Univerzita Pardubice
Fakulta ekonomicko-správní

Bezpečnostní audit podniku

Hana Poddaná

Bakalářská práce
2017

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: **2016/2017**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Hana Poddaná**
Osobní číslo: **E14388**
Studijní program: **B6208 Ekonomika a management**
Studijní obor: **Ekonomika a provoz podniku**
Název tématu: **Bezpečnostní audit podniku**
Zadávající katedra: **Ústav podnikové ekonomiky a managementu**

Zásady pro vypracování:

Prvým cílem práce je obecný popis problematiky bezpečnostního auditu podniku a jeho metod. Dalším cílem je popis vybraného podniku a analýza vybraných problémů jeho bezpečnostního auditu s vyvozením hlavních poznatků a doporučení.

Osnova
- Obecný popis problematiky bezpečnostního auditu podniku.
- Metody a prvky bezpečnostního auditu.
- Popis vybraného podniku a jeho bezpečnosti.
- Analýza vybraného problému bezpečnostního auditu.
- Hlavní poznatky a doporučení.

Rozsah grafických prací:

Rozsah pracovní zprávy: **cca 40 str.**

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

Seznam odborné literatury:

DVOŘÁČEK, Jiří. Audit podniku a jeho operací. Praha: C.H. Beck, 2005, 165s. C.H. Beck pro praxi. ISBN 80-717-9809-6.
KRÁLÍČEK, Vladimír a Jan MOLÍN. Vnější a vnitřní kontrola z pohledu managementu. Praha: Wolters Kluwer, 2014, 231s. C.H. Beck pro praxi. ISBN 978-80-7478-557-3.
SMEJKAL, Vladimír a Karel RAIS. Řízení rizik ve firmách a jiných organizacích. 3., rozš. a aktualiz. vyd. Praha: Grada, c2010, 483s. Expert (Grada). ISBN 978-80-247-3051-6.
STRANKS, Jeremy W. Health and safety pocket book. Boston: Butterworth-Heinemann, 2006, 441s. C.H. Beck pro praxi. ISBN 07-506-6781-8.
VEBER, Jaromír, Marie HŮLOVÁ a Alena PLÁŠKOVÁ. Management kvality, environmentu a bezpečnosti práce: legislativa, systémy, metody, praxe. Praha: Management Press, 2006, 358s. C.H. Beck pro praxi. ISBN 80-726-1146-1.

.

Vedoucí bakalářské práce: **doc. Ing. Radim Roudný, CSc.**
Ústav podnikové ekonomiky a managementu

Datum zadání bakalářské práce: **4. září 2016**

Termín odevzdání bakalářské práce: **28. dubna 2017**

doc. Ing. Romana Provazníková, Ph.D.
děkanka

L.S.

doc. Ing. Marcela Kožená, Ph.D.
vedoucí ústavu

V Pardubicích dne 4. září 2016

PROHLÁŠENÍ

Tuto práci jsem vypracovala samostatně. Veškeré literární prameny a informace, které jsem v práci využila, jsou uvedeny v seznamu použité literatury.
Byla jsem seznámena s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše. .

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 9/2012, bude práce zveřejněna v Univerzitní knihovně a prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 28. 4. 2017 Hana Poddaná

PODĚKOVÁNÍ:

Tímto bych ráda poděkovala svému vedoucímu práce doc. Ing. Radimu Roudnému. CSc. za jeho odbornou pomoc, cenné rady a poskytnuté materiály, které mi pomohly při zpracování bakalářské práce. Rovněž bych chtěla poděkovat panu Mgr. Rosinovi za vstřícnost a poskytnutí podrobných informacích o analyzované firmě. V neposlední řadě bych chtěla poděkovat celé rodině za podporu a pochopení, které mi v průběhu studia poskytovali.

ANOTACE

Obsahem bakalářské práce je obecný popis problematiky, která je zaměřena na řízení bezpečnosti a na bezpečnostní audit podniku. Druhá část bakalářské práce je zaměřena na samotnou analýzu bezpečnostního auditu ve vybraném podniku, který se zabývá poskytováním poštovních služeb.

KLÍČOVÁ SLOVA

Bezpečnost, Bezpečnostní audit, bezpečnost a ochrana zdraví při práci, riziko

TITLE

Security audit of company

ANNOTATION

The content of this bachelor thesis is to describe the problematics of security management and security audit. The second part of the thesis deals with security audit analysis of a chosen company that is focused on provision of postal services.

KEYWORDS

Security, security audit, Health and safety at work, risk

OBSAH

SEZNAM TABULEK

SEZNAM OBRÁZKŮ

SEZNAM ZKRATEK

BOZP	bezpečnost a ochrana zdraví při práci
ČSN	česká technická norma
ČR	Česká republika
EU	Evropská unie
ISO	Mezinárodní organizace pro normalizaci
OHSAS	ochrana zdraví při práci a management bezpečnosti
PO	požární ochrana
s.p.	státní podnik

ÚVOD

Bezpečnost je pro každý podnik velmi důležitý pojem, protože nejen že musí dbát na bezpečnost celého podniku, ale hlavní prioritou je bezpečnost zaměstnanců. Samotná bezpečnost zaměstnanců je upravena v zákoně, kterým by se měl každý zaměstnavatel i podnikatel řídit. Bohužel v řadě případů dochází k častým situacím nedodržování zákona a dochází tak k mnoha rizikům.

Hlavním důvodem výběru tohoto tématu bylo, že autorka práce chce v budoucnosti podnikat a mít vlastní podnik. Součástí podnikání jsou rizika, proti kterým by měl být každý podnikatel zabezpečen. Hlavní prioritou zajištění je bezpečnost zaměstnanců a celého podniku. Proto zpracování práce na téma bezpečnostní audit podniku bude pro autorku přínosem a jistým poučením z chyb jiných podniků.

Samotný bezpečnostní audit se zabývá dvěma základními skupinami, a to především bezpečnostní osob a druhou skupinou a tou je bezpečnost majetku. Hlavním cílem bezpečnostního auditu je porovnat, zdali je bezpečnost v podniku správná a jestli se neodlišuje od reality. Také se bezpečnostní audit zaměřuje na správnost dokumentů, jestli jsou ve skutečnosti vedeny správně podle norem.

První část této bakalářské práce se věnuje teoretickému popisu problematiky bezpečnostního auditu a pojmům týkající se této problematiky. Jsou podrobně rozebrány všechny druhy bezpečnostních rizik a následně popis jednotlivých kroků při řízení rizik, kde jsou rizika nejprve identifikována, poté analyzována a v neposlední řadě zhodnocena. Další kapitola v první části této práce se věnuje rizikům při podnikání, které jsou podrobně rozděleny na vnitřní a vnější rizika, která se mohou vyskytovat při podnikání. Všechny obecné informace v první části jsou čerpány z literárních a internetových zdrojů.

Druhá část práce je zaměřena na praktické provádění auditu ve vybrané společnost. Pro tuto práce byl vybrán státní podnik Česká pošta, která je hlavním poskytovatelem poštovních služeb. Práce se věnuje provádění analýzy v oblasti BOZP, kde je vytvořena na základě disponibilních údajů regresní analýza týkající se pracovních úrazů. Další část práce se věnuje bezpečnostnímu auditu, který je prováděn v oblasti výskytu mimořádných událostí. Informace získané pro analýzu ve státním podniku jsou z výročních zpráv a interních zdrojů podniku.

Prvým cílem práce je obecný popis problematiky bezpečnostního auditu podniku a jeho metod. Dalším cílem je popis podniku, který je zaměřen na poskytování poštovních služeb a realizaci jeho bezpečnostního auditu ve vybraných problémech. Na základě provedené analýzy zhodnotit výsledky bezpečnostního auditu a navrhnout případné doporučení.

1 ŘÍZENÍ BEZPEČNOSTI V PODNIKU

Oblast řízení bezpečnosti v podniku úzce souvisí s řízením rizik, které je zaměřeno na vytvoření nebo trvalé zajištění podmínek. Tyto podmínky pomohou předcházet či snížit identifikovatelná rizika. Pomocí nejrůznějších metod, směrnic, standardů a nástrojů se daný podnik může vyhnout problémům, které by mohly nastat. [26]

Management bezpečnosti se také často nazývá krizový management, který se zaměřuje na problematiku systémů. Snaží se o snížení nežádoucích událostí na přijatelnou míru, ale také řízením, respektive managementem těchto systémů. Každý podnik by chtěl zcela odstranit všechny nežádoucí události ve svém podniku, ale je to nereálné z důvodů charakteru přírodních a technických jevů. Dalším důvodem nereálného odstranění nežádoucích událostí je chování lidí, kteří neúmyslně i úmyslně nežádoucí události způsobují.

Řízení bezpečnosti je soustavná, opakující se sada navzájem provázaných činností, jejichž cílem je zajistit bezpečný provoz a zamezit bezpečnostním rizikům a hrozbám. Tato oblast řízení se z velké části týká zajištění autorizovaného přístupu osob k aktivům organizace zejména financím, informacím, movitému a nemovitému majetku. [25]

1.1 Bezpečnostní strategie (security strategy)

Bezpečnostní strategie má za hlavní cíl nastavit střednědobé a dlouhodobé opatření ke zvýšení bezpečnosti v podniku. Pro podniky je to jedna z dílčích strategií, která doplňuje provozní dokumenty správy majetku, pohybu lidí a pohybu informací. Bezpečnostní strategie nejvíce řeší bezpečnost svých aktiv, a to jak bezpečnost fyzickou (bezpečnost vstupu do budov a areálu), tak bezpečnost informační. [4]

Pro firmu je velmi důležité mít bezpečnostní strategii zpracovanou hlavně pro svá aktiva, jelikož jejich ztráta by mohla napáchat velké potíže nebo dokonce zhroucení firmy. Bezpečnostní strategie se nejčastěji týká:

- bezpečnosti majetku (bezpečnost vstupu do budov, objektů, areálů a jejich ostraze)
- bezpečnosti finančních prostředků (finanční prostředky v bance, hotovosti a cennosti)
- bezpečnost lidí na pracovišti a ochrany zdraví při práci, požární ochrany
- informační bezpečnosti (bezpečnost citlivých informací)
- bezpečnosti ICT (počítačová bezpečnost)

- ochrany proti podvodů a zneužitím

1.2 Okruhy řízení bezpečnosti v podniku

Tato kapitola se zabývá hlavními okruhy řízení bezpečnosti v podniku. Mezi tyto klíčové okruhy patří fyzická bezpečnost, informační bezpečnost, ICT bezpečnost, bezpečnost práce a ochrana zdraví při práci a požární ochrana.

1.2.1 Fyzická bezpečnost

Fyzická bezpečnost je především zaměřena na bezpečnost majetku (například: hotovosti nebo cennosti), bezpečnost budov a ostraha. Dále je orientována na osobní bezpečnost včetně řízení lidských zdrojů. [26]

1.2.2 Informační bezpečnost

Informační bezpečnost se zabývá ochranou informací v podniku. Cílem této oblasti je zajistit dostatečnou ochranu všech údajům a informacím organizace ve všech možných formách. Jedná se tedy jak o automatizovaný informační systém, tak i o neautomatizované písemné dokumenty, rukou psané poznámky, telefonické hovory, obchodní jednání, jednání představenstva a dozorčí rady, poštovní zásilky apod. Informační bezpečnost má také zajišťovat ochranu nosičů dat a informací jako jsou například listiny, audio a video pásky, fotografie, filmy, paměti počítačů atd. Dále pod informační bezpečnost spadá ochrana informací, které přijdou zvnějšku, což jsou například přenosy poštovní, kurýrní, osobní, telefonické nebo faxové. Rizika úniku či zneužití informací hrozí nejen z vnějšího prostředí firmy, ale také z vnitřního prostředí. [28]

1.2.3 Počítačová bezpečnost

Tento typ bezpečnosti je jednou ze součástí informační bezpečnosti, jenom s tím rozdílem, že počítačová bezpečnost se zaměřuje jen na informační a komunikační technologie v podniku. Hlavním cílem této bezpečnosti je předcházet počítačovým útokům a zajistit tak bezpečný provoz.

Mezi okruhy, kterými se počítačová bezpečnost zabývá patří [19]:

- síťová bezpečnost
- internetová bezpečnost
- bezpečnost koncových zařízení

- kryptografie (e-podpis, e-archivace)
- speciální prostředky (odposlech, sledování)

1.2.4 Bezpečnost a ochrana zdraví při práci

Podle zákoníku práce se bezpečnost práce a ochrana zdraví při práci vztahuje na všechny osoby, které se zdržují na pracovišti zaměstnavatele. Zákon stanovuje odpovědnost zaměstnavatele zajistit svým zaměstnancům bezpečné a zdravé pracovní prostředí. [31]

Veškeré povinnosti vůči zaměstnancům a jiným osobám v souladu se zákony o bezpečnosti a ochraně zdraví při práci mohou být absolutní nebo přísné. Pokud nejsou splněny požadavky týkající se ochrany zdraví a bezpečnosti může dojít k zákonné povinnost, která může být přísně absolutní. Příkladem této povinností je, že každý zaměstnavatel zajistí, aby bylo pracovní zařízení konstruováno nebo přizpůsobeno tak, aby bylo vhodné pro daný účel, pro který má být používán nebo poskytnut. [29]

Školení BOZP

Školení bezpečnosti práce a ochrany zdraví při práci upravuje zákoník práce § 37 odst. 5. Každý zaměstnanec, který nastupuje do nové práce musí být seznámen s pracovním řádem a s právními a ostatními předpisy k zajištění BOZP, které zaměstnanec musí při své činnosti dodržovat. Dále je povinností zaměstnavatele seznámit nového zaměstnance s kolektivní smlouvou a s vnitřními předpisy. Podle § 103 je zaměstnavatel povinen zajistit školení o právních a ostatních předpisech k zajištění BOZP, které doplňují požadavky na výkon práce. Zaměstnavatel rozhoduje o osobě, která bude provádět školení.

Osobní ochranné pracovní prostředky

Každá společnost má za hlavní cíl odstranit všechny bezpečnostní rizika, která se vyskytují na pracovišti. Ze zákoníku práce vyplývá, že je zaměstnavatel povinen poskytnout svým zaměstnancům bezplatně ochranné pracovní prostředky. [30]

Osobní ochranné pracovní pomůcky jsou to prostředky, které jsou určené pro zaměstnance podniku. Hlavním úkolem těchto pomůcek je chránit zaměstnance před riziky, která by mohla ohrozit jejich život a bezpečnost. [17]

Pracovní úrazy a nemoci z povolání

Podnik si klade velký důraz na prevenci, ale v řadě případů dochází ke vzniku pracovních úrazů. Z tohoto důvodu zákoník práce uvádí řadu povinností pro zaměstnavatele, které by měl každý podnikatel dodržovat. Mezi tyto povinnosti patří [30]:

- objasnit příčiny a okolnosti vzniku úrazu za účasti zaměstnance, pokud to zdravotní stav zaměstnance dovoluje
- vést v knize úrazů evidenci o všech úrazech, i když jimi nebyla způsobena pracovní neschopnost či byla způsobena pracovní neschopnost nepřesahující tři kalendářní dny
- vyhotovit záznam o pracovním úrazu, který vyvolá pracovní neschopnost delší než tři pracovní dny, a zaslat jej příslušným orgánům
- přijmout opatření proti opakování pracovních úrazů
- vést evidenci zaměstnanců, u nichž byla známa nemoc z povolání, která vnikla na jeho pracovištích

1.2.5 Požární bezpečnost

Požár je havarijní situace, při které dochází k ničení majetku, ale také ve většině případů dochází k závažným ekologickým důsledkům (nebezpečné zplodiny hoření, rozpuštění různých látek při hašení). Dalším rizikem při požáru může být pracovní úraz či jiné poškození zdraví osob, kteří jsou přítomni při požáru, při hašení apod. [30]

Každá právnická či podnikající fyzická osoba mají za povinnost bez ohledu na to, zda se jedná o poskytování služeb nebo o výrobní činnosti, zajistit nebo provést provedení začlenění činností požární ochrany do kategorií podle míry požárního nebezpečí.

