BEZPEČNOSTNÉ MANAŽÉRSTVO
(Bezpečnostný manažment)

ÚVOD

Predpokladaný rozvoj spoločnosti a sním súvisiaci aj nárast množstva hrozieb proti významným záujmom spoločnosti ako celku, ale aj štátnych aj neštátnych inštitúcií, firiem i občanov, kladie neustále zvyšujúce sa nároky na úroveň bezpečnostných štandardov a zároveň tento vysoký štandard neustále ohrozuje. Vysoký bezpečnostný štandard je možné pri neustále sa rozvíjajúcej spoločnosti udržať, len ak sa počet bezpečnostných incidentov bude stále znižovať. K tomu je nevyhnutne potrebný nový rozsiahly systém poznatkov, opatrení a prostriedkov, ktorý ponúka jednotné riešenie bezpečnosti.
Základným princípom je aktívne riešenie bezpečnostných otázok. Ťažiskom je neustále vyhýbanie sa a predchádzanie krízovým situáciám a nehodám. K tomu je nevyhnutné, aby všetky subjekty, ktorých sa bezpečnosť dotýka, venovali primeranú pozornosť otázkam bezpečnosti, v praxi aplikovali manažérstvo bezpečnosti. Základná orientácia vrcholového manažmentu všeobecne, týkajúca sa komplexnej bezpečnosti, musí byť určovaná bezpečnostnou politikou daného subjektu. Na báze manažérstva rizík má reagovať na vzniknuté nežiaduce javy definovanej bezpečnosti a predchádzať im až po prijateľnú mieru rizík. Takáto realizácia bezpečnostnej politiky sa má uskutočňovať metódami a nástrojmi ochrany podopretými právnym a legislatívnym rámcom, zakotveným v bezpečnostnej dokumentácii.
Samozrejme ani bezpečnostné manažérstvo nedokáže zabezpečiť absolútne vylúčenie akéhokoľvek rizika, nehôd a krízových situácií. Ponúka ale nové a lepšie možnosti, spôsoby a metódy preventívneho zaobchádzania s potenciálnymi rizikami. Taktiež otvára nové možnosti odhaľovania a vyšetrovania bezpečnostných incidentov a a krízových situácií a zároveň definuje opatrenia ako im v budúcnosti predchádzať a eliminovať ich.

1 BEZPEČNOSŤ, BEZPEČNOSTNÉ MANAŽÉRSTVO

1.1 Bezpečnosť

Bezpečnosť je základným pojmom bezpečnostnej terminológie a multifaktorovým a mnohoúrovňovým fenoménom. Ako uvádza Mareš (2002) pojem bezpečnosť býva doplňovaný aj rôznymi adjektívami, ktoré sa vzťahujú predovšetkým k charakteru :

a) hrozieb, ktoré bezpečnosť ohrozujú,

b) opatrení, nástrojov alebo inštitúcií, ktoré majú bezpečnosť zabezpečovať a chrániť,

c) objektov, ktorých bezpečnosť má byť chránená

Bezpečnosť možno tiež chápať ako východisko, ako teoretickú konštrukciu a sociálny systém, ktorý má základný význam pre konštituovanie a rozvoj bezpečnostných vied, ktorých objektom, kľúčovým pojmom skúmania je práve tento fenomén.
V literatúre, ktorá sa vyslovuje za vznik bezpečnostných vied, sa zdôrazňuje význam bezpečnosti v súčasnom svete, ako aj zložitosť tohto javu a jeho skúmanie. Holcr a Vicenik (1998) napríklad uvádzajú, že bezpečnosť je zložitý atribút, ktorého obsah, štruktúra a funkcie presahujú hranice nielen jedného vedného odboru, ale dokonca i celých vedných oblastí. Tento fakt možno na základe vlastných teoretických rozborov nielen jednoznačne potvrdiť, ale aj vedecky rozvinúť jeho obsah a formu.
Bezpečnosť a veľmi mnohostranné používanie tohto pojmu v rozmanitých, často protichodných vedných odboroch, spôsobuje jeho eklektickú interpretáciu. Veľmi pragmaticky postihuje tento faktor Porada, Holomek a kol. (2005), a ešte upresňujúcejšie Moller (2001), ktorý rozlišuje päť základných dimenzií bezpečnosti:

- Politická dimenzia
- Ekonomická dimenzia,
- Environmentálna dimenzia,
- Informačná dimenzia
- Sociálna dimenzia

Každá z uvedených dimenzií obsahuje relatívne široký okruh bezpečnostných problémov, subjektov, inštitúcií, činností, aktivít a vzťahov. Okrem

spomínaných dimenzií multidimenzionalita bezpečnosti umožňuje analyzovať aj niektoré jej ďalšie rozmery (vonkajšie, vnútorné, subjektívne, objektívne, individuálne, policajné, vojenské, občianske, spoločenské, ľudské, technologické, kvantitatívne, kvalitatívne, a iné, napr. na VŠBM v Košiciach rozvíjaná bezpečnosť systémov, bezpečnosť informačných technológií, bezpečnosť v doprave a dopravnej infraštruktúre a i.).
Preto je vymedzovaná napr. bezpečnosť vojenská, ekonomická, ekologická, sociálna, ľudská a pod. Predovšetkým z hľadiska objektu, ktorého bezpečnosť má byť chránená (doteraz spravidla národného štátu), možno rozlišovať bezpečnosť vnútornú (ak ide o existenciu, potláčanie a elimináciu hrozieb, ktorá pochádza z vnútra objektu) a bezpečnosť vonkajšiu (ak ide o existenciu, potláčanie a elimináciu hrozieb, ktoré majú svoj pôvod mimo objektu). Všetky vyššie uvedené pojmy sú spravidla vzájomne previazané a ich ohraničenie nie je úplne jednoznačné. Bezpečnosť je teda pojem komplexný.
Pojem bezpečnosť (opak nebezpečenstvo) sa stal frekventovaným pojmom, ktorý vyjadruje podľa zvoleného uhla pohľadu rôzny obsah vo vzťahu ku skúmaným dimenziám. V súčasnej dobe je však celkom zrejmé, že predovšetkým v štátnych orgánoch, v akademickej sfére budú pretrvávať rozdielne názory na efektívny rozsah bezpečnosti z hľadiska štátnej politiky.
Mareš (2002) odporúča definovať všeobecnú definíciu bezpečnosti vo vzťahu k akémukoľvek konkrétnemu objektu. Definuje „bezpečnosť ako stav, kedy sú na najnižšiu možnú mieru eliminované hrozby pre objekt (spravidla národný štát, ale aj organizácia, spoločenstvo, osoba) a jeho záujmy a tento objekt je k eliminácii existujúcich aj potenciálnych hrozieb efektívne vybavený a ochotný pri nej spolupracovať“.

1.2 Obsah a pojem bezpečnostného manažérstva

Vrcholoví manažéri rôznych firiem a organizácií, výrobcov a poskytovateľov služieb majú osobitnú zodpovednosť za bezpečnosť, resp. za manažérstvo bezpečnosti. Skúsenosti z rôznych oblastí výroby a služieb nasvedčujú, že najbezpečnejšie organizácie sú zvyčajne najefektívnejšie. Dosiahnutie a udržanie určitého štandardu bezpečnosti spravidla vyžaduje kompromisy medzi manažérstvom bezpečnosti a nákladmi, ktoré sú na dosiahnutie určitého štandardu nevyhnutné. Manažment musí rozpoznať „skrytú cenu“ dôsledkov bezpečnostných incidentov, ktorá zahŕňa nielen priame straty, ale aj straty dôvery verejnosti, zákazníkov, alebo prípadných obchodných partnerov. Systematickým prístupom k rozhodovaniu a manažérstvu rizík je možné zredukovať straty spojené s prípadnými bezpečnostnými incidentmi.
Manažment má právo a zároveň zodpovednosť za riadenie rizík v rámci organizácie, ktorú riadi. Dosahuje sa to ustanovením systematického spôsobu pre identifikáciu rizík, hodnotenie rizík, prideľovaním priorít týmto rizikám a následne redukciou, alebo elimináciou týchto rizík, ktoré predstavujú najväčšie

potenciálne straty. Samotný manažment má schopnosť zaviesť zmeny do organizačnej štruktúry, personálnej štruktúry, technologického vybavenia a postupov.
Predovšetkým manažment stanovuje organizačné prostredie pre bezpečnosť. Bez absolútneho nasadenia v prospech bezpečnosti bude riadenie bezpečnosti neúčinné. Pozitívnou podporou bezpečnostných opatrení, manažment vysiela odkaz všetkým zamestnancom , že majú záujem o bezpečnosť a že by tento záujem mali mať aj zamestnanci.
Manažment musí zadefinovať bezpečnosť ako základnú hodnotu organizácie. Dosiahnuť to môže stanovením cieľov bezpečnosti, následne rozdelením zodpovednosti medzi manažérov a zamestnancov za dosahovanie týchto cieľov. Zamestnanci sa obracajú na manažment kvôli:

a) ***jednoznačné smerovanie*** vo forme dôveryhodných stratégií, cieľov, štandardov, atď.,
b) ***adekvátnym zdrojom,*** vrátane dostatočného časového priestoru pre plnenie pridelených úloh bezpečným a efektívnym spôsobom, a
c) ***odborným znalostiam***, v zmysle prístupu k skúsenostiam – prostredníctvom literatúry, výcviku, seminárov, atď.

Táto povinnosť sa vzťahuje na manažment bez ohľadu na veľkosť alebo druh organizácie, ktorá príslušné služby poskytuje. (ICAO safety)

Obsah bezpečnostného manažérstva 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.

Bezpečnostné manažérstvo je aj súčasťou prevencie proti kriminalite. V priebehu uplatňovania jeho funkcií ide o plánovanie a realizáciu takých opatrení, ktoré zmenšia pravdepodobnosť vzniku bezpečnostných ohrození tým, že zmenia podmienky tých predpokladov, ktoré umožňujú aktiváciu bezpečnostných rizík na bezpečnostné ohrozenia. Ide o realizáciu takých opatrení, ktoré :

- bránia alebo zabránia vzniku bezpečnostných ohrození (bezpečnostných incidentov),
- ovplyvňujú výšku „nákladov" a „zisku" potenciálneho páchateľa,
- zvyšujú riziko odhalenia a zadržania páchateľa.

Bezpečnostné manažérstvo 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 napr. 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.

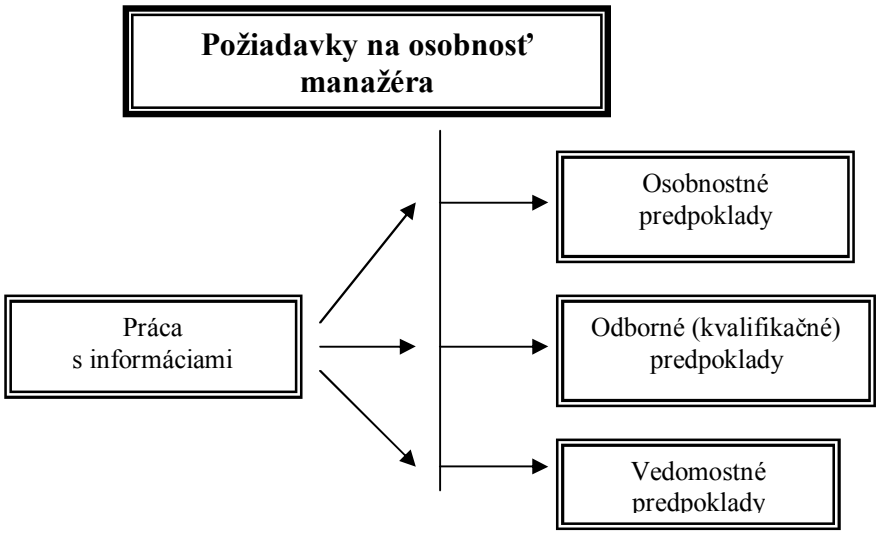
Požiadavky na osobnosť manažéra

V existenčnom procese ako takom, človek ako prvok – systém, vytvára také podmienky a prostredie, aby v ňom mohol a bol schopný následne aplikovať získané teoretické vedomosti. Pokiaľ všetky svoje postupy smeruje len na teoretickú úroveň, nikdy nezíska nové možnosti na inováciu a reštrukturalizáciu svojich doterajších výsledkov. Len vtedy jeho počínanie bude mať v podmienkach praxe význam, pokiaľ svoje získané zručnosti bude aj reálne implementovať v materiálnom prostredí.
V procese manažérskej činnosti má **manažér** nezastupiteľnú úlohu. Túto pracovnú pozíciu môže vykonávať len ten pracovník, ktorý má na to odborné, vedomostné, kvalifikačné a osobnostné predpoklady. Jednoducho, túto prácu musí nielen vedieť robiť, ale aj chcieť robiť. Na osobnosť manažéra sa kladú vysoké nároky a požiadavky, pretože na jeho riadiacich schopnostiach a predpokladoch funguje celý systém – organizácia, a on za svoje rozhodnutia a z nich vyplývajúce dôsledky zodpovedá.

Vo všeobecnosti, manažér by mal mať:
1. *osobnostné predpoklady***:** predstavujú požiadavky intelektu, schopnosť mať predispozície na túto prácu, myslieť ako riadiaci pracovník, schopnosť viesť tím ľudí, vedieť povedať „nie“,
2. *odborné (kvalifikačné)***:** prioritne vzdelanie v oblasti manažmentu, rozšírenie si vedomostí vykonaním odborných a kvalifikačných skúšok, komunikácia s externým (zahraničným) okolím,
3. vedomostné: schopnosť neustále sa vzdelávať a prijímať nové trendy v systéme riadenia, iniciatívne vyhľadávať problematiku manažovania (kurzy, školenia), snaha dopĺňať a prijímať nové možnosti od iných spolupracovníkov.
Zhrnutím tých základných požiadaviek na osobnosť manažéra sa dostávame k všeobecnému pravidlu riadenia – *práca s informáciami***,** ktorá predstavuje podstatnú časť v činnosti manažovania. Ich správne analytické spracovanie a následné vyhodnotenie vedie k podstatným krokom rozhodovania a efektívnej realizácii každej funkcie manažmentu. Efektívna a cielená práca s informáciami zvyšuje kvalitu myslenia a významne šetrí čas.
Základné princípy pri práci s informáciami:
- manažér si vymieňa informácie pri medziľudskom kontakte,
- manažér sa zúčastňuje na procese práce s informáciami a informačnými systémami,

- manažér využíva informácie pri rozhodovaní.

Všetky tieto činnosti predstavujú **komplexný informačný proces**, ktorý je základným predpokladom riadenia a ďalšieho rozvoja organizácie.



Obrázok 1.1: Vzťah medzi požiadavkami na osobnosť manažéra a prácou s informáciami

Pri analyzovaní osobnosti manažéra je potrebné vychádzať aj z iných **predpokladov – vlastností**, ako:

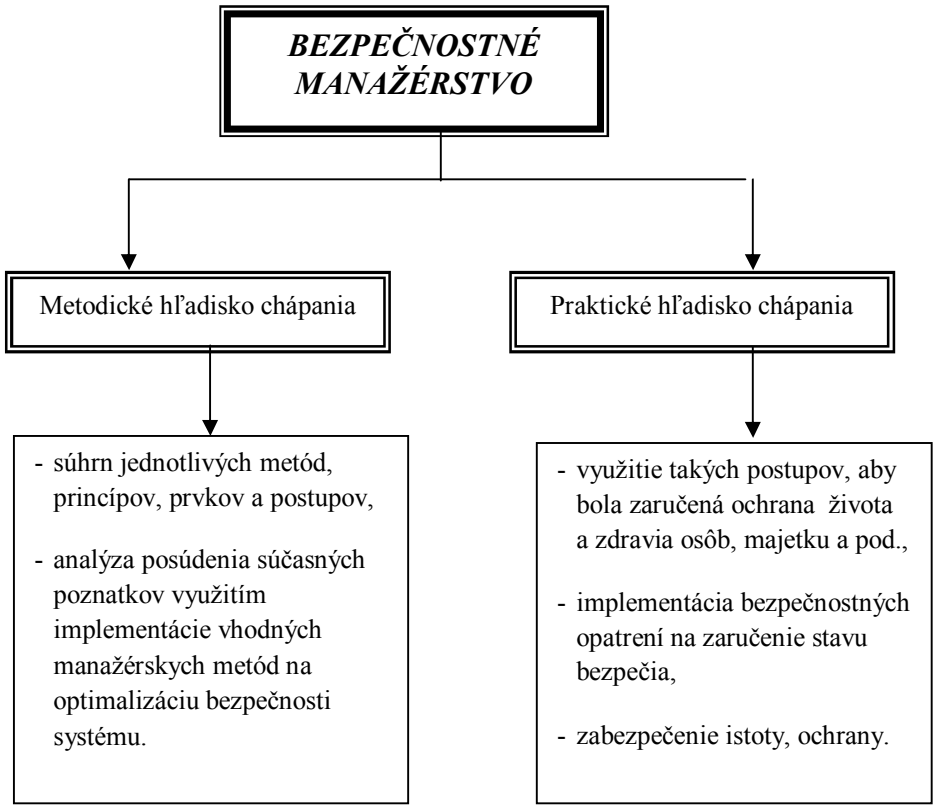
- *aktivačno – motivačné vlastnosti* (postoje, záujmy, hodnoty),
- *sebaregulačné vlastnosti* (svedomie, charakter),
- *výkonové vlastnosti* (fyzické vlastnosti, inteligencia, tvorivosť),
- *sociálno – vzťahové vlastnosti* (vplývať na ľudí, komunikovať).

Kompetencie manažéra môžeme definovať ako **súbor** znalostí, schopností, zručností a skúseností ako aj fyzickej a psychickej pripravenosti tieto kvality využiť na efektívne vykonávanie určitých úloh (funkcií a rolí) v súlade s pridelenou právomocou a všeobecným očakávaním. (Míka-Šimák-Hudáková-Horáček, 2009)

Podstata bezpečnostného manažérstva spočíva v ucelenej a systematickej aplikácií tých metód, postupov a činností, ktorými možno predpokladať splnenie vytýčeného cieľa za určitých podmienok.

Bezpečnostné manažérstvo pre bezpečnostnú prax je nenahraditeľné. Touto problematikou sa zaoberajú nielen subjekty pracujúce v predmetnom prostredí, či už vo verejnom alebo súkromnom sektore, ale čoraz častejšie sa s touto témou môžeme stretnúť v rôznych odborných publikáciách, či v dennej tlači. Čas ukázal, že záujem o študovanie problematiky manažérstva a bezpečnosti ako

takej úmerne stúpa takou konštantou, akou stúpajú sociálne rozdiely, s čím súvisí páchanie kriminality. Oblasť bezpečnosti sa postupom času presunula od jednotlivca k spoločnosti ako celku. V súčasnosti ju kompetentní riešia nielen na teritoriálnej úrovni , ale aj kontinentálnej. Tieto tendencie spôsobujú neustále rastúci záujem a podrobnejšie študovanie *bezpečnosti*, ktorá zaručuje ochranu nielen jednotlivca , ale aj veľkej skupiny ľudí – spoločnosti. Na to, aby tento jav riadne, efektívne ale najmä systematicky fungoval, sa v tej ktorej zložke systému touto problematikou zaoberá určitá skupina ľudí, ktorá nesie zodpovednosť nielen za svoje výsledky, ale predovšetkým za rozhodnutia , ku ktorým po dôkladných analýzach pristúpia.
Súhrne povedané, bezpečnostné manažérstvo sa metodicky zameriava na správnu aplikáciu tých, metód, postupov a princípov, výsledkom ktorých je efektívne fungujúci systém. Z pohľadu bezpečnostnej praxe hovoríme o zabezpečení maximálnej ochrany jednotlivca a celku takým spôsobom, aby jeho stav ohrozenia nebol žiaden, resp. minimálny.



Obrázok 1.2: Rozdielne chápanie bezpečnostného manažmentu

Spoločenský život determinuje rôzne správanie sa ľudí v závislosti od vzniknutej situácie. Samozrejme tento fakt ovplyvňuje celý rad všeobecných

alebo individuálnych aspektov. Je veľmi dôležité uvedomenie si všeobecných podmienok materiálneho prostredia, v ktorom jednotlivec žije a potom následne aj jeho osobnostné črty. Na základe toho sa prejavuje určitým spôsobom pre seba blízkym a jeho konanie je výsledkom myšlienkových postupov, ktoré vyhodnotil podľa neho za najoptimálnejšie.

V tomto prípade je potrebné poukázať na **individuálnosť jednotlivca** v spoločnosti a jeho rôzne vnímanie javov, ktoré sa dejú v jeho prostredí. Aj on potom, bezpečnostné manažérstvo chápe rôznym spôsobom. Jeho podstatu a význam si vysvetľuje tak, ako mu je najbližšie.
Na základe toho sú uvádzané dve úrovne – hľadiská chápania bezpečnostného manažérstva, a to :
- *metodické hľadisko* chápania (založené na teoretickom ponímaní jeho významu),
- *praktické hľadisko* chápania (chápané z pohľadu praktického využitia).

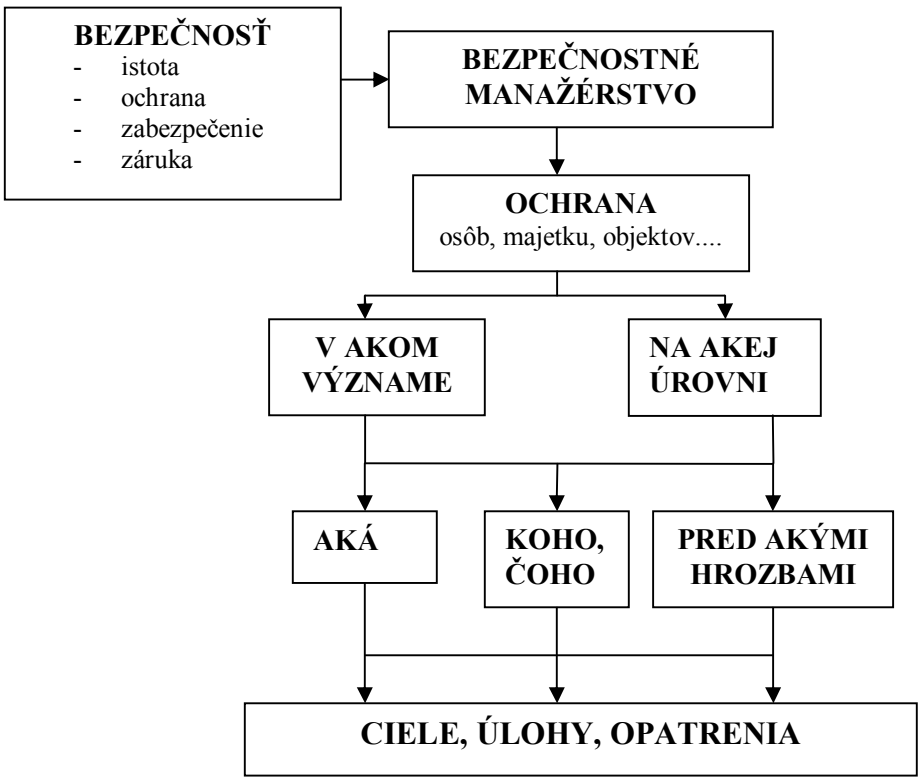
Každé z nich obsahu tie špecifiká, ktoré ho najistejšie vystihujú.

Pozitíva bezpečnostného manažérstva v praxi:

- Bezpečnostné manažérstvo vedie k redukcii bezpečnostných incidentov a krízových situácií,
- Bezpečnostné manažérstvo je pre bezpečnosť a ochranu života, zdravia, majetku a iných dôležitých záujmov štátu, firiem aj jednotlivcov nevyhnutné,
- Bezpečnostné manažérstvo predstavuje systém teoretických poznatkov a praktických opatrení, na základe odporúčaní bezpečnostných štandardov zabezpečuje dokonalú a prehľadnú bezpečnostnú dokumentáciu,
- v Bezpečnostnom manažérstve sú uvedené a jasne vysvetlené všetky zodpovednosti týkajúce sa bezpečnosti,
- existencia Bezpečnostného manažérstva v spoločnosti sa stáva stále významnejším pozitívnym faktorom i pri uzatváraní nových zmlúv s obchodnými partnermi,
- dobrý bezpečnostný štandard v danej spoločnosti je pozitívne vnímaný i vlastnými zamestnancami, obchodnými partnermi a predovšetkým zákazníkmi a v neposlednom rade i spoločenským a politickým prostredím.

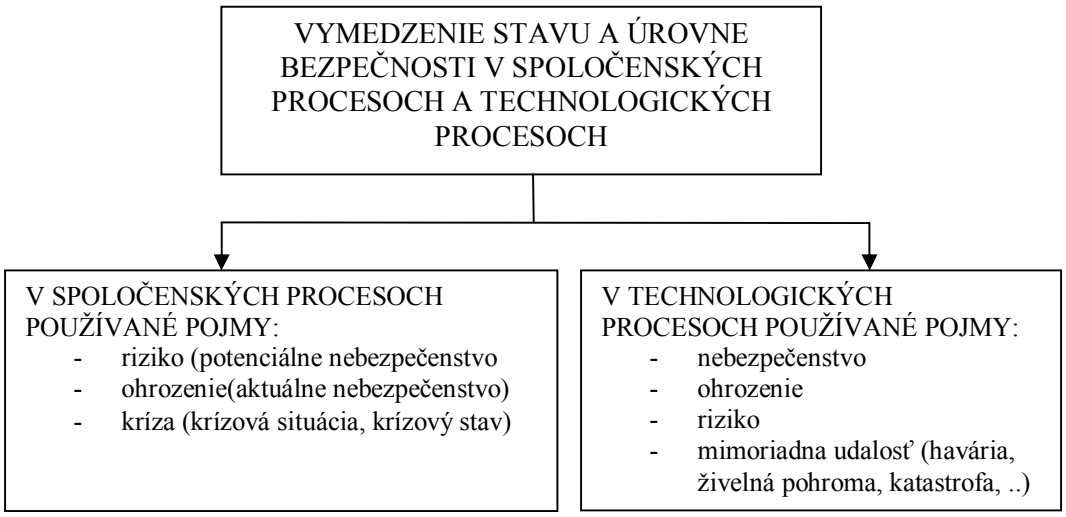
Bezpečnostné manažérstvo predstavuje systematickú integráciu a prepojenie teórie a praxe, bezpečnostných štandardov a opatrení týkajúcich sa každodennej prevádzky daného subjektu (inštitúcie, firmy) s ohľadom na ľudské, technické a organizačné faktory.

Na základe doterajších skúseností a zisťovania príčin bezpečnostných incidentov, nehôd a krízových situácií boli zostavené pravidlá ochrany a eliminácie rizík, incidentov a nehôd. Tento systém porovnáva bezpečnosť s riadením ostatných prevádzkových procesov. Je to vlastne i systematický, prehľadný a rozsiahly proces kontroly rizík. Takýto systém umožňuje jasné stanovenie cieľov, plánovania a kontrolovania bezpečnosti. Bezpečnostné manažérstvo je priamo prepojené s prevádzkou a je zároveň súčasťou podnikateľskej kultúry, pracovných postupov a metód.
Bezpečnostný manažment má za úlohu vytvoriť systém (bezpečnostný), ktorý odpovedá možnostiam, potrebám, prostrediu a požiadavkám maximálnej úrovne ochrany.
K vlastnému riešeniu problematiky bezpečnostného manažérstva je nutné zaviesť jednotnú terminológiu s vedomím aké otázky a v akom rozsahu daný bezpečnostný systém má za úlohu riešiť (obr. 1.1).



Obr. 1.3: Priestor pojmového aparátu bezpečnostného manažérstva

Bezpečnostné manažérstvo predstavuje špecifickú formu manažérskej činnosti, ktorá je zameraná na bezpečnosť v spoločenských procesoch a technologických procesoch, čím sú zároveň vymedzené aj základné oblasti pojmov bezpečnostného manažérstva.



Obr. 1.4: Oblasti pojmov bezpečnostného manažérstva

1.3 Prehľad vybraných pojmov

Vnútorná bezpečnosť štátu **-** je stav, v ktorom sú na minimálnu mieru eliminované ohrozenia štátu a jeho záujmov zvnútra a štát má vytvorené dostatočné právne prostredie, inštitúcie, zdroje, sily, prostriedky a mechanizmy na riešenie možných krízových situácií. Je to tiež spoločnosťou akceptovaná úroveň demokracie, ekonomickej prosperity, ochrany občanov a uplatňovania právnych noriem, ktorých zabezpečovanie je jednou zo základných funkcií štátu.
Verejný poriadok **-** je taká úroveň spoločenských vzťahov vznikajúcich a prejavujúcich sa v správaní ľudí prevažne na verejnosti a regulovaných sociálnymi normami, ktoré sú podľa charakteru miesta, času a verejnej mienky nevyhnutnou podmienkou pre fungovanie verejnej správy, činnosť právnických a podnikajúcich fyzických osôb, pre život občanov, v súlade so zásadami stanovenými právnym poriadkom, ale aj s názormi spoločnosti na správanie ľudí.
Bezpečnostné prostredie - je časť sociálneho a prírodného prostredia, v ktorom sú podmienky existencie a vývoja sociálneho objektov, ich činnosti, vzťahy a záujmy determinované v prvom rade bezpečnosťou. Vyjadruje predovšetkým priestorovú dimenziu bezpečnosti spojenú s pôsobením subjektov v určitom čase a podmienkach. Predstavuje najširší pojem, ktorý vyjadruje bezpečnostnú situáciu v určitom priestore v určitom čase, pričom táto bezpečnostná situácie je výsledkom aktivít relevantných bezpečnostných aktérov (bezpečnostných orgánov, inštitúcií, štátov, koalícií štátov ap.).

Bezpečnostné prostredie vo vzťahu k štátu je súbor vnútorných a vonkajších faktorov ovplyvňujúcich jeho bezpečnostnú politiku. Je ním možné rozumieť priestor nachádzajúci sa vo vnútri štátu i mimo neho, v ktorom sa realizujú a stretávajú záujmy štátu so záujmami iných aktérov medzinárodných vzťahov a kde sa odohrávajú procesy, ktoré majú významný vplyv na úroveň bezpečnosti štátu.

Bezpečnostná situácia - je výsledkom procesov a vzťahov vo sfére nevojenskej i vojenskej bezpečnosti, je súhrnom vzťahov politického, kultúrno-sociálneho, ekonomického, vojenského a ekologického prostredia ako celku. Je tiež určovaná vnútroštátnymi a medzinárodnými bezpečnostnými pomermi a ovplyvňovaná parametrami vnútornej a vonkajšej bezpečnosti štátu a celým súborom aktivít zahraničnej politiky, ekonomického rozvoja krajiny, sociálnej stability, rozvoja demokracie a rešpektovania ľudských práv a súborom bezpečnostných dôsledkov, vyplývajúcich so zmluvných záväzkov štátu.

Ohrozenie – je stav systému, ktorý vzniká a trvá v dôsledku existencie a uvedomenia si potenciálneho narušenia jeho rovnovážneho stavu. Je to aktivizované riziko, ktoré pôsobí proti záujmom subjektu a konkrétnej situácie, ktoré bezprostredne znemožňujú naplnenie jeho záujmov.

Riziko - je potenciálna možnosť narušenia bezpečnosti systému, objektu alebo procesu. Je to pravdepodobnosť vzniku bezpečnostného incidentu a jeho dôsledku.

Predstavuje možnosť, že s určitou pravdepodobnosťou vznikne udalosť z bezpečnostného hľadiska nežiaduca. Riziko je vždy odvodené z konkrétnej hrozby. Mieru rizika, teda pravdepodobnosť škodlivých následkov vyplývajúcich z hrozby a zo zraniteľnosti záujmov, je možné posúdiť na základe tzv. analýzy rizík, ktorá vychádza i z posúdenia pripravenosti čeliť hrozbám. Riziko je pravdepodobnosť, že dôjde k poškodeniu či strate, ktoré postihnú určité ciele. Je to možnosť, že s určitou pravdepodobnosťou vznikne stav líšiaci sa od takého, aký považujeme za žiaduci. Riziko je fenomén sekundárny, t.j. odvodený a odvoditeľný. Riziko je reakciou na hrozbu a na stav pripravenosti (zraniteľnosti) zároveň. Je spojené s rozhodovaním a ľudskou činnosťou.

Vzťah rizika a ohrozenia je najpodrobnejšie rozpracovaný v rámci bezpečnosti informačných technológií. Nasledujúce grafické znázornenie je prevzaté z tejto normy. Ilustratívne znázorňuje povahu vzťahu ohrozenia a rizika a ďalších pojmov (hodnota, zraniteľnosť, proti opatrenia). Tabuľka znázorňuje výsledné riziko, ako súčin veľkosti ohrozenia a predpokladané výšky straty.

Tabuľka č. 1.1 (Analýza vývoja vnútornej bezpečnosti 2010)

vodorovne mohutnosť hrozby / ***zvisle*** výška straty na	**zanedbateľná (1)**	**nízka (2)**	**stredná (3)**	**vysoká (4)**	**veľmi vysoká (5)**

hodnote					
zanedbateľná (1)	riziko celkom zanedbateľné	riziko takmer zanedbateľné	riziko dosť nízke	riziko nízke	riziko stredné
nízka (2)	riziko takmer zanedbateľné	riziko veľmi nízke	riziko nízke	riziko stredné	riziko vysoké
stredná (3)	riziko veľmi nízke	riziko dosť nízke	riziko stredné	riziko vysoké	riziko veľmi vysoké
vysoká (4)	riziko dosť nízke	riziko nízke	riziko stredné až vysoké	riziko veľmi vysoké	riziko mimoriadne vysoké
veľmi vysoká (5)	riziko nízke	riziko stredné	riziko vysoké	riziko mimoriadne vysoké	riziko katastrofických rozmerov

Nebezpečenstvo **-** je latentná vlastnosť daného systému alebo jeho komponentov spôsobovať neočakávané negatívne javy, ktoré narušujú bezpečnosť, ohrozujú stabilitu a fungovanie príslušného systému, prípadne aj jeho okolia.

Analýza rizík - je proces podrobnej identifikácie a rozboru rizík, určovania ich zdrojov a veľkosti, skúmania ich vzájomných vzťahov a predpovedania rozsahu negatívneho vplyvu na systém v prípade vzniku krízovej situácie.

Bezpečnosť chráneného objektu - je kvalifikovaná úroveň fyzickej, technickej alebo funkčnej bezpečnosti chráneného objektu, jeho integrity a funkcií, stav, kedy chránenému objektu reálne nehrozí žiadne nebezpečenstvo a jeho fyzická alebo technická bezpečnosť, sebarealizácia, funkcie, podstata a určené činnosti prebiehajú spôsobom (sú v stave) postavenia, určenia alebo poslania.

Ochrana objektu a ochrana priestoru súbor technických, organizačných a režimových opatrení realizovaných za účelom zabránenia, resp. sťaženia útočníkovi vniknúť do objektu, alebo priestoru, alebo monitorovania činnosti útočníka v chránenom objekte alebo priestore, alebo signalizácie pokusu útočníka o vniknutie do chráneného objektu alebo priestoru, alebo zabránenia protiprávnemu konaniu útočníka v chránenom objekte alebo priestore.

Porucha bezpečnosti chráneného objektu **-** je kvalifikovaná úroveň potenciálneho ohrozenia alebo chyby v systéme (úrovni) bezpečnosti chráneného objektu, stav, kedy bezpečnosť alebo výkon funkcií alebo účel chráneného objektu alebo jeho hodnota, podstata (integrita) sú reálne ohrozené, hrozí alebo vzniká porucha, krízový stav, priamo na chránenom objekte alebo

porucha systému ochrany alebo subjektu zabezpečujúceho ochranu, pričom následok (škoda) ešte nastať nemusel.

Útok na objekt - je bezprostredné ohrozenie bezpečnosti chráneného objektu, najmä priama bojová akcia, teroristický útok, priamo alebo bezprostredne prebiehajúca násilná trestná činnosť alebo iné protiprávne konanie, smerujúce proti bezpečnosti chráneného objektu alebo subjektu zabezpečujúceho ochranu s cieľom získať chránený objekt alebo jeho časť do moci útočníka, pod jeho kontrolu, eliminácie alebo poškodenia chráneného objektu alebo získania politického, ekonomického alebo iného prospechu alebo spôsobenia inej ujmy alebo škody.

Objekt osobitnej dôležitosti - je strategický objekt kritickej infraštruktúry určený vládou Slovenskej republiky na návrh určených orgánov štátnej správy, orgánov miestnej štátnej správy a samosprávy a iných právnických osôb, ktorého poškodenie alebo zničenie by ohrozilo bezpečnosť štátu a životne dôležité záujmy Slovenskej republiky a ktorý podlieha vládou SR schválenému spôsobu ochrany a obrany.

Verejný záujem - je dôležitý spoločenský záujem štátu, regulovaný výkonom verejnej moci, ktorý prevažuje nad oprávneným záujmom fyzickej osoby alebo viacerých fyzických osôb a prináša prospech ostatným fyzickým osobám alebo viacerým z nich. Bez jeho realizácie by mohli vzniknúť rozsiahle alebo nenahraditeľné škody v oblasti bezpečnosti štátu, verejného poriadku, ochrany zdravia, ochrany práv a slobôd iných osôb. Takýmto záujmom je aj bezpečnosť ústavných činiteľov, ústavných inštitúcií a výkon ich ústavných pôsobností.

Ústavný činiteľ - je predstaviteľ Ústavou Slovenskej republiky kreovaného orgánu, najmä moci zákonodarnej, výkonnej a súdnej. Rovnaké postavenie má aj zahraničný štátny predstaviteľ, na roveň postavený ústavnému činiteľovi Slovenskej republiky. ***Bezpečnosť štátu*** – *je s*tav, ktorý umožňuje fungovanie, stabilitu a rozvoj štátu, zachováva mier, zvrchovanosť, územnú celistvosť a nedotknuteľnosť hraníc, vnútorný poriadok v štáte, základné práva a slobody občanov a ochranu životov a zdravia osôb, majetku a životného prostredia.

Civilná ochrana – je systém úloh a opatrení zameraných na ochranu života, zdravia a majetku, spočívajúcich najmä v analýze možného ohrozenia a v prijímaní opatrení na znižovanie rizík ohrozenia, ako aj určenie postupov a činnosti pri odstraňovaní následkov mimoriadnych udalostí. Poslaním civilnej ochrany je v rozsahu určenom zákonom chrániť život, zdravie a majetok a utvárať podmienky na prežitie pri mimoriadnych udalostiach a počas vyhlásenej mimoriadnej situácie.

Kategorizácia územia – je proces začleňovania územných celkov do skupín charakterizovaných porovnateľným stupňom ohrozenia s možnosťou vzniku krízových situácií a následného určovania diferencovaného rozsahu plánovaných preventívnych opatrení na ochranu obyvateľov a majetku.

Kritická infraštruktúra **–** sú to najmä objekty osobitnej dôležitosti, ďalšie dôležité objekty, vybrané informačné a komunikačné prostriedky, zariadenia na

výrobu a zásobovanie vodou, elektrickou energiou, ropou a zemným plynom a ďalšie časti majetku štátu a podnikateľských právnických a fyzických osôb určené vládou SR alebo iným kompetentným orgánom štátnej správy, ktoré sú nevyhnutné na zvládnutie krízových situácií, ochranu obyvateľstva a majetku, na zaistenie minimálneho chodu ekonomiky a správy štátu, ako aj jeho vonkajšej a vnútornej bezpečnosti a ktoré treba špeciálne ochraňovať. Sú to zariadenia, služby a informačné systémy životne dôležité pre obyvateľov a riadenie štátu, ktorých strata funkčnosti alebo zničenie môže ohroziť bezpečnostné záujmy štátu.

Krízový manažment – je súhrn riadiacich činností orgánov krízového riadenia, ktoré sú zamerané na analýzu a vyhodnotenie bezpečnostných rizík a ohrození, plánovanie, prijímanie preventívnych opatrení, organizovanie, realizáciu a kontrolu činností vykonávaných pri príprave na krízové situácie a pri ich riešení. Tiež špecifický druh riadenia využívaný v krízových situáciách. Je to činnosť riadiacich pracovníkov ako systém odborných aktivít smerujúcich k obmedzeniu možnosti vzniku kríz a minimalizácie ich dôsledkov.

Živelná pohroma - je mimoriadna udalosť vyvolaná ničivými prírodnými silami, v ktorej dôsledku sa uvoľňujú kumulované energie a hmoty, prípadne pôsobením nebezpečných látok, alebo iných ničivých faktorov majúcich negatívny vplyv na človeka, zvieratá, materiálne hodnoty a životné prostredie**.** (Analýza vývoja vnútornej bezpečnosti 2010)

Chemické ohrozenie - je nebezpečenstvo použitia útoku chemickou látkou, ktorý môže byť uskutočnený rozptýlením toxických chemických látok do životného prostredia v kvapalnom, plynnom, pevnom (práškovom) stave alebo použitím aerosolov, najmä v priestoroch vysokej koncentrácie obyvateľstva alebo v objektoch a zariadeniach určených na hromadné zásobovanie.

Biologické ohrozenie - pravdepodobná možnosť úmyselného použitia biologických látok, prostriedkov alebo zbraní na živé organizmy alebo vegetáciu za účelom presadenia si individuálnych alebo skupinových záujmov nelegálnym spôsobom.

Jadrové a rádiologické ohrozenie - je nebezpečenstvo, ktoré môže byť spôsobené použitím jadrových alebo rádioaktívnych látok teroristickým útokom, či rôznych druhov prostriedkov na dôležité objekty, zoskupenia obyvateľstva a vodné zdroje za účelom ohrozenia života, zdravia a majetku, prípadne spôsobenia paniky.

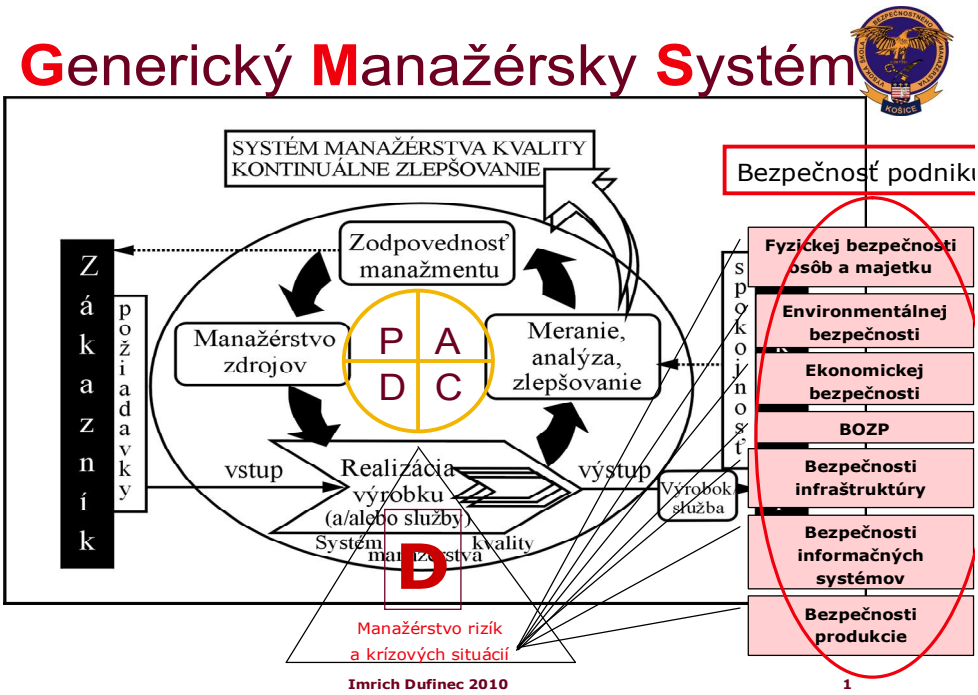
Zdravotnícke zabezpečenie **–** je súhrn zdravotníckych, hygienických a protiepidemiologických opatrení na zabezpečenie zdravotnej starostlivosti obyvateľstva, ozbrojených síl, ozbrojených bezpečnostných zborov a ostatných zložiek v príprave na riešenie krízových situácií a počas ich riešení.

