Univerzita Pardubice
Fakulta ekonomicko-správní

Analýza podniku pro personální zajištění jeho vnitřní ochrany

Tereza Kubová

Bakalářská práce
2011

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: **2010/2011**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Tereza KUBOVÁ**
Osobní číslo:	**E08574**
Studijní program:	**B6208 Ekonomika a management**
Studijní obor:	**Management ochrany podniku a společnosti**
Název tématu:	**Analýza podniku pro personální zajištění jeho vnitřní ochrany**
Zadávající katedra:	**Ústav ekonomiky a managementu**

Zásady pro vypracování:

- studium literatury o vnitřní ochraně podniku a o krizovém řízení podniku,
- formulace cílů práce,
- teoretická analýza organizačních, ekonomických, bezpečnostních a dalších problémů vnitřní ochrany podniku a možných forem jejího zabezpečení,
- výzkum u zvolené organizace,
- vyhodnocení výzkumu,
- zpracování doporučení a závěrů.

Rozsah grafických prací:	-
Rozsah pracovní zprávy:	**cca 30 stran**
Forma zpracování bakalářské práce:	**tištěná/elektronická**

Seznam odborné literatury:

[1] **KÖNIGOVÁ, M. ; ZUZÁK, R. Krizové řízení podniku. 2. vydání. Praha 7 : Grada Publishing, 2009. 256 s. ISBN 978-80-247-3156-8.**

[2] **KISLINGEROVÁ, E. Podnik v časech krize : Jak se nedostat do potíží a jak se dostat z potíží: zkušenosti ze světové recese let 2007 až 2009. 1. vydání. Praha : Grada Publishing, 2009. 208 s. ISBN 978-80-247-3136-0.**

[3] **SMEJKAL, V.; RAIS, K. Řízení rizik ve frimách a jiných organizacích. 3. vydání. Praha : Grada Publishing, 2010. 360 s. ISBN 978-80-247-3051-6.**

[4] **KOCIÁNOVÁ, R. Personální činnosti a metody personální práce. 1. vydání. Praha : Grada Publishing, 2010. 224 s. ISBN 978-80-247-2497-3.**

[5] **MITROFF, I., I. Managing crises before they happen : What every executive and manager needs to know about crisis management. 1. vydání. New York : Amacom, 2000. 165 s. ISBN 0-8144-0563-0.**

Vedoucí bakalářské práce:	**doc. Ing. Josef Janošec, CSc.** Ústav ekonomiky a managementu
Datum zadání bakalářské práce:	**25. června 2010**
Termín odevzdání bakalářské práce:	**30. dubna 2011**

doc. Ing. Renáta Myšková, Ph.D.
děkanka

L.S.

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

V Pardubicích dne 12. července 2010

Prohlašuji:

Tuto práci jsem vypracovala samostatně. Veškeré literární prameny a informace, které jsem v práci využila, jsou uvedeny v seznamu použité literatury.

Byla jsem seznámen 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.

Souhlasím s prezenčním zpřístupněním své práce v univerzitní knihovně.

V Pardubicích dne 2. května 2011

Tereza Kubová

Poděkování

Touto cestou bych chtěla poděkovat doc. Ing. Josefu Janošci, CSc. za cenné rady a připomínky, které mi napomohly při psaní této bakalářské práce. Dále bych chtěla poděkovat vedoucímu pracovníkovi akciové společnosti, který se mi věnoval a poskytl potřebné dokumenty a informace k praktické části. A v neposlední řadě bych chtěla poděkovat své matce, prarodičům a příteli za podporu po celou dobu studia.

ANOTACE

Tato bakalářská práce je rozdělena na dvě základní části – teoretickou a praktickou. Teoretická část se zabývá vymezením pojmů a teoretickou analýzou organizačních, ekonomických, bezpečnostních a dalších problémů vnitřní ochrany podniku a možných forem jejího zabezpečení. Praktická část mapuje stávající situaci nejmenovaného zdravotnického zařízení na území České Republiky a na konkrétní problémy dává řešení vycházející z teoretických znalostí.

KLÍČOVÁ SLOVA

Analýza rizik, Hrozba, Mimořádná událost, Ochrana, Personál, Řízení rizik, Společnost

TITLE

Analysis of the company for the staffing its internal protection

ANNOTATION

This bachelor thesis is divided into two parts - theoretical and practical. Theoretical part deals with the terms definition, analysis of organizational, economic, security, safety and other problems in the internal protection of a company. Practical part of the thesis describes current situation of an unnamed medical facility in the Czech Republic. Itgives us concrete problem solutions based on the theoretical knowledge.

KEYWORDS

Risk analysis, threat, incident, protection, staff, risk management, company

OBSAH

ÚVOD

Téma této bakalářské práce jsem si vybrala z toho důvodu, že právě ochraně by měla být věnována velká pozornost, jelikož jakékoliv narušení z vnějšího, ale i vnitřního, prostředí může mít dopad na celý podnik – od plynulého chodu podniku až po jeho úpadek.

Analýza podniku pro personální zajištění se mi jeví jako jedna z nejvhodnějších možných metod, jak rizikům předcházet. Lidský faktor je v podniku jedním z těch nejdůležitějších, jelikož personál utváří reprezentativní stránku společnosti a může hodně ovlivnit výsledky událostí.

Analýzu konkrétního podniku jsem se rozhodla vypracovat na nejmenované zdravotnické zařízení na území České republiky, jelikož v nemocnici se narodíme, určitě ji nejedenkrát navštívíme v průběhu života, ať už dobrovolně nebo nuceně určitými podněty a bohužel většinou v nemocnici náš život také končí a nějakou tu dobu si v ní „pobudeme“ také po smrti. Právě v této organizaci by měla být velká pozornost věnována ochraně a to ve všech směrech, jelikož jde vždy o lidský život nebo faktor s lidským životem související. Dalšími důvody, proč jsem zvolila zdravotnické zařízení, jsou ne tak starý případ s tzv. „heparinovým vrahem“ a průzkum na nemocnice, dělaný jedním nejmenovaným deníkem, kde z osmi nemocnic prošli pouze dvě, které poskytují svým pacientům dostatečnou ochranu.

Práce je rozdělena do pěti základních kapitol. První část je zaměřena na vymezení základních pojmů, které s danou problematikou úzce souvisí. Druhá část se zabývá problematikou rizik, od jejich členění přes analýzu rizik až po metody jejich snižování. Třetí kapitola teoreticky znázorňuje konkrétní rizika v daném typu podniku – zdravotnickém zařízení. Předposlední část popisuje problematiku ve vybraném podniku. Je zaměřena především na reakce personálu na potencionální hrozby a vyhodnocení bezpečnostního auditu. Poslední část této práce se zabývá vyhodnocením stávající situace ve vybraném podniku, návrhy a doporučeními, které mohou být do budoucna přínosem.

Před vypracování jsem se seznámila s dostupnou literaturou, která souvisí s problematikou rizik a bezpečnosti, dále jsem se seznámila s metodickými pomůckami a provedla konzultace s odborníky, kteří se problematikou zabývají.

Ze struktury práce a jednotlivého členění kapitol vyplynuly i hlavní cíle bakalářské práce, kterými jsou:

1. Teoretický popis problematiky spojené s analýzou rizik a metodami jejich snižování.
2. Seznámení se s problematikou v konkrétním podniku.
3. Zhodnocení situace a vytvoření návrhů a doporučení ke zlepšení.

1 ZÁKLADNÍ POJMY

Tato kapitola je věnována vymezení základních pojmů, které s danou problematikou souvisí. Tyto pojmy se budou objevovat v dalších kapitolách bakalářské práce a objevují se také v odborné literatuře, která je k vytvoření této práce použita.

1.1 Aktivum

„Aktivum je všechno, co má pro subjekt hodnotu, která může být zmenšena působením hrozby.“ (Smejkal, Rais, 2010, s. 94)

Je důležité vymezit si tento pojem, jelikož může být zaměňován s pojmem, který slouží pro účetní potřeby. V účetnictví je aktivum chápáno jako majetek společnosti, který se zachycuje v účetní rozvaze na pravé straně. Náš pojem má sice podobnou definici, avšak z této definice plyne, že aktivem může být mnohem víc, než jen majetek společnosti. Rozdíl mezi účetním aktivem a aktivem, který slouží v předmětu rizikologie je patrný při definování následujících pojmů – objekty, procesy, osoby. Tyto pojmy se dají chápat jako podmnožina aktiva.

1.1.1 Objekty

Objekt je definován jako: „ucelený a vymezený technický, ekonomický nebo jiný systém tvořený prvky hmotné a/nebo nehmotné povahy“. (Tichý, 2006, s. XIII) Ve stejné knize je na objekt nahlíženo jako na pevný, v čase neměnný. V analýze rizika může být objektem:

- technický objekt (např. silnice),
- organizační objekt (např. podnik X),
- provozní objekt (např. strojní vybavení),
- biologický objekt (např. vlastní tělo). (Tichý, 2006, s. 5)

1.1.2 Proces

Proces je definován jako: „souhrn činností nebo skutečností probíhajících v čase; na proces můžeme hledět jako na objekt v čase“. (Tichý, 2006, s. XIII) Jelikož se procesy, oproti objektu, v čase mění, musíme rozlišovat procesy stacionární a nestacionární. U stacionárního procesu je povaha vlastností na čase nezávislá, můžeme to chápat tak, že na konci procesu je daná vlastnost stejná jako na jeho začátku.

U nestacionárních procesů je zřejmé, že tomu bude naopak - během procesu se vlastnosti mění. V analýze rizika může být procesem:

- technický proces (např. doprava),
- organizační proces (např. řízení podniku X),
- provozní proces (např. rekonstrukce),
- biologický proces (např. vlastní život). (Tichý, 2006, s. 5-6)

Pojem může být shrnut do následující jednoduché definice: „Řada na sebe navazujících výkonů, které mají konkrétní vstupy a výstupy.“ (Škrla, Škrlová, 2008, s. 17)

1.1.3 Osoby

Osoba je chápána jako: „obecné označení pro jednotlivce, skupinu lidí, organizaci, fyzickou osobu – podnikatele, právnickou osobu apod.“. (Tichý, 2006, s. XIII)

1.2 Hrozba

Hrozba je definována jako: „Jakýkoliv fenomén, který má potenciální schopnost poškodit chráněné zájmy objektu. Míra hrozby je dána velikostí možné škody a časovou vzdáleností (vyjádřenou obvykle pravděpodobností čili rizikem) možného uplatnění této hrozby.“ Hrozba je na počátku nežádoucího jevu a existuje nezávisle na ohroženém aktivu. (Roudný, Linhart, 2007, s. 8)

Tento pojem má mnoho definic, které se liší vždy jen ve formulaci slov, nebo jejich uspořádání, ale podstata zůstává téměř vždy stejná. Jako další příklad si můžeme uvést obdobnou definici, která však oproti předchozí poukazuje na konkrétní příklady. „Hrozba je síla, událost, aktivita nebo osoba, která má nežádoucí vliv na bezpečnost nebo může způsobit škodu. Hrozbou může být například požár, přírodní katastrofa, krádež zařízení, získání přístupu k informacím neoprávněnou osobou, chyba obsluhy, ale i kontrola finančního úřadu nebo růst kurzu české koruny k evropské měně apod.“ (Smejkal, Rais, 2010, s. 95)

1.3 Riziko

Pojem riziko nemá jednoznačnou definici, každý na tento pojem nahlíží jinak. Často však bývá význam rizika zaměňován s hrozbou. Pro lepší pochopení bude uvedeno několik různých definic.

Za riziko může být považována:

- „Pravděpodobnost či možnost vzniku ztráty, obecně nezdaru.
- Variabilita možných výsledku nebo nejistota jejich dosažení.
- Odchýlení skutečných od očekávaných výsledků.
- Pravděpodobnost jakéhokoliv výsledku, odlišného od výsledku očekávaného.
- Situace, kdy kvantitativní rozsah určitého jevu podléhá jistému rozdělení pravděpodobnosti.
- Nebezpečí negativní odchylky od cíle (tzv. čisté riziko).
- Nebezpečí chybného rozhodnutí.
- Možnost vzniku ztráty nebo zisku (tzv. spekulativní riziko).
- Neurčitost spojená s vývojem hodnoty aktiva (tzv. investiční riziko).
- Střední hodnota ztrátové funkce.
- Možnost, že specifická hrozba využije specifickou zranitelnost systému.“ (Smejkal, Rais, 2010, s. 90)

Další definicí může být riziko chápáno jako: „pravděpodobná hodnota ztráty vzniklé nositeli, popř. příjemci rizika realizací scénáře nebezpečí, vyjádřená v peněžních nebo jiných jednotkách“. (Tichý, 2006, s. 16) Pro naši potřebu nám poslouží následující definice: „Riziko vyjadřuje míru budoucího ohrožení objektu, respektive aktiva hrozbami, které vede ke škodám.“ (Roudný, Linhart, 2007, s. 10) Riziku bude blíže věnována druhá kapitola.

1.4 Krize

V předešlém textu bylo vysvětleno, co je to aktivum, hrozba a riziko. Pro lepší pochopení souvislostí těchto pojmů je vysvětlen i pojem krize. Pokud máme nějaké aktivum, na aktivum působí hrozba, která má určitou pravděpodobnost nastat (riziko) a hrozba skutečně nastane, můžeme říci, že se dostáváme do fáze krize.

„Krize je situace, v níž je významným způsobem narušena rovnováha mezi základními charakteristikami systému (narušeno je poslání, filosofie, hodnoty, cíle, styl fungování systému) na jedné straně a postojem okolního prostředí k danému systému na straně druhé.“ (Roudný, Linhart, 2005, s. 7) Dalším možným pochopením pojmu může být následující definice. „Krizí firmy obvykle rozumíme situace ve firmě, které trvale nebo

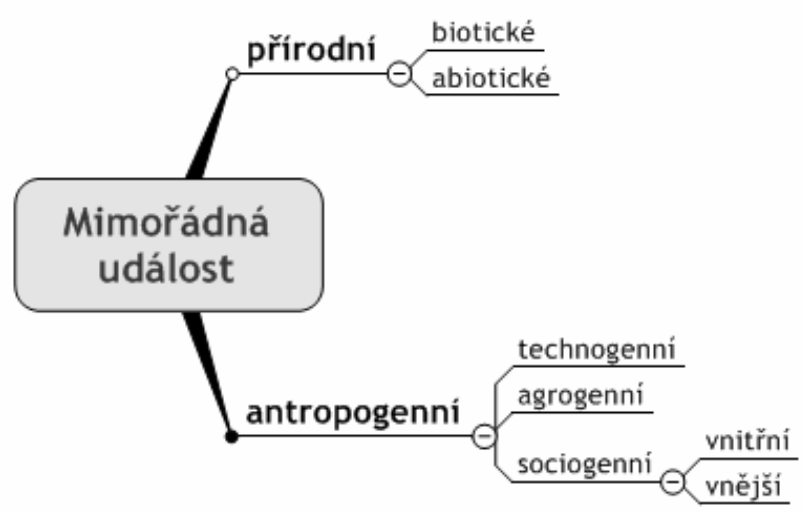
po delší dobu představují negativní odchylku normálního stavu. Ve vztahu k firmě se krize vyznačují dvěma znaky, a to:

1. krize závažné – ohrožují samostatnou existenci firmy,
2. krize méně závažné – dlouhodobě ohrožují základní cíl(e) firmy.“ (Smejkal, Rais, 2010, s. 27)

1.5 Mimořádná událost

Pro doplnění pojmů si uvedeme pojem mimořádná událost, který může být chápán obdobně jako pojem krize, nicméně mimořádná událost má mnohem větší dopad na okolí. „Mimořádné události jsou takové nepříznivé stavy, které vzniknou nechtěně, vždy mají pouze negativní výsledek.“ (Roudný, Linhart, 2005, s. 11)

Viníky mimořádných událostí jsou většinou lidé. Otázkou však zůstává, kdy se jedná o krizi a kdy o mimořádnou událost. V užším smyslu jsou mimořádnou událostí ty události, které osoba nedokáže vyřešit běžnými prostředky a musí je řešit integrovaný záchranný systém a další vnější systémy. Mimořádné události se člení na přírodní, antropogenní a smíšené. (Roudný, Linhart, 2005, s. 11-12) Následující obrázek ukazuje další podrobnější členění mimořádných událostí.