Kategorie podle míry požárního nebezpečí se dělí:

- bez zvýšeného požárního nebezpečí
- se zvýšeným požárním nebezpečím
- s vysokým požárním nebezpečím

Tyto činnosti může provádět v dané organizaci buďto technik požární ochrany, který má ve své kompetenci jen činnosti, které spadaní do kategorie bez zvýšeného požárního nebezpečí nebo se zvýšeným požárním nebezpečím. Druhou osobou, která může začleňovat všechny činnosti bez ohledu na míru nebezpečí je odborně způsobilá osoba v požární ochraně.

Dokumentaci týkající se požární ochrany si podnikatel stanoví sám v Organizační směrnici k požární ochraně. Výjimkou jsou podnikatelé, jejichž činnosti v podniku jsou zařazeny do kategorie zvýšeného nebo vysokého požárního nebezpečí, v tomto případě se musí plnit další

stanované úkoly v PO, které je podnikatel povinen zpracovat v dokumentaci požární ochrany (například požární poplachové směrnice, požární řád atd.) [21]

Tabulka 1: Desatero požární bezpečnosti

1.	**únikové cesty a nouzové východy –** náležitě označené bezpečnostním značením, vždy volně průchodné v potřebné šířce
2.	**hasící přístroje a požárně bezpečnostní zařízení** – vhodně umístěné z důvodu snadného a rychlého použití, vždy provozuschopné a volně přístupně
3.	**technické podmínky a návody** ve vztahu k požární bezpečnosti výrobků, činností a technologických provozů – dodržovat instrukce a doporučení
4.	**bezpečnostní značky, příkazy, zákazy a pokyny** vztahující se k požární ochraně – důsledně označovat pracoviště a potřebná místa
5.	**preventivní požární prohlídka** – pravidelně a ve stanovených lhůtách provádět vlastními zaměstnanci, kteří mají potřebnou způsobilost, nebo zabezpečit smluvně externími speciality
6.	**závady zjištěné při kontrolách** orgánu státního požárního dozoru nebo při preventivních požárních prohlídkách – neprodleně odstraňovat a v případě potřeby provést náhradní opatření
7.	**počínat si obezřetně** – tak aby nedocházelo ke vzniku požáru při používání tepelných, elektrických, plynových a jiných a spotřebičů, požárně nebezpečných látek či otevřeného ohně
8.	**spolupracovat** se specialisty v oboru požární ochrany ve všech oblastech podnikání
9.	**řídit se instrukcemi**, které jsou stanoveny v dokumentaci požární ochrany
10.	**odpovědnost vedoucích pracovníků** – věnovat potřebnou pozornost při schvalování dokumentace požární ochrany, zda jsou navrhovaná opatření reálná, za požární ochranu před zákonem zodpovídá statutární orgán či podnikatel nebo jejich určení zástupci

Zdroj: [22]

1.3 Manažer bezpečnosti

Manažer, který je zodpovědný za fyzickou, informační a personální bezpečnost v organizaci se nazývá manažer bezpečnost neboli CSO (Chief Security Officer). Označení CSO je přijato z americké angličtiny, toto označení manažera se používá ve většině zemí světa. V praxi se můžeme také setkat s označení stejné pozice jako security manažer.

Úkolem manažera bezpečnosti je plně odpovídat za řízení bezpečnosti provozu a následně také průběžně zlepšovat a slaďovat cíle bezpečnosti s cíli dané organizace. Další činnosti této pozice mít odpovědnost za plánování rozvoje bezpečnosti, sledování nových trendů v oblasti bezpečnosti nebo provádět analýzy bezpečnosti, stanovení strategie a politiky bezpečnosti v daném podniku. [6]

Většinou ve větších podnicích jsou k dispozice ještě specialisté na konkrétní druh bezpečnosti podniku. Mezi druhy těchto profesí patří [5]:

- **Manažer informační bezpečnosti (CISO)** - tato profese je zaměřena na informační bezpečnost podniku. Pod zkratkou CISO (Chief Information Security Officer) je velmi známa ve velkých podnicích v několika zemích světa. Hlavním

úkolem manažera je odpovídat za řízení informační bezpečnosti a následně se snažit o zlepšování cílů bezpečnosti.

- **Manažer fyzické bezpečnosti (CSFO)** - pod pojem manažer fyzické bezpečnosti je možné si představit osobu, která je v daném podniku odpovědná za fyzickou bezpečnost. Jeho hlavní úkolem je zabezpečit majetek podniku a také osoby, které pracují v dané firmě.

2 ŘÍZENÍ RIZIK

Řízení rizik neboli risk management je problematika velice široká a podle svého zaměření často odlišná. Existuje mnoho oblastí, které spadají do této problematiky. V tabulce 2 jsou vypsány všechny oblasti, v nichž hovoříme o řízení rizik v podniku. [28]

Tabulka 2: Oblasti řízení rizik

Oblasti řízení rizik
přírodní katastrofy a havárie
rizika ochrany životního prostředí
finanční rizika (investiční riziko, nesolventnost zákazníka atd.)
projektová rizika
obchodní rizika (marketingové riziko, strategické riziko, riziko managementu atd.)
technologická rizika
technická rizika
politická rizika
bezpečnostní rizika (personální bezpečnost, fyzická bezpečnost, informační bezpečnost)

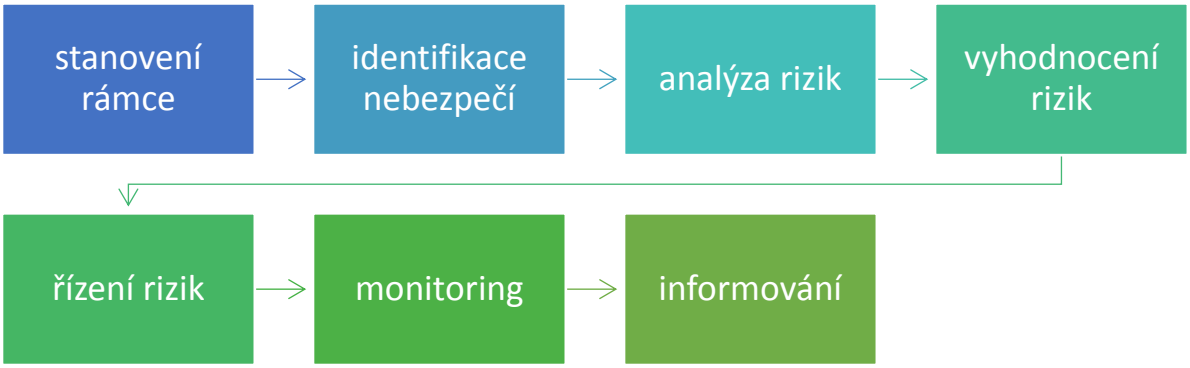
Zdroj:[28]

Řízení rizik je proces, ve kterém se osoba zodpovědná za řízení rizik v podniku snaží zamezit působení už existujících nebo budoucích faktorů a navrhuje případná řešení, která pomáhají odstraňovat účinek nežádoucích vlivů a na druhou stranu umožňují, využít možnosti působení pozitivních vlivů.

Při procesu řízení rizik je nejkritičtější výběr optimálního řešení. Celý tento proces začíná při určení úrovně rizika, dále musí dojí k určitému hodnocení ekonomických nákladů různých řešení. Dalším krokem je zhodnocení dopadů a přínosů a analýza možných důsledků z přijatého rozhodnutí na jednotlivce a jeho okolí. Posledním krokem řízení rizika je rozhodnutí. Ve většině případů je výstupem více variant řešení daného rizika. [28]

2.1 Průběh procesu řízení rizik

V každém podniku by měl určitým způsobem probíhat proces řízení rizik, který se dělí do základních prvků. Na obrázku 1 jsou vyobrazuje jednotlivé kroky procesu řízení rizik. [18]



Obrázek 1: Proces řízení rizik

Zdroj: vlastní zpracování podle [18]

Stanovení rámce, rozsahu

V prvním kroku se jedná o stanovení strategického a organizační rozsahu. Nejdříve se musí vymezit daný objekt nebo systém, u kterého se daná rizika budou posuzovat. V tomto případě se může jednat například o stroj, zařízení, pracoviště nebo činnost, kde se definují kritéria, ke kterých se vztahuje dané riziko. Při posuzování rizik spojených s pracovní činností je důležité uvažovat nejen o běžném pracovním procesu ale také o mimořádné situaci a činnosti. [18]

Identifikace zdrojů nebezpečí

V tomto případě se jedná o identifikování zdrojů případného ohrožení zdraví, majetku nebo životního prostředí. Hlavním zdrojem informací je evidence událostí, které nastaly v minulých letech. Každý podnik by měl zaznamenávat u daného problému zdroje, které se na vzniku události a příslušných následcích podílely. Ale ne každá společnost si tyto záznamy vytváří a proto, když tyto informace nejsou k dispozici je třeba využít některou z metod, které slouží k identifikaci zdrojů nebezpečí.

Mezi základní metody pro identifikaci nebezpečí patří [18]:

- kontrolní seznam (checklist)
- metoda „What-if“ (co se stane, když …) zkoumá pomocí brainstormingu případné neočekávané události, dále definuje místa systému a identifikuje prvky pro metody FMEA a FTA
- metoda FTA (Fault Tree Analysis neboli analýza stromu poruch) vychází z finální poruchy a hledá primární příčiny, které se nacházejí v normě ČSN EN 61025. Jedná se o metodu kvantitativní a kvalitativní analýzy nejčastěji používanou v průmyslovém odvětví.
- Metoda ETA (Event Tree Analysis neboli analýza stromu událostí) jedná se o kvantitativní a kvalitativní analýzy. Tato metoda začíná s nalezeným případem a hledá sledy událostí.

Použití těchto metod v praxi závisí na mnoha faktorech. Každý metoda má své specifické vlastnosti a každý podnik si vybírá podle praktických zkušeností s jejím používáním nebo podle výsledků, kterých chce dostáhnout použitím určité metody. Ve většině případů se metody ještě podkládají různými vnitropodnikovými dokumenty daného podniku. Mezi tyto dokumenty řadíme například pracovní postupy, požární řád, přehled úrazů a nehod nebo údaje o počtu osob v podniku a v okolí.

Analýza rizik

Po identifikaci nebezpečí přichází na řadu analýza rizik, která je chápaná jako proces definování hrozeb, pravděpodobnosti jejich uskutečnění a dopadu na aktiva. Analýza rizik je velmi důležitá a užitečná pro identifikaci rizik a vhodných přístupů k jejich snížení. Také slouží k poskytnutí objektivních informací pro rozhodování. Výsledky z analýzy jsou velmi důležité pro rozhodování o tom, zda je riziko možné přijmout nebo zda jej musíme snížit.

Riziko je chápáno jako nebezpečí vzniku určité ztráty v podniku. Lze jej vyjádřit kvantitativní nebo semi-kvantitativním způsobem nebo kvalitativně. Pro další rozhodování a řízení rizik je lepší využívat buď kvantitativní nebo semi-kvantitativní způsob. a to z důvodů lepšího vyjádření míry rizika.

Prvky pro ohrožení rizika jsou shodné pro všechny zdroje nebezpečí. Jedná se především o frekvence nebo pravděpodobnost, se kterou se ohrožení příslušným zdrojem nebezpečí vyskytuje (např. nepřetržitě, 1x za hodinu, den, měsíc atd.). Dalším typem míry poškození mohou být zdravotní následky (např. smrtelný úraz, úraz s trvalými následky apod.). [18]

Metody analýzy rizik se dělí na:

- **kvantitativní analýza** – hlavním cílem této metody je matematický výpočet rizika z frekvence výskytu hrozby a jejího dopadu. Nejčastěji se dopad vyjadřuje ve finančních termínech (např. tisíce Kč, statisíce Kč …). Kvantitativní metody se považují za přesnější, než jsou kvalitativní. Za nevýhodu této metody se považuje náročnost na provedení a zpracování výsledků, které jsou často vyjadřovány podle formalizovaného postupu.
- **semi-kvantitativní analýza** – u této metody jsou pro vyjádření míry následků a pravděpodobností použity kvalitativní škály. Hlavní cílem je dosáhnout podrobnější analýzy rizik a možností jejich vzájemné porovnání. Tato metoda se v praxi velmi málo využívá, protože na rozdíl od kvantitativní analýzy nevyjadřuje skutečnou míru rizika.
- **kvalitativní analýza** – priorita této metody je postavena na popisu závažnosti potenciálního dopadu a na pravděpodobnosti, že daná událost nastane. Rizika jsou zde vyjadřovány pomocí rozsahu (například jsou obodována <1 až 10> nebo určena pravděpodobností <0;1> nebo slovně <malé, střední, velké>). Tato metoda je mnohem jednodušší a rychlejší, než je kvantitativní analýza.

Vyhodnocení rizik

Po analýze rizika přichází jejich vyhodnocení. Výsledky analýzy jsou vyjádření velikosti rizika a jejich upřesnění, které umožní se dále zaměřit na rizika nejzávažnější. Z důvodu toho, že riziko je ve své podstatě dvourozměrná veličina, je nejčastěji používána jako systém dvou souřadnic x a y. Písmeno x je na ose vyznačováno jako závažnost a písmeno y je na ose vyznačováno jako pravděpodobnost. Když známe údaj o riziku, zaneseme jej do systému a měli bychom získat průsečík hodnoty rozložení rizika v oblasti, kterou jsme na začátku analyzovali. Na základě tohoto kroku se daný podnik může rozhodnout o přijetí bezpečnostního opatření. [18]

Řízení rizik

Hlavní cílem tohoto kroku je snižovaní rizik na přijatelnou úroveň. Pokud je riziko již identifikováno, podnik chce co nejrychleji dané riziko odstranit. Pokud není možné zcela odstranit zdroj nebezpečí je další možností ochrana, anebo minimalizace jeho vzniku tak, že se příslušné bezpečnostní ochranná opatření přímo nainstalují do projektu. Projekt pro bezpečnost musí být vždy vybaven pro snižování škod v případech, že bezpečnostní opatření

a systémy selžou. Minimalizování škod může mít podobu varovné a výstražné signalizace, výcviku, pokynů a procedur pro chování v nebezpečných situacích. [18]

Monitoring

Tato složka řízení rizik poskytuje managementu každodenní přehled o jejím stavu a přijímání případných opravných opatření. Monitoring slouží pro ubezpečení, že ostatní prvky v podniku dobře fungují. Ve většině případů interní auditoři ověřují všechny prvky a systémy v podniku, jestli jsou v pořádku a fungují, jak by měli fungovat.

