ÚVOD

Prirodzenou ľudskou vlastnosťou je vnímať bezpečnosť alebo nebezpečenstvo na základe signálov, ktoré sa vyskytujú v jeho okolí. Aby sa človek mohol cítiť bezpečne musí žiť v bezpečnej krajine s priaznivými podmienkami v súkromnej sfére, ale aj v zamestnaní. Svoju bezpečnosť chápu podnikateľské subjekty v rôznych rovinách. Najčastejšie ju vnímajú z pozície ochrany svojho hmotného majetku, pričom podceňujú dôležitosť ostatných aktív. Bezpečnostná politika predstavuje súhrn opatrení a činností, ktorými subjekt bezpečnosti zabezpečuje svoju ochranu pred pôsobením bezpečnostných ohrození, ktoré negatívne ovplyvňujú jeho záujmy.
Cieľom tejto práce je objasniť miesto a úlohy bezpečnostnej politiky v podniku a navrhnúť jej možnú štruktúru a spôsob implementácie v podniku.

V prvej kapitole som sa venoval charakteristike základných pojmov ako je bezpečnosť, politika, bezpečnostná politika. Ďalšia kapitola je venovaná bezpečnostnej politike v podniku, kde som sa zaoberal právnymi aspektami, obsahom bezpečnostnej politiky. Ďalej som sa venoval metodike spracovania bezpečnostnej politiky, štruktúre a právomoci bezpečnostného manažmentu. V poslednej kapitole som sa zaoberal návrhom možnej štruktúry bezpečnostnej politiky podniku, dosiahnutím bezpečnostného povedomia zamestnancov a časovým plánom implementácie bezpečnostnej politiky.

1 CHARAKTERISTIKA ZÁKLADNÝCH POJMOV

Definovať jednoznačne pojem bezpečnosť je veľmi zložité, nakoľko má široký obsah. Viacerí autori ho vysvetľujú v závislosti od oblasti ich pôsobenia. Bezpečnosť je chápaná ako jedna z najsilnejších ľudských potrieb. V modernej dobe znamená bezpečnosť oveľa viac, ako vojenskú silu na odradenie vonkajších a vnútorných ohrození. V súčasnom svete je ťažšie stanoviť hranice medzi vnútornou a vonkajšou bezpečnosťou. Odstránenie bariér, či už politických, alebo administratívnych medzi niektorými štátmi umožnili voľný pohyb nielen osobám, ale aj peniazom a rôznym tovarom. Definíciu pojmu bezpečnosť nachádzame v slovníkoch, odborných článkoch, či zákonoch. Pojem bezpečnosť rôzne vysvetľujú vojaci, politici, sociológovia a právnici. Z uvedeného dôvodu som vybral nasledovné definície tohto pojmu:

Bezpečnosť – „(lat. securitas, angl. security, nem. Sicherheit - bezstarostnosť, bezpečnosť, istota, ale aj duševný pokoj, ochrana, zabezpečenie, určitosť, nespornosť) - znamená stav, v ktorom je zachovaná vnútorná bezpečnosť a poriadok, demokratické základy štátu, jeho suverenita a integrita a je chránené životné prostredie“ (www.securityrevue.com).

Bezpečnosť je definovaná ako stav, v ktorom je zachovávaný mier a bezpečnosť štátu, jeho demokratický poriadok a zvrchovanosť, územná celistvosť a nedotknuteľnosť hraníc štátu, základné práva a slobody, v ktorom sú chránené životy a zdravie osôb, majetok a životné prostredie (Gašpierik, 2007).

V kontexte „súkromnej bezpečnosti“, resp. „súkromných bezpečnostných služieb“ je najvšeobecnejšia definícia bezpečnosti vyjadrená takto: „Bezpečnosť je ochrana života a zdravia osôb, ochrana majetku všetkého druhu pred stratami, ktoré by mohli vzniknúť v dôsledku nehody, krádeže, podvodu...“ (www.securityrevue.com).

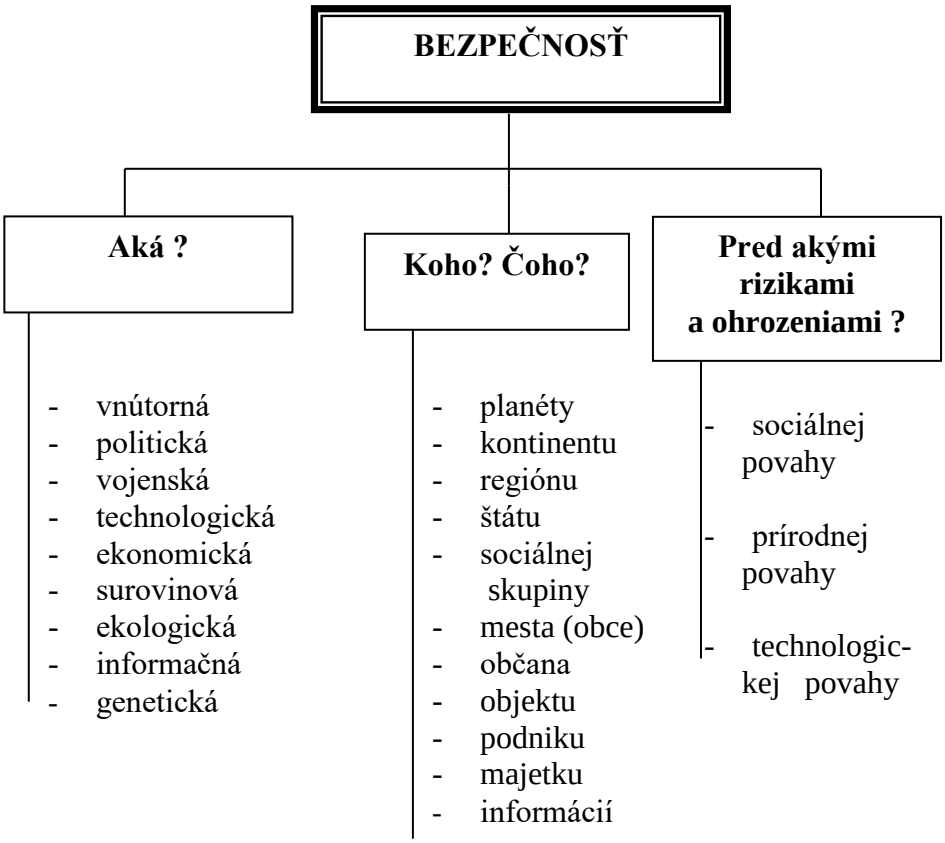
Pojem bezpečnosť je v súčasnosti jedným z najfrekventovanejších pojmov. Pritom je prezentovaný v rôznych odborných kruhoch z rôznych uhlov pohľadu. V Krátkom slovníku slovenského jazyka je pojem **bezpečnosť** vyjadrený ako „*istota, ochrana, zabezpečenie“* .

Obrázok 1 Pyramída ľudských potrieb podľa Abrahama Maslowa

(Zdroj: Reitšpís, J. a kol.: *Manažérstvo bezpečnostných rizík.* 2004, s. 9)

Bezpečnosť má svoj vnútorný a vonkajší rozmer. Vnútorná bezpečnosť je založená na interpretácii vlastného stavu subjektu. Vonkajšia bezpečnosť je založená na pôsobení rôznych ochranných prvkov spoločenského života (vojenských, politických, ekonomických atď.). Je nevyhnutné ju však vnímať, posudzovať i navonok prezentovať spoločne ako komplexný široko štruktúrovaný a mnohorozmerný jav, ktorý súvisí s ochranou života, slobody a majetku občanov, spoločnosti s jej duchovnými hodnotami a štátu ako celku (Hofreiter, 2002).

V praxi sa však takto chápaný pojem používa len veľmi zriedka. V bežnej i odbornej praxi sa výraz bezpečnosť používa s rôznymi prívlastkami, napr. *vonkajšia a vnútorná bezpečnosť, vojenská bezpečnosť, ekonomická bezpečnosť, informačná bezpečnosť.* (obrázok č. 2).



Obrázok 2 Možný obsah a štruktúra pojmu bezpečnosť

(Zdroj: Reitšpís, J. a kol.: *Manažérstvo bezpečnostných rizík.* 2004, s. 13)

„Ekonomická bezpečnosť sa týka prístupu k zdrojom, financiám a trhom, potrebným na zachovanie prijateľnej životnej úrovne a štátnej moci.

V súčasnej dobe je nezávislosť väčšiny štátov a bezpečnosť ich občanov podmienená predovšetkým ich ekonomikou. K strate nezávislosti štátu môže dôjsť už vtedy, ak štát stratí obchodné kontakty, zabrzdí sa prísun kapitálu, alebo mu bude znemožnený prístup k strategickým surovinám“ (Hofreiter, 2002, s.11).

Podnik je jednotka ekonomického rozhodovania a základný ekonomický subjekt trhovej ekonomiky. Sociálny útvar, ktorý je naplnený ľudským konaním zameraným na určitý účel. Plánovito organizovaný ekonomický subjekt na výrobu statkov a služieb. Samostatná hospodárska jednotka, ktorá vyrába výrobky a poskytuje služby určené na predaj. Na rozdiel od súkromných domácností vyrábajú prevažne za účelom cudzej (nie vlastnej) spotreby (www.wikipedia.sk).

Podľa Obchodného zákonníka sa podnikom rozumie „súbor hmotných, ako aj osobných a nehmotných zložiek podnikania. K podniku patria aj veci, práva a majetkové hodnoty, ktoré slúžia na prevádzkovanie podniku“.

„Existuje veľké množstvo kvantitatívnych, či kvalitatívnych kritérií, podľa ktorých členíme podniky. Medzi najpožívanejšie kvantitatívne kritérium môžeme zaradiť počet zamestnancov. Väčšinu podnikov v krajinách Európskej únie tvoria malé a stredné podniky. Používa sa pritom nasledovná klasifikácia:

- mikropodniky: 0 – 9 zamestnancov,
- malé podniky: 10 – 99 zamestnancov,
- stredné podniky: 100 – 499 zamestnancov“ (Kupkovič, 2001, s. 67).

Nová definícia malých a stredných podnikov

Za účelom zlepšenia podnikateľského prostredia v EÚ, ide najmä o uľahčenie prístupu podnikateľov ku kapitálu vo všetkých fázach ich pôsobnosti, táto definícia nadobudla platnosť 1. januára 2005.

Malé a stredné podniky majú v ekonomike kľúčovú úlohu. Sú zdrojom voľných pracovných miest, zvyšujú konkurenciu a zamestnanosť v celej Európe. V únii existuje takmer 23 miliónov mikro, malých a stredných podnikov, ktoré poskytujú 75 miliónov pracovných príležitostí. Rovnaká situácia je aj na Slovensku kde 99% podnikov tvoria práve malé a stredné podniky.

Tabuľka 1 Rozdelenie podnikov podľa EÚ
(Zdroj: www.europa.eu.int)

Kategória podniku	**Počet zamestnancov**	**Ročný obrat alebo Ročná súvaha**	
Stredne veľký	< 250	**<= 50 miliónov EUR** (v r. 1996 40 mil. EUR)	**<= 43 miliónov EUR (v r. 1996 27 mil. EUR)**
Malý	< 50	**<= 10 miliónov EUR** (v r. 1996 7 mil. EUR)	**<=10 miliónov EUR** (v r. 1996 5 mil. EUR)
Mikro	< 10	**<= 2 milióny EUR** (v minulosti nedefinované)	**<= 2 milióny EUR** (v minulosti nedefinované)

Pod pojmom **bezpečnosť podniku** sa rozumie „sústavné a efektívne využívanie dostupných zdrojov, zabezpečujúcich stabilné fungovanie podniku v súčasnosti a stály rozvoj v budúcnosti.

To sa však predpokladá aktívnym prístupom objektu, najmä

v smere:

- nepretržitého odhaľovania bezprostredných príčin ohrozenia svojej bezpečnosti, teda identifikovania, AKO môže byť ohrozená jeho bezpečnosť,
- nepretržitého odhaľovania konečných príčin ohrozenia svojej bezpečnosti, teda zisťovania, PREČO môže byť ohrozená jeho bezpečnosť,
- včasného vytvorenia efektívneho bezpečnostného systému na ochranu všetkých svojich aktív“ (Hofreiter. 2005).

Bezpečnostný manažment (Security Management) je špecifická zmysluplná činnosť, zameraná na odvrátenie alebo minimalizáciu bezpečnostných rizík, resp. bezpečnostných ohrození rôznej povahy a príčiny voči životu a majetku občanov, obcí a spoločnosti, obsahujúca v sebe prvky rizikového, krízového, havarijného a hodnotového manažment.

