Univerzita Pardubice

Fakulta ekonomicko- správní

Řízení bezpečnosti jako součást strategického řízení podniku

Lucie Hřebenová

Bakalářská práce

2011

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

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Lucie HŘEBENOVÁ**
Osobní číslo:	**E08632**
Studijní program:	**B6208 Ekonomika a management**
Studijní obor:	**Management podniku - Management malých a středních podniků**
Název tématu:	**Řízení bezpečnosti jako součást strategického řízení podniku**
Zadávající katedra:	**Ústav ekonomiky a managementu**

Zásady pro vypracování:

Stanovení cílů práce
1. Oblasti strategického řízení rozvoje podniku
2. Pojetí a obecné zásady řízení bezpečnosti v podniku
3. Profil společnosti ČSOB Pojišťovna, a.s.
4. Aplikace obecných zásad řízení bezpečnosti ve společnosti ČSOB Pojišťovna, a.s.
5. Zhodnocení systému řízení bezpečnosti ve společnosti ČSOB Pojišťovna, a.s., doporučení pro zlepšení současného stavu
6. Formulace závěrů

Rozsah grafických prací: -

Rozsah pracovní zprávy: **cca 30 stran**

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

Seznam odborné literatury:

[1] **Http://www.csobpoj.cz [online]. 2010 [cit. 2010-06-19]. ČSOB Pojišťovna. Dostupné z WWW:http://www.csobpoj.cz**

[2] **SMEJKAL V RAIS K. Řízení rizik ve firmách a jiných organizacích. 2. vydání. Praha: Grada Publishing 2006. ISBN 80-247-1667-4.**

[3] **SOUČEK Z. Firma 21. století. 1. vydání. Praha: Professional Publishing 2007. ISBN 80-86419-88-6.**

[4] **THADDEYUS, M. Základy strategického řízení. 1. vydání. Praha: Grada Publishing, 2007. ISBN 978-80-247-1911-5.**

[5] **THOMPSON, J, MARTIN, F. Strategic Management. 4. vydání. Thomson 2003. ISBN 1-84480-0833.**

[6] **TICHÝ M. Ovládání rizika. Analýza a management. 1. vydání. Praha: C. H. Beck 2006. ISBN 80-7179-415-5.**

Vedoucí bakalářské práce: **Ing. Aleš Horčička**
Ústav ekonomiky a managementu

Datum zadání bakalářské práce: **1. prosince 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 2. prosince 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 seznámena s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 30. 4. 2011

Lucie Hřebenová

Poděkování

Tímto bych chtěla poděkovat vedoucímu mé bakalářské práce Ing. Aleši Horčičkovi, za odborné vedení, metodickou pomoc, konzultace a podporu. Dále děkuji Ing. Martinu Pavlíkovi ze společnosti ČSOB Pojišťovna, a.s., za poskytnutí potřebných informací o podniku, pomoc při jejich zpracování a ochotě spolupracovat.

Anotace

Bakalářská práce charakterizuje konkrétní společnost a v ní řízení bezpečnosti jako součást strategického řízení. Objasňuje základní pojmy z oblasti řízení podniku a řízení bezpečnosti. Jsou popsány podoby řízení podniku a oblasti, kterých se řízení bezpečnosti v podniku týká. Součástí práce je i zhodnocení současného stavu řízení bezpečnosti ve sledované společnosti a doporučení pro další zlepšení.

Klíčová slova

Řízení, podnik, strategické řízení, taktické řízení, operativní řízení, strategie, bezpečnost, informační bezpečnost, bezpečnost práce, ČSOB Pojišťovna, a. s.

Title

Safety Management as a Part of Strategic Management

Annotation

The bachelor work describes an individual organization and it safety management as a part of strategic management. Fundamental terms of management and safety management are explained. Forms of management and spheres which concern safety management in a company are described in the work. An evaluation and recommendation of a contemporary state of a safety management in observed company is a part of the work.

Key words

Management, strategic, tactical, operative management, strategy, safety, information safety, safety of working, ČSOB Pojišťovna, a. s.

Obsah

Úvod

Dnešní svět je čím dál složitější a rychlejší. Projevuje se to v běžném životě i na trzích a tím pádem ovlivňuje i podniky. I řízení firmy tedy znamená pohyb v tomto složitém prostoru s nesnadnou orientací. Pravidelně se řeší situace, které potřebují správná rozhodnutí. Pro správná rozhodnutí jsou nezbytní spolehliví spolupracovníci a podřízení, nutné je je správným způsobem stimulovat a jít jim příkladem. Je to symbióza vědy a umění. Každodenní praxe utvrzuje v tom, že bez talentu, popřípadě i štěstí nelze v podnikání a managementu dosáhnout větších úspěchů. Potřebné jsou úplné informace, ale také nadhled nad často se vyskytujícími starostmi a problémy.

Tématem čím dál více článků v tisku nebo diskusním tématem z médií je „bezpečnost," tedy bezpečnost v nejrůznějších formách. Týká se běžného života občanů, ale samozřejmě i trhů a podnikání celkově. Podnikatelé téměř denně řeší nejrůznější útoky zvenčí, které mají na svědomí buď vandalové (vniknutí do objektů, drobné krádeže atd.), ale často je viníkem i konkurence. Konkurence čeká na sebemenší chybičku. Mnohdy jde o útoky s motivem získat utajované informace. Diskutovaným tématem je i bezpečnost práce, díky níž se vedou časté soudní spory. V dnešní době se klade velký důraz na kvalitu životního prostředí, v tomto ohledu se bezpečnost také řeší.

Téma bezpečnosti je nezbytné, aby měl ošetřené každý podnik a ve své organizační struktuře měl vymezené místo pro toto oddělení nebo alespoň určeného odpovědného pracovníka. Bezpečnost se týká všech oblastí řízení v podniku.

Cílem práce je:

1) deskripce významu řízení bezpečnosti v podniku;
2) analýza systému řízení v ČSOB Pojišťovně, a. s.;
3) zhodnocení stavu řízení bezpečnosti a doporučení pro zlepšení;

Během práce bylo využito zpracovávání odborné literatury, literárních rešerší, zpráv z kongresů a článků z odborných časopisů. Bylo čerpáno z českých i cizojazyčných pramenů. Dále bylo využito směrnic a nařízení sledovaného podniku. Podstatnou pomocí byly i konzultace ředitelem odboru outsourcingu a bezpečnosti Ing. Martinem Pavlíkem.

Práce má tří hlavní části. V první části je popsáno řízení podniku z různých pohledů, jeho druhy, podrobněji se věnuje strategickému řízení a strategii. Druhá část objasňuje pojetí bezpečnosti z několika hledisek. Třetí část je praktická, zaměřuje se na sledovaný podnik. Popisuje jeho profil, poté jak řeší organizace oblast řízení bezpečnosti.

V první kapitole je popsáno řízení podniku, jak je řízení vnímáno z různých pohledů, druhy řízení. První kapitola se podrobněji věnuje strategickému řízení a strategii podniku.

Druhá kapitola pojednává o bezpečnosti podniku obecně, hlavních oblastech, které podniky v rámci bezpečnosti řeší, konkrétněji rozebírá informační bezpečnost.

Třetí kapitola představuje podnik ČSOB Pojišťovna, a. s.

Ve čtvrté kapitole je blíže analyzován popsán systém řízení bezpečnosti v ČSOB Pojišťovně.

Pátá kapitola zhodnocuje řízení bezpečnosti v ČSOB Pojišťovně a dává doporučení pro zlepšení současného stavu.

V šesté kapitole jsou formulovány závěry práce.

1 Oblasti strategického řízení rozvoje podniku

Na pojem management lze pohlížet různými způsoby, však většina autorů se shoduje na českém významu řízení.

Řízení v obecném smyslu lze chápat jako cílevědomé působení na určitou soustavu a to směrem k předem stanoveným cílům, včetně definované potřebné zpětné vazby. Týká se dosahování výsledků pomocí efektivního získávání, rozdělování, využívání a kontrolování všech potřebných zdrojů, tedy lidí, peněz, zařízení, budov, vybavení, informací a znalostí. Upřednostňuje racionalitu a osvědčené způsoby řešení, má neosobní postoje k cílům, omezenou volbu, nechuť k rizikům změnám a používá se převážně pro rutinní práce.

Management lze pohlížet v širším a užším pojetí. Širší pojetí zahrnuje řízení technické, biologické a společenské. Řízení technické je řízení ve vztahu „člověk – stroj“ nebo „stroj – stroj.“ Řízení biologické představuje řízení, které je uskutečňováno v živých organismech. A řízení společenské je orientováno na řídicí vztahy mezi lidmi při uskutečňování různých druhů společenských aktivit.

V užším pojetí je management zaměřený na řízení lidí při uskutečňování různých druhů společenských aktivit.

Na řízení se lze dívat i z mnoha dalších pohledů. Například ho lze vnímat jako proces v organizaci nebo ho lze dál členit podle kompetencí.

1.1 Řízení jako proces v organizaci

Řízení každé firmy je ovlivněno různými ukazateli, jedním z nejdůležitějších je stav okolí. Dění je v důsledku stále se rozšiřující globalizace ovlivněno situací v rámci událostí celého světa. Mezi nejvíce probírané patří:

- masivní nástup asijských států (hlavně Čína a Indie) na světové trhy;
- Indie je největším světovým hráčem v oblasti softwaru;
- největší hutnická firma je v Indii;
- Číňané investují v ČR;

- Rusko má přebytek finančních zdrojů;
- Arabští šejkové investují miliardy dolarů do automobilového průmyslu;
- vysoká výkonnost USA a její předstih před ostatními částmi světa;
- manažerské metody v Evropě jsou zastaralé, neefektivní a do světa 21. století nepatří.

Většina dnešních organizací není řízena tím nejšťastnějším způsobem a nereagují na stav a vývoj okolí, což je častým důvodem bankrotů. Proto je nutné postupně zavádět nové metody ve vedení společností. Však žádná jednotná forma úspěšné firmy neexistuje. Nejlepších výsledků dosahují firmy, které se dokážou nejlépe přizpůsobovat okolí, záleží i na mnoha dalších faktorech, které ovlivňují úspěch či neúspěch firmy dnešního století.

1.1.1 Principy úspěšně řízené firmy 21. století

Absolutní orientace na zákazníka

Vztahy mezi dodavatelem a zákazníkem prošly určitým historickým vývojem. V současné době, se zaznamenává vysokou globální převahu nabídky nad poptávkou a vznik zákaznické ekonomiky, lze poté mluvit o absolutní orientaci na zákazníka.

Podnik by se měl stát organizací, s níž se dobře spolupracuje, poskytovat zákazníkům vyšší přidanou hodnotu, naučit své pracovníky pracovat pro obecný prospěch firmy, neprodávat distributorům, ale zákazníkům. Doslova všichni pracovníci si musí být vědomi toho, že úspěch firmy plně závisí na zákaznících. Doporučuje se přemýšlet jako zákazníci, tzn. které hodnoty zákazník vnímá a jak je co nejlépe uspokojovat. Nezbytné je aktivně vyvolávat nové potřeby zákazníků. Důležité je si zákazníka vážit. Udržení dobrého zákazníka je mnohokrát levnější, než získání zákazníka nového.

Silný top management

Silný top management řídí firmu jako jednotný celek na základě jasně formulované a důsledně implementované strategie. Používá účinný a ucelený systém řízení, zajišťující plnění strategických cílů. Systém je založen jak na aktivitě pracovníků, tak i na disciplíně.

Silný top management dokáže správně předvídat nastupující vývojové trendy, odhadnout tendence budoucího vývoje a určit postavení firmy. Formuluje strategii firmy obsahující misi, vizi a strategické operace. Má odvahu provézt radikální změny, používá správný styl řízení firmy jako celku, dokáže přesvědčit spolupracovníky o správnosti a reálnosti strategie a stimuluje je k jejímu splnění, utváří ucelený systém řízení a v neposlední řadě nalézá správné pracovníky na rozhodující pracovní pozice.

Strategické předvídání

M.Hammer: „Řízení podniků vždy bylo a nadále bude jednou z nejsložitějších, nejriskantnějších a nejnejistějších lidských činností.“

Předvídání je předpokladem jakékoli aktivity. Provádění závažných rozhodnutí bez předvídání vzniku určitých situací v okolí i uvnitř organizace je zcela nesmyslné a v mnohých případech vede i k bankrotu. Strategické předvídání umožňuje firmě rychle reagovat na změny, či změny aktivně vytvářet.

Musí se brát v úvahu, že budoucnost je neznámá, zpravidla se odlišuje od minulosti, nelze ji vypočítat matematickými a statistickými metodami. Velkou roli hraje i intuice, která musí být podložena hlubokými analytickými znalostmi a velkým množstvím informací.

Strategické předvídání často není prováděno adekvátními metodami. Mnohdy vychází z naivních představ, že budoucnost je mechanické opakování minulosti, chybí vstupní informace a systém jejich zpracování. Toto vede ke zklamání z výsledků předpovědí. Základem strategického předvídání je velké množství informací a vybudování moderního strategického informačního systému. V současné době je strategické předvídání na nízké úrovni, protože top management mu nepřikládá velkou důležitost, dalším důvodem je nerozvinutá informační základna a neschopnost syntetizovat strategické informace a vyvozovat z nich správné závěry. Přitom získání informací je dnes díky rozvoji internetu, informačních technologií a databázím velmi jednoduché, rychlé a levné. Ani v případě, že se management začne strategickému předvídání věnovat více, nelze očekávat, že budoucnost bude možné přesně určit.

Mezi základní strategická rozhodnutí patří:

- určení charakteristik, ve kterých chce firmy dosáhnout „špiček“ (např. kvalita, ekologičnost, náklady, servis);
- rozhodnutí o struktuře portfolia firmy (tzn. o souboru výrobků/služeb, které firma bude vyrábět/poskytovat);
- důležité je zaměření se na perspektivní obory.

Správný styl řízení

Správný styl řízení je takový, který zajišťuje splnění strategických cílů firmy. V rozdílných ekonomikách je nutné použít různý styl řízení.

Aktivní vytváření poptávky a hledání nových trhů

Existence poptávky je základním předpokladem jakékoliv firmy či instituce. Kdo nemá poptávku, nemůže existovat, přežít a rozvíjet se. Firmy proto musí mít přehled o existující celosvětové poptávce. Samozřejmě zjišťování poptávky u odběratelů dnes nestačí. Moderní firma si poptávku cíleně a systematicky vytváří.

Specifické přednosti a vnímané hodnoty

V dnešním „superkonkurenčním“ světě nemůže přežít žádná firma, která nemá specifické přednosti (tzn. vlastnosti, kterými se odlišuje od ostatních firem). Často se využívá také termín konkurenční výhoda. Podnik tyto výhody musí vytvořit především svojí aktivní činností. I přednosti musí mít určité vlastnosti. Zákazník je především musí vnímat (tzn. musí je umět změřit nebo objevit), dále musí pochopit, že tyto vlastnosti může užitečně využít ke svému prospěchu a samozřejmě za ně musí být ochoten zaplatit cenu, která minimálně pokryje základy na vytvoření. Důležitým faktorem je také, že tyto přednosti nesmí být snadno, rychle a levně napodobitelné.

Orientace na špičkové výsledky

Jestliže firma chce být úspěšná, musí směřovat k tomu, aby dosáhla špičkových výsledků a to v celosvětovém měřítku. Nejdůležitějším měřítkem špičkové úrovně firmy je její celosvětová konkurenceschopnost. K tomuto jsou potřebné kvalifikace pracovníků. Určení charakteristik, u nichž chce firma dosáhnout špičky, patří mezi základní strategická rozhodnutí. Moderní firma usiluje především o využití faktorů necenové konkurence.

Důležité je dodržovat tři základní zásady. Nesmíme se snažit napodobovat produkty těch špičkových firem, jejichž snaha prosadit se na trhu vede k neúčelným inovacím. Dále světové špičky se nedosahuje pouze vysokými objemy výroby. Stále významnější roli hraje Kvalita produktů a služeb a komplexnost. Za třetí je nutné orientovat se na praktické využití nových myšlenek. Špičková firma by měla mít prvenství v oblastech: produkty, organizace, lidské zdroje a spojenci.