Monitorování má za úkol dokumentovat způsob a četnost prováděného posuzování a hodnocení rizik, výsledky auditu a dalších nástrojů monitoringu a také z dokumentovává přijatá opatření ke snížení rizik. [28]

Informování

Posledním krokem průběhu řízení rizik je informování, které je stejně tak důležité jako ostatní kroky. I když se podnik snaží odstranit všechny rizika, která se v podniku objeví, vždy některá zůstávají. Proto je každý zaměstnavatel povinen informovat o těchto rizicích své zaměstnance a všechny osoby, které by dané riziko ohrožovalo. [18]

2.2 Standardy a systémy v oblasti řízení rizik a bezpečnosti

ISO 31000

Tento standard je vydáván jako všechny mezinárodní standardy Mezinárodní organizací pro standardizaci. ISO 31000 je označení standardu pro Management rizik, který obsahuje principy a směrnice. Tuto normu může používat jakákoliv organizace bez ohledu na její velikost či zaměření. [11]

Hlavním úkolem tohoto standardu je pomáhat organizacím zvýšit pravděpodobnost dosažení cílů, zlepšit identifikaci příležitostí a hrozeb a následně efektivně alokovat a využívat zdroje pro řešení rizika. ISO 31000 není určena pro účely certifikace. [10]

ISO 27000

ISO 27000 je skupina standardů, která je zaměřena na řízení informační bezpečnosti v organizacích. Jednotlivé druhy standardů jsou cíleny na různá hlediska informační bezpečnosti v podniku. Mezi základní normy této řady patří [28]:

- ČSN ISO/IEC 27001:2005 – požadavky na systémy managementu bezpečnosti informací

- ISO/IEC 27002:2005 – popisuje sadu bezpečnostních opatření (praktik), které musí organizace provést při implementaci ISMS
- ČSN ISO/IEC 27003:2010 – poskytuje návod k implementaci ISMS podle ISO 27001
- ČSN ISO/IEC 27004:2009 – poskytuje návod, jak uplatňovat metody měření, vhodné ukazatele
- ČSN ISO/IEC 27005:2008 – popisuje principy a požadavky managementu rizik v ISMS

OHSAS 18001

Norma OHSAS 18001 byla vydána Britským normalizačním institutem. Tato norma by měla sloužit jako nástroj, který upřesňuje požadavky na manažerský systém bezpečnosti a ochrany zdraví při práci. Je velmi používanou normou v evropských firmách, které tuto normu využívají jako předlohu požadavků pro zavádění manažerských systémů BOZP. Pokud daná firma chce získat certifikaci OHSAS 18001, musí si vybrat, zda chce získat normu samostatně nebo v spojením s QMS a EMS. [30]

Program „Bezpečný podnik“

V roce 1996 byl ministrem práce a sociálních věcí vyhlášen program „Bezpečný podnik“. Hlavní cílem je zvýšit úroveň bezpečnosti práce v podnicích. Dalšími cíli je zavést efektivní systém podnikového řízení bezpečnosti (ochrany zdraví, životního prostředí a majetku) a podporovat podniky, aby splňovali požadavky směrnic EU a českého práva.

V České republice je už 81 společností, které jsou držiteli osvědčení „Bezpečný podnik“. Státní úřad inspekce práce vydal již 243 osvědčení. V roce 2016 bylo osvědčeno 15 firem, které splňovaly požadavky tohoto programu. Mezi tyto podniky patří například [24]:

- Drůbežářský závod Klatovy a.s. (zpracovatel kuřecího masa)
- Dřevozpracující družstvo (výrobce řeziva a deskových materiálů na bázi dřeva)
- Steel Center Europe, s.r.o. (servisní středisko na zpracování oceli)
- Elektrárna Dětmarovice, a.s. (zajišťuje dodávky elektrické energie a tepla)
- ČEZ, a.s. (výrobce elektřiny, dodavatel plynu a tepla)
- Hyundai Motor Manufacturing Czech s.r.o. (výrobní automobilový závod)

Self audit handbook for SMEs

Tato příručka se do českého jazyka překládá jako Samoprověřovací příručka pro malé a střední podniky. Byla vypracovaná na základě zkušeností a potřeb malých a středních podniků v Evropské unii. Tento dokument byl navržen Evropskou komisí k tomu, aby umožnila určit a posoudit nedostatky a úrazová rizika. Hlavní cílem je pomoci při zlepšování systému bezpečnosti, kvality výroby a pracovních výkonů. Nejčastěji tuto příručku využívají malé a střední podniky, ve velkých podnicích se běžně provádějí samotné audity. [16]

3 RIZIKA PODNIKÁNÍ

Každý podnik se soustředí nejen na svou ziskovost, ale také na případná rizika, která mohou v podniku nastat. Podnik mohou postihnout dva typy rizik, buď se jedná o vnitřní riziko nebo o vnější. Obě skupiny rizik se prolínají a vzájemně na sobě závisí například jakost výrobků musíme řešit v návaznosti na zákazníky a konkurenci, takže v souhrnu vytvářejí podniková rizika. Jak už bylo výše zmíněno rizika podniku se dělí na [25]:

- Vnitřní rizika – týkají se interních podnikových procesů a můžeme je ovlivnit, např. personální rizika, rizika vývoje a výzkumu, informační rizika a výroba a jakost
- Vnější rizika – jsou spojena z vnějšími faktory, které se nevyvíjejí příznivě a nedají se ovlivnit např. vstupy, zákazníci, konkurence, banky, finanční rizika …

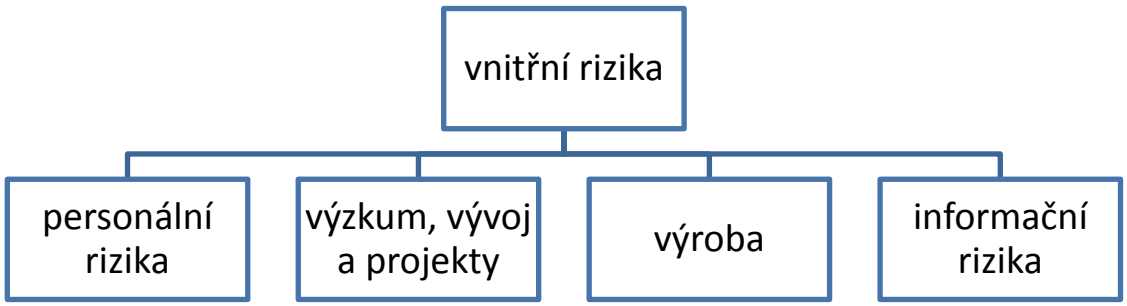
Všechna tato rizika má na starosti management bezpečnosti neboli krizový management, který vytváří bezpečnostní opatření nebo systémy, které snižují nebo zcela odstraní riziko. Při management bezpečnosti se řeší:

- Prevence rizik
- Řešení příznaků
- Řešení krize podniku
- Bankrot a konkurz
- Případná regenerace

3.1 Vnitřní rizika podnikání

Vnitřní rizika jsou charakterizována tím, že se odehrávají uvnitř firmy. Tyto rizika jsou zapříčiněna mimořádnými událostmi, které ohrožují podnik, aniž by to podnik plánoval. Také nežádoucími událostmi a výsledky podnikatelských aktivit, které podnik může naplánovat. Všechny oblasti rizik spolu souvisí. Mimořádná událost může vyvolat problémy aktivit, a naopak krize aktivit může vyvolat větší riziko mimořádných událostí. [25]

Vnitřní rizika se dále dělí na rizika, která jsou specifikovány pro danou oblast v podniku. Rozdělení těchto rizik je zobrazeno na obrázku 2.



Obrázek 2: Hierarchické uspořádání vnitřních rizik

Zdroj: vlastní zpracování podle [25]

3.1.1 Personální rizika

V podniku jsou personální rizika považována za nejsložitější, co podnik řeší. Tyto rizika mohou způsobit samotní vlastníci podniku, vrcholový manažeři nebo ostatní pracovníci. Vlastníci podniku většinou vytváří riziko, tím že rozhodují o celém chodu podniku, protože podnikaní se považuje za nejrizikovější oblast. Manažeři většinou způsobují rizika chybným stylem řízení. Personální rizika se ve většině případů zjišťují pomocí kontroly, která je průběžným nástrojem odstraňování personálních rizik. Kontrolu v podniku zajišťují liniový vedoucí, vnitřní audit nebo reakce zákazníků. [25]

3.1.2 Výzkum, vývoj a projekty

V této oblasti se řeší výrobek, technologie výroby, logistika a předpokládané zákazníky. Ve všech zmíněných oblastech platí pravidlo, čím je vyšší stupeň inovace, tím je větší riziko. V tomto bodě vzniká problém, pokud podnik nepostoupí investiční riziko, hrozí mu vytlačení z trhu a následné likvidaci podniku. Za nejvyšší stupeň výrobkové inovace se nejčastěji považuje splnění požadavků zákazníka.

3.1.3 Výroba

Ve většině případů výrobní rizika vznikají narušením systému produkce od vstupů, jednotlivé operace přes subsystémy, což jsou například střediska až k finálnímu výrobku. K narušení spolehlivosti produkce může být způsobeno systémem organizace výroby nebo spolehlivostí technologií, která se při výrobě produktů využívá. Závady a chyby technologií

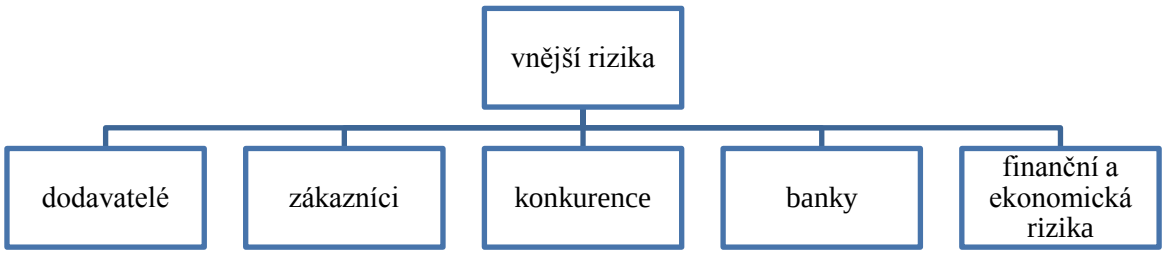
se dají řešit buďto odstraněním všech závad nebo nahrazením výpadku vícesměnným provozem, aby se dohnala časová ztráty, která vznikla při porušení stroje. [25]

3.1.4 Informační rizika

Informace přenášené komunikací mezi lidmi či na papírech nebo informace na počítačích jsou pro daný podnik určitým rizikem. V současné době se většina informací přenáší pomocí počítačových sítí. Z tohoto důvodů řešíme rizika poruchy hardwaru či programu a také rizika dat (nositelé informací). [25]

3.2 Vnější rizika podnikání

Vnější rizika jsou spjata s vnějším prostředím firmy a externími faktory, které na podnik působí. Každý podnik si musí kontrolovat svoje vnější faktory, které ovlivňují celý podnik. Mezi vnější rizika patří dodavatelé, zákazníci, konkurence, banky a finanční a ekonomická rizika, všechna tato rizika jsou v hierarchickém rozčlením zobrazeny na obrázku 3.



Obrázek 3: Hierarchické uspořádání vnějších rizik

Zdroj: vlastní zpracování podle [25]

3.2.1 Dodavatelé (vstupy)

Podle obchodního zákoníku máme právo kontrolovat své dodavatelé už v jeho samotné výrobě. Pro nás je velmi důležité si shromažďovat informace o finanční situaci dodavatele a také o časové spolehlivosti dodávek. Mezi dodávky patří i předání některých úloh externím dodavatelům tzv. outsourcing. Předání může mít několik podob a může představovat značné riziko. Za riziko outsourcingu se považuje ekonomické riziko, kde dodávka může být dražší než vlastní realizace. Další riziko, které muže nastat při outsourcingu jsou bezpečnostní rizika například se jedná o úniky informací nebo krádeže. [25]

3.2.1 Zákazníci

Každý podnik klade velký důraz na spokojenost svých zákazníků, poněvadž jsou velmi důležití pro úspěšnost podniku. Bohužel i zákazníci pro podnik přinášejí určitý druh rizika, proto se musí sledovat. Zákazníci lze sledovat a analyzovat podle:

- objektivních informacích např. počet obyvatel, platová úroveň v dané oblasti
- prodejů z minulosti
- zákaznických průzkumů
- subjektivního hodnocení

3.2.2 Konkurence

Každý podnik při svém podnikání musí nevyhnutelné sledovat a následně vyhodnocovat konkurenčního prostředí, ve kterém se nachází. Pokud by podnik nesledoval a nevyhodnocoval tato rizika konkurence mohlo by dojít k vytlačení daného podniku z trhu a následná likvidace podniku. [25]

3.2.1 Banky

Podnik si při výběru banky dává velký pozor na to, aby banka měla jako prioritu spokojenost zákazníka než vyšší zisk. Proto je výběr banky velmi důležitý bezpečnostním prvkem.

3.2.1 Finanční a ekonomická rizika

Tento druh podnikatelských rizik je spojen s hospodařením a řízením ekonomiky v podniku, s různými chybami v jiných oblastech podniku i s externími činiteli podniku. Vnitřní rizika podniku mohou být spojena s nevhodným finančním řízením včetně důsledků (např. ztráta, zadluženost, problémy s likviditou). Vně podniku se pak jedná o podmínky podnikání – politické, legislativní, obchodní, tržní a ekonomické. Finanční rizika způsobují příčiny vnitřní i vnější, některé uvedeme [25]:

- cenová politika konkurence
- nespolehliví dodavatelé
- nespolehliví zákazníci (např. neplatiči)
- daňová politika

4 BEZPEČNOSTNÍ AUDIT

Bezpečnostní audit zkoumá a identifikuje skutečný aktuální stav procesů a opatření v určených oblastech bezpečnosti: organizační, administrativní, personální, fyzické, počítačové, komunikační a porovnává ho s požadovanými kritérii auditu.

Hlavní cílem tohoto auditu je porovnání a posouzení výsledků shody s aktuálním stavem procesů a opatření bezpečnosti informací. Dále má na starosti zjištění stavu zabezpečení majetku a dalších zájmových objektů jako jsou například informace, data nebo osoby. V každém podniku také dochází ke kontrole funkčnosti a účelnosti stávajících bezpečnostních prvků. Při průběhu bezpečnostního audit se také hledí na funkčnost a aktuálnost příslušných směrnic. Po nalezení nedostatků je důležité navrhnout doporučení a upozornit na možná rizika. [1]

Po odborné kontrole bezpečnostního audit v podniku dostaneme objektivní obraz o stávajícím stavu zabezpečení včetně porovnání krytí rizik stávajícími pojistnými podmínkami. Takže podnik bude vědět, kde bude nejvhodnější investovat a kde naopak na bezpečnosti ušetřit několik korun. Další výhodou po vykonání bezpečnostního auditu je, že daný podnik bude informován o bezpečnostních rizicích a dostane profesionální návrh řešení. [2]

4.1 Druhy auditu

Tato kapitola popisuje jednotlivé druhy auditu. V podniku může být provádět externí nebo interní audit nebo se může audit dělit z hlediska času.

4.1.1 Externí audit

Tento druh audit je vyznačován, tím že je prováděn externími specialisty, kteří v daném podniku provedou analýzu a následné vyhodnocení auditu. Mezi externí audity řadíme účetní audit, audit jakosti, ekologický audit apod. Cílem externího auditu je vyjádřit objektivní názor na to, jestli stav hospodaření podniku odpovídá ekonomické a finanční situaci podniku v daném okamžiku. Další cílem této kontroly je shlédnout, zda výsledky hospodaření podniku jsou v souladu s obecně přijatými zásadami. [12]

4.1.2 Interní audit

Interní audit se nejdříve zabýval jen problematikou finančního auditu a vnitřní účetní kontroly, ale s postupem času se začíná audit provádět ve více oblastech. Hovoříme například o auditu operací, auditu managementu, auditu jakosti nebo auditu ekologické atd. Definice interního auditu se neustále mění. V současné době zní definice takto [12]: „interní audit je nezávislá, objektivní, ujišťovácí a konzultační činnost zaměřená na přidanou hodnotu a zlepšení provozu organizace.“ Hlavním úkolem interního auditu je pomáhat podnikům dosáhnout jejích cíle tím, že zavádí systematické metodický přístup k hodnocení a zlepšení efektivnosti řízení rizik.