Obsah bezpečnostného manažmentu je tvorený logickou postupnosťou krokov, vykonávaných na zabránenie vzniku, prejavov alebo minimalizáciu bezpečnostných rizík a ohrození, ktoré vyvolávajú viktimáciu občanov, ohrozujú majetok obcí i spoločnosti, alebo inak pôsobia proti záujmom občanov, sociálnych skupín a spoločnosti (www.securityrevue.com).

Bezpečnostný manažment je súčasťou priamej a situačnej stratégie prevencie proti majetkovej kriminalite.

Bezpečnostný manažment predstavuje tiež logický súhrn poznatkov o princípoch, metódach a postupoch riadenia v oblasti zaisťovania bezpečnostnej ochrany. Súhrn týchto poznatkov je využívaný pre prípravu odborníkov, ktorí ich majú aplikovať v praxi bezpečnostných služieb pri zaisťovaní ochrany osôb, majetku a objektov.

Pojmom bezpečnostný manažment sa tiež označuje skupina ľudí (výkonný manažment), ktorí majú za úlohu riadenie a správu vytvoreného bezpečnostného systému, resp. prevádzku a kontrolu technických prostriedkov bezpečnostného systému (www.securityrevue.com).

Pod pojmom **politika** sa vo všeobecnosti rozumie „plánovité, organizované a cieľavedomé sociálne konanie, zamerané na vybudovanie, udržanie alebo zmenu určitého stavu. Je tiež chápaná ako umenie spravovať veci verejné, riadiť sociálny objekt a realizovať jeho ciele. Politika je určitý smer, spôsob, obsah , forma a metóda nejakej činnosti“(Hofreiter, 2005, s 11).

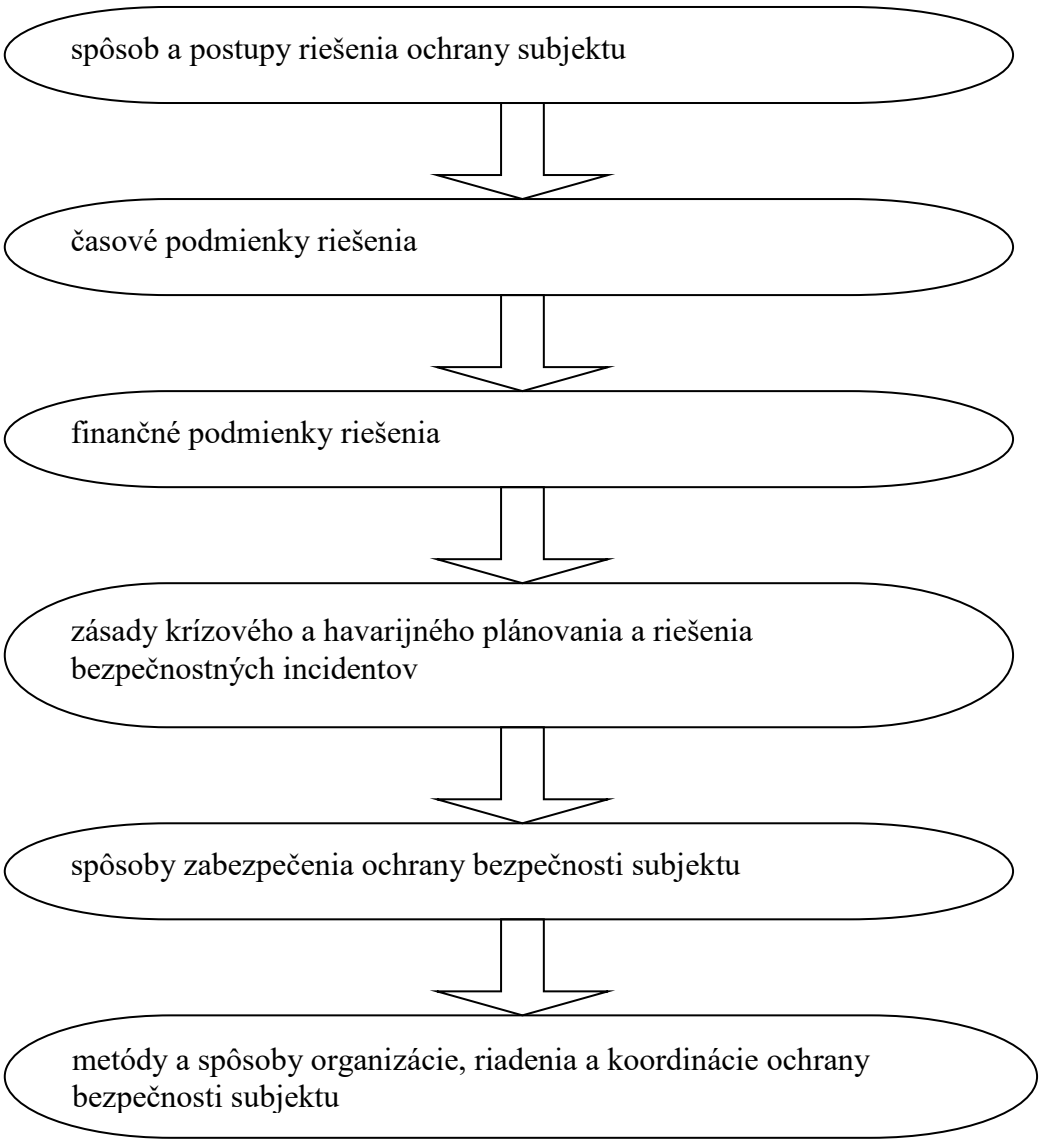
Bezpečnostná politika (v bezpečnostnom manažmente) je základným a východiskovým dokumentom na projektovanie každého bezpečnostného systému. Predstavuje deklaráciu zodpovednosti subjektu bezpečnosti (organizácie, firmy a pod.) za bezpečnosť osôb, ochrany majetku a informácií. Bezpečnostná politika definuje chránené záujmy subjektu a stanovuje systémové zásady, ako tieto záujmy chrániť.

Bezpečnostná politika sa vypracúva spravidla po predchádzajúcej analýze bezpečnostných rizík a vychádza predovšetkým z týchto faktorov:

- z platných právnych noriem a ich priamej aplikácie či aplikácie sprostredkovanej prostredníctvom podnikových alebo iných normatívnych aktov,
- zo špecifík bezpečnostných požiadaviek na zaistenie bezpečnostných záujmov daného subjektu,
- z predstáv subjektu o požadovanom spôsobe ochrany, napr. vlastnou ochranou, dodávateľsky - najatou SBS a pod.,
- z ekonomických možností a ochoty financovať náklady na zaistenie bezpečnosti.

Bezpečnostná politika smerujúca na zaistenie ochrany osôb a majetku sa stala neoddeliteľnou súčasťou interných predpisov podnikov, bánk, dopravných spoločností, telekomunikačných a bezpečnostných organizácií. Svoje opodstatnenie však nájde aj tam, kde sú chráneným záujmom informácie, nehmotný majetok, firemné know-how (Hofreiter, 2005).

Bezpečnostná politika spravidla charakterizuje:



Obrázok 3 Bezpečnostná politika

(Zdroj: Hofreiter, L.: *Prednášky z predmetu Bezpečnosť podniku*. 2005, s.14)

Schválená bezpečnostná politika podniku je základ na projektovanie bezpečnostného systému. Bezpečnostná politika predstavuje komplexný súbor cieľov, zásad, postupov a opatrení štátu na zaručenie bezpečnosti štátu a občanov. Okrem obranného rozmeru v sebe integruje zahraničnú, vnútrobezpečnostnú, ekonomickú, sociálnu, environmentálnu a ďalšie dimenzie (www.securityrevue.com).

Bezpečnostnej politike v podniku sa budem podrobnejšie venovať v druhej kapitole.

2 BEZPEČNOSTNÁ POLITIKA PODNIKU

Každý podnik musí dbať na svoju bezpečnosť, je to základná a nevyhnutná podmienka pre jeho existenciu a úspešné fungovanie. Motívom pre manažment podniku na riešenie otázok bezpečnosti je i plnenie platných právnych noriem. Vedúci pracovník podniku je povinný dbať na ochranu zdravia a života zamestnancov a ochranu majetku v rozsahu svojej pôsobnosti.

2.1 PRÁVNE ASPEKTY BEZPEČNOSTI PODNIKU

Zaručiť bezpečnosť podnikov má dôležitý spoločenský význam. Predchádza sa tým možným negatívnym dopadom, prináša optimalizáciu pracovného procesu a tiež ekonomický efekt, zvýšenie produktivity, efektívnosti a kvality práce. Zaručená bezpečnosť podniku má aj dôležitý humánny aspekt, ktorý prezentuje úroveň kultúrnu a spoločenskú a prispieva ku kvalite života. Riešením otázky bezpečnosti sa vytvárajú predpoklady na ochranu ľudského činiteľa, majetku a ostatných aktív podniku. Týmto sa prispieva k vyššej kvalite života v podniku a k vyššej efektivite podniku. Zvyšuje sa pocit bezpečia zamestnancov, vytvára sa lepšia pracovná atmosféra, tým sa dosahuje zvýšenie výkonnosti v podniku.

Je potrebné si uvedomiť, že dosiahnutie požadovanej úrovne bezpečnosti často nákladné opatrenia, ktoré nie sú dokonalé. Bezpečnosť podniku je úloha najvyššieho manažmentu. Na zabezpečenie trvalého prosperovania podniku je dôležité, aby sa zaviedol riadiaci mechanizmus, ktorý bude zabezpečovať optimálne fungovanie podniku (obrázok 3).

Obrázok č. 4 Stratégia riadenia podniku

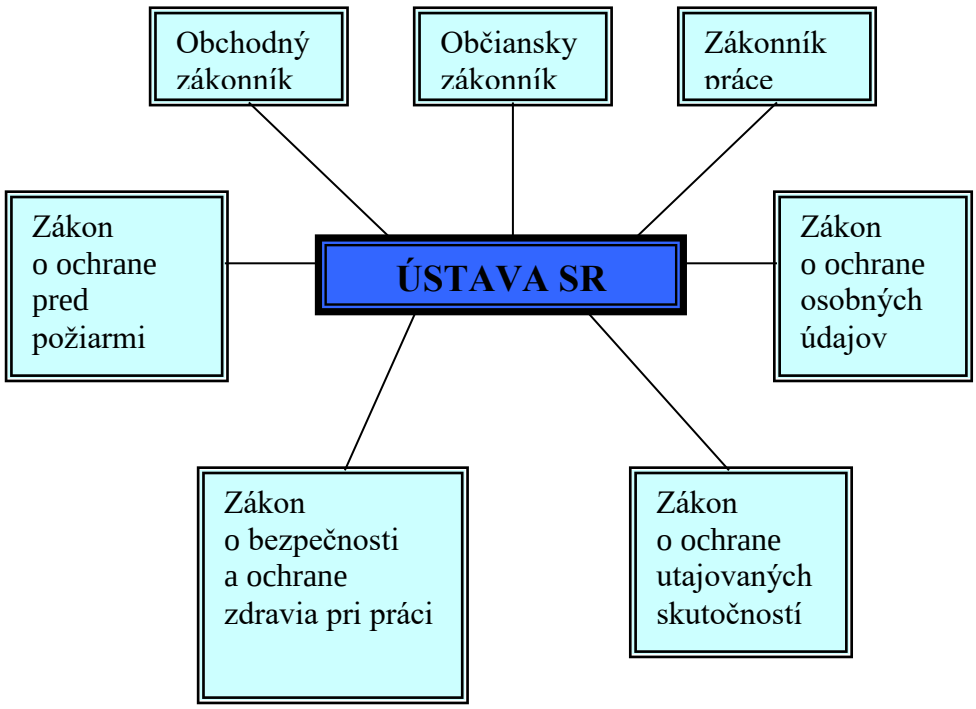
(Zdroj: ALARM, 1/2006, s.10)

Bezpečnostná politika podniku je základným a východiskovým dokumentom podniku. Podnik ňou deklaruje svoje záujmy na implementáciu bezpečnosti do všetkých sfér svojej činnosti. Predstavuje komplexný pohľad na všetky jeho aspekty bezpečnosti. Bezpečnostná politika definuje chránené záujmy podniku, stanovuje princípy, možné ohrozenia, riziká a systémy riadenia bezpečnosti v podniku.