Výkonnost, efektivita, produktivita

Hodnocení výkonnosti firmy se provádí pomocí ukazatelů, hodnotící výsledky firmy v uplynulém období a současně se používají ukazatele, z nichž lze usoudit budoucí vývoj. Dále se používají finanční ukazatele, ale také nefinanční ukazatele, charakterizující především vztahy se zákazníky.

Nejjednodušším kritériem pro hodnocení je zisk. Používají se i další, například podíl firmy na trhu, návratnost aktiv, spokojenost zákazníků, peněžní tok, přidaná hodnota atd. O výkonnosti rozhoduje především rychlost, jednoduchost, transparentnost, správně definované cíle, zpětná vazba, cílený trénink, zdokonalování technické základny firmy.

Správné produkty a jejich zaměření

V dnešní ekonomice má zákazník možnost si vybrat z velkého množství produktů. Aby firma v konkurenci obstála, musí vést její produkt či služba k vyšší spokojenosti zákazníka.

Efektivní portfolio

Firma dnešního století provádí pouze ty činnosti, které dokáže dělat nejlépe a nejlevněji, zákazníci uznávají specifické přednosti. Zbaví se těch činností, u kterých to tak není. Rozhodnutí o struktuře portfolia patří mezi základní strategická rozhodnutí. Firma se musí plně věnovat rozvoji svého hlavního předmětu podnikání, tzv. core business.

Znalosti jako základ úspěchu

Znalosti jsou to, co člověku poskytuje možnost plnit úkoly tím, že se kombinují data z rozdílných externích zdrojů a používají se vlastní informace, zkušenosti a přístupy. Používá se k tomu specializovaný mechanismus znalostního managementu. Tím je myšlen systematický proces hledání, vybírání, organizování, filtrování a prezentování informací způsobem, který zlepšuje znalosti pracovníka v oblasti jeho zájmu.

Rychlost a pružnost

Rychlost se dnes stala jedním ze základních požadavků na všechny aktivity firmy. Čas se tak stává jedním z nejcennějších zdrojů. Výhra v závodě s časem vyžaduje vysokou pružnost firmy. Velkým přínosem zrychlení procesů je také skutečnost, že snižuje riziko a to nejen riziko spojené s vývojem nových produktů, ale i riziko vyplývající z reakce na vývoj poptávky. Další možností, jak urychlit průběh procesů je způsob kontroly kvality. Dnes se také klade důraz na využití distribučních sítí a použití moderních informačních technologií.

Výkonnostní motivační systém

Motivování pracovníci tvoří základní pilíř firmy 21. století. Většina studií uvádí, že nejsilnějším motivačním nástrojem v českých firmách zůstávají peníze. Nové tendence ukazují, že především mladí lidé s vyšším vzděláním začínají preferovat více volného času, zajímavou práci a větší prostor pro samostatné rozhodování. Firma 21. století vytváří u svých pracovníků hrdost na příslušnost k firmě.

Centralizace

České firmy byly do roku 1990 velmi silně centralizovány. Po tomto roce se vytvářely divize, v současnosti je nutné účelnost divizního uspořádání přehodnotit. Konkurenceschopnosti firmy lze dosáhnout pouze tehdy, je-li firma řízena jako komplexní celek, tedy jestliže jsou jednotlivé části účelně propojeny. Firma musí být centralizována tak, aby všechny procesy byly ve firmě prováděny pouze jednou.

Řízení procesů

Pro efektivní fungování procesů musí být vytvořeny organizační předpoklady. Doba provádění procesů se snižuje.

Inovativnost

Inovace jsou často chápány pouze jako změny technických parametrů produktů. Ve skutečnosti musí být zaměřeny na všechny podnikové aktivity – nákup, spotřebu, technologii, organizaci, řízení, marketing, servis, prodej, personalistiku atd. Úspěšnost inovací závisí především na schopnosti předvídat budoucí vývoj a na schopnosti řídit proces změn. Je to jeden z hlavních úkolů. Top management musí podporovat inovativní myšlenky, které by mohly vytvářet prostor pro velké nové příležitosti.

Inovace znamená realizace invence. Invence je jakákoli myšlenka či nápad.

Vítězství „velkých, rychlých, silných a progresivních“

Cesty k tomu, jak se stát velkými jsou různé. Firmy mohou zvolit spojování různé formy (fúze, akvizice, aliance). Obecně jsou u všech forem spojování rozhodující tyto podmínky: volba správného partnera, dobrá organizace součinnosti, přebudování procesů tak, aby vytvořily jednotný celek a dokonalé řízení realizace.

Používání moderních metod managementu

Metody managementu se v posledních letech velmi rychle vyvíjejí. Často souvisí s využitím informačních technologií. Nejnovější průzkumy uvádí, že velká část českých manažerů mnoho moderních metod nejen nezavedla, ale dokonce ani nezná.

Mezi základní přístupy moderního managementu patří:

Management změn

S touto novou metodou nabývá na významu nová disciplína: řízení změn. Většina firem se zaměřuje převážně na změny orientující se na výrobek, jejichž důsledkem je snižování nákladů, zvyšování výsledné kvality nebo zkracování času. Dalšími změnami jsou například revitalizace (oživení podniku), restrukturalizace (obnovení podnikatelských funkcí).

Krizový a risk management

Obecně lze krizový management chápat jako management určený pro řešení krizí. Uplatňuje se ve dvou rovinách: v běžném stavu jako součást managementu dané organizace projevující se hlavně v oblasti prevence a také za krizových situací.

Krize je složitá situace, v níž je významným způsobem narušena rovnováha mezi základními charakteristikami systému.

Krizová situace je taková mimořádná situace, v níž jsou bezprostředně ohroženy základy státu, svrchovanost, územní celistvost, chod hospodářství, státní správa a soudnictví, zdraví a život, životní prostředí. Krizový stav je stav bezpečí nouzový stav, stav ohrožení státu nebo válečný stav.

Procesní management

V procesním managementu jsou firmy budovány na principu integrace Krizová situace je taková mimořádná situace, v níž jsou bezprostředně ohroženy základy státu, svrchovanost, územní celistvost, chod hospodářství, státní správa a soudnictví, zdraví a život, životní prostředí.

Krizový stav je stav bezpečí nouzový stav, stav ohrožení státu nebo válečný stav.

Procesní management

V procesním managementu jsou firmy budovány na principu integrace četností. Dílčí operace je nutné sjednotit do ucelených podnikových procesů ovládaných týmy.

Management jakosti

Kvalita (jakost) je názor zákazníků nebo uživatelů na vlastnosti produktu nebo služby, ale i organizace či systém. Je to míru, o které jsou uživatelé přesvědčeni, že služba nebo produkt splní jejich potřeby a očekávání.

Environmentální management

Environmentální management lze definovat jako systematický přístup k péči o životní prostředí ve všech aspektech podnikání. Jeho implementace je založena na principu dobrovolnosti.

Informační (znalostní) management

Informační management využívá kvalitativně nové možnosti práce s informacemi za podpory informačních technologií v podnikovém systému řízení.

Logistický management

Logistika je vědní disciplína, která se začala používat jako vojenská teorie 19. století. V tomto systému je třeba řídit všechny jeho prvky, pracovníky, operace a to v podniku i mimo podnik.

Category management

Category management je založen na koordinaci strategie obchodníků a výrobců. Je to způsob řízení toku produktů na úrovni kategorií produktů. V tomto procesu úzce spolupracuje výrobce – dodavatel zboží – a prodejce – maloobchodník.

Brand management

Brand management je definován jako řízení značky. „Brand“ je většinou definován v atributech značky: jméno, pojem, značka, symbol, design, pověst.

Využívání moderních informačních technologií

Firma 21. století se bez využití informačních technologií nemůže obejít. Mělo by se dbát na to, aby se efektivita informačních technologií ani nepřeceňovala, ani nepodceňovala.

Ucelený systém řízení a plánování

Všechny procesy ve firmě musí být smysluplně řízeny. Systém řízení musí být jednolitý a kompaktní. Základem všech aktivit podniku je její strategie. Samotná strategie však k řízení nestačí. Záměry se musí promítnout do jednotlivých aktivit každého pracovníka.

Respektování zásad corporate governance, principů etiky, společenské odpovědnosti, bezpečnosti práce a ekologičnosti

Principy Corporate Governance zformulovala Organizace pro ekonomickou spolupráci a rozvoj (OECD) v roce 1999 v Materiálu zvaném „Zásady OECD pro řízení a správu společnosti.“ Jejich úkolem bylo přispět ke zvýšení transparentnosti, integrity, práva a pořádku.

Principy etiky by měly být vyjádřeny ve všech pravidlech, upravujících vztahy k obchodním partnerům, mezi zaměstnanci a vůči externím institucím. Měly by respektovat zákony, předpisy, pravidla vyplývající z „dobrých mravů.“ Principy společenské odpovědnosti jsou výrazem odpovědnosti firmy k veřejnosti, například dobrovolné závazky. Dodržování principů šetrného vztahu k přírodě a bezpečnosti práce je jedním z nových úkolů.

1.2 Úrovně řízení

Management je charakterizován jako ucelený soubor ověřených přístupů, názorů, zkušeností, doporučení, metod, které manažeři užívají ke zvládnutí specifických činností (manažerských funkcí), které jsou nutné k dosažení cílů organizace. Využívá teoretických poznatků ekonomie, ale také psychologie, sociologie, práva, matematiky, statistiky atd.

Řízení bývá zobrazováno jako pyramida, v níž jsou zachyceny jednotlivé hierarchické úrovně řízení. Tyto úrovně na sebe navazují, liší se z hlediska míry kompetencí, odpovědnosti, při stanovování cílů, úkolů a jejich realizaci a v časových horizontech, jimiž se zabývají.

Tabulka č.1: Druhy řízení, zdroj: vlastní zpracování

Druh řízení	Kým je prováděno	Zaměření	Úkol
Strategické	vedoucí pracovníci	soulad mezi cíli, zdroji a prostředím	formulace a kontrola strategií
Taktické	nižší úrovně organizačních jednotek (závody, provozy)	známé, opakující se problémy	rozpracování dlouhodobých cílů
Operativní	nejnižší úrovně organizačních jednotek	denně opakující se problémy	zajištění plánovaného postupu řídících procesů

Druh řízení	Záběr	Stupeň podrobnosti	Stupeň nejistoty	Stupeň neurčitosti	Detailnost	Časové určení
Strategické	široký	nízký	vysoký	vysoký	nízká	dlouhodobé (nad 1 rok)
Taktické	užší	vyšší	nižší	nižší	vyšší	střednědobé (do 1 roku)
Operativní	nejužší	nejvyšší	nejnižší	nejnižší	nejvyšší	krátkodobé

1.3 Řízení dle kompetencí

Řízení dle kompetencí je založeno na harmonickém rozvoji „tvrdých a měkkých“ aspektů podnikání. Vzniklo jako prolnutí dvou světů: cíle a požadavky na výkon a lidské zdroje. Říká se, že všechny úspěchy a neúspěchy jsou způsobeny nesprávnou definicí kompetencí lidí.

1.3.1 Primární řízení

Při primárním řízení firmy dochází k vyjasnění a srozumitelné definici dlouhodobého (strategického) směřování podniku a požadavků na výkon zaměstnanců. Představuje podmínku pro efektivní spolupráci dějů ve společnosti. Primární řízení organizace definuje lidské zdroje, zavádí jejich individuální hodnocení a zaměřuje se na jejich rozvoj. Dále také hodnotí celkový rozvoj firemní kultury.

1.3.2 Sekundární řízení

Sekundárního řízení omezuje operativní řízení a zvyšujeme kapacitu manažerů pro strategické řízení. Díky němu se zmenšuje počet kompetenčních sporů, zlepšují se mezilidské vztahy, externí a interní komunikace a spolupráce, zvyšuje se loajalita a iniciativa lidí ve firmě. Tento druh řízení se orientuje se na zákazníky, kvalitu výrobků a služeb, efektivitu inovací do rozvoje lidských zdrojů a průhlednost firmy. Pozitivní dopad má i na výši tržeb.

1.3.3 Strategie řešení

Strategie řešení se využívá na celofiremní úrovni. Používá se teorie vitality a to buď pyramida vitality, nebo pyramida kultury.

Teorie vitality

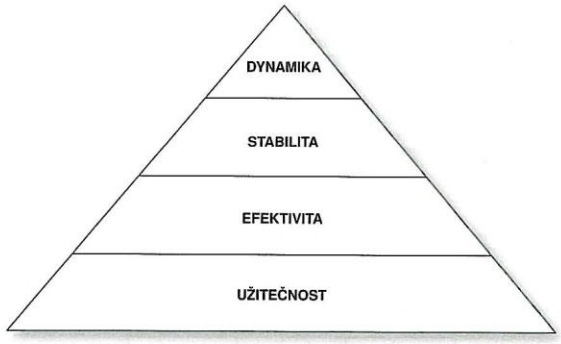
Teorie vitality byla publikována v roce 2000. Vychází ze dvou zdrojů: uplatnění zdravého rozumu a srovnávání firemních systémů s přírodními ekosystémy. Říká, že o přežití a konkurenceschopnosti firmy rozhodují 4 disciplíny: efektivita, užitečnost, stabilita,

dynamika.

Pyramida vitality

Pyramida vitality se zaměřuje na požadavky. Popisuje čtyři vitální znaky:

1) co budeme dělat;
2) jak to budeme dělat;
3) obrana při ohrožení;
4) stabilita vlastních možností.



Obrázek č.1 Pyramida vitality, zdroj: PLAMÍNEK, J, FIŠER, R. *Řízení podle kompetencí : management by competencies v praxi, strategické směrování firmy, řízení procesů a zdrojů, zvládání ohrožujících situací, rozdělení rolí a úloh, hodnocení a motivace lidí*. První vyd. Praha: Grada Publishing, 2005, strana 36.

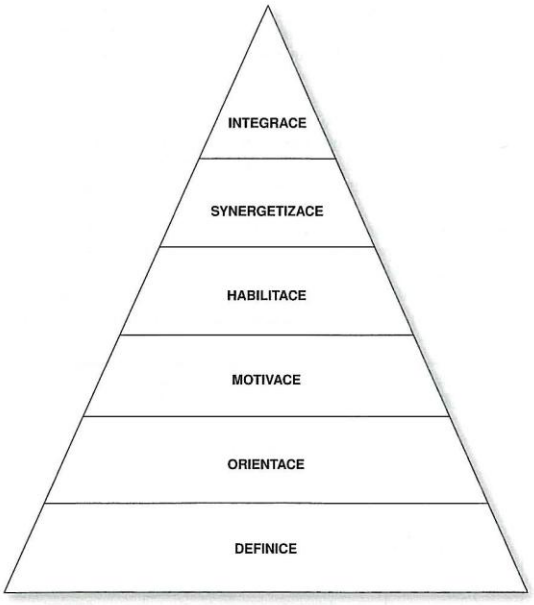
Pyramida kultury

Pyramida kultury se zaměřuje na možnosti. Shrnuje strategii péči o lidské zdroje. Má 6 pater:

1., 2., 3. spodní – usilují o loajalitu vůči firemním myšlenkám;

4., 5. - snaží se nalézt soulad mezi skutečnými a požadovanými schopnostmi lidí;

6. - vrací se k lidským vlastnostem, ty se nedají měnit, ale lze na ně působit tak, aby vygenerovaly efektivitu a nebránily úspěšnému zvládnutí konfliktů.



Obrázek č.2, Pyramida kultury, zdroj: PLAMÍNEK, J, FIŠER, R. *Řízení podle kompetencí : management by competencies v praxi, strategické směrování firmy, řízení procesů a zdrojů, zvládání ohrožujících situací, rozdělení rolí a úloh, hodnocení a motivace lidí*. První vyd. Praha: Grada Publishing, 2005, strana 42.