4.1.3 Druhy auditu z hlediska času

Z hlediska času se audit dělí na 3 základní skupiny a to na [27]:

- Plánovaný audit – tento druh auditu probíhá v předem stanovených pravidelných časech. Interní i externí auditoři musí znát čas provádění audit s předstihem, aby si stihly projít veškerou dokumentaci a prostudovat bezpečnostní politiku daného podniku.
- Mimořádný audit – je v dané organizaci prováděn v případě významných změn v organizaci nebo podmínek, ve kterých působí, nebo pokud nastanou závažné problémy (např. havárie, živelné pohromy, obměna bezpečnostního managementu atd.)
- Následný audit – se provádí na doporučení auditora. Tato situace většinou nastává, pokud plánovaný a mimořádný audit vykazoval nesrovnalosti s bezpečnostní politikou firmy. Na základě zprávy z auditu, auditor vydá v závěrečné zprávě doporučení na sjednání nápravy.

4.2 Postup auditu

Tato kapitola se zabývá jednotlivými kroky při provádění audit v podniku, které jsou zobrazeny na obrázku 4. Každý individuální krok v auditu bude následně vysvětlen a krátce popsán. Tento postup auditu využívá jak interní, tak externí auditor. [7]

Obrázek 4: Proces auditu

Zdroj: vlastní zpracování podle [7]

Porozumění auditovanému objektu

Každý auditor se nejdříve před začátkem auditorské činnosti musí seznámit s objektem, kde se audit bude provádět. Poznávání se týká například identifikace vstupů a výstupů daného systému, organizační struktury, systémů řízení. Je velmi důležité, aby daný auditor byl seznámen s daný objektem a s podnikem. [7]

Stanovení cíle auditu

Hlavní cílem je poskytnou managementu zpětnou vazbu o operacích ve společnosti, identifikovat možnosti ke zlepšení a vytvořit doporučení pro nápravná opatření.

Určení požadovaného důkazního materiálu

Pří získávání důkazního materiálu si auditor musí dávat pozor na význam cíle auditu. Dále musí brát ohled na dostatečnou průkaznost dokladů a také na náklady na pořízení dokladů. V neposlední řadě by auditor neměl zapomínat na riziko, které může vzniknout při chybném závěru auditu. [7]

V tomto případě by měl důkazní materiál splňovat následující kritéria, musí být:

- relevantní pro cíl auditu, což znamená že daný materiál musí přímo ovlivňovat závěr auditu
- oprávněný, z důvodu toho, že by materiál neměl být nedůvěryhodný
- dostačující počet materiálu

Rozhodnutí o vhodných technikách auditu

Různé techniky, které auditorovi dovolují získat nezbytné informace a podrobit je dostačujícímu potřebnému zkoumání. Hlavní cílem těchto technik je umožnit auditorovi vytvořit si vlastní názor o zkoumaném problému. Mezi hlavní techniky, o kterých se auditor rozhoduje jsou např. fyzické zkoumání, testy dokumentace, dotazování, pozorování, výpočty a analýzy, srovnání atd. [7]

Shromažďování a analýza auditorských dokladů

Jedná se o plánovaný postup práce, který je pravidelně monitorován. Monitorování je velmi důležité z důvodu toho, aby bylo zjevné, co již bylo uděláno a co ještě zbývá provést. Daný program auditu může mít podobu, která je obsahem tabulky 3.

Tabulka 3: Program auditu

Typ auditu:			
Předmět auditu:			
Cíl auditu:			
Prověřované oblasti			
Auditované oblasti:			
Místo:			
Audit provede:			
Vztažná kritéria pro posuzování:			
Časový plán auditu:	od	do	náplň práce
• Přípravná práce			
• Podklady pro audit			

• Vlastní audit			
• Poauditní fáze			
Rozsah vyžádané dokumentace:			

Zdroj: vlastní zpracování podle [7]

Vytvoření zjištění a závěry auditu

Ve většině případů zjištění se skládají z formulování počáteční myšlenky, která má být zkoumána. Poté z kritéria, které určuje fungování za ideálního stavu, ze skutečného stavu fungování, důsledku a příčin stavu. Na každé zmiňované zjištění musí být vytvořen alespoň jeden závěr. [7]

Vypracování auditorské zprávy

Při skončení auditu musí auditor sepsat auditorskou zprávu, která poskytuje odborné a nezávislé posouzení zkoumané oblasti v podniku. Zpráva musí být poskytnuta příslušným manažerům, aby mohli co nejdříve napravit zjištěné chyby.

Postaudit

Každý manažer po obdržení auditorské zprávy by měl, co v nejkratší době zrealizovat všechny doporučení a závěry, které jsou uvedeny v závěrečné zprávě. Auditor následně prověřuje, zda nedostatky zjištěné při auditu byla skutečně odstraněny. [7]

4.3 Auditor

Auditorem podle zákona je fyzická osoba (dále jen „auditor“), která je zapsána v seznamu auditorů vedeném komorou (dále jen „seznam auditorů“). Auditorskou činnost mohou vykonávat i právnické osoby, které jsou zapsány v seznamu auditorů. Jménem právnických osob mohou auditorskou činnost vykonávat jen auditoři. [31]

4.3.1 Zpráva auditora

Každý auditor na konci auditu je povinen sepsat zprávu z auditu. V této zprávě by mělo být obsaženo zjištění a navržení určitého doporučení určená k odstranění případných nedostatků, které získal auditor v průběhu prověřování a dokdy by se měly případné nedostatky odstranit. Každá auditorská zpráva musí obsahovat i formální náležitosti, které jsou zde vypsány.

- Přesnost – zpráva nesmí obsahovat žádné chyby nebo překlepy
- Objektivnost – interní auditor musí svůj názor říct nezaujatě, nezkresleně
- Jasnost – zpráva musí být logická a dobře pochopitelná, nesmí obsahovat žádné auditorské pojmy, kterým by daný manažer nerozuměl
- Stručnost – zpráva by měla být krátká a obsahovat jenom ty nejdůležitější informace
- Konstruktivnost – zpráva přináší auditovanému subjektu prospěch a potřebná zdokonalení, nesmí obsahovat žádnou kritiku
- Včasnost – zpráva je napsána v plánovaném termínu

Auditor ve své zprávě z auditu je povinen vyjádřit svůj názor prostřednictvím výroku, který obsahuje takzvané „zhuštěné informace“ o tom, zda účetní závěrka a výroční zpráva věrně zobrazují majetek, závazky, vlastní jmění a výsledek hospodaření. Dané výroky mohou mít tyto formy [12]:

- **Výrok bez výhrad** – tento výrok vydá auditor tehdy, je-li přesvědčen, že všechny náležitosti v podniku jsou v souladu s realitou a s předpisy
- **Výrok s výhradou** – pokud je auditor určitým způsobem omezen ve své činnosti nebo byly zjištěné určité chyby v tomto případě auditor udává ve své zprávě výrok s výhradou
- **Záporný výrok** – tento výrok znamená ztrátu důvěry akcionářů, bank a dalších partnerů společnosti a může mít špatné důsledky na další činnost společnosti
- **Odmítnutí výroku** – tento výrok učiní auditor tehdy, jestliže byl natolik omezen ve své činnosti, že nemůže vyjádřit žádný názor na věrnost zobrazení v účetní závěrce

Závěrečná zpráva musí být nejdříve schválena a prověřena, a to buď vedoucím oddělení auditu nebo jinou pověřenou osobou, a poté může být vydána. Také musí být stanoveno, komu bude závěrečná zpráva předána. [12]

4.3.2 Zákon o auditorech

Zákon č. 93/2009 Sb. o auditorech je hlavní dokumentem, kde jsou vymezeny požadavky, které musí auditor splnit, chce-li získat oprávnění vykonávat auditorskou činnost. Mezi povinnosti patří i složení auditorské zkoušky, které se v zákoně věnuje především § 8. Tento paragraf vymezuje oblasti, z nichž se zkouška skládá, podobu a průběh zkoušky. Pověřená komise se především zaměřuje na teoretické znalosti a schopnosti jejich praktického využití v praxi. Po úspěšném absolvování zkoušky získá každý uchazeč tzv. oprávnění sloužící jako „certifikát“ pro vstup do auditorské profese. [13]

5 ČESKÁ POŠTA, S.P.

Podnik, který bude v této bakalářské práci sloužit jako objekt, při průběhu bezpečnostního auditu je státní podnik Česká pošta. Česká pošta je hlavním poskytovatelem poštovních služeb. Tento podnik byl v souladu se zákonem o státním podniku zapsán do obchodního rejstříku 1. března 1993. Za zakladatele České pošty, s.p. se považuje Ministerstvo vnitra České republiky. [9]

Logo České pošty se neustále zdokonaluje a mění. Nyní má podobu, která je znázorněna na obrázku 5.

Obrázek 5: logo

Zdroj: [9]

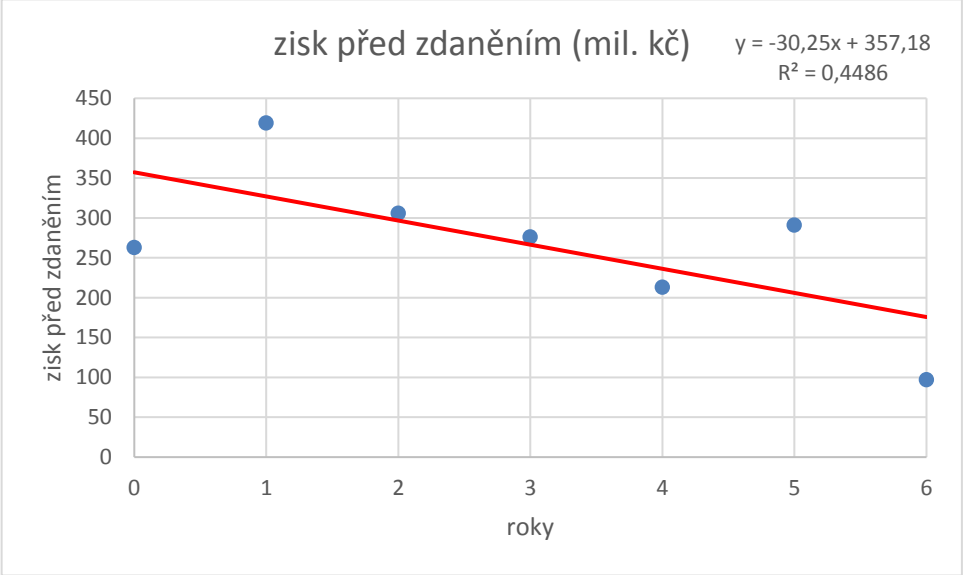
Správa a řízení podniku

Statutárním orgánem České pošty je generální ředitel, který řídí všechny činnosti podniku a jedná jeho jménem. Generální ředitel rozhoduje o všech záležitostech podniku, jestliže nejsou vyhrazeny určitým zákonem nebo jestli daná záležitost není v kompetenci dozorčí rady České pošty. Další orgánem, který působí ve vedení České pošty, je dozorčí rada. Tento orgán dohlíží na činnosti generálního ředitele a uskutečňování podnikatelských záměrů podniku. Dozorčí rada se skládá z deseti členů, kteří jsou jmenování a odvolávány zakladatel podniku. Dalších pět členů je jmenováno a odvoláváno zaměstnanci České pošty. Dalšími pravomocemi dozorčí řady je zřizování výborů dozorčí rady jako své pracovní, poradní a iniciativní orgány. Hlavním úkolem výborů je předběžné a podrobnější projednání materiálů, kterými se následně zabývá samotná dozorčí rada. V současně době jsou založeny tyto výbory dozorčí rady [9]:

- Výbor pro strategii a finance
- Výbor pro audit
- Výbor pro rozvoj lidských zdroj

Finanční pohled na podnik

Tato podkapitola se zabývá finanční pohledem na podnik v uplynulých sedmi letech. Na následujícím obrázku 6 jsou pomocí regresní analýzy vyobrazeny zisky před zdaněním v letech 2010 až 2016. Za 7 let si Česká pošta velice pohoršila, co se týče zisku před zdaněním, který v roce 2016 činil 96 milionů.



Obrázek 6: Zisk před zdaněním v letech 2010–2016

Zdroj: vlastní zpracování podle [9]

Podle statických výpočtu, které jsou uvedeny v tabulce 4 se dá říci, že korelační koeficient vyšel záporně, proto je regresní přímka klesající. Z výsledku bylo také zjištěno, že korelační koeficient v absolutní hodnotě je větší než kritická hodnota na hladině významnosti 0,1, proto zde existuje vztah mezi výši zisku před zdaněním a roky. V druhém případě korelační koeficient v absolutní hodnotě je menší než kritická hodnota na hladině významnosti 0,05, proto zde vztah mezi výši zisku a roky neexistuje

Tabulka 4: Statické výpočty výši zisku před zdaněním

Index těsnosti R^2		0,4486
Korelační koeficient R		- 0,6698
Kritická hodnota R^2	hladina α=0,1	0,6694
	hladina α=0,05	0,7545

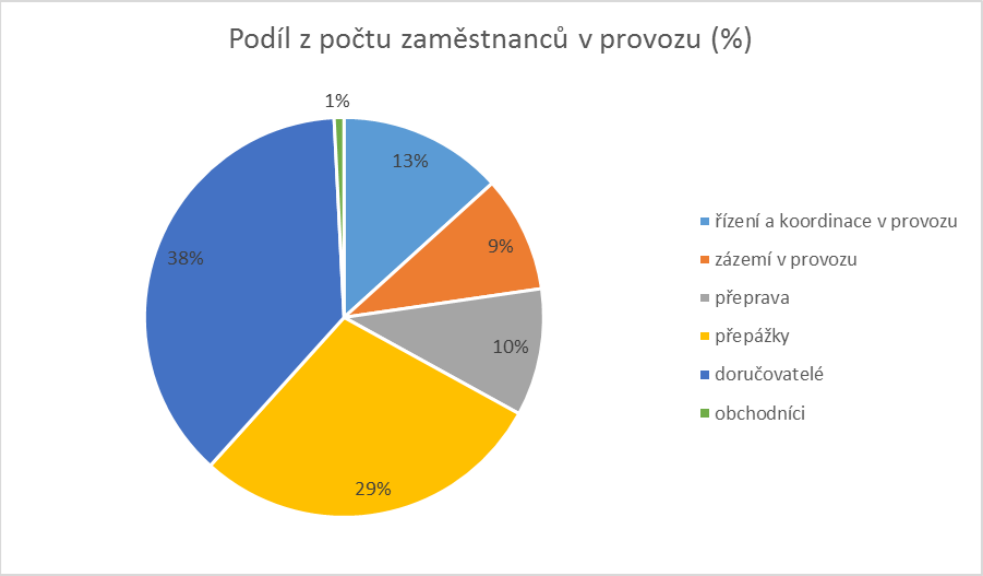
Zdroj: vlastní zpracování

Podle názoru autora, většina lidí, kteří dříve využívali služby České pošty, nyní jsou pohlceny moderním, a hlavně elektronickým světem. Skoro všichni obyvatelé České republiky komunikují přes sociální sítě nebo pomocí emailu. Z důvodů toho, že lidé můžou

komunikovat se svými příbuznými či přáteli z pohodlí svého domova bez žádného čekání ve frontách na poště se zisk před zdaněním snižuje. To je hlavní důvod tak velkého poklesu zisků České pošty.