Jej spracovanie vychádza z vypracovanej bezpečnostnej analýzy a z nasledovných faktorov:

- z platných zákonov v Slovenskej republike a iných právnych noriem, ktoré nadväzujú na tieto zákony,
- z právnych noriem alebo iných normatívnych aktov podniku, ktoré sa môžu ale následne meniť s ohľadom na prijatú politiku bezpečnosti,
- z ekonomických a finančných možností podniku, ktoré chce a môže investovať na svoju bezpečnosť,
- z lokálnych podmienok, ktoré majú vplyv na bezpečnosť podniku (Hofreiter, 2005).

Už samotná Ústava, ako najvyššia právna norma Slovenskej republiky hovorí o princípoch bezpečnosti (článok 36).



Obrázok 14 Právne normy zaoberajúce sa bezpečnosťou

(Zdroj: autor)

Ústava v článku 36 v bode c uvádza ochranu bezpečnosti a zdravia pri práci.

Jednou z noriem, kde sú zakotvené princípy bezpečnosti je i Občiansky zákonník (ďalej len „OZ“), ktorý v § 415 uvádza: „Každý je povinný počínať si tak, aby nedochádzalo ku škodám na zdraví, na majetku, na prírode a životnom prostredí.“
Osobitná preventívna povinnosť odvrátiť škodu je tiež zakotvená v § 417 OZ: „ Komu škoda hrozí, je povinný na jej odvrátenie zakročiť spôsobom primeraným okolnostiam ohrozenia.“

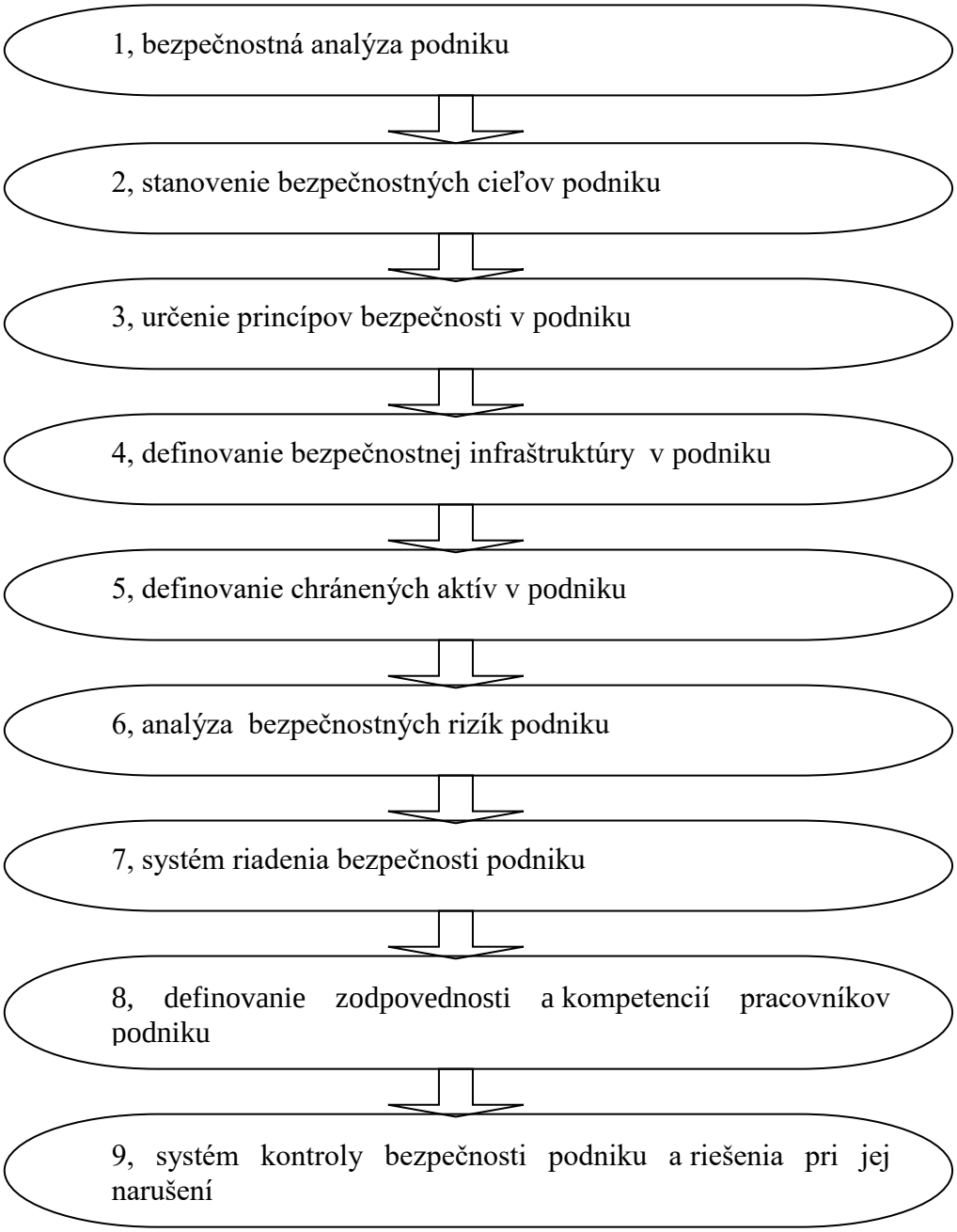
Zodpovednosť vedúceho pracovníka je zrejmá i zo znenia § 420 OZ : „Každý zodpovedá za škodu, ktorú spôsobil porušením právnej povinnosti,“ pričom právna povinnosť vyplýva aj z porušenia interných bezpečnostných predpisov, smerníc a poriadkov.

Podobne sa zodpovednosť vyjadruje aj v § 172, ods. 1. Zákonníka práce: „Zamestnanec zodpovedá zamestnávateľovi za škodu, ktorú mu spôsobil zavineným porušením povinností pri plnení pracovných úloh.“

Zákon o bezpečnosti a ochrane zdravia pri práci sa vzťahuje na všetky odvetvia činnosti výrobnej a nevýrobnej sféry. Zamestnávateľ zamestnávajúci viac ako 10 zamestnancov vymenúva jedného alebo viac zamestnancov za zástupcov zamestnancov. Jeden zástupca zamestnancov by mal zastupovať najviac 20 zamestnancov. Zamestnávateľ zamestnávajúci viac ako 100 zamestnancov je povinný vytvoriť poradný orgán – komisiu bezpečnosti a ochrany zdravia pri práci, ktorá je tvorená zástupcami zamestnancov a zamestnávateľa, najmä odborníkov v danom odbore, nadpolovičná väčšina musí byť však tvorená zo zástupcov zamestnancov (Zákon č. 330/1996 Z. z. o bezpečnosti a ochrane zdravia pri práci).

Zamestnávateľ má zo zákona povinnosť určiť, aké ohrozenia vyplývajú z pracovných činností a z používania pracovných prostriedkov. Na podstatu a metódy posudzovania rizík nie sú pevne stanovené pravidlá. Každý si môže zvoliť vlastný, ale systematický postup, či postupnosť krokov, ktorými sa podarí zlepšiť bezpečnosť a ochranu zdravia, odhaliť organizačné a riadiace nedostatky, zmapovať faktory, ktoré ovplyvňujú pracovnú pohodu a urobiť opatrenia na zefektívnenie práce.

2.2 MOŽNÝ OBSAH BEZPEČNOSTNEJ POLITIKY PODNIKU



Obrázok 5 Možný obsah bezpečnostnej politiky

(Zdroj: ALARM, 1/2006, s.10)

1, Bezpečnostná analýza podniku

Samotné riešenie bezpečnosti podniku predstavuje proces, na začiatku ktorého je bezpečnostná analýza podniku. Bezpečnostná analýza podniku predstavuje analyticko-syntetickú činnosť pred prijatím rozhodnutí v bezpečnostnej politike podniku a ich realizácií podľa jednotlivých bezpečnostných projektov. Základom bezpečnostnej analýzy je zistenie skutkového stavu v rôznych oblastiach bezpečnosti, určenie hrozieb, ktoré sú schopné narušiť integritu podniku ako uceleného systému. Bezpečnostná analýza podniku obsahuje tiež predbežnú analýzu rizík.

Možný obsah bezpečnostnej analýzy podniku:

- dislokácia a popis všetkých objektov podniku,
- popis stavu ochrany majetku,
    - plášťová a perimetrická ochrana,
    - priestorová ochrana,
    - kontrola vstupov,
    - predmetová ochrana,
    - režimová ochrana,
    - fyzická ochrana,
    - protipožiarna ochrana,
    - ochrana pred účinkami priemyselných havárií,
- personálna bezpečnosť,
- administratívna bezpečnosť,
- bezpečnosť informácií a informačného systému,
- ochrana osobných údajov,
- ochrana bankového tajomstva,
- bezpečnostný manažment a manažment rizík,
- čiastkový záver k stavu zabezpečenia ochrany majetku (ALARM, 2006).

2, Stanovenie bezpečnostných cieľov podniku

Stanovenie bezpečnostných cieľov podniku je vecou vrcholového manažmentu každého podniku. Podkladom pre stanovenie bezpečnostných cieľov je bezpečnostná analýza podniku, možnosti každého podniku a predstavy na fungujúci systém bezpečnosti v podniku. Pri stanovovaní cieľov sa zároveň prihliada k princípu bezpečnosti a k princípom, ktorými sa chce podnik riadiť. Podnik stanovuje bezpečnostné ciele konkrétne pre svoje potreby, no vychádza sa z všeobecného rámca.

Rámec pre stanovenie bezpečnostných cieľov podniku:

- vytvorenie bezpečnostného prostredia tak, aby sa chránilo zdravie a život všetkých zamestnancov podniku a všetkých povolaných subjektov. Je potrebné zabezpečiť aj ochranu dôležitých osôb,
- vytvorenie bezpečnostného systému podniku s vymedzením zodpovednosti pre riadiacu zložku, výkonnú zložku a kontrolnú zložku,
- definovanie bezpečnostnej infraštruktúry podniku s najdôležitejšími aktívami podniku,
- definovanie bezpečnostných rizík podniku,
- vytvorenie vonkajšej ochrany objektov ako komplex opatrení na vymedzenie hraníc objektov, kontrola vstupov do objektu a výstupov z objektu. Zabezpečiť monitorovanie možného narušenia stanovených hraníc objektov podniku,
- vytvorenie vnútornej ochrany dôležitých objektov s dôrazom na ochranu chránených priestorov,
- chránenie majetku podniku ako je hmotný majetok, nehmotný majetok a finančné investície. Pri hmotnom majetku sa najväčší dôraz kladie na chránenie budov, stavieb, strojov, dopravných prostriedkov, pozemkov a ostatných investícií. V nehmotnom majetku sa chránia patenty, licencie, software, goodwill a know-how. Pri finančných investíciách sa chránia dlhodobé cenné papiere a dlhodobé pohľadávky. Pri obežnom majetku sa dôraz kladie na ochranu zásob, pohľadávok, krátkodobého finančného majetku a peňažných prostriedkov,

- zavedenie komplexného režimového opatrenia na vonkajšiu a vnútornú ochranu podniku,
- zavedenie komplexných mechanických a technických zábranných prostriedkov, ktoré budú slúžiť na ochranu a monitorovanie hraníc objektu, vstupov do objektu a na ochranu určených chránených priestorov,
- vypracovanie komplexnej krízovej, havarijnej a bezpečnostnej dokumentácie podniku,
- ochrana informačných systémov podniku a zabezpečenie vysokej úrovne bezpečnosti spracovaných informácií,
- zabezpečenie dôveryhodnosti a bezpečnosti pri poskytovaní služieb podnikom,
- zabezpečiť ochranu utajovaných skutočností v podniku,
- zabezpečiť ochranu citlivých informácií o zamestnancoch a ostatných spolupracujúcich subjektoch,
- zabezpečiť ochranu obchodného, výrobného a iných tajomstiev podniku,
- zabezpečiť monitorovanie vykonávanej bezpečnostnej politiky vnútorným auditom podniku.

Vymedzenie bezpečnostných cieľov je vhodné vymedziť vo vertikálnej a horizontálnej úrovni a určiť konkrétnu zodpovednosť, v ich funkčnej, obsahovej, ekonomickej rovine a hlavne v právnej a finančnej rovine (ALARM, 2006).