Strategie je pojem, který se užívá velice často i v běžném životě, většinou však nesprávně, proto je třeba ho důkladně vysvětlit.

1.4 Strategie

M. Porter: „I když se svět točí stále rychleji, bez dlouhodobé strategie není podnikatelský úspěch možný… Trvalé konkurenční výhody lze dosáhnout jen prostřednictvím strategie.“

P. Drucker: „Doba, která je před námi, bude vyžadovat, aby se vrcholové vedení nikoli méně, ale naopak ještě více zajímalo o podnik, jeho záměry, jeho priority a o jeho strategii.“

Strategie je tvůrčí unikátní dílo. Jde o proces, který představuje dlouhodobý rámec, při němž dochází k tvorbě a implementaci hlavní cílů, priorit, aktivit a rozvojových záměrů, které mají zásadní význam pro rozvoj podniku. Na úspěšnou strategii neexistuje žádný univerzální recept. Firma, která nemá kvalifikovaně formulovanou strategii a dobře fungující systém strategického řízení nemůže v současném náročném a čím dál více konkurenčním světě přežít.

Úspěšná strategie:

- má podporu vrcholového managementu podniku;
- je přátelská pro uživatele, nejen pro plánovače;
- je participativní;
- je flexibilní;
- vede k rozhodování o zdrojích;
- zapojuje a stimuluje zaměstnance;
- je dynamická a nepřetržitě inovuje;
- je proaktivní;
- dává návod na dlouhodobé řešení problému;
- dochází k návratnosti v čase.

1.4.1 Důležité charakteristiky strategie

- musí být zpracována v několika variantách (různé tempo růstu tržeb, strukturovaný výrobní program, míra specializace, podíl vyráběných výrobků na nově zaváděných, zaměření se na různé segmenty poptávky atd.), toto se dělá proto, aby nedošlo k tzv. strategickému překvapení (tzn. taková situace, kterou firma svými prostředky není schopna zvládnout);
- je založena na řadě hypotéz;
- obsahuje v sobě prvky neurčitosti;
- musí být permanentně aktualizována;
- varianty strategie musí být kompatibilní, aby nedocházelo k problémům a poklesu efektivity firmy;
- jasně definuje podnikatelský sektor, kompetence lidí, definujeme ekonomické i neekonomické přístupy, kterých chceme dosáhnout, definujeme manažerské úkoly, dává nám návod, jak selektivně investovat do hmotných i nehmotných zdrojů a zajišťuje větší konkurenceschopnost podniku;

- přizpůsobuje zdroje firmy měnícímu se okolí, zejména zákazníkům a uspokojuje očekávání zainteresovaných skupin (stockholderů a stakeholderů);
- vyjadřuje její hlavní zaměření, misi, vizi (tj. budoucí podobu), strategické cíle a strategické operace, tj. aktivity zajišťující naplnění mise, vize a splnění strategických cílů.

Vize bývá definována jako mentální model budoucího stavu procesu, skupiny nebo organizace, ale také odraz budoucnosti, který musí být srozumitelný a motivující, aby udal dlouhodobý směr pro budoucí plánování, stanovení cílů a pro silné jméno podniku. Fungující vize musí být jasná, snadnou pochopitelná, ale musí také svým způsobem provokovat lidi k účasti a ne jen k pasivnímu sledování.

Mise znamená způsob, jakým lze dosáhnout tzv. „zhmotnělé“ vize. Zabývá se současnými aktivitami podniku. Mise odpovídá na otázku „Kdo jsme a co děláme?“ Navíc obsahuje kodex chování organizace tak, aby vedl k naplnění stanovené vize. Udává jasně definovaný směr, kterým se celá organizace ubírá. Mise definuje stav společnosti, stanovuje klíčové kompetence společnosti, soustřeďuje se na hlavní aktivity, obsahuje přednosti společnosti a její plány, jak dosáhnout strategických výhod.

Strategické cíle v zásadě charakterizují stavy, kterých chce podnik dosáhnout prostřednictvím svých aktivit, dále také charakterizují, jakou konkurenční pozici bude mít podnik na trhu. Podnikové cíle dávají smysl stanovenému poslání a pomáhají při formulaci strategie. Při formulaci konkrétního cíle bychom měli dodržovat tzv. akronym „SMART.“

Akronym „SMART“

S – specifický, tzn. každý ve firmě tomu musí rozumět;

M – měřitelný, tzn. definice toho, čeho chce podnik dosáhnout a to v kvantifikovaném množství;

A – akceptovatelný, tzn. akceptovatelný těmi, kteří ho budou plnit a implementovat;

R – realistický, tzn. stanovení si dostatečně náročného cíle;

T – časově vymezený, tzn. určení času, kdy chce podnik čeho dosáhnout.

Strategie je dále ovlivňována mnoha principy, které ji napomáhají lépe definovat.

1.4.2 Principy ovlivňující strategii

Princip permanentnosti

Tento princip upozorňuje na to, že na strategii se musí stále pracovat, to je způsobeno změnami v okolí, zpětnovazebností jednotlivých strategických operací, vývojem poznatků o tom, co ovlivňuje firmu, změnami uvnitř firmy.

Princip celosvětového systémového myšlení

Tento princip předpokládá, že každý pracovník zpracovávající strategii, si uvědomuje vliv celosvětového okolí.

Princip interdisciplinárního myšlení

Tento princip vyžaduje, aby při tvorbě strategie byly využívány poznatky a metody různých vědních disciplín.

Princip tvůrčího myšlení

Tento princip klade důraz na přinášení nových, netradičních myšlenek, námětů a řešení, jeho hlavními znaky je odvaha, angažovanost pro nové myšlenky, osobité oběti.

Princip syntézy exaktního a intuitivního myšlení

Tento princip říká, že strategické řízení je založeno na kombinaci exaktních a intuitivních metod, jejich podíl se u jednotlivých součástí strategie liší.

Princip myšlení v čase

Tento princip považuje za nezbytnou charakteristiku strategického řízení dynamický pohled, protože se strategie vztahuje k dlouhému období.

Princip zpětnovazebního myšlení

Tento princip spočívá ve skutečnosti, že činnost firmy je ovlivňována stavem okolí, ale i na své okolí výrazně zpětně působí, totéž probíhá uvnitř firmy.

Princip agregovaného myšlení

Tento princip popisuje, že strategie musí být zpracována v detailním členění odpovídající potřebám taktického a operativního řízení, avšak ne zbytečně detailně.

Princip koncentrace

Tento princip klade důraz na nutnost přesného určení si strategických cílů firmy, nutná je velká důslednost a odvaha, avšak špičkových výsledků nelze dosáhnout ve všem.

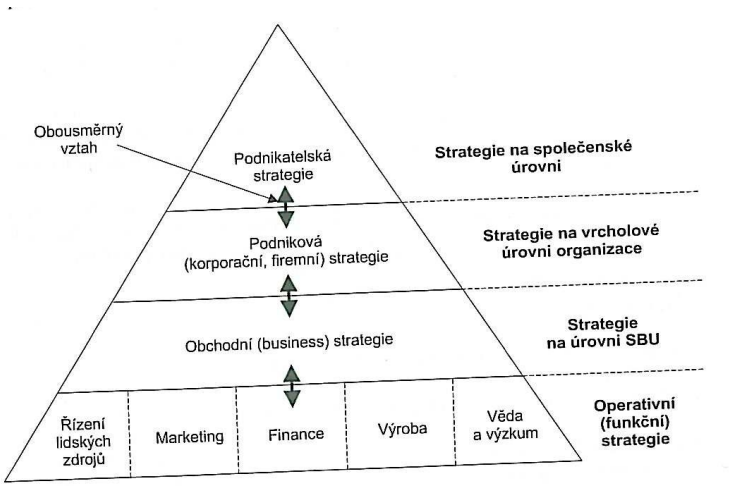
Princip etiky myšlení

Tento princip popisuje velkou roli faktorů, jako je spolehlivost, solidnost, důslednost v plnění závazků, ochota přizpůsobit se potřebám obchodních partnerů. Firma 21. století má zpracovaný etický kodex.

Princip vědomí práce s rizikem

Tento princip upozorňuje na velké riziko, které je spojeno se strategií, ale podnikání bez rizika neexistuje. Vyhlídky na úspěch se zvyšují se zvyšujícím se počtem pokusů a nových iniciativ a cíleným řízením více a méně rizikových projektů.

1.4.3 Druhy strategií



Obrázek č.3: Druhy strategií, zdroj: THADDEYUS, M. *Základy strategického řízení*. První vyd. Praha: Grada Publishing, 2007, strana 36.

a) podnikatelská

Podnikatelská strategie funguje na společenské úrovni, má odpovědnost vůči veřejnosti, ukazuje na principy, hodnoty společnosti, je odpovědná za dopady jednání vnímání společnosti ostatními.

b) podniková (korporační, celopodniková)

Podniková strategie kontroluje dodržování strategie, dává velký prostor jednotlivým podnikatelským jednotkám, řeší základní podnikatelská rozhodnutí (např.: země podnikání, prostředky k podnikání, způsobě řešení atd.).

c) obchodní

Obchodní strategie představuje strategie pro jednotlivé podnikatelské jednotky, definuje úlohy trhu, přednost soutěžení, rozhor výchozí situace, cílové pozice podniku, čas.

d) operativní

Operativní strategie pomáhá plnění strategických cílů na podnikové úrovni a úrovni strategických jednotek (př. řízení lidských zdrojů, rozvoj marketingu a výrobků, využití informačních technologií).

1.4.4 Praktické přístupy ke strategii

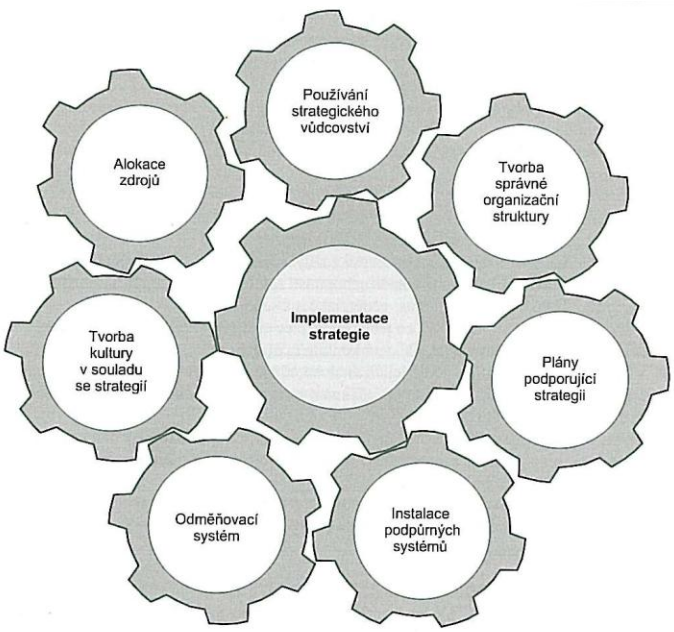
- otevírání se trhům a příležitostem, které trh nabízí;
- znalost vnějšího prostředí;
- jasný cíl;
- dobře stanovené ceny;
- komplexní a odpovědnost manažerů za procesy;
- orientace na zákazníka;
- firemní kultura;
- zaměření se na lidské zdroje.

1.4.5 Identifikace strategie

1) které aktivity jsou klíčové;
2) čeho chceme dosáhnout;
3) které produkty/služby poskytujeme;
4) na kterém trhu prodáváme;
5) vztah mezi cenou, variabilními a fixními náklady;
6) funkční politika (věda, výzkum, marketingová, prodejní, finanční);
7) politika v oblasti informační, plánování, alokace zdrojů.

1.4.6 Implementace strategie

Implementace strategie znamená její uskutečňování a zavedení do reálného života, také základní a nejdůležitější úkol top managementu firmy a východisko pro všechny aktivity organizace, což je základní plnění povinností všech pracovníků firmy.



Obrázek č.4: Implementace strategie, zdroj: THADDEYUS, M. *Základy strategického řízení*. První vyd. Praha: Grada Publishing, 2007, strana 134.

1.4.7 Kontrola a aktualizace strategie

Pověst každé firmy je velice důležitá. Kontrola vede chování zaměstnanců směrem k důležitějším cílům organizace. Kontrolní systémy monitorují, koordinují, odměňují, posilují chování a aktivity, které vedení požaduje. Kontrolní systémy se tvoří, protože strategie je zastaralá, interní i externí prostředí firmy se vyvíjí, také upozorňuje na problémy v organizaci a možnost chybných rozhodnutí v organizaci.

Kontrola strategie se zabývá posouzením efektivnosti strategie, monitorováním vývoje implementace strategie, hodnocením vnějších a vnitřních faktorů, jako například reakce konkurentů, změna slabých a silných stránek konkurentů, tržní pozice a ziskovost konkurentů, odveta konkurentů, spolupráce s konkurenty.

Formy kontroly:

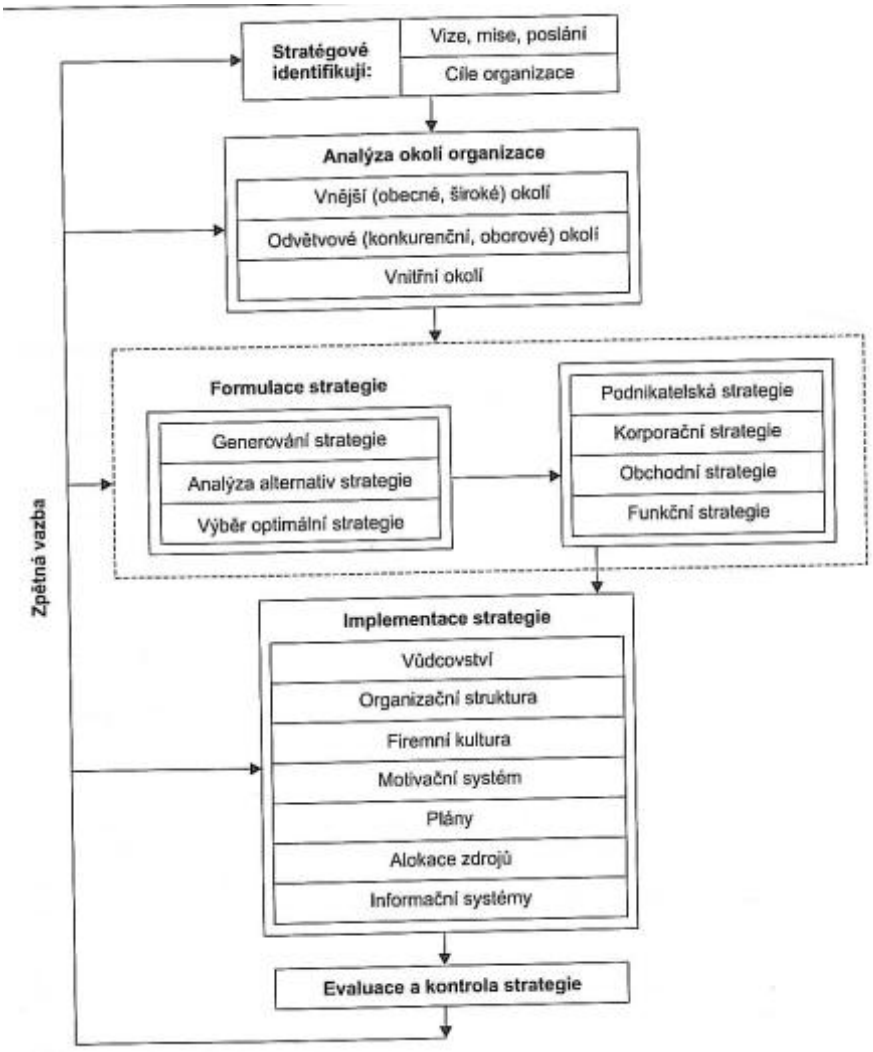
- kontrolní systémy se zaměřují na hodnocení výstupů, procesů a chování lidí;
- kontrolní systémy se zaměřují na celkovou výkonnost organizace nebo její části;
- kontrolní systémy se zaměřují na každodenní operativní aktivity.