Zaměstnanci

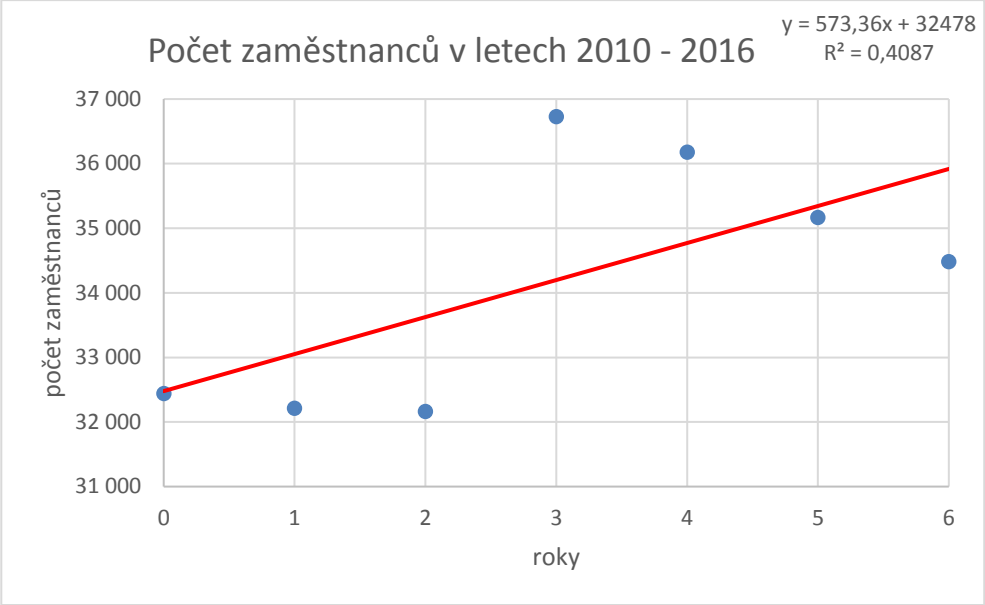
V roce 2016 počet zaměstnanců na České poště byl 34 484 pracovníků. Na následujícím obrázku 7 jsou pomocí výsečového grafu procentě vyobrazeny podíly z počtu zaměstnanců v provozu. Nejčetnější skupinou v provozu jsou doručovatelé, kteří tvoří 38 % ze všech provozních zaměstnanců. Další početnou skupinou jsou pracovníci přepážek, kteří tvoří 29 % z celkového počtu. Zaměstnanci v dopravě tvoří 10 % a pracovníci v zázemí 9 % z počtu provozních zaměstnanců.



Obrázek 7: Graf znázorňující podíly z počtu zaměstnanců v provozu

Zdroj: vlastní zpracování podle [9]

Na obrázku 8 jsou vyjádřeny celkové počty zaměstnanců od roku 2010 do roku 2016. Počet zaměstnanců pracujících na České poště neustále roste, jak je zřejmé z obrázku. Největší počet zaměstnanců byl v roce 2013, kdy Česká pošta zaměstnávala více jak 36 500 pracovníků.



Obrázek 8: Vývoj počtu zaměstnanců

Zdroj: vlastní zpracování podle [9]

Podle statického vyjádření, které je zobrazeno v tabulce 5 můžeme říci, že regresní přímka má rostoucí trend, z důvodů toho že je korelační koeficient kladný. V tomto případě je korelační koeficient v absolutní hodnotě menší než kritická hodnota na hladině významnosti 0,1 a také menší než kritická hodnota na hladině významnosti 0,05, z čehož vyplývá, že korelační vztah mezi počtem zaměstnanců a roky neexistuje. Česká pošta nemůže předpovídat budoucí vývoj zaměstnanosti.

Tabulka 5: Statické výpočty

Index těsnosti R^2		0,4087
Korelační koeficient R		0,6393
Kritická hodnota R^2	hladina α=0,1	0,6694
	hladina α=0,05	0,7545

Zdroj: vlastní zpracování

Lze vyvodit závěr, že pokles počtu zaměstnanců v posledních třech letech byl velmi ovlivněn poklesem zájmu o poštovní služby. Pokud není zájem o poštovní služby, klesají tržby a podnik poté nemá dostatek nákladů na vyplácení mezd nebo dochází k rušení některých poboček České pošty na malých vesničkách, kde jsou minimální tržby.

5.1 Audit České pošty, s.p.

Státní podnik Česká pošta je jedna z podniků, kde se klade velký důraz na bezpečnost. Poskytování poštovní služeb a peněžních služeb je velmi rizikový druh podnikání. Česká pošta má na starosti zajistit základní bezpečnostní požadavky pro plynulý provoz těchto služeb.

V organizační struktuře je samostatný úsek bezpečnosti, který nese odpovědnost za bezpečnost majetku, ochrany klientů České pošty a svých zaměstnanců. Další důležitou povinnosti této sekce je problematika krizového řízení a plánování, řešení vnější a vnitřní trestné činnosti proti České poště či správa utajovaných skutečností v rámci provozu České pošty. Do širšího pojetí bezpečnosti České pošty patří také podnikový compliance program, což je program proti korupci a dalším formám nekalého jednání.

5.1.1 Průběh bezpečnostního auditu

Česká pošta provádí bezpečnostní audit pomocí interního auditu, který je nezávislým odborným útvarem České pošty. Tento útvar se nezabývá jen interním auditem, ale také má na starosti řízení rizik.

Celý průběh bezpečnostní audit na České poště, který je uveden na obrázku 9 začíná rozhodnutím o zahájení auditu, nejčastější příčinou zahájení audit je shledání určitého rizika nebo hrozby, která se musí zkontrolovat. Dále se pokračuje naplánováním auditu, jak daný audit bude probíhat a co vše se bude analyzovat a kontrolovat. V tento moment interní auditor naplánuje jednotlivé kroky auditu a stanoví co bude předmětem. Tedy jaká oblast v podniku bude zkoumána. Dalším krokem je sběr informací, které jsou k dispozici a jsou nutné k analýze případných rizik. Po sběru příslušných informací nastává samotná analýza a poté se dojde k určitému vyhodnocení a následně přijetí opatření.

Obrázek 9: Průběh bezpečnostního auditu

Zdroj: vlastní zpracování podle [9]

Česká pošta je podnik, kde se bezpečnostní audit provádí je na základě rozhodnutí o tom, že se má audit provést. Nejsou zde žádné dané termíny nebo pravidelné intervaly, ve kterých by se audit měl provádět.

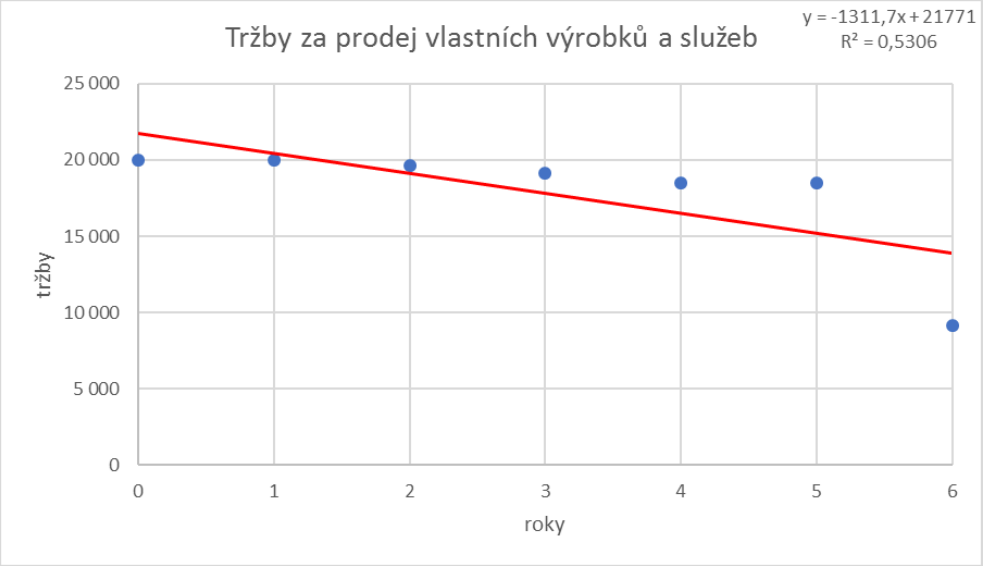
Podle názoru autora by Česká pošta měla provádět bezpečnostní audit pravidelně alespoň jednou ročně. Z důvodů toho, že je Česká pošta považována za podnik, který manipuluje s cennými a utajovanými informacemi a také s peněžními částkami, by měl být více kladen důraz na bezpečnostní audit. Autorka si myslí, že bezpečnostní audit v České poště by měl být prováděn především v oblasti zabezpečení informací, peněz a také poboček, kde je pravděpodobně největší výskyt nebezpečí při loupeži. [9]

5.2 Vlastní zpracování auditu

Z důvodů tohoto, že Česká pošta je velmi známý podnik a nebylo by správné z důvodů bezpečnosti zveřejňovat různé informace týkajících se například nákladů na bezpečnost nebo informace o tom, jak jsou zabezpečeny různé přepážky atd. Proto se autorka této práce rozhodla na základě poskytnutých disponibilních údajů od České pošty provést v některých oblastích bezpečnostní audit a vyhodnotit výsledky.

5.2.1 Hospodaření podniku

Na základě přístupných údajů z výkazu zisků a ztrát byla vytvořena lineární regresní analýza, která ukázala vývoj podnik v oblasti hospodaření. Na obrázku 10 je znázorněna lineární regrese tržeb za prodané vlastní výrobky a služby od roku 2010 do roku 2016.



Obrázek 10: Tržby za prodej vlastních výrobků a služeb

Zdroj: vlastní zpracování podle [9]

Jak je vidět lineární přímka klesá, a to je pro podnik velmi závažné, protože když klesají tržby je větší pravděpodobnost, že je podnik ve velkých problémech a měl by to co nejdříve řešit.

Ze statického hlediska se dá klesající přímka interpretovat z výsledků, které jsou vypsány v tabulce 6. V tabulce je zobrazen korelační koeficient s výsledkem v absolutní hodnotě -1, což je hlavní důvod, proč má regresní přímka klesající charakter. Dále je korelační koeficient v absolutní hodnotě větší než kritická hodnota na hladině významnosti 0,1 tak i na hladině významnosti 0,05, proto zde existuje korelační vztah mezi výší zisku a roky. Jelikož zde existuje korelační vztah mezi výši zisku a roku, Česká pošta může předpovídat budoucí vývoj tržeb za prodej vlastních výrobků a služeb. S největší pravděpodobností budou tržby za vlastní výrobky a služby stále klesat.

Tabulka 6: Statické výpočty tržeb

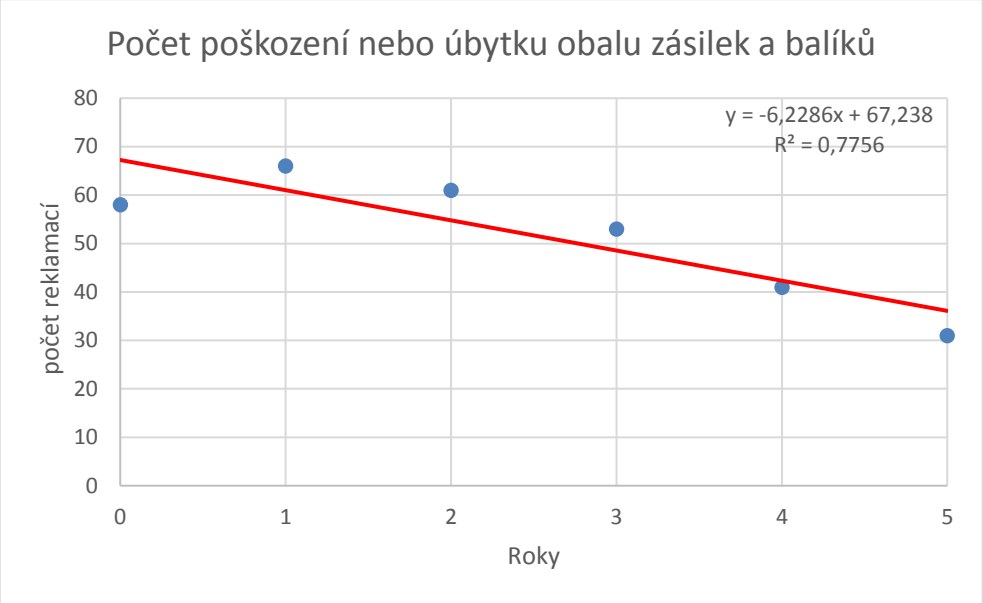
Index těsnosti R^2		0,5306
Korelační koeficient R		-1
Kritická hodnota R^2	hladina α=0,1	0,6694
	hladina α=0,05	0,7545

Zdroj: vlastní zpracování

Pravděpodobně hlavní příčinou, tak velkého poklesu tržeb je klesající zájem o poštovní služby především o listovní zásilky vlivem vyššího používání elektronických způsobů komunikace (e-maily, sociální sítě, datové zprávy aj.).

5.2.2 Reklamace

Každý rok se objevují různé reklamace týkající se poškození či úbytku obalu zásilek a balíku. Obrázek 11 vyobrazuje počty reklamací v letech 2010 až 2015. Jak je zřejmé z regresní přímky, která má klesající charakter, Česká pošta úspěšně snižuje počty reklamací. V roce 2015 bylo na 1 milión podaných poštovních zásilek, u nichž pošta odpovídá za poškození a úbytek obsahu připadlo 31 případů reklamací poškození nebo úbytku.



Obrázek 11: Počet reklamací

Zdroj: vlastní zpracování podle [9]

Podle korelačního koeficientu, který v tabulce 7 vychází záporně je regresní přímka klesající. Korelační koeficient v absolutní hodnotě je větší než kritická hodnota na hladině významnosti 0,1 tak i kritická hodnota na hladině významnosti 0,05, proto zde existuje vztah mezi počtem reklamací a roky. Pomocí těchto výpočtu se dá říci, že Česká pošta je schopna odhadnout budoucí vývoj počtu reklamací s největší pravděpodobní bude počet reklamací v budoucí letech klesat.

Tabulka 7: Statické výpočty reklamací

Index těsnosti R^2		0,7756
Korelační koeficient R		- 0,8807
Kritická hodnota R^2	hladina α=0,1	0,7293
	hladina α=0,05	0,8114

Zdroj: vlastní zpracování

Lze vyvodit závěr, že Česká pošta úspěšně snižuje počty reklamací, týkajících se poškození nebo úbytku obsahu poštovní zásilky či balíku.

5.2.3 Bezpečnost a ochrana zaměstnanců České pošty

Česká pošta klade velký důraz a pozornost na zajištění bezpečnosti a ochrany zdraví při práci a na zajištění požární ochrany. Hlavní cílem BOZP je vytvořit zdravé prostředí pro práci svých zaměstnanců a zajistit odstranění rizik, které by mohli předcházet vzniku pracovních úrazů na pracovištích.

Zákonné normy

V tabulce 8 jsou znázorněny všechny zákonné normy, kterými se musí odbor BOZP/PO řídit a řádně je dodržovat.

Tabulka 8: Zákonné normy

Zákonné normy	
Zákon č. 262/2006 Sb.	Zákoník práce
Zákon č. 309/2006 Sb.	Požadavky BOZP v pracovněprávních vztazích
Zákon č. 258/2000 Sb.	Zákon o ochraně veřejného zdraví
Zákon č. 174/1968 Sb.	Zákon o státním odborném dozoru nad bezpečností práce
NV č. 495/2001 Sb.	Podmínky a rozsah o poskytování ochranných pracovních prostředků, mycích, čistících a dezinfekčních prostředků
NV č. 361/2007 Sb.	Podmínky ochrany zdraví při práci
NV č. 101/2005 Sb.	Požadavky na pracovištích a pracovního prostředí
Vyhláška MZ č. 432/2003 Sb.	Podmínky pro zařazování prací do kategorií prací
Zákon č. 133/1985 Sb.	Zákon o zajištění PO
Vyhláška MV č. 246/2001 Sb.	Vyhláška o stanovení podmínek požární bezpečnosti a výkonu státního požárního dozoru

Zdroj: [9]

Pro Českou poštu je velmi důležité dodržování zákoníku práce a dalších zákonných norem, které se týkají BOZP a PO. Proto bylo v roce 2015 provedeno celkem 2888 kontrol, které byly prováděny vnitřní kontrolní činností. Důležitost problematiky BOZP a PO je také v zájmu kontrolní činnosti státního odborného dozoru. V roce 2015 bylo u státního podniku Česká pošta provedeno celkem 41 kontrol ze strany Hasičských záchranných sborů ČR, 4 kontroly ze strany inspekce práce a 54 kontrol z oblasti hygieny práce, kdy České poště nebyla ze strany státního odborného dozoru vyměřena žádná pokuta za porušení předpisů BOZP a PO. [9]

Školení BOZP

Česká pošta školí se zaměstnance v oblasti BOZP jednou ročně. Na každém školení se procházejí právní předpisy o BOZP a podrobnější detaily o této problematice. Školení zaměstnanců v oblasti BOZP a PO nemusí Česká pošta vynakládat kromě mzdových nákladů žádné jiné náklady, protože školení provádí interní zaměstnanec, který byl řádně proškolen pro tuto profesi.