3, Určenie princípov bezpečnosti v podniku

Skladba princípov bezpečnosti, ktorá bude aplikovaná v podniku:

- **princíp ústavnosti a zákonitosti**, vyjadrujúci nevyhnutnosť realizovania bezpečnostnej politiky podniku v súlade s Ústavou SR, platnými zákonmi SR, s dôrazom na zákony ktoré sa zaoberajú ochranou majetku, tajomstiev, informácií,

- **princíp vedeckosti** v bezpečnostnej politike, vyjadrujúci potrebu uplatňovania vedeckých poznatkov a postupov pri výbere prostriedkov, pri hodnotení ich úrovne a pri ich kontrole,

- **princíp prevencie** v bezpečnostnej politike, vyjadrujúci požiadavky pri definovaní bezpečnostnej politiky podniku vychádzajúci z definovania faktorov bezpečnosti, ktoré ho ovplyvňujú. Vyjadruje previazanosť jednotlivých bezpečnostných opatrení v rámci subjektov podniku, na miestnej regionálnej a ústrednej úrovni,

- **princíp personálneho zabezpečenia** a profesionalizácie bezpečnostnej politiky podniku, vyplývajúci z nutnosti zriadiť v podniku výkonné pracovisko na profesionálnej úrovni,

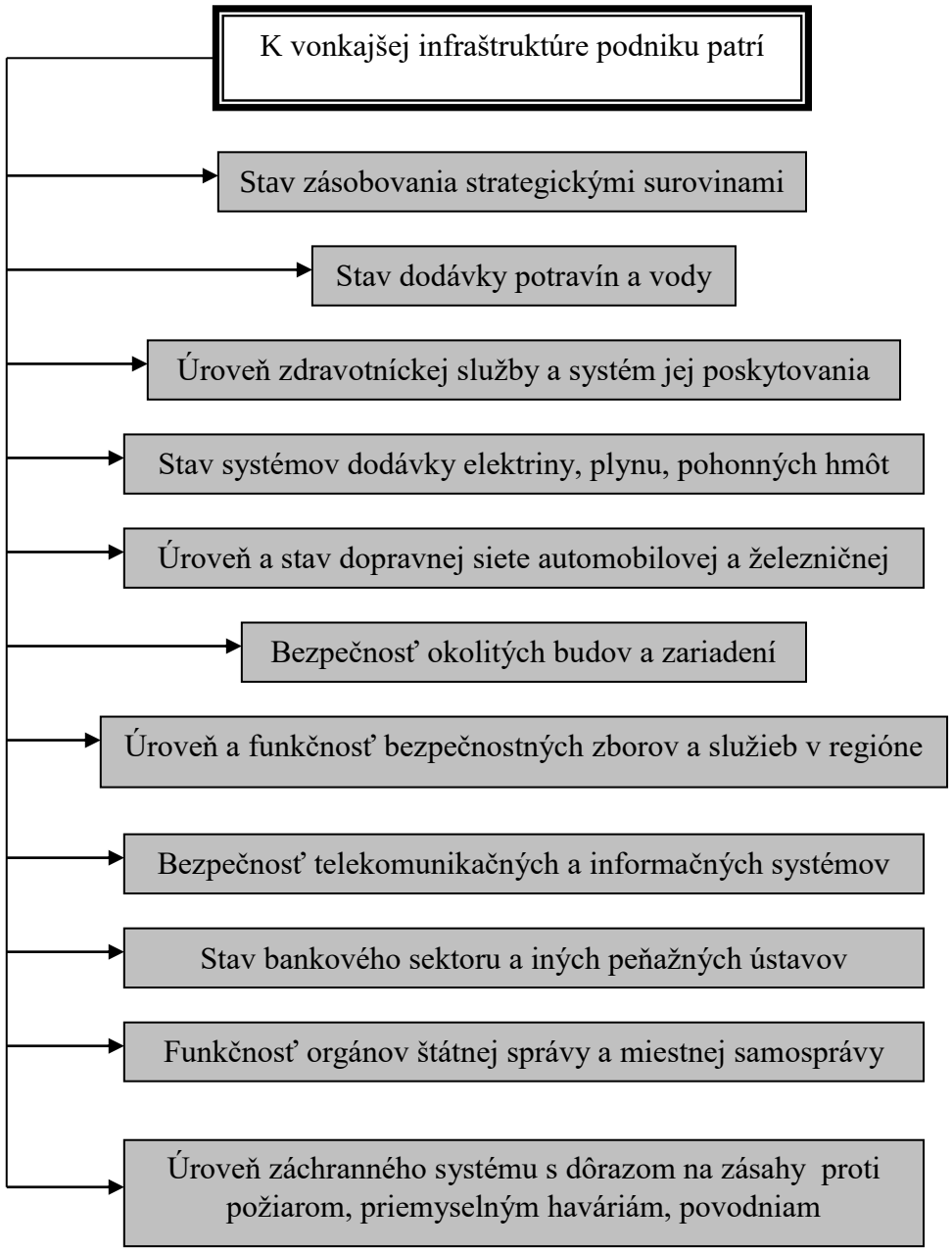
- **princíp informačného zabezpečenia**, vyjadrujúci potrebu získavania, spracovania, sprostredkovania a praktického využitia informácií, vertikálneho a horizontálneho prepojenia subjektov podniku bezpečnostnej politiky, ako aj výmenu informácií so subjektami mimo podniku,

- **princíp aktuálnosti bezpečnostnej politiky**, vyjadrujúci potrebu vychádzať z objektívnych skutočností bezpečnostného prostredia,

- **princíp zodpovednosti za bezpečnostnú politiku**, vyjadrujúci povinnosť, že koncepcia a vypracovanie systému bezpečnosti ako aj jeho riadenie prináleží vrcholovému manažmentu podniku (ALARM, 2006).

4, Definovanie bezpečnostnej infraštruktúry v podniku

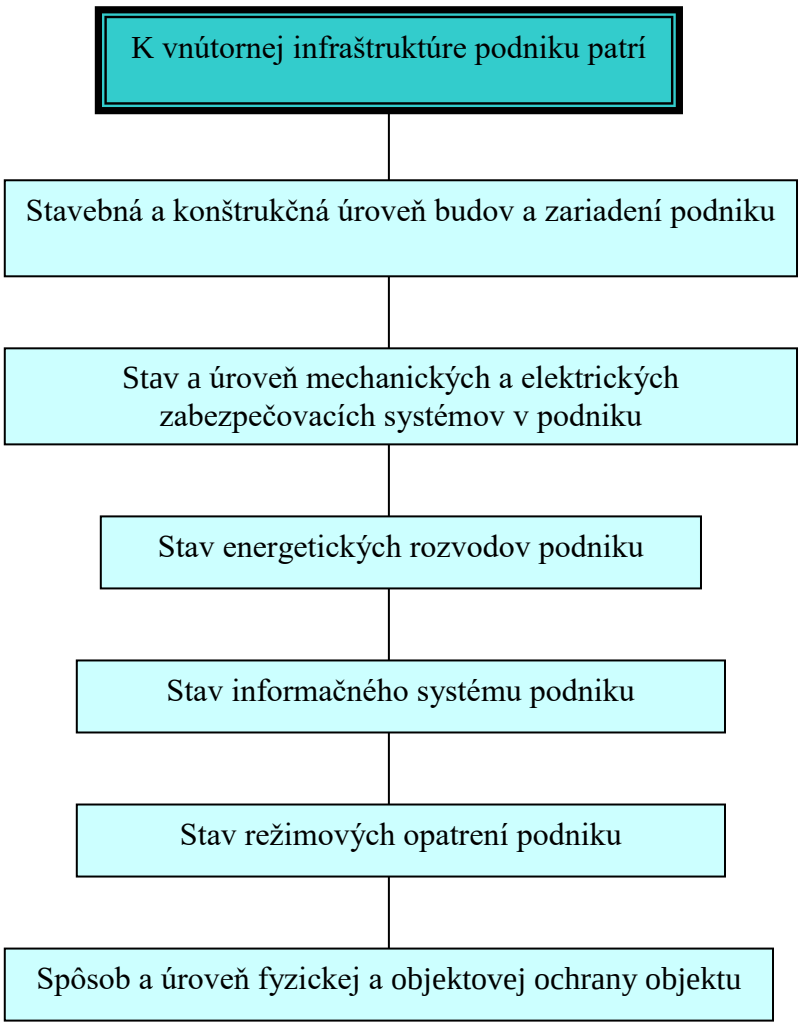
Bezpečnostnú infraštruktúru podniku môžeme rozdeliť na vonkajšiu a vnútornú. Vonkajšia infraštruktúra pôsobí nezávisle na podniku. Vnútorná infraštruktúra podniku je riadená a ovplyvniteľná podnikom.



Obrázok 6 Vonkajšia infraštruktúra podniku

(Zdroj: ALARM, 1/2006, s.12)

Vnútorná bezpečnostná infraštruktúra podniku závisí od veľkosti podniku, produktov ktoré sa vyrábajú, alebo služieb ktoré podnik ponúka.



Obrázok 7 Vnútorná infraštruktúra podniku

(Zdroj: ALARM, 1/2006 str.12)

5, Definovanie chránených aktív podniku

Na určenie chránených aktív podniku vplývajú nasledovné skutočnosti:

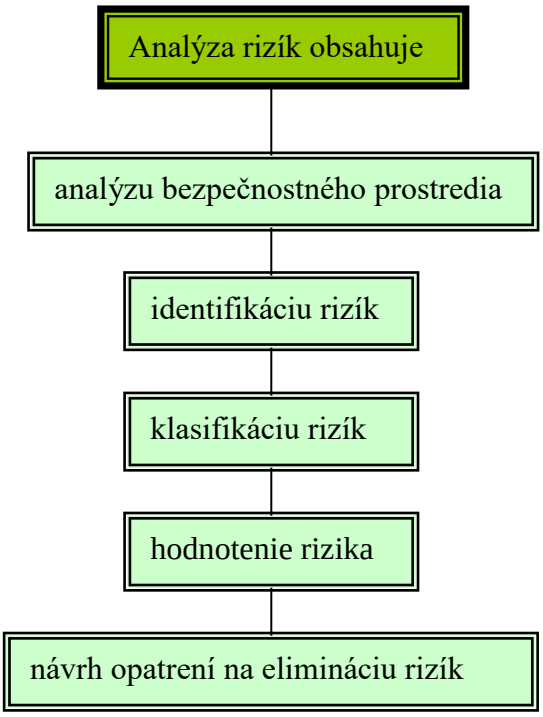
- ochrana zdravia a života zamestnancov podniku a ostatných osôb zdržujúcich sa v podniku,
- dodržiavanie zákonov a právnych predpisov,
- zabezpečenie ochrany všetkého majetku v správe podniku,
- zabezpečenie nepretržitej výroby a poskytovania služieb,
- zabezpečenie vysokej kvality služieb a výroby s neustálym zlepšovaním,

- tvorba optimálnych podmienok pre marketing a realizáciu produktov na trhu,
- udržiavanie vhodné pracovné prostredie a pracovnú morálku zamestnancov,
- dodržiavanie právnych predpisov a vnútropodnikových nariadení.

Z horeuvedeného vyplýva, že chránenými aktívami podniku sú ľudský potenciál, hmotný a nehmotný majetok, produkty, výroba a služby podniku. Podniky svoje aktíva chránia podľa vlastnej potreby (ALARM, 2006).

6, Analýza bezpečnostných rizík podniku

Analýza bezpečnostných rizík sa zaoberá otázkou pred akými hrozbami je nutné podnik chrániť. Analýza rizík je proces, ktorý podrobne identifikuje riziká, určuje ich možný rozsah a skúma vzájomné vzťahy medzi rizikami.



Obrázok 8 Analýza rizík podniku

(Zdroj: ALARM, 1/2006, s.13)

Analýza bezpečnostného prostredia sa zaoberá získavaním informácií o stave, štruktúre, dynamike a tendenciách v bezpečnostnom prostredí, ktoré sú dôležité pre identifikáciu bezpečnostných rizík. Najdôležitejšími pre analýzu sú informácie o prírodných a sociálnych javoch. Analýzou prírodných javov sa získavajú informácie o geofyzikálnych a meteorologických podmienkach, úrovni urbanizácie, charakteristike chránených objektov. Analýza sociálnych javov dáva informácie o demografii obyvateľstva, stave kriminality. Výsledky analýzy sociálnych javov sú stav životnej úrovne, zamestnanosť, štruktúra, úroveň bezpečnostných zborov. „Výsledkom analýzy bezpečnostného prostredia je definovanie predpokladov bezpečnostných rizík sociálnej, environmentálnej a technickej povahy, ktoré by mohli ohroziť chránený záujem“ (ALARM 1/2006 str. 13).