1.4 Štruktúra a princípy bezpečnostného manažérstva

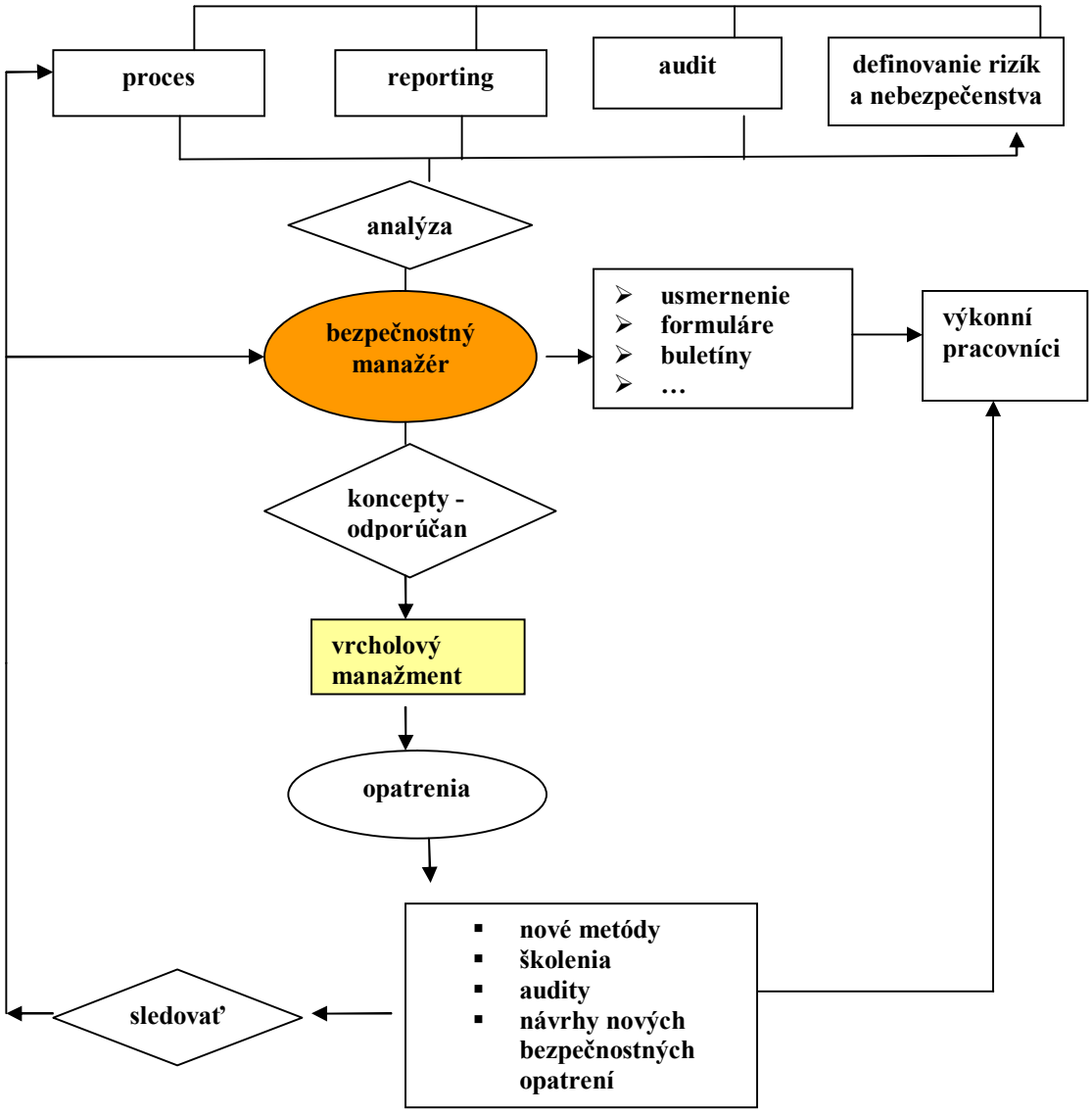
Bezpečnostné manažérstvo môže byť úspešné len za predpokladu, že sa na ňom budú aktívne podieľať a zároveň ho budú plne podporovať všetky zúčastnené subjekty.

Bezpečnostné manažérstvo je zamerané predovšetkým na:

- hlavné bezpečnostné línie podnikania (bezpečnostná politika),
- na funkciu bezpečnostného manažéra,
- procesnú dokumentáciu a stanovenie zodpovedností,
- identifikáciu nebezpečenstiev a manažment rizík,
- reporting relevantných bezpečnostných dôsledkov,
- skúmanie a vyšetrovanie dôsledkov,
- audit a kontrolu v danom subjekte (firme,)
- prispôsobovanie bezpečnostných princípov a metód (manažment zmien),
- stanovenie bezpečnostných opatrení,
- nepretržitá kontrola účinnosti bezpečnostných opatrení,



Obr. 1.5 Bezpečnostné manažérstvo v manažérskom systéme podniku (Dufinec 2011)



Obr. č. 1.6: Štruktúra bezpečnostného manažérstva

Vybavenie bezpečnostného manažéra

Bezpečnostný manažér resp. tím, ktorý riadi, musí disponovať zodpovedajúcimi zdrojmi, aby dokázal splniť náročné úlohy pri zabezpečovaní bezpečnosti a ochrany.
To znamená príprava:

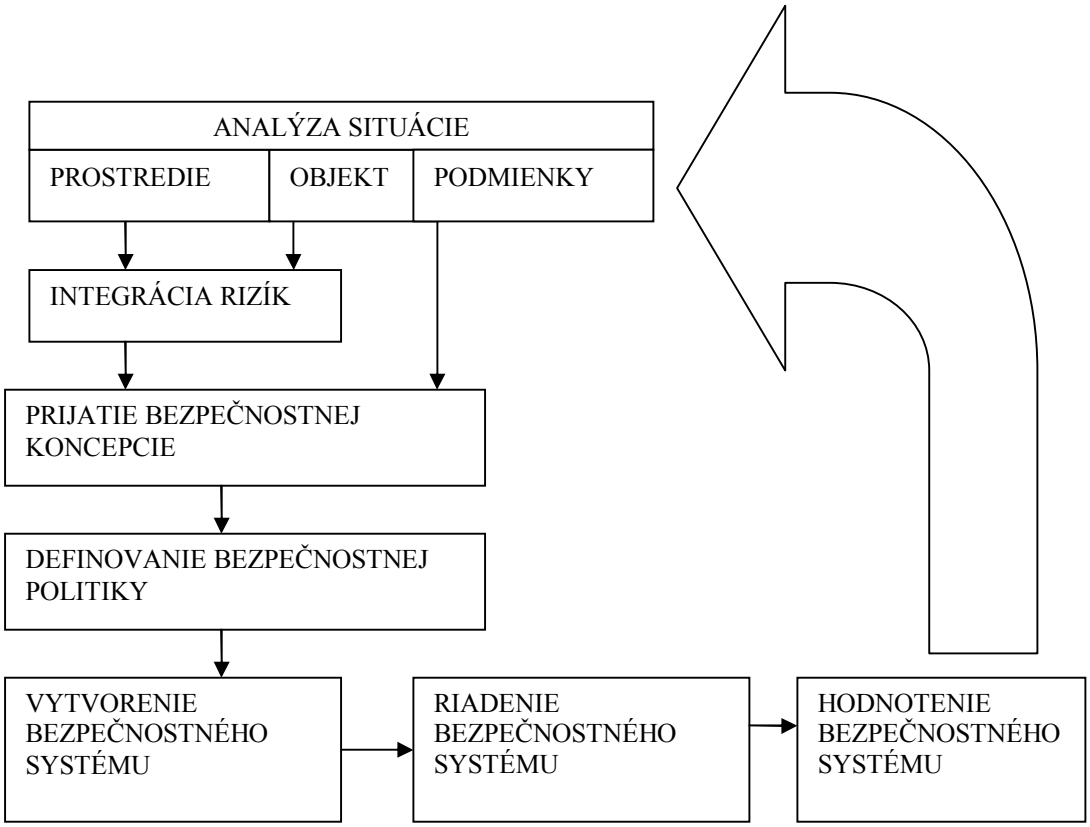
- personálnych zdrojov v súvislosti s možnosťami prevádzky,
- materiálnych zdrojov (kancelárie, rozpočet,...),
- technických zdrojov (telefón, fax, internet,...).

a to v spolupráci s vedením inštitúcie, spoločnosti, firmy....

Spolupráca v rámci bezpečnostného manažérstva

Vrcholový manažment je povinný zabezpečiť, aby všetci zamestnanci dodržiavali relevantné bezpečnostné predpisy a zároveň, aby v prípade potreby spolupracovali s bezpečnostným manažérom..
Splnenie tejto povinnosti je nevyhnutné implementovať s ohľadom na bezproblémové bezpečné fungovanie organizácie.

Proces činnosti bezpečnostného manažérstva

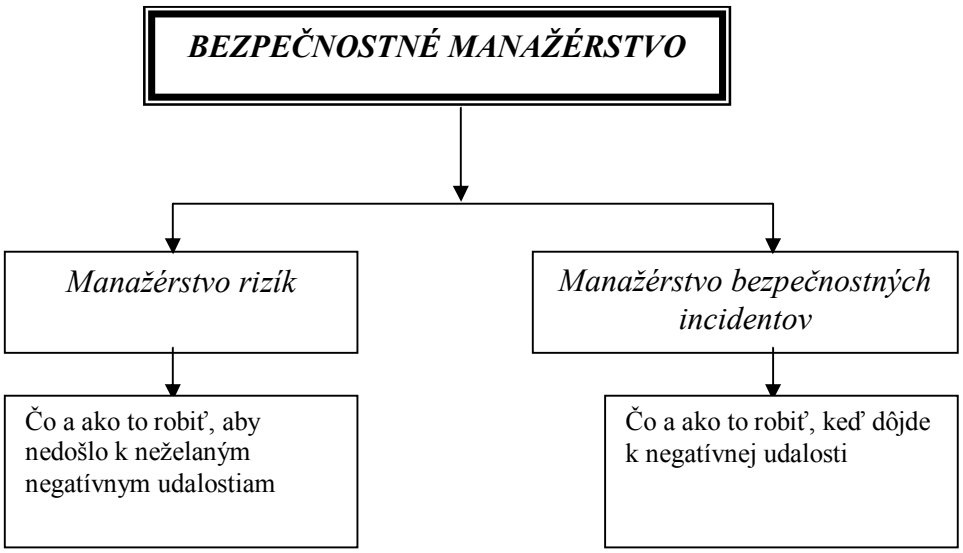


Obr.1.7. Proces činností bezpečnostného manažérstva

Bezpečnostné manažérstvo nerieši len preventívne hľadisko daného procesu, ale zaoberá sa aj represívnym riešením fungovania systému, a to využitím základných prvkov jeho teórie. Inak povedané, nerieši len možné príčiny vzniku nežiaducej situácie, ale analyzuje a spolupôsobí na riešení dôsledkov a ich následnej budúcej minimalizácií.

Riziko ⟶ zavedenie opatrení na zabránenie vzniku nežiaducej situácie

Bezpečnostný incident ⟶ riešenie dôsledku vzniku negatívnej situácie



Obrázok 1.8: Obsah základných činností bezpečnostného manažérstva (Zdroj: Hofreiter, 2002, s.55)

Na základe vyššie uvedeného obrázka môžeme demonštrovať vzájomnú väzbu medzi jednotlivými prvkami bezpečnostného manažérstva, ktorých nezastupiteľnosť je jedinečná. Z toho vyplýva, že ak implementujeme tieto prvky do bezpečnostnej praxe, dostaneme ucelený systém riadneho a efektívneho fungovania.
Ako iné vedné disciplíny, aj bezpečnostné manažérstvo vychádza z určitých zákonitosti, ktoré sa postupom a vývojom bezpečnostnej praxe sformovali do podoby princípov – základných pravidiel.

Princípy bezpečnostného manažérstva

V literatúre sa pojem princíp vymedzuje ako prvopočiatok, vedúcu, základnú ideu, základné pravidlo konania. Pod pojmom princíp sa tiež rozumie to, čo sa týka podstaty dačoho. V tomto zmysle je princíp ústredným pojmom, základom systému, ktorý predstavuje zovšeobecnenie a rozšírenie platnosti svojho rozsahu na všetky javy danej oblasti, princíp ako základná idea vyjadruje zákonitosti vývoja daného druhu činnosti, resp. sociálneho javu.
Princíp je spojený s myšlienkovou činnosťou človeka, je výsledkom, produktom teoretického myslenia.
Princípy bezpečnostného manažérstva najvšeobecnejšie vyjadrujú základné elementy činnosti a sú zároveň aj koncentrovaným výrazom základných myšlienok daného systému činností.

Medzi základné princípy bezpečnostného manažérstva patria :

1) *Princíp zákonnosti***,** ktorý vo svojej podstate znamená právnu povahu bezpečnostných činností. Znamená zvrchovanosť zákona v činnosti bezpečnostných manažérov, znamená , že ich činnosť musí byť vždy v súlade sústavou, ústavnými zákonmi a zákonmi a inými právnymi normami.
2) *Princíp profesionálneho prístupu*. Ochrana majetku (hmotných aj nehmotných aktív), osôb a ostatných záujmov, najmä realizácia opatrení zameraných na predchádzanie bezpečnostným incidentom, riešenie bezpečnostných incidentov bezpečnostnými manažérmi, a nimi riadenými službami je službou organizáciám, občanom, resp. štátu. Občan má právo, aby služba poskytovaná na zmluvnom základe bola na vysokej odbornej úrovni a garantovala mu ochranu jeho záujmov.
3) *Princíp etiky činnosti*. Jeho jadro spočíva v chápaní a uplatňovaní takých spôsobov, metód a foriem činnosti bezpečnostných manažérov, ktoré sú v súlade nielen so zákonmi ale aj morálkou a normami spoločenského správania sa, s princípmi demokratickej spoločnosti a právneho štátu.
4) *3) Princíp synergie* (spolupôsobenia) je významným faktorom, ktorý podstatne umocňuje efektívnosť realizovaných bezpečnostných činností. Základnou podmienkou jeho uplatňovania je vytvorenie pocitu vzájomnej dôvery medzi bezpečnostnými manažérmi, bezpečnostnými službami, policajno-bezpečnostnými orgánmi a občanmi (klientmi) pri dosahovaní spoločného cieľa: dosiahnuť vyššiu úroveň ochrany života, zdravia a majetku občanov a štátu pred trestnou činnosťou.
5) *Princíp subsidiarity* bezprostredne súvisí s princípom synergie. Princíp subsidiarity vyjadruje povinnosť bezpečnostných manažérov, bezpečnostných orgánov a služieb vykonať adekvátne opatrenia vtedy, ak príslušné orgány a organizácie, obce alebo iné bezpečnostné orgány

nereagujú na vzniknutú situáciu (napr. na vznikajúci stav ohrozenia či narušovania chránených záujmov) alebo ju nestačia vlastnými silami zvládnuť.

6) *Princíp primeranosti* činnosti úzko súvisí s princípom zákonnosti. Jeho realizácia znamená vyberať a používať metódy a prostriedky v takom rozsahu, aby boli v súlade so zákonmi a prípadný zásah do práv a slobôd občanov neprekročil mieru nevyhnutnú k dosiahnutiu sledovaného účelu.
7) *Princíp rozumnej dostatočnosti* spočíva vo výbere a realizácii takých foriem a prostriedkov na dosahovanie cieľovej funkcie ochrany, ktoré sú adekvátne k hodnote chráneného záujmu. Jeho uplatňovanie je závislé na aplikácii zásad hodnotového manažmentu pri projektovaní bezpečnostných systémov.
8) *Princíp priority prevencie* spočíva v realizovaní takých situačno-prevetívnych opatrení v činnosti bezpečnostných manažérov a služieb pri ochrane chráneného záujmu, ktoré pôsobia na potenciálneho páchateľa dostatočne demotivujúco a odradia ho od úmyslu páchať trestnú činnosť.
9) *Princíp jednoty utajenosti a transparentnosti* nadväzuje na predchádzajúci princíp. Znamená, že aj keď v záujme situačnej prevencie sú vykonávané opatrenia na odradenie potenciálneho páchateľa, existuje množstvo opatrení, ktorých podstata a spôsob realizácie musí zostať pred nepovolanými osobami utajený. Jedná sa napr. o programovanie a kódovanie prístupových systémov, režimové opatrenia pri preprave cenností, kódovanie trezorových zámkov, prístupy k informačným zdrojom a pod., ale i vytváranie rôznych „pascí". Efektívnosť bezpečnostného systému sa zvyšuje použitím ako transparentných , tak aj skrytých (utajených) prvkov a prostriedkov zaistenia ochrany.
10) *Princíp komplexnosti* (jednoty aktívnych a pasívnych opatrení) vyjadruje podstatu prístupu k projektovaniu bezpečnostných systémov. V záujme dosiahnutia vysokej efektívnosti bezpečnostného systému musia vykonávané opatrenia postihovať čo najširšiu škálu rizík a ohrození, či už z hľadiska voľby prostriedkov technickej ochrany, režimových opatrení, tak aj spôsobom zabezpečenia a riadenia ľudských zdrojov a logistiky bezpečnostnej služby.

Význam princípov bezpečnostného manažérstva spočíva v tom, že :

a) v najvšeobecnejšej podobe odrážajú základné prvky obsahu bezpečnostných činností ;
b) sú koncentrovaným výrazom základných myšlienok systému a organizácie bezpečnostných činností ;
c) vyjadrujú zmysel a podstatu právnej úpravy bezpečnostných činností ;

d) spájajú v sebe jednotu teoretickej (poznávacej) a praktickej (realizačnej) stránky bezpečnostných činností;
e) princípy sa materializujú v reálne existujúcej štruktúre a činnosti organizácie.

2 BEZPEČNOSTNÁ POLITIKA

Bezpečnostná politika je základným dokumentom pre riešenie bezpečnosti v celom komplexe ochrany osôb, majetku, záujmov a aktív subjektu. Je to dokument, ktorý je po prijatí manažmentom záväzný pre všetky osoby v rámci daného subjektu. Definuje východiská a všetky ďalšie aktivity v oblasti bezpečnosti.

Úlohou bezpečnostnej politiky je definovať hlavné ciele pri ochrane osôb, majetku, záujmov a aktív subjektu, stanoviť spôsob, ako bezpečnosť riešiť, určiť právomoci a zodpovednosti osôb.

Dielčími cieľmi bezpečnostnej politiky sú:

- definovanie zásad bezpečnosti subjektu vo forme súboru pravidiel,
- popis spôsobu riadenia bezpečnosti formou definovania postavenia a zodpovedajúcich právomocí a zodpovedností,
- určenie východísk, ktoré majú rozhodujúci význam pre formuláciu zásad a riešenia bezpečnosti prevádzkujúceho subjektu,
- pozitívne pôsobenie na zvyšovanie bezpečnostného vedomia zamestnancov,
- vymedzenie kľúčových pojmov v oblasti bezpečnosti.

Zásady bezpečnostnej politiky predstavujú súhrn požiadaviek, ktoré by sa mali, alebo sa musia splniť v záujme zabezpečenia ochrany daného systému, pri rešpektovaní technických a organizačných možností.

Patria tu:

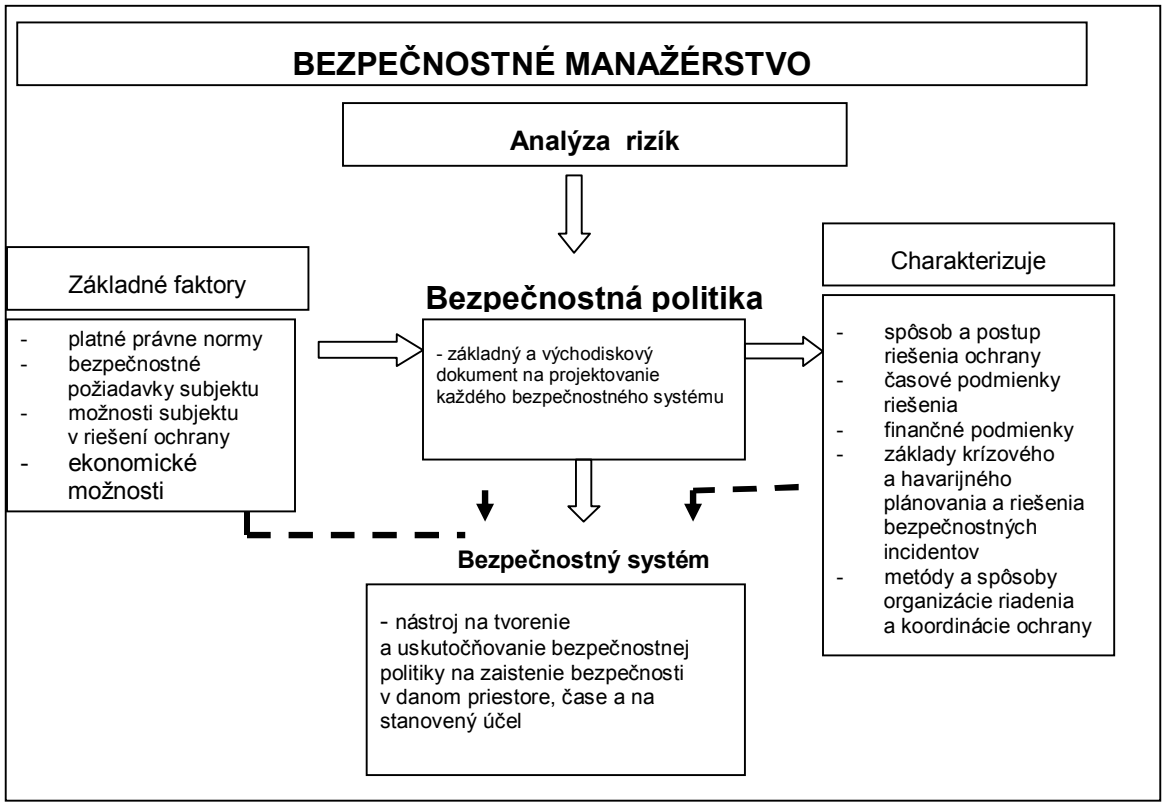
a) fyzická a objektová bezpečnosť, ktorej obsahom je
   - adresa a popis objektu,
   - určenie hraníc chránených priestorov, vrátane popisu ich umiestnenia, vstupov, okien a pod.,
   - základné pravidlá pre ochranu objektu,
   - fyzická ochrana,
   - zhodnotenie požiadavky minimalizovať počet oprávnených osôb,
   - uzamykací režim,
   - požiadavky na elektronickú zabezpečovaciu signalizáciu,
   - zhodnotenie požiarnej bezpečnosti,
   - pravidlá, týkajúce sa elektrického napájania,

b) personálna bezpečnosť, ktorej obsahom sú
   - všeobecné pravidlá personálnej bezpečnosti, ktoré sa majú premietnuť do obsahu pracovnej zmluvy zamestnanca, popisu pracovných činností, vzdelávania a pod.
   - predpoklady pre vznik pracovného pomeru a opatrenia v súvislosti so vznikom pracovného pomeru,

- opatrenia súvisiace so skončením pracovného pomeru,

c) administratívna bezpečnosť, ktorej obsahom je
- určenie zásad prístupu oprávnených osôb k chráneným objektom,
- pravidlá pre odovzdávanie informácií v rámci organizačnej štruktúry prevádzkovateľa,
- pravidlá editovania informačných súborov,
- pravidlá poskytovania informácií externým užívateľom,
- pravidlá sprístupňovania informácií,
- implementácia zásad bezpečnostnej politiky do zmluvných vzťahov,
- bezpečnostná dokumentácia,
- havarijné plány,

d) komunikačná bezpečnosť, ktorej obsahom je
- dohľad nad činnosťou oprávnených osôb,
- dohľad nad činnosťou užívateľov,
- dohľad nad činnosťou sprostredkovateľa, ak bol poverený spracúvaním informácií,
- dohľad na zákonnosťou postupu pri získavaní informácií, ich sprístupňovaní, poskytovaní, resp. ich zverejňovaní,
- komunikácia s dotknutými osobami, ochrana ich zákonných práv,
- zaistenie integrity informácií a informačného systému,
- spoľahlivosť dostupných služieb,
- požiadavky na zabezpečenie informácií pred poškodením, stratou, zneužitím,
- pravidlá identifikácie a autentizácie,
- riadenie prístupu oprávnených osôb do informačného systému.



Obr. 2.1. Bezpečnostná politika (Reitšpís, Mesároš a kol. 2004)

2.1 Rozsah bezpečnostnej politiky

Bezpečnostná politika definuje východiská pre všetky ďalšie aktivity prevádzkujúceho subjektu v oblasti bezpečnosti. Z toho je odvodená požiadavka na úplnosť politiky. Je nevyhnutné, aby bezpečnostná politika pokrývala všetky významné oblasti bezpečnosti.

Rozsah bezpečnostnej politiky je určovaný skutočnosťami, ktoré majú vplyv na požadovanú úroveň bezpečnosti a ktoré sa premietajú do bezpečnostnej politiky a do spôsobu jej realizácie. *Týmito skutočnosťami sú najmä:*

- zákony a vyhlášky, ktoré majú vzťah k predmetu činnosti prevádzkovateľa a k oblasti bezpečnosti,
- charakteristika podnikateľskej stratégie,
- zmluvné vzťahy, ktoré ovplyvňujú obsah bezpečnostnej politiky,
- ďalšie východiská (demografické prostredie a pod.)

Z hľadiska rozsahu rozlišujeme bezpečnostnú politiku na stručnú a rozsiahlu. Obidva druhy majú svoje klady aj nedostatky.

Medzi výhody stručnej bezpečnostnej politiky patrí:

- relatívne rýchla a nenáročná príprava dokumentu,
- vzhľadom k rozsahu a všeobecnosti definovaných princípov, zvyčajne jednoduchší a rýchlejší proces schvaľovania,
- politiku nie je potrebné príliš často aktualizovať, je pomerne stála,
- všetky osoby, ktorých sa dotýka, sa s ňou môžu bez problémov oboznámiť.

Nevýhody stručnej bezpečnostnej politiky:

- hlavný objem prác je presunutý do fázy rozpracovania politiky do formy bezpečnostných štandardov,
- vzhľadom k rozsahu a všeobecnosti definovaných princípov spravidla mnohé problémy nerieši,
- pre osoby, ktorých sa jej realizácia priamo dotýka, môže byť problémom jej konkrétne naplnenie v praxi.

Medzi výhody rozsiahlej bezpečnostnej politiky patrí:

- politika predstavuje komplexný dokument, upravujúci oblasť bezpečnosti,
- definícia hlavných princípov a pravidiel je na jednom mieste,
- vzhľadom k úrovni detailného rozpracovania je eliminovaná možnosť eventuálnej dezinterpretácie alebo nepochopenia,
- bezpečnostné štandardy upravujú veľmi detailné a špecifické oblasti bezpečnosti.

Nevýhody rozsiahlej bezpečnostnej politiky:

- pri akejkoľvek väčšej zmene v spoločnosti je potrebné politiku aktualizovať, je pomerne nestála,
- práce na detailnej politike môžu trvať neúmerne dlho a existuje značné nebezpečenstvo jej nevyváženosti,
- proces schvaľovania politiky býva zdĺhavý a komplikovaný, často s nutnosťou prijímania kompromisov,
- osoby, ktorých sa jej napĺňanie dotýka, nemajú možnosť jednoduchého oboznámenia sa s celým dokumentom, je potrebné pre jednotlivé organizačné skupiny vytvoriť extrakty, čo predstavuje ďalšie náklady.

Jasným cieľom je prostredníctvom kvalitných, hodnotných a ucelených štandardov a smerníc predchádzať rizikám s ohľadom na ochranu života a zdravia osôb a majetku.

Presadzovanie jednotných bezpečnostných opatrení a kontrolných mechanizmov s cieľom dosiahnutia kvalitných štandardov musí byť hlavnou prioritou .

Subjekt si musí byť vedomý všetkých bezpečnostných nárokov na prevádzku, poskytnúť na to požadované zdroje, ktoré zabezpečia bezproblémovú aplikáciu bezpečnostnej politiky v praxi. Bezpečnostná politika a všetky z nej vyplývajúce bezpečnostné štandardy sú pre všetky osoby pôsobiace na pôde subjektu záväzné.

Ciele bezpečnostnej politiky

- zabezpečenie a udržanie usporiadanej a bezpečnej prevádzky,
- predchádzanie a eliminácia nehôd a krízových situácií prostredníctvom zodpovedajúcich štandardov, pravidiel a vzdelávania,
- predchádzanie resp. zneškodňovanie potenciálnych rizikových situácií.

Opatrenia

- pri zapojení všetkých zúčastnených do riadenia bezpečnostného systému je potrebné definovať bezpečnostnú politiku a kultúru v spoločnosti. V riadení bezpečnostného systému sú zosumarizované taktiež i všetky jeho procesy, metódy a výhody, ktoré majú význam v oblasti bezpečnosti,
- implementácia zodpovedajúcich bezpečnostných procesov a metód a stanovenie jasných bezpečnostných štandardov i prostredníctvom auditov a preskúšaní,
- systematický a proaktívny rozvoj prevádzkových bezpečnostných štandardov,
- detailné a efektívne fungujúce komunikačné kanály v prípade nehôd a krízových situácií.

Bezpečnostná politika štátu je mnohodimenzionálny komplex pozostávajúci zo súboru cieľov, zásad, postupov a opatrení na zaručenie bezpečnosti občanov. Integruje v sebe zahraničnú, vnútrobezpečnostnú, ekonomickú, sociálnu, envinromentálnu bezpečnosť a jej ďalšie dimenzie.
Dlhodobým, strategickým cieľom bezpečnostnej politiky štátu je obvykle udržať, prípadne obnoviť stav bezpečnosti, ktorý umožní obrániť a ochrániť prahový záujem spoločnosti.
Úspešná realizácia tohto cieľa sa dosahuje nepretržitou kvalifikovanou analýzou bezpečnostného prostredia a preventívnym pôsobením voči bezpečnostným rizikám, ohrozeniam a krízovým situáciám; zabezpečiť jeho pripravenosť prijímať primerané a včasné odpovede na bezpečnostné výzvy; vybudovať kvalitný bezpečnostný systém.
Samotný strategický cieľ bezpečnostnej politiky Slovenskej republiky vyplýva z jej životných záujmov. Tieto sú v Bezpečnostnej stratégii Slovenskej republiky definované :

- zaručiť bezpečnosť a chrániť základné ľudské práva a slobody občanov;
- zaručiť územnú celistvosť, zvrchovanosť, nedotknuteľnosť hraníc, politickú nezávislosť a identitu;
- rozvíjať demokratické štátne zriadenie, zákonnosť a trhovú ekonomiku;

- vytvárať predpoklady na trvalo udržateľný hospodársky, sociálny, environmentálny a kultúrny rozvoj spoločnosti;
- posilňovať transatlantické strategické partnerstvo, byť spolugarantom bezpečnosti spojencov;
- posilňovať efektívnosť medzinárodných organizácií, ktorých členom je SR a podporovať rozširovanie NATO a EÚ;
- rozvíjať dobré partnerské vzťahy a rozvíjať všetky formy vzájomne výhodnej spolupráce s krajinami, s ktorými máme spoločné záujmy;
- prispievať **k** posilňovaniu a šíreniu slobody **a** demokracie, dodržiavania ľudských práv, zákonnosti, medzinárodného poriadku, mieru a stability vo svete. (Šimák 2006)

3 BEZPEČNOSTNÁ ANALÝZA

Ľudstvo od začiatku svojej histórie hľadá a používa metódy a prostriedky na zaistenie svojej bezpečnosti. Ich druhy a formy sa postupom storočí menia, niektoré sú len zmodernizované prostredníctvom nových technológií, i keď zostávajú vo svojej podstate rovnaké, iné zanikajú. Týka sa to najmä úschovných objektov - technologický pokrok ľudstva premenil staroveké pokladnice - vlastne len dobre strážené miestnosti, a truhlice s cennosťami, akési prvé trezory - na podzemné trezorové priestory bánk, bezpečnostné skrine a trezory s najmodernejšími elektronickými zámkami. (Tallo a kol. 2006)
To, čo svoju funkciu kedysi spoľahlivo splnilo (napr. vodná priekopa, hradby okolo stredovekých miest), po čase túto svoju schopnosť stráca. Je to prirodzený proces, ktorý súvisí nie len s rozvojom stále modernejších technológií, ale často i s prekonávaním psychologických bariér, konvencií a stereotypov ľudských činností.
Bezpečnostná politika napríklad stanoví, že do daného sektora budú mať prístup len určité osoby, ktoré sa musia identifikovať, nemôžu mať so sebou zbraň, na každý balíček či zariadenie, ktoré budú odnášať, budú musieť mať sprievodku, budú povinní sa podrobiť danej bezpečnostnej prehliadke, ktorá toto zaistí s danou spoľahlivosťou a pod. V bezpečnostnom projekte sa potom rozpracovávajú metódy, ako tieto požiadavky bezpečnostnej politiky splniť. (Talo a kol., 2006)
Ktokoľvek, kto sa kedy snažil vedome niečo chrániť - zabezpečiť pred možným nebezpečím, konal tak na základe určitej úrovne poznania. Jeho poznanie určitých skutočností mu potom umožnilo definovať:

- cieľ zabezpečenia (v zmysle dosiahnutia určitého definovaného žiadaného stavu - istoty),
- objekt zabezpečenia (t. j. život alebo zdravie fyzickej osoby, vlastnícke a obdobné práva osôb, organizácií, inštitúcií a štátu a záujem jednotlivcov, organizácií, inštitúcií a štátu),
- spôsob a prostriedky zabezpečenia,
- materiálové a finančné náklady na vykonanie zabezpečenia,
- termíny, dokedy je zabezpečenie nutné realizovať,
- osoby, ktoré za vykonanie zabezpečenia nesú osobnú zodpovednosť. (Brabec, 2001, s. 50-51.)

Len určitá úroveň poznania nám umožní nájsť správnu odpoveď na uvedené otázky. Umožní nám určiť minimálne podmienky, ktoré musíme splniť, aby bola zaistená požadovaná úroveň zabezpečenia, t. j. aby sme docielili požadovanú mieru istoty. Pritom úroveň, účinnosť, použité prostriedky a náklady na zabezpečenie sú priamou reflexiou miery nebezpečenstva alebo ohrozenia. Medzi týmito dvoma pojmami je vzťah závislosti.
Uviedli sme, že na nájdenie správnej miery zabezpečenia je nutná určitá úroveň poznania - znalosti. V procese vedúcom k dosiahnutiu požadovaného stavu je

potrebná úroveň znalostí výsledkom zberu údajov, informácií a dát o zabezpečovanom objekte a ich analýzy. Pretože predmetom tejto analýzy sú skutočnosti týkajúce sa zabezpečenia príslušného objektu a výsledkom tejto analýzy má byť zistenie aktuálneho stavu zabezpečenia, ide o bezpečnostnú analýzu.
Bezpečnostná analýza je dôležitým východiskom pre proces syntézy získaných poznatkov a vypracovaní bezpečnostného projektu, ktorého úlohou je stanoviť úplne konkrétne opatrenia, ktorými bude dosiahnutý cieľ definovaný bezpečnostnou politikou.(Mikolaj, Hofreiter, Mach, Mihók Selinger, 2004, 191 s.) Pritom bezpečnosť nemožno chápať len ako prostý súhrn použitých prostriedkov, opatrení a postupov, ale ako určitý celok - systém, ktorý je vytvorený so zámerom dosiahnuť konkrétny cieľ. Prvky tohto systému vytvárajú logické väzby, ktoré majú svoje zákonitosti. Aby tento systém bol funkčný, musí byť schopný reagovať na zmeny vonkajších podmienok tak, že sa im operatívne prispôsobí bez toho, aby bola znížená jeho funkčnosť. Musí však byť schopný reagovať nielen na zmeny, ktoré už prebehli alebo práve prebiehajú, ale i zmeny, ktoré majú alebo môžu nastať v budúcnosti. Ten, kto systém vytvára, realizuje ho a obsluhuje, musí byť schopný analyzovať všetky dostupné údaje nie len na zistenie aktuálneho stavu, ale i na zistenie budúceho vývoja podmienok. Výsledkom takejto analýzy je teda okrem zistenia súčasného stavu veci i zistenie predpokladaného budúceho vývoja formulovaného v podobe bezpečnostnej prognózy. Schopnosť prognózovať presne a konzistentne je veľmi dôležitá, avšak úplná presnosť je nedosiahnuteľná (v opačnom prípade by potreba formulácie bezpečnostnej politiky - bezpečnostného plánu - bola výrazne nižšia). Je nutné urobiť maximum pre to, čo za daných podmienok je subjekt, ktorý formuluje a realizuje svoju bezpečnostnú politiku, schopný urobiť.
Problém kvalitného a účinného zaistenia bezpečnosti spočíva v schopnosti tých, ktorí rozpracúvajú bezpečnostnú politiku do podoby konkrétneho bezpečnostného projektu, a tí, ktorí sa zaoberajú realizáciou bezpečnostného projektu, že sa zaoberajú nielen pravdepodobnými budúcimi situáciami (proces prognózovania), ale i situáciami menej pravdepodobnými alebo nepravdepodobnými (proces posúdenia hrozieb - analýza rizík).
Bezpečnostná analýza je systémový proces, ktorý v zásade zahŕňa 3 etapy:

1. analýzu bezpečnostného prostredia
2. analýzu rizík
3. návrh technických, organizačných a administratívnych opatrení.

Obsahom procesu analýzy bezpečnostného prostredia je systematický, cieľavedomý, cyklický a kontinuálny proces získavania, zhromažďovania a spracúvania informácií o demografických, sociálno ekonomických, sociálno-psychologických, policajno-bezpečnostných a iných zvláštnostiach prostredia, ktoré môžu byť zdrojom pre vznik a eskaláciu bezpečnostných rizík a ohrození vo vzťahu k chránenému objektu. (Mesároš 2010)
Predmetom analýzy vo vzťahu ku konkrétnemu objektu ochrany môžu byť podľa: informácie o:

- Informácie o **urbanistických charakteristikách prostredia,** pričom pôjde o posúdenie veľkosti sídla, v ktorom je objekt dislokovaný, typu zástavby, charakteristík okolia objektu, ktoré môžu mať vplyv na systém ochrany objektu,
- Informácie o **charakteristikách objektu ochrany,** jeho štruktúre, existujúcom stave ochrany a možných zraniteľných miestach a rizikovosti.
- Informácie o **sociálnych kriminogénnych faktoroch,** za ktoré **sa** môžu považovať
- stav životnej úrovne obyvateľstva, úroveň zamestnanosti, podiel sociálne odkázaných občanov atď.,
- Informácie o **kvantitatívnych a kvalitatívnych ukazovateľoch kriminality** v posudzovanom prostredí a jeho okolí. Pritom je účelné posudzovať:

typ kriminality, ktorý je charakterizovaný najmä predmetnou stránkou (druhmi kriminality a ich formou),

demografický aspekt, ktorý spočíva v uplatňovaní takých hľadísk, ako je pohlavie, vek, sociálny, resp. ekonomický status páchateľa a pod.,

teritoriálny aspekt, ktorý umožňuje skúmať priestorové rozloženie kriminality podľa jednotlivých regiónov; keďže absolútne hodnoty kriminality sú v značnej miere determinované počtom obyvateľov, na objektivizáciu podielu regiónov na celkovej kriminalite je výhodnejšie sledovať a analyzovať relatívne údaje, ktoré výstižnejšie charakterizujú rizikovosť sledovaných priestorových jednotiek (napr. okresov, miest, štvrtí a pod.), vhodným ukazovateľom je index trestnej činnosti (ITČ), ktorý vyjadruje počet trestných činov (T), ktoré pripadajú na určitý počet (N) obyvateľov stredného stavu kriminogénneho obyvateľstva (S), t. j. staršieho ako 14 rokov :

$$ITČ = \frac{T}{S} \cdot N \qquad (3.1.)$$

Za N sa môže dosadiť číslo podľa veľkosti posudzovanej lokality, väčšie číslo (napr. 100 000) sa použije v prípade, ak budeme posudzovať kriminalitu medzi štátmi, číslo, napr. 10 000, 1 000 alebo 100 sa použije pri posudzovaní menších celkov (krajov, okresov, miest a pod.),

urbanistický aspekt, ktorý umožňuje analyzovať podiel obyvateľov urbanistických priestorov (miest, obcí) na celkovej kriminalite i na jej jednotlivých druhoch, pri uplatnení tohto aspektu hodnotenia kriminality vyplýva, že mestá sú z hľadiska kriminality rizikovejšie ako menšie vidiecke sídla, čo je dané aj tým, že v mestách je väčšia anonymita, vyššia koncentrácia ľudí vyplývajúca z väčších pracovných príležitostí, v mestách sa koncentrujú väčšie materiálne hodnoty, väčšie podniky; kriminalitu vo väčších mestách zvyšujú aj migranti z vidieka, ktorí dochádzajú za prácou alebo s cieľom páchať

trestnú činnosť, alebo cudzinci (legálni alebo nelegálni migranti), členovia organizovaných zločineckých skupín a pod.,
vývojové tendencie kriminality, pričom sa posudzujú najmä vývojové tendencie majetkovej kriminality.

Informácie o **stave na úseku ochrany majetku a objektov,** predovšetkým dislokácia policajno-bezpečnostných orgánov, (polícia, SBS) možnosť ich zapojenia do ochrany objektu, možnosti využitia zásahových jednotiek pri ochrane objektu, predovšetkým vzhľadom na čas zásahu a iné.

- Informácie o **stave názorov a nálad, postoji občanov ku kriminalite,** stave právneho vedomia, názory na stav a zaistenie ich bezpečnosti, miera tolerancie občanov k majetkovej kriminalite a pod.
- Informácie o **prírodných podmienkach** v danom prostredí, o početnosti, **rozsahu a závažnosti živelných pohrôm,** ktoré by mohli ohroziť chránený objekt.
- Informácie o stabilných i mobilných **zdrojoch priemyselných havárií** v danom prostredí, ktoré by mohli ovplyvniť bezpečnostný systém ochrany objektu. (Reitšpís, Mesároš a kol. 2004)

Výsledkom tejto etapy bezpečnostnej analýzy je definovanie predpokladov rizík sociálnej, technickej a environmentálnej povahy, ktoré môžu ohroziť chránený záujem - život alebo majetok občanov a právnických osôb.
Je potrebné uvedomiť si, že v oblastí zabezpečenia organizácií nedostáva analytik všetky informácie v podobe, ktorá by sa dala presne kvantifikovať. Zásadné informácie pre bezpečnostnú expertízu organizácie nie sú v podobe presných čísiel, čo samozrejme obmedzuje možnosti výberu a použitia rôznych techník analýzy a prognózy. Sú vypracované rôzne postupy, ktoré sú modifikáciou bežne používaných techník strategickej analýzy v iných oblastiach (napr. oblasť ekonomická a finančná). Medzi takéto analýzy patrí napr. **analýza PEST,** modifikovaná analýza zdrojov a predovšetkým **analýza SWOT.** Veľmi dobre použiteľné sú i niektoré metódy popisnej štatistiky, napr. **Paretov diagram** a iné druhy diagramov. Na vytvorenie bezpečnostnej analýzy môžeme použiť rad technických a rôznych iných prístupov na vyhodnotenie súhrnu získaných informácií a dát, avšak nemôžeme vynechať jednu dôležitú zložku a tou je analýza rizík. Bez vytvorenia tejto časti analýzy by bezpečnostná analýza nebola ani kompletná, ani použiteľná na funkčné riešenie problému bezpečnosti. Analýza rizík, aj keď jej najčastejšie použitie je uvádzané v oblasti bezpečnosti informačných systémov, je použiteľná (a nutná) pri posudzovaní a analyzovaní celkovej bezpečnosti organizácie či inštitúcie. Analýza rizík musí dať odpoveď na tri základné otázky:

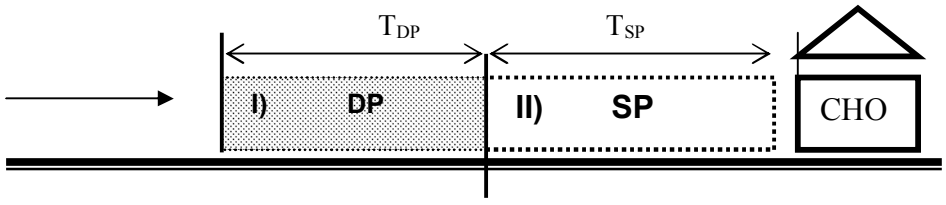
1. aké riziká - hrozby môžu nastať,
2. aká je pravdepodobnosť, že riziká nastanú a dôjde k bezpečnostnému konfliktu,
3. aké budú následky, keď bezpečnostný konflikt nastane.