Lze vyvodit závěr, že školení prováděné jednou ročně je nedostačující, v tak rizikovém oboru podnikání jako je Česká pošta. Školení by se mělo provádět častěji u pozic, u kterých je větší riziko například úrazu, to může být například u obsluhování třídícího stroje na listovní zásilky. [9]

Pracovní úraz

Definice pojmu pracovní úraz je uvedena v § 380 odst. 1 zákoníku práce. Pracovním úrazem se rozumí poškození zdraví nebo smrt, které byly zaměstnanci způsobeny nezávisle na jeho vůli krátkodobým, náhlým a násilným působením vnějších vlivů nebo vlastní tělesné síly při plnění pracovních úkolů.

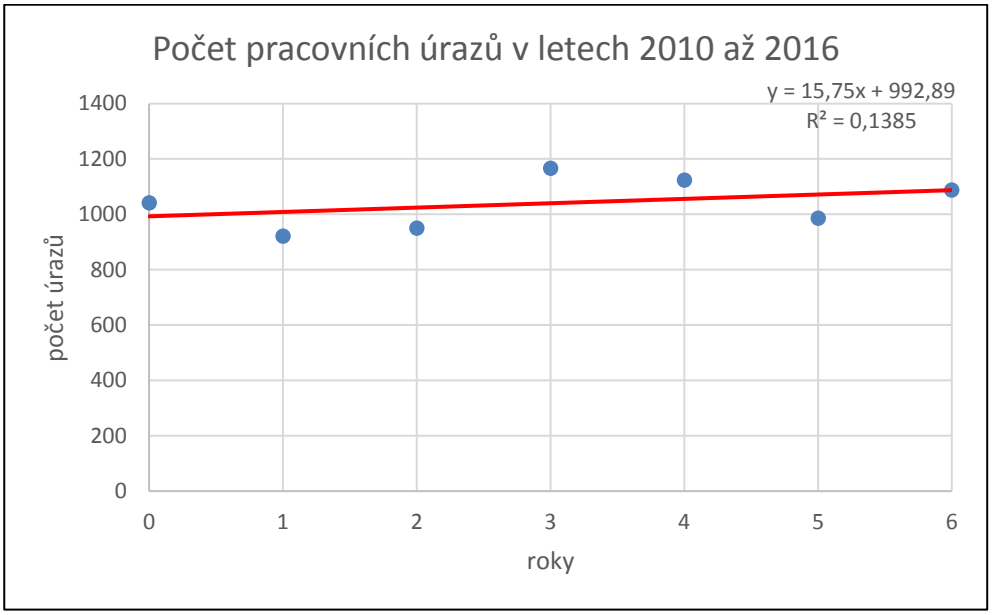
Pracovní úrazy se rozlišují podle druhů na:

- Smrtelný pracovní úraz – je poškození zdraví, na jehož následky postižený zaměstnanec zemřel nejpozději do 1 roku
- Pracovní úraz s hospitalizací delší než 5 dnů
- Ostatní pracovní úrazy

Každý zaměstnanec je povinen nahlásit pracovní úraz svému nadřízenému, který úraz za eviduje do knihy úrazů, která může mít listovní nebo elektronickou podobu. Součástí knihy úrazu je také list, kde se evidují všechny pracovní úrazy v podniku. Vzor tohoto listu je umístěn v příloze A.

Počet úrazů za období 2010 až 2016 se moc neměnil, hodnota počtu úrazů se pohybuje většinou okolo tisíce pracovních úrazů za rok, což není pro Česká poštu žádná vizitka. Spojnicový trend má růstový charakter, což znamená že počet úrazů v pracovní činnosti roste.

Na základě údajů o pracovních úrazech byla vytvořena regresní analýza, která je zobrazena na obrázku 12.



Obrázek 12: Počet pracovních úrazů

Zdroj: vlastní zpracování podle [9]

Ze statistických výpočtu, které jsou zobrazeny v tabulce 9, se dá interpretovat výsledek korelačního koeficientu, který vyšel v kladných číslech, proto má regresní přímka nepatrně rostoucí trend. Poté korelační koeficient v absolutní hodnotě je menší než kritická hodnota na hladině významnosti 0,1 i 0,05, proto zde neexistuje vztah mezi počtem pracovních úrazů a roky. Z toho výsledku Česká počtu nedokáže určit pravděpodobný vývoj počtu úrazů v budoucích letech.

Tabulka 9: Statické výpočty pracovních úrazů

Index těsnosti R^2		0,1385
Korelační koeficient R		0,3722
Kritická hodnota R^2	hladina α=0,1	0,6694
	hladina α=0,05	0,7545

Zdroj: vlastní zpracování

Autor této práce doporučuje zaměřit se více na problematiku pracovních úrazů, kde vznikají nejčastěji nebo jaké příčiny vedou tak k vysokému počtu úrazů. Každý doručovatel jezdící na jízdním kole, by měl nosit bezpečnostní helmu, která zabrání poranění hlavy nebo jinému zranění. Dále by mělo docházet k častějším školení zaměstnanců pracujících u třídících linek, kde je také pravděpodobně velký počet úrazů.

5.2.4 Mimořádné události podniku

Dle zákona č. 239/2000 Sb o integrovaném záchranné systému se mimořádnou událostí rozumí škodlivé působení sil a jevů vyvolaných činností člověka, přírodními vlivy a také havárie, které ohrožují život, zdraví, majetek nebo životní prostředí a vyžaduje provedení záchranných a likvidačních prací.

Mimořádné události lze dělit na [14]:

- Přírodní události, které jsou vyvolané přírodními jevy (např. záplavy a povodně, krupobití, přívalové deště, vichřice, bouřky, sněhové kalamity, požár způsobený například blesk atd.)
- Antropogenní událostí, které jsou způsobené člověkem (např. provozní havárie spojené s velkými požáry, rozsáhlé poruchy energetických sítí, terorismus atd.)
- Kombinované události, které jsou způsobené společným působením člověka a přírody (např. povodně, které jsou způsobené přírodními silami, ale jejich následky jsou zhoršené zásahem člověka při úpravě koryt řek)

Česká pošta se každý rok setkává s mimořádnými událostmi, které se musí řádně a důkladně prozkoumat, aby byly zjištěny příčiny vzniku a následné omezení či odstranění rizik. Analýzu těchto mimořádných událostí má na starosti sekce bezpečnost, která se musí postarat o omezení či odstranění případného rizika. Česká pošta se v letech 2014 a 2016 setkala s několika mimořádnými událostmi, a to především s nebezpečnými zásilkami, povětrnostními vlivy, technologickými poruchami a také s kriminalitou. [9]

Nyní v následujících podkapitolách budou jednotlivé události popsány a grafický znázorněny. Počty mimořádných událostí byly rozděleny do regionů, jejichž rozdělení je zobrazeno v tabulce 10.

Tabulka 10: Rozdělení krajů do regionů

Region	Kraje
Praha	hl. město Praha, Středočeský kraj
západní Čechy	Karlovarský kraj, Plzeňský kraj
východní Čechy	Královehradecký kraj, Pardubický kraj, Vysočina
severní Čechy	Ústecký kraj, Liberecký kraj

jižní Čechy	Jihočeský kraj
jižní Morava	Olomoucký kraj, Zlínský kraj, Jihomoravský kraj
severní Morava	Moravskoslezský kraj

Zdroj: vlastní zpracování

Nebezpečné zásilky

Česká pošta každý den manipuluje s velkým množstvím poštovních zásilek a balíku. Bohužel v některých případech dochází k nalezení nebezpečné zásilky. Na stránkách České pošty si každý zákazník může najít, co nepatří do poštovních zásilek a balíku.

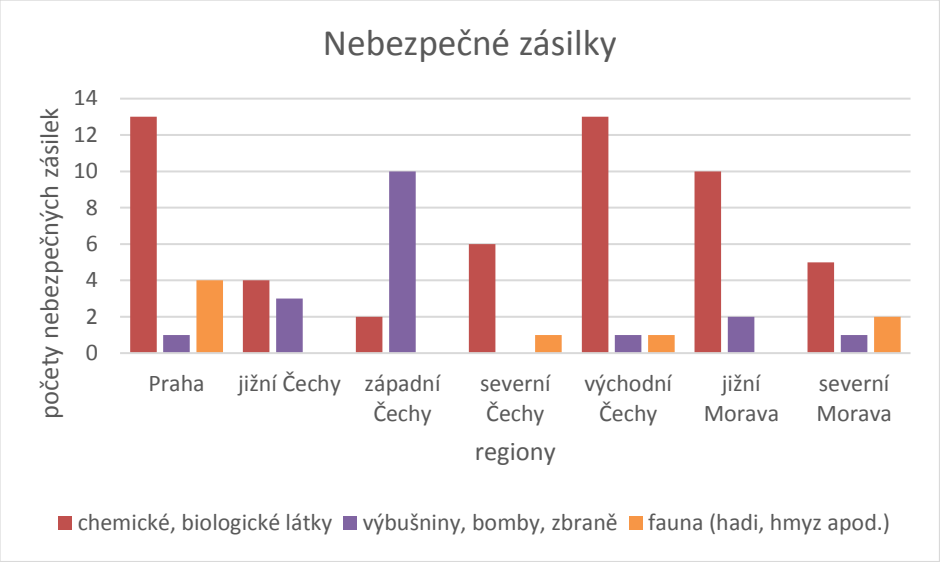
Podle České pošty obsahem poštovních zásilek nesmějí být [15]:

- výbušniny
- radioaktivní látky
- omamné a psychotropní látky
- jedovaté a žíravé látky
- nakažlivé biologické látky a lidské nebo zvíření vzorky
- tuhý oxid uhličitý
- tlakové nádoby, stlačené nebo zkapalněné plyny
- živí obratlovci

Česká pošta se v letech 2014 až 2016 setkala s nebezpečnými zásilkami jejichž obsahem byly chemické a biologické látky, výbušniny, zbraně nebo zvířata (hadi, hmyz apod.). Podle údajů z České pošty nejvíce chemických a biologických látek bylo nalezeno v regionech Praha a východní Čechy. Největší výskyt nebezpečných zásilek, jejichž obsahem byly zbraně nebo různé výbušniny, byl v západních Čechách.

V tomto případě Česká pošta nezabraní vzniku nebezpečných zásilek a ani se proti těmto rizikům nemůže zabezpečit, protože za tvorbu nebezpečných zásilek mohou obyvatelé ČR. Buďto úmyslně zasílají v poštovních balíčkách nebezpečný obsah, nebo si řádně neprostudují, co všechno nesmí být obsahem poštovní zásilky.

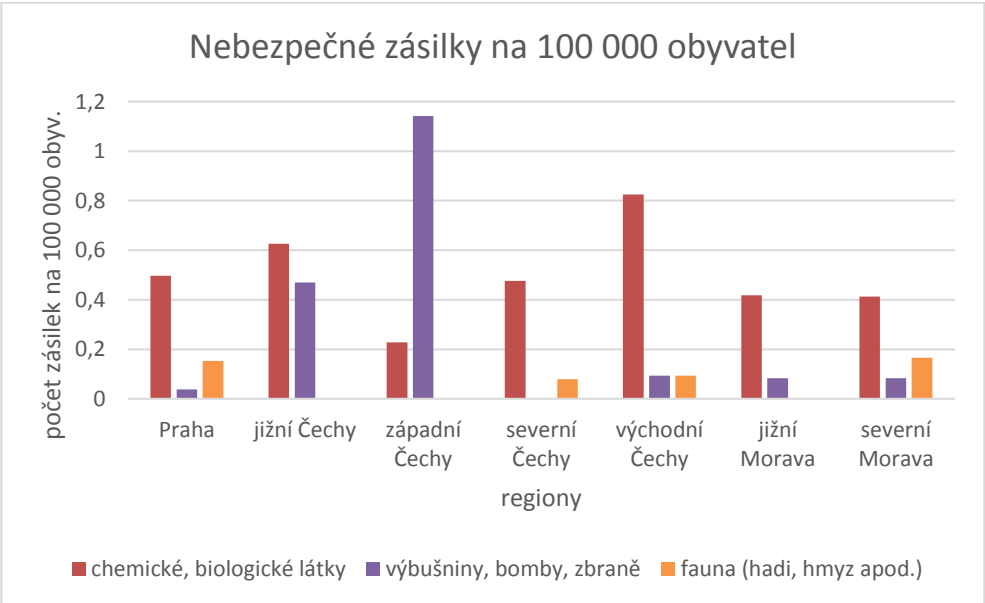
Na obrázku 13 jsou pomocí sloupcového grafu znázorněny celkové počty nebezpečných zásilek od roku 2014 do roku 2016 v jednotlivých regionech.



Obrázek 13: Graf zobrazující počty nebezpečných zásilek

Zdroj: vlastní zpracování podle [9]

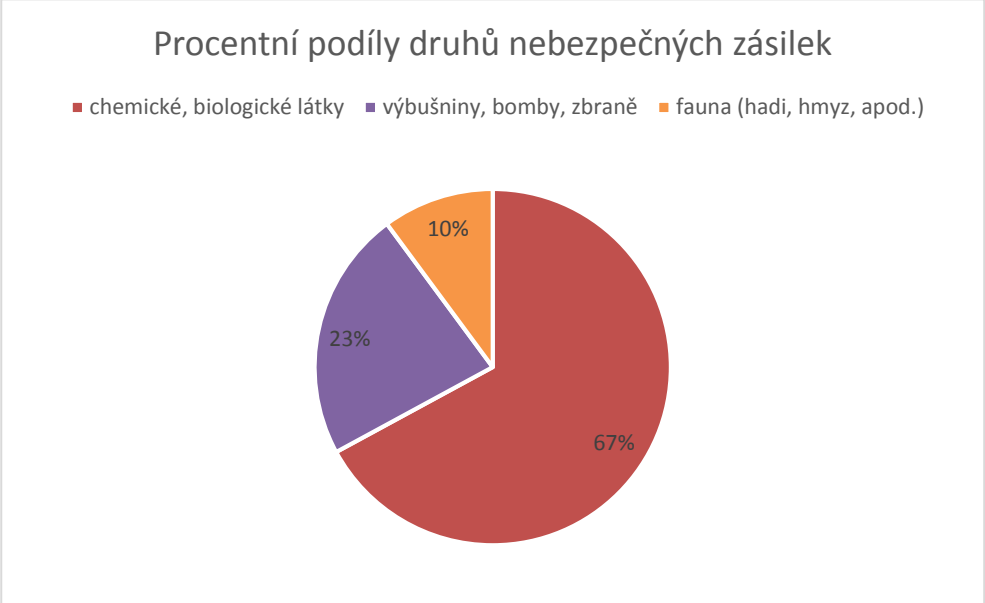
Na obrázku 14 jsou počty nebezpečných zásilek přepočítány na intenzivní ukazatelé, které jsou specifický, tím že charakterizují míru, v jaké jsou extenzivní ukazatelé podnikem využívány. Graf znázorňuje počty nebezpečných zásilek přepočítané na 100 000 obyvatel. I v tomto případě největší počet nebezpečných zásilek s obsahem výbušnin, bomb nebo zbraní je v západních Čechách, kde na 100 000 obyvatel připadá 1 nebezpečná zásilka.