Předpoklady pro efektivní kontrolu strategie:

- hospodárnost;
- musí mít význam;
- generovat užitečné informace;
- přinést včasné informace;
- poskytovat skutečný obraz o dění v organizaci.

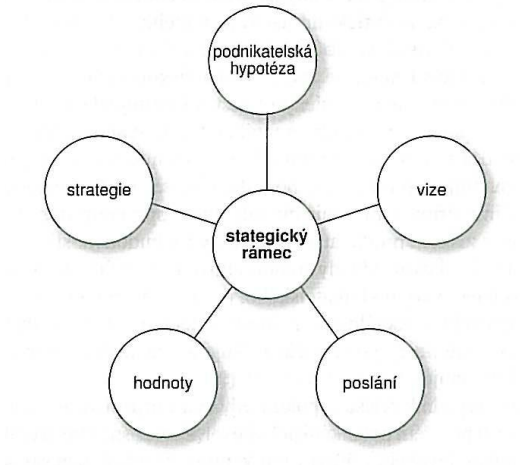
Překážkami kontroly strategie může být složitost prostředí, neurčitá budoucnost, zastaralost plánů organizace, politická situace, improvizace, nesprávná organizace, různé pohledy na situaci, nadměrná kontrola a konfliktní cíle.

Celý proces strategického řízení znázorňuje následující schéma:



Obrázek č.5: Strategické řízení, zdroj: THADDEYUS, M. *Základy strategického řízení*. První vyd. Praha: Grada Publishing, 2007, strana 24.

1.4.8 Strategický rámec



Obrázek č.6: Strategický rámec, zdroj: PLAMÍNEK, J, FIŠER, R. *Řízení podle kompetencí : management by competencies v praxi, strategické směrování firmy, řízení procesů a zdrojů, zvládání ohrožujících situací, rozdělení rolí a úloh, hodnocení a motivace lidí*. První vyd. Praha: Grada Publishing, 2005, strana 76

Strategický rámec znamená soubor firemních myšlenek. Vyplývají z něj dlouhodobé, střednědobé, krátkodobé cíle, definuje produkty/služby, procesy, zdroje, systém monitoringu, zpětnou a dopřednou vazbu, úlohy a kompetence lidí, rozvoj lidských zdrojů atd. Je tvořen lídry a managementem firmy a ohraničuje prostor pro svobodu a aktivitu manažerů. Má dvě fáze: emocionální a racionální. Důležité je i celkové myšlení managementu.

1.4.9 Strategické myšlení

Strategické myšlení není pro většinu lidí vrozené, je to cenná pomoc při životním plánování. V mnoha ohledech pomůže, ale nenahradí tvůrčí schopnosti člověka. Hranice strategií jsou totiž nevypočitatelné, neplánovatelné. Velkou a neméně důležitou roli hrají lidské emoce (marnivost, touha po moci atd.). Důležité je i to, že včerejší strategie není vhodná pro zítřejší. Nesmí se zapomínat, že hlavní roli stále hraje člověk, tedy podnikatel.

1.4.10 Podnikatel jako stratég

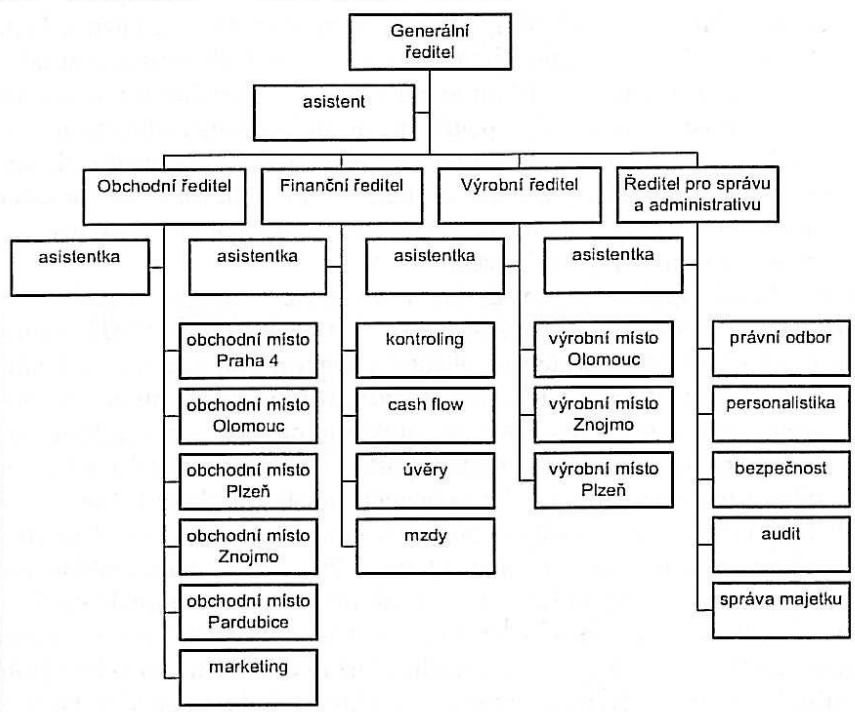
Podnikatel, který se považuje za stratéga, se často srovnává až s umělcem. Navíc musí jít ostatním příkladem, neomlouvá se za špatné výsledky a nevymlouvá se na nepřízeň okolí, okolností a nepochopení ostatních lidí.

1.5 Oblasti řízení

Řízení se dotýká všech oblastí podniku. Například oblasti finanční, personální, odbytu, marketingu, ale také oblasti bezpečnosti. Bez správně definované a řízené oblasti bezpečnosti dnes nemůže fungovat ani jeden podnik.

2 Pojetí a obecné zásady řízení bezpečnosti v podniku

Bezpečnost je téma, které pro svoje fungování musí řešit každý podnik. Není možné ho nechat svému osudu, protože by firma zbytečně vynakládala finanční prostředky. V každém podniku má toto oddělení své místo.



Obrázek č.7: Struktura společnosti, zdroj: RODRYČOVÁ, D, STAŠA, P. *Bezpečnost informací jako podmínka prosperity firmy*. První vyd. Praha: Grada Publishing, 2000, strana 24.

2.1 Bezpečnost podniku

S pojmem bezpečnost souvisí i pojem „nebezpečnost.“ Mezi hlavní faktory, které ovlivňují rozvoj firmy, patří:

- stupeň specializace;
- stupeň byrokracie;
- vztah mezi vlastnictvím a řízením společnosti.

Stále největším původcem problémů, které majitelé a vedoucí podniků řeší, jsou jejich vlastní zaměstnanci. Neinformovaný, nezodpovědný a nespolehlivý člověk dokáže

způsobit více nepříjemností, než například špatně zvolená strategie nebo nevhodný způsob řízení.

Řízení bezpečnosti má v podniku na starost tzv. „bezpečnostní management.“

2.1.1 Bezpečnostní management

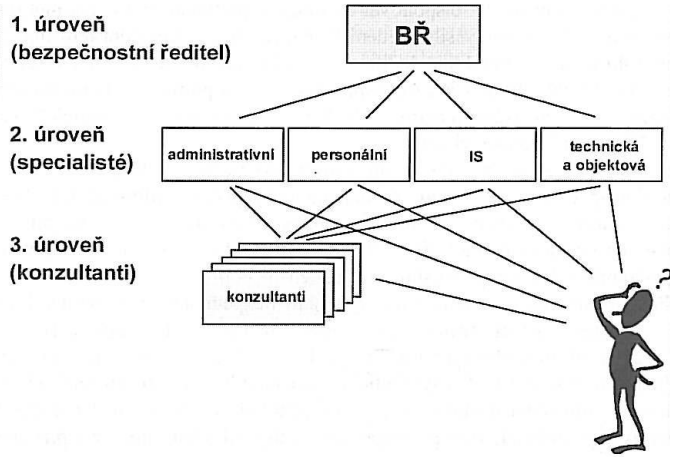
Bezpečnostní management je bezpečnostní infrastruktura, která prostupuje celou organizací a ovlivňuje chod bezpečnostních mechanismů, koriguje, vyhodnocuje funkci.

Pro co nejlepší a efektivní fungování bezpečnostního managementu musí být zajištěn přenos informací oběma směry:

- shora dolů dávat – tzn. provádět rozhodnutí, dávat pokyny, pracovat s minimálními bezpečnostními riziky, zdokonalovat systém reakce na bezpečnostní incidenty;

- zdola nahoru – tzn. dostávat informace o aktuální bezpečnosti situací, hrozbách, incidentech.

Důležité je, aby existovala „hlava“ struktury s pravomocemi a zodpovědností, která dohlíží nad uplatňováním bezpečnostní politiky, řízení a realizaci bezpečnostních projektů a samozřejmě disponuje potřebnými financemi.



Obrázek č.8: Bezpečnostní ředitel, zdroj: RODRYČOVÁ, D, STAŠA, P. *Bezpečnost informací jako podmínka prosperity firmy*. První vyd. Praha: Grada Publishing, 2000, strana 28.

V rámci bezpečnostního managementu existují tři úrovně řízení bezpečnosti:

1. **úroveň = bezpečnostní ředitel**

Bezpečnostním ředitelem je většinou vedoucí pracovník nebo přímý podřízený ředitele podniku. Tuto funkci je vhodné umístit přímo do útvaru generálního ředitele a vyžaduje plné pracovní nasazení. Jeho hlavním úkolem je prosadit bezpečnostní politiku, řídi bezpečnostní specialisty pro oblast administrativní, personální, technickou a objektovou bezpečnost, bezpečnost informačních systémů a kryptografickou ochranu. Bezpečnostní ředitel musí mít odpovídající vzdělání i praxi, znalosti z oboru bezpečnosti a také potřebuje mít přirozenou autoritu a schopnost řídit tým. Kvůli možnému výskytu utajovaných skutečností jsou nutné předpoklady pro prověření ve smyslu zákona č. 148/1998 Sb. pro potřebný stupeň kvalifikace utajovaných informací. Na osobu vykonávající tuto funkci jsou kladeny vysoké požadavky na morální vlastnosti.

2. **úroveň = bezpečnostní specialista**

Bezpečnostní specialisté jsou odborní pracovníci a každý má jinou specializaci. V podniku jsou nejčastěji bezpečnostní specialisté pro oblast administrativní, personální, technickou a objektovou bezpečnost, bezpečnost informačních systémů a kryptografickou ochranu. Tato funkce může být za určitých podmínek sdílena s jinou pracovní náplní (např. pracovník bezpečnosti pro personální oblast může zároveň přijímat nové zaměstnance). Jejich hlavním úkolem je zajistit odbornou a metodickou pomoc pracovníkům třetí úrovně řízení bezpečnostní politiky a bezpečnostních projektů. Bezpečnostní specialisté jsou povinni: zpracovat definici bezpečnostního incidentu, vyhodnotit situaci, incidenty a navrhnout opatření ke zlepšení, spolupracovat při provádění analýzy rizik a doplňovat ji.

- **bezpečnostní specialista pro personální oblast**

Bezpečnostní specialista pro tuto oblast má na starosti obsazování funkčních míst důvěryhodnými pracovníky, seznamování s citlivými informacemi pouze pověřené osoby, dohled nad personálními procedurami, vytváření a realizaci bezpečnostního vědomí a jeho ověřování pomocí externích spolupracovníků, kontrolu a metodickou pomoc konzultantům.

- **bezpečnostní specialista pro administrativní oblast**

Bezpečnostní specialista pro administrativní oblast dohlíží nad bezpečností informací při plnění obchodních funkcí, ochranu citlivých informací firmy, kontrolu a metodickou pomoc konzultantům, tvorbu a úpravu vnitřních předpisů, zajišťování manipulace s informacemi ve smyslu zákona č. 148/1998 Sb.

- **bezpečnostní specialista pro objektovou a technickou oblast**

Náplní práce bezpečnostního specialisty pro objektovou a technickou oblast je zabránění nepovolaným osobám v přístupu do objektů a prostor, ohrožení bezpečnosti informací při ukládání a manipulaci s informačními systémy, vybírá technické prostředky k zajištění bezpečnosti informací, určuje způsob ověřování účinnosti technických prostředků, kontroluje, poskytuje metodickou pomoc konzultantům, zajišťuje předepsanou úpravu informací ve smyslu zákona č. 148/1998 Sb. Má také na starosti: klasifikaci objektů dle důležitosti, stanovení hranic objektů, ochranu objektů, úschovné objekty, zámky, mříže, fólie, skla, prokazování totožnosti, výstražné systémy, detektory střeliva a výbušnin…

- **bezpečnostní specialista pro oblast pro bezpečnost informačních systémů**

Tento bezpečnostní specialista se v podniku zabývá prosazením systému zabezpečení citlivých informací, kontrolou a metodickou pomocí konzultantům, ochranou informací ve smyslu zákona č. 148/1998 Sb., vyhlášky NBÚ č. 56/1999 Sb.

- **bezpečnostní specialista pro oblast kryptografické ochrany**

Funkce tohoto bezpečnostního specialisty je v mnoha podnicích spojována s funkcí bezpečnostního specialisty pro oblast bezpečnosti informačních systémů, protože tyto dvě oblasti spolu úzce souvisí. Náplní práce specialisty pro oblast kryptografické ochrany je návrh a prosazení systému správy a manipulace s klíčovými materiály, zřízení a provoz režimových pracovišť, kontrola a metodická pomoc konzultantům, ochrana informací ve smyslu zákona č. 148/1998 Sb.

První dvě úrovně jsou za bezpečnost „placeni."

3. **úroveň = bezpečnostní konzultant**

Tato funkce je funkce „čestná" odměna z fondu bezpečnostního ředitele, zabývá se bezpečností mimo své pracovní povinnosti, předpokládá se, že zároveň zvládá plnění

dalších pracovních úkonů. Jeho posláním je, co nejvíce se přiblížit obyčejným uživatelům informací. Bezpečnostní konzultant zodpovídá za monitorování bezpečnosti situace v oboru svého pracovního zařazení, sbírá informace o bezpečnostní situaci a distribuuje je dál bezpečnostnímu managementu až koncovým uživatelům. Dále také poskytuje základní bezpečnostní konzultaci při běžném provozu i bezpečnostních incidentech. V každém podniku musí být zajištěna jeho dosažitelnost (každý pracovník se může obrátit na bezpečnostního konzultanta) z každého pracoviště v běžnou pracovní dobu.

2.1.2 Řešení bezpečnosti

Tabulka č.2: Řešení bezpečnosti, zdroj: Zpracováno dle RODRYČOVÁ, D, STAŠA, P. *Bezpečnost informací jako podmínka prosperity firmy*. První vyd. Praha: Grada Publishing, 2000, strana 56.

Interní a externí řešitel bezpečnosti	
Výhody	Nevýhody
Externí řešitel (dodavatel) bezpečnosti	
nezávislost a vnější pohled	nutnost přiznat potřebu externího řešitele
Metodologie	nutnost výběru externí firmy
zkušenost specializovaných řešitelů	potřeba reálných financí
zdroje pro řešení (lidé, HW, SW, nástroje)	neznalost prostředí
kooperace s experty i ve světovém měřítku	zpřístupnění citlivých informací
neexistují vazby na prostředí	
Interní řešitel bezpečnosti	
neformální vztahy	ovlivnitelnost řešitelského týmu
metody prosazení, spojenci	menší rychlost, kvalita, efektivita
interní financování	

2.1.3 Hodnocení bezpečnosti

Hodnocení bezpečnosti vyžaduje stanovit kritéria, podle nichž bude hodnocení probíhat. Kritéria mohou mít obecnou či speciální povahu.

a) standardní kritéria

Předpokládá se, že každý systém musí vyhovovat zákonným a podzákonným normám platným pro jejich provoz. S postupem do Evropy se musíme přizpůsobit i dalším normám (např. NCS – USA, ITSEC, ITSEM…).

b) jednorázové hodnocení – audit

Auditu se nejlépe zhostí specializovaná nezávislá organizace. Je však nutné si zvolit důvěryhodnou firmu. V nejjednodušším případě je verdikt: „vyhovuje, vyhovuje s výhradami a nevyhovuje.“ Bezpečnostní management má trvalý dohled nad bezpečností, avšak dle zkušeností lepší hodnocení poskytuje útvar typu audit. Ten má potřebnou míru nezávislosti a dostatek zkušeností.