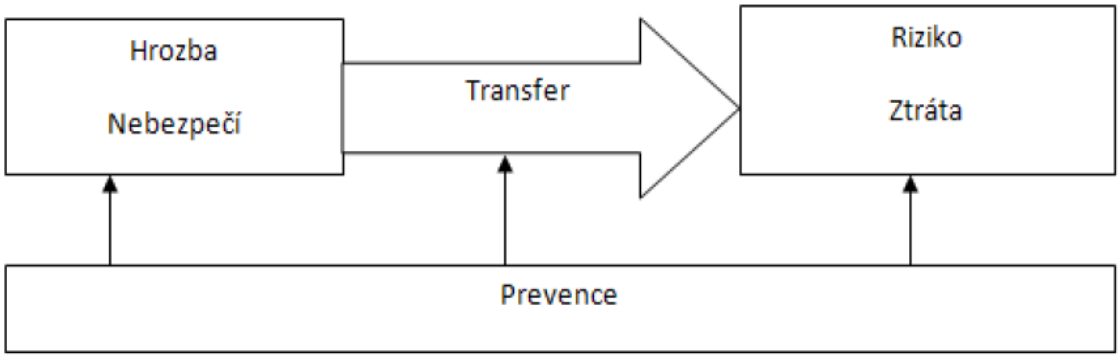


Obrázek 1 – 1: Dělení mimořádných událostí
Zdroj: (VEVERKA, 2003, s. 67)

1.6 Škoda a újma

Škoda je definována jako: „majetková újma vyjádřena obvykle v peněžních jednotkách“. (Tichý, 2006, s. XIV) Pod stejným významem může být vyjádřena také újma, která je definována obdobně jako škoda, jen s tím rozdílem, že se nejedná o majetkovou újmu, nýbrž o poškození osoby. „Újma je souhrnný výraz pro hmotné, fyzické, majetkové, zdravotní nebo jiné poškození Osoby.“ (Tichý, 2006, s. XIV)

V publikacích bývají tyto pojmy označovány také jako ztráta. Ztrátu rozeznáváme na objektu (tj. skutečně vzniklou ztrátu) a vlastní ztrátu (tj. ztráta, která vznikne po odečtu jištění v podobě např. pojištění.) Z následujícího obrázku je patrná posloupnost předpokládaných nežádoucích jevů, vedoucí od hrozby ke ztrátě.



Obrázek 1 – 2: Schéma vzniku rizika
Zdroj: (ROUDNÝ, LINHART, 2007, s. 7)

2 RIZIKO

Tato kapitola je podrobně věnována veškeré problematice s rizikem související, ať už se jedná o analýzu rizik, klasifikaci rizik, řízení rizik či rozhodování za rizika. Nejprve se však podíváme do historie rizika a v dalších kapitolách postupně přejdeme do dnešní doby, kdy je riziku věnována větší pozornost a tato problematika je lépe zpracována.

2.1 Historie

Historický výraz „riziko“ pochází údajně ze 17. století, který se objevil v souvislosti s lodní plavbou. Tento výraz je původem z italštiny („risico“) a bylo jím označováno úskalí, kterému se musela posádka při plavbě vyhnout. Následně bylo tímto pojmem vyjadřováno „vystavení nepříznivým okolnostem“. Dříve byl tento pojem v encyklopediích vysvětlován jako odvaha nebo nebezpečí. Až později se pod tímto pojmem zvažuje možná ztráta. Dnes se rizikem rozumí nějaké nebezpečí vzniku ztráty či poškození a udává se jím pravděpodobnost. (Smejkal, Rais, 2010, s. 90)

2.2 Třídění rizik

Jelikož riziko představuje určitou pravděpodobnost, prakticky se nedá rozčlenit do skupin. V literatuře se však se tříděním rizik setkáváme, jedná se ale o třídění nebezpečí či hrozeb, které jsou takto tříděny z důvodu jiného pohledu na pojmy. Každý subjekt na tuto klasifikaci nahlíží z jiného úhlu, dle svých potřeb. V této kapitole budou příčiny rizik tříděny z různých hledisek.

2.2.1 Vnitřní a vnější rizika

- Vnější:

Nezávisí na konání nebo nekonání osob, které jsou nebezpečí vystaveny. Jedná se například o nebezpečí hurikánu na objekt.

- Vnitřní:

Zdrojem vnitřního nebezpečí je sama osoba, na kterou nebezpečí působí. Jedná se například o poškození majetku jeho nedbalým zacházením. (Tichý, 2006, s. 133)

2.2.2 Primární a sekundární rizika

Sekundární riziko je vyvoláno určitým opatřením, které bylo přijato na snížení primárního rizika. To znamená, že subjekt byl vystaven určitému riziku, které je

primárním rizikem. Například rizikem je vstup na zahraniční trh, proto je podnikem přijato opatření, že vytvoří společný podnik se zahraničním partnerem. Tímto však dojde k dalšímu riziku spojenému s existencí odlišných podnikových kultur, což může být příčinou neúspěchu. Toto riziko je považováno za sekundární riziko. (Hnilica, Fotr, 2009, s. 17)

2.2.3 Finanční a nefinanční rizika

- Finanční:

Jedná se o rizika, která přinášejí finanční ztrátu. Toto riziko zahrnuje vztah mezi subjektem a jměním či očekáváním příjmů, o které může subjekt přijít či se jejich hodnota může snížit. Finanční riziko je převážně ovlivněno třemi faktory – subjektem, aktivy či příjmem a hrozbou.

- Nefinanční:

Nefinančnímu riziku je vystavena ta osoba, která nevlastní nic hodnotného. Tento pojem je však spekulativní, jelikož pro každého jedince má vlastnictví určitou hodnotu. (Smejkal, Rais, 2010, s. 124)

2.2.4 Statická a dynamická rizika

- Dynamická:

Tyto rizika mají příčinu vzniku ve změnách v okolí firmy, ale také ve firmě samé. Vycházejí z množiny faktorů vnějšího prostředí (politika, ekonomika, průmysl, konkurence, spotřebitelé). Změny těchto faktorů nelze obvykle ovlivňovat.

- Statická:

Příčiny těchto rizik se nacházejí mimo změny v ekonomice (např. v přírodních nebezpečích nebo nepoctivosti jednotlivců). Ztráty statického rizika zahrnují zničení majetku důsledkem nepoctivého jednání nebo selháním lidského faktoru. Statická rizika jsou obvykle díky své pravidelnosti předvídatelná. (Smejkal, Rais, 2010, s. 124-125)

2.2.5 Čistá a spekulativní rizika

- Spekulativní:

V těchto rizicích existuje jak možnost ztráty tak také možnost zisku. Typickým příkladem je podnikání nebo hazardní hra.

- Čistá:

Čisté riziko znamená pouze možnost ztráty nebo nedojde k žádné ztrátě. Typickým příkladem je vlastnictví majetku, který může být poničen nebo ztracen (např. havárií). Přesto se však může stát, že se čisté riziko stane opět rizikem spekulativním. K tomu dochází v případech, kdy je majetek nakoupen za účelem dosažení zisku v podnikání (např. nákup budovy a následné její pronajímání). (Smejkal, Rais, 2010, s. 125)

2.2.6 Systematická a nesystematická rizika

- Systematická:

Riziko je vyvolané společnými faktory a postihuje všechny hospodářské jednotky (oblasti podnikatelské činnosti). Zdrojem jsou např. změny peněžní a rozpočtové politiky, celkové změny trhu (např. změny cen surovin a energií). Toto riziko závisí do značné míry na vývoji trhu, proto se často označuje jako riziko tržní nebo také jako riziko nediverzifikovatelné, jelikož jej nelze vzhledem ke společnému charakteru snižovat diverzifikací. Jedná se obvykle o rizika makroekonomická.

- Nesystematická:

Tato rizika jsou specifická pro jednotlivé podniky, nebo pro jejich jednotlivé aktivity. Zdrojem rizika může být mnoho různých faktorů (např. vstup nového konkurenta, odchod klíčových pracovníků aj.). Jedná se obvykle o rizika mikroekonomická. (Hnilica, Fotr, 2009, s. 16-17)

2.2.7 Rizika ovlivnitelná a neovlivnitelná

Toto členění souvisí s možností manažera (podniku) působit na příčiny jejich vzniku.

- Ovlivnitelná:

Tato rizika lze nějakým způsobem eliminovat, snížit pravděpodobnost vzniku nepříznivých situací.

- Neovlivnitelná:

U tohoto typu rizika nemáme možnost působit na jeho příčiny (např. změna kurzu, povodeň aj.), ale je možnost přijmout určitá opatření, která sníží následky. (Hnilica, Fotr, 2010, s. 17)

2.2.8 Rizika dle skupiny nebezpečí

Tato rizika se dělí účelově do skupin, kde kritériem je zdroj, ze kterého nebezpečí pochází. Rozlišuje se několik základních skupin, jež jsou zcela obecné a mohou se použít pro analýzu rizika v jakémkoliv oboru. Mohou být rovněž použita další podrobnější členění dle zaměření podniku a jeho potřeb.

- Technologická nebezpečí
  - Průmyslová, dopravní, energetická, chemická, elektrická, nukleární, elektronická, komunikační, technologická seizmicita, softwarová, internetová atd.
- Ekonomická nebezpečí
  - Platební neschopnost dlužníků a jiná rizika pohledávek, zastarávání technologií, volatilita trhů, obecné změny hodnot ve společnosti, změny kurzů cenných papírů, selhání nemovitých investic, selhání movitých investic, změny kurzů měn, kolaps peněžních ústavů, znárodnění, privatizace, nedostatek, nadvýroba atd.
- Politická nebezpečí
  - Násilné změny politického systému, občanské nepokoje, občanské iniciativy, terorizmus, demokratický vývoj, nacionalizmus, totalitní režim atd.
- Sociální nebezpečí
  - Obecná kriminalita, speciální kriminalita, podvody, nepolitická sabotáž, squatteři, vandalství, nezaměstnanost atd.
- Právní a regulační nebezpečí
  - Zákony, normy, smlouvy, advokáti a jiní právníci, soudy, rozhodci, experti řešení sporů, znalci atd.
- Klimatická nebezpečí
  - Krátkodobé povětrnostní jevy, dlouhodobá kolísání povětrnostních podmínek, změny klimatu atd.
- Geologická nebezpečí
  - Seizmicita, svahové sesuvy, sedání zemin, podzemní vody, poddolování atd.
- Ekologické nebezpečí
  - Kyselý déšť, biologické poškození, elektrické výboje, meteority atd.

- Ergonomická nebezpečí
  - Tělesně postižení lidé (jako zdroj nebezpečí), ovladatelnost mechanizmů, tělesně postižení lidé (jako příjemci nebezpečí) atd.
- Fyziologická nebezpečí
  - Výměšky živých organizmů, zdravotní stav lidí a zvířat, epidemie, pandemie atd.
- Psychologická nebezpečí
  - Ovlivnění nevědeckými teoriemi (geopatogenní zóny, homeopatie, astrologie aj.), vnímaný strach, povědomý strach, panika atd. (Tichý, 2006, s. 133-135)

Jako důkaz, že lze členění uzpůsobit dle potřeb, může být následující rozdělení, které je cílené více do hloubky. Rovněž však zůstává zachováno, že rizika se dělí účelově do skupin, kde kritériem je zdroj, ze kterého nebezpečí pochází.

- Rizika výrobní, technická a technologická – plynou z výrobků, které nemají určité technické parametry, nebo jsou vyráběny zastaralými technologiemi. Mohou být také výsledkem neúspěšného technického výzkumu a vývoje.
  - zastarávání technologie; zastarávání konstrukce a funkčnosti výrobku; zásadní inovace v technologii, použitém materiálu a výrobku; bezpečnost výroby, ekologická čistota výroby a výrobku; výrobní kapacita, úzká místa ve výrobě; údržba a havárie zařízení; vznik požáru, jehož příčinou jsou výrobní nedostatky; vývoj nových výrobků a technologií; kvalita výrobků.
- Dodavatelská a odběratelská rizika – mohou být na straně dodavatele a odběratele, nebo mohou vzniknout zásahem „vyšší moci“. Tato rizika plynou z vazby na další podnikatelské subjekty nebo konečné zákazníky. Patří sem rovněž ztráty při dopravě zboží mezi partnery.
- Informační rizika – se dělí do tří kategorií – datová, softwarová a hardwarová. Tato rizika vyplývají především ze selhání informačních systémů, zabezpečení dat a softwaru před zneužitím.
- Sociálně-pracovní rizika – převážně odrážejí jednání pracovníků jako odraz vztahu zaměstnavatel – zaměstnanec a také pohledu obyvatelstva – zákazníků na podnik.
  - lidské selhání; neodpovídající kvalifikace pracovníků; smrtelný úraz, hromadný úraz, výskyt nemoci z povolání; stávka, problémy v kolektivním vyjednávání; sabotáž pracovníka, krádež nebo poškození zařízení, ztráta informací apod.;

vztahy k zaměstnancům a odborům, nedodržování legislativy; podcenění sociální politiky podniku; zhoršení image podniku v důsledku sociální politiky; korupce; neetické jednání, lobbing, boxing, harassment; diskriminace pracovníků.

- Tržní rizika – trh se nevyvíjí tak, jak podnik předpokládal. Aktivity podniku nenašly na trhu takovou odezvu, jakou podnik očekával.
  - chování konečných zákazníků; chování distributorů; chování konkurentů; substituční výrobek na trhu.
- Politická rizika – nastávají změnou politických systémů, jejich chováním nebo jednáním lidí v důsledku nesouhlasu s politickým systémem.
  - změna politického systému ve vlastní zemi nebo v zemi obchodu; restriktivní opatření (embargo) vůči zemi obchodu; zhoršení vztahů (přerušení diplomatických styků) se zemí obchodu; teroristické akce; státní regulace; politika EU.
- Legislativní rizika – jsou důsledkem pro podnik, pokud dojde k nepříznivým změnám v legislativě ve vlastní zemi nebo v zemi obchodu. Podnikatelské subjekty se mohou snažit tato rizika zmírnit např. tím, že zavedou dovozní přirážky.
- Živelní rizika – plynou z přírodních katastrof, jako jsou např. záplavy, zemětřesení, blesky, epidemie, sucha apod.

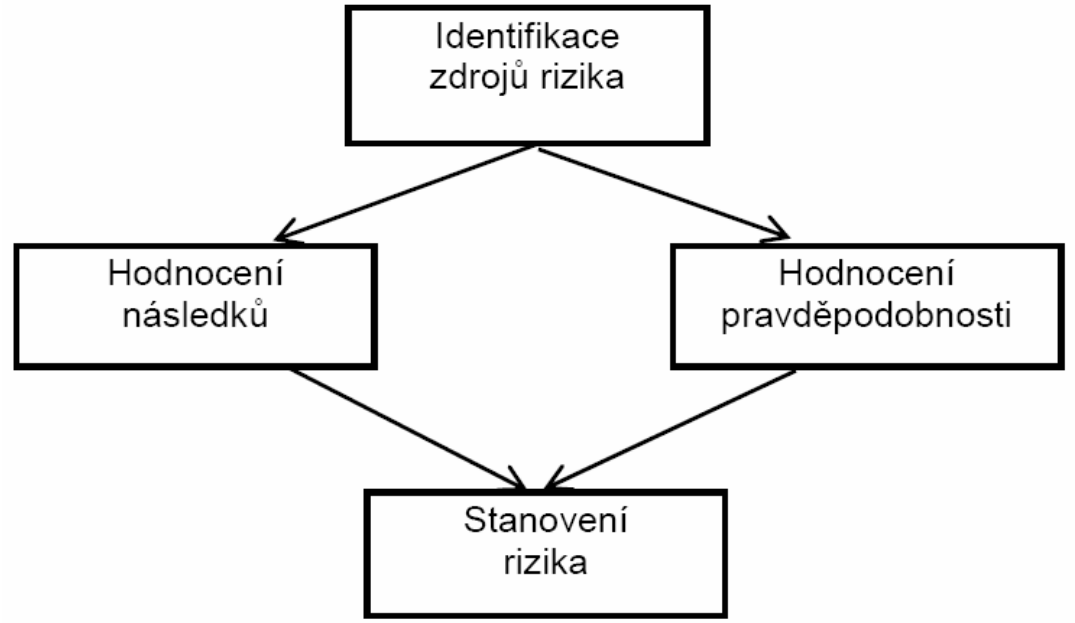
Ani jeden z uvedených výčtů není vyčerpávající a je možné jej dále doplňovat v závislosti na konkrétním podniku. Jednotlivé kategorie rizik se vzájemně prolínají a z toho důvodu lze některé typy rizik zařadit do více kategorií. (Zuzák, Königová, 2009, s. 41-46)

2.3 Analýza rizik

Analýza rizik může být vnímána jako technologie umožňující pochopit způsob působení různých nebezpečí na daný subjekt. Je to jistý poznávací proces. Žádná analýza rizik nemůže prakticky odhalit nebezpečnost zkoumaného systému, jelikož analytický výstup je vždy z části pravdivý, z části hypotetický a odvíjí se od řady faktorů. Analýza rizik je vždy založena na týmové práci a je součástí krizových a havarijních plánů. Je prvním krokem procesu snižování rizik. Druhým krokem je řízení rizik, které bude vysvětleno v další podkapitole.

„Analýza rizika je analýza člověkem vyhodnocených „netolerovatelně“ pravděpodobných hrozeb, znamenající možné ztráty na lidských životech nebo traumatologické, patogenní a psychické zdravotní následky na obyvatelstvu, ekologické a ekonomické ztráty na fauně, floře a nerostném bohatství a na dalších člověkem uznávaných hodnotách hmotného nebo duchovního charakteru zkoumaného systému.“ (Roudný, Linhart, 2007, s. 135)

Jednotlivé kroky analýzy rizika znázorňuje obrázek 2 - 1, které budou vysvětleny v následujících podkapitolách.