Obrázek 14: Počet nebezpečných zásilek na 100 000 obyvatel

Zdroj: vlastní zpracování podle [9]

Pro lepší představu, jsou pomocí výsečového grafu na obrázku 15 zobrazeny procentní podíly jednotlivých druhů nebezpečných zásilek. Největší podíl mají nebezpečné zásilky s obsahem chemických a biologických látek. Druhé jsou výbušniny a zbraně. Nejmenší podíl z celkového počtu nebezpečných zásilek mají zvířata, které se nejméně objeví v poštovních zásilkách nebo balíkách.



Obrázek 15: Graf popisující procentní podíly druhů nebezpečných zásilek

Zdroj: vlastní zpracování podle [9]

Mimořádné události způsobené klimatem

Mezi tyto události patří vichřice, bouřka, povodeň nebo také sněhová kalamita. Všechny tyto druhy mimořádných událostí jsou způsobovány přírodními vlivy. Každý podnik se proti těmto událostem nemůže moc chránit. Pro menší ztráty na majetku nebo menší počtu úrazů si podnik může zajistit určitá prevenční opatření například protipovodňové bariéry. [14]

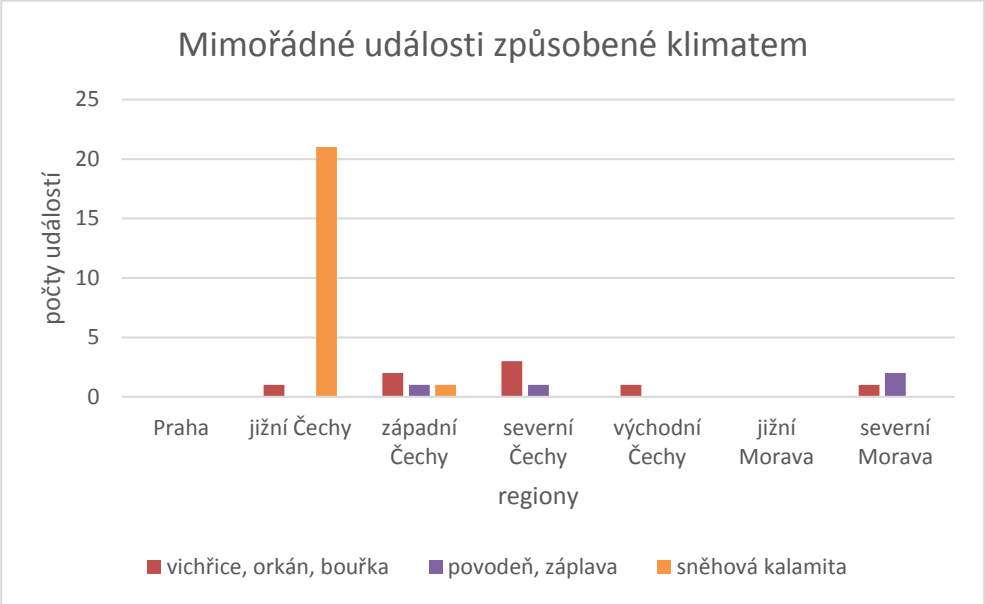
Sněhová kalamita většinou vniká v důsledku intenzivního sněžení, jehož následkem ve většině případů dochází k poškození střech budov a vozidel vahou sněhu nebo ke zvýšení počtu zvýšení počtu zraněných osob.

Bouřky jsou dalším typem mimořádných událostí, které představují další riziko pro podnik. Například blesky mohou způsobit požár budov, při kterém mohou být zraněni i zaměstnanci. Bouřky se mohou vyskytovat na celém území České republiky, největší pravděpodobnost vzniku silných bouřek je v období květen až září.

Vichřice se ve většině případu nejčastěji vyskytuje v horských oblastech. Nebezpečí u tohoto druhu rizika vniká v možném dlouhodobějším výpadku el. energie nebo zničení některých částí majetku. Vichřice se nejčastěji objevují ve vyšších nadmořských polohách.

Celkové počty jednotlivých druhů mimořádných událostí způsobených klimatem jsou zobrazeny a obrázku 16. Největším problémem jsou sněhové kalamity, které se nejčastěji tvoří v jižních Čechách, kde bylo zaevidováno přes 20 událostí. Ostatní mimořádné události jako jsou bouřky, vichřice nebo povodeň mají ve všech regionech mnohem menší počty, než má sněhová kalamita.

Nejvyšší počet sněhových kalamit v jižních Čechách, lze odůvodnit, tím že Jihočeský kraj, který je součástí jižních Čech, má většinu území v nadmořské výšce 400-600 m, s čímž souvisejí poněkud drsnější klimatické podmínky.

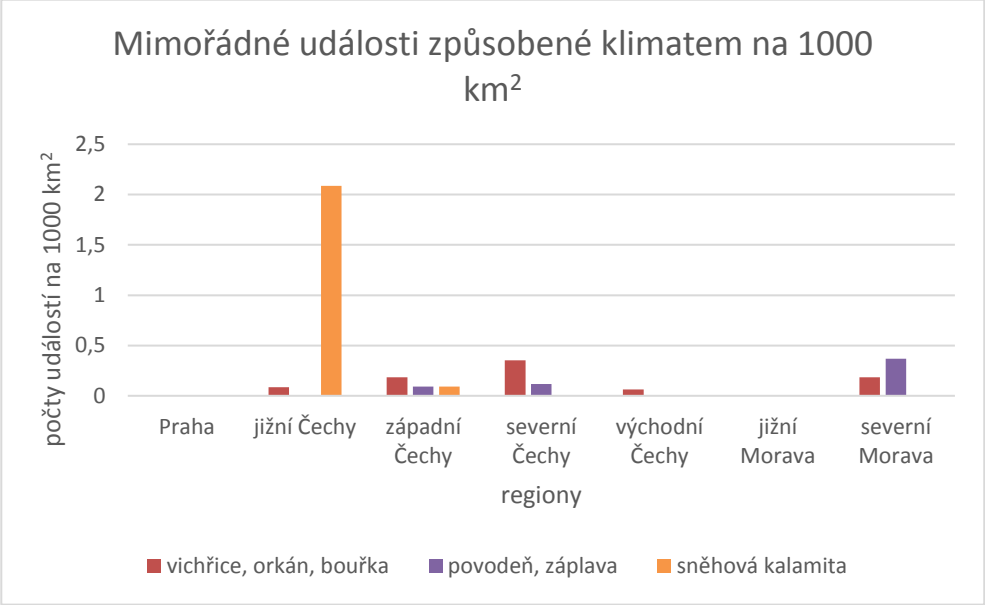


Obrázek 16: Mimořádné události způsobené klimatem

Zdroj: vlastní zpracování podle [9]

Lze vyvodit závěr, že tento typ mimořádných událostí vzniká nejvíce v jižních Čechách, kde je vysoká nadmořská výška. V ostatních regionech je v malém počtu. Proti těmto událostem se Česká pošta nemůže zabezpečit.

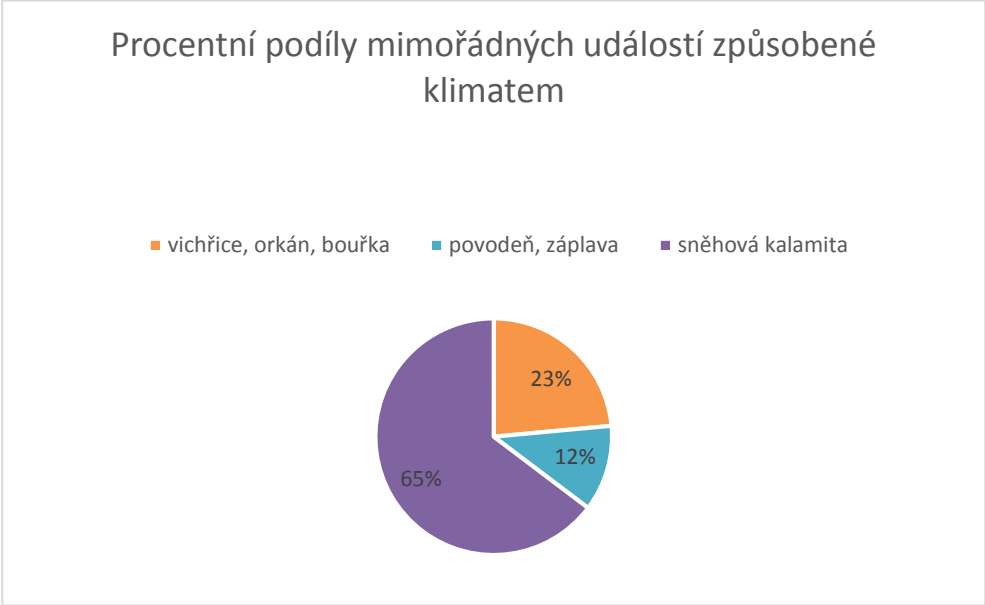
Po přepočítání počtu mimořádných událostí na 1000 km^2 se na obrázku 17 nic závažného nezměnilo. Pořád je největší výskyt sněhových kalamit ve východních Čechách.



Obrázek 17: Mimořádné události způsobené klimatem na 1000 km^2

Zdroj: vlastní zpracování podle [9]

Výsečový graf, který je vyobrazen na obrázku 18, zobrazuje procentní podíly jednotlivých mimořádných událostí způsobené klimatem. Největší podíl z celého počtu mimořádných událostí zaujímá sněhová kalamita, která se objevuje v 65 % mimořádných událostí. Další část výsečového grafu tvoří vichřice, orkán a bouřka, které mají 23 % z celkového počtu.

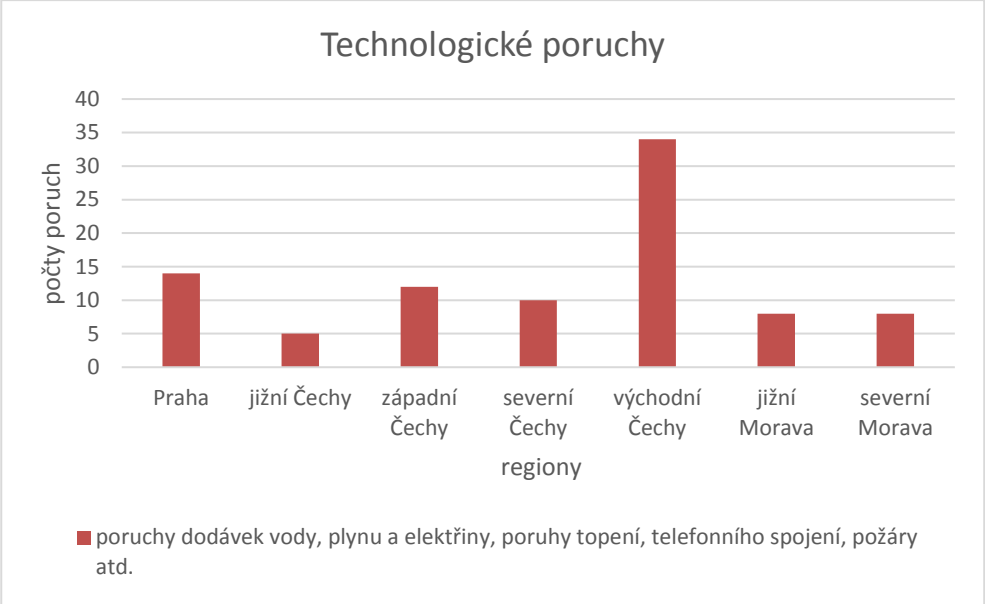


Obrázek 18: Graf znázorňují podíly jednotlivých mimořádných události

Zdroj: vlastní zpracování podle [9]

Technologické poruchy

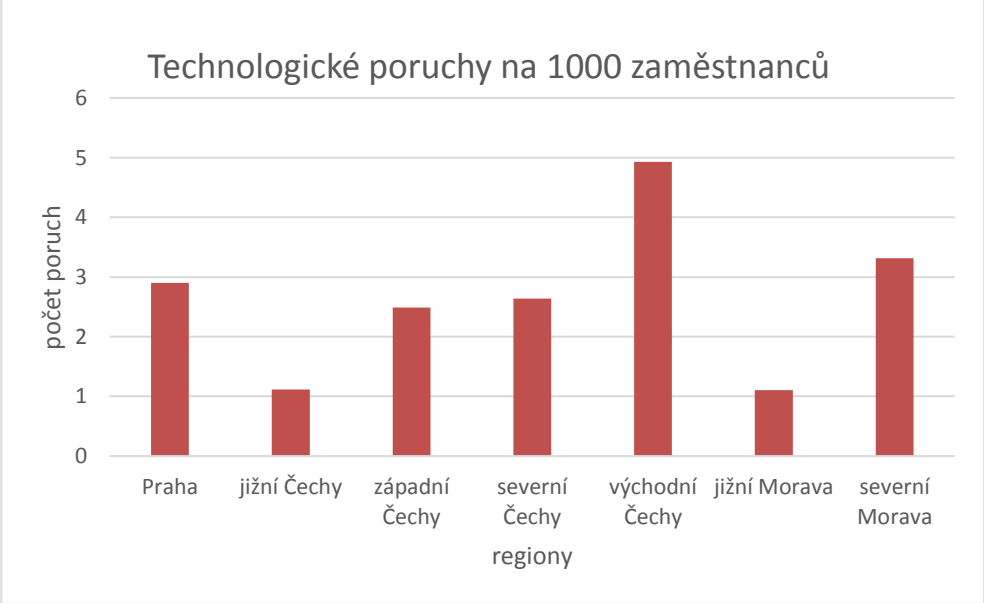
Mezi tyto technologické poruchy se řadí například poruchy dodávek vody, plynu a elektřiny nebo také požáry atd. Nejvíce poruch tohoto typu vzniklo ve východních Čechách, kde bylo zjištěno podle obrázku 19 více jak 34 případů technologických poruch.



Obrázek 19: Technologické poruchy

Zdroj: vlastní zpracování podle [9]

Na dalším obrázku 20 jsou přepočítány technologické poruchy na 1000 zaměstnanců a zobrazeny pomocí sloupcového grafu.



Obrázek 20: Technologické poruchy na 1000 zaměstnanců

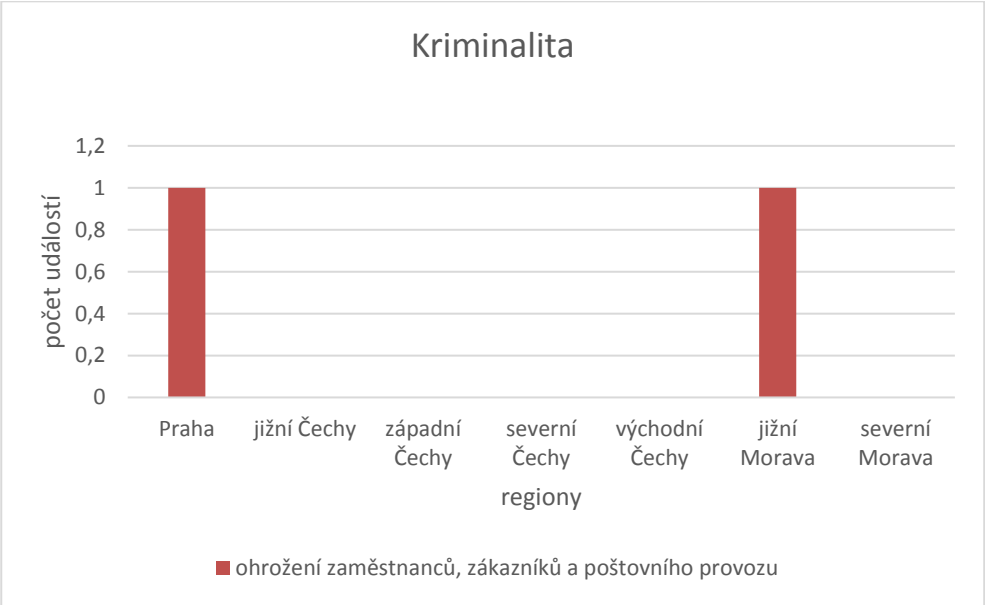
Zdroj: vlastní zpracování podle [9]

Na druhém obrázku, který znázorňuje technologické poruchy přepočítané na 1000 zaměstnanců připadá 5 událostí tohoto typu na 1000 zaměstnanců ve východních Čechách. Na druhém místě je severní Morava a následuje Praha.