Identifikácia rizík je najdôležitejší predpoklad na efektívne riadenie bezpečnostných rizík, pretože riziká ktoré boli identifikované môžu byť v budúcnosti riadené a ovplyvňované v bezpečnostnom systéme. Najdôležitejšou úlohou identifikácie rizík je zistenie všetkých typov a zdrojov rizík vo vzťahu k prostrediu a zistenie predpokladov všetkých rizík. Obsahovou stránkou identifikácie rizík je spracovanie získaných informácií o vonkajšom a vnútornom bezpečnostnom prostredí, vypracovanie registra rizík.

Klasifikácia rizík slúži na zaradenie identifikovaných bezpečnostných rizík do skupín. Kritériom pre klasifikovanie rizík býva zdroj rizika, charakter, doba trvania tendencia, mechanizmus vzniku a pôsobenie rizika. Ďalšie kritériá pre klasifikáciu rizík sú:

- predvídateľnosť, podľa ktorej sa bezpečnostné riziká rozdeľujú na predvídateľné a nepredvídateľné,
- početnosť, podľa ktorej sa klasifikuje riziko na skupinové a individuálne,
- merateľnosť, riziká sa klasifikujú na merateľné a nemerateľné,
- ovplyvniteľnosť, riziká sa klasifikujú na ovplyvniteľné a neovplyvniteľné.

Hodnotením rizika sa rozumie priradenie slovného ohodnotenia alebo číselnej hodnoty ku každému riziku. Metódy využívajúce sa na hodnotenie rizika sú kvantitatívne, ktoré využívajú matematický aparát a kvalitatívne využívajúce expertné ohodnotenie. Kvalitatívne metódy hodnotia riziko ako malé, stredné, prijateľné a neprijateľné.

Návrh opatrení na elimináciu rizík sa určuje v troch základných skupinách:

- eliminácia daného rizika,
- zníženie účinkov rizika,
- rozkladanie rizika na viacero subjektov (ALARM, 2006).

Medzi **základné ciele bezpečnostnej politiky** podniku môžeme zaradiť:

- zabezpečenie ochrany a bezpečnosti aktív podniku,
- vytvorenie podmienok pre spoľahlivé fungovanie podniku,
- zabezpečenie trvalého rozvoja podniku,
- efektívne využívanie všetkých zdrojov vyčlenených na zaistenie bezpečnosti podniku,
- vytvorenie systému spoľahlivého a nepretržitého riadenia bezpečnosti podniku,
- stanovenie zodpovednosti za bezpečnosť aktív.

Ciele bezpečnostnej politiky môžu byť podrobnejšie definované v celkovej bezpečnostnej politike podniku (Hofreiter, 2005).

Princípy, ktoré ovplyvňujú charakter bezpečnostnej politiky:

- **princíp konkrétnej zodpovednosti** – požaduje, aby sa stanovila konkrétna zodpovednosť majiteľa podniku, manažmentu podniku a ostatných zamestnancov za jednotlivé oblasti bezpečnosti a tiež za plnenie konkrétnych povinností pri realizácii bezpečnostnej politiky,

- **princíp bezpečnostného povedomia** – vyžaduje, aby všetci , ktorí plnia úlohy v danom podniku, poznali ciele bezpečnostnej politiky podniku, v potrebnom rozsahu aj realizované bezpečnostné opatrenia a vedeli ich používať,

- **princíp zákonitosti** – vyžaduje, aby sa rešpektovali práva a legitímne záujmy všetkých zainteresovaných subjektov,

- **princíp multifaktorovosti** – vyžaduje, aby boli akceptované všetky faktory bezpečnosti a úrovne riadenia, ako aj celá škála bezpečnostných opatrení, ktorá je využiteľná na ochranu všetkých aktív podniku,

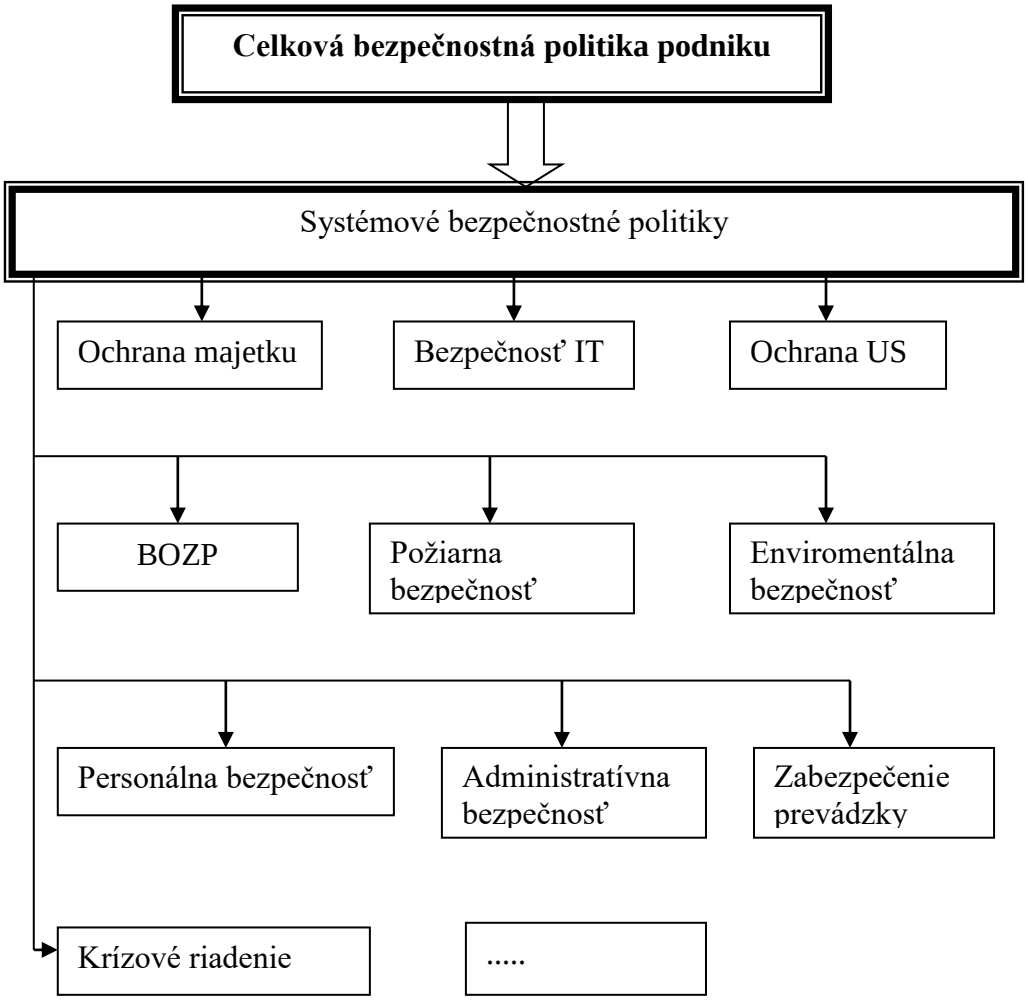
- **princíp efektívnosti** – požaduje, aby rozsah a úroveň realizovaných bezpečnostných opatrení zodpovedal veľkosti bezpečnostných ohrození a možným negatívnym prostriedkom,

- **princíp integrity** – požaduje, aby ciele a oparenia bezpečnostnej politiky boli v súlade s celkovými cieľmi podniku a požadované funkcie bezpečnostnej politiky boli koherentné s funkčnými prvkami daného podniku,

- **princíp aktuálnosti** – požaduje, aby v nadväznosti na trvalú identifikáciu hrozieb a rizík, a aj vzhľadom na vývoj v samotnom podniku, bola bezpečnostná politika pravidelne aktualizovaná (Hofreiter, 2005).

Bezpečnostnú politiku podniku delíme na:

- Celkovú bezpečnostnú politiku.
- Systémové bezpečnostné politiky.



Obrázok 9 Možná štruktúra bezpečnostnej politiky podniku

(Zdroj: Hofreiter L.: *Prednášky z predmetu bezpečnosť podniku.* 2005, s.15)

Celková bezpečnostná politika (CBP) podniku je dokument, ktorý je záväzný a verejný, prijíma sa vedením organizácie ako vnútorná norma. Má strategický charakter prijímaný na obdobie 5 až 10 rokov. Stanovuje štruktúru ochranných opatrení a zodpovednosť za ich realizáciu.

Musí vo všeobecnosti vymedziť nasledovné:

- čo treba chrániť,
- proti čomu treba chrániť,
- ako treba chrániť,
- kto a za čo zodpovedá.

Obsahom CBP podniku je:

- popis podniku, hlavné poslanie podniku,
- bezpečnostná analýza podniku,
- ciele bezpečnostnej politiky podniku, čo chrániť a v akej oblasti,
- špecifikácia štruktúry, zodpovednosti a právomoci bezpečnostného manažmentu podniku,
- definícia a klasifikácia aktív spoločnosti,
- identifikácia bezpečnostných ohrození,
- ohodnotenie bezpečnostných rizík spoločnosti,
- návrhy a odporúčania na dosiahnutie cieľov bezpečnostnej politiky v oblastiach ochrany majetku, bezpečnosti informačných systémov, personálnej bezpečnosti, ochrany osobných údajov, administratívnej bezpečnosti so stanovením zodpovednosti za ich realizáciu,
- identifikovanie obmedzení (časových, priestorových, organizačných, legislatívnych technických),
- časový plán implementácie bezpečnostnej politiky,
- návrh na spôsob dosiahnutia bezpečnostného povedomia v podniku (školenie a osveta) (Hofreiter, 2005).

Systémové bezpečnostné politiky vychádzajú z celkovej bezpečnostnej politiky podnikov a definujú spôsob realizácie celkovej bezpečnostnej politiky v konkrétnych oblastiach. Majú kratšiu platnosť ako CBP väčšinou 2 až 5 rokov. Obsahom SBP sú súbory pravidiel na ochranu technických, režimových, personálnych administratívnych a fyzických opatrení v závislosti od zabezpečovacej oblasti.

Systémová bezpečnostná politika (SBP) obsahuje:

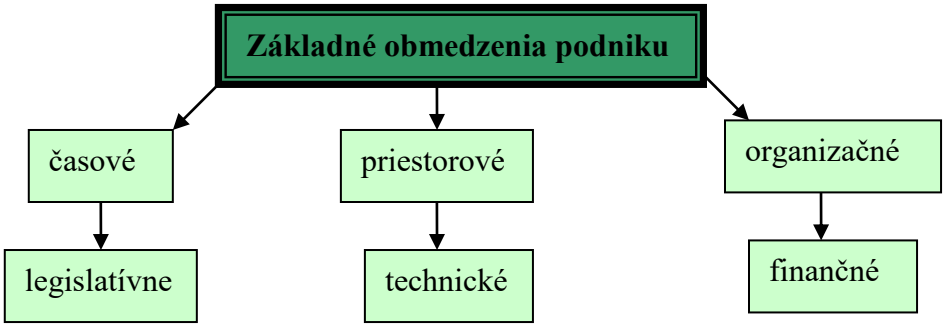
- konkretizáciu aktív danej oblasti,
- konkrétne bezpečnostné ciele,
- konkrétne ohrozenia a riziká identifikované a integrované v danej oblasti,
- bezpečnostnú dokumentáciu,
- havarijné plány,
- plán implementácie SBP: časové plány, rozpis nákladov, potrebné zdroje, zodpovednosť za implementáciu,
- bezpečnostný program – plán školení podľa funkcií a zodpovednosti (Hofreiter, 2005).

2.3 METODIKA SPRACOVANIA BEZPEČNOSTNEJ POLITIKY

Na tvorbe celkovej a systémovej bezpečnostnej politiky by sa mali podieľať odborní zamestnanci, ktorí sú schopní posudzovať nasledovné oblasti:

- systémové riadenie podniku,
- systémy hlavných činností (výroba, predaj, obchod),
- analýza rizík,
- fyzická a objektová bezpečnosť,
- personálna bezpečnosť,
- administratívna bezpečnosť,
- bezpečnosť IS a IT,
- enviromentálna bezpečnosť,
- riešenie mimoriadnych udalostí,
- riešenie krízových situácií (Hofreiter, 2005).