Obrázek 1 – 2: Schéma vzniku rizika
Zdroj: (BARTLOVÁ, BALOG, 1998)

Analýza rizik zpravidla zahrnuje tyto činnosti:

1. Identifikace aktiv – vymezení posuzovaného subjektu a popis aktiv, které vlastní;
2. Stanovení hodnoty aktiv – určení hodnoty aktiv a jejich význam pro subjekt, ohodnocení možného dopadu jejich ztráty, změny či poškození na existenci či chování subjektu;
3. Identifikace hrozeb a slabin – určení druhů událostí a akcí, které mohou ovlivnit negativně hodnotu aktiv, určení slabých míst subjektu, která mohou umožnit působení hrozeb;

4. Stanovení závažnosti hrozeb a míry zranitelnosti – určení pravděpodobnosti výskytu hrozby a míry zranitelnosti subjektu. (Smejkal, Rais, 2010, s. 94)

Identifikace aktiv

V této fázi se vyberou ta aktiva, která budou zahrnuta do analýzy a vytvoří se jejich soupis. Při rozhodování o zařazení aktiva na soupis se uvede název aktiva a jeho umístění. (Smejkal, Rais, 2010, s. 99)

Stanovení hodnoty a seskupování aktiv

Při stanovení hodnoty aktiva se obvykle vychází z nákladů, které souvisí s pořízení aktiva. Můžeme ale také zahrnout výnosové charakteristiky, pokud se jedná o aktivum, které přináší dobře identifikovatelné zisky či jiné přínosy pro podnik. Dalším zohledňujícím faktorem může být postavení na trhu, ochranná známka, know-how apod. V těchto případech je nutné rozlišit, zda posuzujeme jedinečné aktivum nebo aktivum běžně nahraditelné. Pokud tedy podnik nemůže bez daného aktiva plně fungovat a dojde k nějakým škodám, tak i tyto škody mohou být do stanovení hodnoty aktiva promítnuty. Další možností jak stanovit hodnotu aktiva je použití váženého průměru hodnot podle všech použitých hledisek.

V praxi je většinou nemožné zahrnout všechna aktiva vzhledem k velkému množství. V těchto případech se provede seskupení aktiv podle různých hledisek, aby ve skupině byla aktiva podobných vlastností (např. podle ceny, kvality, účelu apod.). Nejdůležitějšími aktivy pak jsou data, informace a znalosti, technické a programové prostředky, komunikační zařízení, listiny, personál podniku. (Smejkal, Rais, 2010, s. 99)

Identifikace hrozeb

Identifikují se ty hrozby, které připadají pro analýzu v úvahu. Vybírají se takovým způsobem, že se zvolí ty, které by mohly ohrozit alespoň jedno z aktiv subjektu. Lze vycházet ze sestavených seznamů podle literatury, vlastních zkušeností, dřívějších průzkumů apod. Každá hrozba se hodnotí vůči každému aktivu a určí se její úroveň vůči aktivu a zároveň se určí úroveň zranitelnosti aktiva vůči této hrozbě.

Při analýze hrozeb se berou v úvahu realizovaná protiopatření, která mohou snížit jak úroveň hrozby, tak úroveň zranitelnosti. Výsledným stavem je seznam dvojic „hrozba – aktivum“ se stanovenou úrovní hrozby a zranitelnosti. (Smejkal, Rais, 2010, s. 100)

Důležitou roli při identifikaci rizik také hraje to, kdo analýzu rizik provádí a jak k ní přistupuje. Každý vnímá nebezpečí jinak a to má významný vliv na rozhodování a chování. Hodnotitel je ovlivněn zejména již zmíněnými zkušenostmi, znalostí situace, informacemi o změnách nebezpečí, ale je ovlivněn také dalšími faktory, kterými mohou být např. věk, pohlaví, osobní situace, důvěra a spoléhání. (Tichý, 2006, s. 130-131)

Pravděpodobnost hrozby

Aby bylo možné určit pravděpodobnost, že nastane nějaká určitá hrozba, musí se nejprve určit, zda je analyzovaný jev náhodný či nikoliv a jaké jsou jeho pravděpodobnostní charakteristiky. Může nastat také situace, kdy pravděpodobnost, s níž nastane určitý jev, je podmíněna výskytem jevu jiného. (Smejkal, Rais, 2010, s. 100)

Pojem pravděpodobnost je chápán v teorii pravděpodobnosti jako veličina P, která nabývá hodnot v mezích [0, 1]. Tento pojem však častěji vyjadřuje pravděpodobnou možnost, která popisuje subjektivní názor hodnotitele nebezpečí. Pro tuto pravděpodobnou možnost se mohou použít různé stupnice např. hodnocení body od 1 do 10 apod. (Tichý, 2006, s. 20)

Při určování výše rizika vycházíme z hodnoty aktiva, jeho zranitelnosti a úrovně hrozby (Smejkal, Rais, 2010, s. 102), což také potvrzuje následující obecná rovnice znázorněná na obrázku 2 - 2, která bere v potaz vynaložená protiopatření.

$$\text{riziko} = \frac{\text{hrozba x zranitelnost}}{\text{protiopatření}} \text{ x hodnota}$$

Obrázek 2 – 2: Rovnice rizika
Zdroj: (Vlastní zpracování podle ANTUŠÁK, E., KOPECKÝ, 2002, str. 34)

2.3.1 Typy analýz

Analýza rizik může být prováděna různými metodami. Záleží vždy na uvážení hodnotitele a potřeb, ke kterým je analýza určena. Podle obecného členění existují dva základní přístupy k řešení – kvalitativní metody a kvantitativní metody. Není ale

vyloučena možnost využít v kombinaci oba přístupy. Jednotlivé metody budou podrobněji popsány níže.

Kvalitativní metody

U této metody se bere v potaz pravděpodobnost, že daná událost nastane a popisuje se, jak závažná tato událost bude. U této metody jsou rizika vyjádřena v nějakém rozsahu. Může to být rozsah bodového ohodnocení (např. <1;10>), určení pravděpodobnosti v intervalu <0;1>, nebo slovního vyjádření <malé, střední, velké> apod. Tyto metody jsou rychlejší, jednodušší, jsou ale také více subjektivní. (Smejkal, Rais, 2010, s. 108)

Hodnotitel při této metodě musí brát také v úvahu dobu trvání nebezpečí a velikost prostoru, ve kterém se může nebezpečí realizovat. Při zvyšování doby či prostoru, totiž roste i pravděpodobnost rizika. Musí se také zmapovat počet nebezpečí, kterým je objekt nebo proces vystaven, jelikož nebezpečí mohou být vzájemně závislá (dokonale nebo částečně), což znamená, že pokud je jedno nebezpečí zdrojem dalšího nebezpečí, tak se pak jedná o jedno nebezpečí. Počet nebezpečí může sloužit jako orientační veličina pro zpracovatele analýzy, která ale nemůže být výstupem analýzy. (Tichý, 2006, s. 148)

Kvantitativní metody

U této metody se rizika vypočítávají matematicky a vychází z frekvence výskytu hrozby a jejího dopadu. Metoda používá číselné ocenění v případě pravděpodobnosti vzniku události, ale také při ocenění dopadu této události. Riziko je nejčastěji vyjádřeno ve formě předpokládané ztráty ve finanční podobě. Tyto metody jsou oproti metodám kvalitativním více exaktní. Provedení těchto metod vyžaduje více času a úsilí, za to ale poskytují finanční vyjádření rizik, které je výhodnější pro lepší nakládání s riziky. Nevýhodou u této metody není jen vynaložené úsilí a čas, ale také vysoce formalizovaný postup, který může vést k tomu, že nebudou zachycena specifika posuzovaného subjektu. To může vést k vysoké zranitelnosti. Je to důsledek „zahlcení“ hodnotitele značným objemem formálně strukturovaných dat. (Smejkal, Rais, 2010, s. 109)

Jak již bylo zmíněno, analýza rizika nemusí být dělena jen z hlediska kvalitativního a kvantitativního. Dále můžeme rozdělovat např. analýzu aprioriní a aposteriorní, nebo analýzu absolutní a relativní.

Apriorní analýza

Tato analýza vychází z jevů, jež jsou zdrojem nebezpečí, a které se již v minulosti minimálně jednou vyskytly. Známe tedy povahu jevu, je to jev skutečný, není vykonstruovaný, a víme, že příslušná událost nastat může. Jev je tedy předem znám, ačkoliv nejsou přesně známy jeho vlastnosti. (Tichý, 2006, s. 121)

Aposteriorní analýza

V případě této analýzy musí rizikový inženýr pracovat s jevy a událostmi, o nichž se domnívá, že mohou nastat, aniž by někdy v minulosti nastaly. To znamená, že riziko odhaduje. (Tichý, 2006, s. 121)

Absolutní analýza

Jedná se o analýzu rizika vyšetřovaného projektu, která má sloužit ke stanovení co nejpřesnější hodnoty rizika s cílem získat podklady pro rozhodování o peněžních tocích, pro eliminaci nebezpečí a rizik, pro přenesení rizik na třetí osoby (pojištění) apod. (Tichý, 2006, s. 122)

Relativní analýza

Tato analýza slouží k porovnávání dvou nebo více projektů z hlediska jejich portfolia rizik, rozhodování o volbě projektu apod. Relativní analýza rizika se někdy také označuje jako preferenční nebo komparativní analýza. (Tichý, 2006, s. 122-123)

2.3.2 Metody analýzy rizik užívané v praxi

Tato kapitola stručně popisuje metody, které se v praxi běžně užívají. Vzhledem k tomu, že užívaných metod je mnoho, je vybráno jen pár nejznámějších metod.

Riziko s vysokým stupněm ochrany (HPR)

Jedná se o metodu, kdy je účelem dosažení maximální ochrany výrobního procesu, logistiky, administrativy, výpočetní techniky, obchodní činnosti a to tak, aby se riziko ztráty snížilo na minimum. Je využíváno všech možných technických prostředků. U nás tuto metodu užívají výhradně mezinárodní společnosti, které tento režim praktikují ve všech svých pobočkách. Statutu HPR nejlépe dosáhneme realizací nového projektu, jelikož ve starém závodě by byla nutná nákladná rekonstrukce, nebo to z technických důvodů není vždy možné.

Výchozím bodem této metody je automatická protipožární ochrana (automatická požární detekce, vnitřní a venkovní požární vodovod, hasicí přístroje apod.). Dále je zavedeno zabezpečení přístupovými právy, kdy mají přístup na pracoviště jen oprávněné osoby. Dalším důležitým krokem jsou pravidelné inspekční prohlídky pracovišť i školení zaměstnanců a jiná další bezpečnostní opatření. (Janata, 2004, s. 43-44)

Periodické inspekce a komparativní hodnocení pracovišť

Úkolem pravidelných inspekcí je zajištění veškerých nedostatků a zlepšení situace. Tyto inspekce provádějí pověření zaměstnanci, kteří by neměli být podřízeni místnímu managementu, ale vedoucímu útvaru rizikového managementu. To, to opatření zaručuje nezávislost inspektorů. Cílem prověřování je průchodnost únikových cest, dostupnost hasicích přístrojů, funkčnost a dostupnost hydrantů, funkčnost nouzového osvětlení apod. Kontrolou prochází ale také personál, zda jsou dodržovány bezpečnostní předpisy a pořádek na pracovišti. Po každé inspekci je proveden záznam se zjištěnými nedostatky a rychlost nápravy zjištěných nedostatků.

Komparativní oceňování pracovišť = rizikový audit. Hodnocení provádí jmenovaný odborník v doprovodu se členem vedení. Opět se zaznamenávají všechny zjištěné závěry. Frekvence návštěv je v průběhu 6 až 12 měsíců.

Postup:

1. Vytvoření souboru kritérií (cca 10 - 40), která budou hodnocena;
2. Přiřazení trestných bodů ke kritériím za zjištěné nedostatky. Součet trestných bodů představuje výsledné hodnocení pracoviště. (Janata, 2004, s. 44-45)

Rizikový profil společnosti

Jedná se o detailní sondu do činnosti hospodářského subjektu. Cílem je objevení základních podmínek spolehlivého chodu a komplexní identifikace nebezpečí, která spolehlivý chod mohou narušit. Postup spočívá v interwiev od členů nejvyššího managementu po střední úroveň. Diskutovány jsou předem stanovené otázky, které se týkají:

- movitého a nemovitého majetku, ostrahy, protipožární ochrany;
- analýzy výroby, zabezpečení energiemi;
- prodeje, nákupu surovin a dodávek;

- vnitropodnikové a vnější dopravy;
- odpovědnosti za výrobek;
- informačních technologií;
- personálních a právních otázek;
- finančních operací;
- možného ohrožení okolí a rizik z okolí apod.

Dále se určí maximální ztráta, kterou je společnost schopna unést bez ohrožení rozpočtu. Rizika se pak roztřídí do kategorií a sestaví do tvaru matice, kde se určuje jejich závažnost, pravděpodobnost, potenciál zábrany a stanovení priority. Výsledky jsou vyjádřeny barevně podle míry tolerance. Takto je sestaven rizikový profil společnosti, který slouží oddělení rizikového managementu. (Janata, 2004, s. 46-47)

Studie přerušení provozu

Tým specialistů určí všechny okolnosti, které mají vliv na činnost hospodářského subjektu. Z této studie plynou postupy, které se začnou realizovat ihned po zvládnutí havarijní situace. Stejně jako předchozí metoda je i tato založena na sérii interview s vedoucími pracovníky a na fyzické inspekci provozních jednotek. Důležitost připadá analýze dosavadního škodného průběhu. Výsledkem jsou scénáře havárií a postupy nápravy. (Janata, 2004, s. 47)

Metoda Monte Carlo

Jedná se o metodu založenou na využití posloupnosti náhodných nebo pseudonáhodných čísel. Tato metoda je velice flexibilní a je možno s ní řešit nejen analýzu rizika, ale také např. odhad pravděpodobnosti vzniku definované události potřebný k odhadu rizika. Metoda je samozřejmě softwarově zpracována, což umožňuje snadnější využití. (Tichý, 2006, s. 165)

U simulace Monte Carlo postupujeme podle jednotlivých kroků, kterými jsou:

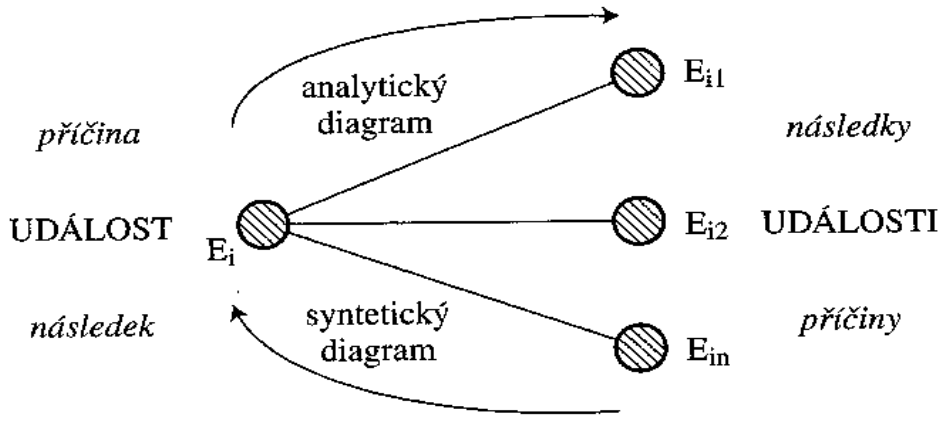
- Tvorba matematického modelu objektu analýzy rizika a zpracování jeho programu v tabulkovém procesoru.
- Určení klíčových faktorů rizika (vstupních veličin modelu), které významně ovlivňují nejistotu výstupů simulace v podobě finančních ukazatelů či kritérií. Analýza citlivosti může být užitečným nástrojem pro výběr klíčových rizikových faktorů.

- Stanoven pravděpodobnosti klíčových faktorů rizika.
- Stanovení statistické závislosti faktorů rizika. Hodnoty některých faktorů rizika mohou záviset na jiných faktorech, proto nelze tyto faktory generovat nezávisle na sobě.
- Vlastní proces simulace s využitím počítačového programu.

