpečnostní firmy. Dříve ovšem tuto službu vykonávali vlastní zaměstnanci či pověření zaměstnanci. Pracovník kontroluje nepovolané osoby jak při vstupu, tak i odchodu z objektu. Služba je zajištěna pouze v pracovní dny v provozní dobu, poté se objekt uzamyká. Mimo provozní dobu je objekt zabezpečen technickými prostředky. Fyzická ostraha slouží taktéž jako vrátnice, a v případě mimořádné události vykonává činnost ohlašovny. Nahlášení se provádí prostřednictvím místního rozhlasu. V objektu se nachází místnosti se zvláštním režimem (spisovna, serverovna a pokladna). V případě návštěvy těchto místností cizím zaměstnancům je třeba, aby se tato osoba zapsala do záznamu zvaného „Zvláštní povolení na vstup do budovy cizím zaměstnancem konající práce pro pracoviště“ umístněném u fyzické ostrahy objektu. Tento záznam obsahuje název firmy/jméno osoby, datum narození, důvod návštěvy, datum a čas příchodu a odchodu, podpis. Nedílnou součástí tohoto záznamu je podpis pověřeného pracovníka pracoviště, a to z toho důvodu, aby bylo patrné, že se o této návštěvě ví.
Fyzická ostraha objektu mimo výše uvedené vede provozní deník, ve kterém jsou zaznamenávány jakékoliv nestandardní stavy, mimořádné výpůjčky klíčů a v neposlední řadě bezpečnostní incidenty.

5.2.2 Technické prostředky

V dnešní době by každý větší objekt měl mít alespoň pár technických prostředků, které odradí pachatele, zmírní případné škody/ztráty, a to jak na lidských životech, tak na majetku organizace. Popisovaný objekt je zabezpečen následujícím:

- mechanické prostředky (oplocení, vstupní otvorové výplně, trezory),
- zařízení elektronické zabezpečovací signalizace (dále jen „EZS“), vyvedené na pult centrální ochrany příslušné smluvně zajištěné organizace,
- tísňové systémy a hlásiče, které jsou součástí EZS,
- elektrická požární signalizace,
- docházkový systém,
- kamerový systém. [32]

Mechanické prostředky

Cílem těchto prostředků je zamezení jakéhokoliv počinu pachatele. Tyto prostředky jsou velmi důležité, jelikož se v objektu nacházejí jak cenné informace, tak i majetek organizace. Mechanické prostředky pracoviště v současné době:

a) *bezpečnostní zámky* – vstupy do objektu jsou opatřeny bezpečnostními zámky, které splňují odolnost proti neoprávněnému otevření pachatelem. Klíče od hlavního vstupu do objektu má pouze ředitel pracoviště, jeho zástupce, správce budovy a ostraha. V případě, že by si řadový zaměstnanec zapůjčil klíč od jiné místnosti než jemu přidělené, je třeba, aby se zapsal do evidenční knihy zapůjčených klíčů.
b) *bezpečnostní fólie* – okna a dveře v přízemních patrech nejsou chráněny mřížemi, ale bezpečnostními fóliemi. Bezpečnostní fólie v prvé řadě plní funkci odolávání tlaku a dále mají za cíl zabránit roztříštění výplňového skla.
c) *oplocení* – ve vnitrobloku se nachází oplocení, jelikož vnitroblok sousedí s dalšími třemi objekty. Oplocení se nachází po celém prostranství, které patří k objektu. Oplocení bylo nedávno měněno za nové.
d) *trezor* – slouží pro úschovu cenných údajů, informací a peněžní hotovosti. Je umístěn v místnosti se zvláštním režimem. V místnosti je instalována přepážka, aby se tak zabránilo případnému poničení trezoru a vniknutí do trezoru. Klíče od této místnosti má pouze ředitel a pověřený pracovník. Úklidový pracovník do této místnosti může pouze v přítomnosti pracovníka pokladny. V ostatních místnostech je úklid prováděn po pracovní době bez přítomností zaměstnanců.

Zařízení elektronické zabezpečovací signalizace

Úkolem EZS je ochrana vstupu do samotného objektu a místností. V každé místnosti jsou umístěna prostorová čidla. Prostorová čidla slouží k identifikaci pohybu v objektu. Vstup do objektu je umožněn pouze po zadání individuálního vstupního kódu EZS. Pro zvýšení bezpečnosti se tento kód nepravidelně mění. Oprávnění k ovládání EZS (vypínání, zapínaní) mají pouze pověření zaměstnanci na základě přidělených vstupních kódů. Zásah do EZS mimo rámec zadávání kódů pověřenými zaměstnanci je přísně zakázán. Tito zaměstnanci jsou k této manipulaci řádně proškoleni. Kontrolu jejich zaškolení zajišťuje ředitel pracoviště nebo jiná oprávněná osoba k těmto úkonům. Seznam aktuálních pověřených osob včetně pořadí přidělených kódů pro EZS i seznamu přidělených klíčů do objektu je uložen u ředite-

le pracoviště. Servis EZS je smluvně zajištěn (1x do roka, případně dle potřeby). Na pult centralizované ochrany (dále jen PCO) je zařízení EZS připojeno rádiovým spojením, GSM signálem, telefonní linkou a internetem. V případě vyhlášení poplachu je vyslán signál na PCO, který následně vyšle zásahovou skupinu za účelem prozkoumání objektu.

Na povel Policie, HZS, IZS a příslušné smluvně zajištěné firmy zabezpečující EZS jsou pověření zaměstnanci povinni se neprodleně dostavit na požadované místo a zajistit potřebnou součinnost s těmito orgány. V praxi to znamená, že by těmto orgánům byl umožněn vstup do uzamčeného objektu, aniž by byl narušen jejich prostředky, a byli zavedeni k místu, které vykazovalo neočekávaný pohyb pachatele.

Obr. 6. Dálková ostraha objektu. [28]

Objekty, které mají nainstalovány EZS, mohou využít jejích dalších funkcí, jako jsou např. pohybový detektor, akustický detektor nebo detektor otřesu. Mezi další funkce EZS se řadí siréna. Tento prvek je využíván v popisovaném objektu. V případě poplachu hlásí signál o síle 90-135 dB tak, jak dovoluje norma. Jedná se o pasivní způsob využití EZS. Úkolem sirény je zastrašit pachatele a upozornit na vniknutí do objektu.

Elektronická požární signalizace

Tento systém chrání objekt ve vybraných prostorech z pohledu požárního rizika. Systém je instalován ve všech místnostech objektu. Na chodbách jsou nainstalovány tlačítkové hlásiče. Hlásiče jsou instalovány na únikových cestách (naproti schodišti). Při vzniku požáru mají sloužit k upozornění, že v objektu vznikl požár, tlačítko spustí osoba, která vznik požáru zpozorovala. EPS je napojen na hasiče přes PCO. EPS se skládá z následujících zařízení:

- kouřový detektor,
- ruční spouštěč signálu,
- automatické hasící systémy,
- detektor úniku plynu.