1. stanovení kritérií pro výběr hodnotící organizace (důvěryhodnost, kvalifikace, znalost prostředí…)

2. určení formy výběru hodnotící organizace (výběrové řízení, inzerát, přes odbornou asociaci atd.)

3. výběr hodnotící organizace

4. stanovení podmínek (předmět hodnocení, termín hodnocení, podmínky, spolupráce, forma a obsah dokumentů, forma a obsah závěrečného dokumentu atd.)

5. příprava podkladů pro hodnocení (tzn. splnění podmínek hodnotitele, obsahuje podklady: Celková bezpečnostní politika, Systémová bezpečnostní politika, dále může dokumenty organizační povahy, dokumenty o IS…)

6. realizace podmínek pro výkon hodnocení (pověření pracovník zadavatelské organizace zkontroluje splnění podmínek pro zahájení hodnocení a materiál se předá hodnotiteli)

7. vlastní hodnocení externí organizací

8. oponentura závěrečného dokumentu z hodnocení

9. přijetí opatření a jejich realizace

10. opakované hodnocení dopadu realizovaných opatření (= nové hodnocení bezpečnosti IS)

c) průběžné hodnocení

Průběžné hodnocení zahrnuje analýzu, řešení, návrh systému, integraci, implementaci k provozu, nad tím vším je neustálé hodnocení probíhajících fází jako zpětná vazba, která zajišťuje stabilitu a funkčnost systému.

2.2 Pojetí bezpečnosti podniku

Každý podnik řeší bezpečnost v takové míře, která odpovídá jeho předmětu podnikání, velikosti, stylu řízení atd.

Většina podniků se nejvíce zabývá tématy jako jsou: informační bezpečnost, ochrana osobních údajů a bezpečnost a ochrana zdraví při práci.

2.2.1Informační bezpečnost

Informační bezpečnost je téma, které se čím dál více dotýká nás všech a všude. Kromě dat na firemních a osobních PC se dnes útoky zaměřují také na „chytré telefony“ a různá přenosná média. Jak ale toto nebezpečí řešit? Nejjednodušší metodou je, tyto prostředky vůbec nevyužívat. To je však v praktickém životě téměř nemožné. Rozvoj informační bezpečnosti je nejvíce patrný při stále častějšímu a potřebnějšímu využívání sítě Internet. Navíc se stále rozšiřuje konkurence, což si žádá změnu chování podnikatelů, státních podniků, bankovního sektoru i ozbrojených sil. Je nutné brát na vědomí, že informace tvoří aktivum organizace. Informace představují zboží s vysokou tržní hodnotou a jejich cena díky vývoji neustále vzrůstá.

Bezpečnost informací se dnes často chápe jako problém počítačových odborníků, přitom informace v tomto směru jsou jen částí toho, co pojem informace znamená. Informační bezpečnost není jednorázová činnost, ale dlouhodobá aktivita, velice důležitý je i vývoj v čase, dříve bylo předmětem zájmu připojení k Internetu, dnes už mezi priority patří užívání elektronického podpisu.

Informace

Informace je aktivum organizace a má svoji hodnotu. Vyskytuje se v různých podobách na různých místech firmy. Vlastník (majitel) informace ví, jaká je její hodnota. Ostatní zúčastnění v procesu jsou uživatelé informace, ti musí tuto skutečnost přijmout. Ohodnocení informace není práce lehká, musí ji provézt majitel informace. Realizace bezpečnosti není levná záležitost.

Bezpečnost informací v ČR

Od roku 1999 probíhá v ČR každé 2 roky průzkum stavu bezpečnosti informací. Přičemž respondenty jsou organizace se sídlem v ČR a s více než 100 kmenovými zaměstnanci.

Hlavním problémem v ČR je nízké bezpečnostní povědomí, předpokládá se, že ho firmy budou snižovat. Podniky se také často potýkají s nedostatkem kvalifikovaných pracovníků.

V rámci bezpečnostní politiky se bude využívat model střední úrovně (ne příliš stručné, ani rozsáhlé).

Bezpečnost informací světově

Bezpečnost informací je tématem téměř každé mezinárodní konference a to hlavně kvůli stále častějšímu výskytu teroristických útoků. Pravidelně se provádí analýza rizik a zvýšila se ochrana před havarijními situacemi. Pomalu se mění i postoj odběratelů. Ti dnes dávají přednost dodávkám komplexního řešení bezpečnosti před dodávkou dílčích řešení.

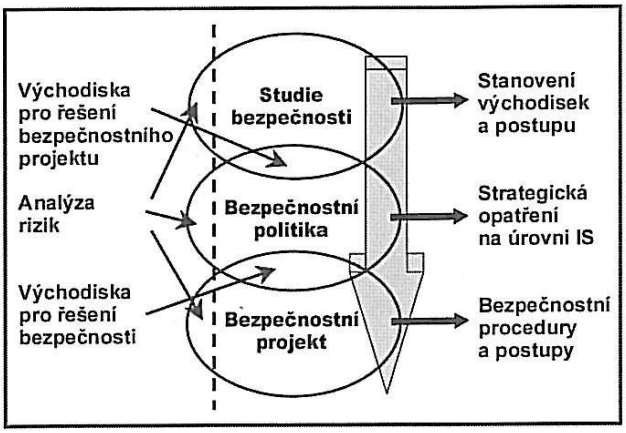
Přínosy řízení bezpečnosti pro organizaci:

- zvýšení efektivnosti hlavních procesů;
- zvýšení konkurenčních výhod organizace;
- vytvoření provozního prostředí zaručujícího bezpečnost informací a ochranu soukromí;
- snížení rizik souvisejících s únikem, nedostupností a ztrátou;

- optimalizace nákladů;
- úspora nákladů souvisejících s bezpečnostními incidenty;
- úspora nákladů souvisejících s výpadkem informačního systému;
- optimalizace nákladů při obnově chodu informačního systému;
- prokázání úsilí o ochranu dat klientům, partnerům, veřejnosti, státní správě;
- zvýšení bezpečnostního povědomí u pracovníků;
- zlepšení prezentace organizace navenek.

Řešení bezpečnosti informací

Při řešení bezpečnosti jsou důležité tři kroky, které jsou znázorněny na následujícím schématu:



Obrázek č. 9: Řešení bezpečnosti informací, zdroj: RODRYČOVÁ, D, STAŠA, P. *Bezpečnost informací jako podmínka prosperity firmy*. První vyd. Praha: Grada Publishing, 2000, strana 24.

Studie bezpečnosti

Studie bezpečnosti je východiskový dokument, znamená „inventura“ dosaženého stavu informační bezpečnosti.

Bezpečnostní politika

Bezpečnostní politika představuje soubor kritérií pro aplikaci bezpečnostních služeb, definuje pravidla, směrnice, zvyklosti bezpečnosti informací, jasně formuluje směřování bezpečnosti informací podniku. Bezpečnostní politiku je nutné pravidelně kontrolovat (kvůli posouzení její vhodnosti, přiměřenosti, efektivnosti). Pro její efektivnost musí být informace definovány jako aktiva a určena zodpovědnost za jejich ohodnocení. Závěrečný dokument „celková bezpečnostní politika organizace“ je hlavním souborem kritérií pro hodnocení IS na úrovni vrcholového managementu.

Bezpečnostní politika se dělí na dvě části, celkovou a systémovou.

Bezpečnostní politika odpovídá na následující otázky:

- Co musí být chráněno?

- Kdo nese zodpovědnost?

- Kdy to bude efektivní?

- Jak to bude vynuceno?

- Kdy a jak to bude uvedeno do praxe?

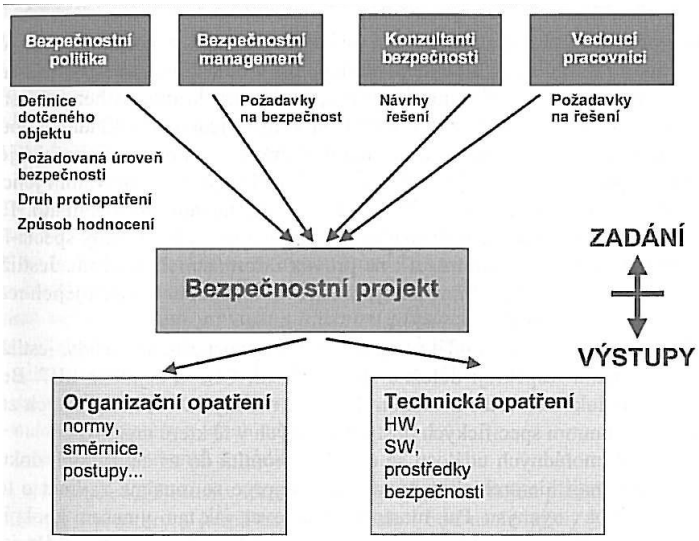
Občas nastává problém, že bezpečnostní cíle nejsou totožné s cíli obchodními. Je nutné, aby bezpečnostní řízení bylo vstřícné k cílům obchodním.

Bezpečnostní řízení není nejdůležitějším produktem organizace, ale jen postupným krokem ke stabilizaci obchodních aktivit.

Bezpečnostní projekt

Bezpečnostní projekt se skládá z více částí, z nichž každá má na starost realizaci samostatné oblasti bezpečnosti (např. oblast administrativní či personální). Představuje konkrétní požadavky na provedení konkrétních činnosti.

Vstupy dává: bezpečnostní politika, bezpečnostní management, konzultanti bezpečnosti a všichni vedoucí pracovníci.



Obrázek č. 10: Bezpečnostní projekt, zdroj: RODRYČOVÁ, D, STAŠA, P. *Bezpečnost informací jako podmínka prosperity firmy*. První vyd. Praha: Grada Publishing, 2000, strana 30.

Nosným pilířem je analýza rizik.

Ve všech fázích bezpečnostního procesu probíhá nepřetržité hodnocení všech aktivit.

Analýza rizik

Riziková analýza má za úkol zjistit jakými riziky jsou informační aktiva ohrožena. Její výsledky jsou jedním z nejutajovanějších dokumentů, protože jsou vlastně návodem, jak organizaci poškodit nebo dokonce zlikvidovat

V rámci analýzy rizik mohou nastat tři různé situace:

- A velké následky, malá pravděpodobnost vzniku,

- B velké následky, velká pravděpodobnost vzniku,

- C malé následky, velká pravděpodobnost vzniku

- D úkolem nás je dostat se při řešení bezpečnosti na místo D, tzn. zvládnout a odhalit rizika.

Realizace bezpečnostních opatření v rámci informační bezpečnosti

Při realizaci bezpečnostních opatření se postupuje podle ISO/IEC 27002:2005- Soubor postupů pro řízení bezpečnosti informací. Tato norma obsahuje 133 bezpečnostních opatření rozdělených do 11 oblastí.

Organizace bezpečnosti informací

Organizace bezpečnosti informací znamená struktura pro řízení bezpečnosti informací. Zaměřuje se na interní nebo externí subjekty.

V rámci interní organizace bezpečnosti informací je důležitá podpora bezpečnosti vrcholovým vedením, koordinace, upřesnění rolí, odpovědností a pravomocí, uzavírání dohod se všemi subjekty o ochraně důvěrných informací, udržování kontaktů na orgány veřejné moci a na zájmové skupiny. Doporučuje se také využívat nezávislý prvek, který by prováděl nezávislé kontroly bezpečnosti a zhodnocoval současný stav.

V rámci externí organizace bezpečnosti informací jde o definování pravidel pro zajištění bezpečnosti informací u externích subjektů, důraz se klade na identifikaci rizik a uzavírání dohod s jednotlivými subjekty, například pro přístup ke klientům atd.

Řízení aktiv

Při řízení aktiv dochází k udržování přehledu o existujících aktivech organizace a stanovení odpovědnosti za udržování požadované míry ochrany těchto aktiv, důležitá je evidence aktiv zajišťující přehled, vlastnictví aktiv a také přípustné použití aktiv.

Bezpečnost informací z hlediska řízení lidských zdrojů

Bezpečnost z hlediska řízení lidských zdrojů vyžaduje vymezení povinností za ochranu informací u všech pracovníků a také zajištění bezpečnostního podvědomí. Základem je stanovení a následná dokumentace bezpečnostních rolí a odpovědností podle požadavků bezpečnostní politiky, pro zajištění přiměřené úrovně bezpečnosti je nutné provádět prověrky nových pracovníků (identita dle dokladů, dokladů o vzdělání, osobní profil, trestní bezúhonnost)

Fyzická bezpečnost a bezpečnost prostředí v rámci informační bezpečnosti

Fyzická bezpečnost a bezpečnost prostředí určuje pravidla pro přístup osob do klíčových prostor a ochrana zařízení. Dále zahrnuje ochranu podniku jako celku a jeho jednotlivých prvků. Řadí se do ní vytvoření fyzického bezpečnostního perimetru (zdi, ploty, mříže, signalizace vniknutí…), kontrola fyzického vstupu (identifikace a označení osob, doprovázení návštěv…), mít dobře zajištěnou např. ohlašovnu požáru, vodu, ….)

Řízení komunikací a řízení provozu

Řízení komunikací a řízení provozu zajišťuje spolehlivý a bezpečný chod produkčních informačních a komunikačních systémů a sledování způsobu využívání dostupných prostředků. Jde o stanovení rozumných provozních procesů, postupů, odpovědností a pravomocí, dokumentace důležitých provozních předpisů, řízení provozních změn, řízení dodávek a služeb třetích osob (outsourcing).

Outsourcing je takový stav, kdy vstup, který by jinak organizace získala ze svých zdrojů, koupí od jiného subjektu jako službu nebo zboží. Při outsoucingu je běžné přesunutí veškeré zodpovědnosti za funkčnost outsourcingované služby na externí firmu tuto službu provádějící.

Součástí řízení provozu a komunikací je i ochrana proti škodlivým programům (antivirová ochrana), zálohování, zajištění správy bezpečnosti komunikační sítě, bezpečnost při zacházení s médii, elektronická výměna informací, služby elektronického obchodu, monitorování provozu informačních sítí.

Řízení přístupu v informačních a komunikačních systémech

Řízení přístupu určuje pravidla pro přidělování přístupu ke všem prostředkům informačních a komunikačních systémů a sledování způsobu využívání dostupných prostředků. Jedná se o stanovení politiky řízení přístupu, která by měla zasahovat do všech informačních systémů a aplikací, řízení uživatelské identity v informačním prostředí (každý uživatel by měl mít jedinečnou identitu), odpovědnost uživatelů (ochrana přístupových hesel, ochrana zařízení, „zásada prázdného stolu a prázdné obrazovky =

zabránění úniku informací tím, že nikdo nepovolaný na jejich pracovním stolu neuvidí, na čem pracují).

Akvizice, vývoj, údržba informačních systémů

V tomto bodu dochází k prosazení principů bezpečnosti informací do různých projektů a k definici bezpečnostních požadavků informačních systémů, zajištění správného zpracování dat v aplikacích.

Zvládání bezpečnostních incidentů

Pro úspěšné zvládnutí bezpečnostních incidentů je důležité jasně definovat pravidla a postupy pro řešení incidentů a shromažďování důkazů. Zahrnuje oblast uživatelskou, kde se jedná o hlášení všech bezpečnostních událostí a oblast odbornou, kde by se měly postihovat všechny bezpečnostní incidenty.

Řízení kontinuity činností organizace

Řízení kontinuity činností organizace zabezpečuje prevenci a minimalizaci škod plynoucích pro organizaci z havárií, živelných pohrom a dalších mimořádných událostí.

Soulad s požadavky

Při prokázání souladu s požadavky musíme doložit naplnění požadavků plynoucích z právních, smluvních a dalších závazků.