Bezpečnosť organizácie tvorí systém opatrení, ktorého cieľom je, aby organizácia ako celok i jej jednotlivé organizačné zložky a jej zamestnanci boli chránení pred vonkajšími i vnútornými vplyvmi (konanie, udalosť), ktoré by jej mohli spôsobiť straty na živote, zdraví, škody na majetku alebo poškodiť jej oprávnené ciele a záujmy späté s existenciou a činnosťou organizácie v procese hospodárskej súťaže. (Tallo, Rak, Tureček 2006)
Analýza sa vykonáva pomocou expertného systému, ktorý je potrebné priebežne aktualizovať. Systém hodnotenia jednotlivých auditovaných oblastí je založený na princípe stanovenia miery zhody zisteného skutkového stavu s definovaným modelom. Parametre modelu sa stanovujú pred hodnotením, podľa základných charakteristík a špecifických podmienok hodnoteného objektu (organizácie).
Existencia bezpečnostných rizík a pôsobenie ohrození najrôznejšej povahy si vyžaduje venovať veľkú pozornosť príprave modelu ochrany objektov , ktoré buď sú objektom ochrany samy o sebe , alebo sa v nich nachádza určitý chránený záujem. Pre vypracovanie modelu ochrany je veľmi dôležitá analytická etapa, ktorá by mala poskytnúť základné východiská pre vytvorenie účinného a efektívneho bezpečnostného systému.

Charakter potenciálnych rizík a ohrození, dôležitosť chráneného objektu a chráneného záujmu v ňom si vyžaduje, aby boli pri projektovaní systému ochrany objektu zohľadnené nasledujúce požiadavky:

1. Systém technických prostriedkov vonkajšej ochrany objektu musí :
    a. odradiť potenciálneho narušiteľa,
    b. detekovať a verifikovať prítomnosť narušiteľa,
    c. spomaliť postup narušiteľa,
    d. zabrániť narušiteľovi vo fyzickom kontakte s chráneným záujmom.
2. Fyzická ochrana musí:
    a. mať včasnú informáciu o narušení prvej vrstvy obvodovej ochrany,
    b. zadržať narušiteľa do doby jeho priblíženia sa k chránenému záujmu.

S ohľadom na uvedené požiadavky by mala schéma systému ochrany objektu vyzerať nasledovne:



Obr. 3.1: Schéma ochrany objektu (Hofreiter, Križovský 2007)

Rozhodujúcu úlohu pri posudzovaní kvality ochrany objektu bude zohrávať veľkosť detekčného priestoru (DP) a spomaľovacieho priestoru (SP). Ich význam bude zrejmý z vyjadrenia doby reakcie fyzickej ochrany (T_{RO}) a doby potrebnej na prekonanie systému vonkajšej ochrany (T_{VO}). Musí platiť, že :

$$T_{RO} \leq T_{VO} \tag{3.2}$$

Podrobnejšie vyjadríme jednotlivé doby :

$$T_{RO} = T_P + T_V + T_{FO} \tag{3.3}$$

kde : T_{RO} je doba reakcie systému ochrany (s),
T_P je čas prenesenia signálu poplach (s),
T_V je čas potrebný na verifikáciu poplachu (s),
T_{FO} je čas potrebný na vydanie pokynov zásahovej jednotke a jej Presun na miesto zásahu (s).

$$T_{VO} = T_{DP} + T_{SP} \tag{3.4}$$

kde : T_{VO} je čas potrebný na prekonanie systému vonkajšej ochrany (s),
T_{DP} je čas, ktorý potrebuje narušiteľ na prekonanie bariér vymedzujúcich detekčný priestor (s),
T_{SP} je čas, ktorý potrebuje narušiteľ na prekonanie spomaľovacieho priestoru (s).

S využitím vzťahov (3) a (4) môžeme vyjadriť koeficient kvality ochrany, ktorý bude:

$$K_{OCH} = \frac{T_{VO}}{T_{RO}} \geq 1 \tag{3.5}$$

To znamená, že čím vyššia bude hodnota koeficientu ochrany, tým kvalitnejší bude systém ochrany objektu.
Pre niektoré objekty osobitnej dôležitosti alebo dôležité objekty bude potrebné rozšíriť oblasť detekčného priestoru aj pre prípady možného pokusu preniknutia narušiteľa zo vzduchu (napr. pomocou ultraľahkých lietadiel, riaditeľných padákov a pod.). Na to treba využiť taký systém detekcie, ktorý zabezpečí dostatočný predstih pre reakciu zásahovej skupiny a zabezpečenie chráneného objektu aj pred narušením zo vzduchu.

Obsahom analytickej fázy pri modelovaní ochrany objektu môže byť:

- popis objektu ochrany (chráneného záujmu),
- vypracovanie zoznamu a popisu relevantných bezpečnostných ohrození,
- vypracovanie prehľadu zraniteľných miest a analýzy zraniteľnosti ,
- odhalenie možných spôsobov napadnutia objektu (ohrozenia chráneného záujmu),
- definovanie rizikovosti objektu.

3.1 Popis objektu ochrany a chráneného záujmu

Pod pojmom objekt ochrany sa rozumie predmet, osoba alebo informácia, ktorá je v pozornosti subjektu s protispoločenskými cieľmi, a na ochrane ktorého má spoločnosť záujem. Za objekt ochrany budeme považovať aj stavebný objekt, v ktorom je umiestnený určitý chránený záujem. Popis objektu ochrany zahrňuje :

- Definovanie typu objektu podľa:
  - určenia napr. prevádzková budova alebo stavba, budova alebo stavba občianskej výstavby (tiež obchodné, administratívne, zdravotnícke objekty), objekty , budova alebo stavba na bývanie, ostatné. Definovanie typu objektu podľa určenia má význam pre určenie rizikovosti objektu.
  - vyhotovenia, napr. murovaný, kovový, betónový, železobetónový, drevený, iný typ. Definovanie typu objektu podľa vyhotovenia má význam pre určenie jeho pasívnej odolnosti voči narušeniu.

- Popis dislokácie objektu spočíva v určení jeho polohy v danom urbanistickom prostredí. Môže byť definovaný:
  - objekt v extraviláne, tzn. ležiaci mimo zastavanej časti sídliska, obce, mesta;
  - objekt v intraviláne, tzn. ležiaci v sídelnej (hromadnej) zástavbe, pričom môže byť ďalej špecifikovaný ako jednotlivý objekt, v radovej zástavbe, v obytnom dome a pod.
  - ťažko dosiahnuteľný objekt, napr. v horských a zalesnených oblastiach bez prístupových komunikácií.

- Popis rozmiestnenia chránených priestorov (zón) znamená presnú špecifikáciu polohy chránených priestorov (zón) v chránenom objekte. Podľa štruktúry objektu môžu byť chránené priestory rozmiestnené napr. v suteréne, na prízemí, na poschodí alebo v podkroví.

- Popis okolia objektu má význam pre riešenie otázok perimetrickej (obvodovej) ochrany objektov. Vzhľadom k dislokácii objektu môžeme definovať :
  - voľné, prehľadné a kontrolovateľné okolie,
  - neprehľadné, ťažko kontrolovateľné okolie.

- Popis objektu z hľadiska prístupových ciest má význam pre projektovanie perimetrickej a plášťovej ochrany, ale aj pre plánovanie úloh súvisiacich z riešením krízových situácií, napr. možnosť prístupu zásahovej jednotky, záchranných síl a prostriedkov a pod. Konkrétny objekt ochrany môžeme charakterizovať podľa :
  - počtu prístupových ciest na objekt s napr. jednou, dvoma alebo viac prístupovými cestami,
  - kontrolovateľnosti prístupových ciest na objekt, napr. s kontrolovateľnými (ulice, cesty, voľné plochy, ale i okná, dvere a pod.), alebo nekontrolovateľnými prístupovými cestami (lesný porast, pivnice, povaly, vetracie šachty, potrubné šachty, garáže spojené s domom a pod).
  - priechodnosti prístupových ciest pre dopravné prostriedky na objekt s priechodnými alebo nepriechodnými , resp. zjazdnými alebo nezjazdnými prístupovými cestami.

- Popis stavebných prvkov objektu ochrany spočíva v popise a ohodnotení prvkov ktoré tvoria plášť objektu a sú prejavom celkovej konštrukcie objektu. Sem patria múry, podlahy, stropy a strechy budov. Hodnotí sa predovšetkým ich mechanická odolnosť proti prelomu. Z hľadiska týchto kritérií môžu byť ohodnotené ako :
  - ľahko prekonateľné,
  - prekonateľné,
  - so zvýšenou pasívnou bezpečnosťou.

- Popis otvorových výplní, ktoré predstavujú vstupy a výstupy objektov. Ich kvalita a mechanické zabezpečenie ovplyvňujú celkovú pasívnu bezpečnosť objektu. Patria sem najmä dvere, okná, balkóny, balkónové dvere, rôzne druhy vetracích otvorov, mreže, rolety, žalúzie, okenice apod. Dôležitá je ich prelomová odolnosť[1] a ich kvalita sa vyjadruje príslušnou bezpečnostnou triedou.

- Hodnotenie existujúceho systému ochrany objektu spočíva v posúdení súčasného stavu ochrany chráneného objektu. Pritom sa posudzuje:

[1] Prelomová odolnosť otvorových výplní sa vyjadruje časom, ktorý potrebuje páchateľ na prekonanie prekážky a dosiahnutie chráneného záujmu.

- stav klasickej ochrany, ktorá predstavuje základný druh ochrany. Tvorí ju súhrn opatrení na priame zabezpečenie objektu a jeho dôležitých častí vytvorením systému zábran, prekonanie ktorých vyžaduje určitý čas, použitie špecifických nástrojov a prostriedkov, zručnosť páchateľa a pod. Zahŕňa predovšetkým prvky perimetrickej (obvodovej), plášťovej ochrany a ochrany otvorových výplní. Stav klasickej ochrany sa hodnotí tým stupňom bezpečnostnej triedy, ktorý dosiahne najslabší (najľahšie prekonateľný) prvok klasickej ochrany.
- Stav fyzickej ochrany objektu, ktorá spočíva v bezprostrednom strážení objektu (priestorov) fyzickými osobami (strážnici, vrátnici, pracovníci SBS a pod.). Hodnotí sa aj spôsob fyzickej ochrany, či už ako trvalá prítomnosť na kontrolnom (strážnom) stanovišti, alebo formou obchôdzky, hliadkovania a pod. Pritom sa berie do úvahy, či pracovník fyzickej ochrany má trvalý prehľad o dianí v chránenom objekte (priestore), alebo či môže páchateľ preniknúť do objektu nepozorovane.
- Stav režimovej ochrany. Vypracúva sa režimová štúdia chráneného objektu, ktorá má posúdiť systém organizačno-administratívnych opatrení, ktorými sa vymedzuje napr. pohyb osôb v chránenom objekte (priestore), ich pracovný režim, systém vstupu/výstupu, pohyb, kontrola a evidencia vozidiel, kľúčový režim, materiálový a expedičný režim, režim návštev, monitorovanie pohybu osôb v režimovom priestore a pod.

  Posúdenie stavu režimovej ochrany umožní odhaliť vnútorné zdroje bezpečnostných rizík.
- Posúdenie použitých technických prostriedkov ochrany. Technické prostriedky ochrany sú zabezpečovacie systémy alebo poplachové systémy, ktoré slúži na ochranu osoby, majetku a chránených objektov pred neoprávnenými zásahmi, vrátane systémov a zariadení umožňujúcich sledovanie pohybu a prejavu osoby v objekte a jeho okolí. Pri ochrane objektu sa môžu použiť elektrické zabezpečovacie systémy (EZS) a prostriedky protipožiarnej ochrany (EPS). Posudzovanie použitých prostriedkov technickej ochrany sa zameriava na :
  - hodnotenie kvality použitých prostriedkov podľa bezpečnostnej triedy ,
  - spôsob vyvedenia poplachovej signalizácie (autonómne- na chránenom objekte, na pult centralizovanej ochrany, pomocou telefónneho hlásiča a i.).

Závery zo zhodnotenia existujúceho stavu ochrany je východiskom pre návrh opatrení na zvýšenie ochrany objektu.

Súčasťou tejto etapy činností je aj popis a ohodnotenie chráneného záujmu. Pod pojmom chránený záujem sa rozumie majetok alebo iné hodnoty, ktoré majú byť (alebo sú) chránené pred odcudzením, poškodením, zničením alebo pred iným spôsobom narušenia.

Obsahom popisu a hodnotenia chráneného záujmu môže byť :

- Popis druhu chráneného záujmu. Základné členenie chráneného záujmu je na:
  - hmotný chránený záujem, ktorý sa môže ďalej členiť na:
    - statický : monolitický, alebo členený,
    - mobilný: cennosti, drogy, jedy, zbrane, výbušniny,...
  - nehmotný chránený záujem, ako napr. informácie, know-how, výrobná dokumentácia, dobré meno spoločnosti a pod.
  - osoby (ústavní činitelia, súkromné osoby – podnikatelia, umelci pod.).

- Definovanie hodnoty chráneného záujmu. Podľa tohto kritéria môžeme členiť hodnotu chráneného záujmu na :
  - vyčísliteľnú, ak je možné hodnotu vyjadriť vo finančnej podobe,
  - nevyčísliteľnú, ak hodnota chráneného záujmu nemôže byť vyjadrená finančne (napr. ľudský život, vzácne umelecké a historické predmety a pod.).

  Definovanie hodnoty chráneného záujmu umožní vyjadriť veľkosť dôsledku bezpečnostného rizika.

- Hodnotenie atraktívnosti chráneného záujmu vychádza z určenia druhu a hodnoty chráneného záujmu. Využívajú sa tiež informácie policajných štatistík, v ktorých je uvádzané, čo je najčastejším predmetom záujmu páchateľov. V súčasnosti majú najvyššiu „prioritu“ peniaze, cenné veci, elektronika, zbrane, výbušniny a drogy.

- Hodnotenie významu chráneného záujmu môže byť vykonané buď podľa objektívnych alebo subjektívnych kritérií.

  Použitie objektívnych kritérií bude použité v prípade posudzovania chráneného záujmu, ktorý má celospoločenský význam a v prípade jeho ohrozenia (znehodnotenia, zneužitia, poškodenia) môže dôjsť k negatívnym dôsledkom s dopadom na celú spoločnosť (napr. energetické systémy, komunikačné uzly, sklady a pod.).

  Použitie kritérií subjektívneho charakteru bude aktuálne v prípade posudzovania chráneného záujmu, ktorý má určitý význam pre obmedzený okruh osôb, príp. menšie spoločnosti.

  V závislosti na použitých kritériách môže byť význam chráneného záujmu hodnotený ako malý, veľký, veľmi veľký ap.

- Popis umiestnenia chráneného záujmu má veľký význam pre následné riešenie spôsobu jeho ochrany. Vychádza sa pritom z metodiky použitej pri popise objektu ochrany. Dôraz treba položiť na podrobný popis priestorov,

v ktorých je chránený záujem umiestnený a na popis prístupových ciest k nemu.

- Popis použitého systému ochrany chráneného záujmu sa môže vykonávať podľa rovnakej metodiky ako pri popise systému ochrany. Táto metodika sa v prípade niektorých druhov chráneného záujmu rozšíri o hodnotenie použitých úschovných objektov.

Úschovné objekty sú objekty určené na bezpečné uloženie cenných predmetov, peňazí, dôležitých dokladov, listín a iných predmetov chráneného záujmu.
Úschovné objekty chránia uložený obsah proti vlámaniu a delia sa na:

- skriňové trezory (mobilné, vstavané)
- komorové trezory.

Predmetom hodnotenia úschovných objektov je hodnota ich prelomovej odolnosti, čo je číselná hodnota, vyjadrujúca odolnosť objektu proti vlámaniu. Podľa vypočítanej hodnoty prelomovej odolnosti sa zaraďuje úschovný objekt do príslušnej bezpečnostnej triedy.
Znalosť bezpečnostnej triedy úschovného objektu má význam pre stanovenie hodnoty chráneného záujmu, ktorý môže byť umiestený (uložený) v úschovnom objekte napr. v súlade s príslušnými poistnými podmienkami, alebo stupňa utajenia utajovanej skutočnosti.

3.2 Prehľad zraniteľných miest

Zraniteľnosť objektu (chráneného priestoru) je vyjadrenie možnosti:

- s akou môžu byť časti objektu a/alebo chráneného priestoru (stavebné prvky, otvorové výplne) alebo prvky systému ochrany objektu a chráneného priestoru (MZP, TZP, režimové opatrenia a pod.) prekonané identifikovanými ohrozeniami,
- ako môžu byť osoby (zamestnanci, príslušníci FO) nápomocní útočníkovi k získaniu neoprávneného prístupu k utajovaným skutočnostiam,
- ako môže byť spôsob manipulácie s utajovanými skutočnosťami zneužitý na získanie prístupu k utajovaným skutočnostiam,
- ako môže dané ohrozenie narušiť, resp. ochromiť bezpečnosť objektu,

Zraniteľné miesta predstavujú tie časti objektu ochrany (stavebné prvky, otvorové výplne) alebo tie prvky systému ochrany, ktoré nezabezpečujú požadovaný stupeň bezpečnostnej ochrany (ochranu zodpovedajúcu príslušnej bezpečnostnej triedy), sú slabým alebo ľahko prekonateľným prvkom v systéme ochrany.

Prehľad zraniteľných miest sa vypracúva na základe analýzy (popisu) chráneného objektu (chráneného záujmu) v nadväznosti na nasledujúce etapy činností. Rozhodujúcimi kritériami pre spracovanie prehľadu zraniteľných miest chráneného objektu je :

- úroveň pasívnej bezpečnosti stavebných prvkov objektu,
- úroveň odolnosti proti vlámaniu pre použité mechanické zábranné prostriedky,
- úroveň prelomovej odolnosti úschovných objektov,
- bezpečnostná trieda použitých prvkov poplachových systémov na hlásenie narušenia,
- spôsob výkonu fyzickej ochrany,
- možnosti zásahových jednotiek vykonať zásah na zadržanie narušiteľa (páchateľa).

Zraniteľnosť chráneného objektu sa potom ohodnotí podľa úrovne zraniteľnosti najslabšieho článku v systéme ochrany a zabezpečenia objektu.

Analýza zraniteľnosti spočíva v odhalení najslabšieho článku – kritického bodu, resp. kritických miest- v systéme ochrany objektu alebo chráneného záujmu. Celkovým zmyslom analýzy zraniteľnosti je integrácia definovaných rizikových faktorov s jednotlivými prvkami systému ochrany objektu (chráneného záujmu) a na základe toho zistenie kritických miest v systéme ochrany, ktoré nezabezpečujú požadovanú triedu bezpečnosti ochrany ale naopak, umožňujú potenciálnemu páchateľovi narušiť , vniknúť do chráneného objektu, preniknúť k chránenému záujmu, príp. ohroziť alebo inak manipulovať s chráneným záujmom.
Pri analýze zraniteľnosti objektu (chráneného záujmu) sa uskutočňuje hodnotenie všetkých skutočností, ktoré súvisia s bezpečnosťou chráneného objektu (chráneného záujmu). Jednotlivé skutočnosti, rizikové faktory a kritické miesta je potrebné hodnotiť samostatne, ale aj vo vzájomných súvislostiach.
Ohodnotenie zraniteľnosti spočíva vo vyjadrení možnosti, že daný typ ohrozenia využije zraniteľné miesta objektu (chráneného priestoru) na ohrozenie bezpečnosti objektu a utajovaných skutočností.

Stupnica ohodnotenia zraniteľnosti môže byť nasledujúca :

- **malá zraniteľnosť** (M) – ak dané ohrozenie môže len ťažko využiť zraniteľné miesto na ohrozenie objektu, osôb a činností, ktoré sa viažu k danému objektu,
- **stredná zraniteľnosť** (S) – ak existuje možnosť, že zraniteľné miesto bude daným ohrozením prekonané (využité na získanie prístupu k chránenému záujmu, alebo ohrozenie osôb a činností),

- **veľká zraniteľnosť** (V) – ak analyzované zraniteľné miesta môžu byť s vysokou pravdepodobnosťou využité na získanie prístupu k chránenému záujmu, resp. zraniteľné miesta nepredstavujú účinnú prekážku na zaistenie bezpečnosti objektu alebo osôb, ktoré sa v objekte nachádzajú, alebo činností, ktoré sa v objekte vykonávajú.

Výsledná zraniteľnosť objektu (chráneného priestoru) je daná hodnotou zraniteľnosti toho zraniteľného miesta, ktoré bolo ohodnotené ako najzraniteľnejšie.

3.3 Možné spôsoby napadnutia (ohrozenia) chráneného objektu

Na základe analýzy objektu, popisu ohrození a definovania zraniteľných miest chráneného objektu je možné pristúpiť k prognóze možných spôsobov napadnutia chráneného objektu alebo ohrozenia chráneného záujmu.
Voľba spôsobu napadnutia objektu bude vždy závisieť od typu páchateľa, od kvality ochranných prostriedkov a od času, ktorý bude mať páchateľ k dispozícii na prípravu a samotné napadnutie objektu. Potom zostáva úloha definovať AKO a KÝM môže byť napadnutý chránený objekt alebo ohrozený chránený záujem.
Pri určovaní možných spôsobov napadnutia objektu zisťujeme všetky možné spôsoby, ktorými môže dôjsť k narušeniu chráneného objektu alebo ohrozeniu chráneného záujmu.
Ak za bezpečnostné riziko budeme považovať napr. krádež vlámaním, potom možným spôsobom napadnutia sú všetky situácie a spôsoby, ktorými sa možno chráneného záujmu zmocniť, napr.

- vylomenie zámky a vypáčenie dverí,
- vniknutie cez okno,
- vniknutie káblovými šachtami, vetracími šachtami a pod.

Voľba spôsobu napadnutia bude vždy závislá od toho, ako sú tieto prístupové cesty zabezpečené proti vniknutiu. Vychádzame z predpokladu, že páchateľ sa vždy zameria na najslabší článok v systéme ochrany (zabezpečenia objektu alebo chráneného záujmu)..

Ak je predmetom ochrany , teda chráneným záujmom napr. informácia, potom spôsoby, ktorými je ju možné získať nezákonným spôsobom, resp. zneužiť ju, sú :

- krádež,
- neoprávnené kopírovanie (rozmnožovanie),
- odpočúvanie,
- vyzradenie inou osobou a pod.

Nemenej dôležité je aj vytypovanie možného páchateľa. Ak uvažujeme o individuálnom páchateľovi, potom môžeme definovať štyri typy páchateľov :

- 1.typ páchateľa (páchateľov), spravidla náhodný páchateľ, nemá žiadne informácie o objekte a použitom systéme ochrany. Koná bez predchádzajúcej prípravy a má k dispozícii obmedzený sortiment ľahko dostupných nástrojov. Používa hrubú silu, snaží sa preniknúť najjednoduchšou cestou k cieľu. Ak narazí na prvky PSN, rozbíja ich.
- 2.typ páchateľa má určité znalosti a informácie chránenom objekte a použitom systéme ochrany. Koná po krátkom období príprav a požíva základný sortiment nástrojov. Nepoužíva hrubé deštrukčné postupy, ak zistí rozmiestnenie prvkov PSN, opustí objekt.
- 3.typ páchateľa je pomerne dobre oboznámený s usporiadaním chráneného objektu a je oboznámený s činnosťou jednotlivých prvkov použitého systému ochrany. Koná po období prípravy a používa úplný sortiment špeciálnych nástrojov a prenosných zariadení.
- 4.typ páchateľa má možnosť spracovať podrobný plán preniknutia (vniknutia) do chráneného objektu. Koná po období prípravy a má k dispozícii kompletný sortiment špeciálnych nástrojov a zariadení, vrátane prostriedkov na elimináciu a náhradu existujúcich elektrického zabezpečovacieho systému.

Okrem toho treba zvažovať aj:

- možnosť pôsobenia organizovanej skupiny, ktorá koná napr. na objednávku (krádeže umeleckých predmetov, zbraní, a pod.),
- pôsobenie ofenzívnych komerčných spravodajských služieb, s cieľom zmocniť sa dôležitých (obchodných, výrobných a pod.) informácií,
- pôsobenie teroristických alebo extrémistických skupín (napr. proti objektom jadrových elektrární, vojenským objektom a pod.).

Definovanie možných spôsobov napadnutia chráneného objektu alebo ohrozenia chráneného záujmu spolu s typológiou možného páchateľa majú zásadný význam pre výber a rozsah bezpečnostného systému. (Hofreiter 2003)

3.4 Hodnotenie odolnosti chráneného objektu

Jedným zo spôsobov , ako určiť odolnosť objektu či chráneného záujmu je vypočítanie koeficientu odolnosti, ktorý vychádza z kvality existujúceho (resp. navrhovaného) systému na zabezpečenie ochrany objektu.. S jeho pomocou potom môžeme exaktne stanoviť stupeň odolnosti konkrétneho objektu podľa nasledujúceho vzťahu:

$$K_R = \frac{\sum_{i=1}^{n} T_i}{T_Z} \qquad (3.6)$$

kde : K_R - je koeficient odolnosti,

n - je počet MZP radených za sebou ako prekážka ;

T_z - je čas potrebný na zásah zásahovej jednotky (PZ,SBS,...)[2]. Pre stanovenie času potrebného na zásah sa použije minimálne súčet nasledujúcich časov :

- čas vyhlásenia poplachového stavu ,
- čas verifikácie poplachu,
- čas vydania rozkazu na zásah,
- čas prípravy zásahovej jednotky (ak je potrebný),
- čas presunu na miesto zásahu.

T_i - je doba minimálnej prelomovej odolnosti jedného MZP. Za T_i je možné dosadiť :

- pre otvorové výplne : čas odolnosti podľa tabuľky 5 normy STN P ENV 1627,
- pre úschovné objekty : hodnotu času prielomovej odolnosti podľa tabuľky 1 a 2 normy STN EN 1143-1,

Pri výpočte časov potrebných na prekonanie existujúceho (navrhovaného) zabezpečovacieho systému a na zásah zásahovej jednotky je potrebné vychádzať z najmenej priaznivých podmienok, tzn. že :

- páchateľ zaútočí v mieste, kde je minimálny počet prekážok (MZP a pod.),ktoré mu bránia v zmocnení sa chráneného záujmu,
- zásahová jednotka bude musieť prekonať maximálnu možnú vzdialenosť (od stanovišťa stáleho výkonu služby k miestu , kde sa nachádza páchateľ).

Zo vzorca (6) je zrejmé, že odolnosť chráneného objektu či chráneného záujmu je tým väčšia, čím väčšia bude hodnota koeficientu rizikovosti K_R.
Jeho hodnota je závislá od kvality (odolnosti) použitých prvkov systému ochrany a od času, za ktorý je schopná zásahová jednotka vykonať zásah v chránenom objekte.
Pri praktickej realizácii ochrany objektov sa odporúča jeho hodnota v intervale $6 \div 12$, v závislosti na dôležitosti a hodnote chráneného záujmu

[2] Aby mohol byť uvažovaný tento časový faktor, musí byť na chránenom objekte inštalovaný elektrický zabezpečovací systém , ktorý bude detekovať pokus alebo prekonanie perimetrickej (plášťovej) ochrany a vniknutie do zabezpečeného priestoru.

4 BEZPEČNOSŤ A BEZPEČNOSTNÝ INCIDENT

4.1 Východiská chápania bezpečnostného incidentu

Vo filozofickej, prírodovednej, technickej i sociálnej oblasti sa vyskytuje pojem incident v rôznych významoch. Ako uvádza Požár (2006, s. 147) v najvšeobecnejšom význame sa pod incidentom chápe jav, proces, úkaz či skutočnosť. Trochu presnejšie vymedzujú incident technické a prírodné vedy ako osobitný súbor okolností, ako fenomén lokalizovaný v jednotlivom bode časopriestoru. Je to základná výskumná entita v teórii vedy. Najvšeobecnejšie je incident definovaný vo filozofii, ktorá ju chápe ako fenomén, ktorý nasleduje a je spôsobený nejakým predchádzajúcim fenoménom. Pod incidentom v informatike sa chápe udalosť v informačnej bezpečnosti, ktorá nastane a spôsobí poruchu alebo výpadok počítačového informačného systému. Procesy a javy, ktoré prebiehajú za určitých podmienok, v časovom slede akcií, operácií sa nazývajú udalosti. Iincident je teda ľubovoľná zmena v čase na danom objekte (Filák, 2006, s. 147-158).

Poznámka: Incident sa niekedy používa v užšom poňatí ako pojem udalosť V predkladanom oznámení preferujeme však pojem incident ako pojem všeobecnejší, zahŕňajúci rozličné typy udalosti, ale vo väčšine prípadov sú to pojmy identické (rovnocenné) a možno ich ľubovoľne zamieňať.

Udalosti sa skladajú z jednotlivých stavov, pričom stavy sú v danom čase nemenné, ale udalosti sú dynamické a teda spôsobujú zmeny jednotlivých stavov.

Stavy sú jednotlivé statické podmienky daného objektu a postupnosť jednotlivých stavov v čase potom tvorí udalosť. Súčasťou podujatia sú procesy a prechody, ktoré realizujú prenosy. Prenosy majú rôznu veľkosť, silu a smer a teda líšia sa od jedného procesu k procesu nasledujúcemu. Takéto prechody sa realizujú pomocou tzv. operátorov prechodu či inak povedané operátorov transformácie.

Pre bližšie štúdium, ako uvádza Požár s odvolaním na Ponceho (2006, s. 148 - 9) je potrebné charakterizovať udalosť ako časovú postupnosť jednotlivých operácií v danom čase. K tomu bol zvolený formálny aparát tzv. stavového (fázového) priestoru, ktorým sa rozumie usporiadaná dvojica:

$$S = (S, \phi), \qquad (4.1)$$

kde S je konečná množina stavu a ϕ je konečná množina operátorov. Operátorom ϕ v tomto kontexte sa rozumie parciálne zobrazenie množiny stavu S do seba.

V tomto zmysle parciálne zobrazenie ϕ množiny S, na rozdiel od bežného zobrazenia (ktoré tiež býva nazývané zobrazením totálnym), nemusí byť definované pre všetky prvky množiny S.
Ak je pre nejaké $s \in S$ *hodnota* ϕ (s) definovaná, potom sa hovorí , že zobrazenie je aplikovateľné alebo použiteľné na s. V konkrétnom prípade bezpečnostnej činnosti si možno predstaviť množinu stavov v danom časovom okamihu ako získané dáta a informácie o charakteristike, a atribútoch napr. údaje z obhliadky miesta činu, údaje získané z miesta dopravnej nehody, informácie z finančného auditu organizácie a pod. Je zrejmé, že sa takéto stavy v priebehu času môžu meniť a nadobúdať iné charakteristiky. Ponce uvádza: "Hlavné časové entity sú fakt a udalosť. Pod faktom rozumieme vec (tvrdenie), ktorá je platná v čase. Ide o statický aspekt sveta. Fakt časovo vymedzujeme vzhľadom k nejakému okamihu (napr. zostatok na účte k poslednému dňu mesiaca) alebo k časovému intervalu. Udalosť je vec, ktorá sa deje v čase. Ide o dynamický aspekt sveta. Udalosti časovo vymedzujeme vzhľadom k časovému intervalu.
Bezpečnostný incident alebo udalosť môže byť popísaná postupnosťou jednotlivých stavov tak, ako táto udalosť prebiehala.
Popis jednotlivých stavov udalosti je potom vyjadrený množinou informácií o tejto udalosti. To možno vyjadriť vektorom informácií

$$\vec{I} = (i_1, i_2, \ldots, i_n), \qquad (4.2)$$

kde $i_1, i_2, \ldots, i_n$ sú jednotlivé informácie o udalosti v danom časovom okamihu. V praxi to však nie je tak jednoduché, pretože sa väčšinou jedná o celý komplex údajov a informácií o stave udalosti, ktoré nemusia a ani často nie sú rozpoznateľné. Sú to údaje a informácie nepresné a ťažko zistiteľné. Z teoretického hľadiska sa jedná o tzv. zle štruktúrované problémy, pretože v takýchto úlohách je pravdepodobnostná čiže stochastická závislosť. Moderné teórie rozpracovávajú tzv. teóriu chaosu.
Uvažuje sa, že udalosť prebieha v danom časovom intervale $<t_0, t_1>$, kde t_0 je čas začiatku udalosti a t_1 nasledujúci časový okamih a platí, že $t_1 \rangle t_0$. Na základe doplňujúcich, dodatočných informácií z rôznych informačných zdrojov času sa potom môžu získať relevantné informácie o nasledujúcom stave udalosti S_{t1}. Prechod zo stavu S_{t0} do stavu S_{t1} je realizovaný operátorom prechodu φ_1. Tento prechod môžeme symbolicky vyjadriť vzťahom

$$\varphi_1 = S_{t0} \rightarrow S_{t1}. \qquad (4.3)$$

Za udalosť sa môže chápať i ďalší časový interval a potom udalosť je ohraničená časovým intervalom $<t_0, t_k>$, kde čas t_k je konečný čas a platí, $t_0 < t_1$

< t_k. Potom udalosť bude charakterizovať konečná postupnosť operátorov (φ_1, φ_2, φ_3,…. φ_k) taká, že operátor φ_1 je použiteľný na stav S_{t0}, operátor φ_2 je použiteľný na stav $S_{t2} = \varphi_1(S_{t1})$ atď. Potom konečný operátor φ_k je použiteľný na stav

$$S_{tk} = \varphi_{k-1}(S_{tk-1}). \qquad (4.4)$$

Takýmto postupom je potom možné získať relevantné informácie o jednotlivých stavoch i operátoroch, ktorí tvoria či tvorili bezpečnostný incident.

4.2 Charakteristika, druhy a prvky bezpečnostného incidentu

Bezpečnostný incident je proces, ktorý sa pripravuje, vzniká, má svoj priebeh a zaniká a ktorý má za následok vznik bezpečnostnej situácie. Bezpečnostné subjekty potom riešia vzniknutú situáciu tak, aby sa objasnil relevantný incident (Požár, 2006, s 149).
Bezpečnostný incident je dej, ktorý sa zvyčajne stal v minulosti, ale môže ísť o dej, ktorý sa pripravuje, prebieha alebo ktorý sa zatajuje.
Klasifikáciu bezpečnostných incidentov možno vykonávať podľa rôznych kritérií. Medzi najvýznamnejšie určujúce kritériá patrí:
právne posúdenie danej udalosti - škodová udalosť, priestupok, trestný čin,
zavinenie danej udalosti – úmyselné zavinenie, alebo zavinenie z nedbanlivosti.
spôsobenie následku (ujmy) – škoda, ublíženie na zdraví, usmrtenie, poškodenie cudzích práv danou udalosťou.
Každý bezpečnostný incident sa vyznačuje svojimi prvkami, ktoré ho determinujú a špecifikujú. Napr. krádež ako druh bezpečnostného incidentu je špecifikovaná spôsobom spáchania, miestom jej spáchania, osobou páchateľa, objektom záujmu páchateľa, škodou, ale aj motívom.
Špecifikácie, resp. konkrétne určenie o aký druh bezpečnostného incidentu sa jedná, ovplyvňuje vznik konkrétneho druhu a zabezpečenie špecifických činností bezpečnostných subjektov, ktoré sú do týchto činností nasadené.

Význam poznávania bezpečnostného incidentu

Význam poznávania bezpečnostných incidentov (podrobne rozoberá Požár 2006, s. 156-157) spočíva predovšetkým v tom, že vzhľadom na svoj druh a dynamiku vývoja vyvolávajú vznik aktivít špecifických bezpečnostných subjektov. Podľa druhu a dynamiky vývoja, bezpečnostné incidenty majú význam najmä pre vznik tzv. počiatočných a neodkladných opatrení (organizačných, bezpečnostných, operatívne pátracích, a iné). Využitie

počiatočných neodkladných opatrení závisí od času vzniku, resp. od času zistenia bezpečnostného incidentu po jeho vzniku, na jeho druhu a charaktere, ako aj na spôsobe a okolností jeho vzniku. Počiatočné a neodkladné opatrenia majú svoj význam najmä pri bezpečnostných incidentoch, ktoré vznikli bezprostredne pred ich oznámením alebo zistením. Najmä pre tieto prípady majú neodkladný a často neopakovateľný charakter. Na včasnosti, rýchlosti a kvalite výkonu počiatočných neodkladných opatrení závisí úspešnosť nasledujúcich bezpečnostných činnosti. Včasné a kvalitné vykonanie neodkladných opatrení má nasledujúci význam:

- zamedzuje vznik novej, prípadne rozšírenie už existujúcej škodlivej udalosti a
- jednak smeruje k vytvoreniu priaznivých podmienok pre cieľavedomé, plánovité a úspešné nasadenie následných bezpečnostných operatívno-pátracích, trestno-procesných, preventívnych a správno-právnych činností (Filák, 2006, s. 156).

5 BEZPEČNOSTNÁ SITUÁCIA

Teoretickému rozboru i praktickým aplikáciám bezpečnostnej situácie sa v podmienkach konštituovania a rozvoja policajných vied a teórie policajnej bezpečnostnej činnosti venovali priebežne niekoľko rokov najmä Požár a Porada (1988 - 2007), Porada, Rak (2002). Poznávaciu činnosť človeka tvorí obvykle istý postup, pri ktorom sa prechádza od jedného vyriešeného problému, poznanie všetkých jeho vlastnosti k problému druhému. Jedná sa o isté zreťazenie a nadväznosti jednotlivých činností. Táto poznávacia činnosť subjektu poznania je spojená s predvídaním, plánovaním, ktorej danej činnosti má predchádzať, pokiaľ ide o činnosť cieľavedomú. Ľubovoľný proces činností, operácií, úkonov potom chápeme ako postupnosť jednotlivých prijímaných a plnených rozhodnutí. Každé rozhodnutie potom určuje výsledok riešenej úlohy, čo umožňuje zobraziť a vytvoriť logickú schému riešenia jednotlivých úloh. Tieto úlohy sú navzájom spojené viacnásobnými priamymi i spätnými väzbami. Úlohy, jednotlivé činnosti, operácie a úkony tvoria systém (Sadovskij, 1979, s. 77). Riešenie jednotlivých úloh sa zvyčajne realizuje podľa interaktívnych cyklov, ktoré v jednotlivých prípadoch môžu viesť k transformácii podmienok úlohy alebo k formulácii novej úlohy (Porada, Požár, 2001, s. 79-89).
Pojmy, ktoré je potrebné pre ďalšie potreby vymedziť, sú pojmy úloha, problém a situácia. Pod úlohou budeme chápať logický výrok v tvare

"dané V; vyžaduje sa W;" (5.1)

vo formálnom zápise <V; W>, kde V sú zadané podmienky danej úlohy a W je explicitne vyjadrený cieľ úlohy.
V prvom priblížení množina daných podmienok V zahŕňa podmnožinu V^S možných stavov skúmaného objektu a podmnožinu V^R operátorov transformácie (prechodu), ktoré prevádzajú objekt z jedného stavu do stavu druhého. Z teoretického hľadiska možno chápať V^R zobrazením množiny V^S do množiny V^S (rovnakej množiny). V konkrétnom prípade budeme množinu V^S chápať ako súbor, súhrn informácií o objekte v danom čase t. Cieľ W je potom vymedzený žiaducimi stavmi objektov v konečnom čase t - $t_{k,}$ kde $t_{k,}$ je čas ukončenia riešenia úlohy. Cieľ W nemusí mať jediný konečný stav, ale je zvyčajne vyjadrený množinou stavov alebo ich postupnosťou v časovom intervale < t_o, t_k>, t_o je čas začatia riešenia úlohy. V tomto prípade sa jedná o trajektóriu (dráhy) v priestore riešenia jednotlivých stavov $V^S = (V^S_1, V^S_2, ….. V^S_{n,})$. Riešenie úlohy je teda procesom výberu postupnosti operátorov, ktoré postupne prevádzajú objekt do želaného stavu, ktorý je zároveň stavom cieľovým $V^S(t_k)$.
Popis jednotlivých stavov objektu je vyjadrený množinou informácií, ktoré tvoria ucelený systém. To možno vyjadriť opisom počiatočného stavu

$V^S(t_o) = f(i_1, i_2, \ldots, i_n)$, (5.2)

kde i_1, i_2, .. …,.i_n, kde sú jednotlivé informácie o objekte, a sú vyjadrené funkčnou závislosťou. V praxi však to zvyčajne nie je len špeciálny prípad funkčnej závislosti, ale sa väčšinou jedná o pravdepodobnostnú alebo štatistickú závislosť.
Na základe doplňujúcich, dodatočných informácií z rôznych informačných zdrojov v čase t_1 (t_o,< t_1,) potom získavame informácie o nasledujúcom stave $V^S(t_1)$. Prechod zo stavu $V^S(t_o)$. do stavu $V^S(t_1)$ je realizovaný operátorom prechodu $V^R(t_1)$. Tento prechod môžeme symbolicky vyjadriť vzťahom:

$V^R(t_1) = V^S(t_o)$ ----> $V^S(t_1)$. (5.3)

Tak postupne získavame v časovom intervale < t_o, t_k>, kde $t_o < t_i < t_k$, ďalšie informácie a tým sa postupne menia stavy $V^S(t_1)$. Vzniká tak postupnosť stavov:

$V^S(t_o)$, $V^S(t_1)$.---, $V^S(t_i)$, --- $V^S(t_k)$, (5.4)

pričom platia prechody z $V^S(t_i)$ ----> $V^S(t_k)$.
Táto postupnosť stavu je popísaná informáciami o objekte, o okolí systému a je konvergentná, blíži sa danému cieľu W.
Je však potrebné poznamenať, že tento algoritmus je zadaný vo všeobecnom tvare. Ťažkosti sa môžu vyskytovať v sémantike, v zabezpečení informačného procesu, t.j. pri získavaní, ukladaní, triedení, výbere a využití relevantných informácií o objekte.
Zovšeobecnený pojem úlohy na metodologickej úrovni bol skúmaný mnohými autormi. Sú to napr Pribam, Galanter, Miller (1960 - 1964), Newel, Somon, Amosov, Kozelskij (1960 - 1977) a iné. Problémom v kanonickom tvare chápeme logický výrok v tvare:
"Požaduje sa W"; formálny zápis: <----, w>, kde nie sú explicitne stanovené podmienky V.
V tomto prípade je problém vyjadrený neúplnou formuláciou úlohy za účelom získania informácií o podmienkach V danej úlohy. Táto etapa stanovenia podmienok vyžaduje isté operácie a úkony, ktoré vedú v konečnom dôsledku k formulácii úlohy, čo môžeme formálne vyjadriť:
"dané <-; w> žiada sa <V; W>".
Pojem situácia, možno podľa Hlavsa (1987, s. 9) chápať v dvoch odlišných významoch:
statický - ako pomery, okolnosti, podmienky a iné,
dynamicky - ako rokovanie a interakcie, ako jednotu správania, tvorené samotným človekom, úseky, scény, činy a iné.