Pracoviště má z výše uvedených instalován pouze kouřový detektor a ruční spouštěč signálu. Kouřový detektor je kontrolován jedenkrát do roka prostřednictvím pověřeného pracovníka smluvně sjednané firmy.

Obr. 7. Hlásič požáru. [vlastní zpracování]

Docházkový systém

Docházkový systém využívají pracovníci objektu (jak při vstupu do objektu, tak odchodu). Slouží taktéž jako bezpečnostní prvek. Díky tomuto systému je v případě mimořádné události (např. vzniku požáru) možno zjistit, kolik osob se nachází v objektu a kolik jich již objekt opustilo.

Obr. 8. Docházkový systém. [vlastní zpracování]

Kamerový systém

Uzavřený kamerový televizní systém (Closed Circuit Television, dále jen „CCTV") pracovišti slouží jako preventivní zajištění bezpečnosti celého objektu, osob a majetku nacházejícího se uvnitř. Provozováním CCTV za účelem preventivního zajišťování bezpečnosti objektu lze provozovat bez souhlasu vstupujících osob, neboť pracoviště nezpracovává z kamerového systému osobní údaje, z tohoto hlediska nevyžaduje souhlasu subjektu ve smyslu § 4 písm. d) zákona č. 101/2000 Sb. – o ochraně osobních údajů. Záznamy z CCTV se uchovávají obvykle 24 hodin, poté jsou automaticky smazány. O zpřístupnění uchovaných záznamů mohou zažádat oprávněné subjekty např. Police ČR či státní zástupce. Objekt informuje vstupující osoby o užití CCTV nápisem umístěným před hlavním vstupem a podél celého objektu – „Objekt je monitorován kamerovým systémem“.

Můžeme se setkat se dvěma druhy CCTV:

- analogové,
- IP kamery.

Uvedené druhy CCTV se od sebe rozlišují způsobem zapojení. Analogové kamery používají koaxiální kabel, který je náchylný na indukci v zapojení a omezenost nastavení každé kamery zvlášť. IP kamery jsou výhodné z důvodu analýzy. IP kamery umožňují analyzovat obličej (upozorní ostrahu na příchod problémové osoby, se kterou měli již konflikt) a analyzovat SPZ (na základě SPZ umožní otevřít závoru). Pracoviště používá systém analogový. CCTV je složen z kamer a kamerového systému. Ukládání záznamu lze provádět místně nebo vzdáleně, tzn., záznamové zařízení se nachází přímo v objektu nebo mimo něj.

Výhody místního úložiště:

- lepší kvalita záznamu.

Výhody vzdáleného úložiště:

- bezpečnost v případě zneužití záznamu.

Nevýhody místního úložiště:

- snadnější zneužití záznamu či jeho zneškodnění.

Nevýhody vzdáleného úložiště:

- horší kvalita záznamu.

5.2.3 Help me systém

Tento systém funguje na bázi tichého upozornění fyzického konfliktu přímo v kancelářích zaměstnanců. Funkce tohoto systému je založena na spolupráci s okolními počítači a mobilními telefony pověřených osob. Každý zaměstnanec objektu má tento systém instalován na ploše obrazovky PC. Jestliže dojde ke konfliktu, kdy zaměstnanci hrozí bezprostřední nebezpečí, přímo klikne na ikonu tohoto systému či zmáčkne klávesovou zkratku, a tím spustí na PC ostatních zaměstnanců žádost o pomoc. Pověřené osoby v co nejkratší době dorazí na místo nahlášení a zjistí stav nahlášeného případu, dle možností posléze poskytnou zaměstnanci potřebnou pomoc.

Obr. 9. Ikona Help me systému. [vlastní zpracování]

5.2.4 Osobní alarm

Alarm slouží pro nouzové upozornění okolí v případě útoku na zaměstnance pracoviště. Tento alarm má pouze určitá skupina zaměstnanců (sekretariát ředitele, podatelna, pokladna, IT pracovníci, lékařská posudková služba). Princip spočívá v odtržení poutka, kdy dojde ke spuštění sirény o hlasitosti 120 dB. Po zasunutí kolíků zpět do alarmu se zařízení vypne. Alarm slouží výhradně k výše uvedeným účelům. V případě přiložení k uchu může dojít k poškození sluchu.

Obr. 10. Osobní alarm. [vlastní zpracování]

5.2.5 Místní rozhlas

Místní rozhlas se v objektu využívá zejména k zajištění bezpečné evakuace všech osob v objektu. Prostřednictvím rozhlasu se vysílají živé přenosy. K tomuto zařízení má přístup pouze ředitel pracoviště, ostraha objektu a pověřená osoba. Zařízení, prostřednictvím kterého se nahlásí evakuace, případně jiná mimořádná událost, se nachází v místnosti sekretariátu ředitele a na vrátnici. V jednotlivých místnostech se nachází samotný rozhlasový reproduktor, díky němuž zaměstnanci uslyší hlášení o evakuaci objektu.

5.2.6 Nouzový východ

Nouzový východ slouží zaměstnancům objektu pro rychlou evakuaci v případě mimořádné události. O tom, kde se nouzový východ nalézá, vědí zaměstnanci díky prováděnému školení pracovníkem BOZP. Jedná se o nejkratší a nejbezpečnější únikovou cestu z objektu.

5.2.7 Zabezpečení prostřednictvím IT technologií

Bezpečnost je důležitou součástí informačních systémů obzvlášť v současné době, kdy probíhá drtivá většina komunikace a oběhu dokladů v elektronické podobě. Níže v textu budou popsána opatření, která mají za cíl eliminovat a zamezit kybernetickému útoku z vnějšího a vnitřního prostředí na dané pracoviště. Je třeba říci, že další důležitá opatření k této tématice jsou zřizována bezprostředně z ústředí IT a řadí se mezi utajované informace, které mi nemohou být poskytnuty ke zpracování této problematiky.

Firewall

Jde o síťové zařízení, které slouží k řízení a zabezpečování síťového provozu mezi sítěmi s různou úrovní důvěryhodnosti a zabezpečení. Zjednodušeně se dá říci, že slouží jako kontrolní bod, který definuje pravidla pro komunikaci mezi sítěmi, které od sebe odděluje. Toto zařízení určuje, komu a s kým komunikaci povolí a komu ji zakáže.

Antivirová ochrana

Je počítačový software, jehož funkcí je identifikace, odstraňování a eliminace počítačových virů a jiného škodlivého software (malware).