Bezpečnostnú politiku ovplyvňujú rôzne faktory, ktoré vyplývajú z externého a interného prostredia podniku. Medzi základné obmedzenia podniku patria:



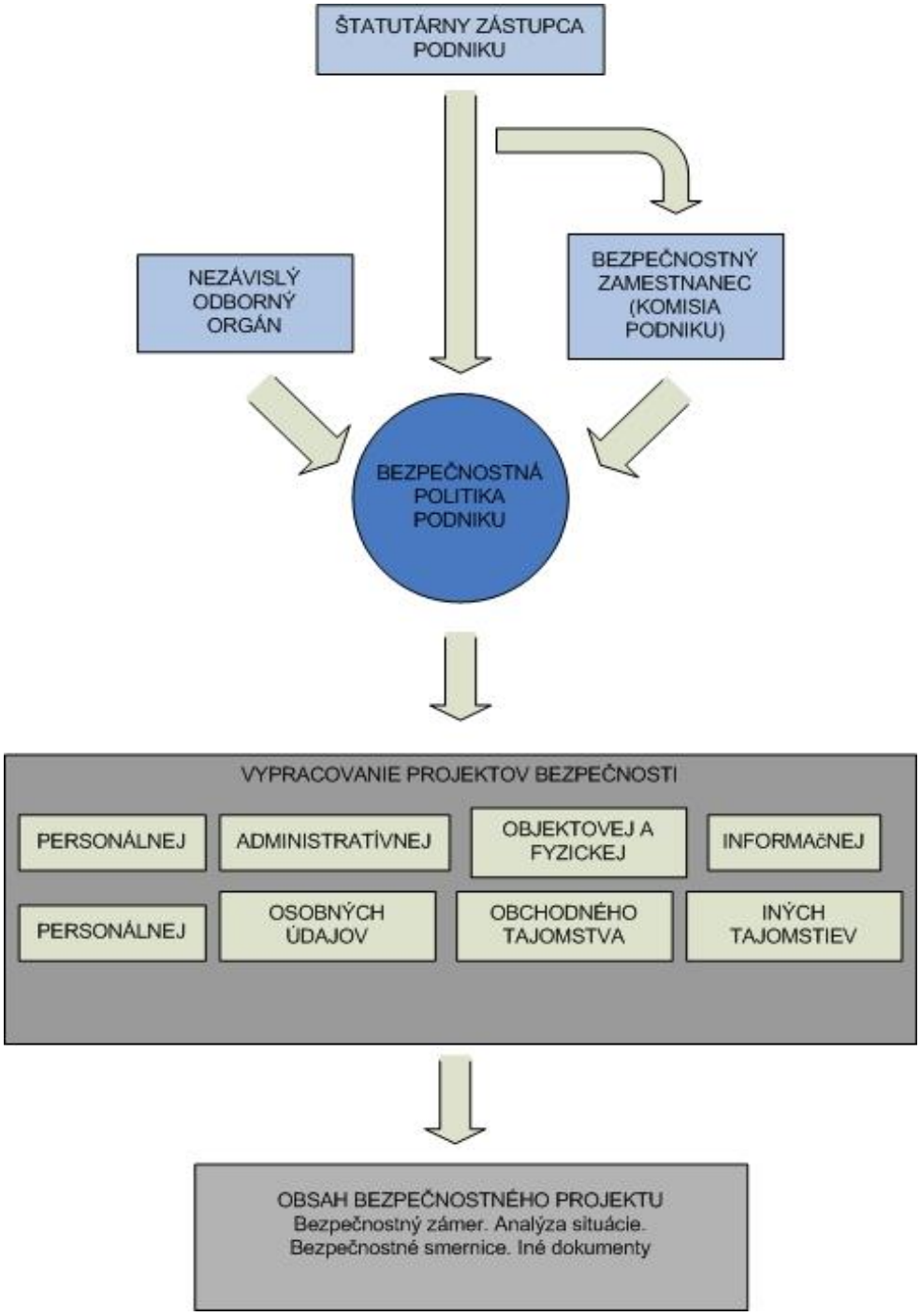
Obrázok 10 Základné obmedzenia podniku

(Zdroj: Hofreiter, L.: *Prednášky z predmetu bezpečnosť podniku* 2005, s.40)

- časové – sú dané dispozičným časom na spracovanie a implementáciu bezpečnostnej politiky v podniku,
- priestorové – môžu ovplyvniť možnosť použitia niektorých bezpečnostných opatrení, ako sú prostriedky perimetrickej ochrany, prostriedky priestorovej ochrany a fyzickej ochrany,
- organizačné – môžu ovplyvniť štruktúru bezpečnostného manažmentu a systém riadenia podniku,
- legislatívne – vytvárajú rámec pre realizáciu bezpečnostnej politiky podniku, ale aj priamo regulujú, respektíve nariaďujú rozsah niektorých opatrení ako je ochrana osobných údajov, ochrana pred požiarom,
- technické – ovplyvňujú možnosť, ale i potrebu realizácie niektorých technických zabezpečovacích prostriedkov, ako je detekcia požiaru, úniku plynu, zaplavenia, otrasové detektory,
- finančné – vytvárajú podmienky na implementáciu bezpečnostnej politiky podniku, vyjadrujú ochotu i možnosť investovať určitý objem finančných prostriedkov na zaistenie bezpečnosti podniku (Hofreiter, 2005).

Postup pri vytvorení bezpečnostnej politiky môže byť nasledovný:

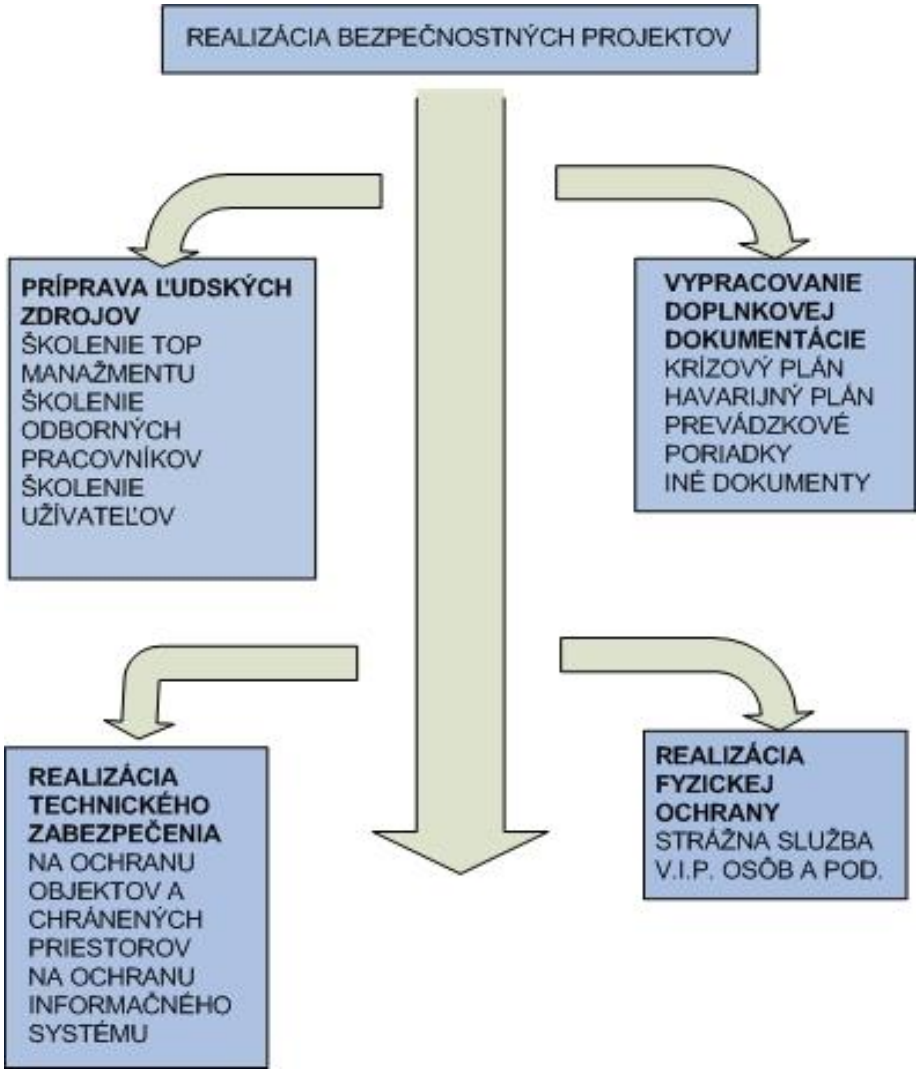
1. fáza



Obrázok 11 Bezpečnostná politika podniku

(Zdroj: ALARM, 1/2006, s.12)

1. fáza	analyticko – systetická	definovanie objektu, cieľov BP, identifikácia a ohodnotenie rizika, definovanie nástrojov a opatrení, vytvorenie BM podniku, vytvorenie dokumentov.
2. fáza		



Obrázok 12 Realizácia bezpečnostných projektov

(Zdroj: ALARM, 1/2006, s.12)

2. fáza	realizačná	realizácia oparení, vypracovanie plánov a smerníc, príprava a školenie zamestnancov,

3. fáza

Obrázok 13 Funkčnosť bezpečnostného systému
(Zdroj: ALARM, 1/2006, s.13)

3. fáza auditačná overenie funkčnosti prijatých oparení.

2.4 ŠTRUKTÚRA, ZODPOVEDNOSŤ A PRÁVOMOC BEZPEČNOSTNÉHO MANAŽMENTU PODNIKU

Cieľ je definovanie úrovní bezpečnostného manažmentu a ich vertikálne a horizontálne väzby. Je potrebné dosiahnuť, aby všetkým úrovniam riadenia podniku zodpovedala aj príslušná úroveň riadenia bezpečnosti podniku, ktorá bude zabezpečovaná kvalifikovanými špecialistami pre dané oblasti ako je napr. oblasť bezpečnosti IT a IS, požiarnej oblasti, BOZP, ochrana majetku a ochrana utajovaných skutočností. Po definovaní štruktúry bezpečnostného manažmentu je nutné definovať aj oblasť zodpovednosti a vybaviť zamestnancov príslušnými právomocami a to ako na horizontálnej, tak i na vertikálnej úrovni.

V bezpečnostnej politike by malo byť stanovené:

- kto je za čo zodpovedný,
- čo je povinný v danej oblasti robiť,
- čo alebo koho riadi a kontroluje,
- čo môže rozhodnúť sám,
- o čom musí informovať nadriadeného.

V súvislosti s bezpečnostnou politikou pod pojmom bezpečnostný manažment rozumieme:

- bezpečnostný manažment je chápaný ako špecifická zmysluplná činnosť, ktorá je zameraná na odvrátenie, alebo minimalizáciu rizík,
- bezpečnostným manažmentom sa tiež označuje skupina ľudí, ktorí majú za úlohu riadenie vytvoreného bezpečnostného systému.

Podľa štruktúry podniku by mala byť vytvorená aj zodpovedajúca štruktúra riadenia systému podniku. Manažment podniku spoločnosti sa bude orientovať na riadenie procesov súvisiacich s hlavným poslaním podniku (Hofreiter, 2005).

Tabuľka 2 Možná organizácia bezpečnostného manažmentu podniku
(Zdroj: Hofreiter, L. Prednášky z predmetu bezpečnosť podniku, 2005. s.7)

Úroveň	Manažment podniku	Bezpečnostný manažment
1.	Vrcholový manažment	Bezpečnostný riaditeľ
2.	Stredný manažment	Systémový špecialisti
3.	Výkonný manažment	Výkonní pracovníci

Základné úlohy jednotlivých úrovní sú nasledovné:
1. úroveň:

- vypracovanie celkovej bezpečnostnej politiky podniku ako strategického dokumentu s dlhodobou platnosťou, ktorý umožňuje vedeniu podniku riadiť bezpečnostné procesy. Je to verejný záväzný dokument, prijatý organizáciou ako vnútorná norma podnik,
- zabezpečuje riadenie bezpečnosti na podnikovej úrovni.