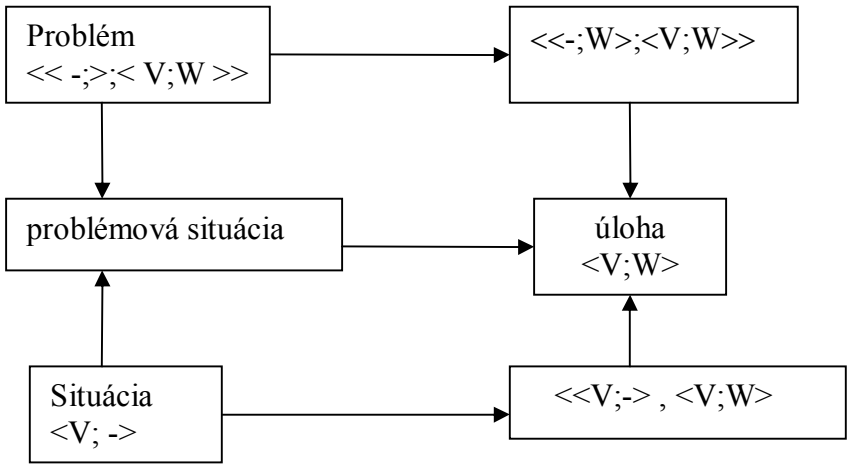
V bezpečnostnom manažérstve situáciu nechápeme staticky. Situácia, činy, udalosti sú priebehom, dejom života, v ktorom ľudia vstupujú do kontaktov a stretov, v ktorých si otvárajú možnosti aj vytvárajú podmienky a prekážky na prekonanie a riešenie týchto situácií.
V najvšeobecnejšom význame situáciou rozumieme súhrn okolností, podmienok vzťahujúcich sa k niekomu, k niečomu v určitej dobe, stav, pomery (Kraus, 2006, s.731). Spoločenské vedy však používajú termín situácie sensu stricto (v užšom slova zmysle). Situácia tu nevyjadruje len stav, okolnosti , ale aj konkrétne súvislosti, väzby v nejakom deji, postupnosť jednotlivých na seba nadväzujúcich udalostí či javov. V tomto prípade sa jedná o dynamickú zložku v činnosti všetkých objektov poznania, kde situácia obsahuje stimuly pre jeho aktivitu a tiež je dôsledkom jeho akcií. To zároveň znamená, že možno istými činnosťami, akciami spätne situáciu ovplyvňovať, pôsobiť na ňu. Na druhej strane závisí situácia na danej rozlišovacej úrovni, cieľoch a ďalších relevantných skutočnostiach.
Situáciou v kanonickom tvare budeme chápať logický výrok tvaru:

"dané V"

formálny zápis: <V; ->, kde V sú zadané podmienky a W ciele. Tu nie je explicitne vyjadrený cieľ W.
V bežnom slova zmysle môžeme v súlade s tým charakterizovať situáciu ako okolnosti, množinu podmienok, ktoré sú dané. V deskriptívnom poňatí je možné situáciu chápať ako množinu vzájomne prepojených faktorov, javov, podmienok, ktoré vyjadrujú konkrétnu etapu úlohy. Tu situáciu skúmame ako neúplné stanovenie úlohy <V; W>, čo možno formálne vyjadriť:

"dané <V; ->, požaduje sa <V; W>.

Tento problém a situácia úzko súvisí s úlohou **dvojakým spôsobom:**
1. Pri relatívne podmienenom chápaní predpokladáme buď existenciu nepriamo vyjadrených podmienok, **hypotetickej situácie,** v ktorej vzniká problém alebo ako orientácii cieľov, ktoré sú stanovené množinou jednotlivých na seba nadväzujúcich situácií.
2. Situáciu a problém môžeme chápať ako počiatočné etapy formulácie úlohy, v ktorej spolu vzájomne súvisia podmienky a ciele úlohy. Formulácii úlohy tak predchádza **problémová situácia,** v ktorej sa objavujú ešte neurčité, "hmlisté" smery, prejavujúce sa predovšetkým v nejasnom, neurčitom stochastickom stanovení cieľa a nepresne stanovených podmienok.
Problémová situácia vlastne vyjadruje hypotézu, v ktorej sa vzájomne spresňuje formulácia situácie a problému na postupnom formulovaní a stanovení stavov podmienok a cieľa, pričom tieto pravdepodobnosti určuje tzv. charakteristickú funkciu úlohy závislej na korektnosti a kvalite riešenia úlohy. Celý tento proces môžeme schematicky **vyjadriť nasledovne:**



Obr.56.1: Schéma vzťahu problému a situácie

V skutočnosti každý človek koná v zložitom komplexe otázok za rôznych podmienok s rôznym cieľom. Vo svojich reakciách volí preto adekvátnu kombináciu podmienok tak, aby dosiahol efektívnym spôsobom stanovené ciele. To je podmienené orientáciou na informačnú stránku, ktorá tvorí odraz reálneho objektu alebo procesu. V danom prípade je týmto objektom a tiež skúmaným procesom **bezpečnostná situácia.**

5.1 Pojem a význam bezpečnostnej situácie

V odbornej literatúre sa možno stretnúť s rôznym označením daného identického pojmu, pre ktorý súčasná teória používa termín **"bezpečnostná situácia".** Ide konkrétne o výrazy "kriminalistická situácia" (Schurich, 1982, s. 23 - 38), "operatívna situácia" (Heřmánek, Stříž, 1971, s. 92 - 142), "operatívno-bezpečnostná situácia" (Bogdanov, Nesnídal, 1982 , s. 112 - 130, Pešek, 1982, s. 40 - 59.), aj napr policajná situácia bezpečnostná situácia. Pre situácie vzťahujúce sa k jednotlivému prípadu vyšetrovaného trestného činu sa v kriminalistike používa termín "vyšetrovacia situácia" (Koldin, 1986, s. 159 - 169).
Už skôr sme vymedzili vo všeobecnej rovine (Porada, Požár, 2001) pojmy úloha, situácia a problémová situácia. Z tohto vymedzenia je zrejmé, že bezpečnostná situácia je vymedzená práve podmienkami, okolnosťami, stavmi, v ktorých je realizovaná bezpečnostná činnosť. Je však potrebné poznamenať, že všetky podmienky nepôsobia rovnako. Ich pôsobenie môže byť priame, nepriame, pozitívne alebo negatívne. Z časového hľadiska možno podmienky, okolnosti a ďalšie vplyvy rozdeliť na krátkodobé, dlhodobé, premenlivé, statické a pomaly sa meniace. V tom sa prejavuje dynamizmus, časová a priestorová

ohraničenosť. Znamená to, že v rôznych etapách bezpečnostnej činnosti sa nevyhnutne budú meniť aj bezpečnostné situácie. Taktiež je nutné podotknúť, že medzi podmienkami, okolnosťami, stavmi, existujú vzájomné vzťahy, väzby; tieto stavy sa tým pádom menia. Zo systémového prístupu (Vepřek, Habr, 1986) vyplýva, že bezpečnostná situácia je systémom, pretože jej prvkami sú dané podmienky, okolnosti aj jednotlivé činnosti, medzi ktorými existujú už spomínané vzťahy. Práve stavové veličiny, ktoré charakterizujú tento systém v istom čase a priestore sa nazývajú stavy systému. V našom prípade budú stavové veličiny bezpečnostnej situácie určované napr. stavom, štruktúrou a dynamikou trestnej činnosti v danom teritóriu, jednotlivými zistenými zločinmi, prečinmi a priestupkami, silami a prostriedkami bezpečnostnej činnosti a iné.

„Pod bezpečnostnou situáciou rozumieme dynamický a zložitý systém stavov, podmienok a okolností, ktoré charakterizujú prvky a atribúty bezpečnostnej činnosti, trestnej činnosti a inú delikvenciu vo zverenom teritóriu a v danom čase, ako aj vzájomné vzťahy medzi nimi“ (Porada, Požár, 2001, s. 84).

Bezpečnostná situácia predstavuje zložitý, viaczložkový objekt poznania, ktorého skúmanie a analýza vyžaduje **systémový prístup**. Na skúmanie a hodnotenie bezpečnostnej situácie, je potrebné pristupovať ako ku kategórii, ktorá existuje objektívne, nezávisle od subjektu bezpečnostnej činnosti, ktorá je však poznateľná.

Má sa za to, že v každej bezpečnostnej situácii je potrebné rozlišovať jej **objektívny obsah,** ktorý je determinovaný a vyjadrený reálnymi javmi a procesmi, prebiehajúcimi v bezpečnostnej činnosti, a **subjektívny význam,** ktorý je vyjadrený subjektívnymi potrebami, záujmami, skúsenosťami, znalosťami a ďalšími vlastnosťami subjektov bezpečnostnej činnosti jednotlivo i v celku. Ako je známe, jeden a ten istý objektívny jav u rôznych ľudí vyvoláva rôzne reakcie; na druhej strane v dôsledku toho vyvoláva aj rôzne rozhodnutia alebo ich mení. Objektívny obsah a subjektívny význam sa môžu mnohokrát aj značne rozchádzať, pričom subjekt má istú predstavu o situácii a jej riešení. Subjektívne chápanie bezpečnostnej situácie úzko súvisí s motivačnou oblasťou osobnosti, s jej znalosťami a skúsenosťami, ktoré potom determinujú aj ciele správania a konania.

Vývoj bezpečnostnej situácie môže prebiehať kontinuálne, plynulo alebo diskontinuálne, náhle. Preto je veľmi užitočné poznať a predvídať jej možné zmeny. Z tohto dôvodu je nevyhnutné v poznávacom procese bezpečnostnej situácie vytvoriť, implantovať adekvátny informačný systém; v našom prípade sa bude jednať o vytvorenie informačného systému a modelu bezpečnostnej situácie. Tento systém a zároveň model musí podľa Ackoffa (1974, s. 87) vyhovovať týmto požiadavkám:

1. dostupnosť a dosiahnuteľnosť poznania spôsobov činnosti, javov a procesov;
2. možnosť registrácie výsledkov týchto spôsobov činností, javov a procesov;
3. znalosť možných stavov a variantov rozhodnutia,
4. pravdepodobnosť možných variantov rozhodnutia;

5. efektívny a dostupný spôsob reakcie na podmienky na dosiahnutie cieľa podľa zvolenej varianty,
6. znalosť významnosti a úžitkovosti možného výsledku.

Je zrejmé, že každá bezpečnostná situácia bude vyžadovať adekvátnu reakciu zo strany subjektu bezpečnostnej činnosti. Voľba postupu reakcie a realizácie rozhodnutia vyžaduje požívať vhodné poznávacie metódy, pretože každá bezpečnostná situácia je konkrétna, neopakovateľná a preto tiež postup jej poznávania musí byť systematický, musí tvoriť istý algoritmus. Veľká väčšina zaznamenaných, zaregistrovaných bezpečnostných situácií vzniká v istej postupnosti pod vplyvom rôznych sociálnych faktorov, ktoré sa v praxi prejavujú konkrétnymi vzťahmi. Preto tiež bezpečnostnú situáciu skúmame vo väzbe na okolité prostredie.

5.2 Základné prvky bezpečnostnej situácie

Ako hlavné hľadisko pre klasifikáciu zvolíme hľadisko stability či premenlivosti jednotlivých skupín prvkov, teda podmienok, okolností, ktoré bezpečnostnú situáciu charakterizujú. Na tomto základe získame prvky relatívne stabilné, potom kvazistabilné a nakoniec prvky variabilné (premenné). Toto delenie vykonali Porada s Požárom v roku 2001. S odstupom času, na základe analýzy prístupov k bezpečnostnej situácii, podľa zvolených kritérií vyjadrujú podstatu bezpečnostnej situácie nasledujúce prvky (Požár, 2006, s. 122-125):
1. Geografické, klimatické, sociálno-ekonomické a iné osobitosti územia, na ktorom bezpečnostné orgány pôsobia.
2. Stav, štruktúra a dynamika trestnej činnosti a stav verejného poriadku.
3. Stav vlastných síl a prostriedkov podieľajúcich sa na boji s trestnou činnosťou, na ochrane verejného poriadku, ako aj efektivita ich využitia.

5.3 Význam skúmania a hodnotenia bezpečnostnej situácie

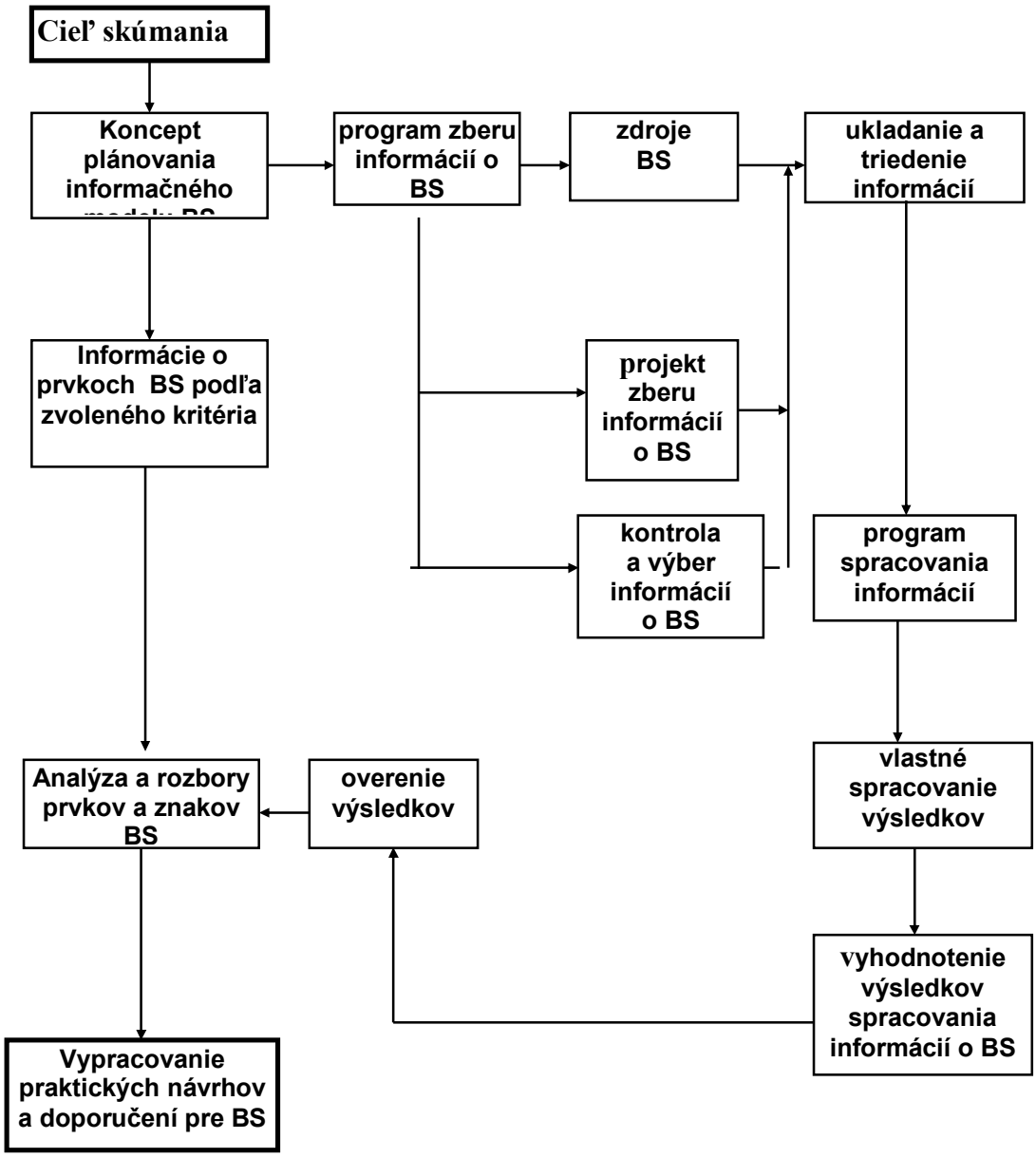
Dôkladná **znalosť bezpečnostnej situácie** sa premieta do **hlavných organizačno taktických foriem bezpečnostnej činnosti a ich jednotlivých druhov** a v konečnom dôsledku ovplyvňuje úroveň ich efektívnosti (Porada, Požár, 2001, Požár, 2006, s. 132-3).
V kriminalistickej bezpečnostnej činnosti vystupuje význam znalosti bezpečnostnej situácie do popredia najmä na úseku odhaľovania a vyšetrovania trestných činov, zisťovanie ich páchateľov, pátranie po nich a pod. To je umožnené využívaním existujúcich špecifických informačných systémov a ich prevod na výpočtovú techniku. To sa realizuje v spojení s ľudským faktorom, optimalizáciou rozmiestnenia dôležitých informačných zdrojov tak, aby boli pokryté miesta predpokladanej trestnej činnosti, miesta koncentrácie

kriminálnych osôb a asociálnych živlov. To všetko je závislé na dokonalej znalosti bezpečnostnej situácie. Až z jej správneho vyhodnotenia vyplynie možnosť ďalšieho efektívneho postupu v poznávacej činnosti bezpečnostných orgánov. Ak subjekt vykoná neobjektívne, subjektivistické vyhodnotenie, potom to má za následok zlé výsledky poznávacích činností a v konečnom dôsledku oslabenie účinnosti systému boja s trestnou činnosťou. Znalosť bezpečnostnej situácie umožňuje ďalej zdokonaľovať už vybudovanú sieť a má aj význam kontrolnej funkcie riadenia bezpečnostnej činnosti v tejto oblasti.

Samotná bezpečnostná činnosť je veľmi rozsiahla a rozmanitá. Zahŕňa v sebe problematiku ochrany osôb a majetku, ochrany objektov, ochrany informácií, obchodného tajomstva, hľadanie osôb, hľadanie majetku, získavanie informácií, ktoré môžu slúžiť ako dôkaz v konaní pred súdom, alebo správnym orgánom, objasňovania trestnej činnosti a iné, aj oblasti, ktoré s ňou nijako nesúvisia. Predovšetkým máme na mysli styk s občianskou verejnosťou a plnenie úloh na úseku štátnej správy. Význam znalosti bezpečnostnej situácie sa premieta napríklad v problematike nasadzovania síl a prostriedkov, riešenie otázok objasnenosti trestnej činnosti, reagencia na zmeny v stave, štruktúre a dynamike trestnej činnosti. Ku všetkým týmto dôležitým rozhodnutiam je nutné mať potrebné vedomosti o minulom priebehu a vývoji bezpečnostnej situácie. V policajnej činnosti je znalosť bezpečnostnej situácie dôležitá napr. pri riadení hliadkovej a obchôdzkovej služby v priebehu ich výkonu, pri tvorbe podkladov pre denné hlásenia, vysielanie nepravidelných hliadok mimo stanovenej trasy, vyhotovenie kriminologických máp pri vydávaní správnych rozhodnutí, prípravy bezpečnostných akcií a pod.

Výsledky skúmania a poznávania bezpečnostnej situácie majú veľký význam pre ďalšie rozpracovanie všetkých bezpečnostných opatrení súvisiacich s implementáciou všetkých úloh bezpečnostných orgánov. Správne hodnotenie bezpečnostnej situácie na danom teritóriu umožňuje rozpracovať a prijímať efektívne riadiace rozhodnutia, efektívne využívanie síl a prostriedkov.

Na základe cieľov bezpečnostnej činnosti je potrebné formulovať aj úlohy skúmania bezpečnostnej situácie. Objektívne skúmanie reálnych podmienok bezpečnostnej činnosti potom umožňuje účinne a cieľavedome formovať, predvídať vývojové trendy vo vývoji trestnej činnosti a na tomto základe tak ďalej zefektívňovať vlastnú bezpečnostnú činnosť jej riadenie a organizáciu. (Filák a kol., 2006, s. 132-133)



Obr. 5.2: Vývojový diagram informačného procesu analýzy bezpečnostnej situácie (upravené podľa Požár, 2006, s. 129)

6 BEZPEČNOSTNÁ IDENTIFIKÁCIA

Z gnozeologického hľadiska ide o špecifický proces, v rámci ktorého dochádza k poznaniu informácií prostriedkami, metódami a postupmi subjektov bezpečnosti. Jedná sa o poznanie odrazov javov, vecí, procesov a udalostí v priebehu bezpečnostných činností (Filák, 2003, s. 19) a v rámci nich predovšetkým o poznanie napr. odrazu rokovaní a osobnosti páchateľa v okolitom prostredí, a to ako v materiálnom prostredí, tak aj vo vedomí ľudí (potenciálnych svedkov). Cieľom bezpečnostných činností je na základe vyhľadania a uchovávania uvedených objektov - nositeľov dôkaznej a inej významné relevantnej informácie vytvárať podmienky pre to, aby napríklad boli trestné činy odhalené, aby sa objasnili všetky závažné okolnosti danej trestnej veci, zaistení páchatelia a ďalší účastníci trestného činu.

Pojem "identifikácia" znamená zisťovanie (určenie) totožnosti a sám o sebe má rôzne významy. Podľa Krausa (2006, s. 335) má pojem identifikácia tieto významy:

1. zisťovanie totožnosti, stotožnenie či proces zistenia úplného súladu medzi viacerými výrazmi, predmetmi, predstavami a pod.,
2. spôsob zisťovania určitých prevádzkových podmienok strojov a zariadení.
3. stotožnenie sa s niekým iným, osobou, s jeho predstavami, záujmami, správaním a konaním (Filák a kol., 2006, s. 134).
4. určenie základných vlastností objektu za účelom jeho zaradenia do príslušnej prírodovednej skupiny, triedy s konečným cieľom určenia jeho individuálnej totožnosti.

Identifikáciou v kriminalistike (Porada, 2001, s. 105) rozumieme proces stotožňovania objektov, v ktorom sa hľadá súvislosť osoby alebo veci s testovanou udalosťou na základe kriminalistických stôp a iných kriminalisticky relevantných informácií. Kriminalistická identifikácia patrí spoločne s kriminalistickou stopou a spôsobom páchania trestného činu medzi základné kriminalistické kategórie a možno povedať, že vo veľkej miere "prelína" všetkými metódami bezpečnostných aktivít.

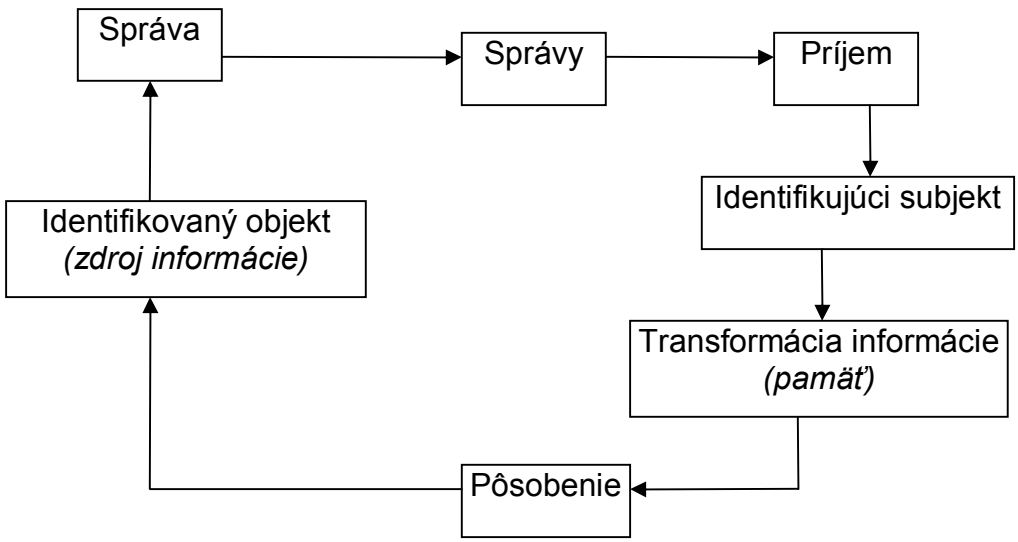
V posledných rokoch sa objavujú možnosti širokého a veľmi efektívneho využívania informačných a komunikačných technológií (výpočtovej techniky) a matematického aparátu v procesoch bezpečnostnej identifikácie. Tak, ako sa vyvíjajú technické prístupy k riešeniu problémov v iných technických vedách, aj do metód bezpečnostných aktivít prenikajú nové princípy a systémové prístupy. Jedným z nových smerov je zavedenie pojmov identifikácia objektov a identifikácia systémov (Porada a kol., 2001) a najnovšie biometrická identifikácia (napr. Rak a kol., 2008, Porada, Šimšík a kol., 2010).

Teoretický základ kriminalistickej identifikácie tvorí systém pojmov, zásad a metód. Tento systém umožňuje vedecky určovať totožnosť materiálnych objektov podľa ich odrazov a využiť takto získané výsledky pre účely trestného konania. Systemizácia pojmov, zásad a metód identifikácie sa môže vykonať podľa rôznych kritérií. Najvšeobecnejší význam má identifikácia z hľadiska určovania totožnosti a využívania výsledkov stotožňovania pri dokazovaní. Všeobecne platí, že identifikácia je poznávací proces, ktorým sa individualizuje vzťah medzi dvomi alebo viacerými prejavmi alebo časťami jedného a toho istého objektu alebo systému (Porada, 1987).

6.1 Identifikácia bezpečnostných činností

Potreba identifikácie bezpečnostných činnosti vznikla v procese konštituovania teórie policajnej bezpečnostnej činnosti (Porada, 1987). Pod pojmom **identifikácia bezpečnostných aktivít** v širšom slova zmysle možno chápať proces stotožňovania našich poznatkov a vedomostí so skutočnosťou. Takto chápaný proces identifikácie neopodstatňuje zaradiť identifikáciu do kategórie poznávacieho procesu (Porada, 1987, Požár, 2006, s. 134-146). Poznávací proces si možno predstaviť ako prípad istej noeticky (Kraus, 2006, s. 335) orientovanej interakcie medzi poznávaným objektom (javom, udalosťou, procesom v bezpečnostnej činnosti) a medzi poznávacím subjektom (bezpečnostným orgánom - pozorovateľom). Orientovaná interakcia vzájomného vzťahu subjektu a poznávacieho objektu značí, že subjekt okrem voľby objektu, javu, procesu, udalosti v bezpečnostnej činnosti si volí aj hľadisko (kritérium) jeho poznávania, t.j. určuje noetický rozklad skúmaného objektu na jednotlivé zložky (prvky) objektu.
Výsledkom poznávacieho procesu je poznanie bezpečnostnej situácie. Relatívnosť poznania je spôsobená voľbou zvoleného kritéria a relatívnosťou obmedzených poznávacích schopností subjektu. Záznamy o poznávaní javu, procesu či udalosti v bezpečnostnej činnosti (objektu), poznávací subjekt formuluje do zistení (faktov, správ, údajov, informácií) o jave, procese, incidente v bezpečnostnej činnosti (Filák a kol., 2006, s ... 135-136). Dôležitú úlohu pri identifikácii má informácia. Pri skúmaní javov, procesov a udalostí v bezpečnostnej činnosti môžeme hovoriť o bezpečnostno relevantnej informácii. Táto informácia sa získava pozorovaním a skúmaním objektu. Prostredníctvom pozorovania a ďalších exaktných numerických metód sa kvantifikuje, ďalej uchováva a pri konkretizácii modelu so známymi a vhodnými prostriedkami spracováva (napr. vhodnou výpočtovou technikou v porovnávacom bloku v rozhodnutí). Takúto informáciu nazývame často empirickou bezpečnostne relevantnou informáciou, získanú pozorovaním daného konkrétneho objektu (javu, procesu, incidentu (udalosti) v bezpečnostnej činnosti.

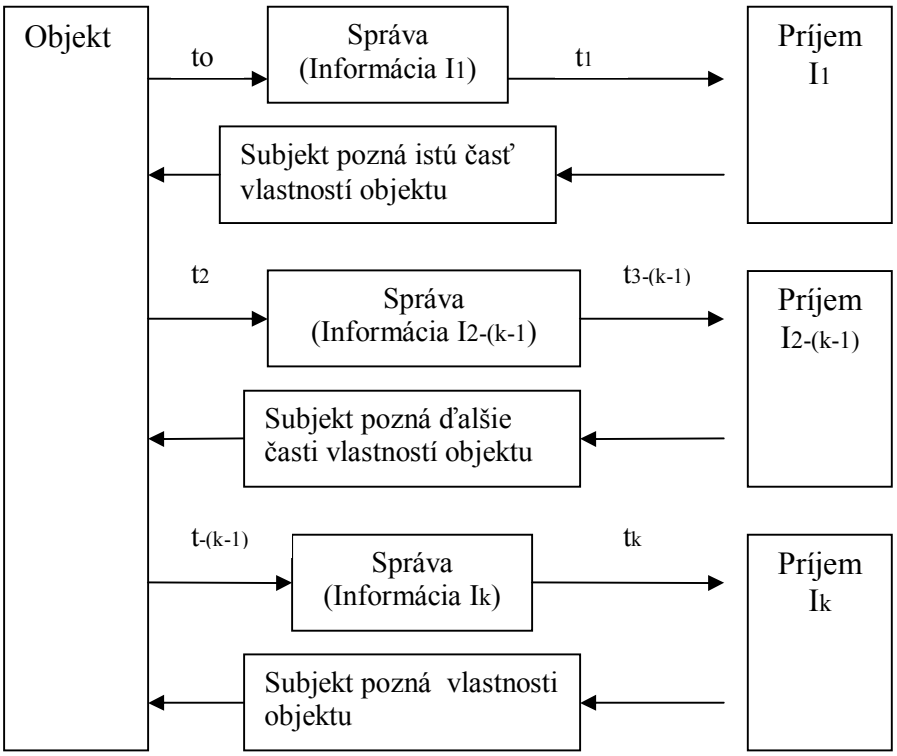
Okrem empiricky relevantnej bezpečnostnej informácie sa využíva v bezpečnostnej činnosti aj tzv. **informácia apriórna** t.j. informácia o do súčasnej doby existujúcich poznatkoch nazhromaždených subjektmi v priebehu bezpečnostnej činnosti pri pozorovaní tried a podskupín objektu, medzi ktoré patrí jav, proces, incident (udalosť) o bezpečnostnej činnosti, ktorý bol podrobený skúmaniu. Tieto poznatky sú usporiadané na danej úrovni poznania do uceleného súboru (systém) teórií a predstavujú nenahraditeľný, bohatý zdroj významných a dôležitých informácií pre vlastnú bezpečnostnú činnosť vrátane jej riadenia (Požár, 2006, s. 136).
Modely bezpečnostnej činnosti predstavujú vhodnú formu na vyjadrenie poznatkov o preskúmaných objektoch (javoch, procesoch a udalostiach); stotožnenie modelu s objektom potom predstavuje kvantitatívny problém. Najčastejšie hľadáme hodnoty parametrov pre už vybranú štruktúru (kvalitatívna závislosť javov, procesov či udalostí v bezpečnostnej činnosti). Pri riešení úlohy stotožňovania v bezpečnostnej činnosti používame vhodné a osvedčené algoritmy. Úspešnosť identifikácie v bezpečnostnej činnosti závisí od vhodného výberu apriórnej a empirickej informácie a identifikačného algoritmu.



Obr.6.1: Schéma procesu identifikácie (Porada, 1987)

Pri tvorbe schémy procesu identifikácie v bezpečnostných činnostiach je zrejmé, že poznávací proces nemôže existovať izolovane, bez postupnosti: poznávanie objektu, jav, proces, udalosť - poznávajúci subjekt a interakcie medzi nimi. Interakciu medzi skúmaným objektom, resp. jeho reprezentantom, substitútom a poznávacím subjektom je založená na teórii odrazu, odraz poznávaného objektu vo vedomí subjektu tvoria jeho model.

Výsledkom poznávacieho procesu v bezpečnostných činnostiach je teda vytvorenie zodpovedajúceho modelu poznávacieho objektu, javu, procesu, incidentu v bezpečnostnej činnosti. Model možno vytvoriť iba na základe informácií, ktoré subjekt skúmania (bezpečnostný orgán) o skúmanom objekte získa a v závislosti, ako ich v pamäti transformuje. Na poznávací proces sa možno teda pozerať ako na proces získavania informácií (odrazov), ich spracovanie (uvedomenie, pamätanie, vytváranie predstáv, vyjadrenie atď.) a spätného pôsobenia subjektu na objekt za účelom ďalšieho prehlbovania a upresňovanie predstáv o bezpečnostnej činnosti (Filák a kol ., 2006, s. 137).
Proces identifikácie v bezpečnostných činnostiach prebieha podľa tohto algoritmu (Porada, 1987, Požár, 2006, s. 137):
- objekt (jav, proces, udalosť) v čase t_0 vyšle správu s obsahom relevantnej bezpečnostnej informácie I,
- subjekt v čase t_1 prijme (je schopný prijať) správu s obsahom informácie I_1..
Príjem a uvedomenie si tejto informácie značí, že identifikujúci orgán už pozná istú časť vlastností objektu.
- Po premietnutí prijatej informácie spätne na objekt, ktorý subjekt vykonal v ďalšom časovom okamihu t_2 a vyslaním ďalšej správy objektom značí, že v čase t_3 orgán prijme už správu s obsahom informácie I_2.. To znamená, že orgán už chápe - spoznáva dokonalejšie vlastnosti objektu, pretože k prijatej informácii I_1 sa informácia I_2 pripočíta.
Proces sa opakuje až do času t_k, kedy subjekt prijme správu s pôvodným obsahom informácie I ktorú zdroj - objekt (jav, proces, udalosť) vysiela už v čase t, a ktorá sa nemení. Pretože relevantná bezpečnostná informácia I vysielaná zdrojom sa nemenila, na strane príjmu informácie rástla, musela sa v procese poznania meniť relatívna obmedzenosť poznávacích schopností subjektu. Poznávacia schopnosť subjektu rástla s rastom informácie, ktorá zase rástla s ohľadom na pamäť subjektu.



Obr. 6.2 Schéma algoritmu procesu identifikácie v bezpečnostných činnostiach

V poznávacom procese v dôsledku relatívnej obmedzenosti poznávacích schopností subjektu vzniká istá **entropia** na strane prijímania správ. Táto entropia klesá s rastom poznania, ale dôsledkom jej existencie je, že nejaká správa vyslaná o bezpečnostnej činnosti v minulosti, môže sa ako informácia s plnou hodnotou prijať až po určitom časovom odstupe. Z toho vyplýva, že schéma identifikácie predstavuje istú obdobu schémy spojovacieho kanála tak, ako je to známe z teórie informácie. Táto skutočnosť oprávňuje k záveru, že na hlbšiu analýzu procesu identifikácie v bezpečnostnej činnosti (všeobecne poznávacieho procesu) mohli by sa využiť niektoré výsledky teórie bezpečnostne relevantnej informácie, ktorú treba ale predovšetkým vytvoriť.

Identifikácia v bezpečnostnej činnosti sa používa v rôznej miere a obsahu. Prešla a prechádza postupne etapami zodpovedajúcimi jednotlivým etapám vývoja procesu poznania v bezpečnostných činnostiach. Od najjednoduchších problémov rozpoznávania znakov, vytvárania pojmov až po vytváranie asociácie a analógie za účelom zovšeobecňovania - generalizácia, napríklad pri analýze a hodnotení bezpečnostnej situácie. V ďalšom období v súvislosti s identifikáciou v bezpečnostných činnostiach bude potrebné rozpracovávať základné problémy

identifikácie a s tým spojené otázky modelovania, rozpracovanie znakov, klasifikácií javov, procesov a udalostí v bezpečnostnej činnosti, teóriu znakov, abstrakcii a mechanizmus zovšeobecňovania a generalizácie. (Porada, 1987, Požár, 2006, s. 137).

Naproti tomu poňatie kriminalistiky (kriminalistickej identifikácie) najmodernejšie vychádza z fyzikálnej interpretácie a následného matematického spracovania základného kriminalistického problému, t.j. správnou interpretáciou stôp trestného činu tento čin rekonštruovať a identifikovať páchateľa. Základné pojmy a teória z nich vytvorená vychádza z predstavy, že každý páchateľ je materiálneho (hmotného) pôvodu a možno ho v zásade usvedčiť na základe jeho interakcie, vzájomného pôsobenia, stopového kontaktu s okolím. Každý páchateľ totiž musí aj proti svojej vôli rešpektovať fyzikálne zákony bilancie energie, zachovania hybnosti, hmoty, entropie a prípadne aj ďalšie. Interakcia páchateľa s okolím je daná práve týmito zákonmi bilancie formulovanými pre príslušné špecifické podmienky trestného činu. Správnou interpretáciou týchto zákonov možno z nich určiť veľké množstvo parametrov charakterizujúcich páchateľa. Rekonštrukcia trestného činu a identifikácia páchateľa je potom vykonávaná pomocou rovnakých parametrov, pomocou ktorých je charakterizovaná jeho interakcia s okolím (Porada, 1987).

6.2 **Druhy identifikácie bezpečnostných činností**

A. Kriminalistická identifikácia objektov.

Identifikácia v kriminalistike znamená proces porovnávania a stotožňovania objektov, aby bola zistená súvislosť osoby alebo veci s testovanou udalosťou podľa stôp či iných zobrazení. Používajú sa rôzne spôsoby porovnávacej metódy tak, aby sa určila totožnosť objektu. Ak sa nepodarí zistiť konkrétny objekt, ktorý zanechal stopy, potom sa proces kriminalistickej identifikácie zužuje na určenie skupinovej príslušnosti objektov, zistenia skupiny, triedy objektov, ku ktorým patrí predmet, ktorý zanechal stopy (Porada, 1987). V tomto zmysle možno totožnosť vymedzovať v dvojakom zmysle: Jednak ako vzťah, jednak ako stav. Pre teóriu a proces kriminalistickej identifikácie je rozhodujúce poňatie totožnosti ako vzťahu (Porada, 1987). Naproti tomu pre teoretické objasnenie kriminalistickej rekonštrukcie je výhodnejšie definovať totožnosť ako stav, t.j. ako stálosť kvalitatívnej určenosti objektu (Musil a kol., 2004, s. 51).
V procese kriminalistickej identifikácie sú na základe učenia o totožnosti, individuálnosti a relatívnej stálosti objektov identifikácie získavané výsledky a formulované závery procesu kriminalistickej identifikácie.

Základným východiskom identifikácie v kriminalistike je teória vzájomného pôsobenia. Z tejto teórie využíva kriminalistická identifikácia tézu o tom, že materiálne objekty podieľajúce sa na trestnom čine (páchateľ, nástroje trestného činu, jeho obuv a pod.) pôsobia v priebehu trestného činu na obklopujúce vonkajšie prostredie - odráža sa, čím v ňom vyvolávajú určitú zmenu - odraz. V kriminalistike majú tieto zmeny najčastejšie podobu stopy. Pri kriminalistickej identifikácii sa využívajú ako stopy vo vedomí ľudí, tak ostatné druhy stôp v materiálnom prostredí.
Základ kriminalistickej identifikácie tvoria učenie o totožnosti, individuálnosti a relatívnej stálosti objektov identifikácie (Porada a kol., 2001). Teória kriminalistickej identifikácie je budovaná na základe dialektickej logiky, kde je konkrétna totožnosť vysvetľovaná ako vzťah protikladov. Vzťah totožnosti poníma dialektický logika ako vzťah medzi dvoma alebo viacerými prejavy (stavy) jedného a toho istého objektu odčerpaného v rôznych formách.
K splneniu úlohy kriminalistickej identifikácie, t.j. na zistenie totožnosti osôb a predmetov podľa ich zobrazenie v materiálnom prostredí a vo vedomí človeka, nie je možné vystačiť len s myšlienkovými operáciami. Proces kriminalistickej identifikácie vyžaduje tiež praktickú poznávaciu činnosť od subjektov identifikácie (vyšetrovateľa, znalca) - ich "dotyk" s realitou, reálne úkony. Hlavné poslanie teória kriminalistickej identifikácie spočíva v objasnení spôsobu, ako skúmať konkrétne objekty, aby bola objasnená ich spojitosť so vyšetrovanou udalosťou.
Súčasná podoba klasickej, tzv. objektovej identifikácie však už dnes veľakrát nestačí na dosiahnutie konečného cieľa, t.j. zistenie totožnosti konkrétneho objektu. Za tým účelom bola novovytvorená forma kriminalistickej identifikácie, tzv. kriminalistickej identifikácie systémov. Identifikácia objektov a systému nie sú v protiklade, vzájomne sa nevylučujú, ale sú v súlade a navzájom sa dopĺňajú. Identifikácia systémov je v súčasnej dobe modernou špecifickou kriminalistickou teóriou, ktorá môže byť užitočná najmä v prípadoch, kedy klasická kriminalistická identifikácia objektov nevedie k úspešnému cieľu a problém sa dá riešiť vytvorením a následnou identifikáciou systémov.

B. Systémová identifikácia objektov

Základy teórie kriminalistickej identifikácie systému zavádza do kriminalistiky Porada, (1987).

Systémový prístup k identifikácii objektov priniesol nové pohľady na poňatie kriminalistiky, ktorá vychádza z fyzikálnej interpretácie a následného matematického spracovania základného kriminalistického problému, t.j.

správnou interpretáciou stôp trestného činu tento čin rekonštruovať a identifikovať páchateľa. Z tohto moderného pohľadu bola skúmaná:

a) identifikácia ako proces stotožňovania objektov,
b) schéma systémového prístupu, stav a štruktúra systému,
c) kritérium zhody objektov s modelovým objektom a
d) vplyv chýb na identifikáciu.

V prípade systémového poňatia identifikácie ide tiež o stotožňovanie, ale iného druhu. Identifikácia v kriminalistike sa líši od identifikácie v iných oblastiach ľudského poznania. Podrobným štúdiom kriminalistickej stopy (identifikačných znakov, mechanizmu vzniku stopy v okolí) sa vyčleňujú tzv. vstupné informácie I_{vst}, pomocou ktorých vytvárame modely (porovnávacej vzorky). V rozhodovacom bloku vzájomným porovnaním výstupných informácií I_{vyst} z kriminalistickej stopy a jednotlivých porovnávacích vzoriek, na základe aplikácie kritérie zhody, zisťujeme totožnosť (hľadaný vzťah totožnosti) medzi stavmi a prejavmi jedného a toho istého objektu. Ide teda o objekt, ktorý spôsobil kriminalistickú stopu, a o príslušnú porovnávaciu vzorku (stotožňujúci objekt známeho pôvodu).

Poznávací proces je teda neustála konfrontácia našich predstáv a modelov (abstraktných i materiálnych) s objektívnou realitou. Tento proces stotožňovania objektívnej reality s jej modelom je identifikácia. Všetky postupy a metódy používané pri tomto procese nazývame identifikačné postupy. Systémový prístup k identifikácii objektov vyústil v posudzovanie zhody systémov vytvorených nad stopami trestných činov a porovnávacích vzoriek.

So systémovou identifikáciou úzko súvisí **diagnostická činnosť bezpečnostných subjektov** (Požár, 2006, s. 141). Je ju možné chápať aj ako proces rozpoznávania, určenie, stanovenie príčin a podmienok problému, kedy hlavným a špecifickým rysom je vzájomná komparácia (porovnávanie, porovnanie). Je to teda porovnávacia vedecká metóda, kedy získané poznatky v bezpečnostnej činnosti sa porovnávajú so skutočnosťou. Identifikáciu systému možno použiť aj ako prechod pre jednoznačné určenie konceptuálnych zložiek systému. Ten sa skladá z troch krokov (Vlček, 1976, s. 50):

1. **Výber prvkov**, ktoré patria do systému to buď jednoducho súpisom, vymenovaním alebo inak zistené relevantné údaje a informácie. Je zrejmé, že výsledky tohto identifikačného kroku ovplyvnia rozlišovaciu úroveň. V praxi policajnej bezpečnostnej činnosti to znamená, že napr. kriminalista či policajný inšpektor hľadá a získava relevantné a podstatné informácie o páchateľovi trestného činu v prípade zisťovania alebo objasňovaní trestného skutku, kedy je doposiaľ neznámy páchateľ.