K zajištění této úlohy se používají dvě odlišné techniky:

- *prohlížení souborů na lokálním disku*, které má za cíl nalézt sekvenci odpovídající definici některého počítačového viru v databázi,
- *detekcí podezřelé aktivity* nějakého počítačového programu, který může značit infekci. Tato technika zahrnuje analýzu zachytávaných dat, sledování aktivit na jednotlivých portech či jiné techniky.

Úspěšnost závisí na schopnostech antivirového programu a aktuálnosti databáze počítačových virů. Aktuální virové databáze se dnes nejčastěji stahují z Internetu.

Zálohování a archivace

Záchrana dat se řadí mezi komplikované, nákladné a někdy nemožné řešení. To vše záleží na okolnostech, které potřebu obnovy dat vyvolají. Nemocím je lépe předcházet než je léčit a v oblasti dat platí prevence trojnásob. Prosté zálohování dat je pouze jedním a nejzákladnějším kamínkem v celé mozaice opatření. Základem je dobře navržená a zkonfigurovaná síťová infrastruktura a uživatelé proškolení ke správnému "síťovému chování". Dále pak správně navržený systém zálohování a archivace s minimem vstupu lidského faktoru. V neposlední řadě pak trvalý servisní dohled nad servery a tím možnost včasné diagnostiky potenciálních problémů.

Dále je zabezpečení řešeno pomocí následujících dvou nástrojů:

- autentizací – ověření identity osoby, která chce začít pracovat s informačním systémem (pro autentizaci se zpravidla používají uživatelská jména v kombinaci s heslem, přístupové kódy, případně certifikáty),
- autorizací – ověření, že daná osoba má právo provést určitou akci (spustit aplikaci, nahlížet do dat).

Pro snížení kybernetických útoků má pracoviště zpracovanou dokumentaci, která obsahuje analýzu rizik a přijatá opatření eliminující kybernetické útoky. Proškolování zaměstnanců spočívá v samostudiu dané problematiky a zakončení testem, který má ověřit znalosti z bezpečnosti informací a ochraně osobních údajů. [33]

5.2.8 Školení zaměstnanců

Školení zaměstnanců pracoviště vyplývá ze zákona č. 262/2006 Sb., zákoník práce, zákona č. 309/2006 (zákon o zajištění dalších podmínek bezpečnosti a ochrany zdraví při práci),

souvisejících právních předpisů a směrnice pracoviště. Školení probíhá 1x za dva roky. Účelem směrnice je, aby bylo zajištěno jednotné plnění úkolů na úseku BOZP a vymezení povinnosti vedoucích zaměstnanců, jednotlivých zaměstnanců a odborných zaměstnanců na úseku BOZP při zajišťování BOZP. Úkoly vyplývající z dané směrnice pracoviště musí plnit všichni zaměstnanci, kteří mají své povinnosti, které budou uvedeny níže. K těmto účelům má pracoviště technika BOZP, který plní povinnosti v této oblasti.

Technik BOZP je pro pracoviště:

- poradním orgánem ředitele pracoviště a ostatních vedoucích,
- kontrolním orgánem z pověření ředitele pracoviště.

Povinnosti technika BOZP:

- zhotovuje dokumentaci BOZP,
- zpracovává vnitřní organizační směrnice BOZP,
- spravuje agendu pracovních úrazů a nemocí z povolání v souladu s právními předpisy,
- vykonává kontrolní činnost BOZP,
- spolupracuje po odborné stránce s vedoucími zaměstnanci při provádění hodnocení rizik a navrhuje preventivní opatření k odstraňování a omezování rizik,
- provádí kategorizaci pracovních činností,
- provádí odborné školení všech zaměstnanců pracoviště,
- pravidelně jedenkrát za rok organizuje prověrku BOZP,
- absolvuje odbornou přípravu pro získání odborné způsobilosti dle § 9 zákona o BOZP.

Povinnosti vedoucích zaměstnanců:

- zajišťují plnění právních předpisů BOZP,
- zajišťují ve spolupráci s technikem BOZP identifikaci, hodnocení a prevenci rizik,
- přijímají opatření pro případy zdolávání mimořádných událostí,
- organizují poskytování první pomoci zaměstnancům pracoviště,
- odpovídá za zpracování dokumentů o pracovních úrazech,
- při zařizování pracovišť a nákupu nových technických zařízení dbají, aby zařízení splňovala požadavky BOZP,
- dohlíží na to, aby vybraná technická zařízení obsluhovali pouze zaměstnanci odborně způsobilí,

- kontrolují, zda zaměstnanci nejsou pod vlivem alkoholu či jiné návykové látky, tuto kontrolu provádějí v případě, jestliže mají podezření,
- zabezpečují plnění zákazů kouření na pracovištích dle platných předpisů.

Povinnosti zaměstnanců:

- musí dbát o svou vlastní bezpečnost, o své zdraví i o bezpečnost a zdraví osob, kterých se bezprostředně dotýká jeho jednání, případně opomenutí při práci,
- podrobit se preventivním prohlídkám a vyšetřením,
- dodržovat právní a ostatní předpisy a pokyny zaměstnavatele k zajištění BOZP, s nimiž byli řádně seznámeni,
- zachovávat při práci stanovené pracovní postupy, používat stanovené pracovní prostředky a dopravní prostředky,
- musí používat ochranné pomůcky,
- zúčastnit se výcviku a školení BOZP,
- nepožívat alkoholické nápoje a jiné návykové látky na pracovišti a v pracovní době i mimo pracoviště a nevstupovat pod jejich vlivem na pracoviště,
- podrobit se na pokyn oprávněného vedoucího zaměstnance písemně určeného zaměstnavatelem zjištění, zda není pod vlivem alkoholu či jiných návykových látek,
- neporušovat zákazy kouření,
- ohlašovat svému nadřízenému vedoucímu zaměstnanci závady BOZP, které mohou ohrozit jejich život či zdraví, případně život nebo zdraví jiných osob,
- nahlásit pracovní úraz. [32]

5.3 Analýza bezpečnostních rizik

Po zvážení zjištěných bezpečnostních rizik jsem si zvolila analýzu pomocí metody What – if s cílem zhodnocení celkových dopadů těchto rizik. Výběr nejvážnějších rizik pro tuto analýzu probíhal formou brainstormingu a následných osobních rozhovorů s jednotlivými zaměstnanci. Rozhovory probíhaly se 7 pověřenými pracovníky pracoviště. Výsledky budou zobrazeny prostřednictvím skórovací metody s mapou rizik.