Soulad s právními normami

Při řešení informační bezpečnosti je nezbytné dodržovat právní normy, které s touto oblastí souvisí. Jedná se o ochranu duševního vlastnictví, záznamů organizace, osobních údajů, prevenci zneužití prostředků pro zpracování informací, kryptografická opatření.

(z.č. 121/200 Sb. o právu autorském a právech souvisejících s právem autorským, z.č. 499/2004 Sb. o archivnictví a spisové službě, z.č. 101/2000 Sb. o ochraně osobních údajů,

z. č. 127/2005 Sb. o elektronických komunikacích, listina základních práv a svobod, z.č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti)

2.2.2 Ochrana osobních údajů

Ochranou osobních údajů se zabývá Zákon č. 101/2000 Sb., o ochraně osobních údajů ve znění pozdějších předpisů. V souvislosti s tímto zákon byl zřízen Úřad pro ochranu osobních údajů se sídlem v Praze. Plní především funkci dozorového úřadu pro oblast ochrany osobních údajů.

Osobním údajem je myšlena jakákoliv informace, která se týká určeného nebo určitelného subjektu (subjektem je fyzická osoba, k níž se údaje vztahují) údajů. Citlivý osobní údaj vypovídá o národnostním, rasovém, etnickém původu, politických postojích, členstvích, zdravotním stavu, sexuálním životě atd. Tyto údaje lze zpracovávat pouze se souhlasem subjektu údajů, dále pak když je to souvisí s životem a zdravím subjektu, jde o zjišťování zdravotní péče, ochrany veřejného zdraví, sledují se politické, filosofické, náboženské či odborové cíle prováděné v rámci oprávněné činnosti.

Za zpracování osobních údajů je odpovědný správce, který stanovuje účel zpracování, prostředky a způsob zpracování, shromažduje osobní údaje, uchovává je pouze po dobu, která je nezbytná k účelu jejich zpracování. Správce je povinen tyto údaje zabezpečit proti neoprávněnému přístupu, změně, zničení, ztrátě, přenosům či dalšímu zpracovávání.

2.2.3 Bezpečnost a ochrana zdraví při práci

Zabývá se jím Systém řízení bezpečnosti a ochrany zdraví při práci (BOZP).

Tento systém by měl být zaveden z důvodů právních, etických, pracovněprávních, finančních, umožňuje rozpoznávat a řídit bezpečnostní a zdravotní rizika, snižovat pravděpodobnost nehod a úrazů, zvyšovat produktivitu práce a celkovou výkonnost. Zavedením tohoto systému dojde k identifikaci, vyloučení a snížení zbytečných a nepřijatelných rizik pro zaměstnance. Dalšími jeho přínosy jsou zjištění úrovně dodržování bezpečnosti práce a stanovení přiměřených cílů, zajištění dodržování bezpečnosti a ochrany zdraví při práci u externích dodavatelských organizací, srovnatelnost a kontrola úrovně ochrany zdraví při práci a pružnost reakce na změny.

Nejrozšířenější je směrnice OHSAS 18001 (Occupational Health and Safety Assessment Series)

- Zabývá se identifikací nebezpečí, právními požadavky, cíli a programy BOZP, zdroji, rolemi, odpovědností, pravomocemi, výcvikem, odbornou způsobilostí, konzultacemi, komunikací, provozním řízením, přípravou na nouzové situace a reakcí na ně, měřením výkonnosti, monitorováním a zlepšováním.

V ČR existuje Národní politika bezpečnosti a ochrany zdraví při práci ČR, odpovědný orgán je Rada vlády pro BOZP. Existuje také program Bezpečný podnik, který vychází z principů a zásad stanovených pro systémy řízení BOZP.

2.3 Zásady řízení bezpečnosti podniku

V současné době existuje program Bezpečný podnik. Cílem tohoto programu je zvýšit u právnických a podnikajících fyzických osob úroveň bezpečnosti a ochrany zdraví při práci, včetně ochrany životního prostředí. Výsledkem má být vyšší úroveň kultury práce, prevence pracovních rizik, lepší pracovní pohoda, vyšší produktivita práce a v neposlední řadě i k větší konkurenceschopnosti právního subjektu. Garantem programu Bezpečný podnik je Český úřad bezpečnosti práce.

Vlastní program je založen na zavedení efektivního způsobu řízení bezpečnosti práce – bezpečnostního managementu, integraci řízení bezpečnosti a ochrany zdraví při práci a ochrany životního prostředí s ostatními řídícími akty podniku, spolupráci zaměstnanců s vedením podniku při zvyšování úrovně bezpečnosti práce a metodické podpoře orgánu státního odborného dozoru nad bezpečností práce podnikům přihlášeným do programu.

Výsledkem je, že bezpečný podnik efektivně využívá všech existujících organizačních prvků, složek i postupů, vytváří systém, který bude pružně reagovat na změny uvnitř i mimo podnik, vytváří funkční vazby, které zajišťují adaptaci i samoregulaci systému řízení bezpečnosti.

3 Profil společnosti ČSOB Pojišťovna, a. s.

V současné době je ČSOB Pojišťovna univerzální pojišťovnou. Její obchodní profil zahrnuje tyto segmenty: fyzické osoby, malé a středně velké podniky, korporátní klientelu, nebankovní finanční instituce, finanční trhy a privátní bankovnictví

3.1 Základní údaje o společnosti

ČSOB Pojišťovna čerpá díky své akcionářské struktuře (75 % akcií vlastní belgická pojišťovna KBC Verzekeringen NV, 25 % Československá obchodní banka, a.s.) nejen z bohatých znalostí evropské nadnárodní skupiny KBC, jejíž kořeny sahají až do roku 1883, ale i z dlouholetých zkušeností celé Skupiny ČSOB. Přímé propojení české a belgické pojišťovny zrychluje transfer know - how z tradičních trhů EU do České republiky v oblasti produktů, křížového prodeje pojišťovacích a bankovních služeb a také v řízení kvality zákaznických služeb. Základ Skupiny ČSOB tvoří Československá obchodní banka – největší domácí banka, která na českém trhu úspěšně působí už od roku 1964.

Její členství v silné finanční skupině ČSOB zajišťuje klientům komplexnost a kvalitu poskytovaných služeb srovnatelnou se zeměmi EU.

3.1.1 Produkty (tzn. služby, které mohou zákazníci využívat) společnosti

- pojištění osob (úrazové, životní);
- vozidel (povinné ručení, havarijní pojištění);
- cestovní pojištění;
- pojištění majetku a odpovědnosti (domácnosti, rodinných domů, bytů, chat, chalup, odpovědnosti při výkonu povolání, odpovědnosti za škodu,);
- pojištění pro firmy (pojištění podnikatelských rizik, životní pro zaměstnavatele).

On – line služby

- výpočet pojistného;
- hlášení pojistné události životního a neživotního pojištění;

- cestovní pojištění, povinné ručení, pojištění domácností;
- komfortní vyúčtování.

3.1.2 Struktura společnosti

- **představenstvo;**
- **dozorčí rada;**
- **management společnosti:**

- generální ředitel a ředitel obchodní divize;
- náměstek generálního ředitele;
- ředitel divize životního pojištění;
- ředitel divize neživotního pojištění;
- ředitel divize finanční;
- ředitel divize IT.

3.1.3 Externí partneři společnosti

ZFP akademie

Společnost ZFP akademie se zabývá finančním poradenstvím pro domácnosti i firmy. Pro občany České republiky nabízíme výhodné sociální, spořící a pojistné programy.

ČSOB Group

Skupina KBC

Belgická finanční skupina KBC Group NV vznikla v roce 1998 sloučením aktivit pojišťovny ABB a bankovních skupin Kredietbank a CERA Bank.

Skupina KBC patří mezi tři největší bankovní a pojišťovací společnosti v Belgii, která je jejím hlavním, domácím trhem. Zároveň se KBC Group řadí mezi největší finanční skupiny ve střední Evropě, kde kromě ČSOB Pojišťovny a Československé obchodní banky ovládá i řadu dalších pojišťoven a bank v Maďarsku, Polsku, na Slovensku a ve

Slovinsku. Skupina KBC dnes působí ve více než 30 zemích a zaměstnává více než 50 000 lidí.

Československá obchodní banka

ČSOB byla založena v roce 1964. Do roku 1989 se soustředila hlavně na financování podniků zahraničního obchodu a na cizoměnné služby. Dnes je ČSOB univerzální bankou, která nabízí své produkty a služby na úrovni evropských standardů všem typům klientů: od studentů po důchodce, od drobných živnostníků po nadnárodní korporace, kteří u ní nacházejí přesně to, co potřebují.

Od června 1999 ČSOB působí ve spolupráci a v koordinaci s novým majoritním vlastníkem, který ji po úspěšné privatizaci stojí po boku: belgická KBC Bank je součástí finanční skupiny KBC Group. Po strategickém spojení s Investiční a poštovní bankou v červnu 2000 vznikla nejsilnější banka v České republice a ve střední a východní Evropě s bezkonkurenčním kapitálovým vybavením.

Hypoteční banka

Hypoteční banka (bývalá Českomoravská hypoteční banka, a.s.), působí od roku 1994 jako jediná specializovaná hypoteční banka s celostátní působností. Jako první česká banka získala 14. 9. 1995 licenci k provozování hypotečních obchodů. Na základě využití mezinárodních zkušeností zavedla velmi dobrou progresivní organizaci své obchodní sítě a v krátké době získala jednoznačně vedoucí postavení na českém trhu hypoték.

ČSOB Leasing

ČSOB Leasing jako univerzální leasingová společnost poskytuje komplexní finanční služby podnikatelským i nepodnikatelským subjektům za účelem financování všech druhů nových i ojetých dopravních prostředků a dále strojů, zařízení, investičních celků a výpočetní techniky. Již od roku 2001 je ČSOB Leasing s nejvyšším tržním podílem nepřetržitě lídrem leasingovho trhu.

ČSOB Penzijní fond Stabilita

ČSOB Penzijní fond Stabilita (dříve Českomoravský penzijní fond) je určen klientům starším 45 let upřednostňujícím kratší dobu spoření, stabilní výnos a zázemí čtvrtého největšího penzijního fondu u nás. PF Stabilita je univerzálním penzijním fondem a

poskytuje všechny druhy penzí a dalších dávek, které může penzijní fond v České republice poskytovat.

ČSOB Penzijní fond Progres

ČSOB Penzijní fond Progres je vhodný pro mladší klienty, kteří chtějí déle spořit. Tento fond nabízí svým klientům nadprůměrné zhodnocení, a to v delším časovém horizontu.

ČSOB factoring

ČSOB Factoring (dříve O.B. Heller) poskytuje finanční služby v oblasti tuzemského, exportního a importního factoringu. Jedná se o financování krátkodobých pohledávek, které vznikají z dodávek zboží či poskytování služeb na nekrytý obchodní úvěr, na základě jejich postoupení factoringové společnosti. Součástí této finanční služby je komplexní správa pohledávek včetně jejich upomínání a inkasa, přebírání rizika neplacení odběratelů a konzultační činnost vedoucí k eliminaci vzniku problematických či těžko dobytných pohledávek.

ČSOB investiční společnost

ČSOB Investiční společnost (dříve OB Invest) je významnou investiční společností, která nabízí možnost zhodnocovat úspory investicemi do rodiny otevřených podílových fondů ČSOB. Otevřené podílové fondy jsou investicí, která dlouhodobě přináší vyšší výnosy než klasické bankovní vklady.

ČSOB Asset management

Společnost vznikla v roce 1995 jako součást skupiny Patria Finance a již od svého vzniku se řadila mezi přední obhospodařovatele aktiv v České republice.

Poštovní spořitelna

Poštovní spořitelna je druhá největší banka v ČR v počtu klientů. Své bankovní služby nabízí více než dvěma miliónům klientů v nejhustější síti obchodních míst a za nejvýhodnější poplatky.

Českomoravská stavební spořitelna, a.s.

Českomoravská stavební spořitelna je největší a nejvyhledávanější tuzemskou stavební spořitelnou. V současnosti eviduje 1,3 milionů platných smluv ve spořící nebo úvěrové fázi.

Na českém finančním trhu působí ČMSS od roku 1993. Tržní podíl ČMSS dosahuje téměř 40 %. Do tohoto postavení ji nominovaly především profesionalita, široce dostupný a vstřícný klientský servis, nejširší prodejní síť, dobré hospodářské výsledky a odpovědná správa svěřených prostředků.

3. 2 Historie společnosti

Současná ČSOB Pojišťovna vznikla prodejem podniku mezi IPB Pojišťovnou, a.s. a ČSOB Pojišťovnou, a.s., ke kterému došlo 1. 1. 2003.

Historie IPB Pojišťovny

IPB Pojišťovna, a.s. byla založena v roce 1992 tehdejší Investiční bankou, a.s. a byla tak jednou z prvních tuzemských pojišťoven, které po demonopolizaci českého pojišťovnictví vstoupily na trh.

Historie ČSOB Pojišťovny

ČSOB Pojišťovna, a.s. byla založena v roce 1994 pod názvem Chmelařská vzájemná pojišťovna a působí na trhu od roku 1996.

V roce 1998 vstoupil do společnosti strategický partner KBC Insurance N.V. a v roce 2001 se stal jejím 100% vlastníkem. V souvislosti s tím změnila Chmelařská pojišťovna název na ČSOB Pojišťovna.

3. 3 Pozice na trhu

Rok 2009 můžeme z pohledu ČSOB Pojišťovny, a. s., člena holdingu ČSOB, hodnotit jako příznivý. ČSOB Pojišťovna vytvořila podle českých účetních standardů čistý zisk 1,426 miliardy korun. V tempu růstu předepsaného pojistného držela společnost krok s celým tuzemským pojistným trhem a potvrdila také své postavení čtvrté největší pojišťovny v ČR, přičemž její odstup od místa třetího se opět zmenšil.

Souhrnný objem předepsaného pojistného loni stoupl o 1,6 % na 9,638miliardy korun, a protože v podstatě stejně rychle rostl i trh jako celek, zůstal tržní podíl ČSOB Pojišťovny podle údajů České asociace pojišťoven na úrovni 6,9 %. V neživotním pojištění došlo k meziročnímu nárůstu o 0,3 % na 4 074 016 tis. Kč. Společnost se v této oblasti v žebříčku

členských pojišťoven ČAP umístila na 6. místě s 5% tržním podílem. V oblasti životního pojištění obhájila ČSOB Pojišťovna 5. pozici s celkovým objemem předepsaného pojistného ve výši 5 564 376 tis. Kč a podíl na trhu dosáhl 9,4 %. Objem předepsaného pojistného byl mírně nad úrovní roku 2008, rovnoměrně rozdělen mezi jednorázově a běžně placené pojistné.

Hospodářská krize změnila preference klientů. Zatímco v roce 2008 bylo motorem neživotní pojištění, v loňském roce byl růst tažen především pojištěním životním, a to hlavně jednorázově placeným. Do jednorázově placených životních pojištění vložili loni klienti ČSOB Pojišťovny bezmála tři miliardy korun, a její podíl na tomto segmentu trhu tak dosáhl 16,3 procenta.

Ve výsledcích neživotního pojištění se zřetelně projevil výrazný pokles prodeje nových automobilů, v jehož důsledku se snížila i poptávka po havarijním pojištění a povinném ručení. Jediným hlavním segmentem neživotního pojištění, ve kterém loni všechny členské pojišťovny České asociace pojišťoven zaznamenaly růst, bylo pojištění podnikatelů.

O příznivé výsledky v neživotním pojištění se zasloužily především pojištění Rodinných domků a domácností s bezmála 18 procentním zvýšením předepsaného pojistného a pojištění podnikatelských rizik s 5 procentním růstem předpisu. Během roku 2009 se podařilo sjednat 466 tisíc nových smluv neživotního pojištění a počet platných smluv vzrostl na konci roku na více než 660 tisíc, tedy o 4 procenta v porovnání s předchozím rokem.