Lze vyvodit závěr, že technologické poruchy mohou být zapříčeny nepříznivými přírodními vlivy jako je například bouřka, která může způsobit výpadek elektrické energie. Technologické poruchy mohou být také zapříčeny lidmi, které mohou způsobit úmyslně či neúmyslně požár.

Ohrožení zdraví

Česká pošta klade velký důraz na bezpečnost svých zaměstnanců, klientů a také na bezpečnost poštovního provozu. Na obrázku 21 jsou pomocí grafu zobrazeny počty událostí, kde došlo buďto k ohrožení zaměstnance nebo klienta nebo došlo k ohrožení celkového poštovního provozu. Jak je vidět na grafu celý rok byli zjištěny dvě ohrožení na životě. Jedno spáchání trestné činnosti bylo v hlavním městě a druhé na jižní Moravě.



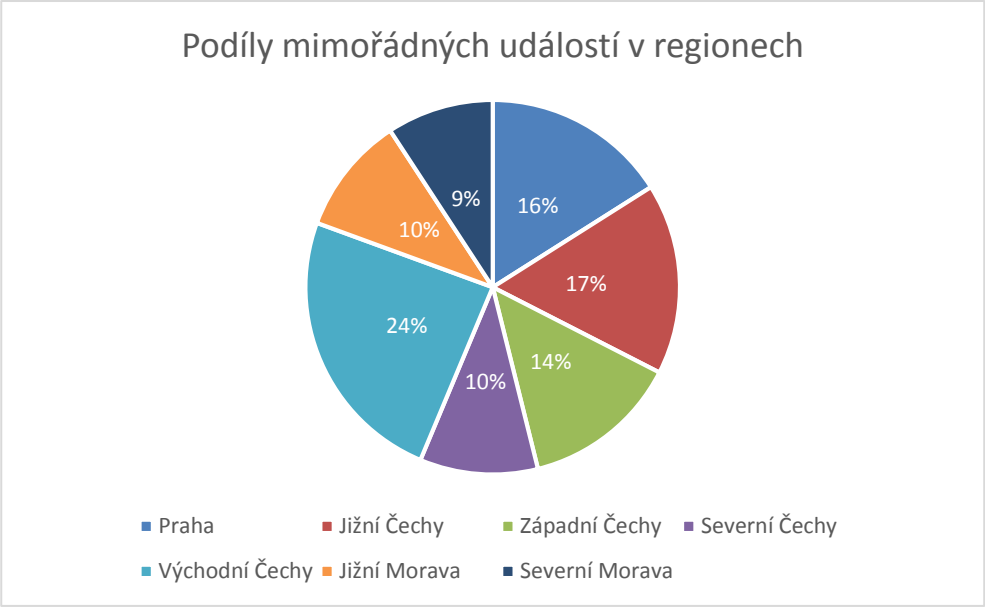
Obrázek 21: Kriminalita

Zdroj: vlastní zpracování podle [9]

Lze vyvodit závěr, že 2 údásloti, které byli evidovány jako ohrožení zaměstnanců, klientů pošty nebo poštovního provozu nízké číslo. Česká je v tomto případě velmi dobře zabezpečená a snáží se ještě o větší bezpečnost, aby se počet těchto událostí snížil na nulu.

Shrnutí mimořádných událostí

V předešlých podkapitálách byly jednotlivé mimořádné události rozděleny na nebezpečné zásilky, mimořádné události způsobené klimatem, technologické poruchy a kriminatu. Nyní na obrázku 22 jsou zobrazeny podíly mimořádných událostí v regionech. Největší počet mimořádných událostí je analyzováno ve východních Čechách, které tvoří 24% z celkového počtu mimořádných událostí. Na druhém místě jsou jižní Čechy se 17 procentama. Nejméně rizikovou oblastí je severní Morava, která tvoří pouhých 9% z celkového počtu mimořádných událostí.



Obrázek 22: Celkové podíly mimořádných událostí na regionech

Zdroj: vlastní zpracování podle [9]

6 HLAVNÍ POZNATKY A DOPORUČENÍ

V této kapitole jsou uvedeny hlavní poznatky zjištěné na základě provedené analýzy vycházející z výročních zpráv a dalších informací poskytnutých Českou poštou. Po provedení analýzy byly zjištěny negativní a pozitivní výsledky auditu.

Pokles tržeb za prodej vlastních výrobků a služeb je velmi negativním zjištěním, protože když klesají tržby klesá i zisk před zdaněním. Tento problém může v budoucnosti vést i k likvidaci České pošty. Již v dnešní době se zavírají malé pobočky na malých vesničkách, kde nedochází k žádným tržbám. Celý tento problém je pravděpodobně zapříčiněn tím, že lidé přestávají využívat služby České pošty, protože jsou obklopeni elektronickým světem. Ke komunikaci mezi přáteli nebo obchodními partnery se využívají sociální sítě, emaily nebo jiná elektronická komunikace Možnou záchranou jsou elektronické objednávky zboží přes internet, které následně doručí Česká pošta.

Další negativní výsledek, který byl zjištěn při provádění auditu, je konstantní a mírně rostoucí počet pracovních úrazů, což je pravděpodobně zapříčiněno nízkým počtem školením. Podle informací od České pošty se školení provádí jednou ročně, což je podle názoru autorky velmi málo. Česká pošta by měla zanalyzovat oblasti, kde se nejvíce vyskytují pracovní úrazy a tam následně provést případná opatření.

Výskyt mimořádných událostí je další z problémů, které musí Česká pošta řešit. Po provedení analýzy této oblasti je zřejmé, že všechny druhy mimořádných události jsou zapříčiněny vnějšími vlivy. Česká pošta má minimální prostředky na snížení či odstranění těchto rizik. Možným opatřením mohou být protipovodňové bariéry.

Velmi pozitivním zjištěním je pokles počtu reklamací, které se týkají poškození či úbytku listovních zásilek. Pokud budou spokojeni zákaznici s poštovními služby, budou nadále využívat služby České pošty, tím by se mohly zvýšit i tržby podniku. Dalším kladný výsledek je počet trestných činů, které byly spáchaných na Českou poštu v letech 2014 až 2016. V této oblasti Česká pošta klade velký důraz na bezpečnost svých zaměstnanců a zákazníků, do budoucna by chtěla snížit počet události na nulu.

.

ZÁVĚR

Cílem bakalářské práce byl obecný popis problematiky bezpečnostního auditu. Byly vymezeny pojmy úzce spjaty s touto problematikou bezpečnosti v podniku. Dále byly podrobně popsány všechny rizika, která by se mohl vyskytnout v podnikání.

Konkrétně byl objasněn celkový management týkající se bezpečnosti a řízení rizik. Dále byly rozděleny rizika podnikání na vnitřní a vnější rizika. V poslední kapitole první části bakalářské práce byl detailně popsán bezpečnostní audit a jeho metody.

V druhé části byl proveden bezpečnostní audit na základě disponibilních údajů ve státním podniku Česká pošta. Pomocí regresní analýzy a grafů byly shledány negativa a pozitiva v podniku.

Při provádění bezpečnostního auditu byly zjištěny negativní i pozitivní výsledky. Jedním z negativních výsledků byl pokles tržeb za prodej vlastních výrobků a služeb, což znamená i pokles zisku před zdaněním. Hlavní příčinou poklesu je snížení zájmu lidí o poštovní služby, z důvodů většího zájmu komunikace před internet. Dalším negativním zjištěním byl neklesající počet pracovních úrazů, který se za uplynulých několik let skoro nezměnil. Tento problém by Česká pošta měla řešit častějšími školeními nebo více osobních ochranných pracovních pomůcek.

Velmi pozitivní zjištěním byl klesající počet reklamací, které se týkaly poškození či úbytku obsahu poštovních zásilek. Toto zjištění je pro podnik velmi dobrá zpráva, protože když budou spokojeni zákaznicí s poštovními služby, zvýší se tak i tržby.

Prvním cílem práce byl obecný popis problematiky bezpečnosti a bezpečnostního auditu podniku, který je popsán v kapitole 1. až 4. Dalším cílem byl popis vybraného podniku, který je obsažen v úvodu kapitoly 5. Vlastní analýza vybraných problémů bezpečnostního auditu je uvedena v kapitolách 5.2. Hlavní poznatky získané provedenou analýzou jsou uvedeny v kapitole 6.

POUŽITÁ LITERATURA

[1] Bezpečnostní audit. Rac [online]. [cit. 2017-04-26]. Dostupné z: http://www.rac.cz/rac/homepage.nsf/CZ/SS/$FILE/RAC%20Bezpecnostni%20audit_Datasheet_CZ_141015.pdf

[2] Bezpečnostní audit. Recourse [online]. [cit. 2017-04-26]. Dostupné z: http://www.recourse.cz/bezpecnostni_audit.htm)%C2%A8

[3] Bezpečnostní audit. Root-it [online]. [cit. 2017-04-26]. Dostupné z: http://www.root-it.cz/bezpecnostni-audit.aspx

[4] Bezpečnostní strategie (Security Strategy). *Managementmania* [online]. [cit. 2017-04-26]. Dostupné z: https://managementmania.com/cs/bezpecnostni-strategie-security-strategy

[5] CISO (Chief Information Security Officer) - Manažer informační bezpečnosti. Managementmania [online]. [cit. 2017-04-26]. Dostupné z: https://managementmania.com/cs/ciso-chief-information-security-officer-manazer-informacni-bezpecnosti

[6] CSO (Chief Security Officer). Managementmania [online]. [cit. 2017-04-26]. Dostupné z: https://managementmania.com/cs/cso-chief-security-office

[7] DVOŘÁČEK, Jiří. Audit podniku a jeho operací. Praha: C.H. Beck, 2005. C.H. Beck pro praxi. ISBN 80-717-9809-6.

[8] Informační bezpečnost. Cleverandsmart [online]. [cit. 2017-04-26]. Dostupné z: http://www.cleverandsmart.cz/informacni-bezpecnost

[9] Interní dokumenty České pošty

[10] ISO 31000 - Risk management. ISO [online]. [cit. 2017-04-26]. Dostupné z: https://www.iso.org/iso-31000-risk-management.html

[11] ISO 31000 Risk management (Řízení rizik - Principy a směrnice). Managementmania [online]. [cit. 2017-04-26]. Dostupné z: https://managementmania.com/cs/iso-31000-risk-management-rizeni-rizik-principy-a-smernice

[12] KOŽENÁ, Marcela. Podniková ekonomika: distanční opora. Vyd. 3. Pardubice: Univerzita Pardubice, 2012. ISBN 978-80-7395-482-6.

[13] KRÁLÍČEK, Vladimír a Jan MOLÍN. *Vnější a vnitřní kontrola z pohledu managementu*. Praha: Wolters Kluwer, 2014. ISBN 978-80-7478-557-3.

[14] MIMOŘÁDNÉ UDÁLOSTI. Krizport [online]. [cit. 2017-04-26]. Dostupné z: http://krizport.firebrno.cz/ohrozeni/mimoradne-udalosti#5

[15] Nedovolený obsah zásilek. *Česká pošta* [online]. [cit. 2017-04-26]. Dostupné z: https://www.ceskaposta.cz/rady-a-navody/nedovoleny-obsah-zasilek

[16] Nejběžnější systémy managementu bezpečnosti v České republice. BOZPinfo [online]. [cit. 2017-04-26]. Dostupné z: http://www.bozpinfo.cz/nejbeznejsi-systemy-managementu-bezpecnosti-v-ceske-republice

[17] Osobní ochranné pracovní prostředky (OOPP). *Ipodnikatel* [online]. [cit. 2017-04-26]. Dostupné z: http://www.ipodnikatel.cz/Bezpecnost-a-ochrana-zdravi-pri-praci/osobni-ochranne-pracovni-prostredky-oopp.html

[18] PALEČEK, Miloš. Prevence rizik. Praha: Oeconomica, 2006. ISBN 80-245-1117-7.

[19] Počítačová bezpečnost (Computer security). Managementmania [online]. [cit. 2017-04-26]. Dostupné z: https://managementmania.com/cs/pocitacova-bezpecnost

[20] Poslání a smysl auditu. Komora auditorů České republiky [online]. [cit. 2017-04-26]. Dostupné z: http://www.kacr.cz/poslani-a-smysl-auditu

[21] Požární ochrana a povinnosti podnikatele. Ipodnikatel [online]. [cit. 2017-04-26]. Dostupné z: http://www.ipodnikatel.cz/Bezpecnost-a-ochrana-zdravi-pri-praci/pozarni-ochrana-a-povinnosti-podnikatele.html

[22] Požární ochrana ve firmě. BOZPprofi [online]. [cit. 2017-04-26]. Dostupné z: https://www.bozpprofi.cz/33/pozarni-ochrana-ve-firme-uniqueidgOkE4NvrWuOKaQDKuox_Z9WivfDW8t3WQM4s2UgKwmw/

[23] Pracovní úrazy. Bozpzeman [online]. [cit. 2017-04-26]. Dostupné z: http://www.bozpzeman.cz/ke-stazeni.htm

[24] Program Bezpečný podnik slaví 20 let. BOZPinfo [online]. [cit. 2017-04-26]. Dostupné z: http://www.bozpinfo.cz/program-bezpecny-podnik-slavi-20-let

[25] ROUDNÝ, Radim a Radovan SOUŠEK. Management bezpečnosti. Pardubice: Univerzita Pardubice, 2014. ISBN 978-80-7395-864-0.

[26] Řízení bezpečnosti (Security Management). Managementmania [online]. [cit. 2017-04-26]. Dostupné z: : https://managementmania.com/cs/rizeni-bezpecnost

[27] SEILER, Milan. Bezpečnostní audit v organizaci [online]. Praha: Soukromá vysoká škola ekonomických studií, 2004 [cit. 2017-04-26]. ISBN 80-867-4420-5.

[28] 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.

[29] STRANKS, Jeremy W. *Health and safety pocket book* [online]. Boston: Butterworth-Heinemann, 2006 [cit. 2017-04-26]. ISBN 978-0-7506-6781-4.

[30] VEBER, Jaromír, Marie HŮLOVÁ a Alena PLÁŠKOVÁ. Management kvality, environmentu a bezpečnosti práce: legislativa, systémy, metody, praxe. Praha: Management Press, 2006. ISBN 80-726-1146-1.

[31] Zákon č. 262/2006 Sb. Zákony pro lidi [online]. [cit. 2017-04-26]. Dostupné z: https://www.zakonyprolidi.cz/cs/2006-262

SEZNAM PŘÍLOH

Příloha A

PŘEHLED VŠECH ÚRÁZŮ V ORGANIZACI

(za tuto stránku se chronologicky vkládají vyplněné očíslované listy Evidence v knize úrazů)

ev. číslo	datum vzniku úrazu	jméno a příjmení zraněného	druh zranění / zraněná část těla (stačí číselné kódy)	pracovní neschopnost		hospitalizace	
				od	do	od	do