Analyzovaná bezpečnostní rizika a stupnice ohodnocení

Na základě provedeného brainstormingu a rozhovoru byla stanovena níže uvedená bezpečnostní rizika *(Tab. 1.*). Rizika budou hodnocena stupnicí rizik *(Tab. 2.)* a dopadem bezpečnostních rizik *(Tab. 3.).*

Tab. 1. Analyzovaná bezpečnostní rizika pracoviště. [vlastní zpracování]

Pořadové číslo rizika	Analyzovaná bezpečnostní rizika
1.	Zneužití identity fyzické osoby
2.	Poškození technického vybavení
3.	Selhání programového vybavení
4.	Kybernetický útok z vnější či vnitřní komunikační sítě
5.	Škodlivý kód
6.	Narušení fyzické bezpečnosti
7.	Přerušení dodávek elektrické energie, vody a tepla
8.	Požár

Tab. 2. Stupnice ohodnocení bezpečnostních rizik. [vlastní zpracování]

Pravděpodobnost vzniku rizika – P	Komentář	Hodnocení
Velmi častý výskyt	Trvalé ohrožení	6
Častý výskyt	Velmi často opakovaný výskyt situací	5
Občasný výskyt	Situace vznikne několikrát po dobu pracovního dne	4
Možný výskyt	Situace není příliš pravděpodobná, ale nelze ji vyloučit	3
Nepravděpodobný výskyt	Výskyt nežádoucí situací je zcela ojedinělá	2
Téměř nemožný výskyt	Vznik situace je téměř nemožná	1

Tab. 3. Stupnice dopadu bezpečnostních rizik. [vlastní zpracování]

Dopad	Hodnocení
Kritický	6
Zásadní	5
Střední	4
Nízký	3
Zanedbatelný	2
Bezvýznamný	1

5.4 Zhodnocení bezpečnostních rizik

Riziko č. 1: Zneužití identity fyzické osoby

Zaměstnanci pracují s velmi důležitými a citlivými údaji. Zaměstnanec má za úkol s těmito údaji náležitě pracovat, z tohoto důvodu je třeba, aby dbal určitých postupů. Mezi tyto postupy řadíme, např. informace se nesmějí vynášet mimo organizaci, v době nepřítomnosti se zaměstnanec musí odhlásit z počítače, aby jiná osoba nemohla pracovat či čerpat údaje z jeho počítače. Uživatel PC se přihlašuje pomocí přístupové karty, která je pod přístupovým heslem (dále jen „PIN“). Zaměstnanec nesmí mít PIN na přístupných místech, poznačen na přihlašovací kartě apod. Je na zaměstnanci, jak naloží s přihlašovací kartou. Doporučovaným opatřením je uzamčení do zásuvky či skříně. V případě jejího odcizení či ztráty spadá veškerá zodpovědnost na zaměstnance karty. V objektu provádí úklidovou službu externí firma, a je tedy možné, že by se k těmto údajům mohla dostat neoprávněná osoba a s těmito údaji nějakým způsobem nakládat, z tohoto důvodu je na pracovišti dodržována zásada prázdného stolu, tím se přechází případnému odcizení. Veškeré úložné prostory s citlivými údaji jsou po pracovní době uzamčeny. Speciální pozornost je věnována bezpečnostním opatřením při převozu spisového materiálu mezi pracovišti. Převoz musejí provádět vždy

dvě osoby, nikoliv jedinec. Veškeré postupy a nařízení jsou prováděny interními předpisy organizace.

Důsledek: porušení směrnic organizace, kárné opatření.

Tab. 4. Zneužití identity fyzické osoby. [vlastní zpracování]

Kvantifikace rizik	1.	2.	3.	4.	5.	6.	7.	Průměrná hodnota	
Možnost výskytu (pravděpodobnost)	3	2	3	3	2	2	2	2,4	
Dopad	5	6	5	5	5	5	5	5,1	
Ocenění rizika = průměrná hodnota pravděpodobnosti x průměrná hodnota dopadu									12

Riziko č. 2: Poškození technického vybavení

Mezi technické vybavení pracoviště zejména patří výpočetní technika, kterou všichni zaměstnanci každodenně využívají. V případě jejího poškození dochází k zásadním ztrátám (např. finančním či ke ztrátě informací, které nejsou zálohované). Každý zaměstnanec je povinen se seznámit s návodem k obsluze těchto zařízení. Jestliže zaměstnanec technické vybavení poškodí, je třeba, aby tuto skutečnost nahlásil co nejdříve svému nadřízenému. Ten poté tuto škodu nahlásí škodní komisi, která postupuje dle interních směrnic. Škodu zaměstnanec uhradí buďto stržením peněz přímo ze mzdy (provede personální oddělení) nebo hotovostně (na pokladně).

Pravidla pro provoz výpočetní techniky:

a) zaměstnanec nesmí:
   - nahrávat data a software z jakýkoliv datových nosičů do PC,
   - poskytnout svůj PC jiné osobě, která nemá s organizací uzavřený pracovní poměr,
   - sdělit své přihlašovací heslo sloužící k přihlášení do systému,
   - umožnit přístup neoprávněným osobám do svého PC a sítě.

b) zaměstnanec musí:

- používat přidělený PC s využitím evidovaného programového vybavení efektivně a výhradně k plnění pracovních úkolů,
- umožnit provedení antivirové kontroly všech komponentů z vnějšího prostředí používané ke své práci,
- dodržovat pravidla bezpečné komunikace v počítačové síti, zejména připojení na Internet, se zřetelem na ochranu osobních údajů,
- neprodleně nahlásit příslušnému administrátorovi počítačové sítě veškeré závažné problémy, týkající se provozu a zásadní problémy s funkčností systému.

Důsledek: nemožnost vykonávat práci, infikace PC, porušování pracovní kázně a směrnic organizace, kárná opatření.

Tab. 5. Poškození technického vybavení. [vlastní zpracování]

Kvantifikace rizik	**1.**	**2.**	**3.**	**4.**	**5.**	**6.**	**7.**	**Průměrná hodnota**	
Možnost výskytu (pravděpodobnost)	4	3	3	4	5	3	3	3,5	
Dopad	6	5	5	5	6	5	6	5,4	
Ocenění rizika = průměrná hodnota pravděpodobnosti x průměrná hodnota dopadu									19

Riziko č. 3: Selhání programového vybavení

K tomu, abychom mohli fungovat na počítačích, potřebujeme programové vybavení neboli software. Software dělíme na systémový a aplikační. Systémový software uživatelům ulehčuje účelně ovládat počítač. Bez tohoto systému bychom nemohli vůbec pracovat. Díky systémovému softwaru máme přístup k ostatním aplikacím. Lze tedy konstatovat, že je to mezičlánek nebo prostředník mezi hardwarem a aplikačním softwarem. Aplikační software umožňuje běžnému uživateli pracovat v různých programech a aplikacích. Aplikační software se dělí do čtyř skupin: kancelářské programy, grafické programy, vývojové programy a zábavní programy. Pracoviště má v počítačích nainstalovány pouze kancelářské programy.