Výhodou této metody je, že vede k hlubšímu poznání rizikové stránky objektů a lépe podloženému rozhodování. Nevýhodou je pak značná pracnost a obtížnost. (Hnilica, Fotr, 2009, s. 71-81)

Stromové diagramy

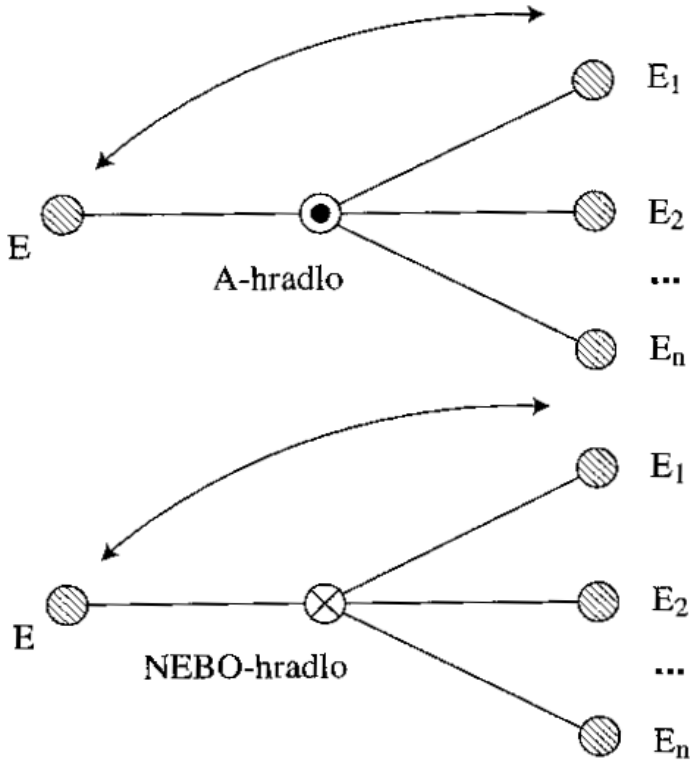
Jedná se o uspořádaný a orientovaný graf popisující vývoj událostí, někdy též nazývaný větvený graf. Může být chápán jako specifický schematický popis procesu. Uspořádání diagramu může být objektivní, subjektivní, smíšené. Stromové diagramy můžeme rozdělit do dvou základních skupin – analytické diagramy (určují, jaké následky E_i plynou z události E anebo jaké příčiny E_i vedou k události E) a syntetické diagramy (jaký následek E plyne z událostí E_i anebo jaká příčina E vede k událostem E_i). Velmi často se však typy stromových diagramů kombinují.



Obrázek 2 – 3: Události, příčiny a následky ve stromových diagramech
Zdroj: (TICHÝ, M., 2006, str. 170)

Větvení stromových diagramů znázorňuje možnosti, jakými se odvozuje několik sekundárních událostí z jedné primární, nebo možnosti, jak se odvozuje sekundární událost z několika primárních událostí. Větvení může být jak objektivní tak subjektivní, kde zpracovatel stromového diagramu vychází z minulosti (apriorní) anebo z odhadu budoucího vývoje (aposteriorní).

Některé události mohou, ale nemusí nastat současně. Nebo se může stát, že událost může nastat, pouze pokud nastane primární událost, a to buď současně, nebo jen některé. Vztahy mezi primárními a sekundárními událostmi jsou ve stromových diagramech popsány a-hradly a nebo-hradly, což znázorňuje obrázek 2 - 4. U a-hradla musí být všechny větve aktivní, kdežto u nebo-hradla každá jednotlivá větev může a nemusí nastat. (Tichý, 2006, s. 169-173)



Obrázek 2 – 4: Základní hradla ve stromových diagramech
Zdroj: (TICHÝ, 2006, str. 173)

What-if analýza

Tato analýza zkoumá pomocí brainstormingu možné neočekávané události. Umožňuje získat určitou představu o citlivosti zisku projektu na současné změny dvou a více vstupů a tím i o rizikovosti projektu. Její podstata spočívá v kombinaci hodnot vstupních veličin, které pak vytváří určitou situaci, která může v budoucnosti nastat. Tato analýza poskytuje více informací, než analýza citlivosti, což je výhodou, ale má také své nedostatky, jelikož informace neposkytují manažerům dostatečně kvantifikované a průkazné podklady, na základě kterých by se měli rozhodnout. (Hnilica, Fotr, 2009, s. 57-59)

FMEA

Jedná se o analýzu selhání a jejích dopadů, která je založená na principu modelování souvislostí popisujících vztah „příčina – důsledek“ nebo „selhání – důsledek“ způsobem odzdola nahoru kvantitativním způsobem. (Roudný, Linhart, 2007, s. 141)

Tato metoda má dvě fáze – verbální a numerickou. Verbální se zaměřuje na identifikaci možného vzniku, možných způsobů a možných následků poruch. Nejčastěji se realizuje brainstormingem, ale dá se postupovat i korespondenčně. Numerická se zaměřuje na tříparametrický odhad rizik projektu, jejichž hodnoty volí experti v rozsahu stupnice sestavené analytikem rizika (např. od 1 do 5). Při použití FMEA je také důležité z čího pohledu se bude projekt hodnotit, zda z pohledu zákazníka, organizace či veřejnosti. (Tichý, 2006, s. 183-184)

HAZOP

Jedná se o analýzu nebezpečí či ohrožení a provozuschopnosti, kde hazard je pojímán jako operace, která může vyvolat ztrátu nebo škodu. Tato metoda vychází z pravděpodobnostního hodnocení hazardů jako zdrojů rizik a jejím principem je expertní týmová práce využívající brainstormingové a brainwritingové přístupy. K identifikaci nebezpečí dochází systémem klíčových slov, která jsou kvantitativní (ne, není, více, méně) a kvalitativní (současně, stejně, částečně, naopak, jinak). Kroky této metody jsou následující:

- popis systému – vymezí se zkoumaný systém nebo činnost, ke které se vztahují hazardy;
- definují se problémy;
- popis subsystému – systém se rozčlení na jednotlivé sekce pro analytické úvahy;
- zkoumání systému;
- použití klíčových slov;
- stanovení příčin.

Po stanovení příčin se určí referenční bod a příčiny se rozdělí do skupin na lidské chyby, poruchy zařízení a vnější události. Poté je vypracován odhad dopadů např. maticí rizik, která je znázorněna pomocí tabulky 2 - 2. (Roudný, Linhart, 2007, s. 142-145)

Tabulka 2 - 1 Matice rizika HAZOP

Očekávání / Újma-škoda	Každý rok	Každou dekádu	Životnost zařízení	Dle podobného zařízení	Nepravděpodobné
Ztráta života	1	1	2	3	NP
Zranění	1	2	3	4	NP
Ztráta času	3	3	4	4	NP
Jiné škod	4	4	4	4	NP
Není to hazard	NH	NH	NH	NH	NP

1 – nepřijatelné, 2 – nežádoucí, 3 – přijatelné s kontrolou, 4 – přijatelné, NH – není to hazard, NP - nepravděpodobné

Zdroj: (ROUDNÝ, LINHART, 2007, s. 145)

Bezpečnostní audit

Jedná se o analytickou metodu postavenou na sestavení kontrolních seznamů pro systematické posuzování vybraných aspektů systému. Pomocí této metody zjišťujeme možné způsoby kontrol potenciálních nehod, problémů v provozu a systému. Používá se předem připravený seznam otázek a matice pro ohodnocení rizik. Aplikace této metody má velmi široké využití. (Roudný, Linhart, 2007, s. 146)

2.4 Řízení rizik

„Řízením rizik rozumíme takové chování, které má za cíl optimalizaci působení Osoby v prostředí, v němž se nalézá, a to jednak v přítomnosti (tj. v blízké budoucnosti), jednak v budoucnosti.“ (Tichý, 2006, s. 199)

Řízení rizik může mít však i další definici: „Řízení rizik je proces, při němž se subjekt řízení snaží zamezit působení již existujících i budoucích faktorů a navrhuje řešení, která pomáhají eliminovat účinek nežádoucích vlivů a naopak umožňují využít příležitosti působení pozitivních vlivů.“ Součástí procesu je rozhodovací proces, který vychází z analýzy rizika. Management pro řízení rizik vyvíjí, analyzuje a srovnává možná preventivní a regulační opatření, z kterých vybere ta, která riziko minimalizují.

Součástí řízení rizika je rovněž šíření informací o riziku a vnímání rizika. Finálním výsledkem řízení rizika je rozhodnutí. (Smejkal, Rais, 2010, s. 112)

Rozeznáváme řízení rizik:

- spontánní nebo intuitivní – rozhodovatel nemá definovaný postup řízení, rozhoduje se velice rychle;
- systematické nebo organizované – rozhodování podléhá předem stanovenému programu.

Můžeme se setkat s těmito výchozími strategiemi:

- ovládání rizik je soustředěno u jedné Osoby, která tento stav respektuje a dle toho se i chová;
- riziko řídí Osoba, které nebezpečí hrozí;
- riziko řídí Osoba, u níž nebezpečí vzniká;
- riziko řídí Osoba, která je schopná riziko ovládat, bez zřetele k dopadu nebo původu rizika;
- riziko neřídí nikdo. (Tichý, 2006, s. 199-200)

Základními oblastmi, kterými se řízení rizik zabývá, jsou:

- přírodní katastrofy a havárie;
- rizika ochrany životního prostředí;
- finanční rizika;
- projektová rizika;
- obchodní rizika;
- technická rizika.

2.4.1 Management podnikatelských rizik

„Management rizik (řízení rizik) je kompletní proces zjištění, kontroly, eliminace a minimalizace nejistých událostí, které mohou subjekt ovlivnit.“

Řízení rizik zahrnuje:

- výběr protiopatření,
- analýzu nákladů/přínosů,
- implementaci protiopatření,
- testování protiopatření.

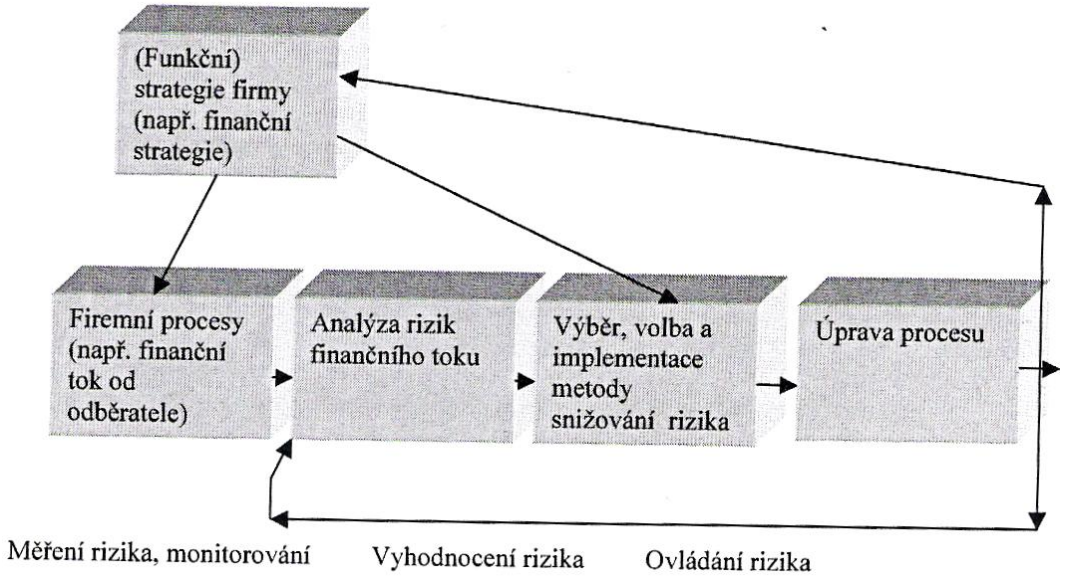
Účinného řízení rizik může být dosaženou pouze pokud:

- je jasně stanovena strategie subjektu vzhledem k jeho hlavním cílům (včetně rizikové strategie);
- funguje celý proces řízení rizik, který je podpořen vhodným informačním systémem;
- management klade důraz na řízení rizik a existují odpovědné osoby za řízení rizik;
- existuje fungující interní kultura a schopnost rozvíjet se a přizpůsobovat se novým výzvám rizik. (Smejkal, Rais, 2010, s. 115)

Je tedy nutné, aby management podniku zajišťoval zejména tyto činnosti:

- monitorování a měření rizika (vyhodnocení),
- analýzu rizika ve vnějším i vnitřním prostředí,
- určení nejvhodnější strategie pro snižování rizik,
- stanovení a implementace nejvhodnější metody snižování rizik do podmínek podniku,
- vyhodnocení uplatněné strategie v praxi.

Za provádění těchto činností nese zodpovědnost Osoba, tzv. risk management. Tento proces řízení, lze schematicky vyjádřit na následujícím obrázku 2 - 5. (Rais, 2003, s. 8)



Obrázek 2 – 5: Proces řízení rizik ve firmě
Zdroj: (RAIS, 2003, s. 8)

2.5 Přístupy ke snižování rizika

Riziko podnikatelské činnosti závisí na konání manažera, který rozhodne a postoupí určité kroky ke snížení rizika. Aktivity, které riziko snižují, můžeme rozdělit do dvou základních skupin:

- aktivity zaměřené na oslabování (eliminaci) příčin vzniku rizika (ofenzivní přístup),
- aktivity zaměřené na snižování negativních dopadů rizika (defenzivní přístup). (Szabo a kol., 2005, s. 116)

2.5.1 Diverzifikace

Spočívá ve snaze rozložit riziko na co největší základnu. Nejrozšířenějším druhem diverzifikace je rozšiřování výrobního programu, což znamená, že podnik zahrne do svého sortimentu více výrobků různé povahy, čím snižuje riziko finanční nestability při neúspěchu výrobku. Dalším typem může být např. diverzifikace geografická, která může snižovat rizika politická, kurzovní apod. (Szabo a kol., 2005, s. 117)

2.5.2 Flexibilnost

Flexibilností podniku lze dosáhnout snížení dopadu nepříznivých situací. Flexibilnost podniku výrobního charakteru lze zabezpečit vícero způsoby. Nejčastějším je volba výrobního zařízení (technologie), které není úzce specializované, ale má univerzální charakter. Další možností flexibilnosti je uplatňování různých forem pronájmu, organizační struktura, formy motivace apod. Všechny tyto a další faktory je třeba brát do úvahy při zabezpečování žádoucí míry pružnosti snižující negativní dopady podnikatelských rizik. Tato pružnost se projevuje především ve zkracování času, za který je firma schopná reagovat na změnu. (Szabo a kol., 2005, s. 119)

2.5.3 Dělení rizika

Při tomto způsobu snižování rizika se riziko rozděluje mezi dva či více účastníků, kteří se společně podílejí na podobné činnosti nebo záměru. Dělení rizika je možné dosáhnout vícero způsoby, např. strategickou aliancí, založení společného podniku apod. Výhodou založení společného podniku je, že každý účastník má takový podíl investicí na podnikatelském projektu, že ztráta v případě neúspěchu neohrozí stabilitu firmy. (Szabo a kol., 2005, s. 119)

2.5.4 Transfer rizika

Často používaným způsobem snižování rizika je transfer na jiné subjekty, např. dodavatele. Mezi nejvýznamnější formy transferu patří:

- utváření dlouhodobých kupních smluv na dodávku surovin, materiálu a polotovarů za předem dohodnutých podmínek;
- uzavírání kontraktů na prodej výrobků za předem stanovených podmínek (např. objem prodeje);
- pronájem výrobního zařízení (jiných prostředků), čímž se snižují finanční rizika spojené s vlastnictvím daného zařízení a plno dalších forem transferu rizika. (Szabo a kol., 2005, s. 120)

2.5.5 Pojištění

Podstatou pojištění je z hlediska teorie směna rizika velké ztráty za jistotu malé ztráty. Tím se rizika přenesou na pojišťovnu, která kryje škody. Pojištění je alternativou k vytváření vlastních rezerv pro budoucí nežádoucí události. Nevýhodou, o které se moc nemluví, může být to, že pojišťovny mají snahu o stanovení pojistných podmínek tak, aby v případě vysokých dopadů bylo možné výši pojistného plnění snížit, či plnění zcela vyloučit. (Smejkal, Rais, 2010, s. 157-159)

2.6 Personální zajištění rizik

Existuje veliká škála rizik, která je potřeba zabezpečit různými možnými způsoby. V některých případech je zabezpečení možné pomocí techniky, většinou je ale potřeba lidského faktoru. Existují tři základní typy, jak zabezpečit rizika pomocí lidského faktoru. Podnik na zabezpečení konkrétního rizika může:

- najmout externí společnost, která se zabývá ochranou objektů (nejedná se o přímý personál podniku);
- přijmout nového zaměstnance do pracovního poměru na pracovní pozici, jejíž náplní je pouze zajištění daného rizika;
- proškolit současného zaměstnance, který bude prevenci rizik provádět při své stávající náplni práce.

Pro každé konkrétní riziko se nejlépe hodí různé typy zajištění. V některých případech se může jednat i o kombinaci typů zajištění.

3 RIZIKA VE ZDRAVOTNICKÝCH ZAŘÍZENÍCH

Tato kapitola popisuje veškeré činnosti související s řízením rizik, které jsou aplikované na specifický typ zařízení, kterým je zdravotnické zařízení. Přes tuto kapitolu se přeneseme na konkrétní zdravotnický podnik.

Vstup České republiky do Evropské unie přinesl zvyšování požadavků na kvalitu a bezpečnost péče, čímž se mění postoj vrcholového managementu k akreditaci SAK ČR (Spojená akreditační komise ČR) nebo k certifikaci ISO 9001:2000. Každý ředitel zdravotnického zařízení chápe důležitost funkce manažera kvality, avšak funkce manažera rizik mu může připadat jako zbytečný a nepotřebný luxus. Tento pohled se však mění s příchodem nějaké neočekávané události, která má za následek negativní dopad.

V menších zdravotnických zařízeních se dají důležité funkce sloučit a řízení kvality může jít „ruku v ruce“ s bezpečnostní péčí. U velkých zařízení je však nutné, aby řízení rizik vedl manažer rizik samostatně.