2. **Priradenie funkcií** (náplne) jednotlivých prvkov v predchádzajúcom identifikačnom kroku. Jedná sa o sumarizáciu a analýzu získaných údajov a informácií. Napríklad v policajne bezpečnostnej činnosti sa môže jednať o previerku relevantných informácií, výsluchom obvineného, svedkov, porovnaním s protokolom obhliadky miesta činu a pod.

3. **Parametrizácie väzieb prvkov** s prihliadnutím k priradeným funkciám. V bezpečnostnej činnosti sa väčšinou jedná o syntézu analytických informácií, z vonkajších informačných zdrojov, ale aj z údajov a informácií získaných z policajných evidencií, vlastných skúseností a pod. Výsledkom je potom súhrn alebo vznesenie obvinenia.

Tento základný postup identifikácie systému je vo všetkých svojich troch krokoch podmienený zvolenou rozlišovacou úrovňou, t.j. podrobnosťou pozorovania a vlastného skúmania celého systému v bezpečnostných činnostiach. Identifikácia systému nie je činnosťou jednorazovou, ale prebieha iterakčným spôsobom, tzn. dochádza k postupnému spresňovaniu jednotlivých verzií systému. Rozpoznanie identifikácie, ale aj verifikácia systému je proces, v ktorom sa identifikujú určité, konkrétne entity (Požár, 2006, s. 141-3). Na základe systémového prístupu Poradu (1987), rozvádza problematiku Požár do radu praktických súvislostí (Požár, 2006, s. 142-143).

C. Biometrická identifikácia a verifikácia

Problematikou biometrickej identifikácie a verifikácie sa zaoberajú najmä Rak, Porada, Šimšík, (2001-2010). Opierajú sa o biometrické charakteristiky ľudského tela a jeho prejavov. Podľa základného princípu identity (totožnosti), každá osoba je identická len a len sama so sebou.
Biometrická identifikácia je využitie jedinečných, merateľných, fyzikálnych alebo fyziologických znakov (tzv. markantov) alebo prejavov človeka k jednoznačnému zisteniu (identifikácia) alebo overenie (verifikácia) jeho identity.
Pod pojmom biometria môžeme chápať merateľné biometrické charakteristiky (obrazce, údaje atď.) živého organizmu, ktoré sa snímajú, spracovávajú, vyhodnocujú a uchovávajú v procese identifikácie alebo verifikácie.
Predpokladom pre využitie každej biometrickej charakteristiky je teda jedinečnosť, stálosť, praktická merateľnosť a technologická možnosť ďalšieho spracovania zameraného na vyhodnocovanie porovnávaných charakteristík, patriacich rôznym jedincom.
Nevyhnutným atribútom, základným rysom biometrickej identifikácie je automatizované využitie jedinečných, merateľných anatomických alebo

fyziologických charakteristík alebo prejavov človeka k jednoznačnému zisteniu alebo overeniu jeho identity.
Rozoznávame biometrickú identifikáciu policajno-súdnu (forenznú), bezpečnostno-komerčnú a ezotorickú. V poslednom období bol výskum v oblasti kriminalistickej biometrickej identifikácii zameraný na zisťovanie totožnosti osôb podľa dynamického stereotypu chôdze človeka (Porada, Šimšík, 2010).

D. Identifikácia a autentizácia v informačných a komunikačných technológiách.

Požár (2006, s. 144-145) uvádza, že v prevádzke výpočtových systémov, najmä v informačných a komunikačných technológiách, je potrebné správne identifikovať všetkých užívateľov, ktorí vstupujú do informačného systému a ďalej s ním pracujú. Každý užívateľ má presne vymedzené práva, podľa ktorých môže jednotlivé informácie len čítať, alebo do systému zapisovať a meniť údaje alebo mať vyššie oprávnenie na úrovni správcu alebo administrátora výpočtového systému. Súčasne je potrebné zabezpečiť identifikáciu a autentifikáciu používateľov, teda určiť spôsob, miesto a čas, t.j. ako, kde a kedy sa prihlási do informačného systému. Vedecká definícia autentizácia uvádza, že "autentizácia je overenie identity používateľa alebo entity (užívateľa) v systéme, väčšinou za účelom riadenia prístupu k zdrojom a objektom v systéme". Znamená to toľko, že totožnosť používateľa alebo systému, s ktorým chce komunikovať, je účelné istým presne definovaným spôsobom overiť pred tým, než je mu umožnený prístup k zdrojom vlastného systému (dátam, strojom času a pod.). Autentizácia je proces overovania, kontroly, ktorý nasleduje po identifikácii, že prihlásená entita (užívateľ), je naozaj tým, za koho sa vydáva (verifikácia osoby).

E. Možnosti identifikácie, simplifikácie a algoritmizácie bezpečnostnej činnosti

Túto oblasť poznania rozpracoval tiež Požár (2006, s. 144-146).

Pri skúmaní postupu pri riešení bezpečnostných problémov a úloh je evidentné, že po získaní počiatočných relevantných informácií, je nutné pomocou výpočtových systémov sumarizovať všetky získané dáta a potom vykonať identifikáciu, či právnu klasifikáciu problému. Z toho vyplýva, že je nutná realizácia postupných procedúr, t.j. zvoliť postup a algoritmus riešenia. Práve metódy informačných a komunikačných technológií spolu s teóriou algoritmizácie činnosti a informačných procesov majú svoje komponenty, ktoré

majú význam pre organizáciu, techniku, taktiku a metodiku a najmä pre manažment bezpečnostnej činnosti.

Pri identifikácii problému a následne úlohy bezpečnostnej činnosti je potrebná simplifikácia (zjednodušenie) a následná formalizácia. Pod formalizáciou úlohy sa rozumie postup získavania dát a relevantných informácií, potom je potrebná dôkladná analýza získaných dát a informácií, spresnenie obsahu prvkov a väzieb systému bezpečnostnej úlohy vrátane fixácie formálnych dát o trestnom čine za využitia informačných a komunikačných technológií. V praxi to znamená po vykonanej analýze dát stanoviť také prvky, ktoré sú stále, nemenné**, t.j. konštanty.** Je však isté, že počet takých konštánt bude malý, pretože bezpečnostná činnosť rovnako ako sociálny problém alebo úloha, je typickým tzv. zle štruktúrovaným problémom (Filák a kol., 2006, s. 144-146).

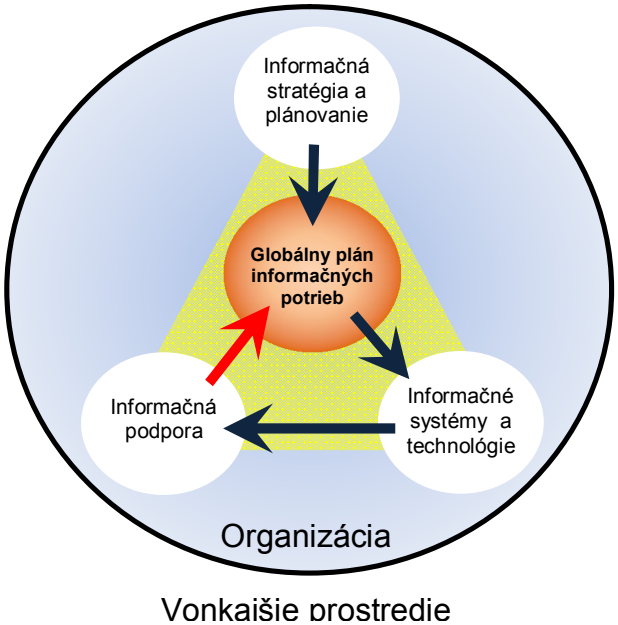
7 BEZPEČNOSTNÁ INFORMÁCIA

7.1 Vymedzenie základných pojmov

Problematika bezpečnostnej informácie je veľmi častá a bola preskúmaná radom autorov z rôznych aspektov (napr. Porada, Požár, 1999, Porada, Požár, 2001, Porada, Rak, 2001, Rak a kol., 2000, Požár, 2005, 2006. Informácia, ako uvádza napr. Požár, (2006, s. 158) sa dnes radí vedľa materiálnych, energetických a finančných zdrojov medzi hlavné faktory podmieňujúce pokrok vo všetkých odboroch ľudskej činnosti. Preto sa tiež hovorí o probléme informačnej explózie. Účelne čeliť tomuto novému fenoménu možno použitím efektívnych spôsobov získavania údajov o stave reálneho sveta a ich racionálne ukladanie, vyhľadávanie a využívanie odvodených dát a informácií. To potom zefektívňuje všetky bezpečnostné činnosti, najmä rozhodovania bezpečnostných pracovníkov a manažérov. Informácia o stavoch, javoch a procesoch potom predstavuje sama o sebe potenciálnu schopnosť ovplyvňovať procesy a meniť ich usporiadanie. Vo všeobecnosti, informácie predstavujú mieru usporiadanosti systémov. Naopak miera neusporiadanosti, chaosu, neurčitosti je vyjadrená entropiou. Organizácia práce s dátami a informáciami skvalitňuje a zrýchľuje nasadenie moderných informačných a komunikačných technológií. Informačnými technológiami rozumieme postupy, algoritmy a metódy, ktorými možno v nadväznosti na technickú štruktúru efektívne a kvalitne vykonávať operácie s veľkými objemami dát a podporiť tak proces zvyšovania pragmatickej hodnoty odvodzovaných dát, informácií a vedomostí (Mesároš, Rak, Porada, 2010). Základné pojmy spojené s bezpečnostnou informáciou:

- **Dáta** sú vyjadrenia skutočností a myšlienok v predpísanej podobe tak, aby ich bolo možné uchovávať, prenášať a spracovávať. Dáta sú objektívne hodnoty vlastností entít (charakteristík objektov), spravidla vyjadrené pomocou symbolov, vzorcov a slov alebo kódov vytvorených kombináciou alfanumerických a iných znakov.
- **Informácie** sú na rozdiel od dát výsledkom určitého procesu (spracovanie). Surovinou tohto procesu sú dáta. Často to je ľudský mozog, ktorý prevádza dáta na informácie. Informácie sú preto štruktúrované, ľudsky pochopiteľné dáta, ktoré tak majú pre človeka význam.
- **Znalosť** je psychologickým výsledkom ľudského vnímania, učenie sa a zdôvodňovanie najrôznejších informácií.
- **Zručnosť** je cvikom získaná motorická alebo myšlienková štruktúra umožňujúca kvalitné a rýchle vykonávanie určitej činnosti.
- **Skúsenosť** je v praxi použitá a overená znalosť a/alebo zručnosť.

- **Spravodajstvo** je znalosť ("spracované informácie") určené na stanovenie nejakého postupu (rozhodnutie konkrétneho človeka, v konkrétnej veci, v danom čase a za daných podmienok.
- **Informačný systém (IS)** je organizovaný celok získavania, prenášania, spracovania a ukladania dát na uspokojovanie informačných potrieb používateľov.
- **Informačné technológie (IT)** sú technologické a organizačné vzťahy a ich kvalita medzi jednotlivými prvkami informačného systému. Patria sem aj znalosti potrebné pre využitie nástrojov pre podporu všetkých procesov, výrobkov alebo služieb, rovnako tak ako ustálené postupy, metodiky a spôsoby práce s informáciami.
- **Informačná potreba** je informácia potrebná na dosiahnutie určitého cieľa. Sú to oprávnené užívateľské nároky na poskytnutie dát alebo informácií v požadovanom rozsahu, kvalite a štruktúre z informačného systému s cieľom zabezpečiť jeho ďalšiu náväznú profesijnú činnosť alebo rozhodovanie.



Obr.7.1: Základný vzťah informačnej stratégie, globálneho plánu, informačných systémov a technológií, informačnej podpory.

- **Informačná podpora** je miera uspokojovanie informačných potrieb jednotlivca alebo organizácie. Vychádza z možností použitých informačných technológií a procesov.
- **Informačná stratégia a plánovanie** je chápaná ako analýza súčasných a budúcich základných (strategických) informačných potrieb

bezpečnostnej organizácie a spôsobov ich naplnenia. Informačná stratégia vychádza z celkovej bezpečnostnej stratégie a je pravidelne upresňovaná v závislosti na vonkajšom a vnútornom prostredí.

- **Globálny plán informačných potrieb** je štruktúrovaný a konkretizovaný výsledok informačnej stratégie a plánovania s určením finančných prostriedkov, priorít, časových horizontov a zodpovednosťou pre jeho naplnenie.
- **Deontológia** je súbor organizačných a etických pravidiel správania jednotlivcov i profesijných skupín pri výkone svojich povinností (v spoločnosti, organizácii, firme a pod).
- **Bezpečnostná organizácia** plní úlohy bezpečnostného charakteru. Bezpečnostnou organizáciou v tomto ponímaní môže byť ministerstvo vnútra, policajné prezídium, bezpečnostná služba a pod.
- **Zložky** ofenzívneho aj defenzívneho spravodajstva, vojenskej polície a pod. a akákoľvek podriadená entita týchto štruktúr.
- **Koordinátor** je samostatný organizačný subjekt alebo osoba, poverená analýzou, riadením a realizáciou organizovaného, plánovitého a efektívneho prenosu vedeckých poznatkov do bezpečnostnej praxe podľa aktuálnych alebo globálnych potrieb všetkých bezpečnostných zložiek.

7.2 Aplikácia informačných a komunikačných technológií pri racionalizácii informačného procesu

Informačné a komunikačné technológie sa v súčasnosti, ale najmä budúcnosti budú podieľať na rozvoji a získavaní bezpečnostných informácií. Bude to predovšetkým v týchto oblastiach:

•Racionalizácia informačného procesu.

•Rozvoj bezpečnostných - policajných a civilno-administratívnych informačných systémov.

• Zvyšovanie kvalifikácie bezpečnostných pracovníkov.

• Skvalitnenie a zefektívňovanie manažérskych štýlov riadenia bezpečnostnej organizácie.

Každá bezpečnostná informácia je súčasťou informačného procesu (Rak, a kol., 2001, Požár, 2005, Požár, 2006, s. 173-174). Pod informačným procesom sa rozumie vykonávanie istých pracovných činností s informáciami. Tým sa menia procesy, činnosti a správania organizácie. Informačný proces je uzavretý cyklus, ktorým informácia prechádza od svojho vzniku až k svojmu použitiu. Na jeho začiatku i konci je nejaká informačná potreba. Informačný proces je zabezpečovaný vhodným informačným systémom.

7.3 Charakteristika a pojem bezpečnostných informácií

Jednotlivé druhy policajných činností, ktoré vyplývajú z bezpečnostných incidentov(udalostí) závisia od druhu, počtu, ako aj kvality policajných bezpečnostných informácií. Bezpečnostné informácie sú základom a materiálom pre vznik jednotlivých druhov bezpečnostných aktivít. Ide o informácie o aspektoch vzniku, priebehu a zániku bezpečnostných udalostí, resp. o rôznych protispoločenských činnostiach, poškodzujúcich, resp. ohrozujúcich životy a zdravie ľudí, majetok, ako aj iné zákonom chránené záujmy spoločnosti.
Informácie bezpečnostného charakteru, teda bezpečnostné informácie sú získavané z vonku, okolia systému bezpečnostných činností, čo vyplýva zo sociálneho charakteru bezpečnostnej činnosti práce, alebo musíme bezpečnostné informácie hľadať vlastnou usilovnou prácou. Z toho teda vyplýva, že bez dobre organizovaného systému informácií ani jeden policajný útvar a bezpečnostná služba nemôže úspešne riešiť zverené úlohy. Na množstve a vierohodnosti bezpečnostnej situácie závisí presnosť zhodnotenia bezpečnostnej situácie, efektívne riadenie bezpečnostnej činnosti, optimálnosť prijímaných rozhodnutí, cieľavedomosť plánovaného opatrenia, zrozumiteľné delegovanie úloh podriadeným subjektom, efektívnosť kontrolných opatrení a pod (Porada, Požár, 2001).
Aplikácia jednotlivých druhov bezpečnostných aktivít priamo závisí od množstva, kvality a vierohodnosti bezpečnostných informácií. Adekvátne množstvo presných a vierohodných informácií pozitívne ovplyvňuje správnosť vyhodnotenia bezpečnostne relevantných situácií, správnosť, presnosť a rýchlosť prijatých rozhodnutí, presnosť a rýchlosť komunikácie pri riešení úloh. Veľmi silne ovplyvňuje aj kvalitu a rýchlosť cieľavedomého, plánovitého, presného vykonávania jednotlivých úkonov a opatrení v rámci jednotlivých bezpečnostných činností a pod.
Pre efektívnosť jednotlivých druhov bezpečnostných činností je tiež potrebná existencia tzv. informačného systému, ktorý je nevyhnutným predpokladom efektívnej činnosti a riadenia bezpečnostnej organizácie (systému), koordinácia činností a vzťahov medzi jednotlivými službami, útvarmi a tímami, v záujme plnenia stanovených cieľov a z nich vyplývajúcich úloh. Špecifický tok bezpečnostných informácií veľmi úzko súvisí s informáciami sociálneho typu. V tomto zmysle je bezpečnostná informácia chápaná, ako osobitný druh sociálnej informácie, ktorá je využívaná v boji proti trestnej a inej protispoločenskej činnosti, na ochranu života, zdravia osôb a majetku, verejného poriadku, bezpečnosti cestnej premávky, ochrany štátnych hraníc a objektov (Filák a kolies., 2006, s. 163 a n.).
Bezpečnostné informácie z hľadiska metodologického, poznávacieho, musia byť podrobené dôkladnej analýze a vyhodnoteniu. Po ich analýze, vyhodnotení sú následne systematicky rozdeľované podľa jednotlivých bezpečnostných činností a slúžia tak ako systém poznatkov pre jednotlivé stupne riadenia

bezpečnostných činností, pri plnení ich úloh. Ide o informácie, ktoré sú syntézou celého množstva poznatkov o teoretických a praktických problémoch týkajúcich sa bezpečnostných udalostí a s nimi súvisiacich bezpečnostných činností (Požár, 2006, s. 165).
Bezpečnostné informácie zabezpečujú plnenie dvoch funkcií:

a) poznávacia
b) organizačná

Poznávacia funkcia spočíva v poznaní všetkých všeobecných i špecifických znakov sledovanej protispoločenskej činnosti, ktorá je objektom výkonu jednotlivých bezpečnostných činností.

Organizačná funkcia spočíva v efektívnej nadväznosti a organizácii činnosti jednotlivých bezpečnostných zborov zapojených do kontroly kriminality ako v oblasti prevencie, tak represie. Čím vyšší bude stupeň poznania objektívnej reality riadiacich orgánov bezpečnosti na príslušnom teritóriu, tým efektívnejší bude stupeň organizácie a riadenia ich výkonných zložiek. Organizácia činnosti bezpečnostného zboru svojím obsahom vyjadruje jednak spôsob realizácie vzťahov podriadenosti, kooperácie a koordinácie zainteresovaných subjektov vo vnútri a mimo systému bezpečnostnej práce. Organizácia činnosti orgánov bezpečnosti zahŕňa tiež aj problematiku optimálneho rozloženia síl a efektívneho využívania prostriedkov v oblasti zverených úloh, napríklad v oblasti kontroly kriminality.

Bezpečnostné informácie predstavujú systém vyhodnotených a systematicky roztriedených poznatkov o vzniku, zmene a zániku bezpečnostných udalostí, umožňujúcich efektívne organizovať, riadiť a koordinovať výkon bezpečnostných činností, zameraných na boj s kriminalitou a ostatnú protispoločenskú činnosť, s cieľom chrániť práva a oprávnené záujmy fyzických a právnických osôb, záujmy spoločnosti a ústavné zriadenie (Požár, 2006, s. 165).

7.4 Význam bezpečnostných informácií

Narušenie informačného procesu, vydávanie alebo získavanie nesprávnych a neadekvátnych informácií, poruchy ich prenosu vedú spravidla k nepresnej, či chybnej funkcii manažérskej činnosti. Schopnosť bezpečnostných pracovníkov a manažérov aj ich spolupracovníkov prijímať informácie a spracovať vo svojej činnosti relevantné informácie, vysporiadať sa s ich nadbytkom alebo naopak s nedostatkom závisí aj na ich vzdelaní a skúsenostiach. To všetko by malo vychádzať najmä (Filák a kol., 2006, s. 167-174):

- zo vzájomného vplyvu spôsobov jednotlivých činností, operácií a prostredia, v ktorom sa daná aktivita realizuje,

- z riešenia problémových bezpečnostných situácií a úloh spojených s rušivými vplyvmi, ktoré sa v bezpečnostnej organizácii vyskytujú.

Čím rôznorodejšie a mnohostrannejšie skúsenosti má bezpečnostný manažér a zamestnanec, tým sú ich činnosti stabilnejšie, tým väčší okruh rušivých vplyvov sú schopní prefiltrovať. Manažérska a bezpečnostná činnosť totiž funguje v podmienkach:

- neustále sa meniaceho prostredia,
- zvyšovania množstva a rôznorodosti informácií, ktoré majú spravidla významný vplyv na výsledok a úspech bezpečnostnej organizácie,
- trestná činnosť páchateľov používa čoraz rafinovanejšie metódy a prístupy pre páchanie najmä finančnej kriminality,
- kedy páchatelia plánujú a taktiež realizujú trestnú činnosť za využitia moderných prostriedkov komunikačných a informačných technológií.

Bez dôležitých a relevantných bezpečnostných informácií nie je možné efektívne riešiť a riadiť akúkoľvek činnosť, teda aj činnosť bezpečnostnú, zabezpečiť racionálne fungovanie a úspešný rozvoj a dosiahnuť vytýčených strategických, taktických i operatívnych cieľov bezpečnostnej organizácie.
Súhrn bezpečnostných informácií a z nich vyplývajúcich poznatkov je nevyhnutým predpokladom pre efektívne organizovanie a riadenie jednotlivých bezpečnostných činností. Čím vyšší počet kvalitných bezpečnostných informácií bude mať riadiaci orgán k dispozícii, tým efektívnejšia bude jeho riadiaca a organizačná činnosť vo vzťahu k podriadeným organizačným celkom. Naopak, nedostatok bezpečnostných informácií, obvykle spojený s pomerne vysokou mierou entropie, môže viesť k subjektivizmu v rozhodovaní, čo má za následok vydávanie intuitívnych a nepodložených rozhodnutí (Porada, Požár, 2001, Požár, 2006, s. 158-160).

8 MANAŽÉRSTVO RIZÍK

Manažérstvo rizík je všeobecne chápané ako *činnosť zameraná na zaistenie bezpečnosti alebo stability riadeného systému, analýzu rizík a možných ohrození a hľadanie vhodných korekčných a preventívnych opatrení na minimalizáciu negatívnych vplyvov rizikových javov a ich prerastanie do ohrození, do krízy.* (Reitšís, Mesároš 2004)
Z hľadiska bezpečnostného manažérstva je manažérstvo rizík chápané ako ***široká škála činností vedúca k zvládnutiu rizík, vrátane vyhodnocovania rizík a overovania účinnosti používaných postupov***. Predpokladá stanovenie cieľov, zber a vyhodnocovanie informácií a aktívne konanie, smerujúce k ovplyvňovaniu chovania ľudí alebo konkrétnych štruktúr. Zvládanie rizík pritom vyžaduje, aby sme sa dokázali pohybovať po ose „anticipácia budúceho" a „vyhodnotenie minulého" .(Burianek 2000)

8.1 Riziko

Riziko *(možnosť, nebezpečenstvo straty, neúspechu, škody)* je určitý druh neistoty, ktorý je možné prostredníctvom štatistických metód kvantifikovať a tak predpovedať vznik nepriaznivých skutočností. Predstavuje tiež pojem na označenie možnosti vzniku straty, škody, alebo dosiahnutie iného výsledku oproti pôvodne predpokladanému, resp. nedosiahnutia očakávaných výsledkov , pričom odchýlky môžu byť buď priaznivé(zisk) alebo nepriaznivé (strata). Riziko však poväčšine v sebe skrýva náboj potenciálneho nebezpečenstva nepriaznivého vývoja.
Historické korene slova **riziko** je možné popísať nasledovným spôsobom:

- rhiza (antické Grécko) - neistota, úzke miesto,
  - možnosť straty nákladu počas námornej plavby,
- resecare (latinský pôvod) - možnosť troskotania lode,
  - prekonanie nebezpečného útesu,
- risigio a neskôr risiko (germanofónna zóna Európy na začiatku 16. storočia) – strata a škoda a s ňou spojený odvážny čin na úseku obchodu a podnikania, (Šimák 2006)

Z hľadiska svojho obsahu a spôsobu používania sa postupne od seba oddeľovali termíny nebezpečenstvo a riziko, ktoré boli dlhú dobu používané ako synonymum. V súčasnosti je možné zvýrazniť hlavne tento rozdiel medzi nimi:

- nebezpečenstvo - má statický charakter a vyjadruje len potenciálnu negatívnu vlastnosť systému, teda časť obsahu termínu riziko,

· riziko - má dynamický charakter, pričom má priamy vzťah k hodnotámspoločnosti, ktorých existenciu ohrozuje,
- predstavuje možný negatívny dopad evolučného vývoja ľudského spoločenstva na životné prostredie a na vlastnú činnosť a samotnú existenciu na Zemi.

Nebezpečenstvo je latentná vlastnosť objektu spôsobiť neočakávaný negatívny jav (t.j. počas činnosti alebo existencie objektu môže vzniknúť mimoriadna udalosť). Je to podstatná, ale skrytá vlastnosť alebo schopnosť materiálu, technického zariadenia alebo pracovnej činnosti, ktorá môže spôsobiť škody. Nebezpečenstvo je zdroj možného zranenia alebo poškodenia zdravia, je to zdroj ohrozenia.

Ohrozenie je stav pôsobiaci na človeka alebo prostredie vznikajúci pri činnostiach, ktorých nebezpečné vlastnosti neboli v plnej miere zohľadnené. Je to možnosť aktivovať nebezpečenstvo v konkrétnom priestore a čase. Je to aktivované nebezpečenstvo, ktoré nebolo plne zohľadnené (závisí na vonkajších a vnútorných podmienkach).

Dôležité je uvedomiť si skutočnosť, že v spoločenských a technických a technologických systémoch sa zaužívalo rozdielne chápanie týchto pojmov a vzťahov medzi nimi:

· v technických a technologických systémoch je ohrozenie dôsledkom neakceptovaného a nezohľadneného nebezpečenstva a riziko mierou ohrozenia,
· v spoločenských systémoch je ohrozenie aktivizované riziko, ktoré pôsobí proti záujmom subjektu a zároveň to môžu byť aj konkrétne situácie, ktoré bezprostredne znemožňujú uskutočnenie plánovaných cieľov a vykonávanie konkrétnych činnosti a procesov.

Vo vedeckých štúdiách, v odbornej literatúre i v právnych normách, sa môžeme stretnúť s rôznymi definíciami pojmu riziko, závisí to na odbore činnosti, pre ktorý sa termín riziko definuje, ale tiež od účelu definície a jej plánovaného využitia.

Príklady niektorých definícií:

Analýza vnútornej bezpečnosti SR: Riziko - je potenciálna možnosť narušenia bezpečnosti systému, objektu alebo procesu. Je to pravdepodobnosť vzniku krízového javu a jeho dôsledku.
Bezpečnostná stratégia ČR z roku 2001: Riziko je možnosť, že s určitou pravdepodobnosťou vznikne udalosť, ktorá je z bezpečnostného hľadiska nežiaduca. Riziko je vždy odvoditeľné a odvodené z konkrétnej hrozby. Mieru rizika, teda pravdepodobnosť škodlivých následkov, vyplývajúcich z hrozby a

zo zraniteľnosti záujmov, je možné posúdiť na základe analýzy rizík, ktorá vychádza aj z posúdenia pripravenosti čeliť hrozbám.
Terminológia krízového riadenia SR: Riziko je potenciálna možnosť narušenia bezpečnosti systému, objektu alebo procesu. Je to pravdepodobnosť vzniku krízového javu a jeho dôsledku.
Smernica EÚ Seveso II: Riziko je pravdepodobnosť špecifických dopadov, ktoré nastávajú v priebehu špecifického obdobia alebo počas špecifických podmienok. (Šimák 2006)

Na základe analýzy rôznych definícií je možné zovšeobecniť niektoré závery a zhrnutia definovania termínu riziko:
a) každá definícia termínu riziko má celý rad osobitostí:

- vyjadruje názory, schopnosti a postoje autora k problému, preklad z jazyka autora nemusí byť presný, pretože každý jazyk má
- v obsahu pojmov svoje špecifiká,
- jeden termín môže byť definovaný rôznymi pojmami a jediná absolútne
- správna definícia použiteľná vo všetkých oblastiach ľudských aktivít neexistuje,
- prevažná väčšina definícií vychádza z pravdepodobnosti vzniku
- krízového javu,
- časť definícií kladie dôraz na možné škody a straty s dôrazom na stratu ľudských životov,
- definície podnikateľských rizík zdôrazňujú rozdiely medzi plánovaným a dosiahnutým stavom, ako aj možnosť straty vložených prostriedkov,
- niektoré definície sú založené na existencii neistoty, ktorá má charakter náhodného javu,

b) absolútne korektná definícia rizika by mala zohľadniť:

- znaky rizika ako udalosti (podmienky vzniku, časový priebeh, intenzita pôsobenia, odolnosť subjektu, ...)
- špecifické charakteristiky rizika (osobitosti z pohľadu pôsobenia rizika i reakcie prostredia na riziko).

Pri definovaní rizika, ako vyplýva z predchádzajúceho textu, sa v prevažnej väčšine prípadov vychádza z dvoch základných skutočností:

- výskyt nežiaduceho dôsledku,
- pravdepodobnosť, s akou tieto dôsledky môžu nastať (t. j. neistota, že bude dosiahnutý plánovaný výsledok prebiehajúcich dejov).

Riziko = neistota x nežiaduci dôsledok

Riziko = <u>nebezpečenstvo (ohrozenie)</u>
preventívne opatrenia (ochrana)

Z uvedeného vyplýva, že:
- riziko je možné znižovať uskutočňovaním preventívnych opatrení, prípadne rôznych foriem ochrany pred reálnym ohrozením,
- riziko nemôže byť nulové,
- samotné uvedomenie si rizika znižuje riziko.

Riziko je možné charakterizovať veľkým počtom rôznorodých znakov, ktoré podrobnejšie popisujú vzťah rizika k referenčnému objektu. Môžeme konštatovať, že riziko:
- j e skryté skoro v každom ľudskom konaní,
- j e súčasťou výsledkov vedeckého bádania,
- popisuje situáciu, ktorú možno s určitým stupňom spoľahlivosti predvídať,
- sa zväčšuje s počtom variantných riešení,
- súvisí s neznámym výsledok budúcich javov, pričom však známe je pravdepodobnostné rozdelenie budúcich javov,
- je možné kvantifikovať (kvantifikácia sa opiera o numerické metódy a o počet pravdepodobností),
- je možné znižovať dobrou bezpečnostnou politikou a zabezpečením proti rizikám súvisiacim s danou dobou (hospodárske úspechy krajiny znižujú podstatnú časť rizík),
- sa vyskytuje v troch prostrediach:
  - v hospodárskom prostredí,
  - v spoločenskom prostredí,
  - v osobnostnom prostredí,
- je často chápané ako:
  - varianty možných výsledkov,
  - nebezpečenstvo straty,
  - určitý stav informovanosti subjektu rozhodovania,
  - nebezpečenstvo chybného rozhodnutia,
  - objektívna a merateľná neistota,
- je stav neinformovanosti subjektu rozhodovania o objekte rozhodovania a o jeho okolí (rozhodovanie subjektu v stave neistoty, pričom na základe matematicko-štatistickej teórie rozhodovania sa určitému javu prisudzuje hodnota zo stanoveného intervalu),
- je rozptyl, čiže variabilita možných výsledkov (berie do úvahy žiaduce i nežiaduce odchýlky od stanoveného cieľa. V literatúre sa tiež prezentuje ako pozitívna a negatívna stránka rizika.).

- je nebezpečenstvo dosiahnutia negatívnych odchýlok od stanoveného cieľa alebo predpokladov (riziko je definované len v zmysle neúspechu, nedosiahnutia stanoveného cieľa),
- je nebezpečenstvo straty (finančná strata pri realizácii plánovaného variantu),
- je nebezpečenstvo chybného rozhodnutia (nepriaznivé dôsledky rozhodnutia na subjekt rozhodovania, finančná strata, strata postavenia, ...).

Z pohľadu ich prijateľnosti pre človeka rozoznávame dve základné skupiny rizík, ktorými sú akceptovateľné a neakceptovateľné riziká. (Šimák 2006)

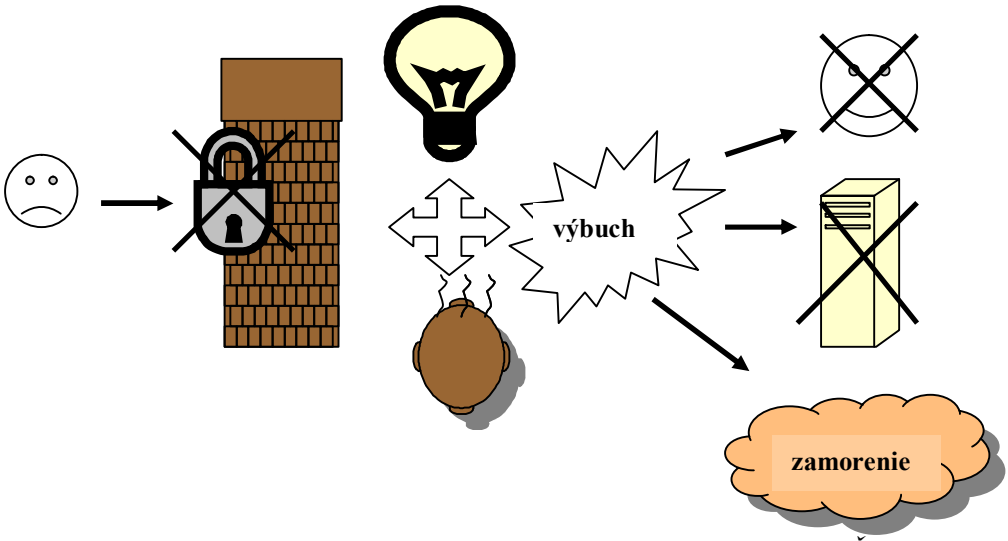
Pásmo akceptovateľných rizík:
- siaha od nulového až po hranicu vzniku neakceptovateľného rizika,
- hodnota rizika v tomto pásme je na úrovni, ktorá je spoločnosťou, právnymi normami a vnútornými podmienkami procesov tolerovaná,
- obsahuje riziká, ktoré umožňujú subjektom existovať a plniť stanovené ciele s vedomím existencie rizika.

Pásmo neakceptovateľných rizík:
- leží medzi hranicou neakceptovateľného rizika a hranicou maximálnej úrovne rizika,
- sú v ňom rozmiestnené riziká, ktoré je nevyhnutné priebežne monitorovať a postupne znižovať,
- pri prekročení hranice maximálnej úrovne rizika sa systém vychyľuje z rovnovážneho stavu.

V praxi sa teda skôr stretávame s **minimálnou úrovňou rizika**, na úroveň ktorého sa snažíme dostať v procese znižovania rizika. Toto riziko má niekedy aj charakter **zostatkového rizika**, ktoré už ďalej nemôžeme znižovať bez zmien v stanovených vnútorných a vonkajších podmienkach (napr. stanovená výrobná cena, prípadne stanovená kvalita surovín, miera bezpečnosti zariadenia, ...). Minimálna úroveň rizika teda predstavuje riziko, ktoré:
- je možné považovať za minimálne možnú úroveň rizika (prakticky však o ňom môžeme hovoriť ako o nemožnom),
- je nutné priebežne monitorovať, aby sme mohli včas zaznamenať prípadne zmeny v miere rizika, ale aj v jeho charakteristike. (Šimák 2006)

Synergický efekt vzájomného vzťahu rizík potvrdzuje skutočnosť, že existujú riziká, ktoré môžu iniciovať vznik celého radu ďalších rizík, ktoré existujú spoločne so zdrojovým rizikom a bez jeho existencie nemôže existovať celá skupina súvisiacich rizík. Na modelovom príklade páchateľ sa vlámal do objektu s výbušným chemickým materiálom, pri krádeži spôsobí poškodenie elektroinštalácie, el. skrat a explóziu s následným vznikom tlakovej vlny,

rozptylom črepín, zamorením priestoru, stratu ľudských životov, poškodenie zdravia a poškodenie majetku.



Obr. č.: 8.1: *Synergický efekt rizikových javov (spracované podľa Šimák 2006)*

Riziko je kvantitatívne a kvalitatívne vyjadrenie ohrozenia, stupeň alebo miera ohrozenia. Je to pravdepodobnosť vzniku mimoriadnej udalosti a jej dôsledok (je spojené s početnosťou a rozsahom mimoriadnej udalosti). Keďže žiadna ľudská aktivita nie je absolútne bezpečná, je nutné stanoviť mieru rizika, ktorú je možné akceptovať (***akceptovateľné riziko***). Akceptovateľné riziko je zo skúsenosti a odborných zdrojov stanovené hodnotou 10^{-5} až 10^{-7}, tzn. že negatívny jav sa môže vyskytnúť jedenkrát zo 100 000 až 10 000 000 prípadov, prípadne jedenkrát za uvedený počet časových jednotiek. Okrem toho existuje ***zostatkové riziko***. Je spojené hlavne s technickými zariadeniami a predstavuje mieru rizika, ktorú nie je možné úplne eliminovať pri konštruovaní príslušného zariadenia. Preto sa uvádza v informácii pre užívateľa vrátane možných dôsledkov príslušného negatívneho javu Uvedené pojmy nie je možné od seba oddeľovať, pretože sú to tri stránky tej istej reality. Nebezpečenstvo je zdrojom ohrozenia a riziko je mierou tohto ohrozenia. Sú teda vzájomne previazané a navzájom sa podmieňujú.(Šimák 2006)

Riziká sú neoddeliteľnou súčasťou všetkých spoločenských procesov. Vyjadrujú možnosť narušenia prebiehajúcich procesov, dejov a činností v konkrétnych bodoch v závislosti na vnútorných a vonkajších podmienkach. Analýza bezpečnostných rizík a ich rešpektovanie v praxi umožňuje predchádzať konkrétnym ohrozeniam, ktoré narušujú stabilitu systému a vnášajú neistotu do plánovaných procesov, znemožňujú reálne prognózy budúcnosti. Riziká sa prejavujú v narušení jednotlivých faktorov bezpečnosti a vyvolávajú príslušnú úroveň ohrozenia.

Riziko teda nie je stav ani proces, ale je to vzťah systému schopného spôsobiť závažnú zmenu v pláne, či jeho narušenie a referenčného systému, ktorého funkcia, ciele a plánované procesy sú ohrozené. Riziko a ohrozenie sú kategóriami, pomocou ktorých označujeme možné narušenie bezpečnosti.
Riziko vyjadruje možnosť ohrozenia subjektu dôsledkami rôznych mimoriadnych udalostí a krízových javov. Sú to očakávané škody a straty (na životoch, zdraví, škody na majetku, prerušenie ekonomických aktivít, atď.) zavinené zmenou vonkajších a vnútorných podmienok v konkrétnom priestore a v konkrétnom čase. Spravidla je založené na matematickej kalkulácii pravdepodobnosti. Výpočet pravdepodobnosti je reálny v prípadoch, keď ide o relatívne sa opakujúce ohrozenia (povodne, dopravné nehody, ...). Na druhej strane sa komplikovanejšie určuje pravdepodobnosť takého rizika, s ktorým nie sú skúsenosti a preto nie je o ňom vytvorený dostatočný štatistický hodnoverný súbor údajov (napr. riziko ohrozenia v prípade kolízie planéty s vesmírnym telesom, poškodenia jadrovej elektrárne, teroristického útoku na významný priemyslový či iný objekt a pod*.)*. Riziko je vždy spojené s objektívnou existenciou ohrozenia, hrozby a subjektívnou pripravenosťou (zraniteľnosťou) túto hrozbu znášať.
Riziko vnímame tiež ako **ohrozenia bezpečnosti** spoločnosti, štátu, sociálno-ekonomického alebo sociálno-politického systému.

8.2 Manažérstvo rizík pri ochrane osôb a majetku

Základom manažérstva rizík je myšlienkový proces, ktorý je založený na predstave o možných rizikách a ohrozeniach na jednej strane, a zdrojoch na ich elimináciu na druhej strane, pričom cieľom manažérstva rizík je využiť dostupné zdroje na zabránenie prerastenia rizík na ohrozenia, resp. do krízových situácií.

Z vyjadrenia rizika ako funkcie pravdepodobnosti vzniku negatívneho javu (udalosti) a veľkosti jej následkov (**R = PxD**) vyplýva, že cieľom manažérstva rizík bude :

- **zníženie rizika ,** čo sa dá dosiahnuť buď:
  a) *ofenzívnymi opatreniami*, zameranými na **zníženie pravdepodobnosti** vzniku negatívnych javov, alebo
  b) *defenzívnymi opatreniami,* zameranými na **znížene následkov** (škôd, strát na majetku, životoch a pod.) formou preventívnych opatrení, čo je možné v prípade potenciálnych negatívnych javov a udalostí ako predvídateľných, tak i nepredvídateľných

- **rozloženie (diverzifikácia) dôsledkov rizika** na viacej subjektov, napr. na bezpečnostné služby, na manažment spoločnosti a pod.

- **prenos (transfer) dôsledkov rizika** v plnom rozsahu napr. buď len na poisťovňu, alebo len na bezpečnostnú službu,
- **akceptácia rizika.**

Proces manažérstva rizík, vzťahujúcich sa na sociálne prostredie, má znížiť riziko na sociálne prijateľnú hranicu – na prijateľné alebo akceptovateľné riziko.

Prijateľné (akceptovateľné) riziko je taká hodnota rizika, ktoré je subjekt bezpečnosti schopný, resp. ochotný znášať. Okrem toho je definované aj **zostatkové riziko,** ktoré vyjadruje hodnotu rizika po uplatnení (vykonaní) všetkých dostupných preventívnych (technických i organizačných) ochranných opatrení.
Vzájomný vzťah prijateľného (akceptovateľného) rizika (R_A) a zostatkového rizika (R_Z) je možné vyjadriť ako :

$$\mathbf{R_Z \leq R_A} \qquad (8.1.)$$

Analýza procesov manažérstva rizík, zameraných na zníženie rizík naznačuje, že neexistuje žiadny jednotný, univerzálny model, platný pre všetky prostredia , podmienky, či inštitúcie.

V podnikateľskom prostredí (Fotr 2001) sú prístupy k riadeniu rizík spoločností definované v nasledujúcich bodoch :
1. Identifikácia rizík a stanovenie ich významnosti.
2. Stanovenie veľkosti rizika a jeho hodnotenie.
3. Príprava, voľba a realizácia opatrení na zníženie rizika.
4. Operatívne riadenie rizika.

V teórii rizík je štruktúra riadenia rizika vyjadrená v piatich bodoch:
a) Identifikácia a ocenenie rizika.
b) Monitorovanie rizika.
c) Politika rizika.
d) Implementácia politiky.
e) Program riešenia rizikových situácií. (Majerník, Mesároš, Bosák 2003)

Pre **prax bezpečnostného manažmentu** je možné definovať nasledujúce postupné činnosti (kroky) pri manažérstve rizík :
1. Identifikácia a hodnotenie rizík .
2. Tvorba a prijatie bezpečnostnej koncepcie a bezpečnostnej politiky.
3. Vytvorenie a riadenie bezpečnostného systému.