Mezi tyto programy zejména spadají MS Office (MS PowerPoint, MS Outlook, MS Word, MS Excel), Adobe Acrobat Reader a programy, které zaměstnanci využívají pro svou danou pracovní oblast (např. ekonomické oddělení pracuje s programem SAP). V případě selhání výše uvedených programů zaměstnanci přijdou o svá aktuálně neuložená data a nebudou moci vykonávat svou pracovní náplň v rozsahu, který se od nich očekává. Daná práce se tak zpozdí. Jestliže k takovéto situaci dojde, je třeba, aby se tato skutečnost okamžitě nahlásila IT pracovníkům, a ti se pokusili problém vyřešit v co nejkratším možném čase. Jednou z možností, jak ohlásit IT problém je, že se vyplní na intranetu žádost o vyřešení incidentu nebo se přímo telefonicky spojí s IT pracovníkem.

Důsledek: nemožnost vykonávat práci, zpoždění pracovních záležitostí.

Tab. 6. Selhání programového vybavení. [vlastní zpracování]

Kvantifikace rizik	1.	2.	3.	4.	5.	6.	7.	Průměrná hodnota	
Možnost výskytu (pravděpodobnost)	6	5	6	5	6	5	5	5,4	
Dopad	6	5	5	6	6	6	6	5,7	
Ocenění rizika = průměrná hodnota pravděpodobnosti x průměrná hodnota dopadu									31

Riziko č. 4: Kybernetický útok

Kybernetické útoky se v současné době velmi rozmáhají a řadí se mezi aktuální témata. Staly se všudypřítomnou realitou v řadě odvětví. Ať už se jedná o politické, firemní či osobní útoky, vždy mají za cíl poškodit anebo ukrást citlivá data uživatelů. Mezi časté případy kybernetického útoku patří „nabourání se“ do emailové schránky, kdy uživatel netuší, že se mu do jeho schránky naboural útočník, který může místo něj odesílat podvodné emaily. Za těmito útoky jsou tzv. hackeři, kteří se neustále zdokonalují. Proto by každá organizace, která pracuje s citlivými daty, o která nechce přijít, měla opatření proti kybernetickým útokům neustále udržovat na vysoké úrovni. V případě, že by pracoviště napadl hacker,

který by měl za cíl poškodit dobré jméno organizace, mělo by to pro celou organizaci zásadní vliv.

Důsledek: poškození jména společnosti, únik citlivých a osobních dat.

Tab. 7. Kybernetický útok. [vlastní zpracování]

Kvantifikace rizik	1.	2.	3.	4.	5.	6.	7.	Průměrná hodnota	
Možnost výskytu (pravděpodobnost)	1	3	3	2	3	3	3	2,5	
Dopad	6	6	6	6	6	6	6	6	
Ocenění rizika = průměrná hodnota pravděpodobnosti x průměrná hodnota dopadu									15

Riziko č. 5: Škodlivý kód

Škodlivý kód, taktéž nazýván malware, je program, jehož cílem je vniknout do cizího zařízení či poškodit počítačový systém. Malware se řadí mezi zákeřné programy. Spadají sem počítačové viry, červy, trojské koně a další. Proti tomuto se organizace brání instalováním antivirů a dalšími opatřeními, která nemohu z důvodu ochrany citlivých údajů zmínit.

Důsledek: selhání systému, přeinstalování PC, znemožnění práce, únik citlivých informací a osobních dat.

Tab. 8. Škodlivý kód. [vlastní zpracování]

Kvantifikace rizik	1.	2.	3.	4.	5.	6.	7.	Průměrná hodnota	
Možnost výskytu (pravděpodobnost)	6	4	3	5	4	3	3	4	
Dopad	5	5	4	4	4	5	5	4,5	
Ocenění rizika = průměrná hodnota pravděpodobnosti x průměrná hodnota dopadu									18

Riziko č. 6: Narušení fyzické bezpečnosti

Narušení fyzické bezpečnosti upravuje Vyhláška č. 528/2005 Sb. o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů. Proti těmto opatřením je popisované pracoviště chráněno příslušnými opatřeními. Tato opatření (zmíněny v kapitole výše) považuji za dostatečná, ovšem i tato opatření mohou pachatelé zdolat a vniknout či porušit objekt a majetek uvnitř. V případě odcizení citlivých dat organizace by škody byly nevyčíslitelné. Co se týče samotného objektu či majetku uvnitř, tyto hodnoty jsou lehce nahraditelné.

Důsledek: finanční náklady (na opravu, koupi nového zařízení), únik citlivých informací a osobních dat.

Tab. 9. Narušení fyzické bezpečnosti. [vlastní zpracování]

Kvantifikace rizik	1.	2.	3.	4.	5.	6.	7.	Průměrná hodnota	
Možnost výskytu (pravděpodobnost)	3	2	3	2	3	2	3	2,6	
Dopad	5	4	5	4	4	4	4	4,3	
Ocenění rizika = průměrná hodnota pravděpodobnosti x průměrná hodnota dopadu									11

Riziko č. 7: Přerušení dodávek elektrické energie, vody a tepla

Výpadek elektřiny je v dnešní době těžko představitelná věc. Bez elektřiny bychom nemohli vykonávat mnoho úkonů, na které jsme již zvyklí. Pracoviště je závislé na dodávce elektrické energie, bez které by zaměstnanci nemohli pracovat např. s počítači, tiskárnami či telefony. Všechny tyto úkony potřebují k tomu, aby byl nějakým způsobem zachován chod pracoviště. V době výpadku by taktéž byl neaktivní např. EZS a kamerový systém. Pro pracoviště se tedy jedná o závažnou skutečnost, která se naštěstí tak často nestává. Jestliže k výpadku dojde, je to otázka pár minut (obvykle to bývá v dopoledních hodinách). V praxi to znamená, že se v daném objektu nachází zaměstnanci a ostraha objektu, nedojde tedy k narušení bezpečnosti z vnějšího okolí. Problém ovšem nastává, jestliže se v době výpadku přepravuje

osoba ve výtahu. Dojde tak k jeho „zaseknutí“. Osoba uvnitř výtahu tak musí vyčkat, než bude obnovena dodávka elektrické energie. Pokud by k této situaci nedošlo během delší doby, musel by situaci řešit údržbář objektu a osobu z výtahu pomocí techniky vytáhnout. Pracoviště nemá svůj záložní zdroj energie, záložní zdroj má pouze serverovna. V případě odstávky vody je v co nejkratší době povolána cisterna s užitkovou vodou, která je k dispozici pro každého, kdo ji v danou chvíli potřebuje. Dojde-li k přerušení dodávky tepla, je povolán údržbář budovy a danou situaci se snaží vyřešit sám. Jestliže nalezne problém, který nezvládne opravit použitím svých prostředků, je zavolána firma, zabývající se touto problematikou.