3.1 Standardy a normy

Tato kapitole se věnuje standardům, normám a zákonům, které je pro bezpečnost v nemocnici nutné dodržovat.

Spojená komise pro akreditaci zdravotnických zařízení (JCAHO) udává globální standardy kvality a bezpečnosti péče. Tato organizace v roce 2002 začlenila do svých standardů požadavek na kontinuální vyhodnocování rizik a procesů ve zdravotnických zařízeních. Většina akreditačních standardů od této organizace se dotýká bezpečí pacientů. Komise vytvořila také efektivní nástroj „Sential Event Alert“, s jehož pomocí lze předejít mimořádným událostem jako např. medikační pochybení, záměna pacienta, stranová záměna při operaci nebo nozokomialní infekce a dalších cca 40 mimořádných událostí v klinické oblasti s fatálními následky.

Stejně jako předchozí komise funguje i již jednou zmiňovaná Spojená akreditační komise České republiky – SAK ČR. Specifické standardy této organizace se zaměřují na rizika medikačního procesu, nozokomiální infekce, na pozitivní identifikaci pacienta, zdravotnickou dokumentaci, ale také na likvidaci odpadů nebo stravovací provoz. Tato organizace má jasně stanovené indikátory k vyhodnocení plnění jednotlivých standardů,

a pokud se zdravotnické zařízení rozhodne použít těchto indikátorů jako kritérií auditů, musí v souladu splnit 50 akreditačních standardů.

Jedním ze systémů řízení kvality je ISO 9001:2000, které obsahuje procesní řízení, zaměření na zákazníka a zaměstnance, dokumentace a kontinuální zvyšování kvality. Cílem je dosažení trvalé shody mezi požadavkem na produkt a produktem. (Škrla, Škrlová, 2008, s. 25-29)

3.2 Role manažera rizik

Manažer rizik řídí složitý proces, který má za úkol kontrolovat a tvořit zabezpečení před celou škálou rizik ve zdravotnickém zařízení, která mohou mít za následek poškození majetku nebo pověsti zdravotnického zařízení, poškození zdraví pacientů, zaměstnanců nebo návštěv, což je ta horší z variant, jelikož se jedná o lidský život. Manažer rizik tedy odpovídá za přípravu řady hlášení a statistických přehledů tzn. za to, že ve zdravotnickém zařízení všichni zaměstnanci akutně vnímají skutečná i potencionální rizika a snaží se je minimalizovat. Manažer rizik by měl motivovat k bezpečnější práci, poskytování bezpečnější léčebné péči, ošetřovatelské péči. Z toho vyplývá, že by měl mít manažer přirozenou autoritu, jelikož právě on vede zaměstnance k tomu, aby se v zájmu budování bezpečnější nemocnice chovali a mysleli jinak. Jeho další povinností je také každodenní dohled nad plněním závazných předpisů a zákonů týkajících se bezpečnosti práce a ochrany zdraví zaměstnanců. Dále koordinuje aktivity spojené s výskytem mimořádných událostí, nozokomiálních infekcí, incidentů, kriminality a pochybení. Vše musí být pečlivě dokumentováno. Pokud je ve zdravotnickém zařízení manažer rizik i manažer kvality, je nutné, aby své aktivity zkoordinovali a vzájemně spolupracovali s vrcholovým managementem. (Škrla, Škrlová, 2008, s. 21–24)

3.3 Rizika z perspektivy lékařů

Jelikož média věnují stále větší pozornost problematice pochybení lékařů a rizikům, která pacient při hospitalizaci postupuje, je potřeba se věnovat řízení rizik i tohoto typu. Může dojít k:

- chybám ve zdravotnické dokumentaci a nečitelnosti zápisů;
- medikačnímu pochybení;
- podceňování nebo trivializování programu kontinuálního zvyšování kvality;
- nedostatečnému sledování nebo podceňování nozokomiálních infekcí;

- vědomému zakrývání pochybení na oddělení;
- nezdravé organizační kultuře na oddělení;
- velké variabilitě v práci jednotlivých lékařů;
- práci lékaře pod vlivem alkoholu;
- nedostatku respektu k pacientovi a jeho lidské důstojnosti;
- praktikám non lege artis;
- nedbalosti.

Vztah mezi lékařem a pacientem je podmínkou radikálního snížení rizika soudních sporů vyvolaných nespokojenými nebo poškozenými pacienty. Řada lékařů však uplatňuje paternalistický vztah oproti partnerskému, nebo jsou lékaři časově zaneprázdněni. (Škrla, Škrlová, 2008, s. 41)

3.4 Rizika z perspektivy ošetřovatelského personálu

Sestry představují nejpočetnější skupinu zaměstnanců ve zdravotnictví. Proto je potřeba věnovat velikou pozornost na rizika v souvislosti s léčebnou péčí ze strany ošetřovatelského personálu. Může dojít k pochybení a omylům ošetřovatelského personálu z důvodu:

- nedostatečné orientace nových sester;
- nedostatečné nebo nevhodné komunikace;
- nedostatečné informovanosti sester;
- nedostatečným dohledem;
- nezajištění bezpečí pacienta;
- nepozornosti v důsledku narušení soustředěnosti;
- neposkytnutí důležité péče včas;
- provádění procedur bez dostatečné znalosti.

S rostoucím počtem pacientů se zvyšuje procento pochybení sester, což může být způsobeno únavou, či počtem odpracovaných přesčasových hodin. (Škrla, Škrlová, 2008, s. 46)

3.5 Hlášení mimořádných událostí a prevence

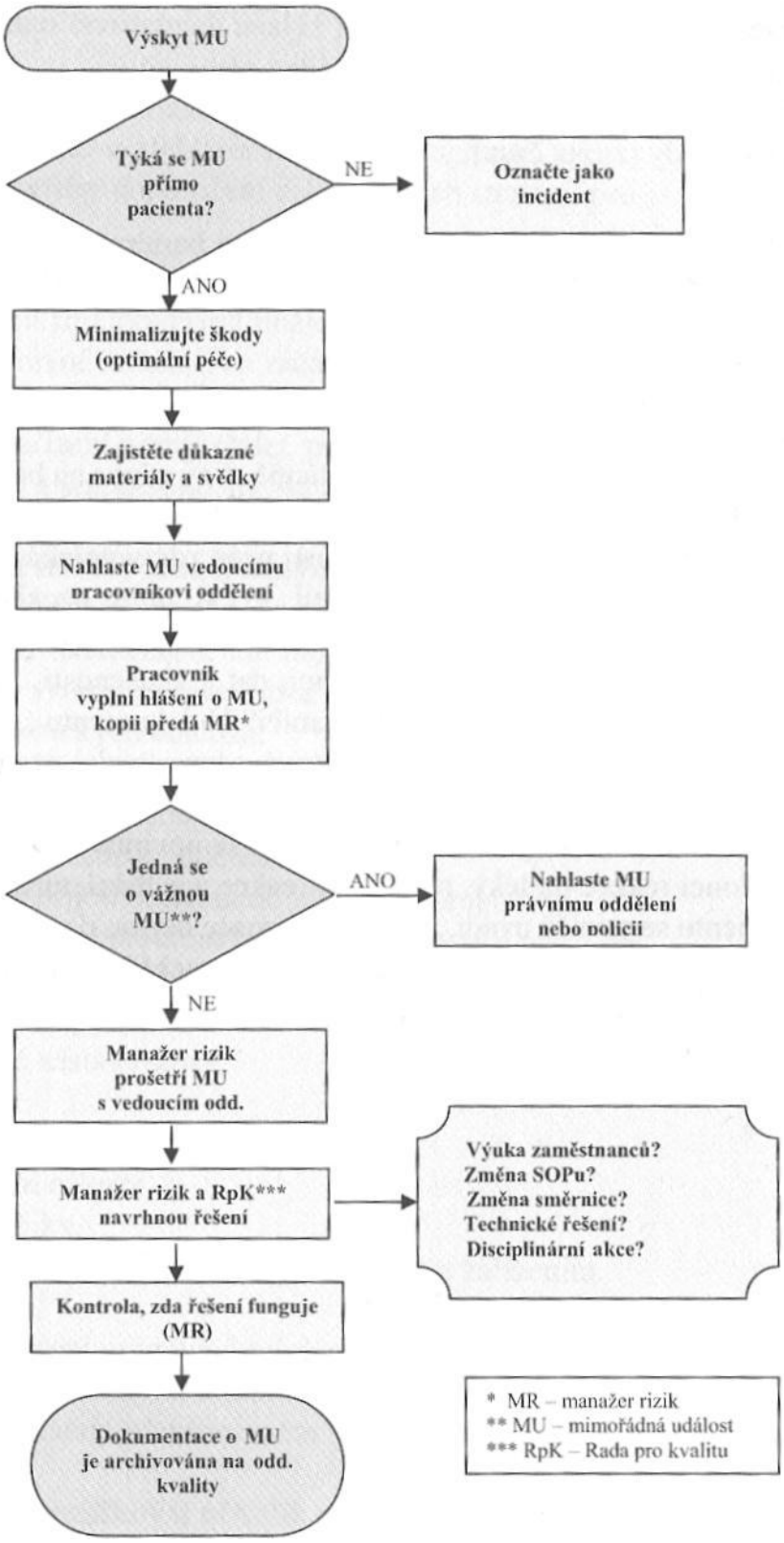
Hlášení mimořádných událostí je důležité zejména pro monitorování mimořádných událostí, kdy se dají snadněji rozpoznat opakující se problémy, které by mohly ovlivnit kvalitu a bezpečí poskytované péče. Dalším odůvodněním pro nutnost hlášení mimořádných událostí je včasná možnost vyhodnocení situace v možném případě soudního sporu. Systém hlášení osobních pochybení má však závažné nedostatky, a to především ze strachu z potrestání, obav z možného soudního postihu, hrdosti, nedostatku času na administrativní práci.

Řada českých zdravotnických zařízení se snaží některé typy mimořádných událostí sledovat, ale ve většině případů se střetávají s negativním postojem zdravotníků. V důsledku toho se debatuje na téma, zda by nebyla vhodnější strategie „anonymního" či „důvěrného" hlášení. Výsledné rozhodnutí je pak na manažerovi zdravotnického zařízení. Pokud však bude manažer vidět hlavní příčinu pochybení v lidech a dle jeho názoru bude nejlepším řešením jak chybám předejít rychlé a rázné disciplinární řízení, pak se dostaví ze strany zaměstnanců obavy a začnou omyly maskovat a zakrývat.

Proces hlášení a řešení mimořádných událostí si každé zdravotnické zařízení nastavuje samo. Formulář hlášení by však měl obsahovat následující údaje:

- identifikaci poškozeného pacienta/zaměstnance/návštěvníka a jeho osobní data,
- charakter události, rozsah a charakter škod/poranění,
- popis události, údaje založené na faktech,
- jméno svědka/svědků, jejich bydliště (nebo zaměstnancovo identifikační číslo a podpis),
- informaci o tom, zda a kdy byl o mimořádné události informován lékař,
- záznam o poskytnutí první pomoci,
- klasifikace mimořádné události,
- připomínky. (Škrla, Škrlová, 2008, s. 48-54)

Následující schéma znázorňuje proces hlášení mimořádných událostí.



Obrázek 3 – 1: Vývojový diagram procesu hlášení mimořádných událostí
Zdroj: (ŠKRLA, ŠKRLOVÁ, 2008, s. 58)

4 VYBRANÉ ZDRAVOTNICKÉ ZAŘÍZENÍ

Představitelé organizace podmínili poskytovat informace pro bakalářskou práci pod podmínkou, že jejich skutečná identita nebude zveřejněna. Vybraná organizace hodnocená v bakalářské práci je zapsána v obchodním rejstříku jako akciová společnost. Společnost je zdravotnickým zařízením s vlastní právní subjektivitou, vystupuje v právních vztazích svým jménem a nese odpovědnost z těchto vztahů vyplývající.

4.1 Představení organizace

Hlavním řídícím dokumentem je Organizační řád společnosti. V něm jsou vymezeny základní aktivity, které charakterizují společnost:

- Poskytuje ambulantní a lůžkovou základní, specializovanou a superspecializovanou zdravotní diagnostickou a léčebně preventivní péči, v rozsahu stanoveném příslušnými předpisy, smlouvami s jednotlivými zdravotními pojišťovnami a jinými plátci zdravotní péče.
- Je povinna zabezpečovat poskytování zdravotnických služeb i obyvatelům mimo vlastní spádovou oblast v rámci svobodné volby lékaře a zdravotnického zařízení, zvláště pak v oblasti poskytování neodkladné péče.
- Provozuje specializovanou knihovnu. Sítě veřejných knihovnických a informačních služeb ve zdravotnictví ve smyslu knihovního zákona. Lékařská knihovna poskytuje služby především odborníkům ze společnosti, studentům a zdravotnické veřejnosti kraje.
- Poskytuje připojení k národní vědecké síti (NREN) CESNET2 organizacím, splňujícím předepsané podmínky.
- V rozsahu stanoveném právními předpisy a pokyny Ministerstva zdravotnictví ČR (dále jen MZ ČR) a v souladu s vnitřními potřebami společnosti jako akreditované pracoviště dle zákona č. 95/2004 Sb. poskytuje další vzdělávání lékařů, farmaceutů a jiných odborných pracovníků.
- Na základě akreditací České lékařské komory na školících pracovištích v systému celoživotního vzdělávání lékařů poskytuje vzdělávací služby s nadregionální působností a je centrem celoživotního vzdělávání lékařů kraje.

- Je pověřeným pracovištěm České stomatologické komory pro praktickou výuku v systému celoživotního vzdělávání stomatologů s regionální působností.
- Je vzdělávacím pracovištěm Národního centra ošetřovatelství a nelékařských zdravotnických oborů (NCONZO) zřízeným za účelem zajištění celoživotního vzdělávání nelékařských profesí ve zdravotnictví s nadregionální působností a je centrem celoživotního vzdělávání nelékařských profesí ve zdravotnictví kraje.
- Realizuje dlouhodobé kvalifikační a certifikované kurzy pro výkon vybraných povolání ve zdravotnictví s celorepublikovou působností, akreditované MZ ČR dle zákona č. 96/2004 Sb. Společnost realizuje praktické stáže v rámci specializačního vzdělávání nelékařů na pracovištích akreditovaných MZ ČR dle zákona č. 96/2004 Sb.
- Zajišťuje od profesních sdružení vydávajících souhlasné stanovisko dle vyhlášky č. 321/2008 Sb. Kreditní systém, přidělení kreditních bodů pro všechny školicí akce.
- Spolupracuje s místní Univerzitou – zajišťuje externí vyučující a je odborným garantem vybraných oborů vysokoškolského studia, zčásti realizovaného ve výukových prostorách společnosti. Umožňuje konání a odborně zajišťuje praktickou výuku studentů.
- Spolupracuje s lékařskými, zdravotnickými a dalšími fakultami vysokých škol, umožňuje konání a odborně zajišťuje praktickou výuku studentů lékařství, ošetřovatelství a dalších oborů ve svých prostorách. Zajišťuje výuku mediků 6. ročníků lékařských fakult.
- Je spolupracujícím pracovištěm Institutu postgraduálního vzdělávání ve zdravotnictví Praha pro oblast vzdělávání ve zdravotnictví.
- Spolupracuje se středními a vyššími zdravotnickými školami. Umožňuje konání a odborně zajišťuje praktickou výuku studentů ve svých prostorách, a to pro získání odborné způsobilosti v oborech dle zákona č. 96/2004 Sb.
- Plní podle zvláštních předpisů a směrnic úkoly spojené s ochranou státního, hospodářského a služebního tajemství a s přípravami zdravotnictví k obraně státu.
- Realizuje vědeckovýzkumnou činnost ve zdravotnictví, řeší klinické studie a projekty na základě grantů získaných na národní a mezinárodní úrovni.
- Zajišťuje činnost pro Národní onkologický registr.

- Zajišťuje superspecializovanou péči v Kardiovaskulárním centru druhého stupně, Traumatologickém centru pro dospělé, Traumatologickém centru pro děti, Komplexním onkologickém centru, Cerebrovaskulárním centru prvního a druhého stupně.
- Zajišťuje činnost Znaleckého ústavu soudního lékařství.

Svou praktickou činností usilují o dodržování jednotných standardů poskytované zdravotní péče a dalších služeb v celé akciové společnosti a budují špičková zdravotnická centra prosazující se i v mezinárodní konkurenci. Chtějí být nejen velkým, ale i vyhledávaným zaměstnavatelem, který umožňuje kontinuální rozšiřování znalostí a dovedností svých pracovníků.

Mají zpracovanou strategii, v níž usilují o:

- orientaci na zákazníka,
- vůdčí úlohu ve zdravotnictví v kraji, přesahující do širšího regionu,
- univerzitní nemocnici součástí společnosti,
- finanční stabilitu,
- jednotnou firemní kulturu při zachování vnitřní soutěživosti.