8.2.1 Identifikácia a klasifikácia rizík

Identifikácia rizík je rozhodujúcim predpokladom a východiskom pre efektívne riadenie rizík. Platí zásada, že riziká, ktoré nie sú identifikované, nemôžu byť a ani nebudú riadené, alebo inak ovplyvňované.
Identifikácia rizík spočíva v odhalení možných neželaných negatívnych udalostí a javov, nachádzajúcich sa (existujúcich) v rôznej forme a podobe v bezpečnostnom prostredí, ktoré môžu privodiť ohrozenie záujmov i existencie samotného subjektu bezpečnosti (občana, sociálnej skupiny, právnickej osoby a pod.).

Základným obsahom identifikácie rizík je :

- spracúvanie informácií o vonkajšom a vnútornom bezpečnostnom prostredí,
- vypracovanie registra rizík, ktoré majú alebo môžu mať vzťah k posudzovanému objektu (chránenému záujmu),
- vyjadrenie pravdepodobnosti alebo plauzibility (vierohodnosti) rizika.

Kritériami pre **klasifikáciu rizík** pre potreby bezpečnostného manažérstva môžu byť :

- teritoriálny rozsah rizík,
- zdroje (príčiny, resp. povaha) rizík,
- nositelia rizík,
- charakter pôsobenia rizík,
- čas trvania (pôsobenia),
- vývojové tendencie rizík,
- mechanizmus vzniku a pôsobenia rizík.

Register rizík

Dôsledná a objektívna analýza bezpečnostného prostredia umožňuje vypracovanie registra všetkých rizík, ktoré sú produktom bezpečnostného prostredia. Ide o to, aby boli zodpovedané otázky :

1. ČO SA môže stať ?
2. PREČO sa to môže stať ?

Riziká, ktoré majú svoj pôvod v danom bezpečnostnom prostredí môžeme rozdeliť do dvoch základných skupín :

- vonkajšie
- vnútorné.

Vonkajšie riziká sú tie, ktorých nositelia (zdroje, príčiny) sa nachádzajú mimo objektu a pôsobia z vonka chráneného objektu. K takým bezpečnostným rizikám patria:

a) **kriminálne skutky** , ako napr. :
- krádeže vlámaním,
- lúpežné prepadnutie,
- krádež utajovaných skutočností (firemných, štátnych, vojenských a pod.),
- vydieranie,
- počítačová kriminalita,
- umiestnenie výbušného nástražného systému,
- narušenie verejného poriadku v blízkosti objektu,
- sabotáž a pod.

Ich nositeľmi (zdrojmi, pôvodcami) môžu byť:
- odporcovia ,
- konkurenti,
- ofenzívne komerčné spravodajské služby,
- cudzie spravodajské služby,
- extrémisti,
- záškodníci,
- teroristi,
- delikventní jedinci,
- zločinecké skupiny (skupiny organizovaného zločinu) a pod.

b) **technologické a výrobné zariadenia,** v ktorých sú možné prípady priemyslových havárií s dosahom na chránený objekt,

c) havárie stacionárnych alebo mobilných zdrojov nebezpečných a škodlivých látok, ktoré môžu privodiť ohrozenie objektu ochrany a chráneného záujmu buď v dôsledku úniku nebezpečných látok alebo pôsobenia iných ničivých faktorov (výbuch, požiar, tlaková vlna a i.).

d) živelné pohromy a katastrofy (záplavy, zemetrasenia, rozsiahle požiare a pod.), pri ktorých nepriaznivé pôsobenie prírodných síl môže mať negatívny vplyv na chránený objekt (chránený záujem) .

Vnútorné riziká sú také, ktorých nositelia sú vo vnútri (sú súčasťou) objektu (chráneného priestoru). K takým rizikám môžu patriť:

a) kriminálne skutky, ako napr.:
- krádeže,
- sprenevera,
- podvodné konanie,
- priemyslová (obchodná) špionáž,
- prezradenie utajovaných skutočností,
- sabotáž a pod.

Ich nositeľmi môžu byť :

- vlastní zamestnanci,
- pracovníci bezpečnostnej služby, ktorí majú príslušné oprávnenia, majú možnosť vstupovať do objektov (chránených priestorov) bez dozoru, poznajú systém ochrany a chránené priestory a mohli by pomôcť narušiteľom zvonka prekonať zabezpečovacie systémy, alebo sa môžu sami dopustiť kriminálnych skutkov.

  Motiváciou takéhoto konania môže byť :

  - pocit krivdy (skutočnej alebo domnelej),
  - povahové črty (ziskuchtivosť, lakomstvo, závisť, sklon k hazardu, náročný spôsob života a pod.),
  - pomsta ,
  - vydieranie inou osobou a pod.

b) technologické a technické zariadenia, ktoré sú súčasťou objektu a môžu v dôsledku ich havárií alebo požiaru spôsobiť ohrozenie chráneného objektu (chráneného záujmu).

Príčinou ohrozenia môže byť:

- porucha systému (zariadenia),
- úmyselné poškodenie (sabotáž),
- havária (zavinená, nezavinená).

Výsledkom je spracovanie zoznamu vonkajších a vnútorných rizík rôznej povahy, ktoré môžu akýmkoľvek spôsobom privodiť ohrozenie objektu (chráneného priestoru), narušiť jeho integritu, spôsobiť nežiaduci negatívny jav (udalosť) alebo spôsobiť ujmu. Spracovaný register bezpečnostných rizík môže mať nasledujúcu formu:

Tabuľka 8.1 Register rizík (Reitšpís a kol. 2004)

Oblasť rizika	**Druh rizika**	**Forma prejavu**	**Príčiny, zdroje ,**
Vonkajšie riziká	Kriminalita	Vlámanie	Náhodný páchateľ
			Organizovaná skupina
			Konkurencia
		Bombový útok	Teroristi
		Sabotáž	Konkurencia
		.....	.....
	Chemická továreň	Zamorenie objektu	Havária
			Sabotáž
	Mobilný zdroj škodlivých látok	Zamorenie objektu	Havária
Vnútorné riziká	Kriminalita	Krádež materiálu	pracovníci výroby
			pracovníci expedície
		Prezradenie	obchodný úsek

		obchodného tajomstva	správca siete
	.....	.....	.....

Z takto vypracovaného registra rizík je možné získať pre ich podrobnú identifikáciu.

8.2.2 Metódy identifikácie rizík

Identifikácia rizík spočíva v odhalení možných neželaných negatívnych udalostí a javov, nachádzajúcich sa (existujúcich) v rôznej forme a podobe v bezpečnostnom prostredí, ktoré môžu privodiť ohrozenie záujmov i existencie samotného subjektu bezpečnosti (občana, sociálnej skupiny, právnickej osoby a pod.).

Na identifikáciu rizík môžu byť použité:

- pravdepodobnostné modely,
- expertné odhady.

8.2.2.1 Pravdepodobnostné modely identifikácie rizík

Identifikácia rizika je neoddeliteľne spätá s určením pravdepodobnosti, že uvažovaná udalosť alebo jav existuje, alebo nastane (Reitšpís, Mesároš a kol. 2004)

Zo známych pravidiel príčinnosti vyplýva, že :

- kedykoľvek existuje nejaká **príčina**, vždy spôsobuje svoj následok, a
- každý **následok** je spôsobovaný súborom príčin, alebo rozličnými nezávislými príčinami.

Pre vytvorenie pravdepodobnostného modelu na identifikovanie bezpečnostného rizika (určenie stupňa pravdepodobnosti, že uvažované riziko existuje a jeho dôsledky nastanú), sa používa metóda vypočítania pravdepodobnosti dôsledku P(D) na základe pravdepodobnosti jednotlivých predpokladov, resp. aplikácia vety o úplnej pravdepodobnosti.

Produkčné pravidlo

Pre potreby identifikácie rizika môžeme použiť produkčné pravidlo (Popper, Kelemen 1988). Potom je možné uviesť :

- **ak** existujú (sú vytvorené) vhodné predpoklady,
- **tak** bude existovať aj riziko narušenia bezpečnosti.

Prvá časť pravidla (antecendent) predstavuje *predpokladovú* časť (**P**), ktorá ak je splnená, platí konzekvent – *dôsledkovú (akčnú)* časť (**R**), uvedená za slovom TAK. Potom zápis v tvare :

$$\mathbf{P \Rightarrow R} \qquad (8.2.)$$

vyjadruje, že ak každý predpoklad P má priradenú určitú pravdepodobnosť, aj pre dôsledok R platí, že každý dôsledok (riziko) je vyvolaný viacerými predpokladmi, ktoré sú viazané operáciou konjunkcie alebo disjunkcie, čo znamená, že :

- na to, aby vznikol dôsledok, sa vyžaduje súčasná platnosť viacerých predpokladov (v prípade konjunkcie), alebo
- na vznik dôsledku postačuje platnosť aspoň jedného zo súboru predpokladov (to v prípade disjunkcie).

Metóda vypočítania pravdepodobnosti dôsledku P(D) na základe pravdepodobnosti jednotlivých predpokladov

Použiteľnosť tejto metódy identifikácie rizík je závislá od možnosti vyjadrenia pravdepodobností predpokladov. Objektívnosť vyjadrenia pravdepodobnosti jednotlivých predpokladov je zase závislá od kvality a objektívnosti viacerých štatistických údajov a ďalších podmienok, ktoré vytvárajú priestor na definovanie predpokladov.

Nevýhodou metódy je, že v prípade, ak je dôsledok podmienený potrebou súčasnej existencie všetkých definovaných podmienok (teda konjunkciou svojich podmienok), dospejeme k neprimerane nízkej výslednej hodnote, s ktorou budú predpoklady podporovať platnosť dôsledku (rizika). Nárastom počtu predpokladov, aj keď budú mať vysokú pravdepodobnosť, výsledná pravdepodobnosť dôsledku monotónne klesá.

Keď bude dôsledok podmienený disjunkciou predpokladov (na to, aby bol definovaný dôsledok, stačí existencia jedného alebo len niekoľkých zo súboru predpokladov), s nárastom počtu predpokladov, hoci aj s nízkou pravdepodobnosťou, výsledná pravdepodobnosť dôsledku monotónne rastie.

Veta o úplnej pravdepodobnosti

Iný variant použitia pravdepodobnostného modelu na identifikovanie rizika je aplikácia ***vety o úplnej pravdepodobnosti***. (Reitšpís, Mesároš a kol. 2004)

Z vety o úplnej pravdepodobnosti vyplýva, že pravdepodobnosť rizika R sa môže vyčísliť ako súčet súčinov pravdepodobnosti každej podmienky P_i s pravdepodobnosťou rizika za tejto podmienky :

$$P(R) = \sum_{i}^{n} P(Pi).P(R / Pi) \qquad (8.3)$$

kde P(R) je pravdepodobnosť rizika,
$P(P_i)$ je pravdepodobnosť predpokladu,

$P(R/P_i)$ je pravdepodobnosť výskytu rizika pri platnosti predpokladu P_i.

Uplatnenie vety o úplnej pravdepodobnosti však predpokladá, že budú známe (alebo dané) pravdepodobnosti predpokladov P_i, čo jej použitie opäť komplikuje.

Z hľadiska bezpečnostnej praxe je výhodnejšie použiť metódy expertných odhadov, pri ktorých sa výpočet pravdepodobnosti nahradzuje iným spôsobom vyjadrenia kvantitatívnych parametrov rizika.

8.2.2.2 Expertné odhady

Pre potreby identifikácie rizík môže byť použitá metóda založená na aplikácii teórie neostrých množín (Popper, Kelemen, 1988).

Pri aplikácii postupov z teórie neostrých množín sa pravdepodobnosť nahradzuje číselným vyjadrením, ktoré sa môže meniť spojito v intervale od **0 – úplne nevierohodné**, až po **1 – úplne vierohodné**. Takéto číslo vyjadruje stupeň pravdivosti, ktorý sa v neostrej logike nazýva ***plauzibilita*** (vierohodnosť) **- Π-** a je určitým analógom pravdepodobnosti.
Východiskové podmienky na uplatnenie tejto metódy budú rovnaké, ako pri použití pravdepodobnostných modelov.

Rovnako budeme vychádzať z aplikácie produkčného pravidla, teda :
- ak každý predpoklad P má priradenú určitú pravdepodobnosť, aj dôsledok R platí s určitou pravdepodobnosťou,
- na to, aby vznikol dôsledok, sa vyžaduje súčasná platnosť viacerých predpokladov (v prípade konjunkcie), alebo
- na vznik dôsledku postačuje platnosť aspoň jedného zo súboru predpokladov (to v prípade disjunkcie).

Rozdiel použitia tejto metódy spočíva v tom, že:
- miesto pojmu pravdepodobnosť budeme používať pojem plauzibilia,
- výpočet pravdepodobnosti rizika bude nahradený vyjadrením jeho plauzibiliy,
- výpočet pravdepodobnosti predpokladov bude nahradený vyjadrením ich plauzibility,
- plauzibilita predpokladov sa vyjadrí pomocou definovania plauzibilizy prvkov každého predpokladu.

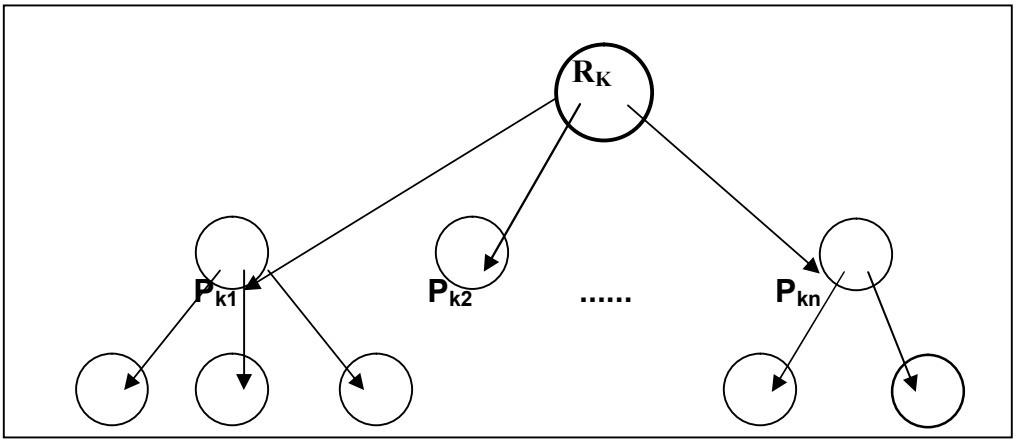
Na vyjadrenie plauzibility rizík je potrebné :

a) Definovanie predpokladov rizík a prvkov jednotlivých predpokladov. Tento postup je znázornený na obrázku 9.1.

b) Definovať stupnicu hodnôt plauzibilít, napr :

Tabuľka 8.2

Slovné vyjadrenie	**číselná hodnota**
Úplne nevierohodné	0
Takmer nevierohodné	0,1
Veľmi nevierohodné	0,2 – 0,3
Nevierohodné	0,4
Vierohodné	0,5 -0,6
Veľmi vierohodné	0,7 – 0,8
Takmer vierohodné	0,9
Úplne vierohodné	1



Obr.8.2: Strom analýzy rizík, ich predpokladov a prvkov predpokladov.(Reitšpís, Mesároš a kol. 2004)

Jednotlivé symboly znamenajú :
R_k - bezpečnostné riziko vybraté z registra bezpečnostných rizík,
P_{kn} - predpoklad **n** bezpečnostného rizika **k**,
p_{knm} –prvok **m** predpokladu **n** bezpečnostného rizika **k**.

c) Definovať prahovú hodnotu na posudzovanie plauzibility – koeficient **α**. Praktický význam tohoto koeficientu spočíva v tom, že na ďalšie posudzovanie sa vyberú len tie bezpečnostné riziká, ktorých plauzibilita bude :

$$\Pi (R_k) \geq \alpha \qquad (8.4)$$

Vyjadrenie plauzibility ľubovoľného rizika bude obsahovať nasledujúce kroky :

a) z registra **s** rizík sa vyberie na posudzovanie bezpečnostné riziko $\mathbf{R_k}$,
b) pre vybraté riziko R_k sa definuje **i** predpokladov P_{ki} a zostaví sa ich register,
c) z registra **i** predpokladov sa vyberie predpoklad $\mathbf{P_{ki}}$,
d) pre predpoklad P_{ki} rizika R_k sa definuje **j** prvkov, ktoré ho podmieňujú a zostaví sa ich register,
e) vyberie sa prvok p_{kij} a expertným odhadom sa vyjadrí sa plauzibilita; postupne sa vyjadrí plauzibilita všetkých **m** prvkov predpokladu P_{ki}
f) po vyjadrení plauzibility všetkých **m** prvkov predpokladu P_{ki} sa vyjadrí plauzibilita tohoto predpokladu,
g) postup popísaný v bodoch c) až f) sa opakuje, kým nie sú vyjadrené plauzibility všetkých **n** predpokladov rizika R_k,
h) keď sú vyjadrené plauzibility všetkých n predpokladov rizika R_k, vyjadrí sa jeho plauzibilita,
i) ak je plauzibilita rizika R_k väčšia ako koeficient prahovej hodnoty α, alebo sa jej rovná, zapíše sa riziko R_k do tabuľky rizík na ďalšie vyhodnocovanie,
j) tento postup sa opakuje, kým nebudú analyzované všetky riziká.

Na vyjadrenie plauzibility rizika (predpokladu rizika) môžeme uvažovať dve základné východiská:

1. riziko je determinované jediným predpokladom (prvkom predpokladu), alebo
2. riziko (predpoklad rizika) je determinované viacerými predpokladmi (prvkami predpokladu).

V prvom prípade, pokiaľ je riziko (predpoklad rizika) determinovaný jediným predpokladom (jediným prvkom predpokladu), a ten je kategoricky vyhodnotiteľný, potom má zmysel vyhodnocovať len to, či je predpoklad (prvok predpokladu) úplne vierohodný, alebo úplne nevierohodný (v číselnom vyjadrení 1 alebo 0). To však nebýva častý prípad.

Z praxe vyplýva, že pre každý zo súboru rizík (predpokladov rizík) je možné definovať určitý počet predpokladov (prvkov predpokladov), ktoré determinujú jeho existenciu, a ktoré sú viazané operáciou *konjunkcie* alebo *disjunkcie.* V takom prípade potrebujeme **metódu vypočítavania výslednej plauzibility rizika** (predpokladu rizika) na základe plauzibility jeho predpokladov (prvkov predpokladu).

Logická postupnosť krokov pri vyjadrovaní plauzibilít spočíva v tom, že sa postupne vyjadrí:

1. plauzibilita prvkov predpokladu,
2. plauzibilita predpokladu,
3. plauzibilita rizika.

Plauzibilita rizika R_k sa potom vyjadrí :

a) ak je determinované **konjunkciou** svojich predpokladov :

$$\Pi(R_k)=\Pi(P_{k1}\wedge P_{k2}\wedge....\wedge P_{kn})=\min[\Pi(P_{k1}),\Pi(P_{k2}),...\Pi(P_{kn})] \qquad (8.5)$$

kde : Π (Rk) je plauzibilita rizika R_k,
Π (P_{kn}) je plauzibilita predpokladu **n** rizika **k**,
$\wedge$ je operátor (A) konjunkcie súčasne sa vyskytujúcich predpokladov.

Pravidlo (8.5) vyjadruje, že plauzibilita rizika tvoreného konjunkciou svojich predpokladov zodpovedá hodnote plauzibility toho predpokladu, ktorý má minimálnu plauzibilitu.
V praxi to znamená, že ak budú realizované také opatrenia, ktoré minimalizujú plauzibilitu (vierohodnosť) jednotlivých predpokladov, aj plauzibilita toho, že bude existovať riziko, bude minimálna.

b) ak je determinované **disjunkciou** svojich predpokladov:

$$\Pi(R_k)=\Pi(P_{k1}\vee P_{k2}\vee....\vee P_{kn})=\max[\Pi(P_{k1}),\Pi(P_{k2}),...\Pi(P_{kn})] \qquad (8.6)$$

kde : : Π (Rk) je plauzibilita rizika R_k,
Π (P_{kn}) je plauzibilita predpokladu **n,** rizika **k**,
$\vee$ je operátor (alebo), vyjadrujúci disjunkciu predpokladov, podmieňujúcich dané riziko .

Pravidlo (8.6) vyjadruje, že plauzibilita rizika tvoreného disjunkciou svojich predpokladov zodpovedá hodnote plauzibility toho predpokladu, ktorý má maximálnu plauzibilitu.

8.2.3 Hodnotenie rizík

Cieľom hodnotenia rizík je priradenie číselnej hodnoty alebo slovného ohodnotenia ku každému identifikovanému riziku (Hofreiter 2002).
Na účely hodnotenia rizík sa využívajú nasledujúce skupiny metód:

- **Kvantitatívne** metódy využívajú numerické ohodnotenie rizík vyjadrením ich pravdepodobnosti, početnosti, vierohodnosti, potenciálu, dôsledkov a pod. Tieto metódy sa dajú použiť predovšetkým v tých prípadoch, ak je dostatok relevantných údajov, ktoré sa dajú hodnotiť štatisticky.

- **Kvalitatívne,** ktoré využívajú slovné vyjadrenie. Tieto sa využívajú v prípadoch, ak ide o jednoduché situácie, alebo ak chýbajú alebo sú ťažko vyjadriteľné číselné hodnoty (údaje) pre kvantitatívne ohodnotenie rizika. Pomocou týchto metód sa dá hodnotiť riziko ako napr. prijateľné alebo neprijateľné, malé, nízke, stredné a pod (Reitšpís, Mesároš 2004).

- **Polokvantitatívne** metódy využívajú kvalitatívne popísanie stupnice , ktoré majú pridelené číselné hodnoty. Kombináciou týchto charakteristík sa určí hodnota rizika. Uvedený spôsob sa používa napr. v bodovej metóde.

8.2.3.1 Kvantitatívne metódy hodnotenia rizika

Kvantitatívne metódy vyjadrenia veličín v procese analýzy rizík je možné charakterizovať takto**:**

- sú založené na matematickom vyjadrení riziká z frekvencie výskytu krízových javov a z ich možných dôsledkov,
- vyjadrujú straty spôsobené krízovým javom (ľudské životy, materiálne hodnoty – finančné vyjadrenie),
- sú spojené s väčšou náročnosťou na spracovanie,
- v niektorých prípadoch môžu byť menej priehľadné,
- využívajú hlavne:
  - štatistickú analýzu (štatistické charakteristiky miery variability - rozptyl, smerodajná odchýlka, variačný koeficient),
  - simuláciu (napr. metóda Monte Carlo),
- na podporu realizácie kvantitatívnej analýzy rizík sa používajú špeciálne nástroje v podobe programov, v ktorých sú metodika a systém analýzy rizík už zapracované. Týchto nástrojov existuje v súčasnosti už celý rad CRAMM, RiskPAC, RiskWatch, @RISK). (Simák 2006)

Kvantitatívne metódy hodnotenia rizika využívajú dva základné prvky:

- pravdepodobnosť (početnosť) vzniku negatívneho javu (negatívnej udalosti),
- dôsledky (škody, straty), ktoré takúto udalosť sprevádzajú, alebo sú ňou spôsobované.

Postup a kritériá pravdepodobnosti rizika je možné stanoviť podľa logického rámca.

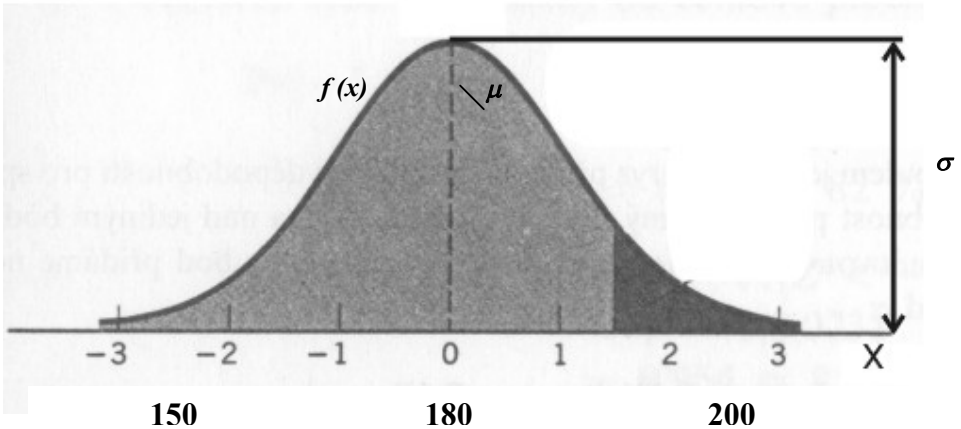
Tab. 8.3 Logický rámec pravdepodobnosti rizika

Existencia zdroja rizika	Existencia motivácie, resp. zámeru útočníka	Výskyt prípadu rizika v minulosti	Pravdepodobnosť rizika
Áno	Áno	Áno	Vysoká
Áno	Áno	Nie	Vysoká
Áno	Je možná	Nie	Stredná
Áno	Nie	Nie	Nízka
Je možná	Nie	Nie	Nízka
Nie	Nie	Nie	Žiadna

Pre presnejšie určenie pravdepodobnosti určitého rizika je možné použiť metódy aplikovanej matematiky pre výpočet pravdepodobnosti, napr. **normálne (gaussovo) rozdelenie pravdepodobnosti:**

Pre mnoho náhodných veličín má rozdelenie pravdepodobnosti tvar zvonu Táto krivka sa nazýva podľa nemeckého vedca Karla Friedricha Gaussa. Je to najviac rozšírené rozdelenie náhodných veličín.

Krivka určuje aká je početnosť udalostí v určitom intervale (počet trestných činov podvodu pomocou krádeže identity). Na základe pravdepodobnosti je ich v strede najviac, ale na začiatku a konci intervalu najmenej. Rozdiel medzi nízkou hodnotou grafu a tou najvyššou určuje pomer **„smerodajná odchýlka“** označovaná ako σ (pozri obr. 8.3). V najvyššom bode krivky sa nachádza **„stredná hodnota“ -** μ . (napr. počet 180) .



Obr. 8.3: Gaussovo rozdelenie pravdepodobnosti

Označenie hodnôt:
stredná hodnota - μ (napr. priemerný počet podvodov formou krádeže identity za posledných päť rokov),
smerodajná odchýlka - σ *(napr. priemerný nárast počtu podvodov za rok),*
meraná hodnota *x (pravdepodobnosť výskytu krádeže identity...)*

Hodnota pravdepodobnosti je rovná **ploche pod krivkou** v danom intervale. Je možné ju vypočítať zo vzťahu:

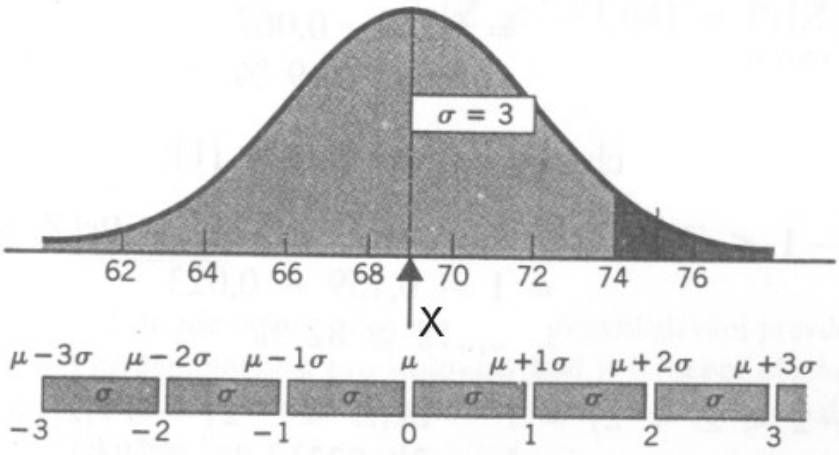
$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} \cdot e^{\frac{-(x-\mu)^2}{2\sigma^2}} \qquad (8.7)$$

Pravidlo 3σ hovorí o tom, že šírku plochy pod krivkou môžeme rozdeliť na niekoľko rovnakých úsekov o veľkosti σ (obr. 8.4). Podľa pravidla potom platí, že 68 % udalosti sa udeje v oblasti grafu, ktorá je od určitého miesta grafu X v intervale (-σ ; σ). Pravidlo ešte hovorí že 95 % udalosti sa nachádza v intervale (- 2σ; 2σ) a *99,8 %* udalosti sa nachádza v intervale (-3σ ; 3σ). Bod X je stred klobúka (stredná hodnota).

Potom platí :

$$\begin{aligned} &P(\mu - \sigma \le X \le \mu + \sigma) \approx 0{,}6826 \\ &P(\mu - 2\sigma \le X \le \mu + 2\sigma) \approx 0{,}9544 \\ &P(\mu - 3\sigma \le X \le \mu + 3\sigma) \approx 0{,}9973 \end{aligned} \qquad (8.8)$$

kde písmeno P označuje pravdepodobnosť, X je bod na osi x. V zátvorkách je rozsah intervalu.



x

Obr. 8.4 Kde X = μ (stredná hodnota)

8.2.3.2 Kvalitatívne metódy hodnotenia rizík

Kvalitatívne metódy hodnotenia rizík sa v bezpečnostnej praxi používajú častejšie, ako kvantitatívne metódy Údaje o pravdepodobnosti sa nevyjadrujú podľa štatistických údajov, ale na základe expertného hodnotenia vzťahu medzi inými faktormi, ktoré dokážeme slovne popísať. Aj na vyjadrenie početnosti alebo dôsledkov sa použije slovný popis, ktorý obsahuje deskripciu hodnoty faktoru podľa názorov expertných posudzovateľov. Kvalitatívne metódy vyjadrenia veličín v procese analýzy rizík sa od kvantitatívnych metód odlišujú tým, že sú založené na verbálnom vyjadrení, ktoré môže byť transformované na vyjadrenie v číslach. Riziká sa vyjadrujú hlavne na základe expertných hodnotení v určitom rozsahu:

- počtom bodov (1-10),
- pravdepodobnosťou (0-1),
- slovne (malé, stredné, veľké).

Kvalitatívne metódy analýzy rizika špecifikujú, čo môže spôsobiť poruchu bezpečnostného systému, aké sú príčiny porúch a havárií jednotlivých zariadení, aké sú ich dôsledky, iba v kombinácii s vhodnými výpočtovými metódami kvantitatívnej analýzy a pomerové vyjadrenie rizika s bezpečnostnými štandardami.

Kvalitatívne metódy analyzujú logické štruktúry poruchových stavov a identifikujú zdroje rizík v chránenom systéme. Pri analýze rizika sa používajú metódy:

Revízia bezpečnosti (Safety Review) – postup využíva prevádzkovú dokumentáciu a smernice pre činnosť zariadení informačného systému ako i spoluprácu s personálom na posúdenie zhody s požiadavkami noriem a predpisov, tiež identifikáciu ohrození v zariadeniach, procesoch,

prevádzkových a údržbových postupoch. Revízia bezpečnosti je spoločným úsilím, zameraným na skvalitnenie celkovej bezpečnosti prevádzky. Na záver revízie sú navrhované konkrétne opatrenia so zdôvodnením, určená zodpovednosť za plnenie konkrétnych opatrení, vrátane termínov.

Analýza pomocou kontrolných zoznamov (Check list analysis) – využíva písomný zoznam položiek a krokov podľa ktorých sa overuje stav systému. Je zameraná na identifikáciu rôznych druhov ohrozenia a nesúladu od štandardného projektovaného stavu a identifikáciu možných nehodových situácií spojených so vstupmi hmotnými i nehmotnými, technologickým vybavením, technologických postupov a riadením procesu spracúvania údajov, predovšetkým na kontrolu súladu procesu s platnými zákonmi a normami.

Analýza Čo-keby? (What – If Analysis – Wl) – je interaktívnou metódou, ktorá pomocou brainstormingu kontroluje spracovateľské zariadenia a postupy. Možno tak hodnotiť budovy, energetické zdroje, vstupné produkty, manipuláciu s materiálmi, praktické aspekty spracúvania osobných údajov, bezpečnosť. Princípom je tímová práca odborníkov, ktorí kladú tematicky vopred zamerané otázky typu „Čo by sa stalo keby? A sledujú celý proces odpovedí. Položené otázky sa zapisujú a triedia podľa oblastí, ktoré analyzujú špecialisti v danom odbore v spolupráci s pracovníkmi prevádzok. Výsledky sú značne závislé na skúsenostiach vedúceho a pracovníkov tímu a tým malej systematickosti, čo môže viesť k nezisteniu niektorých rizík. Na základe identifikácie rizík možno stanoviť predpokladané následky a posúdiť existenciu ochranných a zabezpečujúcich opatrení na zníženie rizika.

Analýza Čo keby v kombinácii s Kontrolným zoznamom (What – If/Check list analysis) kompenzuje nedostatky oboch uvedených metód, je značne závislá na skúsenostiach spracovateľov kontrolných zoznamov. Je využívaná k analýze bežných ohrození, ktoré sa môžu v procesoch vyskytovať. Identifikuje ohrozenia pri zvažovaní všeobecných typov havárií, ktoré môžu nastať v procese spracúvania osobných údajov, zhodnotiť kvalitatívne účinky týchto havárií a určiť či sú ochranné opatrenia proti možným havarijným situáciám zodpovedajúce návrhom spôsobov zníženia rizika. Výstupom analýzy je vyplnený kontrolný zoznam a popis zistených rizík, ochranných opatrení a návrhov.

DELFI (riadený kontakt medzi expertmi hodnotiacej skupiny a zástupcami hodnoteného subjektu),

Bodové hodnotenie

Brainstorming.

Metódy kvalitatívnej analýzy hodnotenia rizík sú jednoduchšie, rýchlejšie, ale subjektívnejšie, ich rozsah je stanovený v prevažnej väčšine prípadov kvalifikovaným odhadom, neumožňujú dostatočnú kontrolu efektívnosti vynaložených nákladov,

Účelnou a prehľadnou formou spracovania analýzy rizík je vyhotovenie vo forme tabuľky.

Legenda k tabuľke:

1 - strata
2 - nedostupnosť
3 - dôvernosť
4 - integrita
5 - autentickosť

Tab.8.4: Prehľadná forma analýzy rizík

AKTÍVUM	SÚČASŤ	IDENTIFIKÁCIA A ŠPECIFIKÁCIA RIZIKA	VPLYV RIZIKA				
			1	2	3	4	5
Papierové dokumenty	dokumenty krízového plánovania, výkazy, rukou písané zoznamy hesiel...	strata, odcudzenie, zabudnutie	x	x	x	x	x
		úmyselné zničenie	x				
		neúmyselné zničenie (vrátane prír. živlov, požiaru)	x				
		vyhotovenie neoprávnených kópií			x	x	x
		poškodenie dokumentu	x				
		modifikácia údajov neoprávneným spôsobom			x	x	x
Kľúčový	zámok vo dverách	poškodenie zámku		x			
systém		dočasné vyradenie z funkcie		x			
		neúmyselné neoznámenia výmeny		x			
		úmyselná výmena zámku		x			
		prekonanie odporu zámku, vlámanie		x	x	x	x
	kľúč	strata	x	x			
		neoprávnené poskytnutie neoprávnenej osobe	x		x		
		zničenie kľúča, pričom oprávnená osoba o tom vie	x				
		neoprávnené vytvorenie kópie			x		x
		strata funkčnosti, zaseknutie sa		x			
Technické zabezpečovacie systémy	riadiaca jednotka	strata funkčnosti		x			
		neodborná manipulácia		x			
		úmyselné vyradenie z činnosti		x			
		neúmyselné vyradenie z činnosti		x			

		prerušenie dodávky el. energie poruchou pri vedení		x			
		prekonanie, vyradenie z činnosti špeciálnymi prostriedkami		x	x	x	x
	senzory	strata funkčnosti		x			
		prekonanie, vyradenie z činnosti špeciálnymi prostriedkami		x	x	x	x
Vyššia moc	prírodné živly	poškodenie stavby, zatopenie, požiar, vietor	x				
		poškodenie tech. prostriedkov a SW vybavenia bleskom	x				
	neoprávnené príkazy	strach pred neuposlúchnutím príjazdu nadriadeného	x	x	x	x	x
		vydieranie	x	x	x	x	x
		manipulácia	x	x	x	x	x
Poverení pracovníci	neprítomnosť	krátkodobý výpadok, choroba ...		x			
		dlhodobý výpadok		x			
		strata vedomostí o heslách po odchode pracovníka /aj úmrtie/		x			
		vedomá zmena hesiel odchádzajúcim pracovníkom		x			
	nespôsobilosť	duševná alebo iná trauma nespôsobilosť vinou závislosti		x			
		vydieranie, hrozba	x	x	x	x	x
		strata bezúhonnosti a dôveryhodnosti	x	x	x	x	x
Návštevy	vyťažovanie	odcudzenie vecných súčastí a písomností	x	x	x	x	x
		vyhotovenie neoprávnených kópií			x	x	x
		zisťovanie údajov od oprávnených osôb, prečítanie informácií			x	x	x
		skrytá inštalácia tech. prostriedkov prieskumu			x	x	x
	modifikácia	úprava tech. prostriedkov, údajov, konfigurácií, hesiel ...			x	x	x
	poškodenie	úmyselné alebo nie úmyselné	x	x			

Vyjadrenie pravdepodobnosti

Najproblematickejšie z celého procesu hodnotenia rizika je vyjadrenie jeho pravdepodobnosti. Pre potreby bezpečnostného manažérstva použijeme model, ktorý umožňuje vyjadriť pravdepodobnosť vzniku neželanej negatívnej udalosti (vlámanie, lúpežné prepadnutie ap.) na základe týchto faktorov :

- **hodnota chráneného záujmu,** ktorú môžeme slovne popísať nasledujúcim spôsobom:
    - malá,
    - nie malá,
    - veľká,
    - veľmi veľká,

  pričom zaradenie chráneného záujmu do príslušnej kategórie bude závisieť od hodnotiteľa
- **zraniteľnosť** objektu ochrany (chráneného záujmu), ktorá zahŕňa slabiny v ochrane objektu, spôsobuje výhodné podmienky pre napadnutie objektu, zvyšuje pravdepodobnosť útoku a úspechu potenciálneho páchateľa. Zraniteľnosť môže byť ohodnotená ako:
    - malá,
    - stredná,
    - veľká,
- **úroveň ochranných protiopatrení**, ktoré sú aplikované na chránenom objekte a predstavujú reakciu na zraniteľnosť objektu a potenciálne ohrozenie objektu. Úroveň ochranných opatrení môže byť ohodnotená ako:
    - veľmi účinné,
    - účinné,
    - neúčinné.

Výsledná pravdepodobnosť vzniku neželanej negatívnej udalosti je priamo úmerná veľkosti zraniteľnosti chráneného objektu a nepriamo úmerná veľkosti a kvalite protiopatrení. Na vyjadrenie pravdepodobnosti použijeme nasledujúcu tabuľku :

Tabuľka 8.5: Vyjadrenie pravdepodobnosti rizika kvalitatívnou metódou (Reitšpís a kol. 2004)

Hodnota chráneného záujmu	**Protiopatrenia**								
	veľmi účinné			účinné			neúčinné		
	Zraniteľnosť								
	malá	stredná	veľká	malá	stredná	veľká	malá	stredná	veľká
Malá	0	1	2	1	2	3	2	3	4
Nie malá	1	2	3	2	3	4	3	4	5
Veľká	2	3	4	3	4	5	4	5	6
Veľmi Veľká	3	4	5	4	5	6	5	6	7

Číslice z číselného radu (0,...,7) znamenajú tieto hodnoty pravdepodobnosti:

Tabuľka 8.6: Tabuľka hodnoty pravdepodobností (Reitšpís a kol. 2004)

0	1	2	3	4	5	6	7
úplne vylúčené	takmer vylúčené	veľmi nepravde-podobné	nepravde-podobné	pravdepo-dobné	veľmi pravdepo-dobné	takmer možné	celko m isté

Takéto pravdepodobnostné ohodnotenie jednotlivých udalostí využíva ***subjektívnu pravdepodobnosť,*** ktorá vyjadruje mieru osobného presvedčenia o výskyte posudzovaného javu (udalosti) v závislosti od definovaných faktorov. Slovná deskripcia pravdepodobnosti je pre väčšinu užívateľov zrozumiteľnejšia a intuitívne prijateľnejšia. Medzi číselnými hodnotami a slovným popisom existuje vzájomná korešpondencia, ktorá však nie je záväznou normou a každý užívateľ ju môže interpretovať podľa vlastných preferencií.

Vyjadrenie početnosti

Okrem numerického vyjadrenia početnosti rizika je možné aj slovné vyjadrenie početnosti. Príklad takého vyjadrenia je v tabuľke :

Tabuľka 8.7: Vyjadrenie početnosti rizika (Reitšpís a kol. 2004)

Početnosť	**Frekvencia vzniku**	**Časové pôsobenie**
Veľmi vysoká	vzniká veľmi často	nepretržité
Vysoká	niekoľkokrát	časté
Stredná	niekedy	zriedkavé
Nízka	málo možné	veľmi zriedkavé
Veľmi nízka	vylúčená	skoro nemožné

Vyjadrenie dôsledkov

Dôsledky bezpečnostného rizika sa môžu vyjadriť ako :

- majetková alebo nemajetková ujma,
- humánne škody a straty,
- negatívne dopady na životné prostredie.

Komplexné vyjadrenie rizika

Na komplexné vyjadrenie rizika (Hofreiter 2003) môžeme podobne ako na vyjadrenie pravdepodobnosti použiť tabuľku. Veľkosť rizika sa na základe ich slovného ohodnotenia zapisujú do polí tabuľky, ktoré zodpovedajú priesečníku ich pravdepodobnosti a predpokladanému dôsledku. Príklady slovného vyjadrenia pravdepodobnosti (početnosti) sú uvedené v tabuľkách 9.4 a 9.5,

dôsledky môžu byť vyjadrené vo forme slovných vyjadrení, napr. podľa tabuľky 9.6, alebo, ako napr. katastrofálne, veľmi veľké, veľké a pod.

Na slovné ohodnotenie bezpečnostného rizika bude použitá nasledujúca stupnica:

- zanedbateľné (Z),
- malé (M),
- stredné (S),
- veľké (V),
- veľmi veľké (VV).