Důsledek: zvýšené riziko vstupu neoprávněné osoby, ztráta informací, nemožnost vykonávat práci, snížený komfort zaměstnanců.

Tab. 10. Přerušení dodávek elektrické energie, vody a tepla. [vlastní zpracování]

Kvantifikace rizik	1.	2.	3.	4.	5.	6.	7.	Průměrná hodnota	
Možnost výskytu (pravděpodobnost)	3	4	4	4	3	4	3	3,6	
Dopad	6	6	5	4	5	5	4	5	
Ocenění rizika = průměrná hodnota pravděpodobnosti x průměrná hodnota dopadu									18

Riziko č. 8: Požár

V objektu nedochází k rizikovému provozu s nebezpečnými a hořlavými látkami. Tato skutečnost ovšem nevylučuje vznik požáru. V celém objektu je přísný zákaz kouření. V souvislosti s prevencí proti požárům či jiným mimořádným událostem mají zaměstnanci za povinnost zdržet se jakéhokoliv jednání, které by způsobilo zvýšení rizika vzniku požáru nebo jiné mimořádné události. Především je nutno udržovat průchodnost únikových cest a východů, přístupnost nástěnných hydrantů i přenosných hasicích přístrojů a zdržet se jakékoliv neoprávněné manipulace s prostředky protipožární ochrany. Taktéž je nepřípustné vynášení zařízení kanceláří a ukládat je v prostorách chodeb či na těchto místech skladovat

archivní a jiný materiál. Detailnější úkoly jednotlivých zaměstnanců v oblasti prevence proti požárům a vzniku mimořádných událostí jsou uceleny v požární dokumentaci a vyplývají z platných organizačních právních předpisů. Vzhledem k tomu, že se jedná o provoz administrativní, nebezpečí požáru by mělo závažné následky. Některé citlivé a osobní údaje nejsou digitalizovány, jsou pouze v papírové formě.

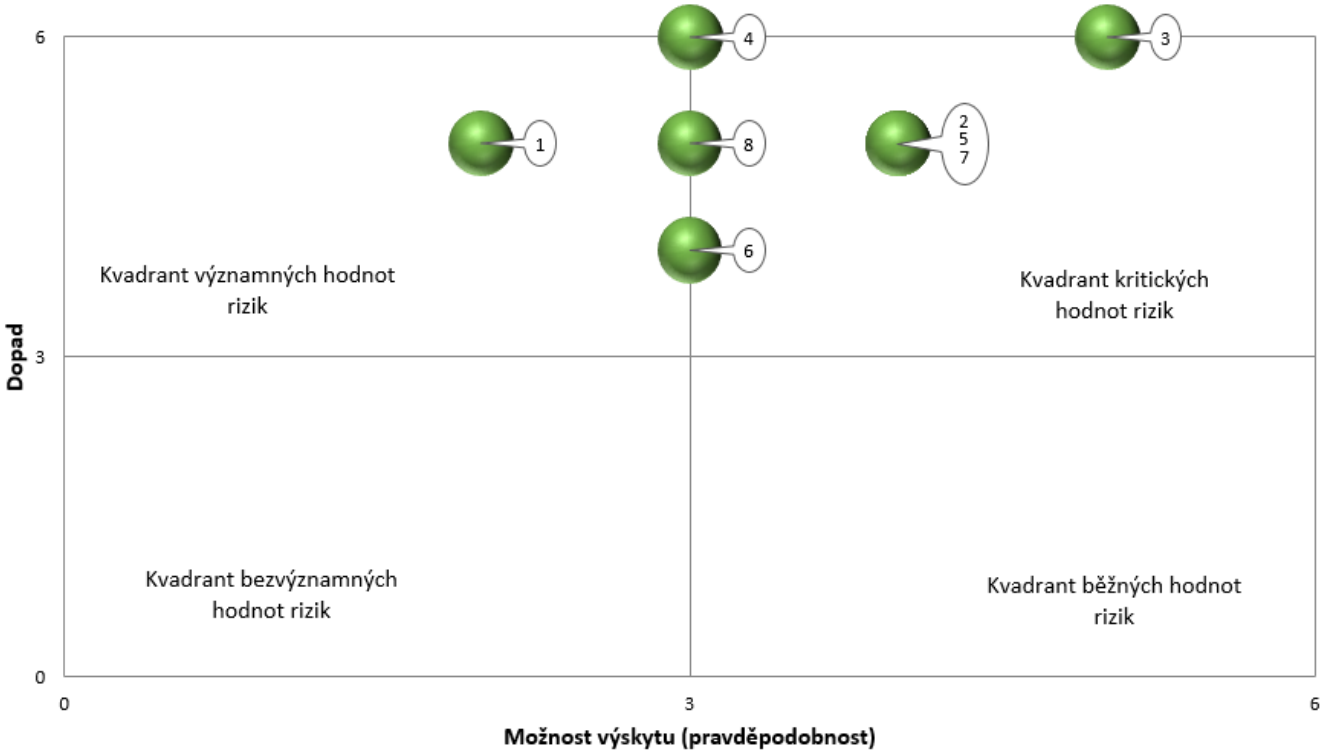
Důsledek: ztráta informací, nemožnost vykonávat práci.

Tab. 11. Požár. [vlastní zpracování]

Kvantifikace rizik	**1.**	**2.**	**3.**	**4.**	**5.**	**6.**	**7.**	**Průměrná hodnota**	
Možnost výskytu (pravděpodobnost)	3	3	2	2	3	2	3	2,6	
Dopad	6	5	6	5	5	5	6	5,4	
Ocenění rizika = průměrná hodnota pravděpodobnosti x průměrná hodnota dopadu									14

5.5 Vyhodnocení bezpečnostních rizik

Následující data byla zpracována na základě výše uvedeného brainstormingu. Zpracovaná mapa bezpečnostních rizik *(Obr. 11.)* prostřednictvím skórovací metody rozčlenila jednotlivá rizika do jednotlivých kvadrantů podle jejich významnosti pro pracoviště.