4.2 Bezpečnostní dokumentace společnosti

Představiteli mi byly poskytnuty důležité výchozí bezpečnostní dokumenty:

- Směrnice o neshodách a mimořádných událostech,
- Trendová analýza mimořádných událostí,
- Dílčí zpráva z bezpečnostního auditu.

Z těchto informačních zdrojů vychází popis systému ve sledované společnosti. Základním přístupem je vznik mimořádné události a postup jejího řešení. Tomu je věnována vypracovaná dokumentace.

4.3 Hlášení mimořádných událostí

Systém hlášení mimořádných událostí společnosti vychází ze směrnice o neshodách a mimořádných událostech.

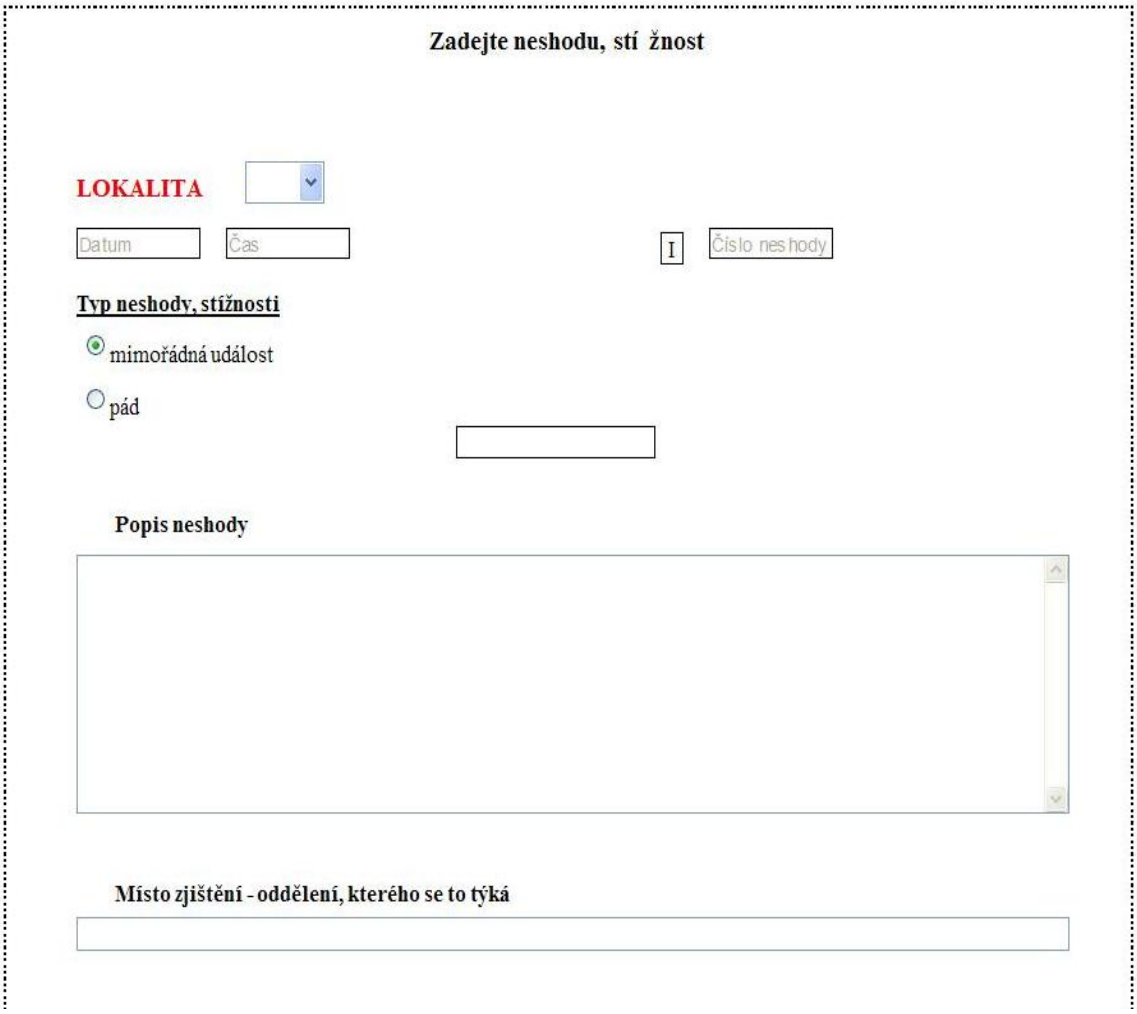
4.3.1 Odpovědnosti a pravomoci

Povinnost nahlásit neshodu (mimořádnou událost) má každý pracovník společnosti, který neshodu zjistí. Pokud se jedná o neshodu týkající se organizační jednotky

zaměstnance nebo tato neshoda má dopad na provoz této organizační jednotky, zaměstnanec informuje současně svého nadřízeného pracovníka. Garantem vypořádání neshody v určité oblasti je vždy vlastník procesu. Za dodržování směrnice je zodpovědný vedoucí pracovník v rámci svého organizačního útvaru.

4.3.2 Systém hlášení

Neshody a mimořádné události jsou hlášeny prostřednictvím aplikace, která je na intranetu společnosti. Některé případy jako interní audity, zápisy z porad, dotazníky spokojenosti apod. lze při výskytu neshody ohlásit jinou písemnou formou. Vyplňují se informace týkající se lokality, o jaký typ neshody se jedná a její popis a místo zjištění, popř. další specifika a vše se odešle procesnímu specialistovi, který hlášení vyhodnotí a určí následné zpracování. Ukázka formuláře je znázorněna na následujícím obrázku.



Obrázek 4 – 1: Formulář o hlášení neshody
Zdroj: Směrnice o hlášení mimořádných událostí

Systémem lze nahlásit cokoliv, existuje však seznam okruhů tzv. povinně hlášených mimořádných událostí, který může být na žádost vlastníka procesu doplněn. Vzhledem k nutnosti monitorovat mimořádné události a včas na ně reagovat z důvodu omezení následků či zamezení opětovnému výskytu, je stanovena povinnost hlásit bez zbytečné časové prodlevy každou následující mimořádnou událost:

- Bezpečnostní incident;
- Hrozba medializací, soudem, trestním oznámení apod.;
- Chování personálu;
- Nehody a neočekávaná zranění či úmrtí;
- Pracovní úraz;
- Problém při podání diety či výživy;
- Problém při podání medicinálních plynů;
- Problém při podávání krve či krevních derivátů;
- Problém s chováním pacienta;
- Problém s klinickou administrativou;
- Problém s klinickým výkonem;
- Problém s medikací či intravenózními roztoky;
- Problém se zdravotnickou dokumentací;
- Problémy s dostupností zdrojů;
- Svévolný odchod pacienta;
- Technické problémy.

Vzhledem k nutnosti ochraně osobních údajů, především těch, týkajících se pacientů, je nutno informace anonymizovat. Stejně tak pokud si nahlašující přeje zůstat v anonymitě, je možnost tuto informaci uvést do popisu neshody.

4.4 Trendová analýza mimořádných událostí

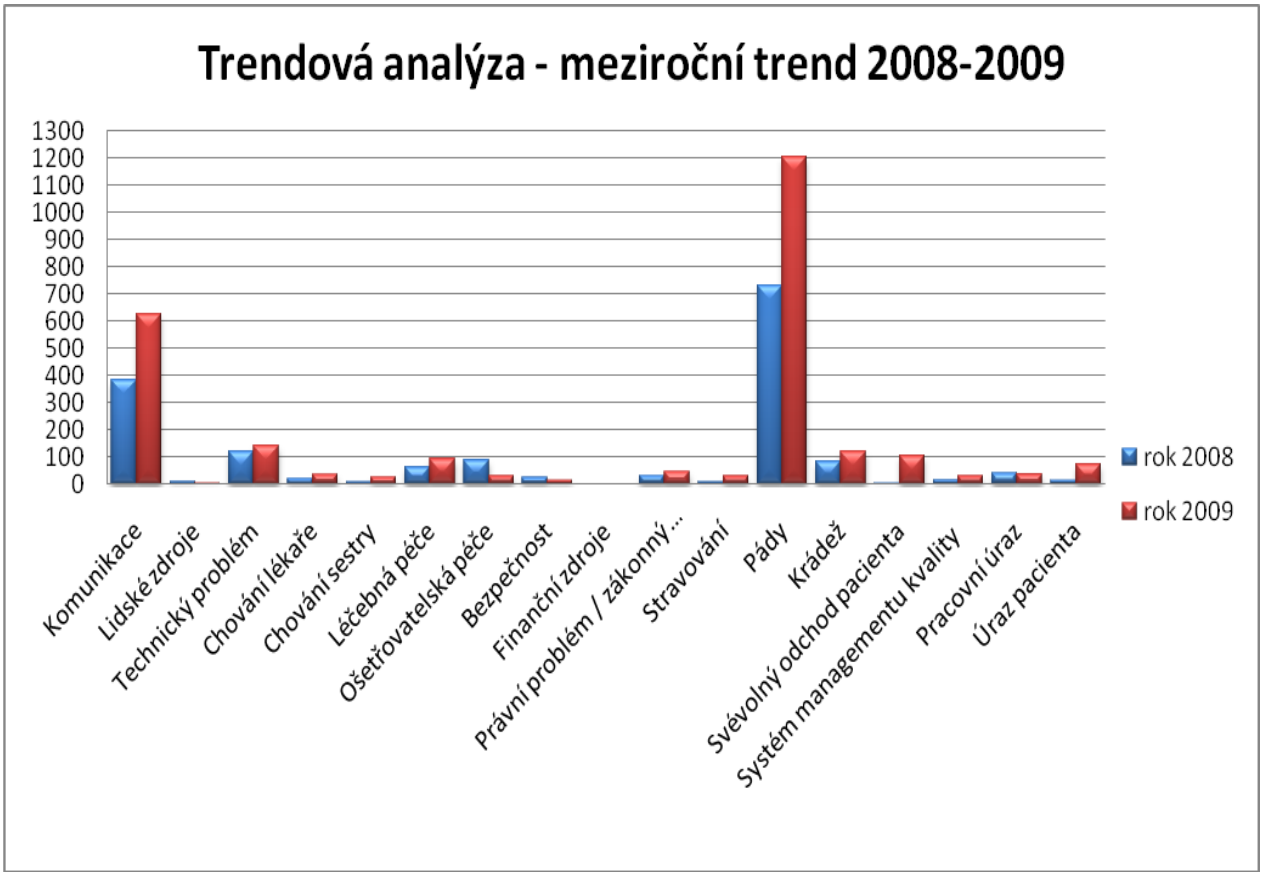
V roce 2008 bylo zahájeno sjednocení systémů sledování neshod a mimořádných událostí, v roce 2009 došlo k doladění aplikace včetně sjednocení typu mimořádných událostí. Meziroční trend mimořádných událostí vykazuje navýšení v roce 2009 na 159% referenční hodnoty roku 2008, což přesně odpovídá trendu systému sledování neshod a mimořádných událostí při zavádění, kdy počet mimořádných událostí roste

s tím, jak jej uživatelé začínají pravidelně využívat, což dokazuje následující tabulka a graf.

Tabulka 4 – 1: Meziroční trend jednotlivých mimořádných událostí

Typ událostí	**rok 2008**	**rok 2009**
Komunikace	386	624
Lidské zdroje	11	5
Technický problém	120	144
Chování lékaře	22	36
Chování sestry	9	27
Léčebná péče	64	93
Ošetřovatelská péče	89	30
Bezpečnost	24	13
Finanční zdroje	0	0
Právní problém / zákonný požadavek	33	47
Stravování	8	29
Pády	730	1202
Krádež	86	123
Svévolný odchod pacienta	1	105
Systém managementu kvality	16	30
Pracovní úraz	40	39
Úraz pacienta	14	75
Celkem	**1653**	**2622**

Zdroj: Trendová analýza mimořádných událostí



Graf 4 – 1: Meziroční trend jednotlivých mimořádných událostí
Zdroj: Trendová analýza mimořádných událostí

Z výsledků analýzy vyplývá lepší sledovanost pádů popř. úrazů pacienta, dále přetrvávající problém v komunikaci (na straně lékařů a sester i na straně pacientů a příbuzných), problém týkající se bezpečnosti – ohrožení majetku pacienta, což plyne z nevyužívání možnosti uložit si své cenné věci v zabezpečených prostorech.

V roce 2009 se stále vyskytují nedostatky ve vedení zdravotnické dokumentace – co se týče čitelnosti a plnění zákonných požadavků (identifikace zápisů do zdravotnické dokumentace), což by se mělo v roce 2010 zlepšit také zavedením nemocničního informačního systému a dále probíhajícími specializovanými audity na vedení zdravotnické dokumentace a pravidelnými školeními.

4.5 Reakce na hrozby

Reakce na hrozby porovnává výčet pravděpodobných hrozeb vyhodnocených akciovou společností a teoreticky možných hrozeb. Na výčet hrozeb bude aplikováno doporučení, k personálnímu zajištění potřebné reakce.

Výčet základních mimořádných událostí, které vyhodnotila akciová společnost:

- Bezpečnostní incident;
- Hrozba medializací, soudem, trestním oznámení apod.;
- Chování personálu;
- Nehody a neočekávaná zranění či úmrtí;
- Pracovní úraz;
- Problém při podání diety či výživy;
- Problém při podání medicinálních plynů;
- Problém při podávání krve či krevních derivátů;
- Problém s chováním pacienta;
- Problém s klinickou administrativou;
- Problém s klinickým výkonem;
- Problém s medikací či intravenózními roztoky;
- Problém se zdravotnickou dokumentací;
- Problémy s dostupností zdrojů;
- Svévolný odchod pacienta;
- Technické problémy.

Obecná problematika bezpečnosti připouští teoreticky následující hrozby podle směru jejich působení na:

- nemovitý majetek – poškození, odcizení části, technická závada;
- movitý majetek – odcizení, poškození, technické selhání, špatná manipulace;
- pacienty – odcizení majetku pacienta, poškození pacienta;
- personál – pracovní úraz, napadení pacientem, šikana na pracovišti, odcizení majetku personálu;

Druhý výčet je jednodušším členěním bezpečnostních problémů podle směru působení hrozby. Jedná se však o subjektivní zhodnocení, které slouží pro porovnávání s výčtem vedeným společností.

Obecnější výčet, který se nezabývá jednotlivými mimořádnými událostmi, ale jejich obecnějším pojmenováním umožňuje její jednodušší začlenění. Dalším rozdílem je zvážení ohrožení životního prostředí. Výčet akciové společnosti se problematikou porušení životního prostředí nezabývá.

4.5.1 Zajištění reakce na hroby

Podnik může na jednotlivé hrozby reagovat několika možnými způsoby:

- Technickými prostředky,
- personálním zabezpečením,
- kombinací obou předchozích.

V následujících úvahách bude rozvíjeno zabezpečení pomocí personálu pro jednotlivé skupiny hrozeb

Zabezpečení nemovitého majetku

Pro většinu mimořádných událostí by zřejmě nejvhodnější bylo technické zabezpečení (kamerový systém, požární hlásiče). V některých místech však není instalace vhodná, nebo není dostačující, proto je žádoucí zajistit reakci na hrozby personálem. Jelikož místní personál má ve většině případů na starost obtížné úkoly, které vyžadují více pozornosti, není vhodné tomuto personálu přidávat další pracovní úkoly ohledně zabezpečení budov apod. Je možné doporučit najmout nový vlastní personál, který by měl za úkol dohlížení na nemovitý majetek, nebo bezpečností agenturu, která se na tuto činnost přímo specializuje.

Zabezpečení movitého majetku

V této skupině se bude zabezpečení lišit podle toho, o jaký movitý majetek se jedná. Ve většině případů by měl na majetek dávat pozor personál, který má majetek k dispozici. Např. pokud se jedná o speciální přístroje, měl by jej užívat důkladně proškolený personál. Dále by měl být personál proškolen v oblasti bezpečnosti, měl by znát negativní dopady v případě špatného zacházení, měl by zajistit zabezpečení majetku před neoprávněnými osobami apod. Tato personální opatření je možné doplnit o technická zabezpečení, např. kamerový systém, autorizační zabezpečení apod.

Zabezpečení pacientů

V mnoha případech je pacient v takovém zdravotním stavu, kdy se ani nemůže postarat o svoji bezpečnost. Je proto potřeba důkladně proškoleného personálu v oblasti péče o pacienty, jednak zdravotních sester, které by měly mapovat pohyb osob na pracovišti, dodržovat pokyny a stanovenou léčbu pacienta, dále by měl zajistit správnou a čitelnou dokumentaci o pacientovi. Samozřejmostí lékařského personálu je znalost ve svém oboru a při lékařských výkonech důkladná péče a pozornost. Nejvhodnější formou

personálního zabezpečení je tedy prostřednictvím místního personálu, který je průběžně školen v otázkách bezpečnosti.