Potom bude tabuľka hodnotenia bezpečnostného rizika v tvare:

Tabuľka 8.8: Vyjadrenie veľkosti rizika

pravdepodobnosť							
7	Z	M	S	V	VV	VV
6	Z	M	S	V	VV	VV
5	Z	M	S	V	V	VV
4	Z	M	M	V	V	V
3	Z	M	M	S	S	V
2	Z	M	M	S	S	S
1	Z	Z	M	S	M	S
0	Z	Z	M	M	M	S
Dôsledky	nepatrné	nie nepatrné	nie malé	veľké	značné	veľkého rozsahu

Ďalšími kritériami na kvalitatívne hodnotenie rizík môžu byť :

1. **Akceptovateľnosť rizika**. Pre subjekt bezpečnosti (občana, firmu ap.) bude akceptovateľné také riziko, ktoré mu nespôsobí majetkovú či nemajetkovú ujmu, nedôjde k zmenšeniu jeho existujúceho majetku ani k narušeniu suverenity jeho obydlia či integrity jeho osobnosti. V tomto prípade bude pre ohodnotenie akceptovateľnosti rizika rozhodujúca veľkosť ujmy, ktorú je subjekt ochotný znášať. Potom môže byť tabuľka hodnotenia rizika v tvare:

Tabuľka 8.9: Vyjadrenie akceptovateľnosti bezpečnostného rizika (Reitšpís a kol. 2004)

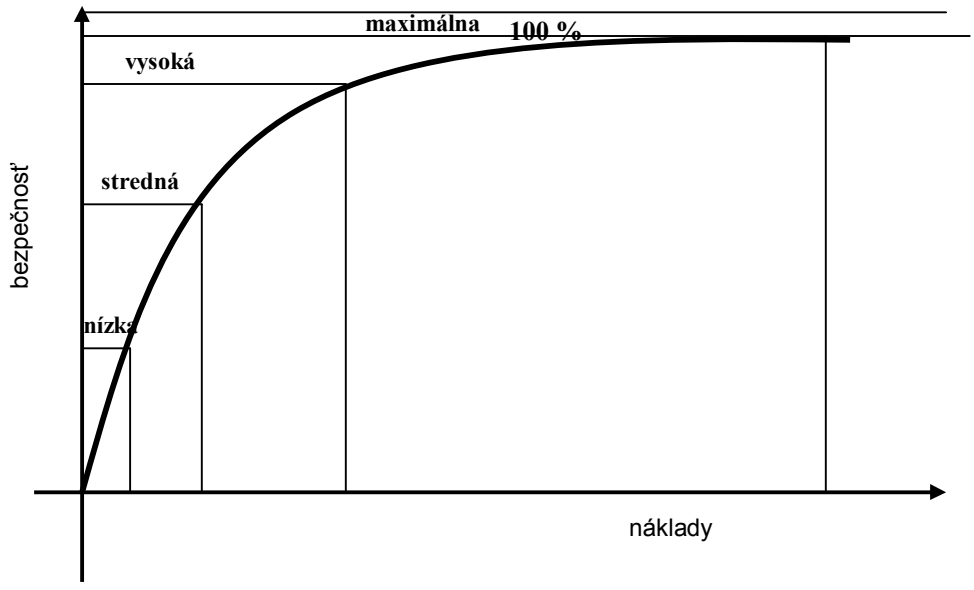
pravdepodobnosť						
7	A	A	N	N	N	N
6	A	A	N	N	N	N
5	A	A	N	N	N	N
4	A	A	N	N	N	N
3	A	A	A	N	N	N
2	A	A	A	N	N	N
1	A	A	A	N	N	N

0	A	A	A	N	N	N
Dôsledky	nepatrné	nie nepatrné	nie malé	veľké	značné	veľkého rozsahu

A- akceptovateľné bezpečnostné riziko
N – neakceptovateľné bezpečnostné riziko

2. **Ovplyvniteľnosť rizika**. Pri hodnotení rizík sa berie do úvahy jeho ovplyvniteľnosť. Zo štruktúry prvkov, ktorými definujeme riziko je zrejmé, že môžeme posudzovať ovplyvniteľnosť jeho pravdepodobnostnej, alebo dôsledkovej zložky. Pritom sa musí vychádzať z charakteru rizika a rozhodnúť, ktorá zložka je ovplyvniteľná a v akom rozsahu.

3. **Náklady na preventívne opatrenia**. Malo by platiť, že náklady na prevenciu (na bezpečnostné a ochranné opatrenia) by mali byť v primeranom pomere k predpokladaným dôsledkom rizika, resp. k hodnote chráneného záujmu. V prípade, ak by výška nákladov na preventívne opatrenia bola neúmerne vysoká a nezabezpečovala by požadovanú efektívnosť plnenia funkcií ochrany, môže byť akceptované aj riziko s relatívne vysokými negatívnymi následkami, ak jeho pravdepodobnosť je nízka.



Obr.8.5: Závislosť prírastku bezpečnosti od zvyšovania nákladov na ochranu (Reitšpís a kol. 2004)

Veľkosť nákladov na zaistenie bezpečnosti chráneného záujmu sa môže porovnávať aj s mierou zaistenia bezpečnosti. V tomto prípade budeme za rozhodujúce považovať veľkosť prírastku bezpečnosti v porovnaní s nákladmi na ochranné opatrenia. Táto závislosť je graficky zobrazená na obr.9.4.

Z grafu na obrázku (8.5) vyplýva, že by po dosiahnutí vysokej bezpečnosti bolo neefektívne zvyšovať náklady na ochranné opatrenia, pretože prírastok bezpečnosti nie je úmerný zvýšeniu nákladov.

8.2.4 Prioritizácia rizík

Určenie správnej a zdôvodnenej priority rizík má veľký význam pre voľbu bezpečnostných a ochranných opatrení, pri navrhovaní bezpečnostnej koncepcie a pri tvorbe stratégie situačnej prevencie. Cieľom prioritizácie rizík je pomocou špecifických kritérií a postupov zoradiť identifikované a ohodnotené riziká v postupnosti podľa ich významnosti (priority).
Ide v podstate o rozhodovací proces, ktorý využíva jedno alebo viacej kritérií na rozhodnutie o priorite konečného počtu identifikovaných a ohodnotených rizík, pričom každé z rizík je popísané minimálne týmito charakteristikami:

- pravdepodobnosťou alebo početnosťou,
- dôsledkami,
- komplexným vyjadrením veľkosti rizika.

Je zrejmé, že pri prioritizácii rizík významnú rolu zohrávajú tieto charakteristiky, ktoré budú slúžiť na porovnávanie či usporiadanie danej množiny rizík.
Z kapitoly o hodnotení rizík vieme, že charakteristiky rizík môžu byť buď kvantitatívne (číselné), alebo kvalitatívne (slovné) deskriptory. Preto na prioritizáciu rizík použijeme metódy, ktoré umožnia rovnocenne pracovať ako s kvantitatívnymi, tak aj s kvalitatívnymi charakteristikami rizík. K takým metódam patria (Lysá 2002) :

- metóda poradia,
- metóda párového porovnania,
- metóda bodového hodnotenia.

8.2.4.1 Metóda poradia

Použitie metódy poradia je jednoduchou metódou určenia priority rizika, ktorá využíva princípy expertného ohodnocovania. Riešenie má tento postup :

1. Každému riziku je expertom priradené poradie podľa jeho dôležitosti (významnosti, nebezpečnosti ap.). Najdôležitejšiemu riziku je priradené

číslo **m**, druhému **m-1** atď. Najmenej dôležité riziko dostáva číslo **0**. Číslo priradené expertom **k** riziku **j** sa označí $\mathbf{w_{kj}}$.

2. Pre každé riziko sa vypočíta súčet čísiel w_j, ktoré mu boli priradené všetkými s expertmi :

$$w_j = \sum_{k=1}^{s} w_{kj} \tag{8.9}$$

kde w_j je súčet všetkých čísiel priradených expertmi riziku j
w_{kj} je číslo priradené expertom k riziku j
s je počet expertov.

3. Vypočítame súčet všetkých čísiel w_j :

$$\sum_{j=1}^{m} w_j = \sum_{j=1}^{m} \sum_{k=1}^{s} w_{kj} \tag{8.10}$$

kde : m je počet rizík

4. Vypočítame váhu v_j každého rizika :

$$v_j = \frac{w_j}{\sum_{j=1}^{m} w_j} = \frac{\sum_{k=1}^{s} w_{kj}}{\sum_{j=1}^{m} \sum_{k=1}^{s} w_{kj}} \tag{8.11}$$

5. Maximálna priorita bude prisúdená tomu riziku, pre ktoré dosiahne jeho váha v_j maximálnu hodnotu.

Príklad použitia metódy je uvedený v tabuľke 8.7.

Tabuľka 8.7: Prioritizácia podľa poradia

Expert	Bezpečnostné riziko R_j			
E_k	R_1	R_2	R_3	R_4
E_1	3	2	1	0
E_2	2	3	0	1
E_3	3	2	0	1
w_j	8	7	1	2
$\Sigma\ w_{kj}$	18			
Váha	0,44	0,38	0,05	0,11
Priorita	1	2	4	3

Z popisu tejto metódy vyplýva, že môže byť použitá bez ohľadu na to, aká metóda bola použitá na ohodnotenie rizík. Veľkosť čísla priradeného danému riziku ja závislá len od intuícii a skúsenosti experta.

Modifikácia metódy poradia môže využívať aj kvantitatívne charakteristiky rizika, ktoré budeme ďalej nazývať kritériá. Ak na prioritizáciu rizík použijeme napr. hodnotu pravdepodobnosti, potom bude tabuľka v nasledujúcom tvare:

Tabuľka 8.8: Prioritizácia podľa jedného kritéria (Reitšpís a kol. 2004)

	Bezpečnostné riziko R_j			
	R_1	R_2	R_3	R_4
Pravdepodobnosť	0,89	0,74	0,56	0,49
Priorita	1	2	3	4

Rovnako môžeme postupovať, ak za kritérium zvolíme napr. početnosť výskytu rizika, jeho dôsledky alebo veľkosť rizika.

8.2.4.2 Metóda párového porovnávania

Metóda párového porovnávania spočíva v určení dôležitosti (význam nosti, nebezpečnosti) rizika postupným porovnávaním každej dvojice rizík. Táto metóda je založená na princípe využitia ordinálnej informácie uloženej v párovom porovnaní dvojíc rizík. Počet všetkých párových porovnaní pre m-prvkovú množinu rizík je :

$$N = \binom{m}{2} = \frac{m.(m-1)}{2} \qquad (8.12)$$

Riziká sa zapisujú v tzv. Fullerovom trojuholníku. Schéma Fullerovho trojuholníka je založená na zápise dvojíc porovnávaných rizík do dvoch riadkov pod seba pre jednoduchosť očíslované 1,2,...m. Riziká pritom nemusia byť usporiadané podľa dôležitosti. V prvom z dvojice riadkov je vždy zapísané číslo rizika, podľa ktorého robíme porovnávanie, v druhom riadku sú vždy riziká s vyšším číselným označením. Schematicky môžeme znázorniť Fullerov trojuholník nasledovne :

$$\begin{array}{cccccc} 1 & 1 & 1 & \ldots & 1 \\ 2 & 3 & 4 & \ldots & m \\ & 2 & 2 & \ldots & 2 \\ & 3 & 4 & \ldots & m \end{array}$$

$$\begin{array}{c} m-1 \\ m \end{array}$$

Začína sa prvým dvojriadkom tak, že dôležitosť rizika 1 porovnávame s rizikom 2 a číslo rizika, ktoré sa považuje za dôležitejšie sa označí, napr. podčiarknutím. Obdobne sa porovnáva s rizikom 3 až do konca dvojriadku. Každý ďalší dvojriadok je o jedno číslo kratší.
Pri vyhodnocovaní sa postupuje tak, že sa spočítajú označené hodnoty a zapíšu sa k príslušnému riziku. Najvyššiu prioritu bude mať to riziko, ktoré bolo najčastejšie označené ako dôležitejšie.

Príklad:
Budeme porovnať napr. šesť rizík. Vytvoríme Fullerov trojuholník a označíme v ňom výsledky porovnávania:

$$\begin{array}{ccccc} \underline{1} & 1 & \underline{1} & \underline{1} & 1 \\ 2 & \underline{3} & 4 & 5 & \underline{6} \\ & 2 & 2 & \underline{2} & \underline{2} \\ & \underline{3} & \underline{4} & 5 & 6 \\ & & \underline{3} & \underline{3} & \underline{3} \\ & & 4 & 5 & 6 \\ & & & \underline{4} & 4 \\ & & & 5 & \underline{6} \\ & & & & \underline{5} \\ & & & & 6 \end{array}$$

Tab. 8.9: Vyhodnotenie (Reitšpís a kol. 2004)

Riziko	R_1	R_2	R_3	R_4	R_5	R_6
Počet priorít	3	2	5	2	1	2
Výsledné priority	2	3-5	1	3-5	6	3-5

Z tohto príkladu vyplýva, že najvyššiu prioritu má riziko R_3 a najmenšiu prioritu má riziko R_5.
Nevýhodou tejto metódy je, že síce kvantifikuje počet priorít rizika, ale nevyjadruje intenzitu rozdielu porovnávaných rizík.

Tento nedostatok môže byť odstránený použitím porovnania intenzity kvalitatívnych rozdielov dôležitosti (významnosti) dvojice porovnávaných rizík).* Výsledok párového porovnávania sa zaznamená v tabuľke.

Tabuľka 8.10 : Vyhodnotenie párového porovnávania pomocou hodnotiacich stupňov (Reitšpís a kol. 2004)

	R_1	R_2	R_3	R_4	R_5	R_6
w_j	4,3	8,625	21	9,54	3,9	11,3
Σw_j	58,64					
v_j	0,073	0,14	0,36	0,16	0,066	0,19
priorita	5	4	1	3	6	2

Legenda k tabuľke :

v_j je váhový koeficient rizika R_j,

w_j je súčet čísiel hodnotiaceho stupňa podľa výsledkov párového porovnania pre riziko R_j,

Σw_j je súčet súčtov všetkých čísiel hodnotiacich stupňov,

Najvyššiu prioritu bude mať to riziko, ktoré bude mať najvyššiu hodnotu čísla váhy v_j.

Z výsledkov použitia tejto metódy je zrejmé, že lepšie odstraňuje neurčitosť výsledkov porovnávania, čo vyplýva aj z rozdielov poradia rizík. Aj keď zostáva prioritné riziko R_3, v porovnaní s prvým variantom metódy párového porovnávania presnejšie je určená priorita rizík R_2, R_4 a R_6 a priorita rizika R_1 sa zmenila.

8.2.4.3 Metóda bodového ohodnotenia

Metóda bodového ohodnotenia je spôsob expertného ohodnotenia priority rizík, pri ktorom sa jednotlivým rizikám priraďuje určitá bodová hodnota, ktorá vyjadruje poradie ich významu (dôležitosti) podľa zvolených kritérií. Použitie metódy bodového ohodnotenia na účely prioritizácie rizík vhodné vtedy, ak sme použili kvalitatívne metódy ohodnotenia rizík.

Postup pri použití metódy je nasledujúci:

1. Stanovíme kritériá na porovnávanie rizík K_1, ...K_s.
2. Každému kritériu stanovíme váhový koeficient zo zvoleného intervalu, napr. $\langle 1,5 \rangle$.
3. Každé riziko bodovo ohodnotíme číslom zo zvoleného intervalu, napr. $\langle 1,10 \rangle$, pričom číslo 1 znamená najmenej a číslo 10 najviac.
4. Bodové ohodnotenie rizika vynásobíme váhovým koeficientom.

* viď. Reitšpís, Mesároš, a kol. Manažérstvo bezpečnostných rizík, Žilina 2004

5. Najvyššiu prioritu bude mať to riziko, ktorého súčin bodového ohodnotenia a váhového koeficientu bude najvyšší.

Príklad použitia metódy bodového ohodnotenia je uvedený v tabuľke 9.11

Na zvýšenie objektivity by sa bodového ohodnocovania malo zúčastniť viacej odborníkov. Celkový počet bodov pre dané riziko sa potom vypočíta podľa vzorca :

$$b(R_j) = \frac{\sum_{k=1}^{s} b_{jk}}{k} \qquad (8.13)$$

kde : $b(R_j)$ je počet bodov rizika R_j
b_{jk} je celkový počet bodov rizika R_j od k expertov,
k je počet expertov.

Tabuľka 8.11: Stanovenie priority rizík metódou bodového ohodnotenia (Reitšpís a kol. 2004)

Kritérium	Váhový koeficient	R_1	R_2	R_3	R_4	R_5	R_6
K_1	2	10 20	7 14	5 10	6 12	1 2	4 8
K_2	3	8 24	9 27	6 18	3 9	7 21	4 8
K_3	1	6 6	8 8	3 3	5 5	4 4	2 2
K_4	4	9 36	7 28	10 40	5 20	4 16	6 24
Počet bodov		86	77	71	46	43	42
Priorita		1	2	3	4	5	6

Ďalší spôsob použitia metódy bodového ohodnotenia spočíva v bodovom ohodnotení zvolených kritérií, napr. početnosti výskytu rizika a jeho dôsledkov. Výsledné bodové ohodnotenie rizika je vyjadrené súčinom bodov zvolených kritérií. Najvyššiu prioritu má to riziko, ktorého bodové ohodnotenie je najvyššie.
Na bodové ohodnotenie kritérií použijeme polokvantitatívnu metódu. Príklad je uvedený v tabuľke 8.12, kde je uvedený príklad pre bodové ohodnotenie rizík a stanovenie ich priority .

Tabuľka 8.14 Bodové ohodnotenie kritérií (Reitšpís a kol. 2004)

Kritérium	Ohodnotenie					
Početnosť	veľmi nízka	nízka	stredná	vysoká	veľmi vysoká	
	1	2	3	4	5	
Dôsledky	nepatrné	nie nepatrné	nie malé	väčšie	značné	veľkého rozsahu
	1	2	3	5	7	10

Tabuľka 8.15 Prioritizácia rizík použitím bodového ohodnotenia kritérií (Reitšpís a kol. 2004)

Bezpečnostné riziko	Početnosť	Dôsledky	Body	Priorita
R_1	1	3	3	3
R_2	3	3	9	2
R_3	4	5	20	1

Výhodou použitia tejto metódy spočíva v tom, že nemusíme poznať pravdepodobnosti výskytu rizík a postačuje nám len ich kvalitatívne ohodnotenie .

Prioritizácia rizík, aj keď je v postupnosti činností pri analýze rizík poslednou, má veľký význam pre rozhodovanie bezpečnostných manažérov o variante bezpečnostného systému. Poznanie dôležitosti, významnosti alebo nebezpečnosti identifikovaných rizík umožní kvalifikovane rozhodnúť o tom, ktoré riziká musia byť eliminované, ktoré stačí znížiť a ktoré je možné akceptovať. Tým bude realizovaný princíp rozumnej dostatočnosti a vytvorený bezpečnostný systém bude dostatočne efektívny.

9 DOKUMENTÁCIA V ČINNOSTI BEZPEČNOSTNÉHO MANAŽÉRA

Na riadenie činnosti bezpečnostného systému pri predchádzaní bezpečnostným incidentom a jeho reakcie v prípade ich reálneho prejavu sa v závislosti na charaktere, dôležitosti či význame chráneného záujmu sa vypracúva potrebná dokumentácia. Uvedená dokumentácia predstavuje súhrn textových a grafických dokumentov, ktoré slúžia na riadenie fyzickej a objektovej bezpečnosti objektov a chránených priestorov. Jej obsah je závislý od kategórie objektu a chráneného priestoru . (Hofreiter, Križovský 2007)

*Z hľadiska **formy** môžeme dokumentáciu rozdeliť na :*

a) **textovú dokumentáciu**, ku ktorej patria všetky dokumenty spracované vo forme textu,
b) **grafickú dokumentáciu,** ku ktorej patria všetky dokumenty spracované vo forme grafických plánov, nákresov a pod.

*Z hľadiska **určenia** môžeme dokumentáciu rozdeliť na :*

a) **analytickú dokumentáciu,** ku ktorej budú patriť dokumenty vzťahujúce sa k bezpečnostným analýzam, , analýze rizík a pod.,
b) **dokumentácia pre riadenie,** ku ktorej budú patriť všetky plány ochrany, prevádzkové poriadky, pravidlá pre výkon fyzickej ochrany a pod.,
c) **pomocná dokumentácia,** ku ktorej bude patriť napr. technická dokumentácia objektu, knihy odovzdania a prevzatia služby, záznamy o vstupe, knihy vjazdu/výjazdu vozidiel ,. zoznamy dokumentácie a pod.,
d) **výkazová dokumentácia,** ktorá bude zahrňovať napr. časť technickej dokumentácie (záznamy z vykonaných kontrol), knihy kontrol a pod.

Dokumentácia pre činnosť a riadenie bezpečnostného systému sa kontroluje a aktualizuje po každej zmene, ktorá by mohla mať vplyv na jej obsah, napr.

- zmena kategórie objektu (chráneného priestoru),
- zmena použitých zabezpečovacích prostriedkov (mechanické, technické..),
- zmeny v štruktúre objektu (priestoru) a pod.,
- pri podozrení z prezradenia systému ochrany alebo po jeho vážnom narušení,
- po vykonaných previerkach alebo nácvikoch systému ochrany, ktoré preukázali vážne nedostatky ,

Dokumentácia sa spracuje tak, aby bola jasná, stručná.

Spracovateľ dokumentácie (bezpečnostný pracovník, resp. bezpečnostný manažér) zodpovedá:

- za zhodu bezpečnostnej dokumentácie so skutočným stavom,
- za jej pravidelnú aktualizáciu,
- za oboznámenie ostatných zamestnancov s bezpečnostnou dokumentáciou v rozsahu nutnom na výkon ich povinností alebo úloh,
- za aktualizáciu bezpečnostnej dokumentácie, ak došlo ku zmenám, ktoré majú vplyv na jej obsah,
- za vedenie knihy kontrol a realizáciu opatrení vyplývajúcich z kontroly bezpečnostnej dokumentácie a a kontroly opatrení fyzickej bezpečnosti a objektovej bezpečnosti.

Bezpečnostná dokumentácia sa vzťahuje k k jednotlivým oblastiam činnosti bezpečnostného manažéra, resp. oblastiam chránených záujmov. Ide najmä o ochranu osôb, ochranu objektov, ochranu majetku, ochranu obchodného tajomstva, ochranu osobných údajov, ochranu utajovaných skutočností, prípadne oblasti ochrany iných záujmov.

9.1 Bezpečnostný projekt ochrany objektu

Bezpečnostný projekt ochrany objektu môže obsahovať tieto časti :

a) umiestnenie a opis objektu, a to najmä opis hranice objektu , počtu vstupov, opis okolia objektu, budov, príp. počet budov alebo podlaží, ak sa objekt skladá z viacerých budov alebo podlaží,
b) určenie kategórie a triedy chránených priestorov, ktoré sa v objekte nachádzajú, spolu s opisom činností, ktoré sa v nich budú vykonávať,
c) určenie hranice objektu a chráneného priestoru vrátane opisu jej umiestnenia, vstupov, hrúbky stien, rozmerov okien, výšky okien nad úrovňou terénu ap.
d) grafické zobrazenie objektu, hranice objektu, chránený priestor a hranice chráneného priestoru,
e) bezpečnostné opatrenia (smernice)

Umiestnenie a opis objektu:

Účelom tejto časti projektu je identifikovať, lokalizovať objekt v urbanistickom prostredí. V bezpečnostnom projekte ochrany objektu sa uvedie:
- názov inštitúcie (spoločnosti, prevádzky, výrobného alebo skladového objektu),
- ulica, číslo popisné, resp. orientačné,
- obec

- typ objektu podľa :
    - určenia,
    - štruktúry,
    - vyhotovenia a pod.,

Opis hranice objektu

Hranicou objektu sa rozumie najmä plášť budovy, oplotenie alebo iné vymedzenie priestoru; hranica objektu môže byť zhodná s hranicou chráneného priestoru.

Hranicu objektu (chráneného priestoru) môžu tvoriť :
- plášť budovy (obvodové múry),
- oplotenie (priehľadné, nepriehľadné),
- bariéry (prenosné, neprenosné – stále),
- mreže,
- závory,
- administratívne vymedzenie, napr. výstražnými tabuľami,
- iné spôsoby, ktorými sa viditeľné vymedzí hranica, za ktorou platia ochranné opatrenia (nemá byť prekročená nepovolanou osobou), prípadne kombinácia predchádzajúcich spôsobov.

Opis vstupov

Za **vstupy** do objektov (chránených priestorov) sa môžu považovať :
- brány v oplotení,
- priechody,
- dvere, (dvere v perimetri objektu),
- úseky v teréne a pod.

Za ďalšie otvory, ktoré môžu byť použité na prienik do objektu (chráneného priestoru) sa môžu považovať :

- okná ,
- strešné okná,
- vetracie šachty,
- káblové šachty,
- parovody,
- kanalizácia,
- technické otvory,
- technologické kolektory a pod.

Popis okolia objektu

Pri popise okolia objektu sa zohľadní najmä:

- prehľadnosť okolia,
- prístupové cesty k objektu
- možnosť kontroly prístupových ciest,
- výskyt zdrojov ohrození ap.

Určenie hranice objektu a chráneného priestoru vrátane opisu jej umiestnenia, vstupov, hrúbky stien, rozmerov okien, výšky okien nad úrovňou terénu ap.

V bezpečnostnom projekte ochrany objektu sa uvedie spôsob vymedzenia hranice objektu a/alebo popis úseku terénu, ktorým prechádza (v ktorom je situovaná).
Pri popise hranice chráneného priestoru sa uvedie jeho umiestnenie v objekte a ktoré prvky (stavebné alebo iné) vymedzujú jeho polohu v objekte. (Hofreiter, Križovský, 2007)

Určia sa vstupy, ktoré budú využívané pre vstupy osôb a vjazdy motorových vozidiel.

Popis hrúbky stien má význam pre posudzovanie prielomovej odolnosti stien, ako základných stavebných prvkov objektov. Podklady pre spracovanie tejto časti je možné čerpať zo stavebnej dokumentácie objektu.

Okná sú súčasťou otvorových výplní objektu (chráneného priestoru). Z hľadiska požiadaviek zaistenia fyzickej bezpečnosti a objektovej bezpečnosti sa popisuje:

- počet a rozmiestnenia okien v plášti objektu,
- ich veľkosť (rozmery),
- výška spodného okraja k okolitému terénu,

Z hľadiska požiadaviek bezpečnostných štandardov sa posudzujú všetky okná (otvory) , ktoré majú väčšie rozmery, ako sú uvedené v tabuľke:

Tabuľka 10.1

Tvar otvoru :	**Rozmer :**
Obdĺžnik	400 mm x 250 mm
Elipsa	400 mm x 300 mm
Kruh	priemer 350 mm

Pre posudzovanie nutnosti použitia zabezpečovacích prostriedkov sa posudzujú všetky okná, ktorých spodný okraj je nižšie ako 5,5 m k úrovni okolitého terénu,

alebo je možný prístup zo strechy, balkónu (vlastného alebo susedného objektu), odkvapových rúr, hromozvodov a pod.

Grafické zobrazenie objektu, hranice objektu, chráneného priestoru a hranice chráneného priestoru

Grafické zobrazenie objektu je dokumentom, v ktorom sa vizualizuje systém opatrení použitých na ochranu objektu a chráneného priestoru. V grafickom zobrazení sa môže v príslušnom merítku zakresľovať :

- relevantné okolie objektu (ak má vplyv na bezpečnosť chráneného objektu),
- objekt (objekty), jeho (ich) hranice s označením prielomovej odolnosti, príp. bezpečnostnej triedy (ak je definovaná),
- chránený priestor a jeho hranice (s označením prielomovej odolnosti, resp. bezpečnostnej triedy). Ak je chránený priestor umiestnený vo vnútri objektu, zakreslí sa jeho poloha v objekte,
- vstupy do objektu (chráneného priestoru), vrátane núdzových východov a iných prielezných (priestupných) otvorov,
- rozmiestnenie mechanických zábranných prostriedkov použitých na:
    - perimetrickú ochranu,
    - otvorové výplne,
- rozmiestnenie bezpečnostných úschovných objektov,
- rozmiestnenie technických zabezpečovacích prostriedkov použitých na :
    - ochranu (stráženie) vstupov do objektu (chráneného priestoru), napr. detektory kovov, systémy kontroly vstupu a pod.
    - perimetrickú ochranu (CCTV systémy, a pod.),
    - plášťovú ochranu (detektory, snímače , kontakty a pod.),
    - priestorovú ochranu (detektory pohybu),
    - predmetovú ochranu,
    - elektrickú požiarnu signalizáciu,
    - vyústenie poplachovej signalizácie (na objekte, na SRP, na stále stanovište fyzickej ochrany,...)
    - kontrolu výkonu strážnej služby (tlačidlá, čítačky,) a iné.

- schéma stanovíšť a trás obchôdzok fyzickej ochrany (pre objekty kategórie „T“ a „PT“ povinné) , pričom sa zakreslia :
    - stanovište stálej služby fyzickej ochrany,
    - systém stálych kontrolných stanovíšť (pri vstupoch/výstupoch a pod),
    - trasy hliadkovania (obchôdzok) variantne v pracovnej dobe, v mimopracovnej dobe, cez deň, v noci, za zhoršenej viditeľnosti a pod.,
    - priestory, do ktorých majú príslušníci fyzickej ochrany zakázaný vstup.

Grafický plán ochrany objektu je vhodné doplniť tabuľkou (napr. v spodnej časti plánu), v ktorej sa uvedú údaje :
- kategória objektu,
- počet vstupov do objektu,
- počet chránených priestorov a ich kategória,
- počet vstupov do chránených priestorov.

Na vypracovanie grafického plánu ochrany sa ako podklad môže použiť stavebná dokumentácia objektu. Na zakreslenie rozmiestnenia použitých mechanických zabezpečovacích prostriedkov (MZP), technických zabezpečovacích prostriedkov (TZP) a systému fyzickej ochrany (FO) sa použijú situačné značky.

V oblasti **ochrany osobných údajov** bezpečnostný projekt vymedzuje rozsah a spôsob technických, organizačných a personálnych opatrení potrebných na eliminovanie a minimalizovanie hrozieb a rizík pôsobiacich na informačný systém z hľadiska narušenia jeho bezpečnosti, spoľahlivosti a funkčnosti.
Bezpečnostný projekt sa spracúva v súlade so základnými pravidlami bezpečnosti informačného systému vydanými bezpečnostnými štandardmi, a právnymi predpismi. Bezpečnostný projekt obsahuje najmä:
a) bezpečnostný zámer,
b) analýzu bezpečnosti informačného systému,
c) bezpečnostné smernice.

Bezpečnostný zámer vymedzuje základné bezpečnostné ciele, ktoré je potrebné dosiahnuť na ochranu informačného systému pred ohrozením jeho bezpečnosti, a obsahuje najmä:
a) formuláciu základných bezpečnostných cieľov a minimálne požadovaných bezpečnostných opatrení,
b) špecifikáciu technických, organizačných a personálnych opatrení na zabezpečenie ochrany osobných údajov v informačnom systéme a spôsob ich využitia,
c) vymedzenie okolia informačného systému a jeho vzťah k možnému narušeniu bezpečnosti,
d) vymedzenie hraníc určujúcich množinu zvyškových rizík.

Analýza bezpečnosti informačného systému je podrobný rozbor stavu bezpečnosti informačného systému, ktorá obsahuje najmä:
a) kvalitatívnu analýzu rizík, v rámci ktorej sa identifikujú hrozby pôsobiace na jednotlivé aktíva informačného systému spôsobilé narušiť jeho bezpečnosť alebo funkčnosť; výsledkom kvalitatívnej analýzy rizík je zoznam hrozieb, ktoré môžu ohroziť dôvernosť, integritu a dostupnosť spracúvaných osobných údajov,

s uvedením rozsahu možného rizika, návrhov opatrení, ktoré eliminujú alebo minimalizujú vplyv rizík, a s vymedzením súpisu nepokrytých rizík,
b) použitie bezpečnostných štandardov a určenie iných metód a prostriedkov ochrany osobných údajov; súčasťou analýzy bezpečnosti informačného systému je posúdenie zhody navrhnutých bezpečnostných opatrení s použitými bezpečnostnými štandardami, metódami a prostriedkami.

Bezpečnostné smernice upresňujú a aplikujú závery vyplývajúce z bezpečnostného projektu na konkrétne podmienky prevádzkovaného informačného systému a obsahujú najmä:
a) popis technických, organizačných a personálnych opatrení vymedzených v bezpečnostnom projekte a ich využitie v konkrétnych podmienkach,
b) rozsah oprávnení a popis povolených činností jednotlivých oprávnených osôb, spôsob ich identifikácie a autentizácie pri prístupe k informačnému systému,
c) rozsah zodpovednosti oprávnených osôb a osoby zodpovednej za dohľad nad ochranou osobných údajov,
d) spôsob, formu a periodicitu výkonu kontrolných činností zameraných na dodržiavanie bezpečnosti informačného systému,
e) postupy pri haváriách, poruchách a iných mimoriadnych situáciách vrátane preventívnych opatrení na zníženie vzniku mimoriadnych situácií a možností efektívnej obnovy stavu pred haváriou.

9.2 Bezpečnostné smernice

9.2.1 Smernica pre ochranu objektu

Smernica pre ochranu objektu môže obsahovať nasledujúce režimové opatrenia :

a) podmienky vstupu osôb a vjazdu dopravných prostriedkov do objektu a chráneného priestoru a podmienky výstupu osôb a výjazdu dopravných prostriedkov z objektu a chráneného priestoru.
b) podmienky pohybu osôb, dopravných prostriedkov v objekte a v chránenom priestore v pracovnom čase a mimopracovnom čase,
c) podmienky používania mobilných telefónov, videokamier,fotoaparátov, audiozáznamových zariadení ap.
d) podmienky a spôsob kontroly objektu a chráneného priestoru po opustení pracoviska zamestnancami
e) ochrana rokovacích miestností,

f) podmienky používania, prideľovania, označovania, úschovy a evidencie originálov a kópií bezpečnostných kľúčov a médií do zámkov a uzamykateľných systémov
g) podmienky používania, prideľovania , úschovy a evidencie kódových nastavení a hesiel používaných na prístup do objektov, CHP a bezpečnostných úschovných objektov,
h) podmienky manipulácie s MZP a TZP a podmienky ich používania,
i) spôsob kontroly dodržiavania týchto opatrení.

Ad a) **Podmienky vstupu osôb a vjazdu dopravných prostriedkov do objektu a chráneného priestoru a podmienky výstupu osôb a výjazdu dopravných prostriedkov z objektu a chráneného priestoru.**

V tejto časti dokumentácie sa odporúča spracovať zásady vstupu a výstupu osôb do objektu a chránených priestorov.

V opatreniach pre vstup/výstup osôb do objektov (chránených priestorov) a vjazdu/výjazdu dopravných prostriedkov sa pri zohľadnení predchádzajúcich zásad vypracujú pravidlá pre vstup/výstup a vjazdu/výjazdu dopravných prostriedkov:
- pre stálych zamestnancov,
- pre zákazníkov, partnerov, dodávateľov,
- pre pracovníkov údržby a upratovacej služby, pričom sa odporúča rozpracovať pravidlá pre pracovnú a mimopracovnú dobu, ako aj pre technicky zabezpečené priestory (rokovacie miestnosti, v ktorých sa prerokúvajú utajované a citlivé informácie).
- pre pracovníkov fyzickej ochrany,
- pre návštevy apod.

V opatreniach sa môže ešte uviesť:
- kategorizácia oprávnení pre vstup do objektov (chránených priestorov), pričom sa zohľadňuje princíp „potrebuje poznať“,
- aký je spôsob preukazovania oprávnenosti vstupu do objektov (chránených priestorov),napr. identifikačné preukazy, magnetické karty, číselné kódy, biometrická identifikácia, alebo ich kombinácia,
- kto a ako zabezpečuje sprievod nepovolaných osôb *(napr. strážna služba, oprávnený zamestnanec*),
- kto je oprávnený povoliť vstup nepovolaných osôb,
- zásady preukazovania oprávnenosti vjazdu/výjazdu dopravných prostriedkov,
- zásady kontroly dovážaného/vyvážaného materiálu,
- miesta vjazdu/výjazdu dopravných vozidiel servisných služieb, dodávateľov a pod.,

- zoznam funkcionárov povoľovať vjazd/výjazd a vyvážanie materiálu
- ako sa zabezpečuje kontrola (záznam) o vstupe a výstupe a ďalšie potrebné pokyny.

Tieto pravidlá sa vypracujú ako pre pracovnú, tak aj pre mimopracovnú dobu.

Ad b) Podmienky pohybu osôb, dopravných prostriedkov v objekte a v chránenom priestore v pracovnom čase a mimopracovnom čase.

V prevádzkovom poriadku objektu sa podľa potreby uvedie :
- podmienky vstupu a pohybu osôb a dopravných prostriedkov v nechránených priestoroch (v administratívnej zóne),
- podmienky pohybu osôb v chránených priestoroch s ohľadom na stupeň oprávnenia,
- opatrenia pre pohyb pracovníkov medzi pracoviskami (napr. čo urobiť pred opustením kancelárie – opatrenia pre zamedzenie neoprávneného prehliadania či prezerania utajovaných skutočností),
- opatrenia pre kontrolu pohybu osôb v rámci chráneného priestoru,
- podmienky pohybu obslužného personálu (údržba, upratovacie služby),
- zásady pohybu vozidiel vo vnútri alebo medzi chránenými priestormi, vymedzenie trás (ciest) pre ich pohyb, systém kontroly pohybu.

Ad c)Podmienky používania mobilných telefónov, videokamier, fotoaparátov, audio-záznamových zariadení ap.

V prevádzkovom poriadku sa uvedie:

- kde sa môžu a a za akých podmienok používať,
- kde sa nemôžu uvedené zariadenia a prístroje používať,
- či je povolené používanie súkromných mobilných telefónov so zabudovanými fotoaparátmi ap.

Ad d) Podmienky a spôsob kontroly objektu a chráneného priestoru po opustení pracoviska zamestnancami

V tejto časti sa uvedie:
- povinnosti zamestnancov pred opustením pracoviska, napr.:
    - kontrola uzatvorenia okien, dverí,
    - zapnutie elektronických zabezpečovacích prostriedkov (EZS),
    - kontrola uloženia médií ap.
- opatrenia na uzamykanie (uzatváranie) priestorov,
- opatrenia pri upratovaní priestorov,
- povinnosti vedúcich zamestnancov a pracovníkov bezpečnostnej služby (vlastnej ochrany) na kontrolu objektov (chránených priestorov) po pracovnej dobe a v dňoch pracovného pokoja,

Ad e) Ochrana rokovacích miestností

V objekte môžu byť, ak si to podmienky vyžadujú, vyčlenené technicky zabezpečené miestnosti, ktoré sú určené na prerokúvanie utajovaných , alebo komerčných či iných citlivých informácií. Takéto miestnosti majú byť zabezpečené proti pasívnemu a aktívnemu odpočúvaniu utajovaných skutočností a proti priamemu pozorovaniu.

Požiadavky:

- miestnosti sa vybavujú akustickými generátormi šumov,
- v miestnostiach s oknami sa musia umiestniť piezoelektrické meniče pripojené na generátor šumu,
- ústia vývodov kanalizácie alebo iné otvory umožňujúce odpočúvanie sa musia zabezpečiť inštaláciou elektroakustických meničov pripojených na generátor šumu,
- rokovacie miestnosti musia mať dostatočnú zvukotesné dvere, steny, podlahy, stropy,
- rokovacie miestnosti musia byť chránené proti priamemu pozorovaniu z vonkajšieho okolia,
- nábytok a zariadenia miestnosti musia byť pred ich umiestnením do rokovacej miestnosti podrobené bezpečnostnej prehliadke, či neobsahujú implantované odpočúvacie zariadenia,
- rokovacie miestnosti musia byť v čase, keď v nich neprebieha rokovanie uzamknuté a kontrolované fyzickou ochranou,
- vstup do rokovacej miestnosti bez sprievodu je povolený len oprávneným osobám,
- kľúče od zámkov rokovacích miestností podliehajú režimu manipulácie s bezpečnostnými kľúčmi,
- rokovacie miestnosti sú pravidelne podrobované technickým bezpečnostným prehliadkam. Bezpečnostné prehliadky sa vykonajú aj po každej rozsiahlejšej rekonštrukcii rokovacej miestnosti (maľovaní, tapetovaní a pod.),
- v odôvodnených prípadoch sa použije vysokofrekvenčná rušička rádiotelefónneho signálu pre mobilných účastníkov blokujúca používanie mobilných telefónov v rokovacej miestnosti a okolí s aktiváciou na čas nevyhnutne potrebný na ochranu utajovaných skutočností.

V dokumentácii sa potom uvedie :

- dislokácia rokovacej miestnosti v chránenom priestore,
- rozsah opatrení na ochranu rokovacej miestnosti, najmä použitých

- mechanických zábranných prostriedkov,
- technických zabezpečovacích prostriedkov,
- režimových opatrení,

- zásady a pravidlá technických bezpečnostných prehliadok.

Ad f) Podmienky používania, prideľovania, označovania, úschovy a evidencie originálov a kópií bezpečnostných kľúčov a médií do zámkov a uzamykateľných systémov

Bezpečnostné kľúče sú kľúče od:

a) bezpečnostných úschovných objektov určených na ukladanie utajovaných skutočností,
b) vstupov do chránených priestorov,
c) vstupov do rokovacích miestností,
d) vstupov do objektov.

V tejto časti prevádzkového poriadku objektu sa odporúča spracovať pravidlá a pokyny pre:

- manipuláciu s kľúčmi od vstupov do objektu a chránených priestorov, spôsob ich prideľovania, výdaja a preberania do úschovy, systém ukladania náhradných kľúčov,
- manipuláciu s kľúčmi od úschovných objektov,
- zásady a oprávnenia na výrobu náhradných (kópií) bezpečnostných kľúčov,
- riešenie straty kľúča (kľúčov),

Pri spracúvaní týchto pravidiel a pokynov sa odporúča rešpektovať tieto zásady:

- kľúče sa prideľujú osobám len v súlade so stupňom (rozsahom) ich oprávnenia a na dobu platnosti ich oprávnenia,
- viesť evidenciu pridelených kľúčov , táto sa pravidelne kontroluje a aktualizuje,
- kľúče sa vydávajú len oprávneným osobám po overení ich oprávnenia,
- náhradné kľúče sa ukladajú v zapečatených obálkach s označením objektu ku ktorému patria (vstupu do chráneného priestoru) a uvedením osoby, ktorá je oprávnená ich vyzdvihovať; miesto uloženia náhradných kľúčov stanoví vedúci pracovník (napr. u priameho nadriadeného, u strážnej služby a pod.),
- náhradné kľúče je vhodné pravidelne obmieňať s používanými, aby boli rovnomerne opotrebúvané,
- je vhodné periodicky obmieňať cylindrické bezpečnostné vložky bezpečnostných zámkov; bezpečnostné vložky by sa mali vymeniť vždy, ak:
    - došlo k strate kľúča,
    - k zmene personálu (prepustenie, odchod na iné pracovisko a pod.),

- bol evidovaný bezpečnostný incident,
- k skutočnému alebo domnelému vyzradeniu prístupových hesiel či kódov.

- evidencii a pravidlám pre kľúčový režim by mali podliehať aj
  - kľúče od elektrických rozvodných a telefónnych skríň, telefónnych ústrední,
  - kľúče od vonkajších brán, núdzových východov apod.,
  - kľúče od zámkov uzáverov parovodov, káblových šácht, klimatizačných a ventilačných šácht, technických otvorov a pod.,
  - kľúče od bezpečnostných kufríkov, kontajnerov, tašiek či vakov,

Ad g) Podmienky používania, prideľovania , úschovy a evidencie kódových nastavení a hesiel používaných na prístup do objektov, CHP a bezpečnostných úschovných objektov

V tejto časti prevádzkového poriadku objektu sa odporúča spracovať pravidlá a pokyny pre:

- zachádzanie s prístupovými kódmi (heslami).
- riešenie prípadov odchodu zamestnanca (prepustenie, strata dôvery a pod.), ktorý mal prístup k prístupovým heslám a kódom, a iné potrebné pokyny.

Pri spracúvaní týchto pravidiel a pokynov sa odporúča rešpektovať tieto zásady:

- prístupové heslá alebo kódy sa prideľujú osobám len v súlade so stupňom (rozsahom) ich oprávnenia a na dobu platnosti ich oprávnenia,
- viesť evidenciu vydaných a platných prístupových hesiel a kódov, táto sa pravidelne kontroluje a aktualizuje,
- heslá sa vydávajú len oprávneným osobám po overení ich oprávnenia,
- prístupové heslá a kódy si majú oprávnené osoby zapamätať, nemali by si ich zapisovať a pod.,
- prístupové heslá a kódy by sa mali obmieňať, aby nedošlo k ich zneužitiu.
- kódy sa musia zmeniť:
  - pri prvom prevzatí zabezpečovacieho prostriedku (EZS, SKV, MZP) do prevádzky v chránenom priestore,
  - ak došlo k zmene oprávnených osôb (odchod, prepustenie, strata oprávnenia a pod.), ktoré poznali kódy,
  - ak došlo k skutočnému alebo domnelému vyzradeniu kódov,
  - bol zaregistrovaný neoprávnený pokus alebo došlo k neoprávnenému prístupu do chráneného priestoru,

- najmenej raz za 12 mesiacov.