Obr. 11. Mapa rizik. [vlastní zpracování]

V kvadrantu kritických hodnot se nachází riziko č. 2 (poškození technického vybavení), č. 5 (škodlivý kód), č. 7 (přerušení dodávek elektrické energie, vody a tepla) a riziko č. 3 (selhání programového vybavení), jsou tedy hodnoceny jako nejvíce rizikové a zároveň s nejvyšší pravděpodobností výskytu. Na hranici kvadrantu významných a kritických hodnot rizik leží rizika č. 4 (kybernetický útok), č. 6 (narušení fyzické bezpečnosti) a riziko č. 8 (požár). Zbývající riziko č. 1 (zneužití identity fyzické osoby) se nachází v kvadrantu významných hodnot a jeho výskyt je tedy závažný, ale nejméně pravděpodobný. Lze tedy říci, že všechna výše uvedená rizika jsou pro organizaci zásadní.

6 NÁVRHY OPATŘENÍ KE SNÍŽENÍ RIZIK

Z vypracované analýzy rizik a dalších poznatků, které jsem mohla získat během zpracování bakalářské práce, bylo zjištěno, že pracoviště plní veškeré své povinnosti a dodržuje směrnice pracoviště. Dle mého názoru jsou bezpečností opatření, které v současné době pracoviště má, na velmi dobré úrovni. Doporučovala bych však několik návrhů pro optimalizaci bezpečnostní situace pracoviště.

Návrhy opatření pro pracoviště:

- kniha návštěv,
- přístupový turniket,
- bezpečnostní mříže do oken,
- digitalizace dat.

Kniha návštěv

V současné době pracoviště nemá zřízenou knihu návštěv pro osoby, které nemají oprávnění pro vstup do objektu (např. rodinný příslušník). Tato kniha by sloužila pro přehled osob, které navštíví tento objekt. V knize návštěv by mohly být uvedeny následující údaje:

- datum návštěvy,
- jméno návštěvy,
- čas příchodu,
- čas odchodu,
- jméno navštívené osoby,
- oddělení,
- podpis návštěvy.

Náklady na knihu návštěv jsou minimální, nevyžadují větší finanční zatížení pro pracoviště. Ceny za knihu návštěv se pohybují okolo 40,- Kč včetně DPH. Toto opatření je snadno aplikovatelné a lze jej zavést ihned, a to bez větších komplikací.

Přístupový turniket

Dle mého názoru by byla velkým přínosem instalace přístupových turniketů. Tato instalace by usnadnila pracovníkům ostrahy práci. Turniket by zamezil pohybu osob, jež nemají čip či jinou přístupovou kartu do objektu. Tento systém využívá mnoho firem (zároveň mohou sloužit jako docházkový systém), kde se předpokládá větší pohyb osob. Finanční náklady

jsou vyšší. Ceny se pohybují okolo 55 000,- Kč bez DPH a montáže. Je tedy na zvážení, zda by pracoviště bylo ochotno zakoupit takové zařízení.

Bezpečnostní mříže do oken

Jak již bylo zmíněno, v oknech nacházejících se ve spodních patrech jsou instalovány bezpečností fólie. Po konzultaci s bezpečnostním technikem bylo zjištěno, že by byla vhodná instalace bezpečnostních mříží. Instalací okenních mříží by tak byla ochrana účinnější než jen s bezpečnostními fóliemi. Na trhu je celá škála typů mříží a ceny se pohybují okolo 10 000,- Kč bez DPH za jedno okno včetně práce. Určitě stojí za zvážení, zda by nebylo vhodné toto opatření implementovat.

Žádné opatření nám nezaručí plnou ochranu před případnými riziky, ale může jej zmírnit.

Digitalizace dat

Digitalizace je proces, při kterém dochází k převodu papírových dokumentů do elektronické podoby. V současné době velmi využívaný způsob v organizacích, které se zabývají administrativní činností a oblastí účetnictví. Tento proces umožňuje jednodušší, levnější a efektivnější zacházení s dokumenty. V případě požáru tak organizace nepřijde o své dokumenty. K digitalizaci je potřeba skenovací zařízení a obslužný software. Ceny za skenovací zařízení jsou individuální, většinou se ceny pohybují od 3000,- Kč bez DPH. Co se týče cen za software, ceny jsou na vyžádání u dodavatelské firmy. Toto opatření se řadí taktéž mezi lehce aplikovatelné a je zde vidina velkého přínosu pro pracoviště.

ZÁVĚR

Cílem bakalářské práce byla analýza a charakteristika bezpečnostních rizik ve vybrané organizaci, respektive na pracovišti, jež spadá pod organizaci ABC.

V teoretické části jsem charakterizovala základní pojmy související s danou problematikou. Těmito pojmy mám na mysli především: definici rizika, zdroje a klasifikace rizik, typy bezpečnostních rizik, nebezpečí, bezpečnost a ochrana zdraví při práci, charakteristika pojmů organizace a veřejná správa. Závěr této části je věnován charakteristice analýzy rizik, kde je popsán obecný postup a metody analýzy rizik.

Úvodem praktické části je seznámení s organizací ABC a pracovištěm, ve kterém byla analýza bezpečnostních rizik aplikována. V krátkosti byla uvedena organizační struktura, historie a současnost organizace ABC. Pro zmíněnou analýzu rizik byla zvolena metoda What – if, brainstorming a skórovací metoda s mapou rizik. Výsledkem analýzy rizik bylo, že všechna analyzovaná bezpečnostní rizika mají na organizaci zásadní vliv a většina se pohybuje v kvadrantu kritických hodnot nebo na jeho pomezí s kvadrantem významných hodnot.

Závěrem bakalářské práce bylo navržení opatření ke snížení bezpečnostních rizik, které by mohla organizace začlenit do svých zabezpečovacích prvků a technik.

Bude mi velkou ctí, jestliže se mými návrhy pracoviště alespoň trochu inspiruje a do budoucna by proběhla implementace některých navržených opatření.

SEZNAM POUŽITÉ LITERATURY

Knižní zdroje:

[1] BARON, Ladislav. *Bezpečnost a ochrana zdraví při práci v malých a středních podnicích: příručka pro zaměstnavatele.* 2. vyd. Praha: TIGIS, 2004. ISBN 80-7071-248-1.

[2] DĚDINA, Jiří a Jiří ODCHÁZEL. *Management a moderní organizování firmy.* 1. vyd. Praha: Grada Publishing, 2007. Expert (Grada). ISBN 978-80-247-2149-1.

[3] HNILICA, Jiří a Jiří FOTR. *Aplikovaná analýza rizika ve finančním managementu a investičním rozhodování.* 1. vyd. Praha: Grada, 2009. Expert (Grada). ISBN 978-80-247-2560-4.

[4] KORECKÝ, Michal a Václav TRKOVSKÝ. *Management rizik projektů: se zaměřením na projekty v průmyslových podnicích.* 1. vyd. Praha: Grada, 2011. Expert (Grada). ISBN 978-80-247-3221-3.

[5] MERNA, Tony a Faisal AL-THANI. *Risk management: řízení rizika ve firm*ě. Vyd. 1. Brno: Computer Press, 2007. ISBN 978-80-251-1547-3.