V životním pojištění došlo k pozitivnímu nárůstu celkového předpisu o 2,63 procenta. Na tomto nárůstu má velký podíl nárůst předepsaného pojistného u jednorázově placených pojištění (o 4,3 %). Na konci roku 2009 měla ČSOB Pojišťovna ve svém portfoliu přes 514 tisíc platných pojistných smluv.

Náklady na pojistná plnění za pojistné události v neživotním pojištění se v roce 2009 zvýšily na 2,15 miliardy korun. Kromě škod souvisejících s rostoucí velikosti kmene pojištění motorových vozidel k tomu přispěly i dvě loňské kalamitní události – březnová vichřice Emma a vichřice z června, které si vyžádaly náklady na pojistná plnění ve výši 81 milionů korun. V životním pojištění sice vzrostly hrubé náklady na pojistná plnění meziročně o 5 procent na 2,769 miliardy korun, plán společnosti však počítal s tím, že nárůst bude ještě o 280 milionů korun vyšší. Celkem v roce 2009 vyřídili likvidátoři

společnosti téměř 167 tisíc pojistných události (88 tisíc ze životního a 79 tisíc z neživotního pojištění).

Provozní náklady společnosti se v roce 2009 podařilo udržet pod kontrolou: zůstaly téměř na úrovni roku 2008 a plánu roku 2009. Celkově vytvořila ČSOB Pojišťovna v roce 2009 čistý zisk 1 426 284 tis. Kč. V porovnání s rokem 2008 se čistý zisk společnosti zvýšil o 879 milionů korun.

4 Aplikace obecných zásad řízení bezpečnosti ve společnosti ČSOB Pojišťovna, a. s.

Bezpečnost je jedno z nejdůležitějších témat, které každá organizace řeší a řešit musí, protože se dotýká všech jejich oblastí, nemůže bez něj správně fungovat ani se stát konkurentem pro ostatní podniky na trhu.

4.1 Bezpečnost a rizika v pojišťovnictví

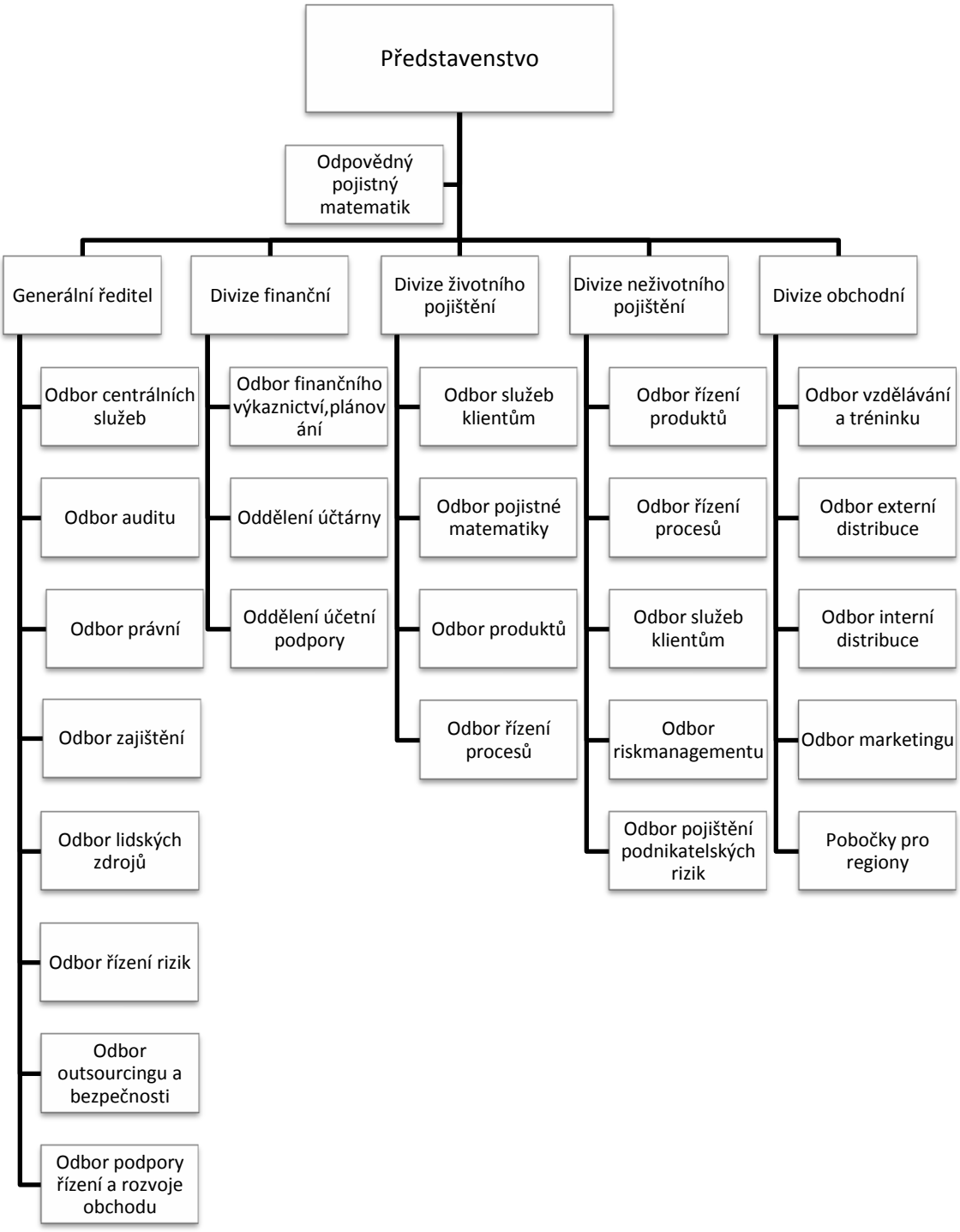
Bezpečnost je téma, které řeší každý podnik a oblasti pojišťovnictví se týká také. V pojišťovnictví se zachází s citlivými informacemi, ty je proto třeba chránit co nejvíce. Většina komunikace probíhá pomocí internetu či interních sítí. K tomu se používají nejmodernější zabezpečovací systémy a bezpečnostní hesla.

4.2 Analýza současného systému řízení bezpečnosti v ČSOB Pojišťovně

ČSOB Pojišťovna se tématem bezpečnosti zabývá neustále, hlavně z důvodu jejího předmětu činnosti. Největší nebezpečí představují pro organizaci její vlastní zaměstnanci, jejich neuvědomělost může způsobit nemalé problémy. Proto jsou všichni důkladně a pravidelně proškolováni, vzděláváni a motivováni, poté pro firmu naopak představují nejúčinnější článek v bezpečnostní strategii.

4.2.1 Oddělení outsourcingu a bezpečnosti

Oblastí bezpečnosti se v ČSOB Pojišťovně zabývá oddělení outsourcingu a bezpečnosti. V posledních deseti letech došlo v řešení bezpečnosti v organizaci k velkým změnám. Nejprve existovalo pouze jedno oddělení, které se zabývalo bezpečností obecně, informační bezpečností a částečně i havarijním plánováním. Havarijní plánování je dnes součástí řízení rizik. Toto oddělení je nezávislé, plní funkci konzultanta a hodnotitele. Oddělení outsourcingu a bezpečnosti řídí tuto oblast pouze metodicky, vlastní provádění má na starosti vedoucí oddělení. Vydává předpisy a nařízení týkající se bezpečnosti a provádí projektovou aktivitu.



Obrázek č.11: Struktura společnosti ČSOB Pojišťovna, a. s., zdroj: vlastní zpracování

Náplní činnosti tohoto oddělení je:

a) v oblasti koordinace outsourcingu:

- podpora řídicích složek, tvorba a správa podkladů pro řídicí složky;
- vydávání a správa interních předpisů týkajících se metodiky pro oblast outsourcingu služeb informačních a komunikačních technologií;
- návrhy na aktualizaci outsourcingové smlouvy a aktuálnost smluvních dokumentů a vedení archivu smluvních závazků;
- udržování evidence nakupovaných služeb, kontrola těchto služeb včetně indikace jejich vlastností, rozsahu a komplexnosti;
- monitoring fungování smluvně dohodnutých vnitřních kontrol poskytovatele služeb;
- přezkoumávání zpráv poskytovatele a tvorba pravidelných zpráv o vývoji, kontinuitě a kvalitě nakupovaných služeb pro potřebu řízení;
- metodika pro komunikaci požadavků a využívání služeb týkajících se informačních a komunikačních technologií;
- podpora a koordinace zaměstnanců ČSOB Pojišťovny;

b) v oblasti bezpečnosti ČSOB Pojišťovny:

- řídí obecnou bezpečnost v ČSOB Pojišťovně;
- řídí informační bezpečnost v ČSOB Pojišťovně;
- řídí oblast ochrany osobních údajů;
- tvorba a aktualizace bezpečnostních standardů;
- vykonávání monitoringu bezpečnosti informačních a komunikačních technologií;
- koordinace součinnosti informační, objektové, personální bezpečnosti a jejich návaznost na havarijní plánování;
- v návaznosti na strategické cíle a koncepci bezpečnosti v pojišťovně zveřejňování bezpečnostních standardů;

- metodika pro oblast fyzické bezpečnosti pracovišť, přístupů do budov a klíčového režimu.

V čele oddělení stojí ředitel odboru bezpečnosti, který je přímo podřízen generálnímu řediteli. Ředitel oddělení metodicky řídí, prosazuje bezpečnostní politiku, má na starosti projektové plánování, schvaluje směrnice a standardy týkající se bezpečnosti, komunikuje s vedením organizace a řídí bezpečnostní specialisty. Dále vytváří a realizuje bezpečnostní povědomí a kontroluje dodržování bezpečnostních pravidel při obchodních jednáních a při zacházení s citlivými informacemi. Tento ředitel vykonává funkci outsourcing koordinátora ve vztahu k informačním a komunikačním službám poskytovaným pojišťovně KBC GS CZ Branch.

V rámci oddělení outsourcingu a bezpečnosti působí ve společnosti ještě bezpečnostní specialista. Tento specialista má na starosti oblast objektovou, technickou, informačních systémů a kryptografickou ochranu. Náplní jeho práce je zabránit ohrožení bezpečnosti informací při manipulaci s informačními systémy, má právo zvolit technické prostředky k zajištění bezpečnosti informací, ochranu objektů a prostor před přístupem nepovolaných osob, správu a manipulaci s klíčovými materiály. V případě bezpečnostního incidentu ho definuje, vyhodnocuje, navrhuje opatření ke zlepšení a pomáhá bezpečnostnímu řediteli při provádění analýzy rizik. Dále spoluvytváří bezpečnostní povědomí a plní funkci školitele zaměstnanců.

4.2.2 Informační bezpečnost v organizaci

Informační bezpečnost je dnes pro každou firmu, ČSOB Pojišťovnu nevyjímaje, to nejdůležitější, co má. Informační bezpečnost je ochrana informací v jakékoliv podobě proti jejich zneužití, prozrazení, neoprávněné úpravě nebo zničení v průběhu celého životního cyklu informace. Jde tedy o minimalizaci rizik, ať už nastalých nebo hrozících a také o odstraňování případných následků nejrůznějších bezpečnostních incidentů a minimalizace jejich dopadů.

Informace se v organizaci dělí podle dvou hlavních kritérií:

a) podle formy:
   - know how;

- papírová informace;
- elektronická informace.

b) podle stupně utajení:

- přísně důvěrné;
- důvěrné;
- interní;
- veřejné.

Informační bezpečnost je pro ČSOB Pojišťovnu nebytná. Vyžadují ji jednak zákony ČR i EU, dále pak zákon č. 101/2000 Sb., zákon o pojišťovnictví, obchodní zákoník…, dále samozřejmě klienti pojišťovny, její zaměstnanci a v neposlední řadě její vlastník, čili KBC.

Informační bezpečnost má za cíl zajištění následujících atributů u všech chráněných informací:

- důvěrnost (confidentiality);
- celistvost (integrity);
- dostupnost (availability);
- odpovědnost (accountability).

Oblasti informační bezpečnosti

a) fyzická bezpečnost

- ochrana budov, přístupové systémy, rozdělení prostor na bezpečnostní zóny, kamerové systémy atd;

b) IT bezpečnost

- nastavování uživatelských práv, monitorování síťového provozu, antivirové ochrany počítačů atd;

c) personální bezpečnost

- ochrana osobních dat zaměstnanců, klientů atd;

d) organizační a administrativní bezpečnost

- citlivé interní dokumenty, plány nových obchodních strategií atd.

Bezpečnostní incident

V případě, že dojde k bezpečnostnímu incidentu, organizace jasně definuje, jak postupovat:

- čas je rozhodujícím faktorem, proto je nutné reagovat rychle;
- jestliže došlo k incidentu vinou zaměstnance, je nezbytné nesnažit se nic ututlat;
- pro tyto události existuje kontaktní osoba.

Aby k těmto nepříjemným událostem nedocházelo, je nutné dodržovat bezpečnostní pravidla:

- před odchodem od svého počítače ho uzamknout nebo se odhlásit;
- pro ochranu informací je nezbytné pravidelné zálohování;
- USB tokeny je nutné brát s sebou;
- citlivé dokumenty se musí zamykat do skříně nebo zásuvky stolu;
- poslední, kdo odchází z kanceláře, ji musí zamknout;
- dávat si pozor, co říkáme na veřejnosti;
- neprobírat citlivé údaje s bývalými kolegy.

Nejčastějším bezpečnostním incidentem je ztráta notebooku. Zaměstnanci si notebooky s údaji a daty o vlastních klientech odnáší domů a mnohdy se stává, že dojde ke ztrátě. Firemní notebooky jsou chráněny speciálním šifrováním, proto ve většině případů tedy jde pouze o finanční ztrátu.

Bezpečnostní hesla

Pro zabezpečení citlivých informací se používají hesla.

Hesla musí splňovat následující předpoklady:

- musí být dostatečně složité;

- nutné je je pravidelně měnit;
- za žádných okolností se heslo neprozrazuje;
- nejbezpečnější je si heslo pouze zapamatovat.

Sociální inženýrství

Sociální inženýrství se týká komunikace s lidmi. Je to určitý způsob manipulace lidí za účelem provedení určité akce nebo získání určité informace. Většinou se postižená osoba nedostane do kontaktu s útočníkem. Tento incident je vysvětlován jako nezákonný podvod nebo podvodné jednání s cílem získat utajené informace o organizaci. Čím dál více se objevují také podvody, kdy útočníci chtějí získat přístup do informačního systému firmy. V organizaci se na toto téma provádí rozsáhlé školení, jež je zakončeno testováním, a kterým musí projít všichni zaměstnanci.

5 Zhodnocení systému řízení bezpečnosti ve společnosti ČSOB Pojišťovna, a. s., doporučení pro zlepšení současného stavu

Současný systém řízení bezpečnosti v ČSOB Pojišťovně dosahuje velmi dobrých výsledků a spolehlivosti. O tom vypovídá důvěra, kterou společnosti dává stoupající počet klientů, partnerů i například výsledek hospodaření.

5.1 Systém řízení bezpečnosti v ČSOB Pojišťovně

Bezpečnost je ve firmě řešena ve většině případů interně. Toto řešení bezpečnosti představuje pro společnost výhodu hlavně v možnosti interního financování a lepších metod prosazení.

Bezpečnost se v pojišťovně řídí pomocí směrnic, metodických pokynů a rozhodnutí představenstva.

Směrnice:

- režim bezpečnosti trezorů;
- režim přístupů do objektů pojišťovny;
- bezpečnostní architektura;
- ochrana osobních údajů;
- dodržování „licenční čistoty“ softwaru;
- užití kryptografických metod;
- antivirová ochrana;
- standard fyzické bezpečnosti pracovišť;
- bezpečnostní standard řízení logického přístupu do informačního systému;
- E – commerce bezpečnostní politika;
- schvalování softwaru pro provoz v počítačové síti.