Zabezpečení personálu

V zájmu personálu by mělo být i chránit sám sebe. V některých případech je to však velice obtížné. Personál by měl být dostatečně proškolen při manipulaci s nebezpečnými látkami, přístroji apod. Dále by měl mít k dispozici dostatečné ochranné pomůcky. Měl by mít k dispozici dostatečně zajištěné místo k úschově svých osobních věcí. V tomto případě může být formou zajištění personál z bezpečnostní agentury, který dohlíží na pohyb osob. Co se týče problému napadení pacientem, tak by měl být personál školen ve způsobu jednání s problémovými pacienty a k dispozici by měl být nedaleko i personál bezpečnostní agentury, který by mohl konflikt řešit. V rámci vztahů na pracovišti by mělo fungovat speciální oddělení, které má na starost případné řešení a zpracovávání problémů v případě šikany na pracovišti apod.

Zabezpečení životního prostředí

Vztah k ochraně životního prostředí záleží na zaměstnancích, na jejich přístupu k nakládání s nebezpečnými látkami, na jejich odpovědnosti. Proto by měl být personál důkladně školen.

4.6 Bezpečnostní audit společnosti

V akciové společnosti byl auditorskou firmou proveden bezpečnostní audit. Z pohledu bezpečnosti je kladen důraz na snadný přístup veřejnosti a zároveň to znamená vysoké nároky na personál v zařízení.

V rámci auditu byl mapován stav bezpečnosti v kapitolách:

- Řízení bezpečnosti,
- Fyzické bezpečnosti,
- Bezpečnosti informací (IT/IS),
- Bezpečnosti zdrojů.

Během auditu byl personálu předložen anonymní dotazník, který přináší odpovědi na otázky, jak je vnímána současná úroveň bezpečnosti.

O stavu bezpečnosti informuje Dílčí zpráva z bezpečnostního auditu, ze které se bude vycházet v následujících kapitolách.

4.6.1 Oblast fyzické bezpečnosti

V oblasti fyzické bezpečnosti byly zjištěny nedostatky, na které jsou dána doporučení v následující tabulce.

Tabulka 4 – 2: Fyzická bezpečnost

Zjištění	Doporučení
Volný přístup na oddělení – personál nesleduje pohyb osob.	Školení personálu o základních principech bezpečnosti. Zvýšení ostražitosti personálu.
Poskytování citlivých informací bez ověření totožnosti, nebo jen na základě tvrzení cizích osob.	Stanovení a vyžadování dodržování interních předpisů pro poskytování informací o všech citlivých otázkách.
Zabezpečovací technologie nejsou vhodně instalovány – lze je bez problémů vyřadit z provozu prostým odpojením napájecího kabelu ze zásuvky 230V.	Vytvoření pravidel pro projektování bezpečnostních technologií, důsledné kontrolování provedení instalace.
Nedodržování zákazu kouření v budovách. Zejména v těsném sousedství dětského oddělení, nedodržování základních předpisů požární ochrany.	*Existuje-li nutnost „povolení" kouření personálu, je nutné zajistit tyto prostory tak, aby do nich neměla přístup veřejnost! Dále je třeba upozornit personál na dodržování základních bezpečnostních pravidel.*
Nefunkční dveře v prostorách určených jako nouzové východy. Dveře bez kování a kliky, nefunkční mechanické části.	Kontrola prostor se zvýšeným bezpečnostním rizikem a nároky na funkčnost.
Nedostatečná nebo zcela neexistující dokumentace elektrických bezpečnostních systémů.	Revize dokumentace. Dopracování dokumentace ze strany dodavatelů (na základě existujících smluv o dílo), dále vypracování jednotného seznamu položek nutných pro bezvadnou dodávku díla.
Nedostatečná ochrana zdrojů z hlediska přístupu k nim a kontroly vstupů.	Zajištění režimových opatření, případně instalace elektrických bezpečnostních zařízení pro přístup k vitálním zdrojům energií a medicinálních plynů.

Zdroj: vlastní zpracování z Dílčí zprávy z bezpečnostního auditu

4.6.2 Oblast bezpečnosti zdrojů

V rámci oblasti bezpečnosti zdrojů byla doporučena opatření na zjištěné nedostatky uvedené v následující tabulce.

Tabulka 4 – 3: Bezpečnost zdrojů

Zjištění	Doporučení
Nedostatečné bezpečnostní značení skladování medicinálních plynů (tanky na kyslík)	Neprodlené doplnění povinného bezpečnostního značení.
Přístup k ovládání zdrojů elektrické energie, vody, medicinálních plynů v prostorách zázemí, které je volně přístupné.	Zamezení přímému ohrožení zdraví a života instalací mechanických zabezpečovacích prostředků. Případně zamezení přístupu nepovolaných osob do těchto prostor.

Zdroj: Vlastní zpracování z Dílčí zprávy z auditu bezpečnosti

4.6.3 Oblast bezpečnosti informací (IT/IS)

Na nedostatky zjištěné v oblasti bezpečnosti informací byla dána následující doporučení v tabulce 4 - 4.

Tabulka 4 - 4: Bezpečnost informací IT/IS

Zjištění	Doporučení
Neexistuje plán pro zachování činnosti – tzv. „Buiness Continuity Plan“ (BCP) pro zajištění chodu zcela klíčového systému.	Vypracování strategického dokumentu, který by zajistil zpracování takového plánu. Chod IT/IS systému je zcela klíčový pro chod zařízení.
Neexistuje aktuální analýza rizik provozu IT/IS.	Zpracování analýzy rizik interním oddělením a jejich hodnocení. Analýza rizik bude sloužit i jako podklad pro BCP. Dále je vhodné využít tuto analýzu pro zpracování projektu integrace IT/IS.

Zdroj: Vlastní zpracování z Dílčí zprávy z auditu bezpečnosti

4.6.4 Oblast řízení bezpečnosti

Oblast řízení bezpečnosti tvoří jednu ze skupin, kde byl zjištěn největší počet nedostatků. Jejich výčet a doporučení na ně znázorňuje následující tabulka.

Tabulka 4 – 5: Řízení bezpečnosti

Zjištění	Doporučení
Bezpečnostní strategie ani bezpečnostní politika není stanovena. Je stanovena Politika kvality (jakosti).	Stanovit bezpečnostní strategii a bezpečnostní politiku.
Odpovědnost za řízení bezpečnosti není určena (bezpečnostní manažer). Dílčí odpovědnosti za bezpečnost v oblastech, kde se vyskytují bezpečnostní rizika, jsou určena Organizačním řádem a dokumenty „Popis pracovního místa a pracovní náplň“.	Určit bezpečnostního manažera s odpovídajícími pravomocemi k výkonu své funkce.
Analýza rizik nebyla zpracována, vedení organizace se tímto tématem nezabývalo.	Zpracovat analýzu rizik zahrnující všechna aktiva společnosti.
Systém řízení bezpečnostních incidentů je částečně zajištěn prostřednictvím systému managementu kvality dle ISO 9001.	Stanovit postup řízení všech bezpečnostních incidentů. Jelikož neshody identifikované v rámci systému dle ISO 9001 souvisí i s řízením bezpečnosti, je zde možnost využít tento nástroj k podrobnější evidenci bezpečnostních incidentů a řízení následných opatření.
Interní komunikace v rámci nemocnice je popsána pouze stručně v Příručce kvality. Konají se porady na všech úrovních nemocnice a porady komisí včetně Rady pro kvalitu. Manažer kvality se neúčastní porad vedení.	Zapojit manažera kvality do porad vedení společnosti, aby byla dána dodatečná důležitost činnostem manažera kvality v rámci nemocnice a aby byl přímo informován o záležitostech, které se managementu nemocnice týkají, případně je mohl ovlivnit, aby nedocházelo k rozporu se zavedeným systémem managementu kvality, potažmo otázkami bezpečnosti, které manažer kvality okrajově také sleduje.
Zdroje: Infrastruktura není zcela jasně vymezena a popsána, ani v rámci systému managementu kvality. Není určen způsob plánování údržby a revizí. Odpovědnosti jsou určeny pouze obecně.	Popsat rozsah infrastruktury nemocnice, určit rozsah prováděné pravidelné údržby a revizí, určit odpovědnosti, určit způsob plánování oblasti a vyhodnocení plánu. Plány provázat s požadavky BOZP aj.

Legislativní předpisy sleduje odbor právních služeb – vyhodnocuje, zda se nové předpisy vztahují na společnost, pokud ano, zasílá informaci vedoucím pracovníkům o obsahu nového předpisu. Pokud vedoucí pracovníci vyhodnotí potřebu zpracovat předpis do interní dokumentace, připraví změnu dokumentu. Odbor právních služeb poskytuje výklad legislativních předpisů a informace pro aplikaci v interní dokumentaci společnosti.	Zaměřit se také na legislativu, která řeší bezpečnostní otázky.

Zdroj: Vlastní zpracování z Dílčí zprávy z auditu bezpečnosti

Vzhledem k probíhající systémové integraci vnitřních předpisů a vysoké fluktuaci na vedoucích pozicích neexistuje jednotná bezpečnostní koncepce. Proces integrace sám o sobě s sebou nese zvýšená bezpečnostní rizika. Tato rizika však nejsou nijak koncepčně minimalizována. Odpovědnost za bezpečnost není jasně deklarována a je jako taková rozprostřena v rámci organizační struktury mezi několik pracovních pozic, což nedává prostor pro koncepční přístup.

Personál v mnoha případech není schopen reagovat na potenciální hrozby, neprověřuje tvrzení osob, nebo vůbec nereaguje a nechává volný pohyb osobám na lůžkových odděleních.

4.7 Výsledky dotazníkového šetření

V rámci bezpečnostního auditu byl personálu předložen anonymní dotazník, který přináší odpovědi na otázky, jak je vnímána zaměstnanci současná úroveň bezpečnosti. Dotazník byl překládán zejména ošetřujícímu personálu – sestrám a lékařům.

Dotazník je vyhodnocen pro malý počet uchazečů, tudíž nemá tak přesnou vypovídací schopnost. Přesto jej však lze pro potřeby základního zpracování brát jako dostačující.

Otázky, které byly personálu kladeny, jsou spolu s procentuálním vyjádřením odpovědí na ně v následující tabulce.

Tabulka 4 – 6: Výsledky dotazníkového šetření

Hodnocení dotazníků	Celkem vyjádřeno v % respondentů		
Otázka č.	ANO	NE	NEVÍM
1. Vnímáte celkovou úroveň bezpečnosti nemocnice jako dobrou?	56%	28%	16%
2. Probíhají školení, týkající se bezpečnostní oblasti, dle Vašeho názoru dostatečně často?	76%	12%	12%
3. Je úroveň těchto školení dostatečná?	68%	4%	28%
4. Zodpovídá obsah těchto školení všechny Vaše otázky?	56%	20%	24%
5. Cítíte se v nemocnici Vy sami při výkonu svého povolání bezpečně?	68%	24%	8%
6. Znáte osoby, které zodpovídají za bezpečnost v objektu?	48%	32%	20%
7. Víte o nějakém závažném porušení bezpečnosti, k němuž došlo v minulosti v tomto objektu?	20%	80%	0%
8. Domníváte se, že pro Vaši bezpečnost by zde mělo být děláno více?	52%	28%	20%
9. Myslíte si, že Vám uvnitř objektu nebo v jeho areálu může hrozit fyzické napadení ze strany cizích osob?	64%	16%	20%
10. Přenechali byste v tomto případě zákrok raději ostraze-profesionálovi?	88%	0%	12%
11. Víte, jakými způsoby je zajištěna bezpečnost objektu?	56%	24%	20%
12. Máte do Vašeho PC na pracovišti nainstalovány bezpečnostní záplaty?	32%	0%	68%
13. Jsou v objektu v dostatečném počtu a na žádoucích místech instalovány bezpečnostní kamery?	28%	36%	36%
14. Máte k Vaší práci k dispozici dostatečný počet adekvátních ochranných pomůcek?	68%	28%	4%
15. Znáte dobře únikové cesty, případně evakuační trasy a shromaždiště v případě vzniku mimořádné události?	96%	0%	4%
16. Víte jak se máte zachovat v případě vzniku mimořádné události v objektu?	96%	4%	0%
17. Jste někdy ze strany zaměstnavatele nuceni k porušování bezpečnostních předpisů?	36%	56%	8%
18. Jsou cizí osoby, vstupující do objektu, dostatečně kontrolovány a prověřovány?"	28%	52%	20%
19. Je cizím osobám, pohybujícím se po objektu, věnována dostatečná pozornost? (např. aby nezacházely do nepovolených míst apod.)	36%	44%	20%
20. Je přítomnost cizích osob v objektu adekvátní, co se týče jejich počtu?	20%	20%	60%
21. Je objekt, dle Vašeho názoru, dostatečně zabezpečen z hlediska fyzické ostrahy?	20%	60%	20%
22. Je objekt, dle Vašeho názoru, dostatečně zabezpečen z hlediska instalování bezpečnostních kamer?	12%	48%	40%
23. Je objekt, dle Vašeho názoru, dostatečně zabezpečen z hlediska požární ochrany?	68%	4%	28%
24. Je objekt, dle Vašeho názoru, dostatečně zabezpečen z hlediska ochrany PC systému?	52%	12%	36%
25. Je dostatečně řešena ochrana a zabezpečení Vašich osobních věcí? (zaparkovaných automobilů, cennosti apod.)	28%	48%	24%
26. Věnují nadřízení dostatečnou pozornost Vašim připomínkám a návrhům na zlepšení bezpečnosti práce?	76%	0%	24%
27. Znáte kontakty na odpovědné pracovníky, které byste měli kontaktovat v případě vzniku mimořádné události?	92%	4%	4%
28. Jsou nouzové východy z objektu ponechávány vždy přístupné a volné?	80%	8%	12%
29. Jsou nouzové východy a únikové cesty dostatečně značené?	92%	0%	8%
30. Sledují bezpečnostní kamery, dle Vašeho názoru, všechna riziková místa?	4%	48%	48%

Zdroj: Příloha k Dílčí zprávě z bezpečnostního auditu

Vzhledem k tomu, že na některé otázky nebyli respondenti schopni odpovědět, budou tyto otázky z výběru vyloučeny, jelikož se nedají objektivně zhodnotit. Jedná se o otázky č. 12, 20 a 30.

Tabulka 4 – 7: Výběr otázek z dotazníkového šetření

Hodnocení dotazníků	Celkem vyjádřeno v % respondentů			Přijmutí/Vyloučení otázky
Otázka č.	ANO	NE	NEVÍM	
1. Vnímáte celkovou úroveň bezpečnosti nemocnice jako dobrou?	56%	28%	16%	P
2. Probíhají školení, týkající se bezpečnostní oblasti, dle Vašeho názoru dostatečně často?	76%	12%	12%	P
3. Je úroveň těchto školení dostatečná?	68%	4%	28%	P
4. Zodpovídá obsah těchto školení všechny Vaše otázky?	56%	20%	24%	P
5. Cítíte se v nemocnici Vy sami při výkonu svého povolání bezpečně?	68%	24%	8%	P
6. Znáte osoby, které zodpovídají za bezpečnost objektu?	48%	32%	20%	P
7. Víte o nějakém závažném porušení bezpečnosti, k němuž došlo v minulosti v tomto objektu?	20%	80%	0%	P
8. Domníváte se, že pro Vaši bezpečnost by zde mělo být děláno více?	52%	28%	20%	P
9. Myslíte si, že Vám uvnitř objektu nebo v jeho areálu může hrozit fyzické napadení ze strany cizích osob?	64%	16%	20%	P
10. Přenechali byste v tomto případě zákrok raději ostraze-profesionálovi?	88%	0%	12%	P
11. Víte, jakými způsoby je zajištěna bezpečnost objektu?	56%	24%	20%	P
12. Máte do Vašeho PC na pracovišti nainstalovány bezpečnostní záplaty?	32%	0%	68%	V
13. Jsou v objektu v dostatečném počtu a na žádoucích místech instalovány bezpečnostní kamery?	28%	36%	36%	P
14. Máte k Vaší práci k dispozici dostatečný počet adekvátních ochranných pomůcek?	68%	28%	4%	P
15. Znáte dobře únikové cesty, případně evakuační trasy a shromaždiště v případě vzniku mimořádné události?	96%	0%	4%	P
16. Víte, jak se máte zachovat v případě vzniku mimořádné události v objektu?	96%	4%	0%	P
17. Jste někdy ze strany zaměstnavatele nuceni k porušování bezpečnostních předpisů?	36%	56%	8%	P
18. Jsou cizí osoby, vstupující do objektu, dostatečně kontrolovány a prověřovány?	28%	52%	20%	P
19. Je cizím osobám, pohybujícím se po objektu, věnována dostatečná pozornost? (např. aby nezacházely do nepovolených míst apod.)	36%	44%	20%	P
20. Je přítomnost cizích osob v objektu adekvátní, co se týče jejich počtu?	20%	20%	60%	V
21. Je objekt, dle Vašeho názoru, dostatečně zabezpečen z hlediska fyzické ostrahy?	20%	60%	20%	P
22. Je objekt, dle Vašeho názoru, dostatečně zabezpečen z hlediska instalování bezpečnostních kamer?	12%	48%	40%	P
23. Je objekt, dle Vašeho názoru, dostatečně zabezpečen z hlediska požární ochrany?	68%	4%	28%	P
24. Je objekt, dle Vašeho názoru, dostatečně zabezpečen z hlediska ochrany PC systému?	52%	12%	36%	P
25. Je dostatečně řešena ochrana a zabezpečení Vašich osobních věcí? (zaparkovaných automobilů, cenností apod.)	28%	48%	24%	P
26. Věnují nadřízení dostatečnou pozornost Vašim připomínkám a návrhům na zlepšení bezpečnosti práce?	76%	0%	24%	P
27. Znáte kontakty na odpovědné pracovníky, které byste měli kontaktovat v případě vzniku mimořádné události?	92%	4%	4%	P
28. Jsou nouzové východy z objektu ponechávány vždy přístupné a volné?	80%	8%	12%	P
29. Jsou nouzové východy a únikové cesty dostatečně značeně?	92%	0%	8%	P
30. Sledují bezpečnostní kamery, dle Vašeho názoru, všechna riziková místa?	4%	48%	48%	V

Zdroj: Vlastní zpracování Přílohy k Dílčímu zprávy z bezpečnostního auditu

Otázka č. 1

56% respondentů považuje celkovou úroveň bezpečnosti jako dobrou, 28% respondentů si nemyslí, že je úroveň bezpečnosti dobrá a 16% respondentů nedokázali otázku přesně zodpovědět, či vyhodnotit úroveň bezpečnosti nemocnice. Většina zaměstnanců odpověděla kladně, což je pro akciovou společnost dobrým statutem.