[6] PALEČEK, Miloš. *Prevence rizik.* Vyd. 1. Praha: Oeconomica, 2006. ISBN 80-245-1117-7.

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

[8] ŠEDIVÝ, Marek a Olga MEDLÍKOVÁ. *Úspěšná nezisková organizace. 2*., aktualiz. a dopl. vyd. Praha: Grada, 2011. Management (Grada). ISBN 978-80-247-4041-6.

[9] ŠEFČÍK, Vladimír. *Analýza rizik.* Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009. ISBN 978-80-7318-696-8.

[10] TICHÝ, Milík. *Ovládání rizika: analýza a management*. Vyd. 1. V Praze: C.H. Beck, 2006. Beckova edice ekonomie. ISBN 80-7179-415-5.

[11] TITTELBACHOVÁ, Šárka. *Turismus a veřejná správa: průniky, dysfunkce, problémy, šance: státní politika turismu České republiky: systémový přístup k řešení problémů.* 1. vyd. Praha: Grada, 2011. ISBN 978-80-247-3842-0.

[12] UHLÁŘ, Jan. *Technické prostředky ochrany objekt*ů. 1. vyd. Praha: Vysoká škola regionálního rozvoje Praha, 2014. ISBN 978-80-87174-33-3.

[13] WOODS, Margaret. *Risk management in organizations: an integrated case study approach.* 1st pub. London [i. e. Abingdon]: Routledge, 2011. ISBN 978-0-415-59173-7.

Internetové zdroje:

[14] ABC organizace: *Informace* [online]. [cit. 2017-04-22]. Dostupné z: https://www.abc.cz/informace

[15] Cleverandsmart: *Informační bezpečnost* [online]. [cit. 2011-04-14]. Dostupné z: http://www.cleverandsmart.cz/informacni-bezpecnost/

[16] ČANDÍK, Marek: *Informační bezpečnost – Information security* [online]. [cit. 2017-01-12]. Dostupné z: http://www.cybersecurity.cz/data/candik2.pdf

[17] Elektron: *Protipožární signalizace* [online]. [cit. 2017-03-24]. Dostupné z: http://www.elektrontrade.cz/protipozarni-signalizace/

[18] Falcocomputer: *Elektronické zabezpečovací syst*émy [online]. [cit. 2017-03-24]. Dostupné z: http://www.falcocomputer.cz/elektroinstalace/ezs-elektronicke-zabezpecovaci-systemy

[19] Guard7, lexikon: *Základní povinnosti zaměstnavatele v oblasti BOZP* [online]. [cit. 2017-02-27]. Dostupné z: http://www.guard7.cz/lexikon/zakladni-povinnosti-zamestnavatele-v-oblasti-bozp

[20] Hasiči – vzdělávání: *Elektronická požární signalizace* [online]. [cit. 2017-01-25]. Dostupné z: https://www.hasici-vzdelavani.cz/content/elektronicka-pozarni-signalizace-eps-uvod-funkce-predpisy

[21] Ipodnikatel: *Povinná školení zaměstnanců* [online]. [cit. 2011-10-27]. Dostupné z: http://www.ipodnikatel.cz/Pracovni-pravo/povinna-skoleni-zamestnancu.html

[22] MALÁN, Martin: *Návrh elektronického zabezpečovacího systému pro ostrahu obytného objektu* [online]. [cit. 2017-01-25]. Dostupné z: https://otik.uk.zcu.cz/bitstream/handle/11025/4733/Bakalarska%20prace.pdf?sequence=1

[23] Managementmania: *Bezpečnostní rizika* [online]. [cit. 2010-10-22]. Dostupné z: https://managementmania.com/cs/bezpecnostni-rizika

[24] Managementmania: *Řízení rizik* [online]. [cit. 2017-02-27]. Dostupné z: https://managementmania.com/cs/rizeni-rizik

[25] Národní bezpečnostní úřad: *Informace – fyzická bezpečnost* [online]. [cit. 2017-01] z: https://www.nbu.cz/cs/ochrana-utajovanych-informaci/fyzicka-bezpecnost-technicke-prostredky-a-dalsi-prvky-fyzicke-bezpecnosti-a-jejich-certifikace/1014-informace/

[26] Národní bezpečnostní úřad: *Ochrana utajovaných informací – personální bezpečnost* [online]. [cit. 2016-12-19]. Dostupné z: https://www.nbu.cz/cs/ochrana-utajovanych-informaci/personalni-bezpecnost/obecne-k-personalni-bezpecnosti/

[27] TZB – info: *Požární bezpečnost staveb, zařízení elektrické požární signalizace* [online]. [cit. 2016-10-10]. Dostupné z: http://www.tzb-info.cz/pozarni-bezpecnost-staveb/14779-zarizeni-elektricke-pozarni-signalizace

[28] VOKO bezpečnostní služba: Pult centrální ochrany [online]. [cit. 2016-10-10]. Dostupné z: http://www.voko-security.cz/pult-centralni-ochrany/

[29] Vlastní cesta: *Informace a bezpečnost* [online]. [cit. 2010-10-23]. Dostupné z: http://www.vlastnicesta.cz/clanky/informace-a-bezpecnost/

[30] ZAHÁLKA, Jiří: *Analýza rizik v průmyslovém podniku* [online]. [cit. 2016-12-14]. Dostupné z: https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=54380

Legislativa, směrnice:

[31] *Směrnice organizace* ABC X/2015.

[32] *Organizační řád organizace* ABC č. X/2015.

[33] *Organizační řád organizace* ABC č. X/2016.

Vyhláška č. 528/2005 - *Vyhláška o fyzické bezpečnosti a certifikaci technických prostředků.*

Zákon č. 181/2014 Sb. *Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů* (zákon o kybernetické bezpečnosti).

Zákon č. 262/2006 Sb. *Zákoník práce.*

Zákon č. 412/2005 Sb. *Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti.*

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

BOZP Bezpečnost a ochrana zdraví při práci

CCTV Closed Circuit Television

ČNR Česká národní rada

ČR Česká republika

ČSN Česká technická norma

dB Decibel

DPH Daň z přidané hodnoty

EPS Elektronická požární signalizace

EZS Elektronická zabezpečovací signalizace

FO Fyzická osoba

GSM Globální Systém pro Mobilní komunikaci

HZS Hasičský záchranný systém

IP Ingress Protection

IT Informační Technologie

IZS Integrovaný záchranný systém

MS Microsoft Office

PC Personal Computer

PCO Pult centrální ochrany

PIN Personal Identification Number

PO Právnická osoba

SAP Systems Applications Products in data processing

SPZ Státní poznávací značka

SEZNAM OBRÁZKŮ

SEZNAM TABULEK