Rozhodnutí představenstva:

- celková bezpečnostní politika pojišťovny;
- bezpečnostní standard v principu vedení informační bezpečnostní politiky;
- bezpečnostní standard v klasifikaci informací;
- řízení kontinuity činností;

- bezpečnostní standard přístupu třetích stran a outsourcing;
- bezpečnostní standard vlastnictví i analýza rizik kritických procesů;
- program bezpečnostní osvěty a vzdělanosti;
- politická bezpečnost informačního systému.

5.2 Zhodnocení systému řízení bezpečnosti v ČSOB Pojišťovně dle různých hledisek

Společnost klade na bezpečnost velký důraz, zejména pak na zajištění bezpečnosti informací, protože zachází s citlivými daty. Toto je také důvodem, proč se oddělení bezpečnosti a outsourcingu se nachází v přímé podřízenosti generálního ředitele. Urychlí se takto komunikace mezi vedením společnosti a oddělením.

Oddělení má výhodné postavení díky své samostatnosti, je mu svěřeno pouze metodické řízení oblasti bezpečnosti. Tato situace není nejvýhodnější pro ředitele odboru bezpečnosti a outsourcingu. Při své řídicí činnosti je takto velmi omezován.

Organizace má všechny oblasti bezpečnosti podrobně, pečlivě a srozumitelně rozpracovány v konkrétních směrnicích, pokynech a rozhodnutích představenstva. Jsou zde jasně definovány kompetence, odpovědnosti a náplně práce jednotlivých pozic v rámci oddělení a také postupy při řešení nejrůznějších bezpečnostních incidentů. Nestane se tedy, že při neočekávané události nikdo neví, co dělat.

Hodnocení řešení bezpečnosti si podnik převážně zajišťuje interně. Tento přístup je úspornější z hlediska nákladů, díky samostatnosti oddělení je k oblasti přistupováno s určitou dávkou nadhledu a objektivity. Další výhodou tohoto přístupu je fakt, že oddělení dobře zná prostředí firmy a není třeba externí organizaci odhalovat interní a citlivé informace.

Velkou předností podniku je šíření bezpečnostního povědomí. Každý pracovník musí projít podrobným školením bezpečnosti, které se po určité době znovu opakuje. Na toto školení navazuje i testování zaměstnanců, zda informacím dobře porozuměli. Je samozřejmé, že toto proškolování stojí společnost nemalé peněžní prostředky, musí zaměstnávat někoho, kdo je schopen toto téma dobře vysvětlit a také to stojí čas.

5.3 Doporučení pro zlepšení současného stavu

Společnost se zaměřuje na bezpečnost informací, což je kvůli jejímu předmětu činnosti nezbytné.

Postavení oddělení bezpečnosti však není nejlepší. Je sice samostatné, ale dává vedení pouze doporučení a vše musí přes vedení „projít.“ Ředitel odboru bezpečnosti by měl mít větší pravomoci a moci oddělení řídit a to ne pouze metodicky. Právě on je tím největším odborníkem pro tuto oblast. Náplň jeho práce je široká, často může být až pracovně přetížen. Nejlepším řešením by byl ještě jeden pracovník, který by pouze komunikoval s vedením. Ředitel by měl více prostoru na řízení oddělení.

V organizaci působí pouze jeden bezpečnostní specialista, který se stará se o oblast objektovou, technickou, informačních systémů a kryptografickou ochranu, dále plní funkci školitele, šíří bezpečnostní povědomí a bezpečnostní incidenty a je odborníkem, který řeší všechny technické problémy.

Společnosti by se vyplatilo zaměstnávat jednoho pracovníka, který by plnil funkci školitele, šířil by bezpečnostní povědomí a řešil by případné dotazy ohledně metodiky týkající se bezpečnosti. Díky tomuto opatření by měl ředitel i bezpečnostní specialista více času na odbornou práci.

Další možnou alternativou, jak šířit bezpečnostní povědomí, by mohlo být školení, jež by se provádělo pouze pomocí videonahrávek umístěných na intranetu společnosti. Testování znalostí by se provádělo pomocí on-line testů. Tato možnost by byla úspornější z hlediska nákladů, řešila by také problém s časovými možnostmi a nezasahovala by do pracovní doby. Pracovníci by mohli školení shlédnout kdekoli, například v práci, doma a testováním projít také kdykoli.

Oddělení outsourcingu a bezpečnosti má ve společnosti výsadní postavení, je nezávislé, však jeho větší zapojení do celkového dění firmy jistě stojí za uvážení.

6 Závěr

Řízení podniku je v dnešním světě nesnadný proces. Působí zde konkurence, globalizace a narůstající požadavky zákazníků. Správně definovaná strategie je nezbytná a pomůže při rozhodování o dlouhodobých faktorech i v běžných každodenních situacích.

Bezpečnost je součástí řízení a toto oddělení či alespoň odpovědný pracovník má mít svoje místo v každé organizační struktuře. Nejčastější oblast, kterou podniky v rámci bezpečnosti řeší, je bezpečnost informační. Většina komunikace a obchodních transakcí mezi organizacemi se provádí elektronicky, ať už po telefonu či přes internet a pomocí e-mailu. Technické zabezpečení je proto nezbytné. V případě, že tato oblast není ošetřena dostatečným způsobem, stává se, že dochází k útokům zvenčí. Další často diskutovanou oblastí v rámci bezpečnosti je bezpečnost a ochrana zdraví při práci. K těmto incidentům dochází velice často. Nesprávně či nedostatečně proškolení pracovníci mohou společnosti způsobit nemalé problémy. Často se vedou rozsáhlé soudní spory, které není snadné vyřešit a organizaci na ně musí vynakládat značné finanční prostředky, jež mohla mnohem účinněji investovat například do podrobnějšího školení a informování pracovníků. K porušování ochrany osobních údajů dochází také ve velké míře. Běžní občané a stejně tak firmy k ochraně osobních či citlivých údajů nepřistupují s takovou vážností, jakou si toto téma zaslouží. Zneužití osobních údajů může „přijít velice draho."

ČSOB Pojišťovna je podnikem, který klade na informační bezpečnost a ochranu osobních údajů velký důraz, protože denně zachází s citlivými daty. Tato data se týkají obchodů, ale také klientů. Spoustu transakcí, operací s klienty a požadavků klientů se řeší přes internet či jsou sjednat on-line a není třeba ani navštívit pobočku. Organizace používá vysokou míru zabezpečení a bezpečnostní incidenty nezaznamenává často. Samozřejmostí je vynakládání nemalých finančních prostředků, které se ale vrací. Například formou většího zájmu klientů o společnost, stejně tak obchodních partnerů, tím poté větší zisk. Pouze finanční prostředky však nepomohou. Je třeba i dostatečné množství kvalifikovaných pracovníků, kteří se touto oblastí budou zabývat. Právě toto ve společnosti chybí. Tito zaměstnanci jsou skutečnými odborníky v oboru, měli by mít dostatek času, prostředků a v neposlední řadě i kompetencí tuto oblast komplexně řídit a moci řešit situace, které nastanou.

Cílem práce bylo popsat vztah řízení bezpečnosti a strategického řízení firmy, dále význam řízení bezpečnosti v podniku a oblasti, které podniky v rámci bezpečnosti řeší. Tento cíl byl naplněn. Bezpečnost se týká všech oblastí v podniku a při řízení se na její dodržování musí brát zřetel. Nejčastějšími oblastmi, které se v rámci bezpečnosti řeší, je bezpečnost informační, s ní související ochrana osobních údajů a bezpečnost práce. S rozvojem informačních a komunikačních technologií informační bezpečnost řeší i malé podniky a má čím dál větší význam.

Bakalářská práce dává pohled na řízení z mnoha úhlů, popisuje zapojení bezpečnosti do řízení. Popisuje oblasti bezpečnosti, které v současné době podniky řeší nejčastěji. Kapitola, která řeší téma „Bezpečný podnik," může manažerům sloužit jako návod, jak v tomto nesnadném prostředí „přežít," na které oblasti se zaměřit a věnovat jim zvýšenou pozornost.

Bezpečnost je téma, které se řeší dnes a řešit bude i v budoucnosti a předpokládá se, že čím dál více. Stále častěji se řeší nejrůznější útoky, ať už na jednotlivé osoby nebo organizace celkově. Větší důraz je také kladen na bezpečnost a ochranu životního prostředí, jež souvisí s každodenním životem a běžnými denními událostmi. Životní prostředí je v zoufalém stavu, který si pozornost zaslouží.

Slovník pojmů

Akvizice

- převzetí podniku na základě koupě nebo prodeje. Může jít o převzetí přátelské nebo nepřátelské.

Audit

- bezpečnostní proces, který zajišťuje, že uživatel je individuálně odpovědný za součinnost při nakládání s utajovanými skutečnostmi.

Byrokracie

- uspořádání osob s funkcí v hierarchickém systému nadřízenosti a podřízenosti.

Centralizace

- jeden ze dvou krajních způsobů rozložení pravomoci a odpovědnosti při řízení složitých systémů.

Data

- způsob záznamu závislý na technologii a schopnosti člověka data vnímat a interpretovat.

Fúze

- dohoda podnikatelů o splynutí jejich podniků v jeden podnik. Splynutím buď všechny podniky zanikají a vzniká nový podnik, nebo jeden podnik existuje dále a ostatní do něho vplynou.

Informace

- význam, který člověk přisuzuje datum. Může být prezentována pomocí symbolů nebo informačních technologií. Dalším významem je charakteristika vykazující jistou míru uspořádanosti.

Informační a komunikační technologie

- hardwarové a softwarové prostředky pro sběr, přenos, ukládání, zpracování a distribuci dat.

Informační společnost

- společnost, která se vyznačuje rozsáhlým využíváním informačních technologií.

Informační systém

- systém, jehož prvky jsou informační a komunikační technologie, data a lidé.

Inovace

- první uvedení na trh nového nebo zlepšeného výrobku nebo první použití nového technologického postupu.

Invence

- nápad, myšlenka, návrh, nápad atd. vedoucí k realizaci inovace.

Jakost

- kvalita.

Join Venture

- právní forma podnikání, do kterého jsou zapojeny podniky různých zemí. Může mít smluvní podobu, tzn. že se nezakládá nový podnik nebo kapitálovou podobu, kdy vzniká nový podnik, na jehož základním kapitálu se podílí partneři dohodnutým podílem.

Likvidita

- míra zpeněžení aktiva při relativně nízké ztrátě.

Management

- řízení.

Náklad

- pokles aktiv nebo přírůstek závazků nebo hodnotově vyjádřené účelné vynaložení ekonomických zdrojů.

Outsourcing

- přesun části činností podniku na externí specializovanou firmu.

Podnik

- tržní subjekt provozovaný zpravidla podnikatelem za účelem dosahování zisku.

Podnikání

- soustavná opakovaná činnost prováděná podnikatelem.

Produktivita

- účinnost výrobních faktorů ve výrobě.

Specializace

- osamotňování činností s cílem jejich racionálnějšího provádění.

Stakeholder

- kdokoli, kdo má ke společnosti nějaký vztah, je to někdo zainteresovaný.

Stocholder

- akcionář podniku.

Strategie podniku

- strategie podniku znamená připravenost na budoucnost.

Výkonnost podniku

- schopnost podniku zhodnocovat vložený kapitál.

Výnos

- zvýšení ekonomického prospěchu, k němuž došlo za účetní období, které se projevilo přírůstkem aktiv nebo snížením závazků.

Zisk

- přírůstek kapitálu z ekonomické činnosti podnikatelského subjektu.

Ztráta

- výnosy podniku jsou nižší než jeho náklady.

Literatura

Klasické dokumenty

[1] CIPRA, T. *Zajištění a přenos rizik v pojišťovnictví*. První vyd. Praha: Grada Publishing, 2004. 260 s. ISBN 80-247-0838-8.

[2] DAŇHEL, J, RADOVÁ, J, DUCHÁČKOVÁ, E. *Analýza globálních trendů ve světovém a českém komerčním pojišťovnictví*. První vyd. Praha Oeconomica, 2007. 63 s. ISBN 978-80-245-1256-3.

[3] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. První vyd. Brno: Computer Press, 2004. 231 s. ISBN 80-251-0106-1.

[4] DOUCEK, P, NOVÁK, L, SVATÁ, V. *Řízení bezpečnosti informací*. První vyd. Praha: Professional Publishing, 2008. 239 s. ISBN 978-80-86946-88-7.

[5] DUCHÁČKOVÁ, E. *Principy pojištění a pojišťovnictví*. Druhé vyd. Praha: Ekopress, 2005. 178 s. ISBN 80-86119-92-0.

[6] JAŠEK, R. *Informační a datová bezpečnost*. První vyd. Zlín: Univerzita Tomáše Bati, 2006. 140 s. ISBN 80-7318-456-7.

[7] KAMENÍK, J, BRABEC, F. *Komerční bezpečnost*. První vyd. Praha: ASPI, 2007. 190 s. ISBN 978-80-7357-309-6.

[8] KEŘKOVSKÝ, M. *Ekonomie pro strategické řízení : teorie pro praxi*. První vyd. Praha: C.H. Beck, 2004. 184 s. ISBN 80-7179-885-1.

[9] KUČEROVÁ, A, NONNEMANN, F. *Ochrana osobních údajů : v otázkách a odpovědích*. první. Praha: Bova Polygon, 2010. 150 s. ISBN 978-80-7273-163-3.

[10] MATES, P. *Ochrana osobních údajů*. První vyd. Praha: Karolinum, 2002. 73 s. ISBN 80-246-0469-8.

[11] PLAMÍNEK, J, FIŠER, R. *Řízení podle kompetencí : management by competencies v praxi, strategické směrování firmy, řízení procesů a zdrojů, zvládání ohrožujících situací, rozdělení rolí a úloh, hodnocení a motivace lidí*. První vyd. Praha: Grada Publishing, 2005. 180 s. ISBN 80-247-1074-9.

[12] RODRYČOVÁ, D, STAŠA, P. *Bezpečnost informací jako podmínka prosperity firmy*. První vyd. Praha: Grada Publishing, 2000. 143 s. ISBN 80-7169-144-5.

[13] ŘEZÁČ, J. *Moderní management: manažer pro 21. století*. První vyd. Brno: Computer Press, 2009. 359 s. ISBN 978-80-251-1959-4.

[14] SMEJKAL, V, RAIS, K. *Řízení rizik ve firmách a jiných organizacích*. Druhé vyd. Praha: Grada Publishing, 2006. 278 s. ISBN 80-247-1667-4.

[15] SOUČEK, Z. *Firma 21. století*. První vyd. Praha: Professional Publishing, 2007. 289 s. ISBN 80-86419-88-6.

[16] STÝBLO, J. *Management současný a budoucí*. První vyd. Praha: Professional Publishing, 2008. 185 s. ISBN 978-80-86946-67-2.

[17] THADDEYUS, M. *Základy strategického řízení*. první. Praha: Grada Publishing, 2007. 346 s. ISBN 978-80-247-1911-5.

[18] THOMPSON, J, MARTIN, F. *Strategic Management*. Čtvrté vyd. Thomson 2003. 421 s. ISBN 1-84480-0833.

[19] VEBER, J a kol. *Management kvality, environmentu a bezpečnosti práce*. První vyd. Praha: Management Press, 2006. 326 s. ISBN 80-7261-146.

[20] ZELENKA, J, ČECH, P, NAIMAN, K. *Ochrana dat : informační bezpečnost - výkladový slovník*. První vyd. Hradec Králové: Gaudeamus, 2002. 164 s. ISBN 80-7041-197-X.

Zprávy, odborné články

[21] ČAPEK, J. *Informace a informační bezpečnost : dílčí zpráva projektu č. VD2006201A06*. První vyd. Pardubice: Univerzita Pardubice, 2008. 68 s. ISBN 978-80-7395-062-0.

[22] KLIMESH, M. *Management and Leadership for 21.century*. Leader Business conference in Athens, 2003.

Elektronické zdroje

[23] *Http://www.csobpoj.cz* [online]. 2010 [cit. 2010-06-19]. ČSOB Pojišťovna. Dostupné z WWW: http://www.csobpoj.cz

Seznam obrázků a tabulek