Otázka č. 2

Většina dotazovaných (76%) se domnívá, že školení v oblasti bezpečnosti probíhá dostatečně často. To může mít dvě příčiny. Z té lepší stránky se může jednat o skutečnost, že školení jsou opravdu velice často prováděná. Z té horší stránky se může jednat o nezájem personálu a neochotu se v této oblasti školit, tudíž jim přijdou tato školení častá. Shodný počet respondentů (po 12%) si myslí, že školení nejsou dostatečně častá, nebo nedokážou na tuto otázku odpovědět.

Otázka č. 3

68% si myslí, že úroveň školení v oblasti bezpečnosti je dostatečné, pouhé 4% si myslí, že ne a 28% respondentů si není jisto odpovědí.

Otázka č. 4

S tím, že školení zodpovídají otázky zaměstnanců, souhlasí 56%. 20% zaměstnanců se odpovědí na své otázky nedočká a 24% zaměstnanců neví, což znamená, že od školení nemají žádné konkrétnější očekávání.

Otázka č. 5

Většina zaměstnanců (68%) se při pracovním výkonu cítí bezpečně, což může být zapříčiněno skutečně dobrý stavem zabezpečení, nebo ale také nepřipouštěním si hrozeb ze strany zaměstnanců. 24% se při pracovním výkonu bezpečně necítí. Jedná se o poměrně vysoké číslo, které může znázorňovat přehnaný strach o sebe samého, či skutečně špatný stav zabezpečení, který je zaměstnanci vnímán. 8% respondentů si nebylo jisto odpovědí.

Otázka č. 6

Necelá polovina (48%) zaměstnanců zná osoby, které odpovídají za bezpečnost objektu. Vzhledem k důležitosti této otázky se domnívám, že jde o poměrně malé číslo. 32% zaměstnanců odpovědné osoby nezná, a 20% si není jistá nebo neví. Této otázce by měla být věnována větší pozornost, aby zaměstnanci věděli, kdo za problematiku bezpečnosti odpovídá.

Otázka č. 7

„Pouze“ 20% zaměstnanců ví o nějakém závažném porušení bezpečnosti a 80% si není porušení vědoma. Jedná se o dobrý výsledek. Otázkou však zůstává, zda to není způsobeno tím, že se o porušení bezpečnosti nemluví a zůstává to pouze v úzkém okruhu lidí.

Otázka č. 8

Více než polovina (52%) zaměstnanců se domnívá, že by pro jejich bezpečnost mělo být děláno více. Tato otázka by měla být pro akciovou společnost výstrahou v oblasti bezpečnosti zaměstnanců. 28% zaměstnanců si myslí, že dělat něco více není potřeba a 20% zaměstnanců při odpovídání nevěděla.

Otázka č. 9

Většina personálu (64%) se domnívá, že by mohli být v areálu nemocnice fyzicky napadeni cizími osobami a to i přesto, že v objektu funguje bezpečnostní ostraha. 16% se domnívá, že jim napadení nehrozí a 20% neví.

Otázka č. 10

Téměř veškerý personál by přenechal problémy fyzického napadení odborníkovi. Pouze 12% si není jistá. Tato otázka svědčí o potřebě bezpečnostní ostrahy.

Otázka č. 11

Většina zaměstnanců (56%) ví, jakým způsobem je bezpečnost objektu zajištěna. Poměrně vysoké procento (44%) respondentů neví, nebo si není jistá. Což může být vysvětleno nezájmem ze strany personálu.

Otázka č. 13

Jen 28% zaměstnanců si myslí, že je instalován dostatečný počet kamer na správných místech. Po 36% si respondenti myslí, že ne, nebo neví. Za zvážení by stála další instalace bezpečnostních kamer.

Otázka č. 14

68% personálu má k dispozici dostatečné množství ochranných pomůcek, 28% si myslí, že dostatek ochranných pomůcek nemá a zbytek neví. Tato problematika by měla být řešena individuálně.

Otázka č. 15

Tato otázka přináší velice dobré výsledky. 96% respondentů zná únikové cesty a shromaždiště v případě mimořádné události. Jen 4% respondentů si nebyli jistí.

Otázka č. 16

Stejně dobře jako předchozí otázka dopadla i tato. Rovněž 96% zaměstnanců ví, jak se zachovat při mimořádné události. Pouhé 4% nevěděli.

Otázka č. 17

Tato otázka je velice závažná a nemělo by na ni být ani jednou odpovězeno kladně. Přesto však 36% respondentů bylo někdy ze strany zaměstnavatele nuceno k porušování bezpečnostních předpisů. V 56% tomu tak nebylo a 8% neví.

Otázka č. 18

28% personálu připouští, že cizí osoby vstupující do objektu jsou dostatečně kontrolovány. 52% si myslí, že kontrola cizích osob není dostačující a 20% neví. Této otázce by měla být věnována vyšší pozornost.

Otázka č. 19

Také většina (44%) se domnívá, že těmto cizím osobám není věnována dostatečná pozornost (např. při vstupu do nepovolaných míst). 36% si myslí, že pozornost je dostatečná a 20% neví.

Otázka č. 21

To, že je objekt dostatečně zabezpečen z hlediska fyzické ostrahy, si myslí jen 20% zaměstnanců. Jedná se však o jejich osobní pohled, který může být zkreslený jejich nezájmem o tuto problematiku. 60% si pak myslí, že objekt po této stránce není dostatečně zajištěn a 20% neví. Této problematice by měla být věnována větší pozornost.

Otázka č. 22

Zabezpečení objektu u hlediska instalování bezpečnostních kamer je podle respondentů nedostatečné. Jen 12% se domnívá, že zabezpečení je dostatečné. Většina (48%) si to nemyslí a poměrně vysoké procento neví.

Otázka č. 23

Z pohledu zaměstnanců je však objekt zabezpečen z hlediska požární ochrany. Myslí si to 68% dotázaných. Pouhé 4% si to nemyslí a 28% neví.

Otázka č. 24

Přibližně polovina (52%) dotázaných si myslí, že objekt je zabezpečen z hlediska ochrany PC systém, 12% si to nemyslí a 36% neví, což může být způsobeno neznalostí v technickém směru.

Otázka č. 25

Otázka ochrany osobních a cenných věcí personálu se poměrně v názorech liší. Je to pravděpodobně způsobeno tím, že každý má ke svým cenným věcem jiný vztah a jinou představu o jejich zajištění. 28% považuje ochranu za dostatečnou, 48% si to nemyslí a 24% neví.

Otázka č. 26

Pro akciovou společnost je tato otázka pozitivně vypovídající, jelikož 76% zaměstnanců souhlasí s tím, že je dostatečně věnována pozornost jejich návrhům na zlepšení bezpečnosti práce. Ani jeden respondent nezaujal negativní postavení a 24% zaměstnanců si není jista.

Otázka č. 27

V případě vzniku mimořádné události zná 92% kontakty na osoby, které by měly být kontaktovány. Jen 4% kontakty neznají, nebo si nejsou jisti.

Otázka č. 28

Zaměstnanci v 80% souhlasí s tím, že nouzové východy jsou vždy přístupné a volné. 8% si to nemyslí a zbytek neví.

Otázka č. 29

Tato otázka souvisí s tou předchozí a zaměstnanci reagují opět velice pozitivně, co se značení únikových cest týče. 92% z nich si myslí, že únikové cesty a východy jsou dostatečně značené. Ani jeden respondent neodpověděl negativně a jen 8% neví.

5 NÁVRHY A DOPORUČENÍ

Současné řešení bezpečnosti podniku již neodpovídá soudobým požadavkům. Přibývají nové a dosud neočekávané typy hrozeb. Podnik by měl pružně reagovat na změny ve svém prostředí. Pokud k tomu nemá připravený a určený personál, nebude schopen nové problémy uspokojivě řešit.

Vyhodnocením informací o vybraném zdravotnickém zařízení je možné označit:

1. **Za hlavní nedostatek: neexistence bezpečnostní strategie** a nejsou určeny konkrétní odpovědnosti zaměstnanců za bezpečnost. K tomu je možné doporučit: Do funkcí pro řízení bezpečnosti určit osoby, které by měly odpovědnost za sestavení bezpečnostní strategie a konkrétní odpovědnosti za bezpečnost. Jejich pracovní náplní bude zpracování bezpečnostní a krizové dokumentace, včetně vyhodnocení rizik a stanovení preventivních opatření.
2. **Za funkční:** systém hlášení mimořádných událostí, který je velmi pěkně propracován do detailů podle vymezení mimořádných událostí. K tomu je možné doporučit:
    a. Pro zjednodušení při výběru typu mimořádné události zavést hlavní obecnější členění. Mělo by zahrnout konkrétní typy mimořádných událostí, které by bylo možné dále doplňovat.
    b. Aby byl počet nahlášených mimořádných událostí stejný jako jejich skutečný počet, důkladně proškolit personál v oblasti bezpečnosti a způsobů hlášení mimořádných událostí. Právě personál ovlivní, zda se událost bude řešit nebo nebude. (Skutečný počet mimořádných událostí je nezbytně nutný pro analýzu rizik, proto by manažer rizik neměl v případě pochybení činit rázné postihy pro nápravu. Právě tento přístup by mohl vést k tomu, že personál ze strachu z následků nebude mimořádné události hlásit.)
3. **Za vhodné:** provádět pravidelný bezpečnostní audit. Poskytnutý podklad o bezpečnostním auditu je dobrý krok ke zlepšení bezpečnosti. Podrobně zjistil veškeré nedostatky a doporučit jejich nápravu. Podnik by měl zvážit důležitost jednotlivých nedostatků a vytvořit postupný plán pro nápravu podle závažnosti.

Podnik by dále neměl zapomínat na průběžnou kontrolu stávajících zabezpečení a měl by pravidelně školit personál nejenom v otázkách bezpečnosti, ale také kvality péče a jejich odbornosti.

Ve finále je v zájmu podniku fungovat v souladu jako celek, nikoliv jako jednotlivé odborné složky podniku.

ZÁVĚR

V bakalářské práci s názvem Analýza podniku pro personální zajištění jeho vnitřní ochrany jsem se zabývala především problematikou bezpečnosti ve vybraném zdravotnickém zařízení a na zjištěné nedostatky hledala řešení. Obecná část byla doplněna obrázky, tabulkami a grafem.

První kapitolu jsem věnovala vymezení základních pojmů, které souvisí s problematikou bezpečnosti a rizik – aktivum, hrozba, riziko, krize, mimořádná událost, škoda a újma.

Druhá kapitola byla zaměřena na problematiku rizik, kde byl popsán historický vývoj pojmu riziko, dále byly uvedené možné způsoby třídění rizik podle různých hledisek. Také jsem se zabývala analýzou rizik a popsala jednotlivé kroky analýzy, uvedla jsem jednotlivé metody, které lze při analýze použít a popsala metody nejčastěji užívané v praxi. V neposlední řadě jsem se zabývala řízením rizik, přístupy ke snižování rizik a uvedla jsem, jakými způsoby je možné rizika zajistit z personálního hlediska.

Ve třetí kapitole jsem se zabývala riziky ve zdravotnických zařízeních obecně. Uvedla jsem, standardy a normy, kterými se musí zdravotnická zařízení řídit v oblasti bezpečnosti, dále jsem vysvětlila funkci role manažera rizik. Zvážila jsem, k jakým rizikům může dojít z perspektivy lékařů a ošetřovatelského personálu. Na závěr této kapitoly bylo popsáno hlášení mimořádných událostí ve zdravotnických zařízeních.

Předposlední, čtvrtá kapitola, byla věnována vybranému zdravotnickému zařízení. Nejprve byla organizace představena, v kterých aktivitách společnost působí. Dále bylo seznámeno s bezpečnostní dokumentací společnosti, bylo popsáno, jak probíhá hlášení mimořádných událostí v této společnosti a byl znázorněn vývoj mimořádných událostí pomocí trendové analýzy. V podkapitole „Reakce na hrozby“ byl porovnán výčet hrozeb ze strany společnosti s teoretickým výčtem a byla popsána zajištění těchto hrozeb. Poslední část této kapitoly popisuje výsledky bezpečnostního auditu společnosti, který byl proveden auditorskou firmou. V závěru kapitoly jsou zpracovány výsledky dotazníkového šetření, které bylo provedeno v rámci bezpečnostního auditu.

Poslední kapitola této bakalářské práce dává návrhy a doporučení na zjištěné problémy v organizaci.

V úvodu bakalářské práce byl určen cíl teoreticky popsat problematiku spojenou s analýzou rizik a metody jejich snižování, seznámit se s problematikou v konkrétním podniku, zhodnotit situaci a vytvořit návrhy a doporučení. Problematika analýzy rizik a metody snižování rizik byly popsány ve druhé kapitole, seznámení se s problematikou v konkrétním podniku popisuje čtvrtá kapitola a návrhy a doporučení dává pátá kapitola. Všechny stanovené cíle byly tedy splněny.

SEZNAM POUŽITÉ LITERATURY

Knižní zdroje:

ANTUŠÁK, E., KOPECKÝ, Z. *Úvod do teorie krizového managementu I*. Praha: Vysoká škola ekonomická v Praze, Oeconomica, 2002. 96 s. ISBN 80-245-0340-9.

BARTLOVÁ, I., BALOG, K. *Analýza nebezpečí a prevence průmyslových havárií*. Ostrava: SPBI Spektrum 7, 1998. 193 s. ISBN 80-86111-07-5.

HNILICA, J., FOTR, J. *Aplikovaná analýza rizika ve finančním managementu a investičním rozhodování*. 1. vyd. Praha: Grada Publishing, 2009. 264 s. ISBN 978-80-247-2560-4.

JANATA, J. *Pojištění a management majetkových podnikatelských rizik*. 1. vyd. Praha: Professional Publishing, 2004. 87 s. ISBN 80-86419-64-9.

RAIS, K. *Řízení podnikatelských rizik a metody jejich snižování: Edice Habilitační a inaugurační spisy, sv. 125*. Brno: Vutium, 2003. 33 s. ISBN 80-214-2507-5.

ROUDNÝ, R., LINHART, P. *Krizový management I.: Ochrana obyvatelstva, mimořádné události*. 1. vyd. Pardubice: Univerzita Pardubice, 2005. 97 s. ISBN 80-7194-674-5.

ROUDNÝ, R., LINHART, P. *Krizový management III.: Teorie a praxe rizika*. 1. vyd. Pardubice: Univerzita Pardubice, 2007. 174 s. ISBN 80-7194-924-8.

SMEJKAL, V., RAIS, K. *Řízení rizik ve firmách a jiných organizacích*. 3. vyd. Praha: Grada Publishing, 2010. 360 s. ISBN 978-80-247-3051-6.

SZABO, L., VARCHOLOVÁ, T., DUBOVICKÁ, L. *Manažment rizika*. 1. vyd. Bratislava: Ekonóm, 2005. 126 s. ISBN 80-225-1949-9.

ŠKRLA, P., ŠKRLOVÁ, M. *Řízení rizik ve zdravotnických zařízeních*. 1. vyd. Praha: Grada Publishing, 2008. 200 s. ISBN 978-80-247-2616-8.

TICHÝ, M. *Ovládání rizika: Analýza a management*. 1. vyd. Praha: C. H. Beck, 2006. 396 s. ISBN 80-7179-415-5.

VEVERKA, I. *Vybrané kapitoly krizového řízení pro záchranářství.* 1. vyd. Praha: PAČR, 2003. 175 s. ISBN 80-7251-126-2.

ZUZÁK, R., KÖNIGOVÁ, M. *Krizové řízení podniku*. 2. vyd. Praha: Grada Publishing, 2009. 256 s. ISBN 978-80-247-3156-8.

Tištěné dokumenty:

Dílčí zpráva z bezpečnostního auditu

Organizační řád akciové společnosti

Směrnice o neshodách a mimořádných událostech

Trendová analýza mimořádných událostí

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM GRAFŮ