Kódy systému kontroly vstupu do chráneného priestoru sa menia najmenej každých šesť mesiacov. O pridelení kódov rozhoduje vedúci zamestnanec.

Ad h) Podmienky manipulácie s mechanickými zábrannými prostriedkami a technickými zabezpečovacími prostriedkami a podmienky ich používania

Pravidlá a pokyny na používanie MZP a TZP sú spravidla obsahom dokumentácie dodávanej výrobcom (montážnou firmou). Ak sa vyskytne potreba spracovať pravidlá a pokyny vzhľadom na špecifické podmienky objektu, potom je dôležité zohľadniť najmä :

- odporúčania výrobcu,
- vplyvy vnútorných faktorov,
- vplyvy vonkajších faktorov.

Návody na obsluhu MZP a TZP sú súčasťou dokumentácie dodávanej spolu s výrobkom. Ak sa MZP alebo TZP montujú na/v objekte z viacerých komponentov (nie sú dodávané ako celok), návod na obsluhu sa vyžaduje od montážnej firmy.

Mechanické zábranné prostriedky

Mechanické zábranné prostriedky, použité na ochranu chráneného priestoru, používajú všetci oprávnení pracovníci.

Použité mechanické zábranné prostriedky si nevyžadujú špeciálne návody na obsluhu.

Pozornosť treba venovať najmä:

- používaniu kľúčov od zámkových systémov, aby nedošlo k ich zalomeniu,
- správnej manipulácii s kľúčmi od zámkov bezpečnostných úschovných objektov (skriňových trezorov),
- dôslednému uzatváraniu bezpečnostných okien ,
- správnemu používaniu dverí a okien , aby nedošlo k poškodeniu magnetických detektorov,
- kontrole stavu MZP, či nejavia známky pokusov o ich násilné prekonanie.

Opravy, údržbu alebo výmenu poškodených MZP alebo ich častí vyžaduje poverený pracovník u dodávateľskej firmy.

Pracovníci z pracovísk chráneného priestoru nie sú oprávnení svojvoľne vykonávať akékoľvek zmeny v usporiadaní MZP, alebo svojvoľne meniť zámkové systémy.

Technické zabezpečovacie prostriedky

Oprávnení pracovníci môžu používať len ovládacie prvky EZS v rozsahu, ktorý je stanovený návodom na obsluhu – t,j. zadávať kódy na vypnutie alebo zapnutie EZS a zadávať kódy na kódovej klávesnici SKV.

Ďalšiu povolenú manipuláciu s EZS a SKV môže vykonávať len poverený pracovník – osoba poverená obsluhou EZS a SKV na základe pokynov osoby zodpovednej za prevádzku EZS. Osoba zodpovedná za prevádzku EZS ďalej poučí o spôsobe manipulácie s klávesnicou a funkciou PSN všetkých nových pracovníkov CHP a ďalšie oprávnené osoby.

Osoba zodpovedná za prevádzku EZS a SKV je okrem toho povinná :

- zaistiť, že prístup k funkciám EZS bude povolený len zaškoleným osobám (s osvedčením od výrobcu, dovozcu alebo montážnej organizácie) a že EZS bude prevádzkovaný v súlade s návodmi na obsluhu a pokynmi pre užívateľa ,
- zaistiť, že bude obsluha EZS povolená iba osobám zoznámenými s návodmi na obsluhu a že EZS bude obsluhované v súlade s týmito návodmi;
- zaistiť, aby boli strážené priestory používané a udržiavané tak, aby nedochádzalo k vzniku falošných poplachových stavov,
- pravidelne preskušovať EZS, aby sa zaistila jeho funkčnosť na požadovanej úrovni,
- okamžite oznámiť zodpovednej montážnej alebo servisnej firme akúkoľvek poruchu EZS, alebo výskyt falošných poplachových stavov,
- oznámiť akúkoľvek zmenu v konštrukcii alebo používaní objektu alebo chráneného priestoru, ktorá by mohla negatívne ovplyvniť funkčnosť EZS,
- udržiavať v poriadku dodanú dokumentáciu EZS a zabezpečiť vedenie prevádzkovej knihy,
- včas vyžadovať pravidelné prehliadky a technické revízie EZS podľa plánu
- periodicky meniť prístupové kódy na ovládanie EZS,
- v prípade, ak treba vyradiť EZS z prevádzky zabezpečí, aby bola primeraným spôsobom zaistená ochrana utajovaných skutočností. Na vyradenie EZS upozorní jednotku FO a túto skutočnosť zaznamená do prevádzkovej dokumentácie.

Pracovníci chráneného priestoru sú povinní :

- používať kódovú klávesnicu a prístupové moduly podľa vydaných pokynov,
- dbať, aby nezapríčinili vyvolanie falošných poplachových stavov,
- kontrolovať mechanické upevnenie, resp. nezatienenie detektorov umiestnených na ich pracovisku,

Ad i) Spôsob kontroly dodržiavania týchto opatrení.

V poslednej časti prevádzkového poriadku objektu sa odporúča uviesť:
- formy kontroly prevádzkového poriadku objektu a jeho aktualizácie
- formy kontroly realizácie opatrení prevádzkového poriadku objektu (pravidelné, tematické, náhodné a pod.),
- periodickosť pravidelných kontrol,
- zodpovednosť za organizáciu a vykonávanie kontrol,
- oprávnenosť osôb na vykonávanie kontrol,
- zásady práce so zápismi z kontrol, s výsledkami kontrol a pod.

O výsledkoch kontrol sa vedie záznam v Knihe kontrol, ktorá sa ukladá u vedúceho (bezpečnostného zamestnanca). V knihe kontrol sa priebežne vedú tieto záznamy:

- dátum kontroly,
- kto kontroloval, príp. číslo oprávnenia na kontrolu,
- objekt (predmet) kontroly, resp. kontrolovaná oblasť,
- zistený stav,
- úlohy na odstránenie nedostatkov, resp. iné návrhy na opatrenia,
- vyjadrenie kontrolovaného,
- záznam o odstránení nedostatkov, resp. o vykonaní opatrení

Ak bol o kontrole spracovaný spis, potom sa v knihe kontrol uvedie v rubrikách len číslo spisu o kontrole (Č.p.) a aj ďalšie informácie o odstránení nedostatkov a vykonaných opatreniach sa evidujú len ako číslo písomnosti, ak boli v tejto forme spracované,

Údaje z Knihy kontrol sa využívajú pre analýzy a hodnotenia stavu a úrovne fyzickej bezpečnosti a objektovej bezpečnosti a na prijímanie účinných opatrení na jeho zlepšenie.

Kontroly vykonávané pracovníkmi fyzickej ochrany v priebehu výkonu služby sa priebežne zaznamenávajú v dokumentácii pre výkon služby. (Hofreiter, Križovský, 2007)

9.2.2 Smernica na výkon fyzickej ochrany

Smernica na výkon fyzickej ochrany objektu a chráneného priestoru môžu obsahovať:

a) spôsob zabezpečenia fyzickej ochrany objektu a chráneného priestoru, najmä:
- kto vykonáva fyzickú ochranu,
- ako je označená,
- ako je vyzbrojená, aké pomôcky má k dispozícii.

b) pokyny na výkon fyzickej ochrany**,** najmä:
- základné úlohy fyzickej ochrany (čo chránia, ap.)
- povinnosti zmeny fyzickej ochrany
- oprávnenia príslušníkov fyzickej ochrany,
- obmedzenia (na čo nemajú oprávnenia, čo nesmú ap.).

c) určenie počtu osôb zabezpečujúcich fyzickú ochranu:
- koľko príslušníkov má zmena FO,

d**)** spôsob kontroly osôb pri vstupe a výstupe a dopravných prostriedkov pri vjazde a výjazde :
- spôsob kontroly vstupu osôb
  - vlastných zamestnancov,
  - dodávateľov,
  - návštev ap.
- spôsob kontroly vjazdu a výjazdu dopravných prostriedkov,
- kontrola dovážaného, vyvážaného materiálu,

a) spôsob vykonávania náhodných prehliadok :
- kto oprávňuje k vykonávaniu náhodných prehliadok,
- ako sa vykonávajú,
- ako sa dokumentujú ap.

f) spôsob vykonávania obchôdzok:
- trasy obchôdzok,
- periodicita obchôdzok,
- úlohy pri obchôdzke , čo sa kontroluje
- záznamy o výsledkoch obchôdzok ap.

Pokyny sa uvádzajú pre pracovnú i mimopracovnú dobu.

g**)** spôsob reakcie na poplachové hlásenia technických prostriedkov:
- kde je vyvedená signalizácia EZS a kde sú umiestnené monitory CCTV,
- činnosť pri zaznamenaní signálu „poplach“ z chránených priestorov

- v pracovnej dobe
- v mimopracovnej dobe

- činnosť pri zaznamenaní núdzového signálu,
- reakcia na kamerový systém
- činnosť pri zistení nepovolanej osoby

h) činnosť pri riešení krízových situácií :

- uvedú sa povinnosti a úlohy pre pracovníkov fyzickej ochrany podľa opatrení rozpracovaných v krízovom pláne

i) spôsob kontroly výkonu fyzickej ochrany:

- kto je oprávnený kontrolovať výkon služby,
- rozsah kontroly podľa oprávnenia.

Grafická časť smernice na výkon služby fyzickej ochrany objektu

Grafická časť sa môže spracovať napr. formou Schémy rozmiestnenia kontrolných (strážnych) stanovíšť . V Schéme sa podľa potreby a situácie zakreslia:

- hranice objektu a chránených priestorov,
- rozmiestnenie stálych a dočasných stanovíšť fyzickej ochrany s vyznačením nebezpečných prístupov,
- rozmiestnenie strážených (kontrolovaných) priestorov,
- osi presunov pri obhliadkach a obchôdzkach (variantne: cez deň, v noci, v pracovnej i mimopracovnej dobe, za zníženej viditeľnosti, pri riešení krízových situácií a pod.),
- rozmiestnenie mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov,
- rozmiestnenie signalizačných prvkov systému kontroly strážnej služby,
- rozmiestnenie prostriedkov protipožiarnej ochrany,
- rozmiestnenie stanovíšť strážnych psov,
- rozmiestnenie zakázaných priestorov (do ktorých nesmie fyzická ochrana vstupovať),
- zakázané smery (v ktorých sa nesmú používať strelné zbrane, aby nedošlo k zraneniu nezúčastnených osôb),
- rozmiestnenie vypínačov elektrickej siete, hlavných uzáverov plynu, vody a pod.

Výkazová dokumentácia

Výkazová dokumentácia slúži pre pracovníkov fyzickej ochrany objektu na vedenie prehľadu o priebehu služby. Môže obsahovať:

- denný záznam o priebehu služby,
- záznamy o odovzdaní a prevzatí služby smeny,
- záznam o bezpečnostných incidentoch a mimoriadnych udalostiach,
- záznam o vykonaných zásahoch ,
- knihu kontrol,
- kniha návštev,
- kniha vjazdu/výjazdu vozidiel,
- evidenciu výdaja kľúčov,
- ďalšiu dokumentáciu podľa potreby, resp. rozhodnutia vedúceho.

Pomocná dokumentácia

Pomocná dokumentácia môže obsahovať :

- vzory osobných identifikačných kariet (kmeňových zamestnancov),
- vzory oprávnení pre vstup/výstup, vjazd/výjazd,
- zoznam funkcionárov oprávnených povoľovať vstup /vjazd do objektu,
- podpisové vzory,
- zoznam dokumentácie pre výkon služby ,
- protipožiarne smernice,
- telefónny zoznam (pre vlastný objekt, ďalej telefónne čísla na PZ, HZZ, zdravotnícke zariadenia, plynári, vodári, elektrikári, servisné firmy a pod.),
- návody na obsluhu MZP a TZP, ktoré obsluhuje (používa) fyzická ochrana,
- poznámkový zošit ,
- ďalšia potrebná dokumentácia podľa podmienok výkonu služby.

9.2.3 Krízový plán

Krízový plán objektu môže obsahovať :

- postup pri narušení objektu a CHP alebo pri pokuse o narušenie objektu a CHP,
- postup v prípade vzniku mimoriadnej situácie, súčasťou môže byť
    - plán na ochranu , evakuáciu materiálu a iných chránených aktív,,

- uvedenie zodpovedných osôb
- spôsob kontroly týchto režimových opatrení

Postup pri narušení objektu a chráneného priestoru alebo pri pokuse o narušenie objektu a chráneného priestoru

Každý detekovaný pokus o vniknutie do objektu (chráneného priestoru) alebo skutočné vniknutie nepovolanej osoby do objektu (chráneného priestoru) sa môže klasifikovať ako bezpečnostný incident.
V krízovom pláne ochrany objektu sa z hľadiska riešenia bezpečnostných incidentov odporúča spracovať:

a) činnosť pri pokuse alebo skutočnom narušení chráneného priestoru v mimopracovnej dobe
b) činnosť pri zistenom pokuse o násilné vniknutie do objektu,
c) činnosť po prijatí oznámenia o uložení výbušného nástražného systému (bomby):
d) činnosť po prijatí podozrivej zásielky:
e) činnosť pri narušenie verejného poriadku v blízkosti objektu ap.

V organizácii sa v závislosti na jej charaktere spracúvajú aj pokyny pre riešenie ďalších krízových situácií, ako sú napr.:
- prepadnutie,
- vydieranie, vrátane vydieranie rukojemníkom (rukojemníkmi),
- ekodemonštrácia s následným preniknutím do objektu,
- a iné hromadné alebo individuálne nátlaky.

Ich rozsah a podrobnosť je závislá na výsledkoch analýzy rizík , na podmienkach daného bezpečnostného prostredia a prostriedkoch, ktoré sú na ich riešenie k dispozícii. V každom prípade sa odporúča pre uvedené prípady spracovať aspoň postup, na koho sa pri vzniknutí bezpečnostného incidentu obrátiť, resp. kto zabezpečuje jeho riešenie.

Postup v prípade vzniku mimoriadnej situácie

Spracovateľ bezpečnostnej dokumentácie na základe výsledkov analýzy rizík spracuje v potrebnom rozsahu pokyny pre činnosť v prípade vzniku identifikovaných mimoriadnych situácií. V pokynoch sa spravidla uvádza:
- kto zodpovedá za riešenia danej situácie,
- komu sa oznamuje,
- kto sa na jej riešenie povoláva na pracovisko,
- s kým sa organizuje súčinnosť, kto pomáha ap.
- aká je činnosť zamestnancov,

- dôležité telefónne čísla ap.

Plán na ochranu , evakuáciu materiálu a iných chránených aktív

Evakuáciu materiálu a chránených aktív z chráneného priestoru vykonať len v prípadoch, ak by ich ponechanie v chránenom priestore mohlo viesť :

- k ich zničeniu alebo rozsiahlemu poškodeniu, napr. v prípade rozsiahleho požiaru,
- k neoprávnenej manipulácii v dôsledku deštrukcie stavebných prvkov objektu a chráneného priestoru a zabezpečovacích prostriedkov (mechanických zábranných prostriedkov, úschovných objektov), napr. po poškodení budovy výbuchom ap.

Ak je nariadená (alebo potrebná) evakuácia , alebo záchranná akcia, treba určiť:

- zásady pre povolenie vstupu osôb, ktoré zabezpečujú alebo vykonávajú záchrannú akciu alebo evakuáciu v objekte alebo v chránenom priestore,
- kto zabezpečuje balenie a vynášanie utajovaných skutočností do určeného priestoru,
- kto zodpovedá za organizáciu stráženia a ochranu evakuovaných utajovaných skutočností, ak sa utajované skutočnosti vynášajú z ohrozených priestorov mimo chráneného priestoru,
- miesto evakuácie utajovaných skutočností.

Pri evakuácii dodržiavať nasledujúce pravidlá:

1. Podľa možnosti vyhotoviť zoznam vynášaných predmetov,
2. Utajované skutočnosti baliť do uzatvárateľných a zamykateľných obalov.
3. Zabezpečiť trvalé stráženie priestoru, kde sa evakuované utajované skutočnosti ukladajú.
4. Ak sa utajované skutočnosti z časových dôvodov nadajú evakuovať z ohrozeného priestoru a existuje možnosť, že sa s nimi môže neoprávnene manipulovať, je každý pracovník povinný ich zničiť takým spôsobom, aby sa nedali reprodukovať. O zničení utajovaných skutočností informuje svojho priameho nadriadeného.

9.2.4 Smernice pre obsluhu Strediska registrácie poplachov

Stredisko registrácie poplachov *(Alarm Receiving Centre)* je trvale obsluhované vzdialené pracovisko (stredisko), do ktorého sa odovzdávajú (prenášajú) informácie týkajúce sa stavov jedného alebo viacej poplachových systémov na hlásenie narušenia.

Poplachové informácie , ako informácie o vzniknutom bezpečnostnom incidente na/v chránenom objekte, slúžia operátorom (obsluhe) Strediska registrácie poplachov na iniciáciu ich ďalšej činnosti.
Spracovaná dokumentácia obsluhy Strediska registrácie poplachov musí v závislosti na signalizovanej situácii – na charaktere bezpečnostného incidentu - formou logicky zostavených pokynov, resp. algoritmov činností umožniť:

- aktivovanie zásahových jednotiek (vlastných, inej bezpečnostnej služby, policajného zboru či požiarnikov),
- vyrozumenie užívateľa (majiteľa) objektu,
- vyrozumenie ďalších potrebných aktérov (plynári, elektrikári, vodári, zdravotníci apod.),
- koordinovať činnosť zásahovej jednotky v mieste zásahu s ostatnými zásahovými jednotkami.

  Pri spracúvaní Smerníc (algoritmov činností) treba rešpektovať tieto zásady:

- operátor musí byť schopný v čo najkratšom čase vyhodnotiť poplachový signál. lokalizovať miesto bezpečnostného incidentu, aktivovať a vyslať zásahovú skupinu
- pri organizovaní zásahu musí miesto bezpečnostného incidentu najprv preveriť zásahová skupina (bezpečnostnej služby, resp. polície) a až potom môže na miesto incidentu byť privolaný, resp. vpustený užívateľ chráneného objektu,
- pri zistení, že došlo k spáchaniu trestného činu, musí byť miesto činu zabezpečené tak, aby nedošlo k znehodnoteniu stôp a iného dôkazového materiálu a privolať orgány činné v trestnom konaní.

9.2.5 Zabezpečenie prepravy finančnej hotovosti

Preprava predstavuje súhrn činností, ktorými sa priamo uskutočňuje premiestnenie osôb a vecí (nákladov) dopravnými prostriedkami alebo dopravnými zariadeniami. Časovo zahŕňa okamih od prevzatia do odovzdania zásielky na určenom mieste. Zodpovednosť za bezpečnosť prepravy finančnej hotovosti a iných cenností prináleží ako prepravcovi, tak aj dopravcovi.
Prepravca je subjekt, ktorý používa prepravu najmä ako odosielateľ alebo prijímateľ zásielky. Je zodpovedný za vhodnosť a odbornú spôsobilosť dopravcu a sprievodcu na sprevádzanie zásielky.
Dopravca je prevádzkovateľ dopravy na uspokojovanie prepravných potrieb iných osôb a organizácií. V prípade prepravy cenností pôjde vždy o prepravu, pre ktorú platia osobitné prepravné podmienky, predovšetkým s ohľadom na bezpečnostnú ochranu.

Rozoznávajú sa tieto druhy prepravy cenností z konkrétneho miesta na miesto určenia :

- prenášanie a
- prevážanie cenností.

Ako dopravca tak aj prepravca pri plnení svojich úloh uplatňujú zásady bezpečnostného manažmentu.

Bezpečnostný manažér spoločnosti, poskytujúcej službu prepravy cenností, musí vypracovať a zabezpečovať celý komplex činností zameraných na odvrátenie alebo zmenšenie rizík, resp. prejavov hrozby bezpečnostných incidentov, ktoré by sa mohli vyskytnúť v priebehu prepravy cenností.

V podstate ide o plánovanie a realizáciu takých opatrení, ktoré zmenšia pravdepodobnosť (vierohodnosť) vzniku neželanej udalosti tým, že zmenia podmienky tých predpokladov, ktoré vznik takých udalostí umožňujú (vyvolávajú).

V súvislosti s riešením problematiky bezpečnosti prepravy cenností pôjde o realizáciu preventívnych stratégií, ktoré :

1. bránia a lebo zabránia vzniku bezpečnostných incidentov ;
2. ovplyvňujú výšku nákladov a zisku potenciálneho páchateľa;
3. zvyšujú riziko odhalenia a zadržania páchateľa.

V praxi sa jedná o realizáciu týchto opatrení :

1. Stanovenie prísnych režimových a organizačných opatrení pre prevoz finančných hotovostí s dôrazom na zabránenie úniku informácií o prevoze a hodnote prepravovaných prostriedkov.

2. Používanie vhodných dopravných prostriedkov. Dopravný prostriedok, ktorým sa uskutočňuje preprava cenností môže (v závislosti od hodnoty prepravovaných cenností) byť

- osobný automobil;
- prostriedok verejnej dopravy;
- pancierový osobný automobil;
- špeciálny pancierový automobil.

Je zrejmé, že prenos cenností v osobných automobiloch a vo verejnej doprave nezabezpečuje potrebnú ochranu prepravovaných cenností.

Pancierový osobný automobil je osobný automobil určený svoju špeciálnou úpravou na prepravu cenností. Má mať tvarované nepriestrelné sklá, vnútorne pancierované nepriehľadné stany, zodpovedajúci technický systém zabezpečenia a spojovacej techniky (elektromechanický uzatvárací a bezpečnostný systém s nútenou väzbou na svetelnú a zvukovú signalizáciu, dorozumievacie a odpočúvacie zariadenie, kryté strieľne a pod). Vozidlo má tzv. „trojkomorový

systém“, ktorý spôsobuje, že pri otvorení vonkajších dverí je vylúčené odcudzenie zásielky a priame ohrozenie posádky. Na streche vozidla by malo byť rozoznateľne umiestnené tzv. „viditeľné znamenie pre vrtuľník“.
Špeciálny pancierový automobil je skriňový automobil s nadstavbou zo špeciálneho pancierovaného materiálu (vysoko legovaná oceľ, doplnená zvláštnymi zliatinami, prípadne špeciálnymi syntetickými alebo keramickými hmotami), vrátane nepriestrelných skiel (sklo, polykarbonát) s požadovanou odolnosťou proti prieniku striel, s dvojitým uzatváraním dverí, troma komorami, vybavený komunikačným systémom (rádiové spojenie a autotelefóny), prostriedkami zvukovej a svetelnej signalizácie a ďalšími prvkami v požadovanej bezpečnostnej triede[1].Môže byť vybavený špeciálnymi pneumatikami, umožňujúcimi pokračovať v jazde aj po ich priestrele, alebo plnenými špeciálnou sceľujúcou zmesou. Na streche vozidla má byť umiestnené „viditeľné znamenie pre vrtuľník“.
K tomuto druhu vozidiel sa tiež počítajú vozidlá, ktoré disponujú kontajnerovým uzamykacím systémom v zadnej časti vozidla. Odobratie jednotlivého kontajneru je možné len po jeho predchádzajúcom uvoľnení vodičom.

3. Prepravu musí zaisťovať potrebný počet odborne spôsobilých osôb. Počet vozidiel a ochranného sprievodu (strážnikov, resp. ochrancov) stanovuje zákon (Zákon č. 473/2005, hl.3, § 56, ods. 7)

4. **Osoby** vykonávajúce a **zabezpečujúce prepravu** (posádka vozidla, sprievod) musia byť špeciálne vycvičené, intelektuálne, fyzicky a morálne spôsobilé pre takúto činnosť. Musia mať špeciálnu vyzbroj a výstroj, napr. nepriestrelné vesty, nepriestrelné prilby, ochranné masky (chrániace proti nervovoparalytickým, dusivým a dráždivým látkam), brokové alebo guľové zbrane, paralyzátory, obranné spraye a pod.

5. Používanie vhodných bezpečnostných prepravných obalov. Cennosti musia byť počas prepravy uložené do špeciálnych, ktoré plnia funkciu ochrany obsahu v osobitných podmienkach. V závislosti na hodnote prepravovaných cenností môžu byť použité :

- pevné tašky alebo kufríky, vybavené najmenej dvoma zámkami s možnosťou uzamknutia;
- bezpečnostné kufríky;
- kontajnery;
- kovové schránky s dvoma zámkami alebo poštové vrecia schváleného typu – sú prípustné pri preprave vozidlami.

Plánovanie prepravy

Plánovanie prepravy cennosti je najzložitejšou otázkou prepravy. treba pritom stanoviť celý pracovný postup pri dodržaní zásady maximálneho utajenia. Plánovanie prepravy musí spracúvať vždy spoľahlivý a preverený vedúci pracovník, ktorý má potrebné skúsenosti. Pri plánovaní prepravy musí predovšetkým určiť a zaistiť :

- kto a ako bude v rámci prepravnej firmy celú akciu riadiť,
- určiť okruh zamestnancov, ktorí budú do prepravných skupín určení,
- kto bude plniť jednotlivé funkcie v transportnej skupine (veliteľ prevozu, vodič, ochranca, resp. ochrancovia, kuriér, resp. posol),
- určiť presné vybavenie dopravnými prostriedkami, výstrojom a výzbrojou a spojovacími prostriedkami,
- zaistiť koordináciu činnosti v miestach nakladania a vykladania a v miestach dotácie a odvodov. Určiť kontrolné osoby a postup činnosti v týchto miestach,
- zaistiť mobilný styk prepravnej skupiny s riadiacim centrom (dispečingom), resp. c pultom centralizovanej ochrany objektov alebo inými dispečerskými pracoviskami,
- zaistiť analýzu rizík prepravy (možnosti úniku informácií, kritické miesta, resp. body na trasách, možné príznaky signalizujúce prípravu na prepad transportu ap.),
- určiť pracovníka zodpovedného za styk s políciou, príp. ďalšími bezpečnostnými službami,
- zaistiť technickú prehliadku vozidiel, najmä vzhľadom na možnosť nasadenia technických prostriedkov sledovania potenciálnymi útočníkmi.

Z taktického hľadiska má preprava niekoľko fáz :

- operatívno-taktický prieskum a analýzu,
- rozhodnutie o preprave na základe syntézy informácií,
- nakladanie a výjazd,
- presun a ochrana počas presunu,
- vykladanie (odovzdanie zásielky, dotácia ap.)

Na celú prepravu by mala byť spracovaná dokumentácia, resp. plány, ktoré by mali obsahovať :

- pôdorysnú analýzu okolia objektu, priľahlých ulíc a budov s vyznačením rizikových objektov,
- popis a analýzu existujúcich alebo možných rizikových situácií,
- vyznačenie spôsobu a miesta prevzatia cenností,
- smer príjazdu a odjazdu, vrátane miesta parkovania,

- presnú trasu vozidla, vrátane najmenej dvoch náhradných trás a ich zaistenie,
- dokumentáciu trasy prepravy, ktorá by mala obsahovať :
    - označenie všetkých analyzovaných rizikových miest, ktorým je možné sa vyhnúť,
    - telefónne čísla na centrálny dispečing, resp. PCO, či ostatné zložky záchranného systému,
    - samostatné určenie dislokácie útvarov polície a zdravotníckych zariadení po trase prepravy,
    - pri použití viacerých vozidiel presne určiť ich úlohy, rozmiestnenie, sektory vykrývania a presné úlohy pre jednotlivých členov osádky (osádok).

Pri spracúvaní dokumentácie pre prepravu cenností je žiaduce, aby sa spracovatelia vžili do rolí potenciálnych útočníkov a vytvárali modelové situácie, umožňujúce identifikovať možné ohrozenia a ich riešenie.

9.3 Riešenie úloh havarijného manažmentu

Do oblasti pôsobnosti havarijného manažmentu budú patriť také situácie, ako:

- prevádzkové havárie,
- priemyslové havárie,
- živelné pohromy.

Z Helsinského dohovoru, Smernice Seveso II i z predpisov OECD vyplýva určité delenie boja proti z haváriám do troch oblastí, a to na oblasť:

1. predchádzania závažným haváriám (protihavarijnej prevencie),
2. pripravenosti na závažné havárie, pre prípad, že k nim dôjde aj napriek opatreniam vykonaným v rámci protihavarijnej prevencie,
3. zmierňovania rozsahu a následkov závažných havárií na život a zdravie ľudí, životné prostredie a majetok, ako aj zdolávania takejto havárie vrátane sanácie jej následkov.

Pri tejto príležitosti však treba podotknúť, že:

a) hranice medzi uvedenými troma oblasťami nie sú obzvlášť výrazné a niektoré opatrenia častokrát zasahujú do dvoch, resp. i do všetkých troch oblastí,
b) dobre zorganizovaná protihavarijná prevencia môže zabezpečiť, že včasný a kvalifikovaný zásah v štádiu
    - nebezpečného stavu zariadenia, alebo
    - iniciačnej udalosti (Initiations Event), alebo
    - prechodovej (medziľahlej) udalosti (Intermediate Event),

zabráni premene tohto stavu ohrozenia (tzv. skoronehoda – near miss) na závažnú haváriu a tým aj zabezpečí buď úplné alebo aspoň podstatné zníženie následkov na ľudí, životné prostredie a majetok (vrátane obmedzenia potreby, zníženia nákladov i času na prípadnú sanáciu).

Havarijné plány

Účelom havarijného plánu je zabezpečenie včasnej a adekvátnej reakcie na závažnú haváriu alebo jej bezprostrednú hrozbu v záujme ochrany životov a majetku občanov a štátu a na vylúčenie, resp. čo najväčšie obmedzenie účinkov (následkov) závažnej na životné prostredie. (Hofreiter, Križovský 2007)

Havarijný plán musí byť zostavený tak, aby zabezpečoval

a) včasnú a adekvátnu reakciu na bezprostrednú hrozbu závažnej havárie alebo na vzniknutú závažnú haváriu a na jej zdolanie,
b) vykonanie opatrení potrebných na zaistenie bezpečnosti a ochrany života a zdravia ľudí, životného prostredia a majetku pred následkami závažnej havárie a na obmedzenie týchto následkov,
c) potrebnú informovanosť dotknutej verejnosti, ako aj príslušných orgánov a organizácií,
d) umožnenie obnovy (sanácie) životného prostredia poškodeného závažnou haváriou.

Havarijný plán obsahuje najmä

a) potrebné údaje objektoch, mená a funkcie osôb, ktorým sa v ňom ukladajú určité povinnosti, ako aj názvy príslušných orgánov a organizácií, s ktorých súčinnosťou sa počíta,
b) mechanizmy na výstrahu a varovanie ohrozených osôb, ako aj na vyrozumenie a zvolanie osôb, príslušných orgánov a organizácií zúčastnených na zdolávaní závažnej havárie a na obmedzovaní jej následkov,
c) scenáre reprezentatívnych druhov závažných havárií a súbory scenárov pre reprezentatívne druhy závažných havárií a opatrení na ich efektívne zdolanie a obmedzenie ich následkov, vrátane určenia zón ohrozenia, opisu potrebného materiálneho, personálneho a iného vybavenia a použiteľných zdrojov ,
d) opatrenia na zabezpečenie evakuácie alebo iného spôsobu ochrany ohrozených osôb alebo majetku,
e) opatrenia na zabezpečenie potrebnej súčinnosti s akciami príslušných orgánov a organizácií na území podniku a podľa potreby aj mimo neho,

f) spôsob školenia a výcviku podnikových útvarov a služieb a jednotlivých zamestnancov o činnostiach, ktoré sa od nich očakávajú, vrátane potrebnej súčinnosti s príslušnými orgánmi a organizáciami.

Ďalšie plány a dokumenty , napr:

- príslušnú dokumentáciu na úseku ochrany pred požiarmi,
- plán ochrany zamestnancov a osôb prevzatých do starostlivosti podľa predpisov o civilnej ochrane obyvateľstva,
- plán havarijných opatrení podľa predpisov na ochranu akosti a množstva vôd,
- plán opatrení na zmierňovanie priebehu a odstraňovanie dôsledkov havarijných stavov podľa predpisov na ochranu ovzdušia,
- havarijný plán pre prípady nakladania s nebezpečnými odpadmi podľa predpisov odpadového hospodárstva.

Organizácia záchrannej služby

Prevádzkovateľ objektu je povinný zabezpečiť vo svojom podniku organizačne, materiálne a personálne vybavenú službu, zloženú z odborne spôsobilých a vycvičených profesionálnych alebo dobrovoľných členov, ktorej úlohou je najmä

a) vykonávať rýchle a účinné zásahy na zdolanie závažnej havárie a obmedzenie jej následkov, vrátane záchrany ľudských životov, ako aj ochrany životného prostredia a majetku,
b) vykonávať iné práce v nedýchateľnom alebo v inak zdraviu škodlivom prostredí (plánované nehavarijné zásahy),
c) spolupracovať na prevencii závažných havárií a pripravenosti na ich zdolávanie a obmedzovanie ich účinkov,

Existencia kvalifikovanej a potrebne vybavenej záchrannej služby, zloženej zo zamestnancov poznajúcich nielen technológiu, ale aj vzájomné súvislosti a nadväznosti v konkrétnom podniku, podstatne zvyšuje účinnosť a rýchlosť prípadného zásahu, vrátane záchrany ľudí a ochrany životného prostredia a znižuje aj celkové riziko, nielen z hľadiska účinkov závažnej priemyselnej havárie (a prác na jej zdolanie) na vlastný podnik a jeho okolie, ale aj z hľadiska bezpečnosti cudzích jednotiek, ktoré sa podieľajú na jej zdolávaní.

V dôsledku aktuálnych prejavov bezpečnostných rizík dochádza k bezpečnostným incidentom. Za bezpečnostný incident sa považuje každé narušenie ochranných opatrení, integrovaných do bezpečnostného systému, alebo evidovaný pokus o takéto narušenie. (Hofreiter, Križovský 2007)

Pre úspešné zvládnutie riešenia bezpečnostných incidentov treba:

- mať definované postupy pre činnosť v prípade vzniku (objavenia sa) bezpečnostného incidentu,
- mať vypracované postupy pre riešenie najpravdepodobnejších bezpečnostných incidentov,
- každý bezpečnostný incident analyzovať, pričom sa zamerať na analýzu časopriestorových charakteristík príčin jeho vzniku, na spôsob jeho prejavov, pôsobenia a negatívnych dôsledkov,
- na základe overených postupov pri eliminácii bezpečnostného incidentu aktualizovať vypracované preventívne programy a pracovné postupy, v prípade objavenia sa nových bezpečnostných rizík vypracovať nové plány riešenie bezpečnostných incidentov. Pritom brať do úvahy zásadu reálnosti a primeranosti.
- v prípade možnosti vzniku závažných havárií mať vypracované havarijné plány a mať pripravené zásahové jednotky v potrebnom rozsahu.

Literatúra:

BOGDANOV, B. E., NESNÍDAL, J. aj. Ochrana majetku v socialistickém vlastnictví, část I., Praha : VŠ SNB, 1982, s. 112 – 130.

BRABEC, F. et al. Bezpečnost pro firmu, úrad, občana. Praha: Flóra s.r.o 2001, s. 50-51.)

DUFINEC, I.: Manažérstvo bezpečnosti podniku, In. Teória a prax nehodovej udalosti na železnici, Zborník príspevkov z odborného semínára, Košice, 2011

FILÁK, A. Policejně bezpečnostní činnost a její hlavní organizačně taktické formy. Praha : PA ČR, 2003, s. 19.

FILÁK, A. a kol. Základy teorie policejně bezpečnostní činnosti II. Praha : Police History, 2006, 214 s.

FOTR, J.: Management rizika (postupy a nástroje). In: Moderní řízení 12/2001

HLAVSA, J. Člověk v životních situacích. Praha : Academia 1987, s. 9.

HEŘMÁNEK, J., STŘÍŽ, B. Základy operativně pátrací činnosti VB. Praha : PF UL, 1971, s. 92 – 142.

HOFREITER, L.: Bezpečnostný manažment, Žilina, EDIS 2002, ISBN 80-7100-953-9

HOFREITER, L.: Bezpečnosť, bezpečnostné riziká a ohrozenia, Žilina, EDIS 2003

HOFREITER L., KRIŽOVSKÝ S.: Manažérstvo bezpečnostných systémov, skriptá, Multiprint Košice 2007, ISBN 978-80-89282-16-6

HOLCR, K., PORADA, V. Úvod do teorie a metodologie policejních věd. Praha : PA ČR, 2004, 112 s.

HOLCR, K., VICENÍK, J. K niektorým vybraným filozofickým a metodologickým otázkám konštituovania policajnej vedy. Policajná teória a prax, č. 1/1998, s. 19-20.

Kol. autorů : Česká bezpečnostní terminologie. Výklad základních pojmů. Brno: ÚSS VA v Brně, 2002, 113 s. (výstup z řešení výzkumného úkolu S-1-031: Perspektivy vývoje bezpečnostní situace, vojenství a obranných systémů do roku 2015 s výhledem do roku 2025).

KRAUS, J. a kol. Nový akademický slovník cizích slov. Praha : Academia, 2006, s. 335, 731.

LYSÁ, Ľ.: Rozhodovanie I. Využitie multikritériálnych metód v rozhodovacom procese riadiaceho subjektu VA, Liptovský Mikuláš 2002

MAJERNÍK, M; MESÁROŠ, M; BOSÁK, M.: Environmentálne inžinierstvo a manažérstvo, ŽU, Košice 2003

MAREŠ, M. Bezpečnost. In : Česká bezpečnostní terminologie. Výklad základních pojmů, Brno: ÚSS VA v Brně, 2002, 113 s. (výstup z řešení výzkumného úkolu S-1-031:
Perspektivy vývoje bezpečnostní situace, vojenství a obranných systémů do roku 2015 s výhledem do roku 2025).

MESÁROŠ, M. – Riadenie bezpečnostných systémov, Košice 2009, VŠBM v KE, Multiprint s.r.o., Ipeľská 1, 040 01 Košice, vysokoškolská učebnica
MESÁROŠ, M., PORADA, V., RAK, R. Informační proces jako nedílná součást transferu vědeckých poznatků do bezpečnostní praxe. Karlovarská právní revue č.3/2010
MILLER, G-A. aj. Plany i struktura provedenija. Moskva : Nauka, 1964.
MIKOLAJ, J., HOFREfTER, L., MACH, V., MIHÓK, J,, SELINGER, P. Terminológia bezpečnostného manažmentu. Výkladový slovník, Žilina; ŽU FŠI 2004, 191 s.)
MUSIL a kol. Kriminalistika. Praha : C.H.Beck., 2004, s. 51.
NESNÍDAL, J. Neodvratnost trestního procesu. Praha : VŠKV, 1989.
PEŠEK, A. aj. Operativně pátrací činnost kriminální služby VB. Praha : VŠ SNB, 1982, s. 40 – 59.
PONCE, D. Některé otázky reprezentace času. Dostupné na Webu: http://hilbert.chtf.stuba.sk/KUZV/download/kuzv-ponce.pdf
POPPER,M; KELEMEN, J.: Expertné systémy, ALFA, Bratislava 1988
PORADA, V. Teorie kriminalistických stop a identifikace. Praha : Academia, 1987.
PORADA, V. Identifikace veřejně bezpečnostních činností. In : Sborník VŠ SNB, Praha, 1987.
PORADA, V., ŠIMŠÍK, D. a kol. Identifikace osob podle dynamického stereotypu chůze. Praha : VŠKV, 2010.
PORADA, V., HOLOMEK, J. a kol.: Teorie a metodologie policejních věd a transfer vědeckých poznatků do policejní praxe. Praha : PA ČR, 2005, 311 s.
PORADA, V. a kol.Kriminalistika. Brno : CERM, 2001, s. 105 a násl.
PORADA, V. a kol. Kriminalistika. Plzeň :Aleš Čeněk,2007.
PORADA, V.,POŽÁR, J. Policejní informace, bezpečnostní situace a identifikace policejní činnosti. Sborník z mezinárodní konference „ Vysokoškolské vzdělávání policistů pro 21. století „. Praha : PA ČR, 1999.
PORADA, V., POŽÁR, J. Pojem, podstata a význam bezpečnostní situace. Bezpečnostní teorie a prax, zvl. č.-1. díl. Praha : PA ČR, 2001, s. 79-89.
PORADA,V., POŽÁR, J. Některé aspekty policejní informace. Praha : PA ČR, 2001.
PORADA, V., RAK, R. Informace jako prostředek poznání bezpečnostní situace a nástroj určování následných bezpečnostních činností. Praha : PA ČR, 2001.
PORADA, V., ŠIMŠÍK, D. a kol. Identifikace osob podle dynamického stereotypu chůze. Praha : VŠKV, 2010.
POŽÁR, J. Některé možnosti využití matematických metod v pátracím procesu. Sborník pátrání po osobách a věcech, Praha : VŠ SNB, 1980
POŽÁR, J. Kybernetické a matematické aspekty modelování informačního procesu operativně bezpečnostní situace. Bratislava : VŠ ZNB, 1984.
POŽÁR, J. Policejně bezpečnostní události a informace. In : Filák, A. a kol. :

Základy policejně bezpečnostní činnosti II. Praha : Police History, 2006, s. 158-174.
POŽÁR, J. Policejně bezpečnostní událost a informace. In. : Filák, A. a kol. : Základy teorie policejně bezpečnostní činnosti II. Praha : Police History, 2006, s. 147-174.
POŽÁR, J. Bezpečnostní situace a identifikace. In. : Filák, A. a kol. : Základy teorie policejně bezpečnostní činnosti II. Praha : Police History, 2006, s. 119-146.
POŽÁR, J., PORADA, V., NESNÍDAL, J. Racionalizace rozboru a hodnocení veřejnobezpečnostní situace využitím exaktních metod. Praha : VŠ SNB, 1988.
POŽÁR, J. Informační bezpečnost. Plzeň : Aleš Čeněk, 2005, 309 s.
RAK, R. a kol. Informatika v kriminalistické a policejní praxi. Praha : MV ČR, 2000.
RAK, R. a kol. Biometrie a identita člověka ve forenzních a komerčních aplikacích. Praha : Grada, 2008.
RAK, R., PORADA, V. : Informační proces jako prostředek poznání bezpečnostní situace a nástroj určování následných bezpečnostních činností. Bezpečnostní teorie a praxe, zvl. Č.-1. díl. Praha : PA ČR, 2002, s. 205-233.
REITŠPÍS,J; MESÁROŠ,M; BARTLOVA, I; ČAHOJOVA, Ľ; HOFREITER, L; SELINGER,P.: Manažérstvo bezpečnostných rizík EDIS, ŽU Žilina,2004, ISBN -80-8070-328-0.
SADOVSKIJ, V. V. Základy všeobecnej teórie systémov. Bratislava : Pravda, 1979, s. 77.
SCHURICH, F. R. K teorii kriminalistické situace. In Aktuální otázky současného vývoje kriminalistických metod. Praha : UK, 1982, s. 23 – 38.
ŠIMÁK, L.: Manažment rizík, Žilina, EDIS 2006
ŠIMŠÍK, D., PORADA, V. a kol.: Analýza pohybu člověka při identifikácii osob v kriminalistike. Košice : Edícia vedeckej a odbornej literatury SjF TU v Košiciach, 2008.
TALLO, A., RAK, R., TUREČEK, J.: Moderné technológie ochrany osôb a majetku, Bratislava 2006,)
VLČEK, J. a kol. Systémové řízení. Praha : Institut řízení, 1976, s. 50.
Ministerstvo vnútra SR, Sekcia krízového manažmentu a civilnej ochrany Č.p.: MV-KMCO-176-/KM-2010 Analýza tendencií vývoja vnútornej bezpečnosti Slovenskej republiky a z nej vyplývajúcich rizík a ohrození Slovenskej republiky dostupné na stránke www.minv.sk/civilna-ochrana
Dokument ICAO 9774