2. úroveň:

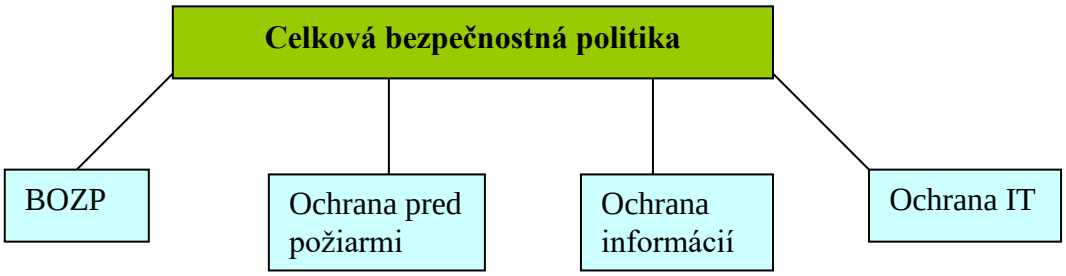
- vypracovanie systémových bezpečnostných politík, kde sa bude definovať spôsob realizácie CBP v konkrétnych oblastiach. Systémové bezpečnostné politiky majú platnosť 2 až 5 rokov,
- vypracovanie realizačných dokumentov a smerníc (plán ochrany objektu, smernice pre výkon fyzickej ochrany, bezpečnostné projekty, bezpečnostná dokumentácia, havarijné plány, plány požiarnej ochrany),
- odborné riadenie pracovníkov,
- kontrolná činnosť v danej oblasti.

3. úroveň:

- realizácia systémových politík,
- plnenie povinností ktoré vyplývajú zo smerníc a plánov,
- spätná väzba pre 2. stupeň riadenia (Hofreiter, 2005).

3 NÁVRH MOŽNEJ ŠTRUKTÚRY BEZPEČNOSTNEJ POLITIKY

Každý podnik má svoje špecifiká, čo sa týka vlastnej bezpečnosti a ochrany majetku. Rozdielnu štruktúru bezpečnostnej politiky má vojenský podnik, nadnárodná spoločnosť, alebo malá rodinná firma. Nie je možné navrhnúť univerzálnu BP nakoľko každý podnik je osobitý. Návrh bezpečnostnej politiky pre podniky by mohol zahŕňať minimálne základné oblasti, ako je to uvedené na obr. č. 15.

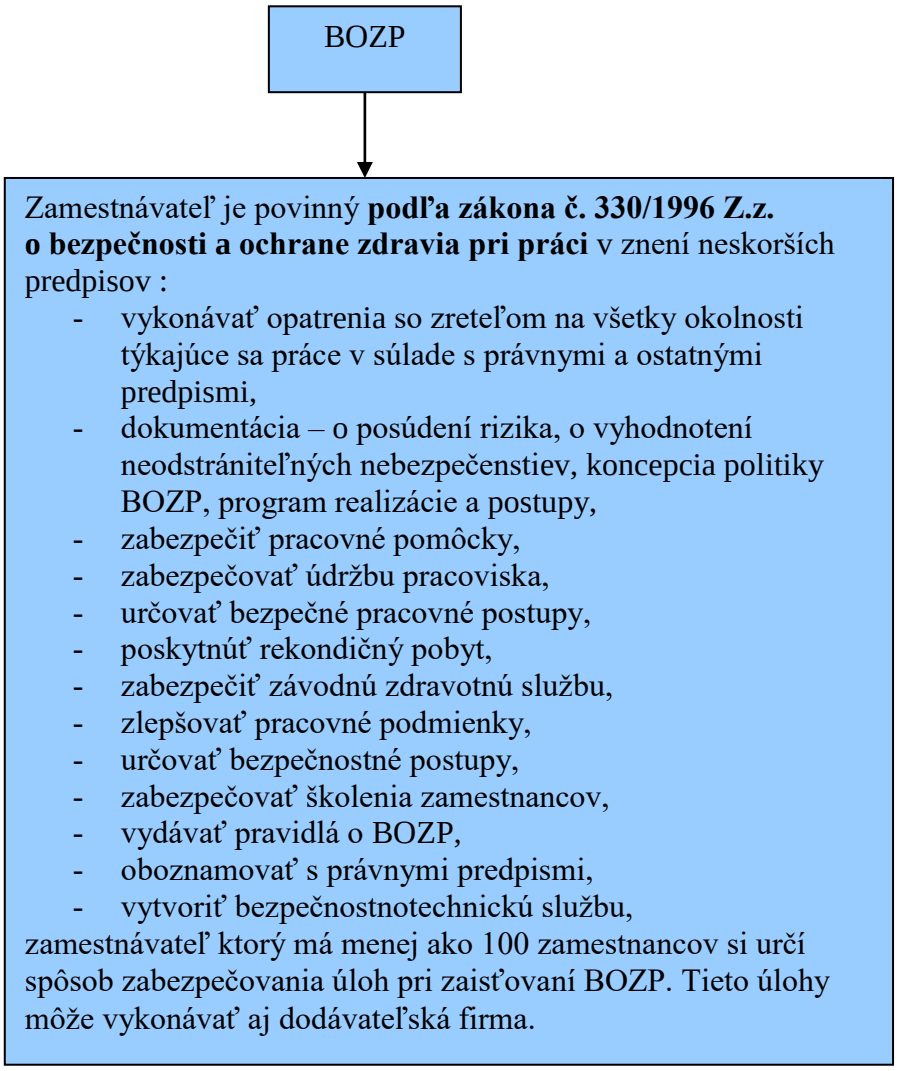


Obrázok 15 Návrh bezpečnostnej politiky

(Zdroj: autor)

Bezpečnosť a ochrana zdravia pri práci

Zákon o bezpečnosti a ochrane zdravia pri práci ustanovuje základné podmienky na zaistenie bezpečnosti a zdravia pri práci a obmedzuje riziká a faktory, ktoré podmieňujú vznik pracovných úrazov a chorôb z povolania.



Obrázok 16 Povinnosti zamestnávateľa podľa zákona o bezpečnosti a ochrane zdravia pri práci

(Zdroj: Zákon č. 330/1996 Z.z. o bezpečnosti a ochrane zdravia pri práci v znení neskorších predpisov)

Postup ako posúdiť riziká na pracovisku

Obrázok 17 Posúdenie rizík na pracovisku

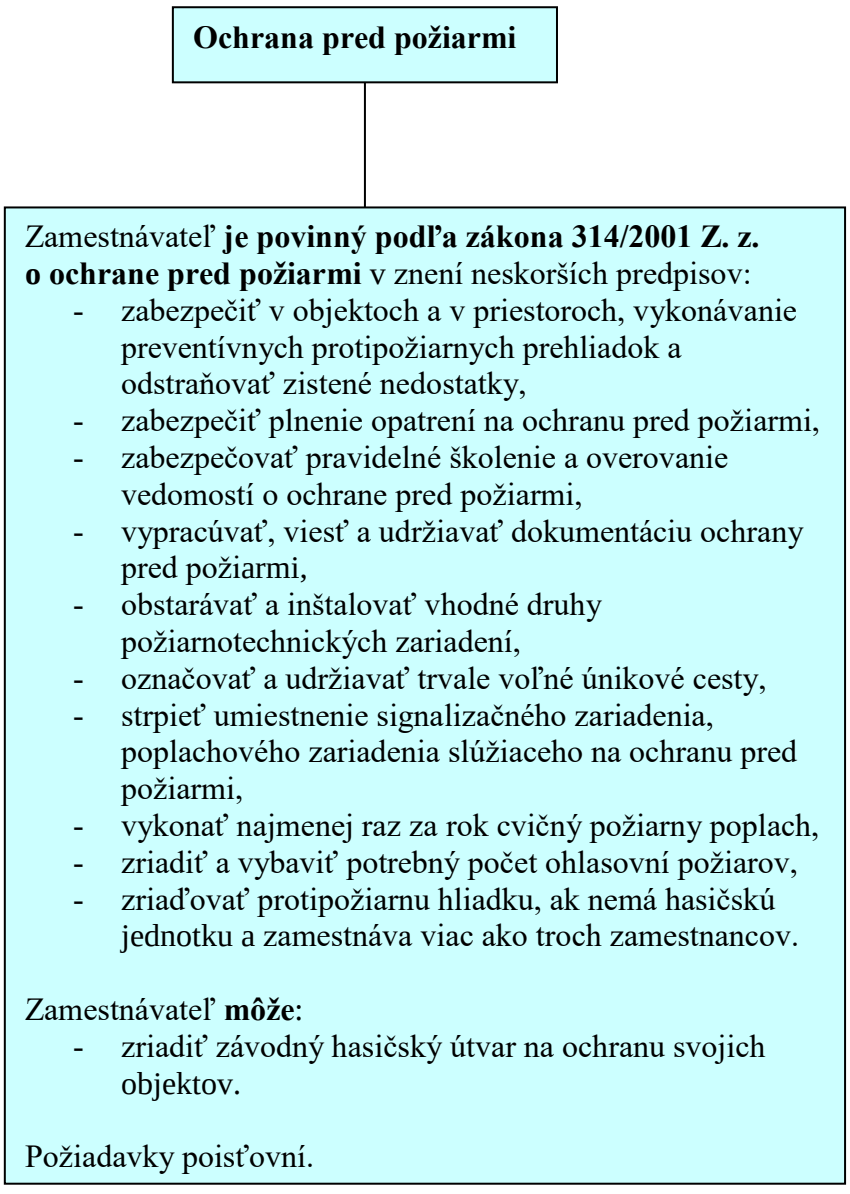
(Zdroj: Systém riadenia BOZP)

Na dosiahnutie účinného riadenia v oblasti BOZP je potrebné:

- aby súčasťou pracovných náplní vedúcich zamestnancov boli presne stanovené
- povinnosti, právomoci a zodpovednosť,
- aby mal každý zamestnanec písomne vymedzenú individuálnu zodpovednosť,
- aby bola vytvorená jasná organizačná štruktúra v oblasti riadenia BOZP, so zodpovednosťou najvyššieho predstaviteľa podniku, s presne vymedzenými vnútornými a vonkajšími vzťahmi, známa všetkým zamestnancom.

Ochrana pred požiarmi

Zákon o ochrane pred požiarmi upravuje povinnosti zamestnávateľa na úseku ochrany pred požiarmi, odbornú prípravu a odbornú spôsobilosť.



Obrázok 18 Povinnosti zamestnávateľa podľa zákona o PO

(Zdroj: Zákon č. 314/2001 Z.z. o ochrane pred požiarmi v znení neskorších predpisov)

Ochrana osobných údajov

Osobnými údajmi sa rozumejú údaje týkajúce sa určenej, alebo určiteľnej fyzickej osoby. Takou osobou je osoba, ktorú možno určiť priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora, na základe jednej či viacerých charakteristík alebo znakov.

Za bezpečnosť osobných údajov zodpovedá zamestnávateľ tým, že ich chráni pred odcudzením, stratou, neoprávneným prístupom k nim a ich rozširovaním. Na tento účel sa prijímajú primerané technické, organizačné a personálne opatrenia zodpovedajúce spôsobu spracúvania. Zamestnávateľ je povinný zachovať mlčanlivosť o osobných údajoch zamestnancov. Za dohľad nad osobnými údajmi zodpovedá zamestnávateľ (zákon č. 428/2002 Z.z. o ochrane osobných údajov v znení neskorších predpisov).

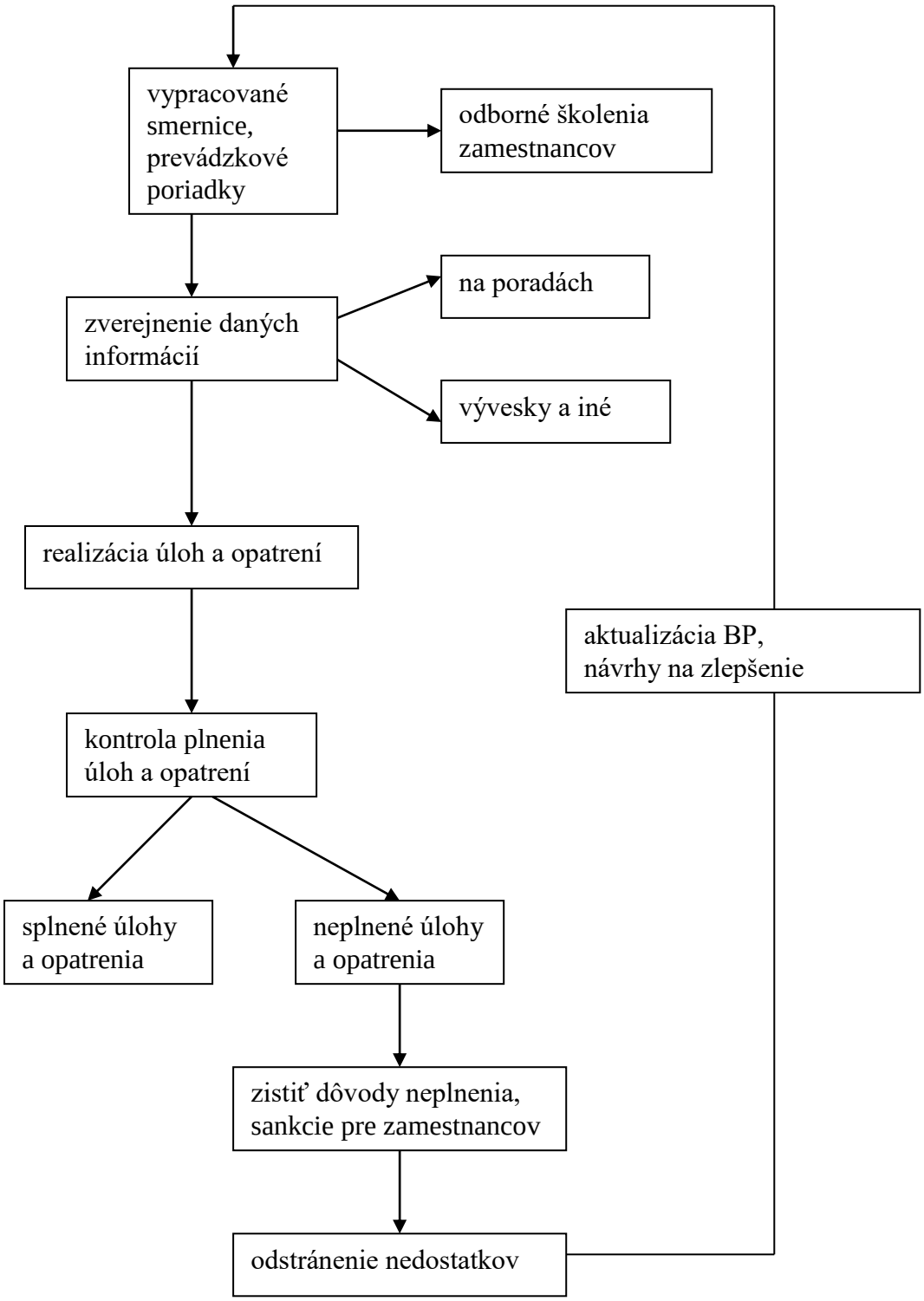
Ochrana utajovaných skutočností

Spôsob práce s utajovanými skutočnosťami upravuje zákon č. 215/2004 Z.z. o ochrane utajovaných skutočností, ktorý ukladá chrániť informácie, personálnu bezpečnosť, administratívnu bezpečnosť.

Bezpečnosť informačných technológií

Informačné technológie spracúvajú stále väčšie množstvo informácií s veľkou hodnotou. Spolu s informačnými technológiami je späté aj spracovanie informácií. V podniku sa najčastejšie jedná o informácie vysokej hodnoty, ako sú daňové priznania, bankové účty, platobné nástroje, výsledky vývoja alebo výskumu, ale aj zdravotné záznamy zamestnancov a pod. Pri zabezpečovaní informačných technológií je nutné si určiť najprv bezpečnostné ciele a spôsob ich dosiahnutia. Bezpečnostná funkcia sa dá kategorizovať podľa spôsobu implementácie. Bezpečnostný mechanizmus môže charakter fyzickej ochrany, administratívneho alebo softwarového oparenia. Opatrenia v uvedenej oblasti bližšie definujú príslušné normy.

3.1 Návrh na dosiahnutie bezpečnostného povedomia zamestnancov



Obrázok 19 Návrh na dosiahnutie bezpečnostného povedomia zamestnancov

(Zdroj: autor)

Ani najlepšími bezpečnostnými opatreniami sa nedá dosiahnuť absolútna bezpečnosť. Preto súčasťou prevencie musí byť aj dôsledná pripravenosť na nežiadúce udalosti. Úspešnosť riadenia vo všeobecnosti závisí od toho, ako je zorganizovaná práca, ako sú stanovené povinnosti a zodpovednosť jednotlivých zamestnancov, či zamestnanci chápu ako efektívne je určená organizačná štruktúra a plnia si svoje povinnosti. Vypracované smernice a prevádzkové poriadky podniku slúžia na zvýšenie bezpečnostného povedomia zamestnancov podniku. Základom trvalej prosperity podniku je vzdelaný, kompetentný a motivovaný zamestnanec. Zamestnávateľ je povinný školiť zamestnancov o príslušných bezpečnostných predpisoch, o zásadách bezpečného správania, o bezpečných pracovných postupoch, o ohrozeniach a rizikách pri práci a o prevencii proti nim. Aj vzdelávanie zamestnancov musí byť systematické. V praxi sa často stretávame s formálnymi školeniami, ktoré sú stratou času pre účastníkov a zbytočným nákladom pre firmu. Aby malo vzdelávanie zmysel, musí vychádzať zo skutočných potrieb, čo majú zamestnanci vedieť. Obsahom vzdelávania má byť okrem sprostredkovania informácií a inštrukcií aj pestovanie zručností, návykov a postojov, nevyhnutných na bezpečný výkon práce a bezpečné správanie sa, ako aj budovanie povedomia. Do osnov je potrebné zahrnúť aj problematiku stresov, pracovnej záťaže, psychológie práce, sociálnych vzťahov a pod. Je dobré investovať do kvalitných školiteľov, ktorí dokážu účastníkov motivovať. Moderné formy vzdelávania využívajú interaktívny prístup, riešenie prípadových štúdií, modelových situácií. Špecializované školenia je potrebné zabezpečiť pre bezpečnostných technikov, zástupcov zamestnancov, odborných pracovníkov (revíznych technikov), požiarnych technikov, a pre zamestnancov, u ktorých sa vyžaduje odborná spôsobilosť podľa osobitných predpisov.

Zamestnávateľ je povinný kontrolovať a vyžadovať dodržiavanie právnych predpisov, zásad bezpečnej práce, ochrany zdravia pri práci a bezpečného správania sa na pracovisku. Kontrolná činnosť musí byť systematická, plánovaná a dokumentovaná. Cieľom systému kontroly stavu BOZP je zabezpečiť aj dôsledné vykonávanie predpísaných prehliadok, skúšok, revízií a meraní, aby bola sústavne zabezpečovaná a overovaná spôsobilosť strojov, zariadení, technológie a bezpečnosť pracovných činností. Súčasťou kontrolného systému je režim odstránenia nedostatkov. Vykonávanie kontrolnej činnosti je v prvom rade zodpovednosťou vedúcich pracovníkov na všetkých úsekoch riadenia. Na kontrolnej činnosti sa podieľajú všetci zamestnanci. Komplexné previerky sa majú v zmysle zákona vykonať najmenej raz za rok.

Súčasťou riadiacej činnosti v oblasti BOZP je vykonanie nápravných a preventívnych opatrení. Podklady na rozhodnutie o nich vyplynú z jednotlivých činností popísaných v predchádzajúcich kapitolách. Vrcholový manažment firmy by mal preskúmať účinnosť riadenia BOZP, či sa naplnili ciele podnikovej politiky, či sú ešte aktuálne, čo by bolo potrebné na nasledujúce obdobie zaktualizovať, doplniť a zlepšiť. Využívať pri tom môžu výsledky kontroly, vlastného hodnotenia alebo spätnú väzbu. Postupnosť krokov systému riadenia predpokladá opakovanie periódy, určenie nových úloh podnikovej politiky, realizácie nových plánov, organizačného zabezpečenia, kontroly a opätovného vyhodnotenia. Opakovanie cyklu zabezpečí novú a vyššiu úroveň.

3.2 Časový plán implementácie bezpečnostnej politiky

Časový plán implementácie bezpečnostnej politiky môže prebiehať spôsobom, ako je to uvedené v tabuľke č. 3.

Tabuľka 3 Časový harmonogram jednotlivých činností v rámci bezpečnostnej politiky (Zdroj: autor)

činnosť	mesiac											
	1	2	3	4	5	6	7	8	9	10	11	12
vypracovanie smerníc	□											
odborné školenie		□				□				□		
zverejnenie informácií		□				□				□		
realizácia úloh		—	—	—	—	—	—	—	—	—	—	—
kontrola plnenia úloh					□						□	
aktualizácia BP												□

Každý podnik je zodpovedný za svoju bezpečnosť a preto jej musí venovať dostatočnú pozornosť a potrebné finančné zabezpečenie. Všetky činnosti sú veľmi dôležité od vypracovania smerníc, cez ich realizáciu, až po následnú kontrolu plnenia úloh.

Kontrola, ako sprievodný jav plánovania, je jednou z najhlavnejších úloh vrcholového manažmentu podniku a završuje celkový proces riadenia. Zisťovanie skutočného stavu a vyvodenie záverov pre ďalšie rozhodovanie je veľmi dôležité pre určenie príčin neplnenia úloh a na následnú zmenu pôvodného plánu. Nesmieme zabúdať ani na potrebu stáleho aktualizovania bezpečnostnej politiky a prispôsobovanie sa zmenám v samotnom podniku.

ZÁVER

Bezpečnostná politika je základným a východiskovým dokumentom pri projektovaní bezpečnostného systému. Predstavuje deklaráciu zodpovednosti podniku za bezpečnosť osôb a ochranu majetku. Bezpečnostná politika určuje chránené záujmy subjektu a stanovuje zásady ako tieto záujmy chrániť. Všetky podniky musia dbať o svoju bezpečnosť, je to základná podmienka pre ich fungovanie. Účelom bezpečnostnej politiky je mať nástroj na zvládanie nebezpečných situácií a najmä zabezpečenia ich riadenia. Bezpečnosť sa začína a končí u zodpovednosti každého zamestnanca. Ľudia bývajú zároveň i najslabším článkom v bezpečnosti, preto je im nutné venovať dostatočnú pozornosť. Podnik si musí zabezpečiť dostačujúce množstvo vzdelaných zamestnancov, alebo si takýchto zamestnancov vychovať prostredníctvom neustáleho vzdelávania a formou školení. Nie je možné navrhnúť univerzálnu bezpečnostnú politiku ktorá by vyhovovala všetkým subjektom.

Cieľom práce bolo objasniť miesto a úlohy bezpečnostnej politiky v podniku a navrhnúť jej možnú štruktúru a spôsob implementácie v podniku. Naplnením tohto cieľa som sa venoval najmä v tretej kapitole. V tejto práci som chcel poukázať na skutočnosť, že bezpečnostná politika, ako záväzný vnútorný dokument podniku, plní svoj účel len vtedy, keď sa ním riadia všetci zamestnanci. Prínosom mojej práce je návrh možnej štruktúry bezpečnostnej politiky, kde som sa snažil objasniť základné oblasti tejto politiky pre všetky podniky. Návrh na dosiahnutie bezpečnostného povedomia zamestnancov a časový plán implementácie bezpečnostnej politiky môže byť spôsob ktorým podniky budú aplikovať bezpečnostnú politiky v praxi.

ZOZNAM POUŽITEJ LITERATÚRY

GAŠPIERIK, L.: *Prednášky z predmetu Manažment bezpečnostných systémov*. 2007.

HOFREITER. L.: *Bezpečnostný manažment*. Žilina: EDIS, 2002.

HOFREITER, L.: *Prednášky z predmetu Bezpečnosť podniku*. 2005.

KUPKOVIČ, M. a kol.: Podnikové hospodárstvo. Bratislava: Sprint, 2001.

REITŠPÍS, J. a kol.: *Manažérstvo bezpečnostných rizík*. Žilina: EDIS, 2004.

ALARM 1/2006.

Bezpečnosť. [cit.2008-01-17]

http://www.securityrevue.com/tbm/part1_b.html#bezpecnost

Bezpečnostný manažment. [cit.2008-01-17]

http://www.securityrevue.com/tbm/part1_b.html#bezpecnostny-manazment

Bezpečnostná politika. [cit.2008-01-17]

http://www.securityrevue.com/tbm/part1_b.html#bezpecnostna-politika

Nová definícia malých a stredných podnikov. (MSP) [cit.2008-03-17]

http://europa.eu.int/comm/enterprise/enterprise_policy/sme_definition/index_en.htm

Definícia podniku. [cit.2008-03-17]

http://www.wikipedia.sk/podnik

Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Zákon č. 314/2001 Z. z. o ochrane pred požiarmi v znení neskorších predpisov.

Zákon č. 330/1996 Z. z. o bezpečnosti a ochrane zdravia pri práci v znení neskorších predpisov.

Zákon č. 428/2002 Z. z. o ochrane osobných údajov v znení neskorších predpisov.

Zákon č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov.