BEZPEČNOSTNÝ MANAŽMENT

MANAŽÉRSTVO BEZPEČNOSTI

prof. Ing. Ľubomír Belan, CSc.

Vydala Žilinská univerzita v Žiline
2015

Publikácia vznikla v rámci riešenia projektu:
"Kvalitné vzdelávanie s podporou inovatívnych foriem, kvalitného výskumu a medzinárodnej spolupráce – úspešný absolvent pre potreby praxe"
ITMS: 26110230090

Moderné vzdelávanie pre vedomostnú spoločnosť / Projekt je spolufinancovaný zo zdrojov EÚ

Vedecký redaktor prof. Ing. Miloslav Seidl, PhD.

Recenzenti prof. Ing. Josef Reitšpís, PhD.
doc. Ing. Libor Gašpierik, CSc.

Za odbornú, jazykovú a technickú úroveň publikácie zodpovedá autor.

Vydala Žilinská univerzita v Žiline/EDIS-vydavateľské centrum ŽU

ISBN 978-80-554-1163-7

OBSAH

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

POUŽITÉ SKRATKY

ASM *(Asset management system)* – Systém manažérstva aktív.
BCM *(Business continuity management)* – Manažérstvo kontinuity činností.
BCMS *(Business continuity management system)* – Systém manažérstva kontinuity činností.
BOZP – Bezpečnosť a ochrana zdravia pri práci.
CCTV *(Close Circuit Television)* – Priemyselná televízia.
CEO *(Chief Executive Officer)* – Riaditeľ organizácie.
CFM *(Certified Facility Manager)* – Certifikovaný facility manažér.
CFO *(Chief Financial Officer)* – Finančný riaditeľ.
CIO *(Chief Information Officer)* – Riaditeľ IT (IKT), správca informačného systému.
CISO *(Chief Information Security Officer)* – Bezpečnostný správca informačného systému.
CHRO *(Chief Human Resources Officer)* – Personálny riaditeľ, riaditeľ ľudských zdrojov.
COO *(Chief Operating Officer)* – Prevádzkový riaditeľ
CRO *(Chief Risk Officer)* – Manažér rizík.
CrMo *(Chief Risk Management Officer)* – Manažér riadenia rizík.
CSO *(Chief Security Officer)* – Bezpečnostný manažér.
EMS *(Environmental management system)* – Environmentálny manažérsky systém.
EPS – Elektrická požiarna signalizácia.
EZS – Elektrický zabezpečovací systém.
HSMS *(Health and safety management system)* – Systém manažérstva bezpečnosti a ochrany zdravia pri práci.
IEC *(International electrotechnical commission)* – Medzinárodná elektrotechnická komisia.
IFMA *(International Facility Management Association)* – Medzinárodná asociácia facility manažmentu.
IKT – Informačné a komunikačné technológie.
IMS *(Integrated management system)* – Integrovaný manažérsky systém.
ISMB – Integrovaný systém manažérstva bezpečnosti
ISO *(International organization for standardization)* – Medzinárodná organizácia pre normalizáciu.
IT – Informačné technológie.
MZP – Mechanické zábranné prostriedky.
NBÚ – Národný bezpečnostný úrad.
PCO – Pult centralizovanej ochrany.
PPS *(Physical Protective System)* – Systém ochrany objektov.
PS resp. PSN – Poplachové systémy.
PTV – Priemyselná televízia.
QMS *(Quality Management System)* – Systém manažérstva kvality.
SBS – Súkromná bezpečnostná služba.
SKV – Systémy na kontrolu a evidenciu vstupov do objektov.
SLA *(Service-level agreement)* – Dohoda o úrovni poskytovaných služieb.
SMB – Systém manažérstva bezpečnosti.
SMIB – Systém manažérstva informačnej bezpečnosti.
SRP – Stredisko registrácie poplachov.
SR – Slovenská republika.
STN – Slovenská technická norma.
TZP – Technické zabezpečovacie prostriedky.
USA – Spojené štáty americké.
VIP *(Very important person)* – Veľmi dôležitá osoba.
ZPH – Závažné priemyselné havárie.

1 ÚVOD

Peter Ferdinand Drucker, jeden z hlavných mysliteľov 20. storočia v oblasti riadenia a podnikania, významný expert v odbore manažmentu definoval, že ***manažment predstavuje riadenie vo všetkých organizáciách***. Uvádza, že manažment je špecifický druh práce, ktorá sa týka organizovania zdrojov na dosiahnutie uspokojivého výkonu. Manažment je špecifickým a charakteristickým ***nástrojom*** doslova každej organizácie pre dosahovanie cieľov nielen v transformačnom procese vo výrobnej sfére, ale aj v ďalších činnostiach, ktoré sa v organizácii vykonávajú *(Drucker, 2000)*.

Do oblasti pôsobnosti a zodpovednosti manažmentu spadá všetko, čo má vplyv na výkonnosť organizácie a na jej výsledky, či už sa to nachádza v jej internom alebo externom prostredí, či už je to pod kontrolou inštitúcie alebo mimo jej kontrolu *(Pugh, Hickson, 1992)*.

Je teda samozrejmé, že na výkonnosť organizácie má, okrem iných hlavných a podporných činností, významný vplyv aj **bezpečnosť.** Na zabezpečenie trvalej a udržateľnej bezpečnosti organizácie, ktorá je potrebná pre ochranu všetkých jej záujmov a záujmov všetkých zainteresovaných účastníkov, je dôležité, aby bol zavedený systematický riadiaci mechanizmus, ktorý zabezpečí jej správne fungovanie a rozvoj, v súlade so všetkými bezpečnostnými požiadavkami. V mnohých dokumentoch i inštitúciách sa na vyjadrenie riadiacej činnosti v oblasti bezpečnosti bežne používa pojem **„bezpečnostný manažment“.**

Slovo **manažment** je viacvýznamový pojem, okrem ***teórie*** a ***umenia riadiť,*** predstavuje ***súbor činností na riadenie organizácie***, ale zvyčajne sa používa najmä vo význame ***„skupina riadiacich pracovníkov, ktorá sa zaoberá touto činnosťou“.*** Obvykle sa používa v personálnom význame, napr. vrcholový manažment, manažment organizácie, bezpečnostný manažment, ale niekedy aj vo význame ***„systém a metódy riadenia činnosti“.***

Takáto viacvýznamová situácia nie je z hľadiska jednoznačnosti komunikácie výhodná, preto podľa jazykovej poradne Jazykovedného ústavu Ľudovíta Štúra je na odlíšenie od viacvýznamového slova **manažment** vhodné vo význame ***„systém a metódy riadenia činnosti“*** používať slovo **manažérstvo**, napr. manažérstvo rizika, integrovaný manažérsky systém, systém manažérstva kvality, systém manažérstva bezpečnosti a ochrany zdravia pri práci, systém manažérstva informačnej bezpečnosti, environmentálny manažérsky systém, systém manažérstva kontinuity činností, produktové manažérstvo a pod.

Na základe uvedeného zdôvodnenia a v súlade s technickými normami budú v ďalších častiach učebnice používané pojmy:

- **Bezpečnostný manažment** – širší, viacvýznamový pojem, ***špecifický druh manažmentu***, zameraný na ***teóriu, personálne zabezpečenie a špecifickú aktivitu manažmentu*** na ***zachovanie bezpečnosti organizácie***.
- **Manažérstvo bezpečnosti** – ***systém a metódy riadenia bezpečnosti*** organizácie.

Doterajšie publikácie o bezpečnostnom manažmente boli väčšinou zamerané na jeho technickú a technologickú stránku, bez využitia teórie manažmentu. Pre bezpečnostný manažment i manažérstvo bezpečnosti je preto potrebné vytvoriť nový systém poznatkov, ktorý ponúka jednotné riešenie bezpečnosti z hľadiska manažmentu, pretože absolventi druhého stupňa štúdia študijného programu Bezpečnostný manažment budú ***manažéri v rôznych oblastiach bezpečnosti.***

Cieľom učebnice je – na základe teórie bezpečnostného manažmentu poskytnúť základné údaje o manažérstve (riadení) bezpečnosti v organizáciách. Učebnica rieši najmä nasledovnú problematiku:

- **manažment** – rozhodovanie, plánovanie, organizovanie, vedenie ľudí, kontrola,
- **bezpečnostný manažment** – definície, zameranie, významy a prístupy k vymedzeniu bezpečnostného manažmentu,
- **systém manažérstva bezpečnosti –** definícia systému, riadiaci a riadený systém, štruktúra manažérstva bezpečnosti,
- **proces manažérstva bezpečnosti** – cyklický proces manažérstva bezpečnosti, plánovanie, zavedenie, monitorovanie a preskúmavanie, zdokonaľovanie systému manažérstva bezpečnosti, bezpečnostná dokumentácia (Bezpečnostná politika, Plán implementácie Systému manažérstva bezpečnosti, Havarijný plán), audit,
- **integrovaný systém manažérstva bezpečnosti** – riadenie systému, centrálny útvar bezpečnosti a jeho zložky,
- **systémy a zložky ochrany osôb a majetku** – systém ochrany objektov, požiarna ochrana,
- **manažérstvo incidentov,**
- **bezpečnostné zložky integrovaného manažérskeho systému** – Systém manažérstva BOZP, Systém manažérstva kontinuity činnosti BCMS, Environmentálny manažérsky systém EMS, Systém manažérstva informačnej bezpečnosti SMIB.

Pri tvorbe učebnice boli využité výsledky vedeckovýskumnej a publikačnej činnosti Katedry bezpečnostného manažmentu Fakulty bezpečnostného inžinierstva Žilinskej univerzity v Žiline a medzinárodné a národné právne normy pre bezpečnostný manažment a manažérstvo bezpečnosti. Publikácia je určená pre študentov študijného programu Bezpečnostný manažment, môže sa využiť aj pre iné študijné programy a na komerčné potreby, pretože v ucelenej podobe poskytuje informácie potrebné na vytvorenie, zavedenie a prevádzkovanie systémov manažérstva bezpečnosti v jednotlivých organizáciách.

1.1 LITERATÚRA

DRUCKER, P. F. [2000]: *Výzvy managementu pro 21. století*. Praha: Management Press, 2000. ISBN 80-7261-021-X.

PUGH, D. S. – HICKSON, D. J. [1992]: *Napísali o organizáciách*. In: Nadácia City University Bratislava ako čítanka kurzového materiálu Efektívny manažér, preklad The Open University UK, ISBN 80-8904-535-9.

2 ZÁKLADY MANAŽMENTU

Riadenie sa stalo nevyhnutným prostriedkom na zabezpečenie koordinácie individuálnych úsilí odvtedy, keď ľudia začali vytvárať skupiny, aby splnili ciele, ktoré nemohli dosiahnuť ako jednotlivci. Čím viac sa začala spoločnosť spoliehať na skupinové úsilie a čím viac sa zväčšovali organizované skupiny, tým viac narastal význam riadiacich pracovníkov. **Riadenie sa tak stalo jednou z najdôležitejších ľudských činností v histórii**.

Riadenie je činnosť, v ktorej sa na základe predpísaného algoritmu sleduje systém a po zistení odchýlky od požadovaného stavu alebo priebehu, sa vykonajú korekcie, aby sa do neho systém vrátil. Pojem riadenie má v rôznych kontextoch rôzny špecifický význam:

1. **v spoločenských a ekonomických systémoch** – sústava zásad, nástrojov, prostriedkov i osôb, usmerňujúcich istú činnosť – riadenie spoločnosti, hospodárstva, národnej ekonomiky, podniku, organizácie, teória riadenia,
2. **v technických systémoch** – mechanizmus na ovládanie niečoho – automatické riadenie, riadenie lietadla, riadenie techniky, strojov, technologických procesov,
3. **v živých organizmoch** – riadenie fyziologických, biologických, mikrobiologických procesov.

Vývoj poznatkov riadenia je možné historicky zaradiť do nasledovných generácií:

1. **generácia** – ***prvopočiatky riadenia v staroveku a rozvoj riadiacich aktivít v stredoveku:***
   a) prvopočiatky riadenia v staroveku:
   - Sumerskí obchodníci, egyptskí stavitelia pyramíd alebo stavitelia Čínskeho múru,
   - je dokázané, že práve *kompetencie a zručnosti v oblasti plánovania, organizovania, kontroly a koordinácie práce* tisícok pracovníkov boli predpokladom napr. *výstavby Cheopsovej pyramídy, niekedy v treťom tisícročí pred naším letopočtom,*
   - neskoršie civilizácie, najmä grécka a rímska, rozšírili potrebu *plánovania a organizovania*, podporovali podnikanie v oblasti komunálnych i vládnych programov, ako napr. *dláždenie ulíc, stavanie vodovodov a ciest naprieč Európou, Malou Áziou, Palestínou, a severnou Afrikou a pod.*
   - *rozhodovanie, získavanie a spracovanie informácií a funkcie riadenia sa významne využívali vo vojenstve,*
   - v staroveku je mobilizovanie ľudí spojené najmä s požitím násilia (otroci).

   b) rozvoj riadiacich aktivít v stredoveku:
   - civilizácia renesančnej Európy a Blízkeho východu podporovala riadenie najmä v oblasti vodného inžinierstva, budovania kanálov, priehrad a prístavov,
   - rozvojom moderných náboženských kultúr, budovaním nových kostolov, katedrál a kláštorov sa zvyšoval význam zložitých projektov,
   - novinky, ako rozšírenie arabských čísel (5.-15. storočie) a kodifikácia podvojného účtovníctva (1494) však už vtedy poskytli nástroje pre manažérske *hodnotenie, plánovanie a kontrolu,*
   - v stredoveku je mobilizovanie ľudí spojené najmä s požitím násilia (nevoľníctvo).
2. **generácia** – ***vytvorenie teórie vedeckého riadenia*** (na prelome 19. a 20. storočia),
3. **generácia** – ***chápe manažment ako podnikový manažment (riadenie podnikových činností) v subjektoch, ktoré produkujú zisk*** (do 2. svetovej vojny),
4. **generácia** – ***manažment je potrebný vo všetkých organizáciách,*** nielen vo výrobných alebo produkujúcich zisk (až po 2. svetovej vojne), od 80. rokov 20. storočia – vodcovstvo *(leadership).*

Vývoj a charakteristika manažmentu

Vývojom kapitalizmu postupne vzrástla zložitosť a význam riadenia natoľko, že iba tradície a zvyklosti v riadení už nestačili zabezpečiť potrebné správanie sa jednotlivcov a skupín v podnikoch. S rozvojom priemyselnej výroby a so zväčšovaním jej rozsahu vznikajú nové požiadavky *napr. na evidenciu, kalkuláciu nákladov, sledovanie výkonu a kontrolu,* čo vyžadovalo nutnosť *venovať pozornosť najmä*:

- procesom riadenia v smere k podriadeným,
- správaniu, jednaniu a vystupovaniu riadiacich pracovníkov.

Do tohto časového obdobia je situovaný **začiatok novodobého manažmentu**. Od týchto čias dochádza k prechodu od poháňania, dozoru a trestu najmä k ekonomickým stimulom, ktoré znamenajú humanizáciu aktivačných prostriedkov.

Pojem **m a n a ž m e n t**, vyjadrujúci ***riadenie v podnikoch, založené na vedeckom základe,*** sa začal používať koncom 19. storočia v USA pri skúmaní a rozpracovaní teoretických poznatkov o riadení výroby a organizácií, fungujúcich v podmienkach trhového hospodárstva.

Manažment je od svojho vzniku neustále preverovaný reálnym životom a prešiel týmto vývojom:

1. **Vytvorenie teórie vedeckého riadenia** o riadení výroby a organizácií, fungujúcich v podmienkach trhového hospodárstva – **manažmentu,** klasický prístup na prelome 19. a 20. storočia:
   - ***vedecké riadenie*** – použitie vedeckých metód pre stanovenie najlepšieho spôsobu vykonania práce – Frederick Winslow Taylor (1856-1915),
   - ***administratívne riadenie*** – procesný prístup k riadeniu – všeobecná teória o organizácii z hľadiska objektu riadenia a činnostiach, ktoré vykonávajú manažéri, zdôraznenie riadenia ako osobitnej činnosti ktorú treba skúmať, študovať a zdokonaľovať – Henry Fayol (1841-1925),
   - ***byrokratické riadenie*** – súčasť administratívneho riadenia, zdôrazňuje existenciu presne určenej formálnej organizácie, pri ktorej je jednoznačne určená hierarchia právomoci a spôsob fungovania – Max Weber (1864-1920).
2. **Manažment v ekonomických organizáciách, najmä ako podnikový manažment** (riadenie podnikových činností v subjektoch, ktoré produkujú zisk), do 2. svetovej vojny:
   - ***sociálne prístupy*** (behavioristická škola) – základy riadenia ľudí v organizácii, prístup zdôrazňujúci medziľudské vzťahy, skúmanie vplyvu pracovných podmienok na pracovníka – Elton Mayo (1880-1949), zakladateľ teórie medziľudských vzťahov, Abraham Maslow (1908-1970) – otec humanistickej psychológie.
3. **Moderná teória manažmentu – základy riadenia činností a produkcie**
   - ***rozhodovací prístup*** – vychádza z toho, že jadrom riadenia je rozhodovanie, pozornosť na skvalitnenie rozhodovacích procesov v manažmente, metódy a techniky rozhodovania *(Simon, 1946),*
   - ***matematický (kvantitatívny) prístup*** – aplikácia matematických a štatistických metód a operačnej analýzy v manažmente, pozornosť na tvorbu modelov ako zdroja informácií pre rozhodovanie a využitie výpočtovej techniky v manažérskej práci *(Gass, Dantzig, 2011),*
   - ***systémový prístup*** – aplikácia systémovej teórie zameranej na tvorbu synergických efektov v organizácii *(Bertalanffy, 1976),*

- ***empirický prístup*** – zameraný na analýzu a hodnotenie poznatkov manažérskej praxe a ich následnom zovšeobecnení, manažment chápe ako vedu a umenie riadiť, pričom umenie chápe skôr ako vec intuície a nadobudnutých skúseností:
  Peter Ferdinand Drucker (1909-2005):
  - **manažment vo všetkých druhoch organizácií** (nielen vo výrobných alebo produkujúcich zisk, ide aj o nemocnice, univerzity, štátnu správu atď.)
  - **manažment ako umenie** a ako **súbor poznatkov na riadenie podnikovej činnosti.**
- ***integrované prístupy*** k manažmentu
  - systémový prístup,
  - situačný kontingentový prístup,
  - operačný procesný prístup.

Slovné vyjadrenie pojmu manažment je [mænɪʤmənt], zriedkavo *menežment* alebo *menedžment.* Slovo *„manage“* pochádza z talianskeho *maneggiare*, zo starolatinského ľudového *„manidiare“,* ktoré pochádza z latinského *„manus“ (ruka)* – prazákladom bolo ručné ovládanie koní. Francúzske slovo *„mesnagement“,* neskôr *„ménagement“* – vedenie domácnosti, ovplyvnilo vývoj významu anglického slova. Anglicky *„management“* od *„to manage“* znamená riadiť, zvládať, byť vo vedúcej funkcii, viesť, spravovať, zvládnuť, ovládať nástroj, uspieť, dokázať, dobre hospodáriť, zariadiť.

V našich podmienkach sa pojem „manažment“ začal používať v 90. rokoch minulého storočia, dovtedy ho nahradzoval pojem „**t e ó r i a r i a d e n i a**“.

V prípade podniku sa používa alternatívne pomenovanie ***manažment podniku, podnikový manažment, riadenie podniku, podnikové riadenie*** resp. vo význame: ***manažérstvo podniku, podnikové manažérstvo*** alebo trochu nepresne ***vedenie podniku, podnikové vedenie*** (angl. *Business management*, nem. *Unternehmens führung*). Z uvedených pomenovaní je v súlade s technickými normami výraz **„manažérstvo podniku“.**

V teórii manažmentu sa nachádza viac rôznorodých definícií odborníkov, ktoré sa zameriavajú na zdôraznenie:

a) Vedenia ľudí:
- Manažment je proces vytvárania a udržiavania určitého prostredia, v ktorom jednotlivci pracujú spoločne v skupinách a účinne/efektívne dosahujú vybrané ciele (*Koontz, Weihrich, 1993*).

b) Špecifických činností, vykonávaných riadiacimi pracovníkmi:
- Manažment je proces plánovania, organizovania, vedenia a kontroly organizačných činností zameraných na dosiahnutie organizačných cieľov.
- Manažment sú typické činnosti, ktoré manažér vykonáva, ako je rozhodovanie, organizovanie, plánovanie, kontrolovanie, vedenie ľudí, koordinovanie, motivovanie atď.

c) Tvorivý prístup, predmet štúdia a jeho účel:
- Manažment je oblasť štúdia, ktorá sa venuje stanoveniu postupov, ako čo najlepšie dosiahnuť ciele organizácie (*Robbins, 2004*).
- Manažment možno chápať ako „proces vytvárania a ďalšieho aktívneho rozvíjania podnikateľsky orientovaného správania sa organizácie“ (*Vodáček, 2009*).

Okrem toho je množstvo definícií, ktoré **manažment hodnotia z celkového pohľadu:**

- Manažment je **dynamický proces,** v ktorom sa manažéri v podmienkach neustále sa meniaceho prostredia, snažia prostredníctvom ľudského potenciálu ***dosahovať ciele*** organizácie ***pri hospodárnom a účinnom využívaní obmedzených zdrojov*** (*Papula, 1995*).

- Manažment treba chápať nielen ako riadenie, ale **umenie riadiť**, odbornosť v riadení je daná schopnosťou ***plánovať, organizovať, motivovať a viesť ľudí, koordinovať, komunikovať a kontrolovať tak, aby podnik fungoval úspešne*** *(P. F. Drucker).*
- Manažment je **súbor prístupov, názorov, skúseností, odporúčaní a metód,** ktoré vedúci pracovníci (manažéri) používajú na ***„zvládnutie špecifických činností (manažérskych funkcií), smerujúcich k dosiahnutiu sústavy cieľov organizácie“*** *(Vodáček, 2008).*

V širšom slova zmysle je možno vedecké riadenie (manažment) charakterizovať ako *organizované pôsobenie ľudí na spoločenský systém ako celok alebo jeho jednotlivé zložky (spoločenskú výrobu, sociálno-spoločenský život, kultúru,* ***bezpečnosť*** *a iné), ktoré sa uskutočňuje s poznanými objektívnymi zákonmi a progresívnymi tendenciami v spoločnosti, v záujme zabezpečenia jej optimálneho fungovania a vzostupného vývoja.*

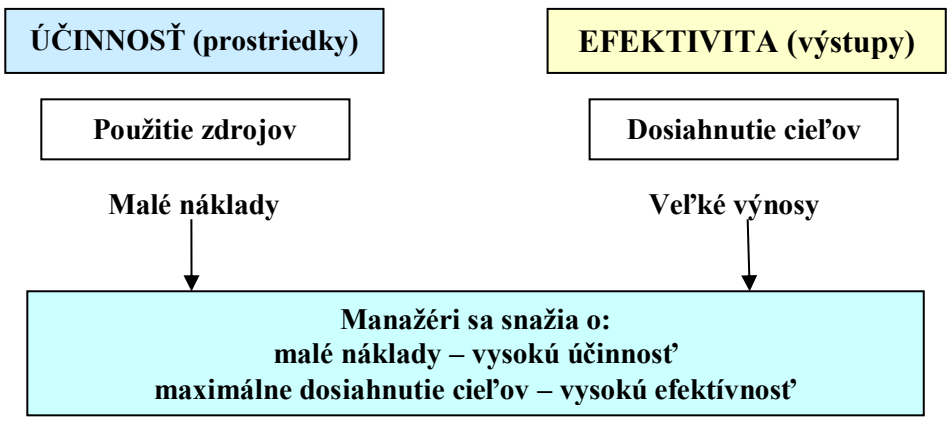
Manažment je *mnohostranná uvedomelá a aktívna tvorivá činnosť, v rámci ktorej* **riadiaci subjekt** *(riadiace centrum, top manažment)* stanovuje ciele, ovplyvňuje metódy, prostriedky a spôsob správania viacerých (výkonných) prvkov (objektov), aby celá **riadená sústava (systém)** optimálne plnila určené funkcie a dosahovala stanovené ciele v určenom čase a kvalite.

Veľmi výstižným spôsobom definuje manažment Robbins: „Manažment predstavuje **proces *koordinácie pracovných aktivít ľudí*** tak, aby boli ***vykonané účinne a efektívne***“:

- **proces** – reprezentuje prebiehajúce funkcie alebo hlavné aktivity manažérov (práca s informáciami, rozhodovanie, plánovanie, organizovanie, vedenie a kontrolovanie),
- **koordinácia práce ostatných** – je to, čo manažéra odlišuje od nemanažérov,
- **účinnosť** – znamená dosiahnuť väčšie výstupy ako vstupy, preto je dôležité efektívne využiť zdroje, ktoré sú k dispozícii – robiť veci správne,
- **efektivita** – robiť správne veci – je spojená s dosiahnutím cieľov organizácie (obr. 1).

Stručne povedané – **manažment je to, čo robia manažéri, ktorí sú vykonávateľmi manažérskych funkcií** – ***pomocou racionálnych aktivít usmerňujú premeny vstupov (zdrojov), tieto kombinujú a usilujú sa zabezpečiť ich efektívnu transformáciu na požadované výstupy.***

Poslaním manažmentu je ***dosiahnutie stanovených cieľov***. Hlavným prvkom organizácie sú ľudia, preto manažéri pôsobia predovšetkým na ľudí a koordináciou ich individuálnych úsilí zabezpečujú plnenie cieľov. Proces manažmentu je založený na myšlienke, že ***manažment predstavuje trvalé rozhodovanie a konanie, v ktorom manažéri plánujú, organizujú, vedú a kontrolujú.***



Obr. 1 Účinnosť a efektivita manažmentu (zdroj Robbins, Coulter)

Manažment je zameraný nielen na vykonanie určitých činností a dosiahnutie cieľov organizácie (efektivita – maximálne zisky), ale tiež na to, aby bolo všetko vykonané čo najúčinnejšie (správne využitie zdrojov, malé straty). Podľa obr. 1 v úspešných organizáciách ide vysoká účinnosť a vysoká efektivita vedľa seba, zlý manažment sa často vyznačuje nízkou účinnosťou a nízkou efektivitou alebo efektivitou, dosiahnutou vďaka nízkej účinnosti *(Robbins, Coulter, 2004).*

Podľa Druckera všetci manažéri musia vykonávať **päť základných činností**:

1. stanoviť **ciele,** ktoré je treba v organizácii plniť,
2. **organizovať prácu**, rozdeľovať činnosti na čiastkové a priradiť ich k pracoviskám, vytvárať organizačnú štruktúru, vyberať vedúcich pracovníkov,
3. **motivovať** ľudí a zabezpečovať **komunikáciu** medzi nimi,
4. **merať a hodnotiť výsledky práce**, to znamená správne posudzovať kvalitu a kvantitu dosiahnutých výsledkov a spravodlivo hodnotiť a odmeňovať pracovníkov,
5. zabezpečiť **kvalifikačný rast pracovníkov**.

Na základe spoločných znakov a rôznych prístupov k vymedzeniu obsahu, možno formulovať všeobecnú definíciu manažmentu:

Manažment je otvorená sústava poznatkov *o špecifických činnostiach manažérov* *(využívanie informácií, rozhodovanie, plánovanie, organizovanie, vedenie, kontrolovanie),* ***ktoré sú potrebné na dosiahnutie stanovených cieľov organizácie, prostredníctvom usmerňovania premeny vstupov, resp. zdrojov na požadované výstupy.***

2.1 LITERATÚRA

BERTALANFFY, L. VON. [1976]: *Perspektives on General System Theory: Foundations, Development, Applications*, New York: George Braziller, revised edition: ISBN: 978-08-0760-798-5.

CRAINER, S. [2000]: Moderní management – základní myšlenkové směry. Praha : Management Press. ISBN 80-7261-019-8.

DONELLY Jr., J. H. – GIBSON, J., L. – IVANCEVICH, J. M. [1997]: *Management*, GRADA Publishing, Praha. ISBN 80-7169-422-3.

DRUCKER, P. F. [2004]: *To nejdůležitejší z Druckera v jednom svazku.* Praha: Management Press, 2004, ISBN 80-7261-066-X.

DRUCKER, P. F. [2004]: *Výzvy managementu pro 21.století*. Praha: Management Press, 2000. ISBN 80-7261-021-X.

FAYOL, H. [1949]: *General and Industrial Management*. (C. Storrs, Trans.). London: Sir Isaac Pitman & Sons, LTD. (Original work published 1918).

GASS, S. I. – DANTZIG, G. B. [2011]:. *Profiles in Operations Research*. International Series in Operations Research & Management Science. ISBN 978-1-4419-6280-5.

KOONTZ, H. – WEIHRICH, H. [1993]: *Management*. Victoria Publishing, Praha. ISBN 80-8560-545-7.

MASLOW, A. H. [2014]: *O psychologii bytí*, preklad Hana Antonínová. Praha: Portál.

MAYO, E. [1933]: *The human problems of an industrial civilization.* Cambridge, MA: Harvard.

PAPULA, J. [1995]: *Minimum manažéra alebo profesia, ktorá stojí zato*, Elita, Bratislava.

ROBBINS, S. P. – COULTER, M. [2004]: *Management,* GRADA Publishing, Praha.

SIMON, H. A. [1946]: *Proverbs of Administration.* Public Administration Review, *6* (1), pp. 53–67.

TAYLOR, F. W. [1911]: *The principles of Scientific Management.* Harper & Row, vyšlo v roku 1967 v knižnici WW Norton & Company, Inc., 500 Fifth Avenue, New York, ISBN 0-393-00398-1.

VEBER, J. a kol. [2009]: *Management. Základní moderní manažérske přístupy, výkonnost a prosperita.* Praha: Management Press.ISBN 978-80-7261-200-0.

VEBER, J. a kol. [2007]: *Management – základy, prosperita, globalizace.* Praha: Manage ment Press, ISBN 807-80-7261-029-5.

VODÁČEK, L. – VODÁČKOVÁ, O. [2009]: *Moderní management v teorii a praxi, druhé. rozšířené vydání.* Praha: Management Press, ISBN: 97-8807-261-197-3.

WEBER, M. [1922]: *Wirtschaft und Geselschaft (Hospodárstvo a spoločnosť).*

3 BEZPEČNOSTNÝ MANAŽMENT

V terminologickom slovníku bezpečnostného manažmentu je **bezpečnostný manažment** definovaný ako: *„Špecifická zmysluplná činnosť riadiacich funkcionárov a bezpečnostných pracovníkov v organizáciách, zameraná na odvrátenie alebo minimalizáciu vonkajších i vnútorných bezpečnostných rizík, resp. bezpečnostných ohrození rôznej povahy a príčiny, pre ochranu života a majetku občanov, obcí a spoločnosti, obsahujúca v sebe prvky rizikového, krízového, havarijného a hodnotového manažmentu.*

Obsah bezpečnostného manažérstva je tvorený logickou postupnosťou krokov na zabránenie vzniku, prejavov alebo minimalizáciu bezpečnostných rizík a ohrození, ktoré v organizáciách môžu spôsobiť ujmy zamestnancom, ohrozujú hmotný i nehmotný majetok a fyzickú a objektovú bezpečnosť. Bezpečnostný manažment je aj súčasťou priamej a situačnej stratégie prevencie proti majetkovej 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“.

Táto veľmi rozsiahla definícia bezpečnostného manažmentu bola vytvorená na začiatku skúmania problematiky bezpečnosti v organizáciách a v súčasnosti sa už prejavujú jej niektoré nedostatky, najmä:

- definícia je zameraná zbytočne na podrobnosti,
- niektoré časti sa opakujú *(zameraná na odvrátenie alebo minimalizáciu vonkajších i vnútorných bezpečnostných rizík, resp. bezpečnostných ohrození – zabránenie vzniku, prejavov alebo minimalizáciu bezpečnostných rizík a ohrození),*
- podľa STN ISO 31000:2011 Manažérstvo rizika, zásady a návod je viac možností na zaobchádzanie s rizikom, než je ich *odvrátenie alebo minimalizácia,*
- nie je v nej jednoznačne vymedzená oblasť, pre ktorú je bezpečnostný manažment určený *(v organizáciách – pre ochranu života a majetku občanov, obcí a spoločnosti),*
- zbytočne k bezpečnosti osôb a majetku uvádza navyše fyzickú a objektovú bezpečnosť *(môžu spôsobiť ujmy zamestnancom, ohrozujú hmotný i nehmotný majetok a fyzickú a objektovú bezpečnosť),*
- uvádza, že *bezpečnostný manažment je súčasťou priamej a situačnej stratégie prevencie proti majetkovej kriminalite*, prečo nie aj prevencie proti ohrozeniu zdravia a života osôb a pod.,
- posledná veta definície je veľmi zložitá a chybne uvádza, že riziko sa aktivuje na ohrozenie *(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).*

Najväčším nedostatkom definície je, že ***nevychádza zo zásad manažmentu*** a ***je zameraná väčšinou len na fyzickú a objektovú bezpečnosť.*** Bezpečnosť je však mnohostranná, a keď ju niekto chce riadiť, ***musí riešiť všetky podsektory bezpečnostného sektora referenčného objektu.***

Vzhľadom na tieto nedostatky a nepresnosti je v súčasnosti potrebné znovu sa zamerať na túto definíciu a upraviť ju, aby bezpečnostný manažment bol chápaný nielen z technického hľadiska ochrany objektov a chránených priestorov, ale aby definícia obsahovala aj prvky manažmentu a zamerala sa všetky oblasti v sektore bezpečnosti organizácie.

3.1 DEFINÍCIE BEZPEČNOSTNÉHO MANAŽMENTU

Pri charakterizovaní bezpečnostného manažmentu je potrebné vychádzať zo ***všeobecnej teórie manažmentu,*** ktorá sa uplatňuje vo všetkých oblastiach riadenia činnosti organizácie. Potom je možné vytvoriť základnú definíciu:

Bezpečnostný manažment je špecifický druh manažmentu,
zameraný na manažérstvo bezpečnosti referenčných objektov.

Podľa Kodanskej školy sa pojem **bezpečnosť** vzťahuje priamo na konkrétny **subjekt** alebo **subjekty,** ktoré usilujú o dosiahnutie svojej bezpečnosti – teda **aktérov bezpečnosti,** ktorých nazýva **referenčné objekty. Referenčný objekt** je ***základným prvkom bezpečnosti***, odpovedá na otázku o čiu bezpečnosť ide, je to jednotka, ktorú je treba chrániť, pokiaľ je existenčne ohrozená – ***chránená hodnota.*** **Referenčné objekty** sú ***entity, ktoré sú existenčne ohrozené a môžu si legitímne nárokovať právo na prežitie.***

Referenčné objekty a činnosti, ktoré sa v nich uskutočňujú, boli popísané z hľadiska druhu ohrozených subjektov, z organizačného hľadiska ohrozených subjektov a z právneho hľadiska v 3. kapitole prvého dielu učebnice Bezpečnostný manažment. Bezpečnosť a manažérstvo rizika. Belan, 2015.

Z organizačného hľadiska medzi referenčné objekty patria najmä: *štátne orgány a organizácie, jednotky územnej samosprávy (vyššie územné celky, mesto, obec),výrobné podniky, nevýrobné podniky poskytujúce služby, ďalšie organizácie poskytujúce služby a dobrovoľné ziskové a neziskové organizácie.* Vo všetkých týchto referenčných objektoch je množstvo aktív, ktoré môžu byť ohrozené a preto je nutné ich chrániť.

Bezpečnostný manažment je možné porovnať najmä s **krízovým manažmentom**, ktorý je zameraný na ***predchádzanie a riešenie krízových situácií*** a ktorý je tiež špecifickým druhom manažmentu.

Špecifickosť v bezpečnostnom manažmente spočíva v tom, že nie je zameraný na *výrobný transformačný proces, vytvárajúci produkty, ani na proces poskytujúci služby, či iba na riešenie krízových situácií,* ale je výlučne zameraný na riadenie (manažérstvo) **špecifickej podpornej činnosti**, ktorá je životne dôležitá pre nerušené ***dosiahnutie stanovených cieľov*** – na nepretržité **manažérstvo bezpečnosti referenčných objektov.**

Zaoberá sa teda riešením problematiky **bezpečnosti *vo všetkých podsektoroch bezpečnostného sektora organizácie.*** Všeobecne je možné hovoriť o rôznych druhoch **organizácií,** ich priestoroch a jednotlivých objektoch, v ktorých sú umiestnené rôzne druhy **aktív** (*osoby, majetok* vo forme hmotných a nehmotných aktív a rôznych výrobných a nevýrobných činností i *životné prostredie*). Bezpečnosť týchto aktív je v organizácii zameraná najmä na bezpečnosť:

1. **osôb** – napr. fyzická ochrana osôb, bezpečnosť a ochrana zdravia pri práci, ochrana osobných údajov a pod.
2. **majetku** v objektoch a chránených priestoroch – napr. ochrana objektov, ochrana infraštruktúry, najmä kritickej, požiarna ochrana, ochrana informácií a informačných systémov (informačná bezpečnosť), ochrana utajovaných skutočností, ochrana pred závažnými priemyselnými haváriami, udržiavanie kontinuity činností a pod.
3. **životného prostredia** – činnosti, ktorými sa predchádza znečisťovaniu alebo poškodzovaniu životného prostredia alebo sa toto znečisťovanie alebo poškodzovanie obmedzuje a odstraňuje.

Bezpečnostný manažment možno aplikovať:

- pre akúkoľvek veľkosť organizácie (v malých i veľkých organizáciách),
- pre všetky typy organizácie (v ziskových i neziskových podnikoch) a to vo výrobných odvetviach i v odvetviach poskytujúcich služby,
- na všetky úrovne riadenia (spoločnosť, podnik, prevádzku, dielňu, kolektív),
- vo všetkých oblastiach činnosti organizácie (obchodná, technická, výrobná, personálna, účtovná, informačná a pod.).

3.2 VÝZNAMY BEZPEČNOSTNÉHO MANAŽMENTU

Bezpečnostný manažment je špecifickým druhom manažmentu a možno ho charakterizovať ako:

1. **pojem na označenie profesie manažérov, ktorí sa zaoberajú bezpečnosťou,**
2. **špecifickú riadiacu aktivitu manažmentu** na riadenie bezpečnosti organizácie ***(manažérstvo bezpečnosti organizácie)***,
3. **teóriu *(vednú disciplínu)*** o manažérstve bezpečnosti,
4. **umenie** riadiť bezpečnosť.

Bezpečnostný manažment ako profesia

Pojmom **bezpečnostný manažment** sa často označuje ***skupina ľudí,*** ktorí majú zodpovednosť za bezpečnosť organizácie. Bezpečnostný manažment je teda **špecifická, uvedomelá ľudská činnosť,** smerujúca k ***dosiahnutiu vopred stanovených bezpečnostných cieľov***.

Na manažérstve bezpečnosti sa spoločne podieľajú najmä:

a) **vrcholoví manažéri,**
b) **líniový manažéri,** ktorí zodpovedajú za bezpečnosť vo svojich úsekoch, napr. vedúci divízie alebo prevádzky, majster v dielni a pod.,
c) **bezpečnostní manažéri.**

Bezpečnostný manažment ako špecifická aktivita

Bezpečnostný manažment predstavuje aj **špecifickú, uvedomelú ľudská činnosť,** smerujúcu na ***dosiahnutie vopred stanovených bezpečnostných cieľov***. Je to **špecifická aktivita manažmentu,** zameraná na ***manažérstvo bezpečnosti referenčného objektu,*** predstavuje druh ľudskej práce, jednu z najdôležitejších ľudských činností, ktorá umožní bezpečné vykonávanie všetkých činností na dosiahnutie stanovených bezpečnostných cieľov.

V súčasnosti predstavuje značne špecializovanú činnosť **manažérstva bezpečnosti**, bez ktorej sa neobíde žiadny väčší organizačný celok. Najvšeobecnejšie ju možno charakterizovať ako ***súhrn všetkých činností, ktoré je treba urobiť, aby sa dosiahla, zaistila a upevňovala bezpečnosť osôb, majetku a životného prostredia organizácie.***

Cieľom bezpečnostného manažmentu je prostredníctvom manažérstva bezpečnosti v referenčných objektoch zabrániť zraneniam ľudí alebo stratám na životoch, škodám a stratám majetku a narušeniu životného prostredia.

Proces manažérstva bezpečnosti organizácie uskutočňujú ***manažéri*** v súčinnosti ***s bezpečnostnými manažérmi a bezpečnostnými pracovníkmi*** v štruktúre **Systému manažérstva bezpečnosti**. Manažéri a bezpečnostní manažéri organizácie získavajú a vyhodnocujú bezpečnostné informácie so zameraním na vonkajšie a vnútorné bezpečnostné riziká, rozhodujú sa a vykonávajú manažérske funkcie.

Dôležitou oblasťou aktivity bezpečnostného manažmentu je ***účasť v procese strategického riadenia organizácie***, v ktorom vrcholový manažment:

- formuluje poslanie, vízie a ciele organizácie,
- tvorí stratégie (analýzy vonkajšieho a vnútorného prostredia organizácie, voľba vhodnej stratégie na podnikateľskej a organizačnej úrovni),
- implementuje stratégie (návrh organizačných zmien, administratívnych opatrení a kontrolného systému na realizáciu stratégie).

Medzi špecifické aktivity bezpečnostného manažmentu patrí najmä riešenie nasledovných druhov bezpečnosti:

- bezpečnosť osôb,
- bezpečnosť objektov a chránených priestorov s utajovanými skutočnosťami,
- bezpečnosť objektov s inými aktívami,
- bezpečnosť práce a ochranu zdravia,
- bezpečnosť prevádzkových činností – technicko-prevádzkovú bezpečnosť, bezpečnosť technických zariadení, bezpečnosť kontinuity činností (BCM), predchádzanie závažným priemyselným haváriám,
- protipožiarna bezpečnosť,
- počítačová bezpečnosť a informačná bezpečnosť – bezpečnosť informačných systémov, bezpečnosť dôležitých informácií, ochrana utajovaných skutočností, ochrana osobných údajov,
- bezpečnosť pred podvodmi a zneužitím,
- bezpečnosť vnútorného poriadku a riešenie incidentov,
- bezpečnosť vnútorného i vonkajšieho životného prostredia,
- a ďalšie oblasti bezpečnosti.

Bezpečnostný manažment ako teória (vedná disciplína)

Bezpečnostný manažment predstavuje súhrnný, logicky usporiadaný **súbor poznatkov** o zásadách, metódach a postupoch riadenia v oblasti bezpečnosti osôb, majetku a životného prostredia v referenčných objektoch, ktoré sú vypracované na základe empírie a abstrakcie a ktorým sa možno učiť a aj ich vyučovať. Tieto poznatky by mal každý manažér poznať ako východisko pre svoju prácu, v konkrétnych situáciách ho vedieť vhodne aplikovať, kombinovať a prípadne aj tvorivým spôsobom rozvíjať.

Bezpečnostný manažment pritom ***neposkytuje vyčerpávajúce, jasné a univerzálne návody ako riadiť bezpečnosť v akejkoľvek organizácii,*** pretože je spojený s realitou a tá sa do istej miery neustále mení. Počas manažérstva bezpečnosti musia byť rešpektované faktory teritoriálne, časové a ďalšie.

Bezpečnostný manažment má svoj vlastný predmet skúmania ako aj vlastné zdroje poznávania. **Predmetom skúmania** je ***bezpečnosť referenčných objektov,*** s cieľom dosiahnuť bezpečnosť osôb, majetku a životného prostredia na základe identifikácie a vyhodnotenia vonkajších a vnútorných bezpečnostných rizík.

Bezpečnostný manažment je študijným programom študijného odboru 8.3.1 Ochrana osôb a majetku a ako *multidisciplinárna teória* sa opiera o poznatky viacerých študijných odborov v oblastiach:

- ***manažmentu*** – Manažment, Ekonomika a manažment podniku, Podnikový manažment, Finančný manažment, Účtovníctvo, Poisťovníctvo,
- ***bezpečnosti*** – Manažérstvo rizika, Environmentálny manažment, BOZP, Požiarna ochrana, Krízový manažment, Záchranné služby, Doprava v krízových situáciách, Právne problémy bezpečnosti, Kriminalistika, Kriminológia, Prevencia kriminality,
- ***technických vied*** – Informačný manažment, Elektrotechnika, Automatizácia a riadiace systémy, Informačné a komunikačné technológie, Projektový manažment, Životné prostredie,
- ***prírodných vied*** – Matematika, Pravdepodobnosť a matematická štatistika, Počítačové a informatické vedy, Fyzika, Chémia, Biológia,
- ***spoločenských vied*** – Psychologické vedy, Sociológia, Právne vedy, Verejná správa, Teória organizácie a riadenia, Personálny manažment (Manažment ľudských zdrojov),
- ***a ďalších.***

Bezpečnostný manažment je **praxeologická disciplína**, čo sa prejavuje v jej orientácii na konečný výsledok – ***bezpečnosť referenčného objektu***. Z toho vyplývajú aj hlavné ciele teórie bezpečnostného manažmentu:

- zdokonaliť prax manažérstva bezpečnosti, čo nie je možné bez zvládnutia elementárnych poznatkov z manažmentu a bezpečnostného manažmentu,
- pomáhať pri výchove bezpečnostných manažérov a adeptov na tieto funkcie (študentov), ktorí sa majú učiť a porozumieť princípom, metódam a postupom manažérstva bezpečnosti, ako aj tomu, ako tieto poznatky aplikovať v praxi,
- ukázať oblasti a problémy bezpečnostného manažmentu, ktoré vyžadujú osobitný výskum a ďalšie rozpracovanie.

Poslaním bezpečnostného manažmentu je ***vytvoriť metodológiu manažérstva bezpečnosti,*** ktorej uplatnenie umožní zvyšovať efektívnosť fungovania organizácií. Manažérstvo bezpečnosti má za úlohu vytvoriť ***systém manažérstva bezpečnosti,*** ktorý zodpovedá možnostiam, potrebám, prostrediu a požiadavkám maximálnej úrovne ochrany. V praxi je tento systém spravidla tvorený účelným usporiadaním a používaním disponibilných ľudských zdrojov, technických prostriedkov, organizačných a režimových opatrení.

V teórii bezpečnostného manažmentu dochádza k ***internacionalizácii***, pretože problémy bezpečnosti, ktoré skúma, sa vyskytujú vo všetkých organizáciách, bez ohľadu na štátnu príslušnosť. Z toho dôvodu sa odborníci na túto relatívne mladú disciplínu v jednotlivých štátoch spájajú, vzájomne si vymieňajú skúsenosti a spoločne hľadajú odpovede na otázky, ktoré sa pred nimi vynárajú.

Bezpečnostný manažment ako umenie

J. D. Rockefeller pri hodnotení úspešnosti svojho podnikania povedal: „*Schopnosť riadiť ľudí je tovar, ktorý sa dá kúpiť ako cukor alebo káva. Som ochotný zaň dať viac, než za akýkoľvek iný tovar na svete*“. Táto myšlienka jednoznačne zdôrazňuje, že pre manažérov je najdôležitejšia schopnosť riadiť podriadených.

Manažment sa začal považovať skôr za umenie ako vedu pod vplyvom úspechov japonského manažmentu koncom 60. rokov minulého storočia. Medzi najvýznamnejších predstaviteľov tohto prístupu patrí P. F. Drucker, ktorý umenie riadiť považuje za jeden z rozhodujúcich kľúčov k úspechu manažérov – podnikateľov novej doby *(úspešný manažér je ten, koho podnik prosperuje – **úspešný bezpečnostný manažér je ten, kto dosiahne požadovanú úroveň bezpečnosti s najnižšími nákladmi**)*.

Manažment ako umenie znamená „vedieť ako“ hľadať a umiestniť *správnych ľudí na správne miesta,* komunikovať *s nimi,* reálne ich motivovať *individuálne i ako členov tímu,* kreovať *tím, predvídať vývoj,* rozumne *riskovať atď.*

Prvkami umenia v bezpečnostnom manažmente sú:

- individuálne schopnosti bezpečnostných manažérov ako sú *organizačné schopnosti, umenie jednať s ľuďmi, vystupovanie, schopnosť kvalifikovaného rozhodovania* a pod.,
- *intuícia, kreativita, schopnosť predvídať a v pravú chvíľu riskovať* pri uplatňovaní manažérskych nástrojov, techník a princípov,
- schopnosť *vyhľadávať vhodné príležitosti* na zlepšovanie systému manažérstva bezpečnosti a ovplyvňovanie bezpečnosti organizácie,
- schopnosť *vytvoriť schopný tím bezpečnostných pracovníkov* v systéme manažérstva bezpečnosti organizácie,
- schopnosť *vytvárať vízie pre bezpečnosť organizácie,* nájsť príležitosti tam, kde ostatní vidia iba chaos, rozpory a konflikty.

3.3 CHARAKTERISTIKY BEZPEČNOSTNÉHO MANAŽMENTU

Bezpečnostný manažment je možné skúmať z rôznych hľadísk. Prístupy k charakteristike bezpečnostného manažmentu možno rozdeliť do dvoch skupín:

- jednodimenzionálne prístupy,
- viacdimenzionálne prístupy.

Pri jednodimenzionálnej charakteristike bezpečnostného manažmentu sa vychádza ***z jedného hľadiska*** a podľa toho sa vymedzuje a štrukturalizuje, čo nemôže vyčerpávajúco opísať celý proces manažmentu. Prednosťou tohto prístupu a charakteristiky bezpečnostného manažmentu je dôslednosť jeho interpretácie zo zvoleného hľadiska, čo umožňuje odkryť a popísať niektoré jeho stránky. Nedostatkom je najmä, že pri zveličovaní jedného hľadiska sa neberú do úvahy iné, nemenej dôležité stránky a čiastkové charakteristiky a tým sa nedoceňuje rozmanitosť procesu bezpečnostného manažmentu.

Komplexný systémový prístup k bezpečnostnému manažmentu

Viacdimenzionálna charakteristika bezpečnostného manažmentu **integruje jednotlivé čiastkové hľadiská a prístupy do celku** a tie sa stávajú súčasťou teórie bezpečnostného manažmentu. Obsah, jadro procesu bezpečnostného manažmentu a tým aj jeho teórie možno posudzovať z troch hľadísk:

a) podľa informačného hľadiska,
b) podľa rozhodovacieho hľadiska,
c) podľa funkčného hľadiska *(pomocou manažérskych funkcií).*

Rozhodovací a informačný proces a manažérske funkcie sa prejavujú najmä **v procese manažérstva bezpečnosti,** ktorý je založený na myšlienke, že manažment predstavuje:

- nepretržité získavanie a využívanie ***bezpečnostných informácií,***
- na nepretržité ***rozhodovanie,***
- a vykonávanie ***manažérskych funkcií*** na dosiahnutie stanovených bezpečnostných cieľov organizácie.

Každá charakteristika procesu manažérstva bezpečnosti sa zameriava na jeden aspekt, preto dáva o ňom len jednostranný, zúžený pohľad. V jednote a vzájomnej súvislosti umožňujú ucelenú predstavu o procese bezpečnostného manažmentu, pričom sa navzájom rozličným spôsobom prekrývajú, čím vzniká vnútorne integrovaný systém s vyššou kvalitou. V reálnom živote tieto stránky procesu neexistujú oddelene, vždy ide o konkrétnu, pritom mnohotvárnu praktickú činnosť.

Proces manažérstva bezpečnosti by sa nemal rozkladať na jednotlivé charakteristiky a tým ukončiť rozbor. Všetky prístupy sú potrebné, pokiaľ prispievajú k uskutočneniu procesu manažérstva, chápaného v jednote a komplexnosti. Len syntéza výsledkov získaných v rámci rozličných prístupov k procesu manažérstva bezpečnosti môže dať o ňom ucelený obraz.

3.3.1 Informačná charakteristika bezpečnostného manažmentu

Nahromadenie nových vedeckých a vedecko-technických poznatkov, rozvoj informačných a komunikačných technológií, spôsobili, že **informácie** sa stávajú ***kľúčovým zdrojom rozvoja spoločenského života*** v globálnom meradle a najvýznamnejším ***zdrojom inovácií a zmien.***

Manažérstvo bezpečnosti v organizácii predstavuje veľmi zložitú prácu s informáciami. Celý proces manažérstva bezpečnosti organizácie sa môže v určitom zmysle skúmať ako proces ***získavania, zhromažďovania, triedenia, vyhodnocovania, uschovávania a využitia*** **informácií o bezpečnosti** *smerom hore, ale aj dole.*

Na tomto základe vzniká a existuje **informačný systém** organizácie a prostredníctvom neho sa prakticky realizujú všetky manažérske činnosti.

Manažéri, bez ohľadu na typ organizácie alebo jej úroveň, zastávajú a vykonávajú podľa Mintzberga *(1973)* okrem **interpersonálnych rolí** *(reprezentant, vodca, styčný dôstojník)* a **rozhodovacích rolí** *(podnikateľ, riešiteľ sporov, alokátor zdrojov, vyjednávač)* aj **informačné roly:**

a) pozorovateľ *(monitor),*
b) šíriteľ informácií *(informátor),*
c) hovorca.

Manažér ako pozorovateľ:

a) sleduje bezpečnostné právne normy a ich zmeny, ktoré musí zapracovať do vnútorných noriem a smerníc,
b) vyhľadáva, zhromažďuje, využíva a uschováva informácie *o stave bezpečnosti,* so zameraním na informácie o:
- stave organizácie, aktívach, ktoré treba chrániť a zavedených opatreniach na ich ochranu,
- stave manažérstva bezpečnosti a manažérstva rizika,
- stave bezpečnosti práce (BOZP, bezpečnosť technických zariadení, bezpečnosť pracovného prostredia a pracovných podmienok),
- stave bezpečnosti objektov (plášťová a obvodová ochrana, priestorová ochrana, kontrola vstupov, predmetová ochrana, režimových opatreniach, fyzická ochrana, protipožiarna ochrana a pod.),
- stave bezpečnosti hlavných a podporných činností,
- výskyte nebezpečných látok, ktoré môžu spôsobiť havárie,
- výskyte bezpečnostných incidentov,
- stave ochrany utajovaných skutočností, ochrany osobných údajov, ochrany citlivých informácií a ochrany tajomstva,
- stave informačnej bezpečnosti a bezpečnosti informačných a komunikačných zariadení,
- iných dôležitých oblastiach bezpečnosti.

c) získava informácie o *vonkajších a vnútorných rizikách,*
d) získava informácie o *zainteresovaných účastníkoch, ich potrebách a očakávaniach,*
e) vyhodnocuje získané informácie a rozhoduje, ktoré informácie, kedy a akým spôsobom môže ***využiť pri rozhodovaní o riešení otázok bezpečnosti***.

Manažér ako šíriteľ informácií má za úlohu:
- poskytovať podriadeným také bezpečnostné informácie, ktoré nie sú schopní sami inak získať, poskytuje im informácie aj vtedy, ak navzájom nemajú rýchly a ľahký kontakt,
- odovzdávať prijaté bezpečnostné informácie (externé a od podriadených) ďalším pracovníkom,
- pri poradách informovať o bezpečnostných opatreniach.

Manažér ako hovorca sa sústreďuje najmä na ***externú komunikáciu***, ktorá spočíva v rokovaniach s ľuďmi mimo danej organizácie. Informácie o bezpečnostnej politike, bezpečnostných plánoch, postupoch, manažérstve bezpečnostných rizík a ďalšie bezpečnostné informácie je nutné poskytovať všetkým zainteresovaným účastníkom.

Pre manažérov a bezpečnostných manažérov je dôležité:
- mať bezpečnostné informácie, ktoré práve potrebujú,
- mať ich včas a vtedy, keď sú aktuálne,
- mať ich tam, kde ich je možné najefektívnejšie využiť,

- vedieť s nimi efektívne pracovať.

Bezpečnostné informácie majú význam najmä vtedy, keď:

- prinášajú údaje o vonkajších i vnútorných rizikách,
- rozširujú vedomosti o nových spôsoboch riešenia bezpečnosti a ochrany osôb, majetku a životného prostredia,
- sú využiteľné pre dosiahnutie zvolených bezpečnostných cieľov.

Veľmi úzka spätosť je medzi informačným a rozhodovacím procesom, keď existuje zložitý systém priamych i spätných väzieb. **Prijímanie rozhodnutí vyžaduje vždy informácie.** Stupeň odôvodnenosti rozhodnutí závisí predovšetkým od ***úplnosti, hodnovernosti a včasnosti informácií.*** Majú prispieť k tomu, aby sa podľa možností prijímali optimálne rozhodnutia.

Prijatie rozhodnutia vytvára informáciu, ktorú dostávajú jeho vykonávatelia vo forme plánov, úloh, noriem, príkazov a využívajú ju ako impulz pre cieľavedomú a koordinovanú činnosť. Na jej základe sa má dosiahnuť splnenie prijatých rozhodnutí. Veľmi dôležité je aj šírenie bezpečnostných informácií medzi zamestnancov a všetkých zainteresovaných účastníkov.

3.3.2 Rozhodovacia charakteristika bezpečnostného manažmentu

Významným predstaviteľom **rozhodovacieho prístupu k manažmentu** bol Herbert Alexander Simon (1916–2001). Organizáciu chápal ako systém, v ktorom sú ľudia mechanizmami robiacimi rozhodnutia. Skúmal použitie matematických metód v rozhodovaní, pozornosť venoval modelovaniu rozhodovacích procesov s využitím výpočtovej techniky, vrátane vypracovania programov na heuristické riešenie úloh rozhodovania.

Rozhodovací proces je ***hlavným článkom riadiaceho procesu,*** jednou z najdôležitejších aktivít, ktoré vykonávajú manažéri. Rozhodovanie súvisí so všetkými fázami a stránkami manažmentu, týka sa teda každej jeho časti. Rozhodovacie procesy, ktoré zasahujú do manažérskych funkcií, zabezpečujú ich vzájomné prepojenie a uzatvárajú spätnú väzbu.

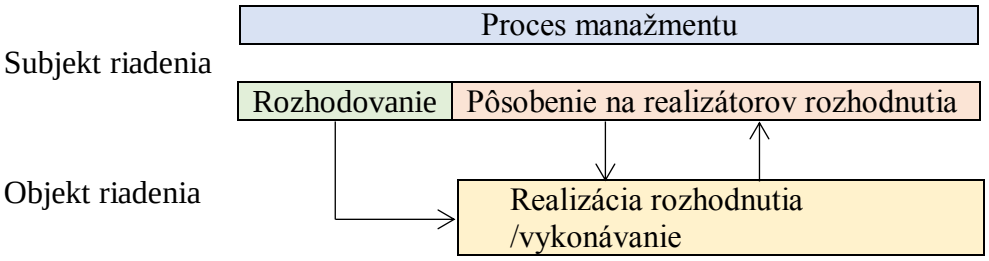
Rozhodnutia predstavujú ***hlavný produkt riadiaceho systému***, prijímajú sa na všetkých úrovniach a vo všetkých organizáciách. Prostredníctvom rozhodnutí sa ovplyvňuje smerovanie a činnosť a tým aj efektívnosť fungovania organizácie.

V každej organizácii sa uskutočňuje veľký počet rozhodovacích procesov v rôznych oblastiach činnosti. Všetky možno považovať za jediný vnútorne závislý celok, ktorý možno nazvať **systémom rozhodovacích procesov.** Rozhodovacie procesy sa navzájom prekrývajú, časovo na seba nadväzujú a vytvárajú hierarchicky usporiadanú štruktúru. Do tohto systému rozhodovacích procesov patrí aj ***rozhodovanie pri riešení otázok bezpečnosti v organizácii.***

Rozhodovanie tvorí iba časť, nie celý proces manažmentu. Podľa toho môžeme proces rozhodovania rozdeliť na dve hlavné časti:

- ***na prípravu a prijatie rozhodnutia (rozhodovanie),***
- ***na zabezpečovanie realizácie rozhodnutia***.

Pri zabezpečovaní **realizácie rozhodnutia** subjekt riadenia pôsobí na objekt riadenia, na realizátorov rozhodnutia, s cieľom dosiahnuť jeho kvalitné a včasné splnenie. V tejto fáze dochádza k medzipersonálnym vzťahom, keď subjekt riadenia kontroluje a vedie objekt riadenia (obr. 2).



Obr. 2 Proces manažmentu z hľadiska rozhodovania (zdroj Sedlák, 1997)

Pre rozhodovanie sú charakteristické tieto znaky:

a) existuje možnosť výberu medzi niekoľkými variantmi riešenia,
b) výber riešenia je vedomý, zakladá sa na myšlienkovom procese,
c) výber je cieľavedomý, zameriava sa na dosiahnutie jedného cieľa (alebo niekoľko cieľov),
d) výber riešenia sa uskutočňuje podľa určitých kritérií, čomu zodpovedá aj výber prostriedkov na dosiahnutie cieľa (cieľov),
e) výber sa končí konaním, to znamená, že rozhodnutie vyvolá reťaz cieľavedomých činností, ktoré smerujú k jeho uskutočneniu a vedú k výsledkom.

Bezpečnostný manažment z hľadiska rozhodovania

Bezpečnostný manažment z hľadiska rozhodovania sa chápe ako ***postupné riešenie problémov bezpečnosti*** v príslušnom dynamickom systéme, ako ***postupnosť vzájomne súvisiacich rozhodnutí a zabezpečovanie ich realizácie*** pri tvorbe bezpečného prostredia v organizácii.

Rozhodovací proces sa uplatňuje ***vo všetkých etapách procesu manažérstva bezpečnosti*** organizácie. V praxi manažérstva bezpečnosti záleží na kvalite, rýchlosti a efektivite rozhodovacieho procesu. Od jeho výsledkov sa odvíja úroveň bezpečnosti osôb, majetku a životného prostredia organizácie.

K základným prvkom rozhodovacieho procesu v manažérstve bezpečnosti patria:

1. **cieľ rozhodovania** – teda budúci stav bezpečnosti, ktorý má byť dosiahnutý, aby sa mohli úspešne splniť stanovené ciele,
2. **subjekt rozhodovania** – jednotlivec či skupina, ktorá rozhoduje (prijíma rozhodnutie),
3. **objekt rozhodovania** – predstavovaný časťou objektívnej reality, ktorej sa rozhodnutie týka – bezpečnosť, riziká, osoby, majetok a životné prostredie,
4. **možné alternatívy (možnosti)** – najmä na riešenie spôsobov zaobchádzania s rizikom,
5. **kritériá rozhodovania** – sú určené na posúdenie vhodnosti jednotlivých variantov.

Rozhodovacie procesy v manažérstve bezpečnosti sú v bežnom živote každodenné, často sú to rutinné úkony, niekedy životne ťažké situácie. Rozhodovací proces je súbor psychických procesov riadiacich funkcionárov a bezpečnostných pracovníkov, ktorých zmyslom je vyhľadať optimálny cieľ bezpečnosti a vhodný spôsob konania pre dosiahnutie, zaistenie a zlepšovanie bezpečnosti.

Medzi **najdôležitejšie rozhodovania** v bezpečnostnom manažmente patrí najmä rozhodovanie o:

- prijatí záväzku a zodpovednosti manažmentu za bezpečnosť organizácie,
- stanovení kritérií rizika,
- rizikách, ktoré vyžadujú zaobchádzanie a ich prioritách pre zaobchádzanie – rozhodnutie o rizikách, ktoré vyžadujú zaobchádzanie,
- výbere jedného alebo viacerých spôsobov zaobchádzania s rizikom a spôsobe ich zavedenia,

- tom, či zvyšková úroveň rizika je prípustná,
- rozsahu Systému manažérstva bezpečnosti (SMB),
- vyčlenení zdrojov na činnosť SMB a dosiahnutie bezpečnostných cieľov organizácie,
- obsahu a rozsahu bezpečnostnej politiky na zabezpečenie prijateľnej úrovne bezpečnosti organizácie,
- rolí, zodpovedností a právomocí v manažérstve bezpečnosti,
- vyhlásení havarijného stavu v prípade incidentu, havárie a pod.

3.3.3 Funkčná charakteristika bezpečnostného manažmentu

Funkčná charakteristika manažmentu je najznámejšia a najviac rozvinutá charakteristika, pri ktorej sa bezpečnostný manažment vníma z pohľadu činností, ktoré plní.

Manažérska funkcia je:
- relatívne oddelená, pomerne samostatná, ale ucelená časť pracovnej činnosti v riadení,
- fáza riadenia s vymedzeným účelovým určením, v ktorej sa prejavuje určitý spôsob cieľavedome zameraného vplyvu (pôsobenia) subjektu riadenia na riadený objekt.

Na začiatku 20. storočia Henry Fayol uviedol, že všetci manažéri vykonávajú päť manažérskych funkcií: *plánovanie, organizovanie, prikazovanie, koordinovanie a kontrolu.* Luther Gulick a Lindal Urwick v 30. rokoch manažérske funkcie usporiadali do tzv. systému POSDCORB: *plánovanie (Planning), organizovanie (Organizing), personálne zabezpečenie (Staffing), prikazovanie (Directing), koordinácia (Coordinating), evidencia (Reporting) a vytváranie rozpočtov (Budgeting).* V polovici 50. rokov sa uvádzali najmä funkcie: *plánovanie, organizovanie, personalistika, prikazovanie a kontrola.*

Manažérske funkcie majú univerzálny charakter, vyskytujú sa v každej organizácii, sú veľmi integrované a platia pre akékoľvek procesy riadenia, prejavujú sa teda aj v procesoch **manažérstva bezpečnosti** v organizácii.

Funkcie manažmentu sa prelínajú celým **procesom manažérstva bezpečnosti**. Sú charakteristické pre riadiaci systém na ktoromkoľvek stupni riadenia, musí ich uplatňovať každý subjekt manažérstva bezpečnosti. Je samozrejmé, že na jednotlivých stupňoch riadenia nadobúdajú tieto funkcie iný význam.

Pracovný proces i proces manažérstva bezpečnosti majú ***cyklický charakter*** a skladajú sa z jednotlivých fáz (etáp):

a) Etapa prípravná – prípravné, predbežné riadenie: jadrom je ***plánovanie***, k nemu v podstate patrí aj ***organizovanie***,

b) Etapa realizačná – priebežné riadenie (riadenie v užšom slova zmysle), za ktoré sa niekedy považuje *regulovanie*, inokedy ***vedenie ľudí***,

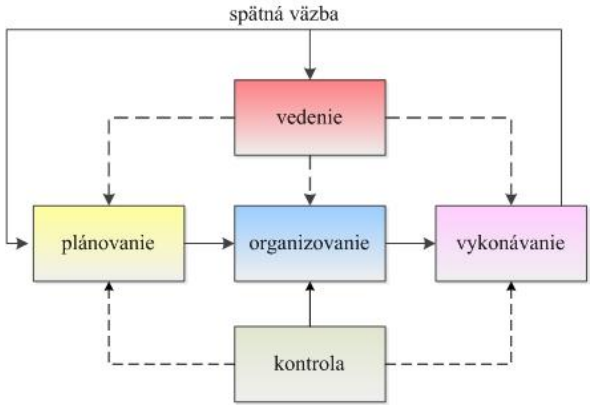
c) Etapa hodnotiaca – ***kontrola***, ktorá jednak preniká celou výkonnou fázou (priebežná kontrola) a jednak sa uskutočňuje na konci výkonnej fázy a slúži na celkové porovnávanie výsledku práce s cieľom a úlohami.

Proces manažérstva bezpečnosti organizácie odkazuje na aktivity v organizácii zložené z týchto hlavných manažérskych funkcií:

1. **plánovanie** (*planning)* – ako proces prípravy budúcich činností, stanovuje bezpečnostné ciele, postupy, zdroje, termíny a zodpovednosť za ich dosiahnutie,
2. **organizovanie** (*organizing)* – proces tvorby podmienok pre realizáciu rozhodnutia a plánu, určuje ľuďom ako majú a v akej štruktúre zaisťovať plánované úlohy na dosiahnutie bezpečnosti,

3. **personálne zaistenie** *(staffing*) – výber a rozmiestňovanie bezpečnostných pracovníkov, školenie, hodnotenie ich schopností, zručností, napĺňanie profesijných a kvalifikačných predpokladov disponibilných ľudských zdrojov,
4. **vedenie ľudí** *(leading)* – priame a nepriame usmerňovanie, komunikácia, koordinácia, stimulovanie a motivovanie jednotlivcov i kolektívov, aby včas a efektívne plnili určené úlohy bezpečnosti,
5. **kontrola** *(controlling)* – proces sledovania, rozboru, hodnotenia kvality SMB a stavu bezpečnosti a prijímania záverov v súvislosti s odchýlkami medzi plánom a realizáciou.

Plánovanie určuje výsledky, aké chce organizácia dosiahnuť. Organizovanie špecifikuje, ako chce organizácia dosiahnuť naplánované výsledky. Kontrolovanie určuje, či tieto výsledky dosiahli. Vedenie vykonávané manažérom ich spája dovedna (obr. 3).



Obr. 3 Proces manažmentu ako sústava manažérskych funkcií (zdroj Sedlák, 1997)

Na jednotlivé fázy manažmentu a manažérske funkcie nemožno pozerať ako na úplne izolované a jednoznačne oddelené. V reálnom prostredí sa ani vždy nevyskytujú v takom logickom usporiadaní, ako na obrázku. Všetky funkcie sú navzájom späté, úzko súvisia, dopĺňajú sa a navzájom sa prekrývajú. Jednotný cyklus tvoria iba v nerozlučnej jednote, vo vzájomnom pôsobení. Systémová závislosť a podmienenosť jednotlivých riadiacich činností dáva samotnému riadeniu charakter nepretržite sa uskutočňujúceho procesu.

Táto charakteristika definuje manažérstvo bezpečnosti ako proces postupne sa striedajúcich etáp, tzv. cyklus riadenia. Všetky jeho funkcie by mali byť vo vzájomnej rovnováhe, ak z nejakého dôvodu nastane degenerácia niektorej z nich, naruší sa obvykle celý proces manažmentu. Z tohto hľadiska je **manažérstvo bezpečnosti *cyklický, relatívne uzavretý proces, ktorý sa začína vytýčením cieľov a končí sa ich splnením a dosiahnutím určitého výsledku.*** Na základe informácií o výsledkoch sa vytyčujú nové úlohy, určuje sa nový cieľ a cyklus začína odznova.

Plánovanie v bezpečnostnom manažmente

Plánovanie v bezpečnostnom manažmente je manažérska aktivita zameraná na budúci vývoj bezpečnosti v organizácii, ktorá určuje čo a ako má byť dosiahnuté, čo sa má stať a nie iba ako reakcia na to, čo sa stalo. Plánovanie rozhoduje o blízkej i vzdialenejšej budúcnosti bezpečnosti organizácie. Plánovanie je východiskom pre všetky ďalšie manažérske funkcie. Je to proces, v ktorom manažéri stanovujú budúce ciele organizácie a tvoria plány na ich dosiahnutie. Tento proces umožňuje porovnať reálne výsledky so stanovenými cieľmi a v prípade potreby korekcie prijať potrebné opatrenia.

Táto etapa zdôrazňuje vysokú dôležitosť manažérstva rizika. Keď organizácia zvýrazní ***riziká***, je potrebné stanoviť, ako sa budú riešiť prostredníctvom plánovania. Fázy plánova-

nia musia ukázať, ***aké, koho, ako a kedy riziká*** musia byť riešené. Tento prístup nahrádza preventívne kroky a neskôr znižuje potrebu nápravných opatrení. Osobitný dôraz sa tiež kladie na ***ciele SMB***, ktoré by mali byť ***merateľné, monitorované, oznamované, zladené*** s politikou manažérstva bezpečnosti a v prípade potreby ***aktualizované***.

Etapa plánovania v bezpečnostnom manažmente obsahuje určenie:

1. **Činností, ktoré sa zaoberajú rizikami a príležitosťami**.
2. **Cieľov manažérstva bezpečnosti a spôsobov ich dosiahnutia.**
3. **Bezpečnostných cieľov organizácie a spôsobov ich dosiahnutia.**

Plánovací proces vychádza z **pochopenia súčasného stavu bezpečnosti organizácie, jej externých a interných súvislostí** a zahŕňa:

a) **plánovanie manažérstva rizika, stanovenie cieľov manažérstva rizika** a postupov na ich dosiahnutie, ich integrovania a zavedenia do procesov SMB a spôsobov vyhodnocovania efektívnosti týchto postupov – ***Plán manažérstva rizika, Plán zaobchádzania s rizikami, Plán komunikácie v manažérstve rizika,***
b) **plánovanie bezpečnostných cieľov organizácie**, spôsobov a kritérií (bezpečnostných noriem) na ich vyhodnocovanie, spôsobov kontroly ich dosahovania a určenie zodpovedností a termínov na ich dosiahnutie – ***Celková bezpečnostná politika,***
c) **plánovanie bezpečnostných cieľov v podsektoroch bezpečnostného sektora organizácie,** spôsobov a kritérií (bezpečnostných noriem) na ich vyhodnocovanie, spôsobov kontroly ich dosahovania a určenie zodpovedností a termínov na ich dosiahnutie **– *Systémové bezpečnostné politiky, Bezpečnostný plán ochrany objektu*** (OUS), ***Bezpečnostný plán*** (kritická infraštruktúra), pre iné objekty ***Bezpečnostný plán ochrany objektu*** alebo ***Projekt ochrany objektu, Bezpečnostný projekt (smernica) na ochranu osobných údajov v informačnom systéme, Plán manažérstva incidentov, Akčný plán (programy) environmentálneho manažérstva,***
d) **plánovanie vytvorenia a implementácie SMB** – ***Plán implementácie SMB***,
e) **plánovanie zdrojov** na zavedenie SMB, manažérstvo rizika a dosiahnutie bezpečnostných cieľov organizácie,
f) **plánovanie odozvy na núdzové (krízové) situácie – *Bezpečnostná správa*, *Havarijný plán, , Plán ochrany obyvateľstva, Plán kontinuity činností, Plán obnovy činností a pod.***

Na **určovanie vlastností cieľov v období plánovania** je vhodné použiť metódu SMART – *(Doran, 1981),* ktorá je klasikou v oblasti plánovania:

- **S –** SPECIFIC – špecifické, konkrétne ciele,
- **M –** MEASURABLE – merateľné ciele, na konci cieľa musíme vedieť zistiť, či sme uspeli alebo naopak – nedosiahli, čo sme chceli, k tomu nám pomáhajú konkrétne kvalitatívne alebo kvantitatívne ukazovatele dosiahnutia cieľa,
- **A –** ACHIEVABLE/ ASSIGNABLE – dosiahnuteľné/určiť kto ich dosiahne,
- **R –** RELEVANT/REALISTIC **–** významné/realistické (vzhľadom k zdrojom),
- **T –** TIME SPECIFIC/TIME-RELATED – časovo špecifické/špecifikovať, kedy môže byť dosiahnutý výsledok.

Výsledkom plánovania je vytvorenie **plánov,** ktoré budú koordinovať a integrovať jednotlivé činnosti pri dosiahnutí, zaisťovaní a trvalom zlepšovaní stavu bezpečnosti. Plány sa v organizácii tvoria podľa hierarchie, ktorá zodpovedá jej organizačnej štruktúre. Plány majú obsahovať tieto **prvky plánovania**: ***ciele, činnosti na dosiahnutie cieľov (stratégie, taktiky), zdroje, termíny a zodpovednosti.***

Plány na každom stupni zohrávajú dvojakú úlohu – určujú ciele, ktoré majú byť dosiahnuté prostredníctvom plánov na nižšom stupni a následne sa samotné stávajú nástrojom

realizácie cieľov, určených plánom vyššieho stupňa. Postupom plánov zhora nadol sa zvyšuje ich konkrétnosť a podrobnosť a znižuje sa ich časový horizont.

Všeobecne sa uznávajú dva základné druhy plánov:

1. **Plány strategické**, ktoré sa orientujú na dosahovanie všeobecných cieľov organizácie, plnenie jej základných cieľov, určujú príčinu prečo a za akým účelom daná spoločnosť existuje.
2. **Plány operačné**, ktoré vytyčujú spôsoby, ako uskutočniť strategické plány, delia sa na:
   - ***jednorazové plány***, ktoré sa vypracúvajú vzhľadom na dosiahnutie čiastkových, konkrétnych cieľov a po ich dosiahnutí strácajú svoj význam,
   - ***trvale platné plány***, ktoré určujú normalizovaný spôsob postupu pri opakovaných a predvídaných situáciách.

Vzhľadom na **časové horizonty a funkcie**, ktoré plnia pri riadení organizácie sa plány delia na:

a) **dlhodobé:** určujú základnú stratégiu spoločnosti, plánovanie sa viaže na zásadné ciele a prostriedky spoločnosti;
b) **strednodobé:** určujú množstvo a druhy nákladov, manipuláciu s množstvom výdavkov, efektívnosť využitia ľudských zdrojov, materiálov a kapitálu;
c) **krátkodobé**: sú orientované na jednotlivé činnosti, potrebné na dosahovanie cieľov.

Organizovanie

Organizovanie prestavuje cieľavedomú činnosť, ktorej konečným cieľom je usporiadať prvky v systéme, ich aktivity, koordináciu a kontrolu tak, aby prispeli maximálnou mierou k dosiahnutiu stanovených cieľov systému. Ide o vymedzenie:

- **právomoci a zodpovednosti** *jednotlivých skupín a jednotlivcov,*
- **vzájomných vzťahov medzi nimi,** čiže tvorbu *organizácie*.

Zmyslom organizovania je vytvoriť podmienky na koordináciu úsilia pomocou vytvárania:

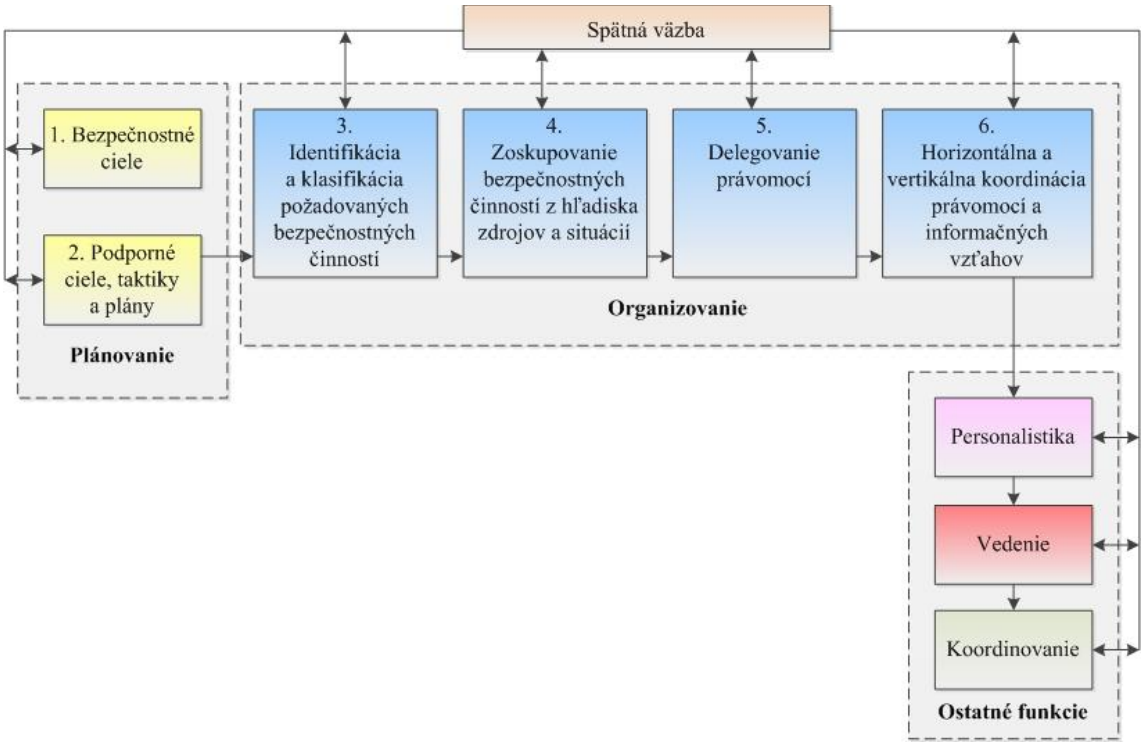
a) **štruktúry procesov** (deľba práce a koordinácia špecializácií) – pod týmto pojmom sa chápe cieľavedomé úsilie manažérov zamerané na určenie spôsobov, ako majú pracovníci vykonávať dané práce a ich koordináciu. Organizovanie je **procesom deľby práce** medzi jej jednotlivými skupinami a jednotlivcami v organizácii.
b) **štruktúry vzťahov *medzi úlohami, právomocami a zodpovednosťou*** (stabilná organizačná štruktúra) – vyjadruje pomerne stabilnú **organizačnú štruktúru,** niekedy označovanú ako kostra organizácie, ktorej poskytuje základňu na jej fungovanie. Organizačná štruktúra vytvára prostredie pre pracovný výkon, čím sa stáva nástrojom manažmentu a nie je samoúčelná.

Podstata organizovania v bezpečnostnom manažmente spočíva v tvorbe vykonávacej **organizačnej štruktúry SMB organizácie**, ktorá vytvorí vhodné prostredie pre efektívnu spoluprácu jednotlivcov a skupín pri dosahovaní stanovených bezpečnostných cieľov.

Organizovanie plní svoje poslanie v integrácii s ďalšími manažérskymi funkciami, najmä s personálnym zaistením (obr. 4). Niektorí autori v rámci organizovania uvádzajú aj ***výber a rozmiestňovanie bezpečnostných pracovníkov, hodnotenie ich schopností, zručností, napĺňania profesijných a kvalifikačných predpokladov (personalistika).***

Keď je zvolený ***cieľ*** v budovaní bezpečnosti a v **pláne** sú uvedené ***alternatívy postupov***, ako ho dosiahnuť, je treba zvolený postup efektívne zorganizovať. Ďalšie úlohy manažmentu na dosiahnutie bezpečnostných cieľov a splnenie plánov sú:

- **rozmiestniť a usporiadať všetky disponibilné zdroje** organizácie tak, aby existovala reálna šanca vytýčené ciele zvoleným postupom a v stanovenom časovom horizonte dosiahnuť,
- **rozhodnúť, kto práce vykoná**, čiže určiť, ktorí ľudia (jednotlivci, skupiny) majú prácu urobiť na efektívne dosiahnutie bezpečnostných cieľov organizácie,
- **dosiahnuť koordinované úsilie týchto ľudí** navrhnutím usporiadania vzťahov medzi jednotlivými ***úlohami a právomocami***, určiť ***povinnosti a zodpovednosti***, kto má podávať hlásenia, kto je za čo zodpovedný (organizačná štruktúra).



Obr. 4 Vzťah organizovania a ďalších manažérskych funkcií

Personálne zaistenie

Personalistika spočíva ***v personálnom zabezpečení riadiacich a riadených procesov,*** ktoré sú vyjadrené v organizačnej štruktúre. Je to proces získavania potrebných a schopných pracovníkov, ich adaptácie v novom prostredí a udržania na zvolenej pozícii. Využíva poznatky z oblasti psychológie, sociológie, práva a organizácie práce.

Vedenie ľudí

Vedenie ľudí predstavuje činnosť manažérov zameranú na cieľavedomé ovplyvňovanie (motiváciu, stimuláciu, koordináciu, komunikáciu, usmernenie) jednotlivcov i kolektívov, pri ktorej sa vedúci s využitím svojej právomoci usiluje o dobrovoľnú, ochotnú účasť podriadených na dosahovaní bezpečnostných cieľov. Vedenie ľudí obsahuje najmä ***prikazovanie (velenie), motivovanie, komunikovanie a riešenie konfliktov*** a nemožno ho chápať ako časovo ohraničenú činnosť, pretože ľudia sa musia viesť nepretržite.

Ide o ***určenie noriem, zásad a pravidiel dodržiavania bezpečnosti*** pre organizáciu, skupiny a jednotlivcov a tiež ovplyvnenie ľudí týmito normami, napríklad *stanovenie strategického smeru (vízia, hodnoty, úloha a / alebo zámery) a metód organizovaného uplatňovania vedenia na dosiahnutie stanoveného smeru.*

Vedenie ľudí charakterizujú najmä:

- používané **štýly vedenia** (spôsob prikazovania),
- **motivácia** podriadených, ovplyvňovanie jednotlivcov alebo tímov,
- **komunikácia** – výber najvhodnejších komunikačných ciest,
- **zvládanie problémov**, spôsobených správaním zamestnancov,
- **práca tímov.**

Kontrola

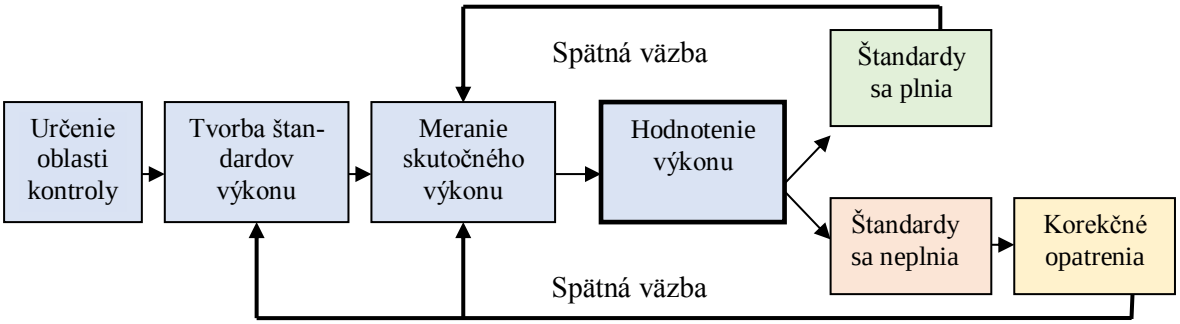
Kontrolou a kontrolovaním sa zaoberá manažment na každom stupni organizačnej štruktúry. Kontrola završuje celkový proces manažmentu, je úzko spojená s plánovaním, rozhodovaním a organizovaním. Bez hodnotenia a kontroly dosahovaných výsledkov nie je možné posúdiť účinnosť a úspešnosť ostatných funkcií bezpečnostného manažéra a tým ani účinnosť a úspešnosť jeho manažérskej práce a činnosti celého systému manažérstva bezpečnosti.

Hlavným cieľom kontroly v bezpečnostnom manažmente je **zmerať a zhodnotiť kvantitu a kvalitu:**

- **činnosti SMB,**
- **dodržiavania bezpečnostných opatrení v organizácii.**

V podstate ide o porovnanie kvantity a kvality stanovených zámerov (cieľov, plánov, noriem, štandardov, kritérií) s dosiahnutými výsledkami. Zjednodušene **– kontrola porovnáva bezpečnostné ciele organizácie** (plány, štandardy, normy, rozpočty, limity) **a ciele SMB s dosiahnutým výsledkom**.

Poslaním kontroly je včas a hospodárne zistiť odchýlky v procese manažérstva bezpečnosti, predstavujúce rozdiely medzi zámerom a jeho realizáciou, ktoré môžu byť pozitívne alebo negatívne, ich rozbor a na základe toho prijatie záverov a ich uplatnenie. Kontrola znamená kritické zhodnotenie reality vzhľadom na riadiace zámery, určenie, či sa dosiahla zhoda vo vývoji kontrolovanej reality voči špecifikovaným požiadavkám (obr. 5).



Obr. 5 Fázy kontrolného procesu (zdroj Sedlák, 1997)

Kontrolný proces v organizácii je rovnaký, bez ohľadu, čo je jeho objektom a kto ho vykonáva, platí teda aj pre **manažérstvo bezpečnosti**. Kontrola obsahuje zber, vyhodnocovanie a porovnávanie informácií o stave bezpečnosti s plánovanými cieľmi, určenými v bezpečnostnej politike, ktoré spätnou väzbou umožňuje napravovať chybné, či nedostatočné plnenie úloh a určiť, v čom možno aktivity členov organizácie zlepšiť. Postupný **súbor spätnej väzby** predstavuje monitorovanie a regulovanie (korekcia, koordinácia) systémov, procesov a primeraných štruktúr v súlade so stanovenými cieľmi.

Ako **štandardy** sa požívajú najmä ***normy bezpečnosti*** stanovené v ***medzinárodných a národných štandardoch ISO, zákonoch, vyhláškach a nariadeniach*** pre jednotlivé oblasti

a zložky bezpečnostného sektora. V prípade nežiaducich odchýlok reality od plánovaného stavu je treba ***prijať príslušné opatrenia na odstránenie týchto odchýlok.***

V procese manažérstva bezpečnosti sa v etape kontroly vykonáva:

a) interný bezpečnostný audit,

b) porovnávanie skutočného vývoja bezpečnosti s plánmi, ktoré boli stanovené rozhodnutím riadiaceho subjektu, zisťovať eventuálne odchýlky skutočného vývoja od určeného vývoja, ako aj príčiny týchto odchýlok,

c) vyvodzovanie záverov pre ďalšie rozhodovanie o manažérstve bezpečnosti s cieľom:
- odstrániť nežiaduce odchýlky a ich príčiny alebo zmeniť pôvodné rozhodnutie, ak sa v priebehu kontroly ukáže ako nesprávne,
- využiť poznatky o príčinách pozitívnych odchýlok,

d) prijímanie preventívnych a nápravných opatrení,

e) posudzovanie zhody a nezhody právnych predpisov,

f) vedenie záznamov o bezpečnosti a manažérstve rizika.

Na vykonanie kontroly musia byť splnené nasledujúce podmienky:
- subjekt má dostatok bezpečnostných informácií na kontrolovanie,
- existujú objektívne kritériá na hodnotenie úrovne bezpečnosti,
- subjekt je schopný zisťovať príčiny odchýlok od požadovaných stavov bezpečnosti.

Poznatky a závery z kontrolnej činnosti sa využívajú v analytickej a hodnotiacej činnosti riadiacich pracovníkov a zároveň slúžia ako podklady pre aktualizáciu a inováciu bezpečnostného systému.

3.4 LITERATÚRA

BELAN, Ľ. – BELAN, L. [2004]: *Manažment a jeho charakteristika z rozhodovacieho a informačného hľadiska.* Liptovský Mikuláš. Vojenská akadémia v Liptovskom Mikuláši, Fakulta pozemného vojska. ISBN: 80 -8040-223-X.

BELAN, Ľ. – BELAN, L. [2004]: *Manažérske funkcie.* Liptovský Mikuláš. Vojenská akadémia v Liptovskom Mikuláši, Fakulta pozemného vojska. ISBN: 80 -8040-224-8.

BELAN, Ľ. a kol. [2011]: *Manažment.* Liptovský Mikuláš. Akadémia ozbrojených síl gen. M. R. Štefánika. ISBN: 978-80-8040-434-5.

DORAN, G. T. [1981]: *There's a S.M.A.R.T. way to write management's goals and objectives*. Management Review (AMA FORUM) 70 (11).

FAYOL, H. [1931]: *Zásady správy všeobecné a správy podniků.* Praha. Orbis.

GULICK, L. – URWICK, L. [1993]: *Papers on the Science of Administration.* New York: Institute of Public Administration. Weihrich Management Praha. Victoria Publishing. ISBN 80-85605-45-7.

MINTZBERG, H. [1973]: *The Nature of Managerial Work (Povaha manažérskej práce)*. New York. Harper & Row.

SEDLÁK, M. [1997]: *Manažment.* 1. vydanie. Bratislava. Elita. ISBN: 80-8044-015-8.

SENNEWALD, Ch. A. [2003]: *Effective Security Management. Fourth edition.* Elsevier-Science (USA), ISBN 0-7506-7454-7.

SIMON, H. A. [1946]: *Proverbs of Administration*. Public Administration Review, *6* (1), pp. 53–67.

4 MANAŽÉRSTVO BEZPEČNOSTI ORGANIZÁCIE

Manažérstvo bezpečnosti je *prvkom zodpovednosti vrcholového manažmentu organizácie,* **ktorá prijala zámer *riadiť vlastnú bezpečnosť ako neoddeliteľnú súčasť celkovej činnosti*, na čo stanovila** *bezpečnostnú politiku.*

Bezpečnosť je takto deklarovaná ako ***najvyššia priorita organizácie.*** Na vytvorenie bezpečnosti, ako základnej hodnoty organizácie, je nutné, aby sa bezpečnosť stala neoddeliteľnou súčasťou Strategického plánu organizácie. Stanovené strategické ciele organizácie sa ďalej rozpracujú v taktickom plánovaní do najdôležitejších oblastí činností organizácie.

Manažérstvo bezpečnosti je definované ako ***systém a metódy riadenia bezpečnosti*** organizácie. Je to sústavný, opakujúci sa súbor navzájom previazaných aktivít, ktorých cieľom je:

- zaistiť ***bezpečnosť všetkých činností*** na dosahovanie cieľov,
- ***zamedziť bezpečnostným rizikám*** spôsobiť poškodenie zdravia, straty životov, majetkové škody a škody na životnom prostredí.

Medzi **základné zásady manažérstva bezpečnosti** patria:

a) Záväzok k zásade zachovania bezpečnosti – zahŕňa vyhlásenie o záväzku vrcholového vedenia organizácie, aby sa zabezpečilo, že všetky činnosti v organizácii budú spĺňať ciele bezpečnosti. Bezpečnosť je deklarovaná ako najvyššia priorita organizácie. Tieto ciele sa dosiahnu prostredníctvom ďalšieho záväzku organizácie **poskytnúť potrebné zdroje pre efektívne manažérstvo bezpečnosti.**

b) Zodpovednosť za bezpečnosť – zásada vyžaduje, aby všetci zamestnanci organizácie mali ***osobnú zodpovednosť*** za svoje konanie vzhľadom na bezpečnosť a že vedenie je zodpovedné za bezpečné činnosti organizácie.

c) Plánovanie bezpečnosti – je dôležitým predpokladom pre aktívnu implementáciu SMB. To umožňuje ***stanovenie cieľov bezpečnosti*** organizácie a vytvorenie ***stratégií, prístupov a konkrétnych plánov*** pre dosiahnutie prijateľnej úrovne bezpečnosti všetkých činností.

d) Stanovenie bezpečnostných štandardov – zásada zabezpečuje zhodu s platnými požiadavkami bezpečnostných predpisov a úsilie organizácie prijať medzinárodne uznávané bezpečnostné normy a osvedčené postupy v oblasti riadenia bezpečnosti.

e) Riadenie bezpečnosti – potvrdzuje ho záväzok na jasný a efektívny prístup k bezpečnosti prostredníctvom formálnej štruktúry SMB, zahŕňa aspekty vytvorenia organizačnej štruktúry SMB a vyžaduje, aby bezpečnostná štruktúra riadenia as tým súvisiace úlohy a zodpovednosti boli stanovené v rámci organizácie.

f) Dosiahnutie bezpečnosti – zásada vyžaduje, aby používané prostriedky, procesy, postupy a zdroje (napr. posúdenie rizika, hlásenie udalostí a vyšetrovanie atď.) zabezpečili vysokú úroveň bezpečnostných cieľov organizácie a ich dosahovanie.

g) Zaistenie bezpečnosti – zahŕňa prostriedky, procesy, postupy a zdroje na preukázanie zhody s bezpečnostnými normami a uvádza požadované dôkazy o dosiahnutej úrovni bezpečnosti (napríklad preskúmanie bezpečnosti, záznamy o bezpečnosti atď.). Metódy zaistenia bezpečnosti organizácia používa aj na podporu identifikácie otázok bezpečnosti a vytvorenie odporúčaní pre zvýšenie úrovne bezpečnosti.

h) Propagácia bezpečnosti – zásada zabezpečuje, že poučenia o bezpečnosti a kľúčové bezpečnostné informácie sa šíria v celej organizácii, podporuje sa komunikácia o otázkach bezpečnosti a zmeny systematicky smerujú k zlepšeniu bezpečnosti.

4.1 SYSTÉMOVÝ PRÍSTUP K MANAŽÉRSTVU BEZPEČNOSTI

Základom pre chápanie manažérstva bezpečnosti organizácie je ***systémové myslenie.*** Aplikácia **systémového prístupu** k manažérstvu bezpečnosti umožňuje integrovať do tohto celostného pohľadu rôzne poznatky v záujme skvalitňovania bezpečnostného manažmentu organizácie.

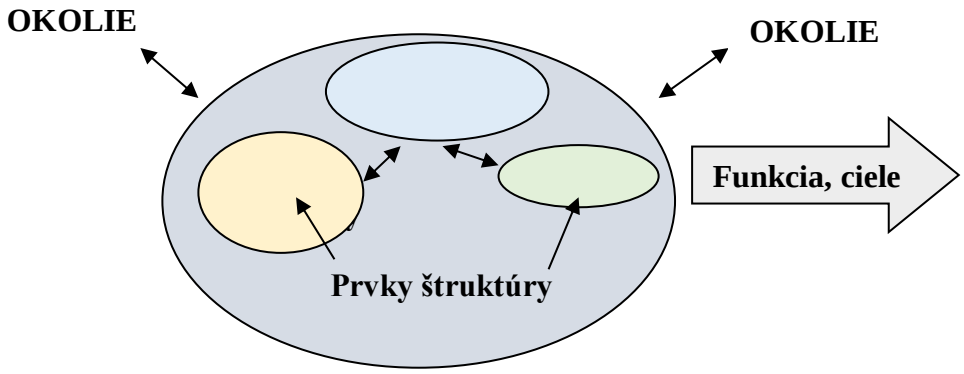
Teória systémov sa zameriava v prvom rade na štúdium všeobecných abstraktných systémov, je založená na interdisciplinárnom chápaní pojmu systém. Využíva rozsiahly logicko–matematický aparát výskumu formálnych systémov a zjednocuje aspekty správania sa rôznych druhov systémov. Vyvíja metódy pre definovanie a skúmanie systémov, ich zložiek, okolia, pre zobrazenie, analýzu a optimalizáciu štruktúry systémov a pre analýzu a optimalizáciu ich správania. Základy teórie systémov vypracoval Ludwig von Bertalanffy.

Systém

Systém je ***súbor*** vnútorne prepojených a vnútorne závislých častí, ktoré tvoria jednotný celok. Je to účelovo definovaná neprázdna množina **prvkov** a **väzieb medzi nimi**, pričom obe množiny určujú ***vlastnosti celku (systému),*** usporiadaný komplex vzájomne pôsobiacich prvkov, spolu s ich vlastnosťami a stanoveným účelom.

Základné znaky každého systému sú (obr. 6):

- **cieľ,** alebo sústava cieľov,
- **funkcia** – t. j. ***účel*** systému, hlavný dôvod, prečo systém vznikol,
- **štruktúra** – množina ***prvkov*** či podsystémov, ich ***hierarchia a usporiadanie*** (kompozícia), interné ***vzťahy medzi nimi*** (informačné väzby),
- **interakcia s prvkami okolia.**



Obr. 6 Organizácia ako systém (zdroj Míka, 2006)

Systém je charakterizovaný svojou **štruktúrou a správaním *a ich vzájomným prepojením.*** **Štruktúra systému** vyjadruje:

- ***množinu prvkov systému***,
- ich ***hierarchické usporiadanie*** a ***vzájomné vzťahy***.

Štruktúru systému možno znázorniť:

- ***slovným popisom*** – len pri malých a prehľadných systémoch, inak sa stráca prehľadnosť a názornosť,
- ***graficky*** – do určitej veľkosti systému je to najprehľadnejšie a najnázornejšie vyjadrenie,
- ***tabuľkou väzieb*** – využíva výhody maticového spôsobu zápisu prvkov a väzieb medzi nimi, stĺpce matice označujú prvky ovládané, riadky ovládajúce.
- ***všeobecným tvarom***.

Správanie sa systému je ***prejav reakcií systému na podnety z vonkajšieho prostredia***, ktoré vyjadrujú charakteristické vlastnosti systému ako celku v jeho vzťahu k okoliu.

Prvok systému je ***základná stavebná časť systému***. Prvky vytvárajú vnútorné členenie, ktoré už nie je možné ďalej členiť, ale z hľadiska zákonitostí vnútornej stavby zachovávajú všeobecnú vlastnosť systému. Systém je zároveň aj prvkom iného systému na nižšej rozlišovacej úrovni. Prvkom môže byť človek, činnosť, podnik, symbol a pod.

Pre definovanie prvku je dôležitá **rozlišovacia úroveň,** ktorá predstavuje „hĺbku" pohľadu do systému. Ak sa zvýši rozlišovacia úroveň, môže sa prvok stať systémom, ak sa zníži, môže sa systém stať prvkom. Pre systém „podnik" je prvkom „závod", pre systém „závod" sú prvkami „strediská", pre systém „stredisko" sú prvkami „pracovníci". Prvok systému je na zvolenej rozlišovacej úrovni nedeliteľná časť celku, ktorého štruktúru nemôžeme alebo nechceme rozlišovať.

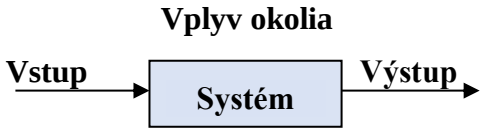
Väzba je vzájomné spojenie (interakcia) medzi dvoma prvkami systému navzájom alebo medzi prvkom systému a prvkom okolia systému. Väzby sa rozlišujú podľa:

- ***formy:*** priame, spätné, sériové, paralelné, zvodné, rozvodné, otvorené, uzavreté, kombinované atď.,
- ***obsahu:*** hmotno-energetické, informačné, organizačné atď.

Vzťah systému a okolia

Systém má zvláštnu jednotu a súdržnosť s okolím. **Okolie systému** predstavuje ***množina prvkov, ktoré nie sú súčasťou systému, ale majú väzby s jeho prvkami.*** Niektoré z týchto prvkov okolia sú ***v priamej väzbe so systémom***. Tieto prvky tvoria podstatné okolie systému, čo je účelovo definovaná množina prvkov okolia, ktoré sú v bezprostrednom styku s hraničnými prvkami systému prostredníctvom vstupných a výstupných väzieb systému.

Vzťah systému k okoliu je vytváraný prostredníctvom vstupov a výstupov (obr. 7).



Obr. 7 Základný model systému

Vstupom systému sa rozumie väzba, prostredníctvom ktorej ***okolie pôsobí na systém (podnet)***. **Podnet** je stav vstupu do systému, charakterizujúci dané pôsobenie okolia na systém v určitom časovom okamihu.

Výstup systému je vonkajšia väzba systému, ktorou ***systém pôsobí na okolie (odozva).*** **Odozva** je stav výstupu zo systému (jeho reakcia) charakterizujúca dané pôsobenie na okolie, vyvolané podnetom na vstupe systému.

4.2 RIADENIE SYSTÉMOV

Riadenie systémov je proces účelného pôsobenia, ktorého cieľom je ***prevod dynamického systému z jedného stavu do stavu iného***, takým spôsobom zo súhrnu jeho správania, aby sa zabezpečilo čo najefektívnejšie ***dosiahnutie cieľa***. Z toho vyplývajú podmienky, pri ktorých dochádza k riadeniu systému *(Míka, 2006)*.

Pre **efektívne riadenie** je potrebné počínať si tak, aby sa ***ciele dosahovali za:***

- ***čo najkratší čas,***
- ***s minimálnymi nákladmi,***
- ***ale v požadovanom stupni kvality.***

V súčasnosti je možné formulovať nasledujúce **hlavné zásady riadenia** *(Allan a kol., 2003):*

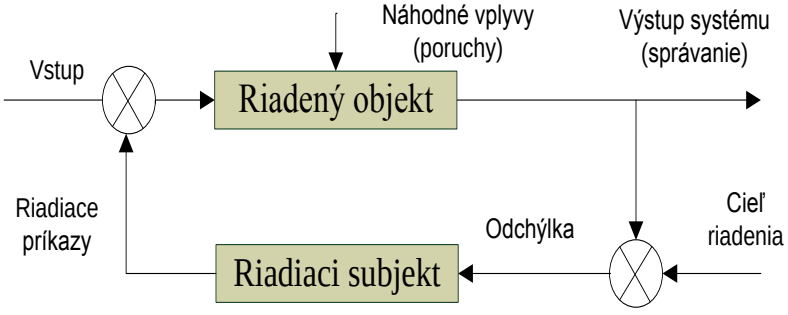
- **Objektívnosť** – spočíva v rešpektovaní skutočných možností a konkrétneho stavu vývoja spoločnosti a systému.
- **Konkrétnosť** – pojednáva o skutočnosti, že riadiť je možné len na základe objektívnych informácií, skúmať, ako sa dané informácie menia v čase a vyvodzovať pre prax vhodné závery.
- **Optimálnosť** – hovorí o tom, že pri dosahovaní cieľov by sme mali vynaložiť čo najmenej finančných prostriedkov, ľudskej energie a splniť cieľ riadenia v najkratšom čase.
- **Stimulácia** – bez vhodného odmeňovania nie je možné dosiahnuť vysokú efektivitu pracovníkov.
- **Jeden zodpovedný vedúci** – skupina alebo kolektív sa majú podriadiť jednému vedúcemu, ktorému prislúchajú riadiace funkcie, týmto sa odstraňuje tzv. kolektívna nezodpovednosť.

4.2.1 Riadiaci a riadený systém ako organická jednota

Každý sociálno-ekonomický objekt predstavujúci **systém, sa skladá z dvoch navzájom spojených podsystémov**, ktoré v určitých reláciách pokladáme za systémy, ktorými sú:

a) riadiaci podsystém, resp. systém – subjekt riadenia,
b) riadený podsystém, resp. systém – objekt riadenia.

Zjednodušene možno vo všeobecnosti každý systém riadenia znázorniť schémou podľa obr. 8.



Obr. 8 Základná schéma riadenia

Základný cyklus riadenia potom bude prebiehať takto:

- **od riadiaceho subjektu** prichádzajú do **riadeného objektu** určité veličiny – ***vstupy a riadiace príkazy***,
- úlohou **riadeného objektu** je podľa stanoveného cieľa riadenia ***transformovať tieto vstupy a príkazy na požadované výstupy,***

- na správanie sa systému pritom okrem jeho vstupov pôsobia aj **náhodné vplyvy** (jeho okolie), ktoré riadiaci subjekt nie je schopný ovplyvniť.

Výstupy – reálne správanie sa systému je potrebné sledovať a porovnávať so stanoveným cieľom riadenia. Ak sa reálne správanie sa systému odlišuje od požadovaného, teda od cieľa riadenia, riadiaci subjekt túto odchýlku vyhodnotí a vydá riadiace príkazy na ovplyvnenie správania sa systému, najčastejšie zmenou vstupov.

Riadiaci a riadený podsystém (systém) spolu tvoria organickú jednotu. Každý z nich má svoje funkcie a jeden voči druhému plní špecifické úlohy. Ich rozlíšenie a vymedzenie v sociálno-ekonomickom objekte nie je z rozličných príčin jednoduché a jednoznačné.

Pojem riadiaci systém sa geneticky viaže na technickú sféru, riadiace a riadené časti sú v nej fyzicky i priestorovo jednoznačne rozlíšené.

Polarizácia riadiaceho a riadeného systému v sociálno-ekonomických objektoch je relatívna a poznamenaná účelom skúmania, rozlišovacou úrovňou a pod. Deliaca čiara je veľmi „nejasná“, lebo sám riadiaci systém musí byť neustále organizovaný a riadený, najmä preto, že na priebehu riadenia participuje aj samotný riadený systém. Sociálne systémy, akými sú aj podniky (firmy, spoločnosti), sú zložitými systémami a budujú sa na základe hierarchického viacstupňového princípu. Každý stupeň či úroveň riadenia riadi jeho nižší stupeň, ale súčasne je riadený, je objektom riadenia zo strany vyššieho stupňa riadenia.

Hranica medzi riadiacim a riadeným systémom nie je celkom jasná aj preto, prípadne sa komplikuje tým, že pracovník môže byť súčasťou objektu riadenia, ale súčasne i riadiaceho systému, napríklad členom valného zhromaždenia, predstavenstva alebo iných orgánov riadenia. Riadenie v sociálno-ekonomickom objekte pôsobí nielen na tú jeho časť, ktorú pokladáme za riadený systém, ale aj na tú, ktorá je riadiacim systémom, pretože musí riadiť i sám seba, aby správne fungoval a zabezpečoval vlastný rozvoj. Objektom riadenia, teda tým, na čo riadenie pôsobí, je príslušný objekt (systém) ako celok, napr. celý podnik.

Systém je **v neustálej interakcii** s externým prostredím a **úlohou manažérov** je ***koordinovať a hodnotiť činnosti systému vo vzájomných vzťahoch interného a externého prostredia*** v záujme podpory vzniku synergických efektov. Systémový prístup umožňuje skúmať vzájomnú závislosť interného a externého prostredia.

4.2.2 Riadiaci systém

Riadiaci systém je možné pri určitom zjednodušení charakterizovať ako **tú časť systému, ktorej poslaním je riadiť jeho riadený systém**. Vypracúva **strategický zámer, víziu, poslanie a ciele celého systému** a **usmerňuje jeho činnosti** tak, aby sa rozvíjali v súlade s nimi. Riadiaci systém ***zabezpečuje racionálny, efektívny vývoj každého riadeného systému***, preto má voči nemu aktívnu úlohu.

Riadiaci systém sociálno-ekonomických objektov možno charakterizovať z dvoch hľadísk, ako:
- ***riadiaci systém v statike*** **– štruktúra riadiaceho systému (štruktúra manažérstva),**
- ***riadiaci systém v dynamike*** **– proces riadenia ako činnosť (proces manažérstva).**

Riadiaci systém teda tvorí organickú jednotu **štruktúry riadenia** a **procesu riadenia.** Medzi nimi existuje vzťah obsahu (činnosť) a formy (organizačná štruktúra).

Štruktúra riadiaceho systému

Štruktúrou riadiaceho systému vo všeobecnosti sa rozumie ***skladba jeho prvkov a väzieb a vzájomné pôsobenie medzi nimi.*** Štruktúra systému podmieňuje celostnosť fungovania prvkov. Podľa zvoleného hľadiska členenia prvkov je možné definovať rozličné štruktú-

ry riadiaceho systému, napríklad ***personálnu, technickú, útvarovú a pod.*** Základom je ***organizačná štruktúra riadiaceho systému či systému manažérstva*** (príp. len jednoducho organizačná štruktúra).

Prostredníctvom organizačnej štruktúry sa riadiaci systém inštitucionalizuje. Jeho hlavným prvkom sú **ľudia,** ktorí – organizovaní v orgánoch, útvaroch a na pracoviskách – rozličným spôsobom pôsobia na riadený systém podniku.

Organizačná štruktúra ako výsledok organizovania, t. j. procesu jej tvorby a zdokonaľovania, vytvára základňu na uskutočňovanie ***procesu riadenia*** (manažmentu) ***výkonných činností,*** zjednodušuje a uľahčuje jeho priebeh. Je teda dôležitým faktorom, ktorý ***významne ovplyvňuje efektívnosť riadenia i efektívnosť výkonných činností.***

Proces riadenia

Proces riadenia (proces manažmentu) ***je riadiaci systém v dynamike***, uskutočňovaný v rámci určitej organizačnej štruktúry. Je to ***fungovanie a činnosť orgánov, útvarov, pracovníkov vykonávajúcich riadenie*** v súlade s cieľmi a zásadami manažmentu a používajúcich rozličné metódy a prostriedky na jeho uskutočňovanie. V porovnaní s organizačnou štruktúrou má proces riadenia tvorivejší charakter, je v ňom viac umenia.

Ide o **integráciu rôznych činností riadiaceho systému**, ktoré **vykonáva *v rámci jednotlivých manažérskych funkcií, pri rozhodovaní a v informačnom procese.***

Proces riadenia (manažérstva) zahŕňa najmä:

- ***prácu s informáciami,***
- ***rozhodovanie,***
- ***vykonávanie manažérskych funkcií*** *(plánovanie, organizovanie, personálne zaistenie, vedenie ľudí, kontrola).*

V porovnaní s organizačnou štruktúrou má proces riadenia tvorivejší charakter, je v ňom viac umenia. Má tiež pevné zásady, podľa ktorých sa riadi.

4.2.3 Riadený systém

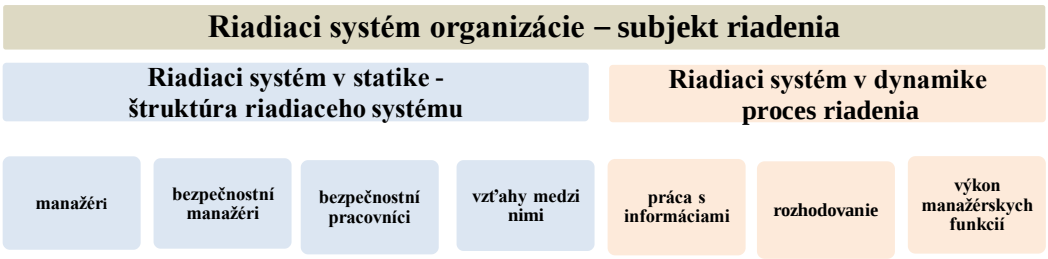
Základ sociálne-ekonomických systémov tvorí ***riadený systém***, lebo sa v ňom uskutočňuje hlavná činnosť – procesy, ktoré zodpovedajú účelu, pre ktorý je tento systém určený a bez ktorých žiadny z nich nemôže existovať.

Z inštitucionálneho hľadiska patria medzi **objekty riadenia** jednotlivé organizačné celky organizácie:

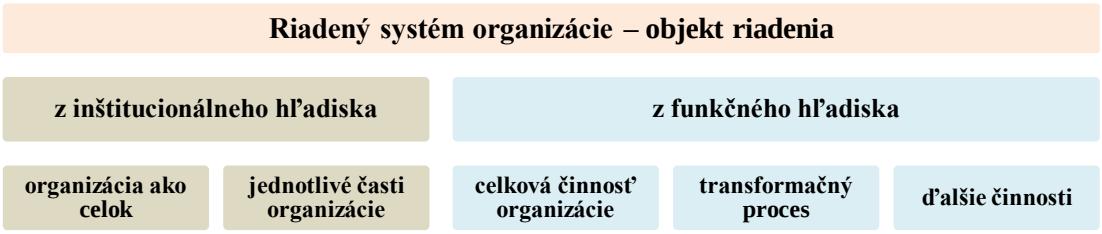
- ***organizácia ako celok***
- ***jej jednotlivé časti*** (závody, útvary, prevádzky, dielne).

Z funkčného hľadiska (z pohľadu vykonávaných činností v organizácii) sú **objektmi riadenia:**

- ***celková činnosť organizácie podľa jej účelu,***
- ***zamestnanci, ktorí vykonávajú hlavné činnosti umožňujúce vyrábať produkty alebo produkujúce služby –*** *obstarávanie výrobných faktorov; zhotovovanie, čiže výroba produktov; predaj, resp. odbyt a pod.,*
- ***zamestnanci, ktorí vykonávajú podporné činnosti –*** *napr. personalistika, administratíva, údržba a servis objektov a technologických zariadení, energetické zabezpečenie, informačné zabezpečenie, výskum a vývoj, a iné činnosti.*



Obr. 9 Riadiaci systém organizácie



Obr. 10 Riadený systém organizácie

4.3 ORGANIZÁCIA AKO SYSTÉM

Vymedzenie pojmu organizácia je rozličné. Míka za najdôležitejšie interpretácie pojmu organizácia, za jeho základné významy pokladá **organizáciu ako** *(Míka, 2006)*:

1. **reálny objekt** – ako ***systém sociálnych prvkov, vzťahov a cieľov*** v inštitucionalizovanej materializovanej podobe (podnik, škola, bezpečnostný zbor, vojenská jednotka, záujmová organizácia, politická strana a pod.)
2. **proces organizovania** – ako ***usporiadaný priebeh procesov,*** ako ***ľudská činnosť*** – napr. organizácia záchranných prác, organizácia evakuácie ohrozenej dediny a pod.,
3. **štruktúra objektu** – ako ***vnútorné usporiadanie***, výsledok ľudskej činnosti zameranej na účelovo optimálne usporiadanie štruktúry prvkov, vzťahov a funkcií.

Každá organizácia je určitým **prostredím** pre fungovanie jej jednotlivých prvkov. V ňom existujú a fungujú jednotlivé organizačné prvky, v ňom existujú relatívne stabilné, formálne i neformálne väzby medzi nimi. Ani organizácia neexistuje izolovane od vplyvov mnohých prvkov okolitého prostredia.

Organizácia je na základe systémového prístupu chápaná ako určitý previazaný ***systém*** **prvkov, vzťahov a funkcií,** ktoré sledujú základný zmysel existencie systému, jeho hlavné ciele. Takto chápaný systém funguje ***v širšom vonkajšom prostredí,*** s ktorého prvkami je v interakcii.

Prvky z organizačného hľadiska predstavujú ***štruktúrne jednotky podľa rozlišovacej úrovne a miery zoskupenia*** – závody, výrobne, jej úseky, odbory, sekcie, oddelenia či ďalšie útvary.

Vzťahy medzi prvkami predstavujú ***informačné väzby***, ktoré pomáhajú realizovať nevyhnutné informačné prepojenie na zladené plnenie vykonávaných procesov, je to:

- informačný prenos výsledkov rozhodovania po hierarchickej úrovni,
- výmena informácii v rámci vzájomnej spolupráce jednotlivých prvkov,
- a poskytovanie informácii o splnení úlohy.

Funkcie z funkčného hľadiska predstavujú ***hlavné a podporné činnosti*** vykonávané v organizácii.

Hlavné činnosti sú charakterizované ako dominantné funkčné procesy, uskutočňované v organizácii jednotlivcom, skupinou jednotlivcov, organizáciou, za účelom ***splnenia základnej primárnej funkcie***. Podľa účelu, pre ktorý je podnikateľská organizácia vytvorená, sem možno zaradiť: *riadenie, obstarávanie, skladovanie, financovanie, výrobu, služby, odbyt, doprava, marketing a iné dôležité činnosti, ktoré sú pre organizáciu nosné a ktoré prinášajú podnikateľským subjektom najvyššiu pridanú hodnotu*.

Podporné činnosti sa vykonávajú za účelom ***zaistenia efektívneho fungovania hlavných činností***. V organizácii zahŕňajú najmä oblasti: *personalistika (riadenie ľudských zdrojov), investovanie, výskum a vývoj, všeobecná administratíva, správa majetku, riadenie prevádzky, údržba a servis objektov a technologických zariadení, verejné obstarávanie, energetické zabezpečenie, informatika a telekomunikácie, revízie a odborné prehliadky, havarijná služba a iné činnosti.*

Z hľadiska manažmentu chápeme organizáciu ako riadenú sociálnu sústavu, cieľavedome usporiadaný, konkrétny reálny, relatívne uzavretý **celok,** ***vytvorený za účelom plnenia stanovených cieľov.***

Základnými podmienkami pre riadenie **organizácie ako systému** je existencia organizovaného systému s týmito vlastnosťami:

- má aspoň dva prvky (riadiaci a riadený),
- má uzavretú spätnú väzbu (priamu alebo nepriamu),
- riadiaci prvok je schopný samostatne riadiť riadený (výkonný) prvok, kontrolovať jeho výkon a rozhodovať o jeho ďalšom vývoji – je teda schopný určovať podmienky stability a realizovať cieľové správanie,
- schopnosť riadiaceho prvku určiť cieľ správania, alebo realizovať cieľ vložený do systému,
- určitá miera voľnosti riadiaceho prvku pri výbere, vzhľadom na dosiahnutie daného cieľa správania a právo obmedziť mieru voľnosti pomocou rozhodnutia,
- existencia dostatočného množstva vstupov medzi okolím a systémom, to znamená, že do systému musí vstupovať dostatok informácií potrebných na rozhodnutie o riadiacom pôsobení v čase.

Na základe tohto chápania je **organizácia** považovaná za ***systém vzájomne prepojených a závislých činností (subsystémov) vytvárajúcich jednotný celok***. Tento systém môže byť súčasťou (podsystémom) iného systému vyššieho stupňa. Každý stupeň, či úroveň riadenia riadi svoj nižší stupeň, ale súčasne je riadený vyšším stupňom riadenia.

Organizačná štruktúra

Pre úspešné riadenie si organizácia musí vytvoriť správnu organizačnú štruktúru. P. F. Drucker prehlásil: *„Najjednoduchšia organizačná štruktúra, ktorá plní svoje poslanie, je to najlepšie. Čím jednoduchšia je štruktúra, tým menej je toho, čo môže ísť zle"(Drucker, 1994).*

Organizačná štruktúra je ***vnútorná štruktúra prvkov organizácie*** – t. j. útvarov, pracovísk a ***vzťahov medzi nimi.*** Niekedy sa označuje aj ako **architektúra** (obr. 11). Jej úlohou je organizačne vymedziť základné prvky organizačného celku a definovať vzťahy medzi nimi. Cieľom je vytvárať podmienky pre účinné riadenie.

Organizačná štruktúra organizácie závisí od jej ***účelu, veľkosti, rozsahu, členitosti, spôsobu deľby práce, deľby právomocí a zodpovednosti.*** Musí zohľadňovať svoje prostredie, nemôže byť nikdy statická, čiže musí vychádzať vždy z danej situácie, tak, aby bola efektívna.

Organizačná štruktúra ako výsledok organizovania vytvára základňu na uskutočňovanie **procesu riadenia výkonných (operačných, prevádzkových) činností, *zjednodušuje a uľahčuje jeho priebeh.*** Je teda dôležitým faktorom, ktorý výrazne ovplyvňuje efektívnosť riadenia i efektívnosť výkonných činností.

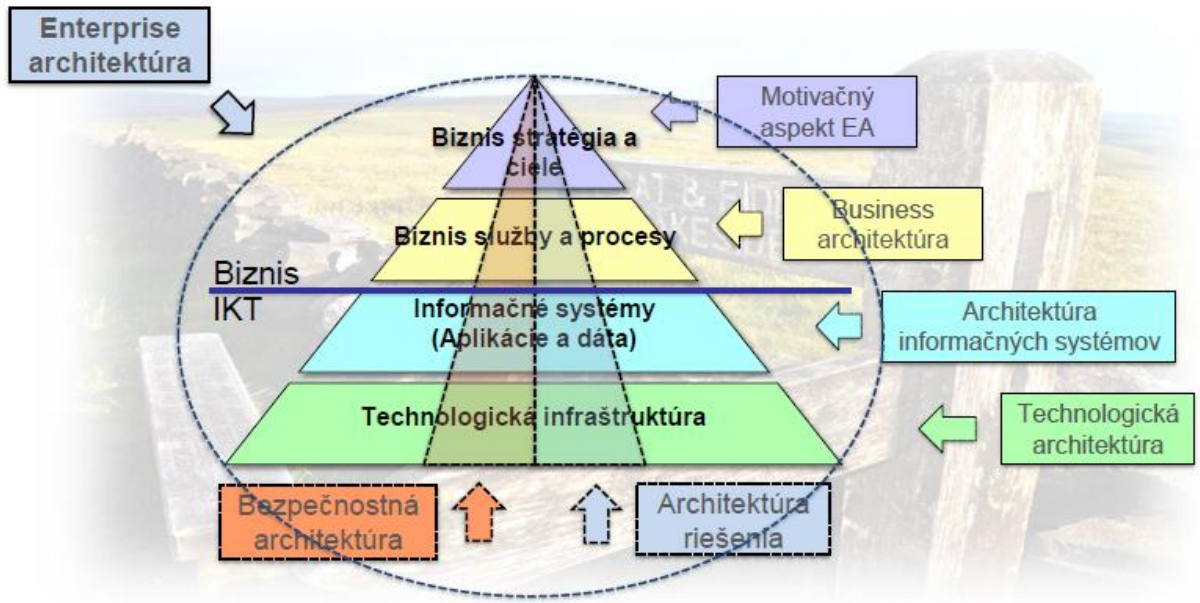
Štruktúra organizácie má byť podľa Senewalda vytvorená **podľa určitej logickej schémy,** ktorá zahrnie nielen všetky ***primárne (hlavné) činnosti*** *(core business),* ale aj všetky ***sekundárne (podporné) činnosti*** *(Senewald, 2003).*

Formálny systém vzťahov v rámci organizácie umožňuje ***diferencovať a zároveň aj integrovať činnosti a pracovníkov***, vykonávajúcich tieto činnosti do jedného celku. Môžeme je preto chápať ako **formu usporiadania procesu deľby práce** pre racionálne zabezpečenie určitého potrebného počtu riadiacich a výkonných činností:

- stanovenie ***úloh*** a ***povinností, právomoci a zodpovednosti*** vedúcim a zamestnancom,
- stanovenie a usporiadanie ***všetkých činností***,
- zaistenie deľby práce podľa ***špecializovaných činností,***
- preskupenie činností s cieľom ***zladenosti a efektívnosti***,
- ***koordinovanie*** činností ľudí, úloh a formálnych vzťahov,
- zabezpečenie efektívneho ***informačného systému.***

Podľa Míku sa väčšina autorov zhoduje na dôležitosti takých **zásad usporiadania organizácie,** ako sú *(Míka, 2006):*

- **Zameranie na ciele** predstavuje všeobecnú zásadu riadenia, lebo cieľ je hlavný dôvod vzniku organizácie, základný hlavný cieľ je východiskom pre čiastkové vedľajšie ciele. Je dôležité dať do súladu definované ciele organizácie s funkciou jednotlivých štruktúr a s vymedzením formálnych vzťahov medzi nimi.
- **Špecializácia a koordinácia** znamená, že sa v organizácii vytvárajú špecializované pracoviská s nárokmi na špeciálnu pripravenosť, ale aj na odbornú pružnosť, flexibilnosť. Usporiadanie organizácie musí umožňovať kooperáciu a koordináciu špecializovaných štruktúr.
- **Celistvosť a jedinečnosť** vyjadruje to, že každá organizácia vystupuje voči okoliu, voči verejnosti, ako jeden subjekt (právna subjektivita), jedinečnosť spočíva v špecifickosti, vo vnútornom zložení, vo vzťahoch, v kultúre organizácie, ale napr. aj v kvalite výrobkov a pod.
- **Komunikácia** znamená, že organizácia musí umožňovať naplnenie komunikačných potrieb organizácie, umožniť fungovanie potrebných informačných tokov a zabezpečiť napĺňanie informačných potrieb manažmentu (prijímať a odovzdávať vybrané informácie).
- **Zásada delegovania** znamená umožnenie posunutia plnenia úlohy a zodpovednosti za jej splnenie na nižšie články, na toho pracovníka, ktorý je k tomu najviac spôsobilý.



Obr. 11 Štruktúra organizácie (zdroj Architektonická kancelária verejnej správy, 2015)

4.4 BEZPEČNOSTNÁ FUNKCIA ORGANIZÁCIE

Veľmi dôležitou podpornou činnosťou v organizácii je **zaisťovanie jej bezpečnosti.** V súčasnosti sa **bezpečnostná funkcia organizácie** vníma ako dvojsmerná:

a) z hľadiska bezpečnosti pre organizáciu:
- schopnosť odolávať vonkajším rizikám, napr. bezpečnosť priestorov a objektov, bezpečnosť osôb a majetku,
- schopnosť odolávať vnútorným rizikám, napr. bezpečnosť práce, informačná bezpečnosť, bezpečnosť prevádzky a pod.,

b) z hľadiska bezpečnosti okolia, v ktorom funguje – schopnosť zabrániť ohrozeniu bezpečnosti vonkajšieho prostredia (napr. priemyselnými haváriami, emisiami, odpadom a pod.).

Z uvedených dôvodov by sa pri projektovaní štruktúry organizácie mala rešpektovať skutočnosť, že pre jej fungovanie má zaistenie bezpečnosti vysoký význam nielen z pohľadu celej organizácie a jej jednotlivých zamestnancov *(Mesároš, 2007),* ale aj zo strany zainteresovaných účastníkov a širokého okolia.

Na bezpečnostnú funkciu podniku upozorňoval už Henry Fayol

Každá organizácia by mala medzi **prvky celkovej organizačnej štruktúry** zaradiť aj ***štruktúry manažérstva bezpečnosti.***

Prvky manažérstva bezpečnosti sa vytvárajú na:
- centrálne riadenie bezpečnosti,
- riadenie bezpečnosti v podsektoroch bezpečnostného sektora organizácie,

Štruktúra manažérstva bezpečnosti organizácie by mala riešiť najmä tieto ***podsektory bezpečnostného sektora organizácie:***
- bezpečnosť osôb,
- bezpečnosť objektov a chránených priestorov s utajovanými skutočnosťami,
- bezpečnosť objektov s inými aktívami,
- bezpečnosť pred požiarmi – *požiarna ochrana,*
- bezpečnosť práce – *BOZP, bezpečnosť technických zariadení a hygiena práce (pracovné prostredie),*
- bezpečnosť prevádzkových činností – *technicko-prevádzkovú bezpečnosť, bezpečnosť kontinuity činností (BCM), predchádzanie závažným priemyselným haváriám,*
- protipožiarnu bezpečnosť,
- počítačovú bezpečnosť – *bezpečnosť informačných a komunikačných technológií,*,
- informačnú bezpečnosť – *bezpečnosť informačných systémov, bezpečnosť dôležitých informácií, ochrana utajovaných skutočností, ochrana osobných údajov a rôznych druhov tajomstva,*
- bezpečnosť pred podvodmi a zneužitím,
- bezpečnosť vnútorného poriadku a riešenie incidentov,
- bezpečnosť vnútorného i vonkajšieho životného prostredia,
- ďalšie špecifické druhy bezpečnosti.

Pri koncipovaní organizačnej štruktúry je treba pamätať aj na ***zložky, ktoré sa podieľajú na kreovaní bezpečnosti,*** napr.:
- tvorbou rôznych ***bezpečnostných dokumentov***, napr. plánov, smerníc, režimových opatrení, a pod.,
- svojou pripravenosťou ich v prípade potreby realizovať – ***havarijné tímy, záchranné tímy,***

- vykonávaním ***manažérstva rizika***,
- ***školením bezpečnostných pracovníkov a zamestnancov*** na zvládanie núdzových situácií a kríz rôzneho charakteru,
- ***inými bezpečnostnými činnosťami***.

Organizačná štruktúra manažérstva bezpečnosti sa obvykle vytvára v závislosti na veľkosti organizácie a jej aktív.

V **menších organizáciách** sa obvykle venuje bezpečnosti menej bezpečnostných pracovníkov, pre ktorých sa obvykle vytvára

BEZPEČNOSTNÝ PROGRAM.

Bezpečnostný program má umožniť dosiahnutie prijateľnej úrovne bezpečnosti – predstavuje integrovaný súbor pravidiel a aktivít, zameraných na dosahovanie bezpečnosti v dôležitých činnostiach. Zahŕňa najmä bezpečnostné opatrenia, ktoré vyplývajú z európskych a slovenských bezpečnostných právnych noriem. Okrem toho môže obsahovať aj opatrenia pre špecifické bezpečnostné oblasti, napr. *hlásenie incidentov, bezpečnostné vyšetrovanie, bezpečnostné audity, podpora bezpečnosti* atď.

Vo **väčších a zložitejších organizáciách** je na realizáciu bezpečnostných činností potrebné venovať väčšiu pozornosť, vyšší počet bezpečnostných pracovníkov a vyššie náklady. Organizácie sa musia zamerať nielen na opatrenia, vyplývajúce z právnych štandardov, ale musia vytvoriť podmienky pre bezpečnosť vo všetkých oblastiach činnosti. Na plnenie týchto úloh sa vyžaduje ucelený

SYSTÉM MANAŽÉRSTVA BEZPEČNOSTI.

4.4.1 Centralizované a decentralizované manažérstvo bezpečnosti

V závislosti na druhu a veľkosti organizácie môže byť manažérstvo bezpečnosti v organizácii:

- centralizované,
- decentralizované.

Centralizácia znamená ***sústreďovanie rozhodovacej právomoci vo vrcholovom manažmente*** organizácie, spôsob vykonávania moci, riadenia a kontroly z jedného centra. Centralizované manažérstvo bezpečnosti sa vytvára obvykle vo väčších a zložitejších organizáciách (najmä v zahraničí). Tvorí ho ucelená štruktúra, od vrcholového manažmentu až po výkonný manažment a všetkých zamestnancov. Vrcholový manažment rozhoduje nielen o strategických otázkach, ale aj o väčšine taktických a operatívnych otázok riadenia.

Výkonné činnosti manažérstva bezpečnosti organizácie zastrešuje **bezpečnostný manažér,** zaradený do vrcholového manažmentu, ktorému sú podriadení všetci ***bezpečnostní pracovníci*** a ***bezpečnostné štruktúry*** vo všetkých oblastiach bezpečnostného sektora.

Decentralizácia znamená ***umiestnenie rozhodovacej právomoci na rôznych úrovniach manažmentu*** organizácie – rozdelenie moci a prenášanie práv, povinností, zodpovedností a oprávnení na iné zložky (delegovanie). Decentralizované manažérstvo bezpečnosti sa vytvára spravidla v menších a menej zložitých organizáciách. Systém je tiež riadený vrcholovým manažmentom, značná časť rozhodovacích právomocí však patrí iným riadiacim orgánom, ako to funguje v mnohých organizáciách v podmienkach SR. Týmto sa podstatne rozširuje počet pracovníkov, ktorí sa zúčastňujú na riadení, na druhej strane si každá zložka riadi len svoju oblasť a nekoordinuje svoju činnosť s ďalšími bezpečnostnými pracovníkmi, ani s bezpečnostným manažérom.

Bezpečnostný manažér môže byť zaradený vo vrcholovom manažmente alebo je v podriadenosti personálneho (alebo iného) riaditeľa, ale ďalšia štruktúra bezpečnostných zložiek už nie je centralizovaná. Bezpečnostný manažér riadi priamo väčšinu bezpečnostných zložiek, niektoré však nie sú v jeho podriadenosti a pôsobia samostatne, napr. informačná bezpečnosť, BOZP, manažérstvo kontinuity činností a pod.

Absolútna centralizácia alebo decentralizácia neexistuje. Prejavujú sa tendencie smerom k jednej alebo druhej strane, pritom na všetkých stupňoch riadenia existujú v určitom rozsahu tak centralizácia, ako aj určitá samostatnosť nižších článkov riadenia pri riešení úloh.

Predpokladom efektívneho fungovania organizácie je zabezpečenie optimálnej deľby rozhodovacej právomoci, t. j. optimálna kombinácia jej centralizácie a decentralizácie. Nadmerná centralizácia vedie k byrokracii, prehnaná decentralizácia smeruje k anarchii. O tom, akú veľkú právomoc prideliť jednotlivým činnostiam a tým, ktorí tieto činnosti vykonávajú, rozhodujú manažéri.

Pri riešení vzťahu medzi centralizáciou a decentralizáciou manažérstva bezpečnosti v organizácii je treba brať do úvahy:

- dôsledne ***centralizovať využívanie všetkých informačných zdrojov*** a zabezpečiť prístup každého rozhodovacieho miesta k potrebným informáciám,
- ***rozhodnutie prijímať rýchlo a blízko zdroja informácií,***
- dodržať ***vyváženosť vydávaných úloh a právomocí***, ktoré vykonávanie úloh podmieňujú, ako aj ***zodpovedností,*** ktoré z nich vyplývajú,
- objasniť, ***ktoré rozhodovacie právomoci možno decentralizovať a ktoré musia ostať centralizované.***

Podľa toho možno **právomoci deliť na tie:**

- ktoré sa nemôžu decentralizovať a musia ostať centralizované,
- ktoré sa môžu úplne decentralizovať (delegovať),
- ktoré sa môžu čiastočne decentralizovať (delegovať).

Delegovať znamená zveriť moc (poveriť, splnomocniť) vybranému funkcionárovi, ale ponechať si konečnú zodpovednosť. Delegovanie šetrí čas vedúceho a rozvíja schopnosti podriadených. Sú oblasti, do ktorých by mal manažér začleniť každú úlohu:

- úlohy, ktoré má manažér plniť sám – hodnotenie pracovníkov, definovanie strategických cieľov,
- úlohy, ktoré väčšinou rieši manažér sám, ale môže ich delegovať – úlohy s cieľom podporiť rozvoj pracovníkov, alebo úlohy delegované v časovej tiesni,
- úlohy, ktoré by manažér mal delegovať – pracovníci majú pre ich riešenie kompetencie a kvalifikáciu,
- úlohy, ktoré jednoznačne musia byť delegované – základné úlohy potrebné pre fungovanie oddelenia, či firmy.

4.4.2 Manažérstvo bezpečnosti v súčasných organizáciách

Štátne a súkromné organizácie a inštitúcie majú v súčasnosti vo svojej organizačnej štruktúre začlenené niektoré útvary, ktoré riešia bezpečnosť, napr. útvary:

- krízového riadenia,
- bezpečnosti práce a ochrany zdravia,
- manažérstva rizika,
- manažérstva incidentov,
- požiarnej ochrany,
- ochrany osôb a objektov,

- informačnej bezpečnosti,
- zabezpečenia kontinuity všetkých činností, a ďalšie.

Tieto bezpečnostné útvary, najmä vo väčších organizáciách:

- môžu byť **stabilnými prvkami organizačnej štruktúry** (vlastné bezpečnostné služby, vlastné hasičské a iné záchranárske útvary a pod.),
- môžu sa **vytvárať z vyškolených vlastných zamestnancov,** napr. bezpečnostní technici a iní bezpečnostní pracovníci, alebo sa využijú **externé organizácie na základe zmluvy,** napr. fyzická ochrana osôb a objektov.

Zaradenie a názov týchto bezpečnostných zložiek a obsah ich činnosti je ***v kompetencii vrcholového manažmentu pri rešpektovaní príslušných zákonov***. Hlavný dôraz je pri tom potrebné položiť na vybudovanie **riadiacej zložky pre manažérstvo bezpečnosti.**

V súčasnosti sa v jednotlivých organizáciách bezpečnosť obvykle riadi decentralizovaným spôsobom v niekoľkých podsystémoch, ktoré majú oddelené riadenie. Najčastejšie sú jednotlivé súčasti bezpečnostného sektora organizácie v podriadenosti útvaru bezpečnosti a rôznych úsekov riadenia (obr. 12).

a) Útvar bezpečnosti vo vedení organizácie:
- bezpečnosť a ochrana zdravia pri práci,
- fyzická a režimová ochrana objektov a chránených priestorov,
- požiarna ochrana,
- ochrana životného prostredia,
- havarijná bezpečnosť,
- vyšetrovanie incidentov.

b) Personálny úsek – ochrana osobných údajov a citlivých údajov (OUS), personálne previerky.

c) Stavebný úsek – ochrana objektov (mechanické a technické prostriedky ochrany).

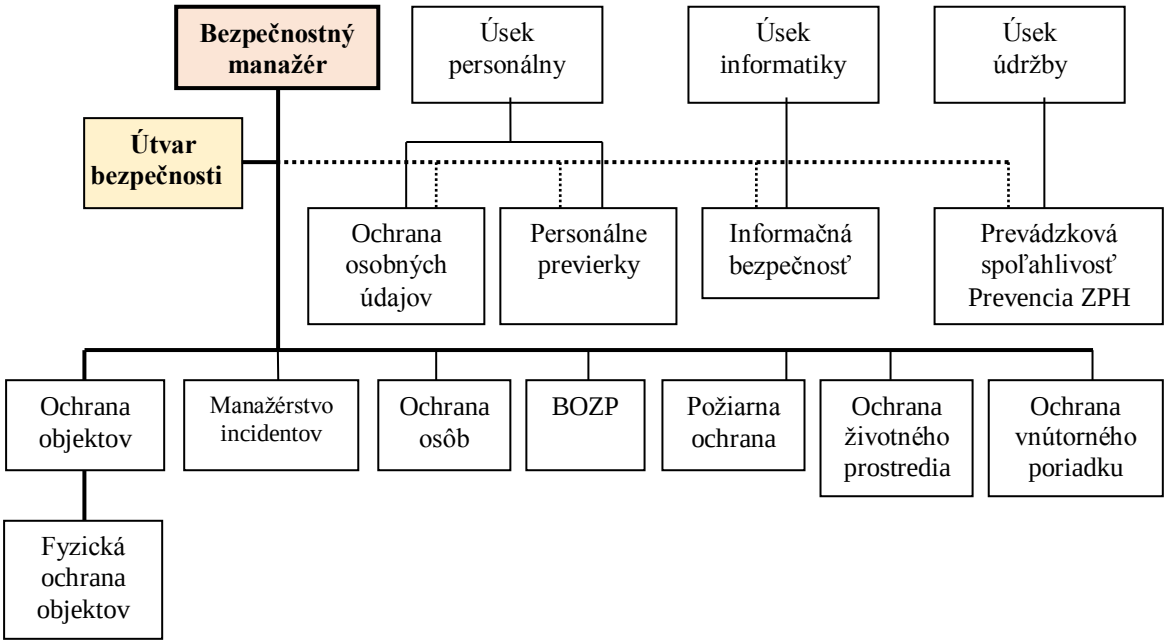
d) Úsek informatiky – ochrana IKT, informačná bezpečnosť.

e) Úsek údržby – technicko-prevádzková bezpečnosť, bezpečnosť technických zariadení.

Útvar bezpečnosti, podriadený bezpečnostnému manažérovi, by mal mať zverené zložky bezpečnostného sektora, ktoré prechádzajú celou organizáciou a vyžadujú jednotné vedenie. Ďalšie oblasti sú zatiaľ zverené do kompetencie jednotlivých funkčných úsekov.

V týchto súčastiach nie sú však zaradené niektoré zložky bezpečnosti, ako sú: vyšetrovanie, ochrana dôležitých osôb, ochrana vnútorného poriadku, vymáhanie pohľadávok a pod. Na základe tohto rozdelenia a doplnenia môže organizačná štruktúra SMB väčšej a zložitejšej organizácie mať podobu, uvedenú na obrázku. V menších organizáciách rozhodne vrcholový manažment, ako skombinuje rozdelenie všetkých úloh na menej pracovísk.

Bezpečnostný manažér osobne riadi hlavné sektory bezpečnosti a spolupracuje s odborníkmi personálneho úseku a úsekov informatiky a údržby na riadení ochrany osobných údajov, OUS, personálnej bezpečnosti, bezpečnosti IKT a prevádzkovej spoľahlivosti a technickej bezpečnosti.



Obr. 12 Možná organizačná štruktúra systému manažérstva bezpečnosti organizácie

4.5 PERSONÁLNE ZAISTENIE MANAŽÉRSTVA BEZPEČNOSTI

Na manažérstve bezpečnosti sa v organizáciách spoločne podieľajú manažéri a bezpečnostní manažéri. Je zrejmé, že vrcholoví a líniovímanažéri organizácie sa budú orientovať viac na riadenie procesov súvisiacich s jej hlavnými činnosťami (podnikateľským poslaním), víziou a cieľmi. Preto je pre **manažérstvo oblastí bezpečnostného sektora** potrebné, aby vo formálnej organizačnej štruktúre organizácie mali miesto i ***bezpečnostní špecialisti a bezpečnostní pracovníci***.

Týchto manažérov možno zaradiť do nasledujúcich **úrovní:**

a) vrcholový (top) manažment,
b) stredný manažment,
c) manažment prvej úrovne.

Prehľad jednotlivých manažérskych úrovní je uvedený v tab. 1.

Tab. 1 Prehľad manažérskych úrovní

	Manažment organizácie	Bezpečnostný manažment
1.	**Vrcholový (top) manažment** – napr. *riaditeľ organizácie* , riaditeľ závodu, sekretariát, riaditelia štábnych odborných útvarov: finančný riaditeľ, prevádzkový riaditeľ, výrobný riaditeľ, správca informačného systému personálny riaditeľ alebo riaditeľ ľudských zdrojov, technický riaditeľ, marketingový riaditeľ, podnikový právnik	Bezpečnostný manažér organizácie. Bezpečnostný správca informačného systému. Manažér BOZP a ochrany životného prostredia alebo Manažér BOZP, Environmentálny manažér. Prevádzkový bezpečnostný manažér Manažér Systému manažérstva kontinuity činností. Projektový bezpečnostný manažér
2.	**Stredný manažment:** líniovímanažéri vnútropodnikových útvarov (závodov, divízií a pod.), vedúci rôznych odborných útvarov (vývoja, výskumu, manažérstva rizík a pod.)	Bezpečnostní špecialisti: *Manažér rizík,* *Technik požiarnej ochrany,* *Veliteľ závodného hasičského zboru, útvaru,* *Autorizovaný bezpečnostný technik BOZP,* *funkcionári fyzickej ochrany*
3.	**Manažment prvej úrovne – základná úroveň manažmentu** líniovívedúci prvej úrovne (majstri)	Výkonní (poverení) pracovníci – *špecialista požiarnej ochrany, hasiči, bezpečnostní technici BOZP, príslušníci pracovnej zdravotnej služby, veliteľ zmeny fyzickej ochrany* a ďalší.

Vrcholoví manažéri

Hlavnú zodpovednosť za prihlásenie sa k manažérstvu bezpečnosti, bez ohľadu na veľkosť, druh či zložitosť organizácie, má jej **generálny riaditeľ** a **vrcholový manažment**.

Vrcholoví manažéri sú špičkoví vedúci pracovníci, ktorí usmerňujú a koordinujú činnosť organizácie ako celku. Sú nositeľmi strategického rozvoja, realizátormi dlhodobých zámerov a určujú vnútroorganizačný ekonomický režim. Medzi vrcholový manažment patrí aj vedúci pracovník, bezprostredne zodpovedný za stav bezpečnosti organizácie – **bezpečnostný manažér**.

Vrcholý manažment má predovšetkým vytvárať organizačnú ***klímu pre bezpečnosť,*** musí byť schopný vytvoriť a udržiavať ***bezpečné a spoľahlivé prostredie.*** Bez úprimného prijatia záväzku na bezpečnosť, bude manažérstvo bezpečnosti z veľkej časti neúčinné. Na pozi-

tívne posilnenie bezpečnostných činností manažment vyšle správu všetkým zamestnancom, že sa naozaj stará o bezpečnosť a oni by sa o to mali starať tiež.

Vrcholoví manažéri organizácii obvykle vytvárajú **riadiaci orgán bezpečnosti**, v ktorom sú zaradení najmä zástupcovia úsekov: finančného, prevádzky, výrobného, informačného, personálneho, technického, marketingového, právneho a pod. Názov tohto orgánu nie je stanovený, obvykle sa používajú výrazy: rada bezpečnosti, výbor bezpečnosti, kancelária bezpečnosti a pod. *(Security Board)*. Do riadiaceho orgánu bezpečnosti by mal patriť aj bezpečnostný manažér organizácie.

Vrcholoví manažéri zodpovedajú najmä za:

- **prihlásenie sa k uplatňovaniu bezpečnosti,** prijatie záväzku na bezpečnosť,
- **zaradenie bezpečnosti do Strategického plánu organizácie** a rozpracovanie strategických cieľov pre bezpečnosť v taktickom plánovaní do najdôležitejších oblastí činností organizácie.
- **pochopenie organizácie a jej súvislostí** (bezpečnostného prostredia),
- **pochopenie potrieb a očakávania zainteresovaných účastníkov,**
- stanovenie **bezpečnostných cieľov, bezpečnostných noriem a kritérií rizík,**
- **stanovenie rozsahu a vytvorenie Systému manažérstva bezpečnosti organizácie,**
- vypracovanie a implementáciu **celkovej Bezpečnostnej politiky organizácie** ako dokumentu strategického významu s dlhodobou platnosťou, ktorý umožňuje vedeniu riadiť bezpečnostné procesy,
- určenie **rolí, zodpovednosti a právomoci za bezpečnosť,**
- **plánovanie bezpečnosti –** určenie postupov na riešenie rizík a príležitostí, cieľov manažérstva bezpečnosti, bezpečnostných cieľov organizácie a stanovenie bezpečnostných noriem a kritérií rizík,
- vypracovanie a implementácia **Plánu implementácie SMB a Havarijného plánu,**
- **podporovanie bezpečnosti – poskytnutie potrebných zdrojov,** stanovenie konkrétnych kompetencií osôb vykonávajúcich bezpečnostné činnosti, vytváranie povedomia bezpečnosti, udržiavanie vnútornej a vonkajšej komunikácie, určenie rozsahu zdokumentovaných informácií o bezpečnosti,
- **riadenie bezpečnostných činností –** organizovanie bezpečnosti, personálne zaistenie bezpečnosti, prevádzka SMB, manažérstvo rizík,
- **hodnotenie výkonnosti bezpečnosti** – monitorovanie, meranie, analýzy a vyhodnotenie, interný audit, preskúmanie manažmentom,
- **zlepšovanie bezpečnosti –** riešenie nezhôd a nápravné opatrenia, trvalé zlepšovanie.
- **propagovanie bezpečnosti** v celej organizácii.

Manažéri strednej úrovne

Manažéri strednej úrovne sú veľmi rôznorodou skupinou, zodpovedajú za:

- vypracovanie **Systémových bezpečnostných politík** a **Havarijných plánov** pre jednotlivé zložky bezpečnostného sektora podniku na obdobie 2-5 rokov, v ktorých sa definuje spôsob realizácie celkovej bezpečnostnej politiky v konkrétnych oblastiach,
- **manažérstvo rizík**,
- odborné **riadenie bezpečnostných pracovníkov na tretej úrovni, školenie a výcvik,**
- **kontrolnú činnosť** v oblasti bezpečnosti,
- vypracovanie a implementáciu ďalšej **bezpečnostnej dokumentácie,** napr.:
  - Plán manažérstva rizika, Plán zaobchádzanie s rizikom, Plán komunikácie v manažérstve rizika,

- Bezpečnostné projekty a smernice (ochrana osobných údajov v informačných systémoch, ochrana technických prostriedkov s utajovanými skutočnosťami),
- Bezpečnostný plán ochrany objektu,
- Smernice pre výkon fyzickej ochrany,
- Plán požiarnej ochrany a pod.

Manažéri prvej úrovne

Manažéri prvej úrovne ovplyvňujú svojimi rozhodnutiami transformáciu výrobných činiteľov na úžitkové hodnoty, zodpovedajú za zadávanie úloh výkonným pracovníkom a za ich plnenie. Zodpovedajú za:

- **realizáciu Bezpečnostných politík, Havarijných plánov** a ďalších bezpečnostných dokumentov v jednotlivých zložkách bezpečnostného sektora podniku,
- **plnenie povinností** vyplývajúcich z **bezpečnostných smerníc a plánov**,
- **spätnú väzbu** pre 2. stupeň riadenia.

4.5.1 Manažéri zodpovední za riadenie organizácie

Vedenie jednotlivých organizácií nemá jednotnú štruktúru manažmentu, každá organizácia si vytvára manažérske pracovné miesta podľa vlastnej potreby a možností. Iní funkcionári sú v mestských a obecných zastupiteľstvách, bankovom a finančnom sektore, športových, kultúrnych a iných organizáciách a iné v štátnych alebo neštátnych podnikoch.

Názvy manažérskych funkcií nie sú záväzné, každá organizácia ich nazýva podľa svojich potrieb. Obvykle však v organizačnej štruktúre podnikových organizácií sú začlenení:

a) riaditeľ organizácie – *Chief Executive Officer, CEO* – niekedy aj ako ***generálny riaditeľ*** alebo ***výkonný riaditeľ*** – štatutárny orgán, vystupuje a koná v mene organizácie, je najvyšší vedúci organizácie, jeho postavenie závisí od vymedzených kompetencií, komplexne riadi činnosť a zodpovedá za výsledky organizácie, najvyšší konateľ spoločnosti alebo správca zodpovedný za celkové riadenie, ale nie vždy aj prezident spoločnosti,

b) sekretariát – vykonáva všetky bežné administratívne práce podľa pokynov riaditeľa, napr. prijíma návštevy, eviduje došlú poštu, spracováva a odosiela bežnú poštu, pripravuje materiály, kontroluje termíny plnenia úloh a pod.,

c) štábne odborné útvary – vytvárajú sa na horizontálnej osi riadenia, podľa jednotlivých funkčných oblastí, pričom môžu mať rôzne názvy napr. výroba, odbyt, marketing, personalistika, financie. Na čele štábnych útvarov sú **riaditelia,** vnútorne sa členia na ***odbory*** (vedúci alebo riaditeľ odboru), ***oddelenia*** (vedúci oddelenia), ***referáty*** (pracovisko, ktoré zabezpečuje výkon vymedzených činností),

d) líniové útvary – vytvárajú sa po vertikálnej osi riadenia, sú to závody, divízie, prevádzky, dielne. Na čele líniových útvarov sú **línioví vedúci**: závod – **riaditeľ**, divízia a prevádzka – **vedúci**, dielňa – **majster**.

Medzi riaditeľov štábnych útvarov patria najmä:

- **finančný riaditeľ –** Chief Financial Officer, CFO **–** zodpovedá za riadenie financií v celej organizácii, v mnohých spoločnostiach je považovaný za druhého najdôležitejšieho človeka, plánuje financie, vykonáva finančné analýzy, riadi finančné toky a vykonáva nákladové analýzy pomocou rôznych finančných ukazovateľov.
- **prevádzkový riaditeľ** – Chief Operating Officer, COO – zodpovedá za prevádzku organizácie, jej každodenné fungovanie, vedľa generálneho a finančného riaditeľa je najvyššie postavený manažér v organizácii, jeho úlohou je plánovať, viesť, organizovať, rozhodovať a kontrolovať ľudí, procesy a informácie v každodennej prevádzke.
- **výrobný riaditeľ** – zodpovedá za riadenie a optimalizáciu výrobného procesu, analyzovanie výrobných postupov s cieľom optimalizovať výkonnosť, kvalitu a zvýšiť bezpečnosť

práce. Je zodpovedný za ***dodržiavanie systémov kontroly kvality a bezpečnostných predpisov.***

- **riaditeľ IT (IKT) –** Chief Information Officer, CIO – v našich podmienkach ***správca informačného systému*** – patrí medzi najvyššie postavených manažérov v organizácii, zodpovedázaoblasťinformatiky, riadenie prevádzky a rozvoja informatiky v organizácii, zosúladenie cieľov organizácie a ich podpory informáciami a informačnými a komunikačnými technológiami.
- **personálny riaditeľ, riaditeľ ľudských zdrojov** – Chief Human Resources Officer, CHRO – patrí medzi najvyššie postavených manažérov v organizácii, zodpovedá za oblasť personalistiky a ľudských zdrojov, jeho úlohou je zodpovedať za riadenie prevádzky aj rozvoja ľudských zdrojov, zosúlaďovanie cieľov organizácie s potenciálom a schopnosťami ľudí a rozvoj ľudského kapitálu. Väčšinou je priamo podriadený generálnemu riaditeľovi.
- **technický riaditeľ** – Chief Technology Officer alebo Chief Technical Officer – obvykle je priamo podriadený CEO, zodpovedá za výskum a vývoj, predovšetkým dohliada na vývoj nových technológií (rôznych typov). V jeho úlohách je aj ***identifikácia príležitostí a rizík pre podnikanie*.**
- **marketingový riaditeľ –** Chief Marketing Officer **–** zodpovedá za marketingové aktivity v organizácii, najčastejšie je priamo podriadený generálnemu riaditeľovi, má primárnu alebo spoločnú zodpovednosť za riadenie predaja, vývoj produktov, riadenie distribučných kanálov, marketingovej komunikácie (vrátane reklamy a propagácie), oceňovanie, prieskum trhu a služby zákazníkom, spoločnej organizácie trhu.
- **podnikový právnik –** Chief Compliance Officer **–** zodpovedá za dodržiavanie zákonných ustanovení, platných noriem etického kódexu a profesionálnych noriem vo vnútri organizácie, aby sa zamedzilo rizikám, ktoré by mohli vyplynúť z pochybení organizácie, jej rozhodovacích orgánov alebo zamestnancov pri plnení svojich povinností. Obvykle priamo spolupracuje s generálnym riaditeľom alebo prevádzkovým riaditeľom.

Bezpečnostní funkcionári

Okrem funkcionárov manažmentu, zodpovedných za celkové riadenie organizácie, ktorí sa zapájajú do manažérstva bezpečnosti vo svojich podriadených oblastiach, stanovuje vrcholový manažment na základe veľkosti, štruktúry a zložitosti organizácie aj funkcionárov, výlučne zodpovedných za manažérstvo bezpečnosti.

Medzi hlavných bezpečnostných funkcionárov patria:

- **bezpečnostný manažér** – Chief Security Officer, CSO,
- **manažér rizík** – Chief Risk Officer, CRO alebo **manažér riadenia rizík** – Chief Risk Management Officer, CrMo,
- **bezpečnostný správca informačného systému –** Chief Information Security Officer, CISO,
- **manažér BOZP a ochrany životného prostredia –** niekedy ako samostatné funkcie **manažér BOZP** a **environmentálny manažér**,
- **manažér (koordinátor) systému manažérstva kontinuity činností**,

4.5.2 Bezpečnostný manažér

Bezpečnostný manažér (CSO) je ***vedúci pracovník, zodpovedný za stav celkovej bezpečnosti organizácie.*** Je vymenovaný z predstaviteľov vedenia, má hlavnú zodpovednosť a inštitucionálnu právomoc vo veciach bezpečnosti v celej organizácii. Všeobecne vystupuje ako vedúci pracovník organizácie, zodpovedný za vytvorenie vízie, stratégie, politiky a programov bezpečnosti organizácie, ich implementáciu a riadenie.

Termín Chief Security Officer sa najprv používal najmä v oblasti informačných technológií (IT) na určenie osoby zodpovednej za bezpečnosť IT. V minulosti boli bezpečnosť a informačná bezpečnosť organizácie riadené samostatnými oddeleniami. V mnohých organizáciách CSO zodpovedá aj teraz za zabezpečenie počítačovej a informačnej bezpečnosti, niekde sa však táto oblasť rieši samostatne.

V našich podmienkach je bezpečnostný manažér v pracovných ponukách niekedy označovaný aj názvami *Security Manager, Safety&Security Manager, Bezpečnostný manažér/technik.* Mal by byť vymenovaný v každej organizácii, ale napriek tomu, že patrí medzi top manažment organizácie, je v mnohých menších organizáciách zaradený do podriadenosti personálneho alebo iného oddelenia (skupiny), odkiaľ riadi podriadené bezpečnostné zložky. V prípade, že nie sú vyčlenení niektorí bezpečnostní špecialisti, dokonca vykonáva aj ich povinnosti (najmä v malých organizáciách).

Všeobecne sa však stále viac presadzuje, že **CSO** je výkonný pracovník, **zodpovedný za stav celkovej bezpečnosti organizácie, *fyzickej i digitálnej,*** čo znamená, že ***zodpovedá aj za informačnú bezpečnosť*.** Okrem toho **sám** alebo **v spolupráci s odbornými bezpečnostnými manažérmi** sa podieľa na súvisiacich oblastiach, ako je ***manažérstvo BOZP*, *manažérstvo kontinuity činností, environmentálne manažérstvo, prevencia škôd, predchádzanie podvodom a ochrana utajovaných skutočností.*** V podmienkach SR sa však nie všade darí túto myšlienku presadiť.

Zlučovanie všetkých foriem bezpečnosti do jedného organizačného celku sa donedávna považovalo za kontroverzný prístup. Na taktickej úrovni však technológie môžu byť zahrnuté medzi nástroje fyzickej a objektovej bezpečnosti, ktorá je stále viac riadená s využitím informačných technológií. Na praktickej úrovni potom možno hovoriť, že takto holisticky chápaná bezpečnosť môže poskytovať lepšiu bezpečnosť pri nižších nákladoch.

Na strategickej úrovni generálni riaditelia a predstavenstvá presadzujú široký pohľad na prevádzkové riziko v rámci celej organizácie. **Súčasný prístup vedenia k bezpečnosti *sa teda presadzuje v rámci manažérstva rizika organizácie vo všetkých oblastiach.*** Toto ***spoločné (integrované) manažérstvo všetkých rizík organizácie*** sa môže riešiť samostatným holistickým oddelením alebo samostatnými útvarmi.

CSO je vrcholový pracovník bezpečnosti v organizácii, podáva správy priamo jej hlavným funkcionárom (CEO, COO, CFO), **dohliada** a **koordinuje** bezpečnostné úsilie celej spoločnosti, ***vrátane informačných technológií, ľudských zdrojov, komunikácie, práva, riadenia podporných činností (facility management) a iných skupín, a bude určovať bezpečnostné programy a normy.***

Rozsah oblastí jeho činností je závislý od veľkosti, zamerania a štruktúry organizácie a stanovuje ho vrcholový manažment organizácie.

Do náplne práce bezpečnostnéhomanažéra patrí najmä:

- viesť ***manažérstvo rizika*** na zvýšenie hodnoty organizácie a jej značky *(brand),*
- ***dohliadať na sieť bezpečnostných pracovníkov a zamestnancov***, ktorí chránia majetok spoločnosti, duševné vlastníctvo a počítačové systémy, rovnako ako fyzickú bezpečnosť zamestnancov a návštevníkov,
- identifikovať ***ciele bezpečnosti*** a spôsob merania ich dosahovania, v súlade so strategickým plánom organizácie,
- riadiť tvorbu a implementáciu celkovej ***bezpečnostnej politiky, bezpečnostných noriem, smerníc a postupov*** v súčinnosti s vrcholovým manažmentom a neustále zdokonaľovať štandardizované postupy, s cieľom zabezpečiť nepretržité udržiavanie **bezpečnosti,**
- stanoviť jasné *poradie* ***právomocí a zodpovedností*** v bezpečnostných štruktúrach,

- ***spolupracovať s ďalšími vedúcimi manažérmi*** pri uprednostňovaní bezpečnostných iniciatív a tvorbe rozpočtu na zabezpečenie bezpečnosti,
- zaistiť pravidelné ***vyhodnocovanie a kontrolu*** úrovne bezpečnosti a podávanie hlásení,
- udržiavať ***vzťahy s orgánmi verejnej moci,***
- organizovať ***školenia*** personálu o interných predpisoch a smerniciach z oblasti bezpečnosti,
- dohliadať na ***plánovanie reakcie na incidenty,*** ako aj na ***vyšetrovanie*** narušenia bezpečnosti a podľa potreby pomáhať riešiť ***disciplinárne a právne otázky spojené s takými narušeniami,***
- pracovať s externými poradcami, vhodnými pre nezávislé ***bezpečnostné audity.***

V niektorých organizáciách sa pre samostatné objekty vytvárajú pracovné miesta **bezpečnostný manažér – junior.** Na riadenie všetkých podporných činností sa v objektoch budov stále viac vytvára funkcia **facility manažér**.

Kompetencie bezpečnostného manažéra

Bezpečnostní manažéri majú v procese manažérstva bezpečnosti nezastupiteľnú úlohu. Na osobnosť manažéra sa kladú vysoké nároky a požiadavky, pretože na jeho riadiacich schopnostiach a predpokladoch funguje celý systém alebo časť bezpečnosti organizácie a on zodpovedá za svoje rozhodnutia a z nich vyplývajúce následky. Túto pracovnú pozíciu môže vykonávať len pracovník, ktorý má na to ***odborné, vedomostné, kvalifikačné a osobnostné predpoklady.*** Na zvládnutie a vykonávanie konkrétnej funkcie bezpečnostného pracovníka je potrebné mať aj potrebné **profesijné kompetencie**.

Základné predpoklady pracovnej spôsobilosti bezpečnostného manažéra tvoria:

a) osobný potenciál–súhrn všetkých vlastností a schopností, ktoré umožňujú dosiahnuť pracovné aj spoločenské ciele, premieta sa do nasledujúcich rovín:
   - **osobnosť –** fyzické a osobnostné vlastnosti,
   - **odbornosť –** schopnosti, vzdelanie a prax vo vzťahu k profesii,
   - **efektivita –** miera využitia znalostí a schopností,
   - **stabilita –** schopnosť adaptácie na zmeny,
   - **dynamika –** pôsobenie na okolie.

b) vedomosti – všeobecné a špecifické poznatky nadobudnuté štúdiom alebo skúsenosťou, odborné znalosti, vedomosti;

c) zručnosti – naučené spôsoby vykonávať určité činnosti;

d) schopnosti – dispozície na vykonávanie určitých činností, vlastnosti osobnosti, dôležité pre kvalitný rozvoj a správne vykonávanie určitej činnosti, je treba ich rozvíjať v činnostiach, človek sa s nimi nerodí, pokiaľ sa schopnosť žiadnym spôsobom nerozvíja, nemusí sa vôbec prejaviť;

e) právomoci (a s tým spojené zodpovednosti), ktoré dávajú manažérovi „silu“ jeho rozhodnutie realizovať.

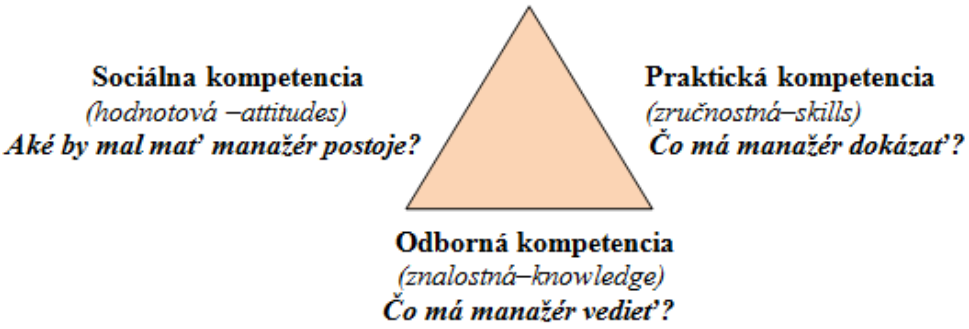
Kompetencie manažéra možno definovať ako ***súbor vedomostí, schopností, zručností a skúseností ako aj fyzickej a psychickej pripravenosti tieto kvality využiť na efektívne vykonávanie určitých úloh (funkcií a rolí) v súlade s pridelenou právomocou a všeobecným očakávaním*** *(Míka, 2006).*

Základné kompetencie manažérov možno podľa Webera *(2003)* zadeliť do nasledovných **dimenzií** (obr. 13):

1. Sociálna zrelosť – (aké má mať osobné postoje), predstavuje vedomé, alebo nevedomé ***zachovávanie základných princípov správania sa,*** vďaka ktorým sa zachováva celostnosť

osobnosti. Sociálne zrelým sa človek stáva vďaka vlastnostiam, ktoré získava geneticky dedením (vrodené vlastnosti) a výchovou a vzdelávaním (rozvoj danosti). Sociálna zrelosť je záležitosťou vnútra človeka, je to jeho filozofia, jeho cítenie, a preto sa tento pilier nazýva aj **múdrosťou.** Múdrosťou však nie je učenosť, lebo nie každý učený je aj múdry, a pravdaže, nie každý múdry je nutne v bežnom zmysle aj učeným človekom – lebo múdri sú aj medzi ľuďmi bez školského vzdelania.

2. **Odborné vedomosti –** (aké má mať odborné vedomosti), manažér potrebuje mať odborné vedomosti, ***aby sa dokázal rozhodovať***, sú to vedomosti potrebné na vykonávanie špecializovaných aktivít pri riadení bezpečnosti, získavajú sa predovšetkým vzdelávaním, ale aj získaním skúseností z toho, čo manažér prežije. Odborné kompetencie umožňujú bezpečnostnému manažérovi poznať svoju oblasť činnosti a jej súvislosti, možno k nim zaradiť najmä **vzdelanie a prax v danej oblasti či odvetví**, ďalšie, najmä **ekonomické a právne vedomosti** a **všeobecný rozhľad**, pričom úroveň jednotlivých čiastkových schopností bude závisieť od špecifík každej konkrétnej situácie.
3. **Praktické zručnosti –** (čo má dokázať), znamenajú schopnosť vykonávať svoju funkciu zručne, schopne, šikovne.



Obr. 13 Základné kompetencie manažérov

R. L. Katz *(1974)* identifikoval **tri základné skupiny zručností**, nutné pre manažérov:

a) **Ľudské (interpersonálne) zručnosti** sú založené na schopnosti spolupracovať s vedúcim, podriadenými, nadriadenými a s manažérmi na rovnakej úrovni. Manažéri s dobrými ľudskými zručnosťami sú schopní dostať zo svojich ľudí to najlepšie, vedia ako komunikovať, motivovať, hodnotiť, viesť a prebúdzať nadšenie a dôveru a zlepšovať ich výkonnosť. Požiadavky na ľudské zručnosti sú dominantné pri strednom manažmente, ale sú dôležité aj pre ďalšie stupne manažérov, pretože komunikácias ľuďmi tvorí významnú neoddeliteľnú súčasť práce manažéra. Tieto zručnosti sú kľúčové, pretože manažéri jednajú priamo s ľuďmi, sú nevyhnutné pre efektívnu komunikáciu a budovanie pozitívnych vzťahov s ostatnými.
b) **Technické zručnosti** zahŕňajú využívanie špeciálnych technických a technologických poznatkov a skúseností pri výkone práce. Predstavujú zručnosti v určitých špecifických oblastiach (schopnosti manažéra uplatňovať špecifické znalosti, techniky, metódy a postupy na realizáciu výkonných činností a procesov). Sú potrebné pre väčšinu manažérov najmä na nižšej úrovni, osobitne sú dôležité najmä pre prvostupňových manažérov, pretože pracujú s ľuďmi, ktorí tvoria. Sú tvorené súborom zručností, ktorý sa vzťahuje na konkrétnu funkciu.
c) **Koncepčné zručnosti** sú schopnosti viesť organizáciu ako celok. Ide o pochopenie zložitosti organizácie a jej bezpečnosti, ako sa rôzne funkcie organizácie ovplyvňujú, ako je spojená s okolím a ako zmeny v jednej zložke vplývajú na celú organizáciu. Predstavujú

schopnosť koncepčne a komplexne myslieť, predvídať vývoj prostredia, odhaľovať príležitosti a nebezpečenstvá existujúce v prostredí, identifikovať silné a slabé stránky svojho kolektívu. Koncepčné zručnosti umožňujú manažérovi vytyčovať ciele, stanovovať plány a organizovať činnosť na ich splnenie, s predstihom sa pripraviť na riešenie budúcich problémov a situácií. Koncepčné zručnosti sú veľmi dôležité pri rozhodovaní hlavne na vrcholovom stupni riadenia.

Bezpečnostný manažér junior

Funkcia bezpečnostného manažéra juniora sa obvykle vytvára v samostatnom objekte organizácie, má tieto povinnosti:

- riadi, kontroluje a pripravuje bezpečnostný tím v objekte,
- zodpovedá za plnenie zmluvného dojednania medzi klientom a poskytovateľom služieb,
- spracováva správy klientovi a vedeniu organizácie,
- pravidelne vyhodnocuje bezpečnostnú situáciu v objekte, navrhuje bezpečnostné opatrenia,
- zodpovedá, že všetci pracovníci objektu absolvovali povinné školenie pre výkon činnosti,
- zodpovedá za prípravu mzdových podkladov, prípravu fakturačných podkladov, za plnenie právnych povinností pre výkon činnosti SBS, za obsadzovanie pozícií bezpečnostného tímu a riadi ľudské zdroje, vrátane mzdového rozpočtu,
- rieši mimoriadne udalosti v objekte,
- spolupracuje s orgánmi štátnej správy.

4.5.3 Ďalší bezpečnostní funkcionári

Manažér BOZP a ochrany životného prostredia

Riadiaci pracovník (manažér) bezpečnosti a ochrany zdravia pri práci a ochrany životného prostredia – alternatívne názvy Manažér bezpečnosti a životného prostredia, Manažér (vedúci) BOZP a EMS navrhuje, riadi a kontroluje procesy spojené s budovaním a rozvojom systémov riadenia bezpečnosti a ochrany zdravia pri práci a zodpovedá za vytváranie politiky bezpečnosti a ochrany zdravia pri práci a za riadenie činností v oblasti životného prostredia v súlade s platnými právnymi normami.

Facility manažér

Facility manažér je riadiaci pracovník (manažér), ktorý zodpovedá za oblasť facility manažmentu. Ide o riadiaceho pracovníka, ktorý je zodpovedný za stratégiu facility manažmentu, jej rozpracovanie do taktického zadania, zadania výberu externých poskytovateľov a kontrolu ich výkonov. Iná definícia hovorí, že pracovnou náplňou facility manažéra je „*riadenie všetkých úkonov tak, aby technológie a stavebné prvky objektu boli optimálne funkčné v súlade s potrebami ich užívateľov*“.

IFMA (International Facility Management Association) – profesijné združenie vedie a rozvíja odborníkov facility manažmentu tým, že poskytuje služby, produkty, zdroje a príležitosti,definuje 3 úrovne certifikácií facility manažéra:

1. Facility Management Professional – základný, stanovený certifikát. Ide o hodnotenie založené na programe, ktorý vedie k posúdeniu osvedčeného pochopenia základov facility manažmentu. V septembri v roku 2010, bol FMP aktualizovaný a rozšírený na zosúladenie s najnovšími IFMA o analýzy úloh a zabezpečenie toho, aby učili a testovali znalosti vyžadované podľa dnešných globálnych zamestnávateľov.
2. Sustainability Facility Professional – pomáha získať možnosť profesionálne zvládnuť kľúčové schopnosti pri vytváraní, manažovaní a prevádzkovaní zariadení tým, že im poskytuje zručnosti, aby neustále zlepšovali dopad týchto zariadení na životné prostredie a komunitu. Získanie tohto certifikátu pomáha preklenúť priepasť medzi profesionalitou a majetkovos-

ťou, učí manažérov ako implementovať koncepty udržateľnosti, ktorá sa vyrovnáva firemnej stratégie. Je tiež vytvorený pre získanie on-line pomoci pre manažérov na niektoré kritické problémy manažmentu, ktoré sa objavia ako následok manažovania.

3. Certified Facility Manager – je určený na posúdenie kompetencie v danej oblasti prostredníctvom pracovných skúseností, vzdelania a schopnosti prejsť súhrnnými testami.

Rozlišuje sa **externý** a **interný facility manažér**, kde externý manažér je zodpovedný za výkon služieb, ide o riadiaceho pracovníka poskytovateľa (vykonávateľa), t. j. outsourcera.

Interný facility manažér by mal byť vo vedení každej spoločnosti, je to v prvom rade riadiaci pracovník. Jeho hlavným poslaním je nájsť takú formu riadenia, pri ktorej dochádza s akceptovateľnými nákladmi k najkvalitnejšej podpore všetkých zamestnancov spoločnosti, k optimálnemu zabezpečeniu evidencie a chodu nehnuteľností a majetku (vybavenia).

Je to riadiaci pracovník (manažér), zodpovedný za riadenie a koordináciu pracovného prostredia naprieč celou organizáciou. Jeho cieľom je zladiť pracovné prostredie, pracovníkov a pracovné činnosti. Je to manažér a zároveň aj odborník, ktorý vo svojej osobe musí spájať znalosti z rôznych odborov, ako z technických, procesných, ekonomických, ekologických, psychologických a etických. Zahŕňa v sebe princípy obchodnej administratívy, architektúry, humanitných a technických vied.

Medzi jeho najčastejšie úlohy patria:

- prevádzka, údržba a servis objektu a technologických zariadení,
- záručný a pozáručný servis – zastupovanie klientov pri rokovaní s tretími osobami,
- revízie, odborné technické prehliadky podľa platných vyhlášok a noriem (napr. elektrická inštalácia, výťahy, spotrebiče, ainé),
- diaľkový monitoring – napojenie objektu na systém merania a regulácie, diaľkové odchytávanie porúch, poruchové hlásenia atď.,
- nepretržitá havarijná služba – možnosť zamedzenia vzniku ďalších škôd na majetku, odstránenie porúch,
- činnosť požiarnej ochrany a BOZP – kontrolná činnosť požiarnym technikom,
- vedenie kľúčového hospodárstva – evidencia kľúčového hospodárstva, systém generálneho kľúča.

Jeho zodpovednosťou je čo najefektívnejšie riadiť podporné procesy v organizácii tak, aby bola nastavená optimálna úroveň procesov vzhľadom k ich nákladom. Do jeho zodpovednosti patrí správa nehnuteľností, infraštruktúry, redukcia prevádzkových nákladov, zvýšenie efektivity pracovníkov (technikov, údržbárov, upratovania), ale i spokojnosť zamestnancov na pracoviskách. Facility manažér je garantom bezchybného chodu podporných činností v organizácii.

Musí ísť o koncepčne orientovaného riadiaceho pracovníka, ktorý má zvládať strategické, dlhodobé a strednodobé plánovanie, finančné plánovanie, problematiku štandardizácie, špecifikáciu požiadaviek poskytovateľom (vrátane špecifikácie ich merania) a v neposlednom rade musí efektívne kontrolovať výkon týchto služieb.

Ďalšou nevyhnutnou vlastnosťou facility manažéra je komunikácia vo všetkých jej formách (forma dohadovania, rokovania so stranami, vysvetľovania, presvedčovania, asertivita pri rokovaní s nájomníkmi, ale aj znalosť najmodernejších komunikačných technológií).

Facility manažér musí byť schopný obhájiť kvalitnú koncepciu facility managementu vo vedení spoločnosti. Často býva súčasťou tohto vedenia, jeho oblasť je však tou poslednou, ktorú je vedenie spoločnosti pripravené riešiť. Preto len na jeho komunikačných schopnostiach záleží, ako presadí svoje potreby medzi požiadavkami kolegov z oblasti základného

podnikania, obchodu či personalistiky. Od jeho schopností často závisia kvalitné služby, predĺženie životnosti majetku i spokojnosť zamestnancov.

Hlavný manažér rizík (manažér riadenia rizík)

Manažér rizík (CRO) alebo manažér riadenia rizík (CrMo) organizácie je konateľ zodpovedný za účinné a efektívne manažérstvo významných rizík a s nimi súvisiacich príležitostí na podnikanie. CRO má zvyčajne na starosti doručovaniepodkladov, potrebných pre správne rozhodovanie v oblasti riadenia rizíkpre vrcholový manažment. Hlavnou prioritou pre CRO je zabezpečiť, aby organizácia žila v súlade s platnými bezpečnostnými predpismi. Môže sa tiež zaoberať témami, ktoré sa týkajú poistenia,interného auditu, vyšetrovania podvodov a bezpečnosťou informácií.CRO by mal mať postgraduálne vzdelanie a dlhodobé skúsenosti s podnikaním, znalosťou poisťovníctva, účtovníctva, ekonómie a práva.

Správca informačného systému a bezpečnostný správca informačného systému

Podľa Vyhlášky NBÚ č. 339/2004 Z. z. o bezpečnosti technických prostriedkov za bezpečnosť prevádzky informačného systému zodpovedá **prevádzkovateľ informačného systému** v súlade s bezpečnostným projektom a smernicami. Na jeho prevádzku určuje oddelene:

- **správcu informačného systému** – vykonáva správu systému a jeho zdrojov,
- **bezpečnostného správcu informačného systému (CISO)** –vykonáva správu bezpečnosti informačného systému, najmä prideľovanie prístupových práv, správu autentizačných funkcií a autorizačných funkcií, vyhodnocovanie kontrolných záznamov o činnosti informačného systému, vypracúvanie správ o neoprávnených manipuláciách informačného systému a úlohy vyplývajúce zo smernice o používaní technického prostriedku.

4.6 LITERATÚRA

ALLAN, J. – POLÁK, V. – LETKOVÁ, S. [2003]: *Riadenie. Riadenie v organizáciách*, Bratislava: Nadácia City University Bratislava, ISBN 8089045510.

BERTALANFFY, L. VON. [1976]: *Perspektives on General System Theory: Foundations, Development, Applications,* New York: George Braziller, revised edition: ISBN: 978-08-0760-798-5.

DRUCKER, P. F. [1994]: *Řízení v turbulentní době.* Management Press, Praha *ISBN: 80-85603-67-5.*

HUBA M. – HUBINSKÝ P. – ŽÁKOVÁ K. [2002]: *Teória systémov.* Vydavateľstvo STU Bratislava.

KATZ, R. L. [1974]: *Zručnosti efektívneho správcu.* Harvard Business Press, 1974.

MÍKA, V. T. [2006]: *Základy manažmentu.* Virtuálne skriptá. [on line]. Vybrané prednášky pre študentov externého štúdia FŠI ŽU. Žilina: ISBN 978-80-88829-78-2.

PRNO, I. [2002]: *Teória systémov a riadenia*. P+M Turany. 2002. ISBN: 80-968742-0-9.

5 SYSTÉM MANAŽÉRSTVA BEZPEČNOSTI

Systém manažérstva bezpečnosti – SMB *(Security management system, Safety management system, Sicherheits management system, SMS)* predstavuje systematický prístup k riadeniu bezpečnosti, ktorý zahŕňa potrebné ***organizačné štruktúry, zodpovednosti, zásady a postupy***.

SMB organizácie tvorí určitú **časť celkového systému riadenia organizácie**, ktorá je určená na ***manažérstvo bezpečnosti*** pre ochranu osôb, majetku a životného prostredia organizácie.

Základom pre tvorbu SMB sú v každej organizácii:

- **bezpečnostné právne normy,**
- **vonkajšie a vnútorné bezpečnostné riziká,**
- **veľkosť aktív organizácie a ochota investovať ich do vlastnej bezpečnosti.**

Znamená to, že pri tvorbe tohto systému sa vychádza z povinností zamestnávateľov, ktoré im predpisujú bezpečnostné normy a rizík, ktorým sú vystavené ich aktíva. Každá organizácia pritom na ochranu svojich aktív vyčlení finančné náležitosti, primerané hodnote týchto aktív.

SMB organizácie sa v niektorých literárnych zdrojoch nazýva aj ako: *systém manažmentu bezpečnosti, systém riadenia bezpečnosti, systém bezpečnostného manažmentu alebo bezpečnostný systém organizácie.*

SMB predstavuje ***integrovaný súbor reálnych prvkov, ktoré majú stanovené funkcie a úlohy na zaistenie bezpečnosti*** v danom čase a priestore a sú medzi sebou spojené sieťou vzťahov, medzi ktorými pôsobí aj spätná väzba.

Musí byť vytvorený tak, aby pomocou disponibilných **síl, prostriedkov a režimových opatrení *zabezpečoval prevenciu a efektívnu ochranu*** pred pred udalosťami s negatívnymi následkami v podsektoroch bezpečnostného sektora. Zahŕňa množinu základných inštitucionálnych a systémových nástrojov na zaistenie bezpečnosti, ktorú predstavuje sústava:

- prvkov **manažmentu** organizácie – vrcholový manažment, líniovímanažéri,
- prvkov **bezpečnostného manažmentu** organizácie – bezpečnostný manažér, odborní bezpečnostní manažéri,
- **pracovníkov bezpečnosti**, vlastných i prenajatých,
- **bezpečnostných informácií** o vonkajšom a vnútornom bezpečnostnom prostredí a bezpečnostných rizikách,
- **rozhodovacích a komunikačných procesov,**
- súvisiacich **bezpečnostných právnych noriem**,
- súboru nariadení a obmedzení v podobe **režimových opatrení,**
- **síl a materiálnych prostriedkov** (technológií) na ochranu osôb, majetku a životného prostredia,
- **vzájomných väzieb a vzťahov**.

Uvedená sústava prvkov a vzťahov predstavuje nástroj na tvorbu a uskutočňovanie bezpečnostnej politiky, zaručuje bezpečnosť organizácie, jej zamestnancov, materiálnych hodnôt a životného prostredia v danom prostredí a čase. Vzhľadom na neustále narastajúci počet útokov na aktíva organizácie je potrebné vytvoriť taký systém bezpečnosti, ktorý by organizácii pomohol rýchlejšie a efektívnejšie sa orientovať vo všetkých sektoroch bezpečnosti, ktoré sú pre organizáciu podstatné.

5.1 CHARAKTERISTIKY SYSTÉMU MANAŽÉRSTVA BEZPEČNOSTI

SMB je výsledkom činnosti vrcholového manažmentu organizácie, ktorá **prijala zodpovednosť *riadiť vlastnú bezpečnosť*** *ako neoddeliteľnú súčasť celkovej činnosti*, na čo stanovila *bezpečnostnú politiku.*

SMB organizácie rovnako ako riadiaci systém každej organizácie ***formuluje ciele, plánuje, organizuje a hodnotí úroveň bezpečnosti.*** Pomocou stanovených cieľov, stratégií a politík hierarchicky rozvrhuje oblasť riešenia bezpečnosti od úrovne celej spoločnosti až po jednotlivé chránené oblasti – ľudských zdrojov, informačnej a pod.

SMB organizácie má plniť najmä tieto úlohy:

a) zabezpečiť jednotný systém riadenia vo všetkých podsektoroch bezpečnosti organizácie,
b) vytvoriť bezpečnostnú stratégiu organizácie,
c) prijať a implementovať Bezpečnostnú politiku,
d) definovať aktíva organizácie,
e) uskutočňovať manažérstvo rizika:
   - určiť kritériá rizík v závislosti na veľkosti aktív organizácie,
   - identifikovať vonkajšie a vnútorné bezpečnostné riziká, ktoré môžu ohroziť bezpečnosť aktív organizácie a zisťovať ich príčiny a tendencie vývoja,
   - analyzovať riziká a určiť ich úroveň,
   - vyhodnotiť jednotlivé riziká podľa prijatých kritérií rizika,
   - v súlade s dostupnými zdrojmi a kapacitami rozhodnúť o spôsoboch zaobchádzania s neakceptovateľnými a prípustnými rizikami,
   - spracovať Plán zaobchádzania s rizikami, s ktorým zoznámiť všetkých zamestnancov organizácie,
   - monitorovať zvyškové riziká a možný vznik nových bezpečnostných rizík,
   - viesť záznamy o procese manažérstve rizika,
f) vytvoriť a zabezpečiť plánovacie dokumenty,
g) vypracovať a realizovať ďalšie bezpečnostné dokumenty,
h) vytvoriť systémy ochrany (ochranných opatrení a prostriedkov) na zaistenie bezpečnosti osôb, majetku a životného prostredia,
i) určiť postupy na riešenie bezpečnostných incidentov a nehôd,
j) zabezpečiť vzdelávanie a výcvik v jednotlivých oblastiach bezpečnosti,
k) udržiavať plynulú komunikáciu s externými a internými zainteresovanými účastníkmi o dodržiavaní bezpečnosti,
l) monitorovať a vyhodnocovať stav úrovne bezpečnosti v organizácii,
m) neustále zlepšovať svoju činnosť a zvyšovať bezpečnosť organizácie.

5.1.1 Funkcie systému manažérstva bezpečnosti

SMB organizácie by mal zabezpečovať nasledujúce funkcie:

- **preventívnu –** zameranú na predchádzanie vzniku nebezpečných udalostí, ktoré môžu spôsobiť významné škody alebo ohroziť existenciu objektu,
- **pohotovostnú –** zameranú na zaistenie trvalej pripravenosti potrebných síl a prostriedkov, vyčlenených na riešenie rizikových situácií,
- **informačnú –** zabezpečujúcu trvalú analýzu bezpečnostného prostredia, manažérstvo bezpečnostných rizík a včasné upovedomenie o vznikajúcich alebo vzniknutých rizikových situáciách,

- **vykonávaciu** – reakcia na vzniknuté rizikové situácie spočíva v schopnosti včas a efektívne nasadiť disponibilné sily a prostriedky na zníženie včasné odstraňovanie následkov negatívnych udalostí.

Pôsobenie SMB organizácie je možné charakterizovať tromi základnými spôsobmi:

1. **z právneho hľadiska** je to súhrn zákonov a ďalších právnych noriem, ktoré vytvárajú základný rámec jeho pôsobenia,
2. **z administratívno-organizačného hľadiska** je to inštitúcia (súhrn inštitúcií) vybavená kompetenciami, danými zákonmi a ďalšími právnymi a inými normami:
   - ktorá má špeciálny aparát pripravovaný na pôsobenie v bezpečnostnej oblasti a riešenie problémov v nej,
   - ktorá vlastní prostriedky na riešenie bezpečnostných problémov v organizácii.
3. **zo sociálneho hľadiska** je to fenomén, vnímaný a hodnotený jednotlivcami, skupinami, organizáciami a inštitúciami, ktoré majú od neho určité požiadavky a očakávania.

Pre zavedenie SMB do organizácie existujú tri **aspekty –** morálny, právny a finančný:

- **morálny aspekt** predstavuje ***morálny záväzok zamestnávateľa***, že zaistí bezpečnosť na pracovisku,
- **právny aspekt** predstavuje ***splnenie právnych požiadaviek bezpečnosti*** definovaných v právnych normách,
- **finančný aspekt** znamená presvedčenie, že efektívne vynaložené prostriedky na bezpečnosť práce (pri znížení rizík na pracoviskách), môžu ***znížiť finančné náklady organizácie*** o priame a nepriame náklady, spojené s následkami úmyselného napadnutia osôb a majetku, náhodných porúch a havárií a ohrozenia životného prostredia.

5.1.2 Výhody zavedenia systému manažérstva bezpečnosti

SMB sa zavádzajú **vo všetkých odvetviach, najmä vo väčších organizáciách**, ktoré sú vystavené bezpečnostným rizikám, pretože sa zistilo, že hlavnou príčinou incidentov, nehôd prerušenia činností alebo havárií sú možné chyby techniky a personálu a závažné nedostatky v organizácii. Podceňovanie SMB môže viesť k vážnemu narušeniu chodu organizácie, pričom následky môžu byť vážne pre organizáciu i jej vedenie.

SMB je súčasťou štruktúry organizácie, stáva sa súčasťou jej bezpečnostnej kultúry. Ukazuje, akým spôsobom majú zamestnanci vykonávať svoju prácu pri zachovaní bezpečnosti. Pre zvýšenie efektívnosti bezpečnosti sa musí stať súčasťou každodennej praxe.

Zavedenie SMB v organizácii umožní:

- efektívnu činnosť bezpečnostných pracovníkov a využitie zdrojov organizácie,
- dosiahnutie bezpečnostných cieľov organizácie v jednotlivých oblastiach bezpečnostného sektora,
- pridelenie zodpovednosti za jednotlivé oblasti bezpečnostného sektora a dodržiavanie zásad, noriem a pravidiel bezpečnosti,
- koordináciu aktivít rôznych bezpečnostných zložiek organizácie,
- vytvorenie vnútorných bezpečnostných noriem vo všetkých oblastiach činnosti,
- nepretržité manažérstvo bezpečnostných rizík,
- vytvorenie komplexného systému ochrany na zachovanie bezpečnosti a ochrany života, zdravia, majetku, životného prostredia a iných dôležitých záujmov organizácie aj jednotlivcov,
- redukciu bezpečnostných incidentov,
- vnútornú a vonkajšiu komunikáciu o otázkach bezpečnosti,
- vypracovanie právne podloženej a prehľadnej bezpečnostnej dokumentácie,

- vytvorenie lepších podmienok pre uzatváranie nových zmlúv so zainteresovanými účastníkmi,
- pozitívne vnímanie obchodnými partnermi a predovšetkým zákazníkmi a v neposlednom rade i spoločenským a politickým prostredím.
- prispôsobenie zmenám v okolí,
- spokojnosť zamestnancov, sociálne uspokojenie členov, ktorí pracujú v SMB.

SMB je základným prvkom istoty manažmentu, že aktíva organizácie sú dostatočne zabezpečené proti poškodeniu alebo zničeniu. Dovoľuje každej organizácii dosiahnuť bezpečnostné ciele primeraným spôsobom k jej modelu a možnosť dosiahnuť výsledok spôsobom, ktorý je prispôsobený jej individuálnym činnostiam.SMB prispieva k odstráneniu zranení a smrteľných úrazov a je prevenciou pred zničením alebo poškodením majetku a ohrozením životného prostredia v organizácii i v jej okolí.

5.2 ŠTRUKTÚRA SYSTÉMU MANAŽÉRSTVA BEZPEČNOSTI

Štruktúra *(z lat. Struer, skladať, zostavovať, budovať, organizovať)* označuje ***spôsob zloženia, vnútorného usporiadania určitého objektu***, najmä ak vykazuje nejaké pravidelnosti a zákonitosti. Je to ***súhrn vzťahov medzi prvkami*** nejakého zoskupenia. Často sa chápe aj ako ***účelné usporiadanie prvkov, častí alebo zložiek nejakého celku podľa zjednocujúceho princípu alebo plánu.***

Štruktúra systému predstavuje ***vnútorné usporiadanie prvkov a väzieb v systéme,*** je to usporiadaná množina vzťahov medzi prvkami systému. Pri poznávaní a skúmaní systému možno v ňom vymedziť viac štruktúr (v závislosti od zvolených hľadísk), vtedy hovoríme o multištrukturalite systému. Znalosť štruktúry systému umožňuje predvídať vývoj jeho správania a vzhľadom na plnenie stanovených cieľov uskutočňovať aj účinné zmeny v jeho štruktúre. Zásah do štruktúry systému znamená nielen nové usporiadanie prvkov a väzieb, ale aj zaradenie nových prvkov a vyradenie tých, ktorých vlastnosti neumožňujú plniť ciele systému.

Štruktúra SMB sa vytvára a je zaradená **v rámci *organizačnej štruktúry danej organizácie.*** Od vrcholového manažmentu organizácie potom záleží, či vytvorí:

- ***centralizovanú*** organizačnú štruktúru SMB, s podriadením všetkých jej prvkov bezpečnostnému manažérovi,
- alebo ***decentralizovanú organizačnú*** štruktúru SMB, s podriadením niektorých prvkov bezpečnostnému manažérovi a ďalších do iných útvarov (personálny, stavebný atď.).

Formálna organizačná štruktúra

Organizačná štruktúra SMB je **formálna organizačná štruktúra**, je chápaná ako štruktúra organizačných jednotiek vo formálne organizovanej organizácii, kde je jednoznačne daná ***nadriadenosť a podriadenosť, zodpovednosti a právomoci jednotlivých vedúcich a celých útvarov.*** Vyjadruje stav tohto systému, usporiadanie jeho jednotlivých stupňov, členenie po stránke horizontálnej i vertikálnej.

Organizačnú štruktúru SMB tvorí súbor:

- ***riadiacich orgánov*** *(osoby, inštitúcia alebo aparát poverený výkonnou mocou) – manažment,*
- ***bezpečnostných pracovníkov,***
- ***útvarov a pracovísk bezpečnosti,***
- ***a vzťahov (väzieb) medzi nimi.***

Riadiace orgány v SMB predstavujú riadiaci podsystém – subjekt riadenia, ktorý tvoria:

- ***vrcholoví manažéri***, zodpovední za celkový chod organizácie i jej bezpečnosť,
- ***líniový manažéri***, zodpovední za bezpečnosť na svojej úrovni a úsekoch,
- ***bezpečnostný manažér,*** zodpovedný za celkovú bezpečnosť a ochranu osôb, majetku a životného prostredia v organizácii,
- ***odborní bezpečnostní manažéri,*** zodpovední za **jednotlivé odborné oblasti bezpečnosti –** informačnú, kontinuity činností, BOZP, environmentálnu a iné, ktoré často vystupujú ako samostatné subjekty,
- ***vzťahy medzi nimi.***

Bezpečnostní pracovníci sú zamestnanci, ktorí vykonávajú činnosti na ochranu osôb, majetku a životného prostredia v jednotlivých podsektoroch bezpečnostného sektora organizácie.

Útvary bezpečnosti predstavujú organizačnú jednotku alebo jej zložku, zameranú na bezpečnosť, napr. požiarny útvar (zbor), strážni, tím plánovania bezpečnosti, tím manažérstva rizík, tím manažérstva incidentov a pod.

Pracovisko bezpečnosti predstavuje miesto alebo inštitúciu, kde sa vykonávajú činnosti na zabezpečenie ochrany osôb, majetku a životného prostredia v jednotlivých podsektoroch bezpečnostného sektora organizácie, napr. kontrola vstupu, pracovisko personálnej bezpečnosti, hasičská zbrojnica a pod.

Formálna organizačná štruktúra je obvykle deklarovaná pomocou organizačných poriadkov a charakterizovaná pomocou organizačných schém. Predstavuje plánovanú koordináciu činností skupín pracovníkov na dosiahnutie spoločného a explicitne stanoveného bezpečnostného cieľa, a to na základe deľby práce, funkcií a vymedzenej právomoci a zodpovednosti.

Formálna organizačná štruktúra má byť pružná a má poskytovať priestor pre:

- voľnosť jednania,
- výhodné využívanie tvorivých talentov,
- poznanie individuálnych záujmov a schopností – individuálne úsilie však musí byť usmerňované tak, aby bolo v súlade s cieľmi skupiny a organizácie.

Funkcionálna organizačná štruktúra

Organizačná štruktúra SMB je **funkcionálna organizačná štruktúra,** charakterizuje ju ***jej rozčlenenie na útvary****,* v ktorých sa zoskupujú rovnaké alebo príbuzné funkcie (bezpečnostné činnosti). Výhody a nevýhody funkcionálnej organizačnej štruktúry sú uvedené v tab. 2.

Tab. 2 Výhody a nevýhody funkcionálnej organizačnej štruktúry

Výhody funkcionálnej organizačnej štruktúry	**Nevýhody funkcionálnej organizačnej štruktúry**
dôsledná deľba práce podľa činnosti, jednotnosť riadenia príslušnej funkcie, možnosti unifikácie prác, obmedzenie duplicity prác, účelné využitie špecializovaných odborníkov, pomerne nízke režijné náklady.	prílišná centralizácia rozhodovania, nutnosť väčšej koordinácie medzi jednotlivými funkčnými oblasťami, dlhá komunikačná cesta, sklon k jednostrannému riešeniu komplexných úloh.

Organizačná štruktúra SMB je teda organizačnou formou, v ktorej sa **bezpečnostní pracovníci *združujú podľa rovnakých alebo príbuzných funkcií*** vo **funkčne špecializovaných útvaroch** podľa ***jednotlivých podsektorov bezpečnostného sektora organizácie***, napr.:

- Systém manažérstva BOZP – *bezpečnostný technik, autorizovaný bezpečnostný technik alebo iný odborník na prevenciu a ochranu v špecifickej oblasti bezpečnosti a ochrany zdravia pri práci, odborní zdravotnícki pracovníci kvalifikovaní na výkon pracovnej zdravotnej služby.*
- Systém požiarnej ochrany – *technik požiarnej ochrany, špecialista požiarnej ochrany, členovia požiarnej hliadky, hasiči.*
- Ochrana utajovaných skutočností – *referent OUS.*
- Systém manažérstva informačnej bezpečnosti – *správca informačného systému, bezpečnostný správca informačného systému.*
- Systém fyzickej ochrany objektu – *strážni* atď.

Zmyslom organizačnej štruktúry SMB je ***rozdeliť práce medzi jej funkčnými útvarmi a koordinácia ich aktivít*** tak, aby boli zamerané na dosahovanie bezpečnostných cieľov organizácie. **Vedúci funkčne špecializovaných útvarov** by mali podliehať bezpečnostnému manažérovi, v súčasných podmienkach sa však táto zásada u nás často nedodržiava.

Činnosť špecifických útvarov v štruktúre je popísaná **organizačným poriadkom**, náplň pracovných miest v **popisoch práce**.

Tvorba organizačnej štruktúry

Na zloženie organizačnej štruktúry SMB nie je určená žiadna šablóna, mala by však zodpovedať celkovej organizačnej štruktúre organizácie. Organizačné štruktúry sektora bezpečnosti sa v jednotlivých organizáciách môžu líšiť, pretože:

- každá organizačná štruktúra odráža vnímanie priorít organizácie a bezpečnostného sektora vrcholovým manažmentom a bezpečnostným manažmentom,
- podoba bude závislá aj od bezpečnostného personálu,
- štruktúra musí byť pružná, vysoko premenlivá, aby odrážala všetky bezpečnostné činnosti.

Organizačná štruktúra SMB by mala:

- podporovať efektívne fungovanie organizácie a korešpondovať s jej strategickými zámermi,
- byť jednoduchá, prehľadná z hľadiska členitosti, hierarchie i komunikačných väzieb,
- byť prostriedkom skvalitnenia riadenia, nie jeho cieľom.

Okrem toho by **organizačná štruktúra SMB mala byť vytvorená podľa nasledovných zásad** *(Sennewald, 2003)*:

- **logické rozdelenie úloh alebo povinností**,
- **jednotné velenie** – podriadený by mal byť pod priamou kontrolou iba jedného priameho nadriadeného,
- **vymedzenie právomoci a zodpovednosti** – vo vnútri úseku bezpečnosti špecificky, v celej organizácii všeobecne,
- **delegovanie zodpovednosti aj s primeranou právomocou** – za pridelenú právomoc musí byť aj primeraná zodpovednosť,
- **rozpätie riadenia** – jeden vedúci môže efektívne riadiť len obmedzené množstvo podriadených a tento limit by nemal byť prekročený, od maximálne piatich podriadených na najvyššej úrovni po maximálny počet dvanásť podriadených, na najnižšej úrovni v organizácii,
- **koordinovanie** všetkého úsilia jednotlivých jednotiek a personálu pre harmonické dosiahnutie cieľov organizácie.

Efektívnosť SMB sa dosahuje tým, že ***náklady na jeho zavedenie by nemali byť väčšie, ako očakávané straty vzniknuté pôsobením bezpečnostných rizík.*** S čím menšími nákladmi dokážeme účinne chrániť aktíva organizácie, tým je efektívnosť SMB vyššia. Ak SMB nedokáže účinne ochrániť aktíva organizácie, potom budú následky negatívnej udalosti zvýšené aj o náklady, ktoré sme vynaložili na jeho vytvorenie.

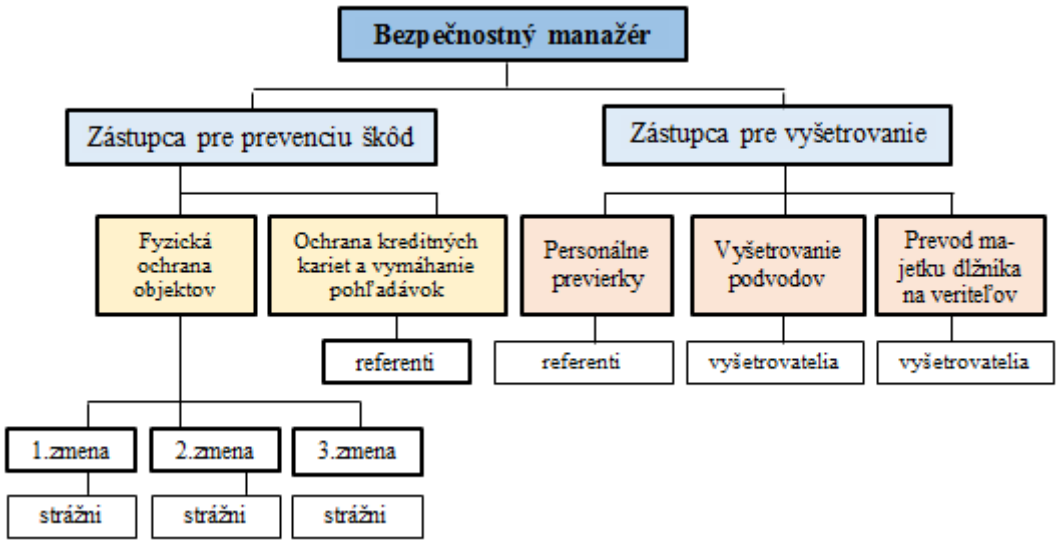
Zo skúseností vyplýva, že každá organizácia si zavádza taký systém bezpečnosti, ktorý funguje najlepšie v jej konkrétnych podmienkach a situácii, pričom platí, že:

- starostlivosť o bezpečnosť si musí zaisťovať každá organizácia ***sama,***
- starostlivosť o bezpečnosť je ***trvalý*** (permanentný) ***proces,*** ktorý si vyžaduje profesionálny prístup,
- bezpečnosť musí byť ***dosiahnuteľná a cenovo prístupná.***

Neexistuje optimálna organizačná štruktúra, existujú len organizačné štruktúry, ktoré optimálne využívajú manažérov a bezpečnostných pracovníkov na dosiahnutie bezpečnostných cieľov organizácie. Ak je manažér schopný organizátor, ním vyprojektovaná organizačná štruktúra vytvára také prostredie, v ktorom jednotlivci fungujú a ktoré podporuje dosiahnutie stanovených cieľov.

Príklad organizačnej štruktúry SMB

Podľa Sennewalda je organizačná štruktúra úseku bezpečnosti organizácie dvojrozmerná. Na vodorovnej rovine je uvedené rozdelenie oblastí povinností, na zvislej rovine sú definované úrovne právomoci alebo hodnosti (obr. 14).



Obr. 14 Príklad formálnej organizačnej štruktúry úseku bezpečnosti (zdroj Sennewald, 2003)

Zodpovednosť za bezpečnosť pod vedením bezpečnostného manažéra je rozdelená na dve oblasti: oblasť prevencie škôd a oblasť vyšetrovania. Na vrchole uvedenej hierarchie bezpečnosti je **bezpečnostný manažér**, ktorý je osobne zodpovedný za manažérstvo bezpečnosti. Podľa uvedeného príkladu zodpovedá len za fyzickú ochranu objektov a vyšetrovanie, nie sú tu zahrnuté všetky sektory bezpečnosti, v ktorých sa vyskytujú bezpečnostné riziká a ktoré niekto musí riešiť, napr. BOZP, prevádzka, informačné systémy a pod.

Bezpečnostný manažér má svoju autoritu a delegovanú zodpovednosť a právomoc, nemal by sa vyhovárať na iných manažérov, pretože ***bezpečnosť je výlučne jeho zodpovednosťou***. Nemôže však vykonávať všetky bezpečnostné činnosti sám a potrebuje talentovaných ľudí z organizácie, aby mu v tejto činnosti pomohli. V závislosti na veľkosti organizácie a rozsahu bezpečnostných úloh môže podľa autora bezpečnostný manažér potrebovať 2 až 300 ľudí, ktorí majú mať v otázkach bezpečnosti tiež zodpovednosť a právomoc.

Zástupcovia bezpečnostného manažéra pre obe uvedené oblasti v tomto príklade sú na rovnakej úrovni, ale zodpovedajú každý za svoju oblasť, pričom sú obaja podriadení bezpečnostnému manažérovi. Podobne sú rozdelené povinnosti pri prevencii škôd na vedúcich oddelení ochrany objektov a vymáhania pohľadávok *(Sennewald, 2003).*

Nejednotnosť a často decentralizované riadenie jednotlivých zložiek SMB *ovplyvňuje celkové manažérstvo bezpečnosti, komunikáciu a spoluprácu jednotlivých úsekov.* Na skvalitnenie účinnosti SMB je preto vhodné zavádzať *komplexný prístup k procesu budovania bezpečnosti,* v **Integrovanom systéme manažérstva bezpečnosti.**

5.3 INTEGROVANÝ SYSTÉM MANAŽÉRSTVA BEZPEČNOSTI

Bezpečnosť je záležitosťou celej organizácie, preto by mala byť aj centrálne riadená. Vedenie organizácie musí rozhodnúť, akým spôsobom sa chce zaoberať bezpečnosťou, aký systém manažérstva bezpečnosti bude v organizácii implementovať a ako bude stav bezpečnosti hodnotiť a formovať jej budúci vývoj. Pre väčšie a zložitejšie organizácie je výhodné v rámci celkového systému riadenia postupne vytvárať Integrovaný systém manažérstva bezpečnosti.

Integrovaný systém manažérstva bezpečnosti (ISMB) je jednotný ***integrovaný systém pre centralizované riadenie všetkých bezpečnostných štruktúr a procesov***, aby boli splnené bezpečnostné ciele organizácie a uspokojení všetci zainteresovaní účastníci.

Takýto systém v sebe spája všetky súvisiace komponenty bezpečnosti organizácie pre jednoduchšiu správu a prevádzku. Nejde o obyčajné spojenie samostatných systémov, ale skôr o ich integráciu so vzájomnými väzbami tak, že ich štruktúry a procesy sú plynule riadené a vykonávané bez duplikácie.

Súčasti ISMB, ktoré sú **spoločné** pre všetky jednotlivé systémy manažérstva bezpečnosti a ochrany zahŕňajú ***zdroje (***ľudia, zariadenie a vybavenie atď.) a ***procesy*** (dokumentované v jednotlivých technických normách a uplatňované v rámci celej organizácie).

Štruktúru ISMB organizácie obvykle tvoria:

1. **generálny riaditeľ,**
2. **riadiaci orgán bezpečnosti** – výbor alebo rada bezpečnosti,
3. **líniovímanažéri,** zapojení do manažérstva bezpečnosti vo svojich úsekoch,
4. **bezpečnostný manažér s podriadenými zložkami:**
   a) **centrálny útvar bezpečnosti,**
   b) **systémy manažérstva bezpečnosti,**
   c) **systémy ochrany osôb a majetku.**

Riadiaci orgán bezpečnosti

Do výboru alebo rady bezpečnosti sú zaradení najmä ***vrcholoví manažéri***, zastupujúci najdôležitejšie úseky organizácie, ktorí majú významný podiel na organizovaní bezpečnosti, napr. *finančný, výrobný, informačný, personálny, technický, marketingový, právny* a pod. Okrem nich by do neho mal byť zaradený aj bezpečnostný manažér organizácie.

Riadiaci orgán bezpečnosti v súčinnosti s ***centrálnym útvarom bezpečnosti*** zodpovedá za:

- **prihlásenie sa k uplatňovaniu bezpečnosti** – vydáva ***prehlásenie o zavedení systému manažérstva bezpečnosti*** v organizácii,
- určenie ***strategického zamerania, vízie a cieľov bezpečnosti,***
- vytýčenie jasného smeru v podobe dôveryhodnej ***bezpečnostnej politiky,*** ako dokumentu strategického významu s dlhodobou platnosťou, ktorý umožňuje vedeniu riadiť bezpečnostné procesy,
- stanovenie ***bezpečnostných štandardov a kritérií rizík,***
- vytvorenie ***ISMB*** a jeho implementáciu využitím Plánu implementácie ISMB,
- určenie ***primeraných zdrojov*** na dostatočne dlhú dobu,
- zvyšovanie ***odborných znalostí o bezpečnosti***, prostredníctvom bezpečnostnej literatúry, školení, seminárov a pod.,
- ***propagovanie bezpečnosti*** v celej organizácii.

Systémy manažérstva bezpečnosti

Zabezpečenie úspešnosti organizácie rôznymi druhmi systémov manažérstva niektorých oblastí bezpečnosti sa v dnešnej zložitej ekonomickej situácii stáva čoraz viac samozrejmosťou podľa medzinárodne uznávaných štandardov. K **systémom manažérstva bezpečnosti** patria najmä tieto systémy:

a) **Systém manažérstva bezpečnosti a ochrany zdravia pri práci** *(Health and Safety Management System, HSMS).*
b) **Environmentálny manažérsky systém** *(Environmental Management System, EMS).*
c) **Systém manažérstva informačnej bezpečnosti** *(Information Security Management System, ISMS).*
d) **Systém manažérstva kontinuity činností** *(Business Continuity Management System, BCMS).*
e) **Systém manažérstva incidentov** *(Incident Management System).*
f) **Manažérstvo aktív – Manažérske systémy –** *(Asset management – Management systems).*
g) **Facility manažment – Integrovaný manažérsky systém –** *(Facilities Management – Integrated Management System).*
h) **Systém manažérstva bezpečnosti – Posúdenie rizika podvodu a zneužitia** *(Security Mangement System – Fraud risk assessment).*
i) **Systém manažérstva poskytovania služieb súkromnej bezpečnosti (***Management system for private security operations).*
j) **Systém manažérstva bezpečnosti potravín** *(Food safety management system).*
k) **Systém manažérstva bezpečnosti cestnej premávky** *(Road traffic safety management system).*

Systém manažérstva aktív bol popísaný v prvej časti učebnice Bezpečnostný manažment. Systém manažérstva BOZP, Enviromentálny manažérsky systém a Systém manažérstva informaćnej bezpečnosti tvoria v mnohých organizáciách spoločne so Systémom manažérstva kvality **Integrovaný manažérsky systém,** charakterizovaný v kap. 7.

Systémy ochrany osôb a majetku

V ISMB sa na zaistenie **ochrany osôb a majetku organizácie** v niektorých podsektoroch, oblastiach a zložkách bezpečnostného sektora organizácie vytvárajú **špecifické systémy ochrany,** najmä **systémy:**

1. **Ochrany osôb:**
   a) ochrany VIP osôb a klientov (Bodyguarding),
   b) ochrany zamestnancov pred fyzickým a nefyzickým násilím.
2. **Ochrany priestorov a objektov (budov):**
   a) ochrany objektov a chránených priestorov s utajovanými skutočnosťami,
   b) ochrany priestorov a objektov s inými aktívami (majetkom),
   c) ochrany objektov kritickej infraštruktúry,
   d) ochrany objektov jadrových zariadení.
3. **Požiarnej ochrany.**
4. **Ochrany zdravia pri práci:**
   a) ochrany pracovného prostredia a pracovných podmienok,
   b) ochrany technických zariadení a ich prevádzky.
5. **Ochrany prevádzkových činností:**
   a) ochrany prevádzky priemyselných podnikov s nebezpečnými látkami a ich okolia pred priemyselnými haváriami – prevencia závažným priemyselným haváriám,

b) ochrany prevádzky jadrových zariadení a ich okolia pred jadrovými haváriami.

6. **Ochrany dôležitých informácii:**
   a) ochrany utajovaných skutočností (OUS),
   b) ochrany osobných údajov,
   c) ochrany pred podvodmi a zneužitím,
   d) ochrany komerčných informácii (obchodné, bankové, listové tajomstvo a pod.).
7. **Ochrany vnútorného poriadku v organizácii.**
8. **Ochrany ďalších bezpečnostných záujmov organizácie**.

Každý z uvedených systémov ochrany predstavuje **integrovaný súbor reálnych prvkov,** *ktoré majú stanovené funkcie a úlohy na zaistenie bezpečnosti* v danom čase a priestore a sú medzi sebou spojené sieťou ***vzťahov (väzieb)***, medzi ktorými pôsobí spätná väzba.

Vyvárajú sa **v súlade s ustanoveniami bezpečnostných právnych noriem**. Integrujú ***ľudí, prostriedky a postupy*** na ochranu osôb a majetku (objektov) pred násilným napadnutím a ochranu životného prostredia pred závažnými haváriami.

Každý uvedený systém ochrany osôb a majetku obsahuje:

- **štruktúru systému ochrany,**
- **proces ochrany.**

Do **štruktúry systému ochrany** sú zapojené:

- **sily manažmentu a bezpečnostného manažmentu** organizácie, ktoré nepretržite využívajú ***bezpečnostné informácie*** o vonkajšom a vnútornom bezpečnostnom prostredí a bezpečnostných rizikách, na ***rozhodovanie a komunikáciu*** s nadriadenými i podriadenými o stave bezpečnosti a bezpečnostných opatreniach.
- **sily ochrany**, ktoré tvoria vlastní i prenajatí ***bezpečnostní pracovníci***,
- **prostriedky ochrany**, ktoré tvoria najmä materiálne prostriedky a technológie na ochranu osôb a majetku,
- **režimové opatrenia,** ktoré tvorí súbor nariadení a obmedzení.

Väčšina uvedených systémov ochrany osôb a majetku bola riešená v prvom diele učebnice Bezpečnostný manažment. V ďalšej časti učebnice sa budú riešiť len *Systém ochrany objektov a Systém požiarnej ochrany.*

5.4 CENTRÁLNY ÚTVAR BEZPEČNOSTI

Centrálny útvar bezpečnosti, priamo podriadený bezpečnostnému manažérovi, je výhodné vytvoriť vo väčších organizáciách. Tento útvar môže mať rôzny názov (*sekcia, oddelenie, skupina).* Do tohto útvaru je potrebné zaradiť niektoré tímy alebo skupiny pracovníkov, ktoré budú **riešiť základné všeobecné zodpovednosti a úlohy bezpečnosti prelínajúce sa v rámci celej organizácie.**

Medzi tieto úlohy patria najmä: *riadenie systému manažérstva bezpečnosti; manažérstvo rizika; plánovanie bezpečnosti; manažérstvo ľudských zdrojov; manažérstvo bezpečnostných incidentov; vyšetrovanie; kontrola a zabezpečenie požadovanej kvality bezpečnosti.*

V závislosti na druhu a veľkosti organizácie ho môžu tvoriť najmä tieto organizačné útvary (tímy):

a) výkonného manažmentu bezpečnosti (*Security Management Team),*
b) manažérstva rizika *(Risk Management Team),*
c) plánovania *(Plan Development Team),*
d) manažérstva ľudských zdrojov *(Human Resource Management Team):*
- personálne previerky,
- ochrana osobných údajov,

e) manažérstva incidentov *(Incident Management Team),*
f) organizovania školenia a nácvikov (*Exercise Management Team),*
g) kontroly a zabezpečenia požadovanej kvality bezpečnosti.

Okrem uvedených, môžu byť v centrálnom útvare zaradené aj ďalšie tímy, napr. na ***riešenie krízových situácií, záchranný tím*** a pod. Ďalšie špeciálne tímy, ktoré tu môžu byť zaradené, sa vytvárajú v ***Systéme manažérstva kontinuity činností.***

V mnohých prípadoch, najmä v menších organizáciách, sa pre zníženie počtu zamestnancov **delegujú** úlohy niektorých tímov iným zložkám, napr. bezpečnostný manažér plní aj úlohy plánovania, kontroly bezpečnosti a manažérstva rizika, alebo sa spája vyšetrovanie s manažérstvom bezpečnostných incidentov a pod.

Výkonný manažment bezpečnosti

Výkonný manažment bezpečnosti predstavuje **odborný orgán pre manažérstvo bezpečnosti,** priamo podriadený bezpečnostnému manažérovi, ktorý:
- špecifikuje požiadavky na vytváranie, zavádzanie, prevádzku, monitorovanie, preskúmanie, udržiavanie a zlepšovanie SMB,
- vykonáva proces manažérstva rizík (ak nie je na to vyčlenený samostatný tím),
- stanovuje požiadavky na vykonávanie bezpečnostných kontrol,
- zostavuje plán na tvorbu a schvaľovanie bezpečnostných dokumentov,
- zodpovedá za obsah bezpečnostných dokumentov a zaisťuje ich schválenie vo vedení organizácie,
- rieši všetky vzniknuté problémy v rámci ISMB.

Všetky tieto úlohy v minulosti často plnil a v niektorých menších organizáciách ešte plní osobne bezpečnostný manažér. Veľkosť manažérskeho tímu závisí od veľkosti, zložitosti a účelu organizácie. Kto má byť v tomto manažérskom tíme na riadenie bezpečnosti závisí od rozhodnutia vrcholového manažmentu. Členmi tímu by mali byť ***zástupcovia zo všetkých podsektorov bezpečnostného sektora organizácie,*** z ktorých jeden je vedúcim. Súčasťou je aj sekretariát bezpečnostného manažéra (ak je vytvorený). Podmienkou je, aby členovia tímu

mali dostatočné skúsenosti s manažérstvom bezpečnosti vo svojich odbornostiach a aby boli schopní vydávať a riadiť plnenie úloh a niektoré aj vykonávať osobne.

Tím manažérstva rizika

V zložitejšej organizácii je za manažérstvo rizika všeobecne zodpovedný **manažér pre manažérstvo rizika**, *ktorý* má v podriadenosti **tím manažérstva rizika**.

V tíme manažérstva rizika môžu byť najmä:

- ***analytik riadenia rizík,***
- ***manažér na posudzovanie pracovnej nespôsobilosti,***
- ***havarijný referent,***
- ***technici pre riadenie rizík,***
- ***asistenti.***

Odborníci na manažérstvo rizika plnia nasledujúce úlohy:

- posudzujú ***externé a interné súvislosti*** organizácie,
- vytvárajú **Politiku manažérstva rizika,**
- identifikujú: ***vlastníkov rizika, osoby zodpovedné za*** vývoj, zavedenie a udržiavanie ***štruktúry*** manažérstva rizika a ďalšie osoby na všetkých úrovniach organizácie, zodpovedné za ***proces manažérstva rizika,***
- vytvárajú procesy ***merania výkonnosti*** manažérstva rizika, ***podávania externých a interných správ*** a zdokonaľujúcich procesov,
- spracovávajú a zavádzajú **Plán manažérstva rizika** a jeho integráciu do iných plánov organizácie, napr. do strategického plánu,
- vytvárajú mechanizmy internej ***komunikácie*** a oznamovania informácií o rizikách,
- vytvárajú **Plán komunikácie so zainteresovanými účastníkmi,**
- ***zavádzajú štruktúru manažérstva rizika*** do všetkých procesov organizácie,
- ***realizujú komunikáciu a poradenstvo*** s externými a internými zainteresovanými účastníkmi počas všetkých etáp manažérstva rizika,
- ***analyzujú vonkajšie a vnútorné bezpečnostné prostredie*** organizácie,
- ***určujú ciele, stratégiu, rozsah a parametre činnosti*** organizácie alebo jej častí na ktoré sa aplikuje proces manažérstva rizika,
- ***spolupracujú*** s vrcholovým manažmentom ***na tvorbe kritérií rizík,***
- ***identifikujú*** vonkajšie a vnútorné ***zdroje rizík***, oblasti ich následkov, udalosti a ich príčiny a potenciálne následky, a vytvoria ***zoznam rizík*** založený na udalostiach, ktoré by mohli vytvoriť, podporiť, zabrániť, znehodnotiť, urýchliť alebo pozdržať dosiahnutie zámerov,
- ***analyzujú riziká*** určením následkov a ich pravdepodobnosti a ďalších vlastností rizika,
- ***hodnotia riziká*** porovnaním zistenej úrovne rizika s kritériami rizika a rozhodnú o potrebe zaobchádzania s nimi,
- ***navrhujú spôsoby zaobchádzania s rizikami,***
- spracovávajú a zavádzajú **Plán zaobchádzania s rizikami,**
- ***monitorujú a preskúmavajú*** stav bezpečnosti s dôrazom na zvyškové riziká.

Tím plánovania bezpečnosti

Tím plánovania bezpečnosti je špecializovaným tímom, zodpovedným za vytvorenie a implementáciu ISMB v organizácii. Posudzuje rozdielne stanoviská vo veci ochrany aktív, rieši konflikty, ktoré môžu vznikať medzi organizačnými jednotkami jednotlivých oblastí bezpečnosti. Tím by mal priamo riadiť bezpečnostný manažér, na práci tímu pri plánovaní sa podieľajú vedúci všetkých vymedzených súčastí sektora bezpečnosti v organizácii.

Tím v spolupráci s vrcholovým manažmentom a manažmentom ISMB konkrétne vypracováva hlavné bezpečnostné dokumenty, napr. Bezpečnostnú politiku, Plán implementácie

ISMB, Havarijný plán, Bezpečnostný plán ochrany objektu alebo Projekt ochrany objektu a ďalšie plány, smernice, metodiky činnosti a iné organizačné dokumenty.

Tím manažérstva ľudských zdrojov

Na riadenie ľudských zdrojov v oblasti bezpečnosti je možné vo veľkých a zložitých organizáciách vytvoriť samostatný **tím manažérstva ľudských zdrojov,** alebo na plnenie týchto úloh ***využiť príslušníkov personálneho oddelenia*** (skupiny) organizácie. Vytvorený samostatný tím by mal úzko spolupracovať s personálnym úsekom, ktorý rieši väčšinu personálnych záležitostí. Personálni pracovníci, ktorí riešia personálne otázky bezpečnosti:

- organizujú ***nábor a výber bezpečnostných pracovníkov***,
- zabezpečujú ***bezpečnostné previerky bezpečnostného personálu*** (Vyhláška NBÚ č. 331/2004 Z. z. o personálnej bezpečnosti a o skúške bezpečnostného zamestnanca),
- spolupracujú pri zabezpečovaní ***ochrany osobných údajov všetkých zamestnancov*** (Zákon č. 122/2013 Z. z. o ochrane osobných údajov),
- spracovávajú **Program bezpečnostného vzdelávania zamestnancov,** spojený s implementáciou bezpečnostných opatrení,
- uskutočňujú ***prípravu všetkých zamestnancov i poskytovateľov služieb*** podľa spracovaného programu, na zvýšenie bezpečnostnej kultúry organizácie,
- pravidelne ***vyhodnocujú vzdelávanie*** vlastného personálu i poskytovateľov služieb o bezpečnosti.

Tím kontroly

Na kontrolu sa môže vytvárať **tím kontroly** alebo ju vykonávajú ***určení jednotlivci*** vo svojich úsekoch. Ich úlohou je:

- vykonávať ***periodické alebo náhodné kontroly*** na identifikáciu úrovne procesu manažérstva bezpečnosti,
- zaistiť ***program na vyhodnotenie SMB,*** na zistenie či smeruje k dosiahnutiu bezpečnostných cieľov a rešpektuje bezpečnostné štandardy,
- zaistiť, že externý ***poskytovateľ bezpečnostných služieb*** poskytuje služby a plní povinnosti v súlade s uzavretou zmluvou a národnými právnymi predpismi.

5.5 LITERATÚRA

BELAN, Ľ [2015]: *Bezpečnostný manažment. Bezpečnosť a manažérstvo rizika*. Žilina: Edis – vydavateľstvo ŽU. ISBN ISBN 978-80-554-1138-5

MÍKA, V. T. [2006]: *Základy manažmentu.* Virtuálne skriptá. [on line]. Vybrané prednášky pre študentov externého štúdia FŠI ŽU. Žilina: ISBN 978-80-88829-78-2.

SENNEWALD, Ch. A. [2003]: *Effective Security Management*. Elsevier Science USA, ISBN 0-7506-7454-7.

6 PROCES MANAŽÉRSTVA BEZPEČNOSTI

Zabezpečenie úspešnosti organizácie prostredníctvom rôznych ***systémov manažérstva*** podľa medzinárodne uznávaných štandardov sa v dnešnej zložitej ekonomickej situácii stáva čoraz viac samozrejmosťou.

Vzhľadom na podstatné rozšírenie podnikateľských činností sa množstvo organizácií snaží o zavedenie a certifikáciu **viacerých systémov manažérstva**, napr. ***systém manažérstva kvality***, ale aj ***systém manažérstva bezpečnosti organizácie*** i ***manažérstva bezpečnosti*** niektorých **podsektorov bezpečnostného sektora,** ako sú ***BOZP, environmentálny, informačný či kontinuity činností*** a pod. To vyžaduje, aby sa tieto jednotlivé systémy dali ľahko kombinovať alebo integrovať efektívnym a účinným spôsobom.

Pretože pre každý systém manažérstva bola zavedená samostatná norma, bolo potrebné nájsť účinný a efektívny spôsob pre ich spojenie či integrovanie. Doteraz existovali rôzne rozdiely medzi požiadavkami a terminológiou v jednotlivých systémoch, pre čo bola ich integrácia problematická.

Spoločná technická koordinačná skupina Medzinárodnej organizácie pre normalizáciu preto vytvorila **prílohu SL** (*Annex SL, predtým v ISO Guide 83*), s cieľom priniesť zhodné a kompatibilné normy pre systémy manažérstva, aby tento proces uľahčila.

Úlohou Spoločnej technickej koordinačnej skupiny (JTCG) je koordinovať všetky práce technických výborov (TC). Než tento poradný orgán ISO vznikol, bola každá norma pre systémy manažmentu vytváraná samostatne príslušným technickým výborom. Manažment kvality mal na starosti TC 176, environmentálny manažment riadil TC 207 atď., v súčasnosti je v JTCG zapojených niekoľko ďalších TC. Skupina si dala za cieľ zjednotiť štruktúru systémových noriem a obmedzovať, resp. bezdôvodne nepovoľovať výnimky.

Príloha SL predstavuje záväzný návod, podľa ktorého sa od mája 2013 majú riadiť všetci spracovatelia noriem ISO. Je jednou z príloh Nariadenia ISO/IEC, P1 „Konsolidovaný dodatok – Špecifické postupy ISO“. Existujú desiatky príloh Nariadenia ISO P1, preto je príloha „S“ ďalej rozdelená až na „SL“.

Príloha SL všeobecne definuje **rovnakú štruktúru, jadro textu a spoločné pojmy a definície** pre budúce generácie **systémov manažérstva** a má veľmi významný vplyv na organizácie, poradcov, certifikačné orgány, akreditačné orgány, audítorov a systémy manažérstva. Táto príloha prakticky predstavuje **postupnosť procesu manažérstva pre všetky jeho druhy.**

Pre používateľov noriem ISO 9001, ISO 14001 nebo ISO 27001 je dôležitá časť 2 Prílohy SL, ktorá určuje usporiadanie noriem a zjednocuje v nich pojmy. **Príloha 2 je záväzná a určuje desať častí (etáp), ktoré musia byť pre všetky systémy manažérstva zhodné.** Tým by sa mala dosiahnuť zásadná redukcia textu v príručkách pre integrované systémy riadenia (manažérstva).

Všetky normy pre systémy manažmentu sú teraz riadené z jedného miesta, ktoré dbá na dodržiavanie pravidiel. Je určená pevná štruktúra manažérskych systémov, normy majú asi 30 % identického spoločného textu požiadaviek. Základné pojmy a ich definície boli zjednotené. Konečne existuje záväzný postup pre vytváranie noriem pre systémy manažmentu, nové požiadavky sú prehľadné a dá sa s nimi rýchlo pracovať.

Podľa tejto prílohy sa budú **riadiť všetky nové manažérske systémy** a ***všetky aktuálne manažérske systémy budú na tento model prechádzať.*** V budúcnosti by všetky manažérske systémy mali byť konzistentné a kompatibilné – všetky budú mať rovnaký základ a pro-

stredie, čo by mohol byť začiatok konca konfliktov, duplikácie, zmätkov a nepochopenia medzi rôznymi systémami. Toto pomôže zaistiť súdržnosť medzi budúcimi a revidovanými normami systémov manažérstva a umožní užívateľom normy ľahšie pochopiť. Bude tiež jednoduchšie a efektívnejšie na tomto základe integrovať viac noriem v rámci jednej organizácie.

V súčasnosti je príloha SL už zapracovaná v normách manažérstva:

- ISO 9001:2015 Systémy manažérstva kvality – Požiadavky.
- ISO 27001:2014 Informačné technológie: Bezpečnostné techniky, Systémy manažérstva informačnej bezpečnosti – Požiadavky.
- ISO 22301:2012 Spoločenská bezpečnosť: Systémy manažérstva kontinuity činností – Požiadavky.
- ISO 39001 Bezpečnosť premávky na pozemných komunikáciách – Systémy manažérstva.
- ISO 55001 Manažérstvo aktív (plánované na rok 2014, v súlade s prílohou SL).
- ISO 26000:2010 Manažérstvo spoločenskej zodpovednosti.

V nasledujúcich rokoch sa pripravuje zapracovanie prílohy SL do noriem:

- *ISO/CD 45001:2016 Systémy manažérstva bezpečnosti a ochrany zdravia pri práci – Požiadavky.*
- *ISO 14001:2016 Environmentálny manažérsky systém.*
- *ISO 55000 Systém manažérstva aktív.*

V novele ISO 9001:2015 (i v novelách ISO 14001:2015, ISO 45001:2016, STN ISO/IEC 27001:2014 a STN ISO 22301:2013) bude kladený značný dôraz na **manažérstvo rizika podľa STN ISO 31000:2011** Manažérstvo rizika. Zásady a návod.

6.1 ŠTRUKTÚRA NORIEM SYSTÉMOV MANAŽÉRSTVA

Príloha SL určuje jednotnú postupnosť procesu manažérstva pre všetky systémy manažérstva v nasledujúcej podobe:

0 ÚVOD
1 ROZSAH
2 CITOVANÉ NORMATÍVNE DOKUMENTY
3 TERMÍNY A DEFINÍCIE

4 SÚVISLOSTI ORGANIZÁCIE
4.1 Pochopenie organizácie a jej súvislostí.
4.2 Pochopenie potrieb a očakávaní zainteresovaných účastníkov.
4.3 Stanovenie rozsahu Systému manažérstva XY (zameranie systému manažérstva, napr. kvality, informačnej bezpečnosti a pod.).
4.4 Systém manažérstva XY.

5 VEDENIE
5.1 Vedenie a záväzok.
5.2 Politika.
5.3 Roly, zodpovednosti, právomoci a riadiace orgány v organizácii.

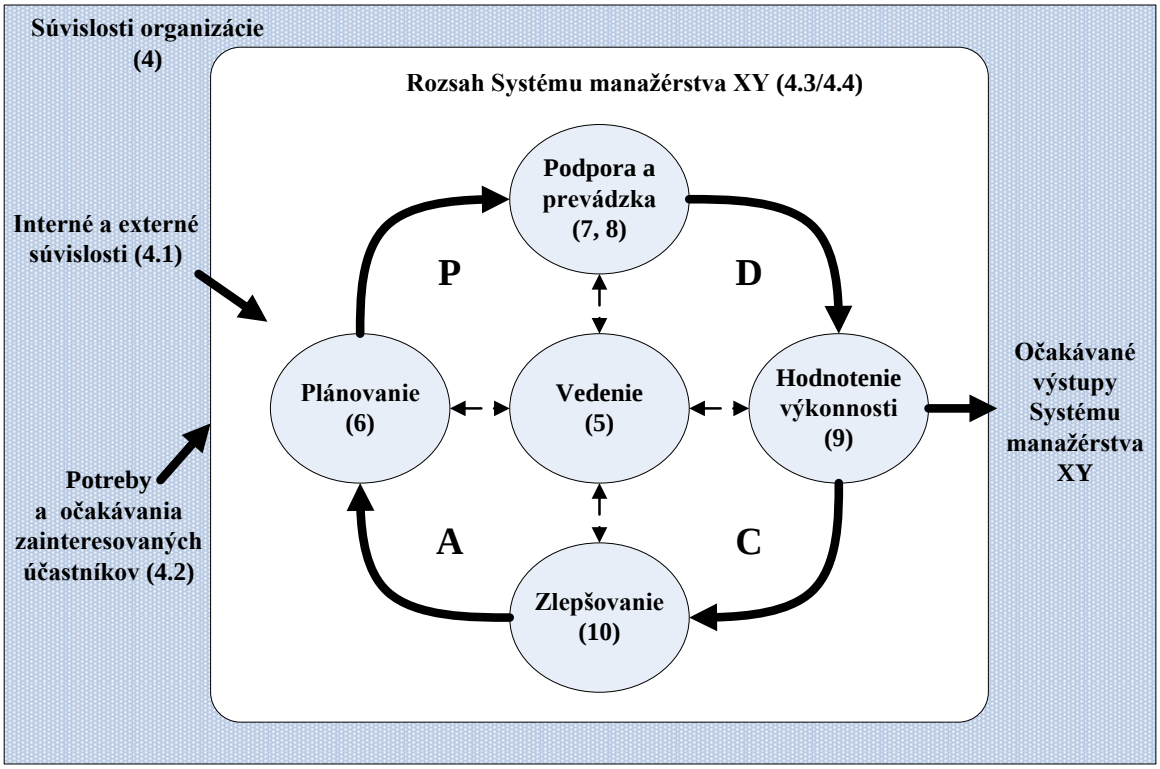
6 PLÁNOVANIE
6.1 Činnosti, ktoré sa zaoberajú rizikami a príležitosťami.
6.2 Ciele XYa plánovanie ich dosiahnutia.

7 PODPORA
7.1 Zdroje.
7.2 Kompetencie.
7.3 Povedomie.
7.4 Komunikácia.
7.5 Zdokumentované informácie.
7.5.1 Všeobecne.
7.5.2 Vytváranie a aktualizácia.
7.5.3 Riadenie zdokumentovaných informácií.

8 PREVÁDZKA
8.1 Operatívne plánovanie a riadenie.

9 HODNOTENIE VÝKONNOSTI
9.1 Monitorovanie, meranie, analýzy a vyhodnotenie.
9.2 Interný (vnútorný) audit.
9.3 Preskúmanie manažmentom.

10 ZLEPŠOVANIE
10.1 Nezhoda a nápravné opatrenia.
10.2 Trvalé zlepšovanie.



Obr. 15 Model systému manažérstva XY

Obsah normy je možné rozdeliť na časti podľa obr. 15:

1. **Všeobecná časť** – body 0 až 3.
2. **Vstupy do procesu manažérstva** – bod 4.
3. **Cyklický proces manažérstva podľa modelu P** (5, 6, 7), **D** (8), **C** (9), **A** (10).

Charakteristika normy pre systémy manažérstva

Úvod, rozsah a **citované normatívne dokumenty** budú mať odlišný, špecifický obsah pre každý systém manažérstva.

0. **Úvod –** Príloha SL charakterizuje štruktúru pre všeobecný systém manažérstva. Táto všeobecná štruktúra bude vyžadovať doplnenie – špecifické požiadavky na to, aby sa vytvorili špecifické normy pre kvalitu, životné prostredie, manažérstvo služieb, bezpečnosť potravín, kontinuitu činností, informačnú bezpečnosť, systém manažérstva energie.

   V budúcnosti budú mať všetky nové normy systémov manažérstva rovnakú všeobecnú formu a obsah. Súčasné normy systémov manažérstva prechádzajú obdobím ich revízie, ktorá by mala byť dokončená v priebehu niekoľkých rokov. Príloha SL poskytuje šablónu pre ich prepracovanie. V týchto nových normách je potrebné sústrediť sa na špecifické požiadavky v časti 8. Prevádzka. V budúcnosti by všetky normy ISO pre systémy manažérstva mali byť zladené a kompatibilné.

   Pre audítorov systémov manažérstva to bude znamenať, že pre všetky audity tam bude hlavný súbor všeobecných požiadaviek, ktoré musia byť splnené bez ohľadu na to, ktorý systém manažérstva sa preveruje.

1. **Rozsah** – mal by definovať ***„plánovaný výsledok“,*** termín „očakávaný výsledok“ sa nebude používať. Audítori by mali brať do úvahy zosúladenie súvislostí organizácie (časť 4.) pre všetky systémy manažérstva.
2. **Citované normatívne dokumenty** – poskytujú odkazy, odvolávajúce sa na normy alebo jednotlivé publikácie špecifických noriem.
3. **Termíny a definície** – pojmy a definície použiteľné v konkrétnych normách pre systémy manažérstva.
4. **Súvislosti organizácie –** organizácia má túto časť vykonať ešte pred zvážením zavedenia akejkoľvek normy ISO systému manažérstva. Predstavuje základ pre systém manažérstva – ide o určenie, prečo vlastne organizácia existuje. Organizácia potrebuje určiť:
   - svoje závažné ***vnútorné a vonkajšie súvislosti***, ktoré môžu mať vplyv na to, čo chce dosiahnuť,
   - všetkých ***zainteresovaných účastníkov a ich požiadavky,***
   - ***rozsah a rozhranie systému manažérstva*** – čo je vo vnútri a čo je mimo neho.

   Uvedené skutočnosti sú potrebné na určenie cieľov organizácie. Nakoniec organizácia potrebuje ***vytvoriť a prevádzkovať svoj systém manažérstva***. Identifikované problémy a požiadavky sa budú riešiť v časti 6. Plánovanie.

   Audítori budú mať v spracovaných súvislostiach stručný a jasný ***zoznam*** zistených skutočností, aby ich mohli identifikovať a potvrdiť. V tomto zozname by mali byť:
   - ciele organizácie a plánované výsledky,
   - vnútorné a vonkajšie problémy,
   - významní zainteresovaní účastníci a ich požiadavky,
   - rozsah systému manažérstva.

Tieto údaje poskytnú súhrnný významný vnútorný pohľad na organizáciu. Nemalo by ísť iba o prostý zoznam, ale o ***zoznam, ktorý poskytne súhrnný významný vnútorný pohľad na organizáciu, ktorý je jasný a zrozumiteľný.***

5. **Vedenie** – na prvý pohľad sa táto časť zdá byť len opätovným zdôraznením predchádzajúceho – ***politika, roly, zodpovednosti a právomoci*** v organizácii atď. Nové ustanovenia pre najvyššiu úroveň vedenia kladú ***osobitný dôraz na vedenie, nielen riadenie,*** ako je stanovené v predchádzajúcich štandardoch. To znamená, že vrcholový manažment má teraz väčšiu zodpovednosť a zapojenie do systému manažérstva. Je potrebné:
   - začleniť požiadavky systému manažérstva do hlavných podnikateľských procesov organizácie,
   - zabezpečiť, aby systém manažérstva dosiahol svoje plánované výsledky,
   - prideliť mu potrebné zdroje.

   Vrcholový manažment je tiež zodpovedný za ***komunikáciu*** systému manažérstva a ***zvýšenie povedomia*** o jeho dôležitosti a za ***zapojenie zamestnancov***. Navyše musí dať najavo svoj ***záväzok na uistenie, že systém manažérstva vytvorí.*** Zapojenie vrcholového manažmentu do systému manažérstva je potom jednoznačné a aktívne.

   Politika XY (určitého systému manažmentu) sa tým tiež zosilní. Musí zahŕňať záväzok na splnenie platných požiadaviek a trvalé zlepšovanie systému manažérstva. Musí byť oznámená vo vnútri organizácie a byť k dispozícii pre zainteresovaných účastníkov.

   Audítori budú môcť potom ľahšie preveriť záväzok manažmentu – požiadavky sú oveľa viac špecifické a reálne, a požadované dôkazy by mali byť samozrejmejšie.

6. **Plánovanie** – táto kapitola vyzdvihuje ***manažérstvo rizika na prvé miesto***. Keď organizácia takto zvýrazní ***riziká a príležitosti***, je potrebné stanoviť činnosti, ktoré sa nimi budú zaoberať. Fázy plánovania musia ukázať, ***aké, koho, ako a kedy riziká*** musia byť riešené. Tento proaktívny prístup nahrádza preventívne kroky a neskôr znižuje potrebu nápravných opatrení.

   Osobitný dôraz je tiež kladený na ***ciele systému manažérstva***, ktoré by mali byť ***merateľné, monitorované, oznamované a zladené*** s politikou systému manažérstva a v prípade potreby ***aktualizované***. Ciele musia byť stanovené pre ***dôležité funkcie a úrovne***. Časť 6. kladie väčší dôraz na ***plánovanie v určitej časti organizácie,*** ktoré je základom podnikania.

   Audítori majú byť oboznámení s rizikom – následky udalosti a pravdepodobnosť výskytu – ako modifikovať riziko. Potrebujú sa tiež zamerať na pozitívne aspekty – príležitosti pre podnikanie a jej optimalizovanie. Identifikované riziká a príležitosti umožňujú vytvoriť ciele a politiky. Mali by byť schopní identifikovať a sledovať problémy a požiadavky na riešenie rizík a príležitostí a tvorbu politík a cieľov.

7. **Podpora** – po vyriešení súvislostí, záväzku a plánovania sa bude musieť organizácia zamerať na podporu potrebnú pre dosiahnutie svojich zámerov a cieľov. Organizácia potrebuje:
   - vytvoriť ***zdroje na tvorbu tovarov a služieb,***
   - zvážiť nutnosť ***internej a externej komunikácie***, ktorá sa týka systému manažérstva – čo, kedy a s kým bude komunikovať,
   - ***zdokumentovať informácie.***

   Skôr používané pojmy, napr. *dokumenty, dokumentácia a záznamy* sa nepoužívajú. Požiadavky na ***zdokumentované informácie*** pre manažérstvo nie sú nové, výnimočné či nadmerné. Informovanosť a komunikácia audítorov by mala byť ľahšia. Audítori by mali nájsť

zodpovedajúce definície a požiadavky pre kompetencie a podporu. Potrebujú pochopiť a používať pojem zdokumentované informácie.

8. **Prevádzka** – ktorákoľvek podnikajúca organizácia potrebuje plánovať, implementovať a riadiť potrebné procesy. Toto zahŕňa ***vnútroorganizačné procesy a procesy outsourcingu***, zatiaľ čo celkový proces manažérstva zahŕňa adekvátne kritériá pre riadenie týchto procesov, rovnako ako spôsoby, ako spravovať plánované a neočakávané ***zmeny.*** Audítori musia dobre pochopiť všeobecný proces manažérstva pred jeho špecifikáciou, ktorá so sebou prinesie špecifické požiadavky.

9. **Hodnotenie výkonnosti** – organizácia musí ***určiť čo, ako a kedy má byť sledované, merané, analyzované a vyhodnotené***. Súčasťou tohto procesu je tiež interný audit a manažérske preskúmanie. ***Interné audity*** poskytujú informácie o tom, či systém manažérstva je prispôsobený požiadavkám organizácie a normám a je účinne zavedený a udržiavaný. ***Preskúmanie manažmentom*** je určené na zodpovedanie otázky: ***je systém manažérstva vhodný, primeraný a účinný?***

   Audítor by mať vychádzať z porovnania súboru požiadaviek pre kontrolu oproti plánu. Existuje množstvo **objektívnych ukazovateľov**, ktoré môžu byť identifikované a potvrdené, napr.:
   - ***zmerané hodnoty,***
   - ***plány,***
   - ***vyhodnotenia,***
   - ***nezhody a nápravné opatrenia,***
   - ***monitorovanie a výsledky merania,***
   - ***výsledky auditu a preskúmania manažmentom.***

10. **Zlepšovanie** – Občas sa vyskytujú nežiaduce veci a preto je potrebné určovať ***nezhody a nápravné opatrenia***. Tam, kde sa robia veci lepšie, tam je aj trvalé zlepšovanie. Požiadavky zlepšovania sú známe a dobre pochopené, ale nie je jasné čo je preventívna činnosť. Ako niektorí argumentovali v priebehu mnohých rokov, jedným z cieľov manažérstva je preventívna činnosť.

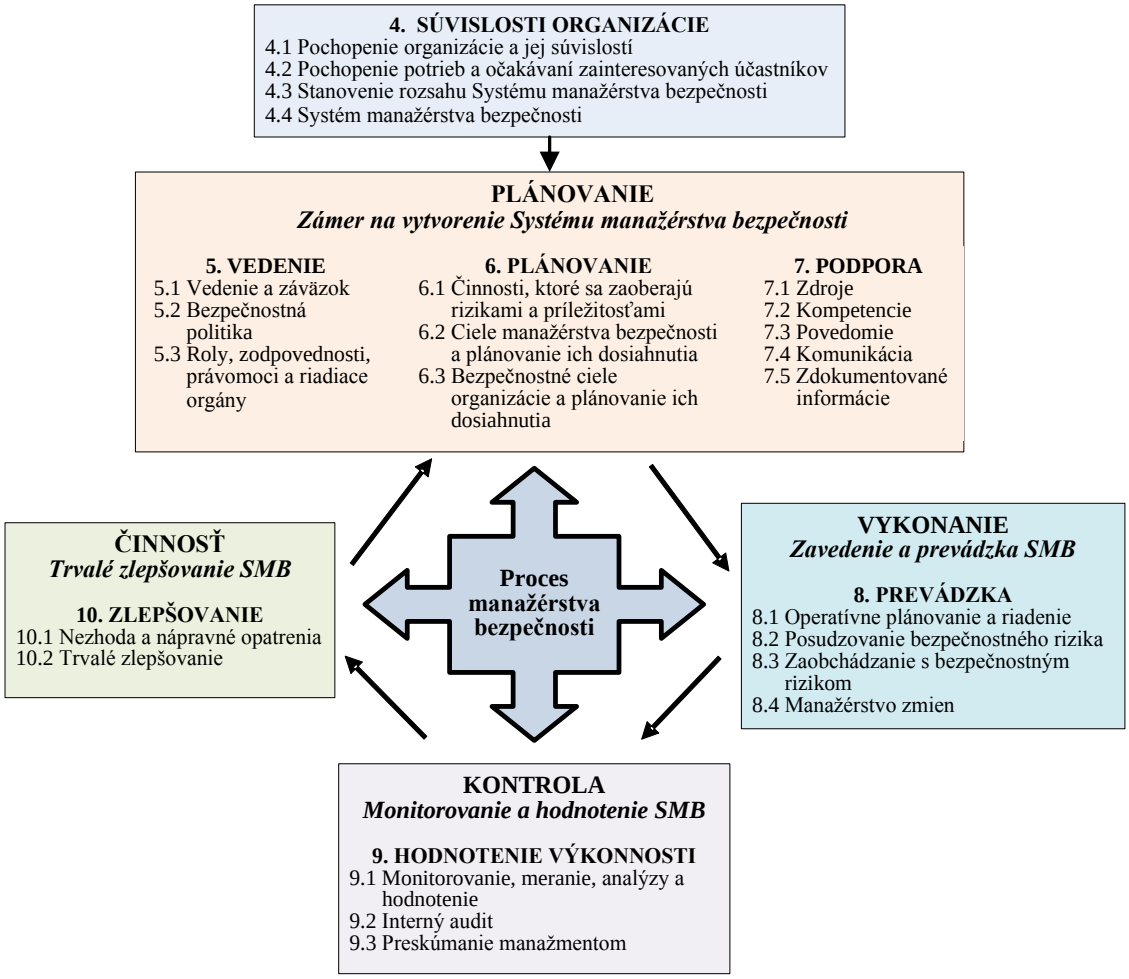
    Požiadavky v časti 4.1 „stanoviť externé a interné súvislosti organizácie, ktoré sa týkajú jej účelu a ovplyvňujú jej schopnosť dosiahnuť plánované výsledky využitím svojho systému manažérstva“ a v časti 6.1 „určiť riziká a príležitosti potrebné na uistenie, že systém manažérstva môže dosiahnuť svoje plánované výsledky, predísť alebo redukovať nežiaduce účinky, dosiahnuť trvalé zlepšovanie“ nielenže ***obsahujú preventívne činnosti ale ich presahujú.*** Audítori sa nakoniec budú pozerať späť na systém manažérstva XY založeného v časti 4.4, preskúmaného manažmentom v časti 9.3 a trvalo zlepšovaného.

Podľa uvedenej štruktúry manažérstva bude v nasledujúcej kapitole spracovaný aj **všeobecný proces manažérstva bezpečnosti organizácie.**

6.2 OBSAH PROCESU MANAŽÉRSTVA BEZPEČNOSTI

Manažérstvo bezpečnosti predstavuje sústavný, opakujúci sa súbor navzájom previazaných aktivít organizácie na plánovanie, zavedenie, prevádzkovanie, monitorovanie, hodnotenie a trvalé zlepšovanie SMB s cieľom dosiahnuť požadovanú úroveň bezpečnosti organizácie.

Na stanovenie postupnosti procesu manažérstva bezpečnosti je možné využiť všeobecnú normu, predpísanú pre systémy manažérstva, uvedenú v predchádzajúcej kapitole. Proces manažérstva bezpečnosti organizácie je potom možné názorne zobraziť s využitím PDCA cyklu (Demingov cyklus), ktorý je vhodným modelom pre všetky typy manažérskeho zlepšovania procesov, kvality výrobkov, služieb, aplikácií, dát, prebiehajúci formou opakovaného vykonávania štyroch základných činností uvedených na obr. 16.



Obr. 16 Proces manažérstva bezpečnosti organizácie

6.3 SÚVISLOSTI ORGANIZÁCIE

Základom tejto etapy je určenie, **prečo vlastne organizácia existuje**. Organizácia potrebuje identifikovať vnútorné a vonkajšie súvislosti (prostredie), ktoré môžu mať vplyv na jej zamýšľané výsledky, rovnako aj všetkých zainteresovaných účastníkov a ich požiadavky. Je potrebné tiež určiť rozsah a rozhranie systému manažérstva – všetko v súlade s podnikateľskými cieľmi. Etapa súvislosti organizácie obsahuje:

1. **Pochopenie organizácie a jej súvislostí.**
2. **Pochopenie potrieb a očakávaní zainteresovaných účastníkov.**
3. **Stanovenie rozsahu Systému manažérstva bezpečnosti.**
4. **Systém manažérstva bezpečnosti.**

Pochopenie organizácie a jej súvislostí

Základom pre pochopenie organizácie a jej súvislostí je **zistenie aktuálneho stavu bezpečnosti v organizácii**, ***kladov a nedostatkov*.** Aktuálny stav bezpečnosti v organizácii je možné zistiť vykonaním **analýzy stavu bezpečnosti organizácie**, ktorá neskúma problematiku bezpečnosti v rovnakom rozsahu, ako analýza vonkajšieho a vnútorného bezpečnostného prostredia v priebehu manažérstva rizika. Zameriava sa obvykle len na podstatné záležitosti bezpečnosti a na jej vykonanie stačí skrátený čas.

Postup pri riešení **súvislostí organizácie** sa má vykonať v súlade s bodom **4.3.1 Chápanie organizácie a jej súvislostí normy STN ISO 31000:2011 Manažérstvo rizika,** kde je uvedený obsah hodnotenia externých i vnútorných súvislostí organizácie.

Analýza stavu bezpečnosti organizácie môže potom obsahovať:

a) ujasnenie základných údajov o organizácii:
- účel, vízia, ciele, stratégia, umiestnenie, organizačná schéma, činnosti, funkcie, služby, produkty, partnerstvo, dodávateľské reťazce, vzťahy si zainteresovanými účastníkmi a potenciálny dopad spojený s rušivým incidentom,
- väzby medzi uplatňovanou politikou bezpečnosti a cieľmi organizácie a ďalšími politikami, vrátane stratégie manažérstva rizika,
- ochota organizácie prijímať riziká.

b) posúdenie a pochopenie externých súvislostí (podľa STN ISO 31000):
- sociálne, kultúrne, politické (vnímanie verejnosťou– imidž), integrotívne, verejnoprávne, finančné, technické, ekonomické, prírodné a konkurenčné faktory prostredia na medzinárodnej, národnej, oblastnej alebo miestnej úrovni,
- kľúčové motívy a trendy, ktoré ovplyvňujú ciele organizácie,
- vzťahy s externými zainteresovanými účastníkmi, ich chápanie a hodnoty.

c) posúdenie a pochopenie interných súvislostí (podľa STN ISO 31000):
- riadenie, organizačná štruktúra, úlohy a zodpovednosti,
- politika, ciele a stratégie, ktoré sa využívajú na ich dosiahnutie,
- spôsobilosť organizácie v zmysle zdrojov a znalostí (napr. kapitál, čas, ľudia, procesy, systémy a technológie),
- informačné systémy, tok informácií a procesy prijímania rozhodnutí (oficiálnych i neoficiálnych),
- vzťahy s internými zainteresovanými účastníkmi, ich vnímanie a hodnoty,
- vnímanie hodnôt a kultúry organizácie,
- normy, návody, a modely prijaté organizáciou,
- formu a rozsah zmluvných vzťahov, ale aj iné skutočnosti.

d) analýzu aktuálnej úrovne bezpečnosti v jednotlivých podsektoroch a oblastiach bezpečnostného sektora:
- zistenie stavu manažérstva bezpečnosti a manažérstva rizika, klady a nedostatky,
- posúdenie stavu ochrany osôb a majetku – plášťová a obvodová ochrana, priestorová ochrana, kontrola vstupov, predmetová ochrana, režimové opatrenia ochrany, fyzická ochrana, protipožiarna ochrana, ochrana pred účinkami priemyselných havárií a pod.,
- posúdenie stavu informačnej bezpečnosti – personálna, administratívna, fyzická a objektová, OUS, ochrana osobných údajov, ochrana bankového a iného tajomstva atď.,
- posúdenie stavu bezpečnosti infraštruktúry organizácie atď.

Metódami na zistenie (meranie) súčasného stavu bezpečnosti môžu byť napr.:

a) prieskum medzi zamestnancami - zameriava sa na parametre, ktoré určujú ***stav bezpečnostnej kultúry***, najmä ako ju vnímajú zamestnanci a poznajú jej hodnoty.

b) analýza bezpečnostnej politiky – poskytuje informácie o oficiálnych hodnotách organizácie a požadovaných štandardoch na jej vykonávanie, toto meranie by sa malo opakovať v pravidelných intervaloch.**,**

c) pohovory s manažérmi, zodpovednými za bezpečnosť a pod.

Pochopenie potrieb a očakávaní zaiteresovaných účastníkov

Pri vytváraní SMB musí organizácia určiť:
- ***zainteresovaných účastníkov***, ktorí majú vzťah k SMB,
- ***požiadavky*** týchto zainteresovaných účastníkov (ich potreby a očakávania, či už boli vyhlásené všeobecne alebo sa predpokladajú, či sú záväzné),
- postupy pre identifikáciu, zaistenie prístupu a posudzovanie príslušných ***požiadaviek zákonov a predpisov***, ku ktorým sa zaviazala, tieto použiteľné požiadavky zákonov a predpisov zohľadňovať, dokumentovať a udržiavať ich aktuálne, nové požiadavky alebo zmeny požiadaviek zákonov a predpisov oznamovať dotyčným zamestnancom a zainteresovaným účastníkom.

Pri stanovení rozsahu a hraníc SMB sa berú do úvahy:
- strategické ciele organizácie,
- hlavné produkty a služby,
- kritériá rizika,
- a všetky usmernenia, zmluvy alebo záväzky so zainteresovanými účastníkmi.

Organizácia v tomto kroku musí stanoviť **hranice a aplikovateľnosť SMB** pre ustanovenie rozsahu pôsobnosti, pričom musí zvážiť vonkajšie a vnútorné súvislosti organizácie a požiadavky zainteresovaných účastníkov.

Okrem toho organizácia musí:

a) určiť časti organizácie, ktoré majú byť zaradené do SMB,

b) určiť požiadavky SMB, ktoré zohľadňujú poslanie organizácie, jej dlhodobé zámery, vnútorné a vonkajšie záväzky a zodpovednosti vyplývajúce zo zákonov a predpisov,

c) identifikovať produkty a služby a všetky s nimi spojené činnosti v rámci SMB,

d) do úvahy vziať aj potreby a záujmy zainteresovaných účastníkov, ako sú zákazníci, investori, akcionári, dodávateľský reťazec, vstupy od verejnosti alebo spoločenstiev a ich potreby, očakávania a záujmy,

e) definovať rozsah SMB v podobe vhodnej pre veľkosť, povahu a komplexnosť organizácie.

Organizácia musí **vytvoriť, zaviesť, udržiavať a trvale zlepšovať SMB**, vrátane potrebných procesov a ich vzájomných väzieb, podľa požiadaviek noriem.

6.4 VEDENIE

Etapa vedenia obsahuje:

1. **Vedenie a záväzok.**
2. **Bezpečnostná politika.**
3. **Roly, zodpovednosti, právomoci a riadiace orgány v organizácii.**

Vedenie a záväzok

Osoby vo vrcholovom manažmente a ďalších podobných manažérskych funkciách v celej organizácii musia **demonštrovať svoju vodcovskú rolu** vo vzťahu k SMB. Táto vodcovská rola a záväzok sa môžu preukázať motiváciou a zmocnením osôb prispievať k efektívnosti SMB.

To znamená, že **vrcholový manažment musí mať zodpovednosť a byť zapojený do SMB**. Je potrebné začleniť požiadavky SMB do hlavných procesov organizácie, zabezpečiť, aby dosiahol svoje plánované výsledky a prideliť mu potrebné zdroje. Vrcholový manažment je tiež zodpovedný za dôležitosť komunikácie SMB a zvýšenie bezpečnostného povedomia a zapojenia zamestnancov.

Manažérstvo bezpečnosti nie je jednorazový projekt, ale ide o trvalú a neprerušovanú aktivitu a ako taká, si vyžaduje jasný a trvalý **záväzok**. Záväzok predstavuje povinnosť, vyplývajúcu zo záväzného sľubu, zmluvy a pod.

Aby bol záväzok trvalý, musí byť iniciovaný **mandátom** zo strany vedenia organizácie, implementovaný vyšším manažmentom a podporovaný na všetkých úrovniach organizácie. Mandát znamená ***splnomocnenie (poverenie, oprávnenie) funkcionára*** mať zodpovednosť za riadenie určitej oblasti bezpečnosti v organizácii.

Vrcholový manažment musí **demonštrovať svoju vodcovskú rolu a záväzok** vzhľadom **na SMB:**

a) zaistením:
- že sú vytvorené bezpečnostné politiky a ciele SMB a že sú v súlade so strategickým smerovaním organizácie,
- integrácie požiadaviek na SMB do podnikateľských procesov organizácie,
- zdrojov potrebných pre SMB,
- že SMB dosiahne svoje zamýšľané výstupy,
- vykonávania interných bezpečnostných auditov,

b) ustanovením rolí, zodpovedností a právomocí pre bezpečnostný manažment,

c) komunikovaním o význame a potrebe efektívneho SMB,

d) nasmerovaním a podporovaním osôb na prispievanie k efektívnosti SMB,

e) aktívnym zapojením do nácvikov a testovania,

f) podporovaním trvalého zlepšovania SMB a bezpečnosti organizácie,

g) podporovaním ďalších manažérskych rolí na preukázanie ich vodcovskej roly a záväzkov, ktoré sa vzťahujú k ich oblastiam zodpovednosti za bezpečnosť.

Bezpečnostná politika

Bezpečnostná politika (stratégia bezpečnosti) je základný a východiskový dokument, ktorým organizácia deklaruje svoj záujem na implementáciu bezpečnosti do všetkých sfér činnosti. Predstavuje súhrn najvýznamnejších rozhodnutí, zameraných na zabezpečenie prijateľnej úrovne bezpečnosti organizácie. Je to prvý dôležitý míľnik implementácie SMB, ktorý definuje hodnotu bezpečnosti v celkovej činnosti organizácie a spôsob dosiahnutia bezpečnosti v rámci organizácie.

Bezpečnostná politika hovorí o význame bezpečnosti, kto je zodpovedný za bezpečnostné funkcie a aká úroveň bezpečnosti sa má dosiahnuť. Má potvrdiť zodpovednosť organizácie za oblasť bezpečnosti a jednoznačne ukázať, že zaistenie bezpečnosti je najvyššou prioritou v poskytovaní služieb. Predstavuje deklaráciu zodpovednosti subjektu bezpečnosti (organizácie, podniku a pod.) za bezpečnosť osôb, ochranu majetku, informácií a životného prostredia. Definuje chránené záujmy subjektu a stanovuje systémové zásady, ako tieto záujmy chrániť.

Prijatie zodpovednosti a záväzku vrcholovým manažmentom za dodržiavanie a zavedenie všetkých bezpečnostných noriem v bezpečnostnej politike veľkej i malej organizácie je významným krokom, ktorý vylepší ich hodnotu a povesť, získa dôveru investorov a klientov, zvýši motiváciu a oddanosť zamestnancov a produktivitu práce a zníži náklady na úrazy, choroby a poistenie. Manažment sa týmto zaväzuje, že bude podporovať zavádzanie SMB, čo v praxi znamená, že to spoločnosť bude stáť v najlepšom prípade ľudské zdroje a financie. V prípade certifikácie SMB, bude toto prvý dokument, ktorý vyžadujú audítori. Organizácia preto musí zdokumentovanú informáciu o bezpečnostnej politike uchovávať.

Ide o vyhlásenie záväzku vrcholového manažmentu organizácie, že zabezpečí, aby všetky oblasti činností a poskytovaných služieb splnili ciele bezpečnosti v súlade so všeobecne záväznými medzinárodnými a národnými právnymi normami, vnútornými normami organizácie a jej zmluvnými záväzkami.

Bezpečnosť je v bezpečnostnej politike deklarovaná ako najvyššia priorita organizácie. Ciele bezpečnosti sa dosahujú prostredníctvom ďalšieho záväzku organizácie poskytnúť potrebné **zdroje** pre efektívne riadenie bezpečnosti. Prijatie záväzku v bezpečnostnej politike obsahuje:

a) vyhlásenie manažmentu o podpore bezpečnostnej politiky organizácie,
b) stanovenie **úloh manažmentu organizácie** pri zaisťovaní bezpečnosti a integrity,
c) zabezpečenie **zhody bezpečnostných noriem organizácie** so všeobecne záväznými právnymi predpismi, vnútornými predpismi organizácie a jej zmluvnými záväzkami,
d) vytvorenie **základného a východiskového dokumentu**, ktorým organizácia deklaruje svoj ***záujem na implementáciu bezpečnosti do všetkých sfér činnosti organizácie*** v súlade s medzinárodnými a národnými požiadavkami, ktorý musí byť podpísaný zodpovednými vedúcimi organizácie, s názvom **Bezpečnostná politika.**
e) vytvorenie **systémových bezpečnostných politík**.

Roly, zodpovednosti, právomoci a riadiace orgány v organizácii

Vrcholový manažment musí zaistiť, že v rámci organizácie sú pridelené a oznámené zodpovednosti a právomoci pre príslušné roly. Zodpovednosť a právomoc musí byť pridelená pre:

- zaistenie, že systém manažmentu zodpovedá požiadavkám bezpečnostných noriem,
- podávanie správ vrcholovému manažmentu o plnení úloh SMB v rámci organizácie.

Obsahom tohto kroku je najmä:

a) určenie zodpovedného vedúceho pracovníka alebo pracovníkov, ktorí musia, bez ohľadu na ďalšie úlohy, mať konečnú zodpovednosť za zavedenie a udržiavanie SMB,
b) vytvorenie riadiaceho orgánu bezpečnosti (výbor alebo rada bezpečnosti) za účelom vyhodnocovania výkonnosti bezpečnosti,
c) určenie zodpovednosti všetkých členov manažmentu, bez ohľadu na ďalšie úlohy a zodpovednosti, vzhľadom na výkonnosť systému manažérstva bezpečnosti v otázkach bezpečnosti,

d) zdokumentovanie zodpovednosti a právomoci za bezpečnosť a **zoznámenie** celej organizácie (musí obsahovať stanovenie úrovní manažmentu s právomocou prijímať rozhodnutia vzťahujúce sa na prijateľnosť bezpečnostného rizika),

e) menovanie kľúčových bezpečnostných pracovníkov, najmä:

- ***bezpečnostného manažéra*** ako zodpovednú samostatnú a hlavnú osobu pri zavádzaní a udržiavaní účinného systému manažérstva bezpečnosti,
- ***manažéra rizík*** a ***tím manažérstva rizika*** na čo najskoršie začatie procesu manažérstva rizík v celej organizácii,

f) vymedzenie pomeru zodpovednosti za bezpečnosť medzi manažmentom organizácie a vonkajšími spoločnosťami (bezpečnostnými službami),

g) menovaním jednej alebo viac osôb zodpovedných za SMB s primeranou právomocou a kompetenciami pre prijatie zodpovednosti za zavedenie a udržiavanie SMB (tieto osoby môžu mať i iné zodpovednosti v organizácii), obvykle sa vytvára tím pre implementáciu SMB a zabezpečuje sa jeho príprava a školenie.

6.5 PLÁNOVANIE

Táto etapa zdôrazňuje vysokú dôležitosť **manažérstva rizika**. Keď organizácia takto zvýrazní ***riziká a príležitosti***, je potrebné stanoviť, ako sa budú riešiť prostredníctvom plánovania. Fázy plánovania musia ukázať, ***aké, koho, ako a kedy riziká*** musia byť riešené. Tento prístup nahrádza preventívne kroky a neskôr znižuje potrebu nápravných opatrení.

Osobitný dôraz sa tiež kladie na ***ciele SMB***, ktoré by mali byť ***merateľné, monitorované, oznamované*** a ***zladené*** s politikou systému manažérstva a v prípade potreby ***aktualizované***.

Etapa plánovania obsahuje:

1. **Činnosti, ktoré sa zaoberajú rizikami a príležitosťami:**
   a) všeobecne,
   b) posudzovanie rizík,
   c) zaobchádzanie s rizikami.
2. **Ciele manažérstva bezpečnosti a plánovanie ich dosiahnutia.**
3. **Bezpečnostné ciele organizácie a plánovanie ich dosiahnutia.**

Činnosti, ktoré sa zaoberajú rizikami a príležitosťami

Pri plánovaní činnosti SMB musí organizácia zvážiť závery z pochopenia svojich vonkajších a vnútorných súvislostí a zainteresovaných účastníkov a určiť riziká a príležitosti, na ktoré je potrebné sa zamerať pre:

- zaistenie, že SMB môže dosiahnuť svoje zamýšľané výstupy,
- zabránenie alebo zníženie nežiaducich účinkov,
- dosiahnutie neustáleho zlepšovania.

Organizácia musí plánovať:

- činnosti, ktoré sa zaoberajú rizikami a príležitosťami (posudzovanie rizika, zaobchádzanie s rizikom),
- ako integrovať a zaviesť tieto činnosti do procesov SMB,
- ako vyhodnocovať efektívnosť týchto činností.

Posudzovanie rizika

Organizácia musí definovať a použiť **proces posudzovania rizika** ktorý:

a) stanoví a udržiava **kritériá rizika**, ktoré zahŕňajú:
   1. kritériá pre špekulatívne (podnikateľské) riziká;
   2. kritériá pre bezpečnostné riziká;

b) zaručuje, že **opakované posudzovanie bezpečnostného rizika** vytvorí zodpovedajúce, platné a porovnateľné výsledky.

c) identifikuje riziká:
   1. používa metódy a techniky posudzovania rizík na identifikáciu rizík podľa STN EN 31010:2011,
   2. identifikuje vlastníkov rizík.

d) analyzuje riziká:
   1. používa metódy a techniky posudzovania rizík na identifikáciu rizík podľa STN EN 31010:2011,
   2. posúdi potenciálne následky, ktoré by nastali v prípade realizovania identifikovaných rizík,
   3. posúdi reálnu pravdepodobnosť výskytu identifikovaných rizík,
   4. zistí úroveň každého rizika;

e) vyhodnocuje riziká:

1. porovná výsledky analýzy rizík s kritériami rizík,
2. rozhodne a vydá rozhodnutie o rizikách, ktoré vyžadujú zaobchádzanie a zoradí ich podľa dôležitosti pre zaobchádzanie.

Organizácia musí uchovávať zdokumentované informácie o procese posudzovania rizík informačnej bezpečnosti.

Zaobchádzanie s rizikom

Organizácia musí definovať a aplikovať **proces zaobchádzania s rizikami** na:

a) výber vhodného spôsobu zaobchádzania s rizikom, vzhľadom na výsledky posudzovania rizika,
b) určenie všetkých opatrení, ktoré sú nevyhnutné na zavedenie vybraného spôsobu zaobchádzania s rizikom (organizácia môže navrhnúť opatrenia podľa požiadaviek, alebo ich môže identifikovať z ľubovoľného zdroja).
c) formulovanie **Plánu zaobchádzania s rizikami**,
d) získanie súhlasu vlastníkov rizika s Plánom zaobchádzania s rizikami a prijatím zvyškových (reziduálnych) rizík.

Organizácia musí uchovávať zdokumentované informácie o procese zaobchádzania s rizikami.

Manažérstvo rizika

Posúdenie rizík a proces zaobchádzania s rizikami v tejto medzinárodnej norme je v súlade so zásadami a všeobecnými pokynmi uvedenými v ISO 31000:2011 Manažérstvo rizika, zásady a návod. **Manažérstvo rizika** predstavuje značne špecializovanú činnosť, bez ktorej sa neobíde žiadny väčší organizačný celok. Aktíva predstavujú pre organizáciu významnú hodnotu, ktorú je potrebné nielen chrániť, ale najmä rozvíjať. Na jednej strane na ne vplývajú rôzne negatívne udalosti, ktoré sa prejavujú ako bezpečnostné riziká, na druhej strane majú potenciál pre pozitívne udalosti, ktoré sa prejavujú ako podnikateľské riziká, umožňujúce získať zisk.

Proces manažérstva rizika sa musí vykonávať nepretržite, pretože z neho vyplýva návrh opatrení, ktoré by mali modifikovať zistené riziká, aby sa na jednej strane mohol dosiahnuť zisk alebo, na druhej strane, znížili možnosti strát, zabránilo zraneniam ľudí alebo stratám na životoch a škodám na majetku a životnom prostredí.

Manažéri i bezpečnostní pracovníci organizácie využívajú systematický a logický proces manažérstva rizika tak, že najprv **vyhodnotia chránené záujmy** a **určia kritériá rizika**. Chráneným záujmom je život, zdravie, majetok, infraštruktúra alebo iné hodnoty, ktoré chránime pred zničením, poškodením, odcudzením alebo inou ujmou, sú to teda **aktíva** organizácie.

V priebehu **posúdenia rizika** identifikujú, analyzujú a vyhodnotia každé riziko, a rozhodnú, či sa ním budú zaoberať, aby vyhovovalo vopred určeným kritériám. Počas tohto procesu organizácia komunikuje a konzultuje so zainteresovanými účastníkmi, monitoruje a preskúmava riziko a vyberá **spôsoby zaobchádzania** s ním, ktoré ho modifikujú, s cieľom dosiahnuť, že sa nebude vyžadovať jeho ďalšie riadenie.

Manažérstvo rizika sa má **začleniť do všetkých postupov a procesov organizácie,** nesmie sa oddeľovať. Osobitne sa má zahrnúť do politiky vývoja, podnikania, strategického plánovania a preskúmavania, ako aj do procesov manažérskych zmien. V priebehu tohto procesu majú dôležitú úlohu vrcholoví manažéri i bezpečnostní pracovníci.

Vrcholový manažment v riadiacom orgáne bezpečnosti organizácie v priebehu procesu manažérstva rizika:

a) **identifikuje všetky aktíva organizácie** (hmotné a nehmotné aktíva a významné činnosti) a určí zodpovednosť za ne,
b) **určí chránené objekty a chránené priestory** v nich a hodnoty chráneného záujmu v jednotlivých priestoroch (**aktíva**),
c) **vytvorí Politiku manažérstva rizika,**
d) **určí zodpovednosti za manažérstvo rizika**, **vytvorí štruktúry na riešenie rizík** podriadené manažérovi rizík alebo priamo bezpečnostnému manažérovi,
e) **spracuje Plán manažérstva rizika,**
f) **definuje kritériá rizík,** v porovnaní s ktorými sa bude hodnotiť každé riziko na určenie jeho prijateľnosti, prípustnosti alebo neprijateľnosti, vzhľadom na veľkosť aktív organizácie.

Bezpečnostný manažér s manažérom rizík, tímom manažérstva rizika a odborníkmi na manažérstvo rizika v ďalšom priebehu procesu manažérstva rizika:

a) **analyzuje vonkajšie a vnútorné bezpečnostné prostredie** (vonkajšie a vnútorné súvislosti),
b) **identifikuje vonkajšie a vnútorné riziká,** ktorým sú alebo môžu byť aktíva vystavené (udalosti a ich príčiny a potenciálne následky, proces hľadania, spoznávania a opísania rizika),
c) **spracuje Zoznam rizík,** v ktorom uvedie slovný popis jednotlivých rizík, ich pravdepodobnosť a následky a iné dôležité údaje o riziku,
d) **analyzuje každé riziko** uvedené v zozname rizík, **zistí jeho úroveň** podľa vzťahu pravdepodobnosti výskytu udalosti a jej následku,
e) **vyhodnotí každé riziko** porovnaním úrovne rizika zistenej v analýze rizika s kritériami rizika určenými manažmentom organizácie pri hľadaní súvislostí a zaradí riziko do príslušnej kategórie (prijateľné, prípustné znesiteľné, prípustné nežiaduce, neprijateľné),
f) **rozhodne o rizikách, ktoré vyžadujú zaobchádzanie a ich prioritách pre zaobchádzanie,**
g) **v procese zaobchádzania s rizikami, ktoré vyžadujú zaobchádzanie** rozhodne o výbere jedného alebo viacerých spôsobov zaobchádzania s rizikom a spôsobe ich zavedenia,
h) **spracuje Plán zaobchádzania s rizikami,**
i) **v priebehu monitorovania a preskúmavania** vykonáva pravidelné kontroly a merania efektívnosti a účinnosti zmiernenia dopadov rizík po ich modifikovaní (zvyškových rizík) a vyhľadáva novo vzniknuté riziká,
j) **spracuje Záznam procesu manažérstva rizika** o celej činnosti v procese manažérstva rizika.

Ciele manažérstva bezpečnosti a plánovanie ich dosiahnutia

Vrcholový manažment musí zaistiť, aby ciele manažérstva bezpečnosti boli prijaté a oznamované podľa príslušnej úrovne a funkcie v rámci organizácie. **Ciele manažérstva bezpečnosti musia:**

- byť zladené s bezpečnostnou politikou,
- zohľadniť minimálnu úroveň produktov a služieb, ktorá je prijateľná pre organizáciu, aby dosiahla svoje ciele,
- byť merateľné,
- zohľadniť použiteľné požiadavky,
- byť monitorované a aktualizované, pokiaľ je to vhodné.

Organizácia musí udržiavať **zdokumentované informácie o cieľoch manažérstva bezpečnosti.** Na dosiahnutie týchto cieľov musí organizácia určiť:

- kto bude zodpovedný,
- čo sa má vykonať,
- aké zdroje budú požadované,
- kedy to musí byť dokončené,
- ako budú vyhodnocované výsledky.

Bezpečnostné ciele organizácie a plánovanie ich dosiahnutia

Dôležitým predpokladom pre aktívnu implementáciu SMB je **plánovanie bezpečnosti.** V jeho priebehu sa formulujú ***ciele*** pre bezpečný výkon organizácie, určujú ***stratégie (postupy na ich dosiahnutie)*** a spracovávajú konkrétne ***plány*** na dosiahnutie prijateľnej úrovne bezpečnosti.

Podkladmi pre stanovenie bezpečnostných cieľov sú:

- ***analýza stavu bezpečnosti organizácie***,
- výsledky ***manažérstva rizika***,
- ***možnosti*** každej organizácie a ***predstavy o fungujúcom systéme manažérstva bezpečnosti*** v organizácii.
- ***zákonné bezpečnostné normy***.

Stanovenie bezpečnostných cieľov je **vecou vrcholového manažmentu** každej organizácie. Organizácia stanovuje **bezpečnostné ciele** konkrétne pre svoje potreby, no vychádza zo všeobecného rámca, podľa ktorého možno definovať niektoré ciele, napr.:

- definovať infraštruktúru a najdôležitejšie aktíva organizácie, ktoré je potrebné chrániť,
- identifikovať, analyzovať a vyhodnotiť bezpečnostné riziká a modifikovať neprijateľné a prípustné riziká na požadovanú úroveň,
- vytvoriť bezpečnostné prostredie na ochranu zdravia a života príslušníkov manažmentu, všetkých ďalších zamestnancov a všetkých zainteresovaných účastníkov,
- vytvoriť SMB organizácie s vymedzením zodpovednosti pre riadiacu zložku, výkonnú zložku a kontrolnú zložku,
- vybudovať vonkajšiu ochranu objektov ako komplex opatrení na vymedzenie hraníc objektov, kontrolu vstupov do objektu a výstupov z objektu,
- zabezpečiť monitorovanie možného narušenia stanovených hraníc objektov organizácie,
- zaviesť potrebné mechanické zábranné prostriedky a technické zabezpečovacie prostriedky na ochranu a monitorovanie hraníc objektu, vstupov do objektu a ochranu chránených priestorov,
- vytvoriť vnútornú ochranu dôležitých objektov s dôrazom na ochranu chránených priestorov,
- zaviesť komplexné režimové opatrenia na vonkajšiu a vnútornú ochranu organizácie,
- vypracovať komplexnú, havarijnú a iné bezpečnostné dokumenty organizácie,
- vytvoriť podmienky pre ochranu utajovaných skutočností, citlivých informácií, ochranu osobných údajov a vytvoriť systém manažérstva informačnej bezpečnosti,
- zabezpečiť ochranu obchodného, výrobného a iných tajomstiev,
- vytvoriť systémy manažérstva BOZP ,ochrany životného prostredia organizácie (EMS) a kontinuity činností,
- vytvoriť systém vyšetrovania incidentov a podvodov,
- zabezpečiť monitorovanie, kontroly, audit a vyhodnocovanie výkonnosti SMB a úrovne bezpečnosti organizácie.

Bezpečnostné ciele je vhodné ***vymedziť vo vertikálnej a horizontálnej úrovni, určiť konkrétnu zodpovednosť, v ich funkčnej, obsahovej, ekonomickej rovine a hlavne v právnej a finančnej rovine.***

V priebehu stanovenia bezpečnostných cieľov organizácie a plánovania ich dosiahnutia sa najmä:

1. **stanovujú konkrétne bezpečnostné ciele** organizácie, ***spôsoby a kritériá ich vyhodnocovania*** a ***spôsoby kontroly ich dosahovania***,
2. **určujú bezpečnostné normy** v jednotlivých sektoroch a oblastiach bezpečnosti,
3. **plánuje implementácia SMB** do procesov organizácie – ***Plán implementácie SMB,***
4. **plánujú postupy na dosiahnutie bezpečnostných cieľov v podsektoroch bezpečnostného sektora** v jednotlivých plánoch, napr.:
   - **BOZP** – ***Plán bezpečnosti a ochrany zdravia pri práci na stavenisku***.
   - **ochrana objektov** s využitím už spracovaného Plánu zaobchádzania s rizikami – ***Bezpečnostný plán ochrany objektu*** (OUS), ***Bezpečnostný plán*** (kritická infraštruktúra), pre iné objekty ***Bezpečnostný plán ochrany objektu*** alebo ***Projekt ochrany objektu,***
   - **informačná bezpečnosť,**
   - **ochrana osobných údajov** – ***Bezpečnostný projekt (smernica) na ochranu osobných údajov v informačnom systéme,***
5. **koordinuje plánovanie reakcie na núdzové situácie,**
6. **plánujú postupy na riešenie incidentov** – ***Plán manažérstva incidentov,***
7. **stanovuje program environmentálneho manažérstva** – ***Akčný plán (programy) environmentálneho manažérstva.***

Určenie bezpečnostných noriem

Normy bezpečnosti musia dodržať súlad s platnými požiadavkami bezpečnostných predpisov a zabezpečiť snahu organizácie prijať medzinárodne uznávané bezpečnostné normy a osvedčené postupy v oblasti manažérstva bezpečnosti. Organizácia v prvom rade musí **dodržiavať normy stanovené v zákonoch a smerniciach,** ktoré môže doplniť svojimi štandardmi.

Je potrebné:

a) určiť, aké **bezpečnostné právne normy** zaviesť v organizácii,
b) definovať **prijateľnú úroveň bezpečnosti** (minimálny stupeň/úroveň bezpečnosti, ktorú musí SMB dosiahnuť v praxi,
c) stanoviť **výkonnostné ciele bezpečnosti a ich hodnoty –** kvantifikované ciele, ktoré zabezpečia požadovanú úroveň bezpečnosti organizácie,
d) nastaviť **ukazovatele výkonnosti v oblasti bezpečnosti (indikátory bezpečnosti**) a ich **hodnoty** – parametre na určenie, či sa dosiahla požadovaná úroveň bezpečnosti, napr.: rast, frekvencia, počet nehôd; rast, frekvencia, počet incidentov; úroveň zhody s právnymi normami atď.,
e) dodržiavať existujúce, nové a zmenené technické a prevádzkové normy alebo iné podmienky určené v technických špecifikáciách interoperability, národných bezpečnostných predpisoch, iných predpisoch a v rozhodnutiach bezpečnostného orgánu.

Plánovanie implementácie SMB

Plán implementácie SMB organizácie má zaistiť konzistentný, cielený a komplexný prístup k rozvoju potrebnej organizačné štruktúry SMB, procesov a postupov manažérstva bezpečnosti. Plán implementácie SMB organizácie:

- **stanovuje prístup organizácie** k riadeniu bezpečnosti spôsobom, ktorý zodpovedá cieľom bezpečnosti pre organizáciu,

- **identifikuje náklady** na školenie a plánovanie, navrhne rozpočet pre realizáciu SMB,
- **vytvorí a udržiava dokumenty SMB**, ktorá popisuje politiku a ciele bezpečnosti, požiadavky na SMB, procesy a postupy SMB, zodpovednosti a právomoci pri procesoch a postupoch a výstupy SMB,
- **schvaľuje vrcholový manažment organizácie.**

Ako súčasť dokumentácie SMB sa obvykle vytvorí a udržiava **Príručka systémov manažérstva bezpečnosti** *(Safety Management Systems Manual)* schválená právne zodpovedným manažérom, aby bola celá organizácia zoznámená s prístupom k manažérstvu bezpečnosti.

Plánovanie BOZP

Podľa § 18 ods. 4 Zákona o bezpečnosti a ochrane zdravia pri práci a Nariadení vlády SR č. 396/2006 Z. z. o minimálnych bezpečnostných a zdravotných požiadavkách na stavenisko sa spracováva **Plán bezpečnosti a ochrany zdravia pri práci na stavenisku**, ktorý:

- ustanoví pravidlá na vykonávanie prác na stavenisku,
- obsahuje aj osobitné opatrenia pre jednotlivé práce s osobitným nebezpečenstvom, uvedené v prílohe 2 nariadenia,
- a využíva sa ako podklad, ktorý obsahuje príslušné informácie o bezpečnosti a ochrane zdravia pri práci, ktoré je potrebné zohľadňovať pri všetkých ďalších prácach.

Koordinácia plánovania reakcie na núdzové situácie

Koordinácia plánovania odozvy na núdzové situácie znamená vhodnú koordináciu plánov, ktoré riešia reakciu organizácie na núdzové situácie, s plánmi tých organizácií, s ktorými musí byť v spojení počas poskytovania svojich služieb:

a) v rámci **prevencie závažným priemyselným haváriám** je prevádzkovateľ podľa Zákona č. 261/2002 Z. z. o prevencii závažných priemyselných havárií a Vyhlášky ministerstva životného prostredia SR č. 490/2002 Z. z. o bezpečnostnej správe a o havarijnom pláne povinný vypracovať: ***Bezpečnostnú správu*** (prevádzkovateľ organizácie kategórie B), ***Havarijný plán*** a spolupracovať na vypracúvaní ***Plánu ochrany obyvateľstva*** podľa zákona NR SR č.42/1994 Z. z. o civilnej ochrane obyvateľstva.

b) v **systéme manažérstva kontinuity činností** sa spracováva ***Plán kontinuity činností*** (*Business Continuity Plan*), okrem toho sa používajú aj ***Plán obnovy činností*** (*Business Recovery Plan)* alebo ***Plán obnovy po havárii*** (*Disaster Recovery Plan).*

c) podľa Zákona č. 541/2004 Z. z.**o mierovom využívaní jadrovej energie (atómový zákon)** sa spracovávajú: ***Predbežný vnútorný havarijný plán, Vnútorný havarijný plán, Plán ochrany obyvateľstva, Havarijný dopravný poriadok.***

d) podľa Zákona č. 364/2004 Z. z. **o vodách** v znení neskorších predpisov ***Havarijný plán*** predstavuje plán preventívnych opatrení na zamedzenie vzniku neovládateľného úniku škodlivých látok a obzvlášť škodlivých látok do životného prostredia a na postup v prípade ich úniku.

e) podľa Zákona č. 24/2006 Z. z. o **posudzovaní vplyvov na životné prostredie** v znení neskorších predpisov sa spracováva ***Havarijný plán,*** ktorý tvorí súčasť prevádzkového poriadku skládky odpadov.

Pri vypracúvaní havarijného plánu sa vychádza z konkrétnej situácie v organizácii a jej okolí s osobitným zreteľom na výsledky manažérstva rizika.

Plánovanie manažérstva incidentov

Manažérstvo bezpečnostných incidentov sa týka detekcie a reakcie na bezpečnostné incidenty a s nimi súvisiace plány komunikácie na ohlasovanie a informovanie, vrátane urče-

nia úloh a zodpovednosti. Monitorovanie a kontrolné postupy majú byť schopné odhaliť nielen zrealizované narušenia, ale aj pokusy o narušenie bezpečnosti.

Na riešenie incidentov sa spracováva ***Plán manažérstva incidentov*** *(Incident Management Plan)*. Postupy reakcie na jednotlivé druhy bezpečnostných incidentov majú obsahovať analýzu bezpečnostných incidentov, stratégiu reakcie v technickej, riadiacej a právnej oblasti, opatrenia a činnosti na obnovu alebo náhradu postihnutých aktív organizácie.

Od všetkých zamestnancov organizácie aj tretích osôb sa má vyžadovať, aby si všímali a hlásili informácie a okolnosti o možnom ohrození bezpečnosti a zraniteľnosti sietí a služieb. Možný postup organizácie:

- stanovenie štandardov a postupov manažmentu bezpečnostných incidentov pri zisťovaní bezpečnostných incidentov a reakcií na vzniknuté incidenty, ako aj zabezpečenie prevencie pred vznikom alebo opakovaním bezpečnostných incidentov,
- určenie vedúceho tímu pre riešenie incidentov a spôsobu doplňovania tímu odborníkmi a zodpovednými pracovníkmi v prípade incidentu,
- určenie metodiky hlásenia incidentu, spôsobu zaznamenávania a riešenia,
- stanovenie dokumentácie pre riešenie incidentov.

6.6 PODPORA

Po vyriešení súvislostí, záväzku a plánovania bezpečnosti sa bude musieť organizácia zamerať na podporu, potrebnú pre dosiahnutie svojich zámerov a cieľov. Toto zahŕňa zdroje, zameranie internej a externej komunikácie, ako aj zdokumentované informácie, čím sa nahrádzajú skôr používané pojmy ako dokumenty, dokumentácia a záznamy. Etapa podpory obsahuje:

1. **Zdroje –** organizácia musí určiť a poskytnúť zdroje potrebné pre vytvorenie, zavedenie, udržiavanie a trvalé zlepšovanie SMB a zaistenie bezpečnosti vo všetkých oblastiach činnosti.

2. **Kompetencie –** organizácia musí:
   - stanoviť konkrétne kompetencie osôb vykonávajúcich bezpečnostné činnosti, ktoré majú vplyv na výkonnosť bezpečnosti,
   - zaistiť, aby tieto osoby boli kompetentné na základe vhodného vzdelania, výcviku a skúseností,
   - tam, kde je to vhodné prijať opatrenia na získanie potrebnej kompetencie a vyhodnotiť účinnosť prijatých opatrení,
   - udržiavať vhodnú zdokumentovanú informáciu ako dôkaz o kompetencii (prístup k nim znamená možnosť povolenia nazerať do nich alebo právomoc meniť ich).

3. **Povedomie –** osoby, ktoré vykonávajú práce v rámci organizácie si musia uvedomiť:
   - bezpečnostnú politiku,
   - svoj príspevok k bezpečnosti a účinnosti SMB, vrátane výhod zlepšenia výkonnosti SMB,
   - následky neplnenia požiadaviek SMB,
   - svoje vlastné úlohy pri incidentoch

4. **Komunikácia –** organizácia musí určiť potrebu ***vnútornej a vonkajšej komunikácie***, ktorá sa vzťahuje na SMB a obsahuje:
   - o čom sa bude komunikovať,
   - kedy sa bude komunikovať
   - s kým sa bude komunikovať.

   Organizácia musí ustanoviť, zaviesť a udržiavať **postupy:**
   - vnútornej komunikácie medzi zainteresovanými účastníkmi a zamestnancami organizácie,
   - vonkajšej komunikácie so zákazníkmi, partnerskými entitami, miestnymi komunitami a ďalšími zainteresovanými účastníkmi, vrátane médií,
   - na prijímanie, dokumentovanie a reagovanie na komunikáciu zainteresovaných účastníkov,
   - na prevzatie a integrovanie národného alebo regionálneho systému informovania o hrozbách alebo obdobného systému do plánovania a používania, pokiaľ je to vhodné,
   - na zaistenie dostupnosti prostriedkov komunikácie počas rušivého incidentu,
   - na uľahčenie štruktúrovanej komunikácie s príslušnými orgánmi a zaistenie vzájomnej spolupráce niekoľkých reagujúcich organizácií alebo pracovníkov, kde je to vhodné,
   - prevádzku a testovanie komunikačných prostriedkov určených na použitie pri narušení normálnych komunikácií.

5. **Zdokumentované informácie –** rozsah zdokumentovaných informácií pre SMB sa môže v rôznych organizáciách líšiť, podľa veľkosti organizácie a druhu jej činností, procesov,

produktov a služieb, komplexnosti procesov a ich vzájomných väzieb a kompetencie osôb. Informácie SMB organizácie musia obsahovať:

- zdokumentované informácie požadované v bezpečnostných normách,
- zdokumentované dokumentácie, ktoré organizácia určí ako nevyhnutné pre efektívnosť SMB.

Rozsah zdokumentovaných informácií

Pri stanovení rozsahu zdokumentovaných bezpečnostných informácií (bezpečnostnej dokumentácie) musí organizácia vychádzať z platných zákonov a ďalších právnych noriem, v ktorých sú tieto dokumenty stanovené. Bezpečnostné dokumenty predstavujú okrem uvedených plánovacích dokumentov ďalšie dokumenty SMB, manažérstva rizika a jednotlivé bezpečnostné smernice, metodiky a nariadenia vo všetkých podsektoroch a oblastiach bezpečnostného sektora.

Vytváranie a aktualizovanie zdokumentovaných informácií

V tejto etape sa určujú **spracovatelia a termíny na spracovanie potrebných dokumentov**. Pri vytváraní a aktualizovaní zdokumentovaných informácií musí organizácia zaistiť:

- vhodnú identifikáciu a popis (napr. názov, dátum, autora alebo číslo odkazu),
- vhodný formát (napr. jazyk, verziu softvéru, grafiku) a média (napr. papierová alebo elektronická), preskúmanie a schválenie z hľadiska vhodnosti a primeranosti

Riadenie (správa) zdokumentovaných informácií

Zdokumentované informácie požadované v SMB a v medzinárodných bezpečnostných normách musia byť spravované pre zaistenie:

- ich dostupnosti a vhodnosti pre požitie tam, kde je to potrebné,
- primeranej ochrany (napr. proti strate dôvernosti, nevhodnému použitiu alebo strate integrity).

Na uloženie zdokumentovaných informácií sa musí vytvoriť **samostatné pracovisko.** Pri ich spravovaní musí organizácia, pokiaľ je to akceptovateľné, zohľadniť nasledujúce činnosti:

- rozosielanie, prístup, vyhľadávanie a použitie,
- skladovanie a ochranu vrátane ochrany čitateľnosti,
- riadenie zmien (napr. riadenie verzií),
- uschovávanie a zaobchádzanie,
- vyhľadávanie a použitie,
- ochranu čitateľnosti (či je zdokumentovaná informácia dostatočne rozpoznateľná, aby sa dala prečítať),
- ochranu nezamýšľaného použitia zastaraných informácií.

Zdokumentované **informácie externého pôvodu**, ktoré organizácia určila ako nevyhnutné pre plánovanie a prevádzku SMB, musia byť podľa potreby identifikované a spravované.

Prístupom sa rozumie rozhodnutie týkajúce sa povolenia na zobrazenie iba zdokumentovanej informácie, alebo povolenie a oprávnenie zobraziť a zmeniť zdokumentované informácie a pod.

6.7 PREVÁDZKA

Etapa prevádzka obsahuje:

1. **Operatívne plánovanie a riadenie.**
   a) **Organizovanie bezpečnosti.**
   b) **Personálne zaistenie bezpečnosti.**
   c) **Prevádzka SMB.**
2. **Posudzovanie bezpečnostných rizík.**
3. **Zaobchádzanie s bezpečnostným rizikom.**
4. **Manažérstvo zmien.**

1. Operatívne plánovanie a riadenie

Operatívne plánovanie manažérstva bezpečnosti je základným nástrojom riadenia, ktorý vychádza z konkrétnych a detailných požiadaviek na bezpečnosť. Úlohou operatívneho plánovania bezpečnosti je za organizáciu ako celok, ako aj za všetky jej funkcionálne oblasti v kratšom časovom horizonte ***realizovať' ciele a strategické zámery podnikateľskej a bezpečnostnej stratégie*** prijaté v rámci strategického plánovania.

Zatiaľ čo **plánovanie** stanoví ciele a prostriedky manažérstva bezpečnosti a ich vzťahy na dlhšie obdobie a v globále, **operatívne plánovanie** ich určuje podrobne a na krátke obdobie dopredu. Jasne a konkrétne vytyčuje úlohy príslušného obdobia ***podľa druhu bezpečnosti*** a stanovuje začiatok aj koniec ich vykonávania. V operatívnom plánovaní sa premieňajú všetky ciele a plány, ktoré sú dlhodobo stanové v strategickej koncepcii na konkrétne oblasti bezpečnosti. Od systému operatívneho plánovania sa vyžaduje predovšetkým jeho integrita. Systém operatívneho plánovania bezpečnosti sa skladá z viacerých čiastkových plánov pre jednotlivé druhy bezpečnosti.

Každodenné **operatívne riadenie** je nevyhnutnou súčasťou riadenia SMB. Zvládnutie veľkého množstva úloh na udržanie bezpečnosti, prichádzajúcich z rôznych podsektorov bezpečnostného sektora v organizácii, musí byť spoľahlivo zabezpečené. Efektívna tvorba hlásení pre potreby ďalšieho rozhodovania a taktiež meranie výkonnosti bezpečnostných procesov, od ktorých výkonnosti závisí chod organizácie, priamo ovplyvňuje úroveň, spoľahlivosť a účinnosť SMB.

1.a Organizovanie bezpečnosti

Organizovanie bezpečnosti predstavuje manažérske funkcie ***organizovanie a personálne zaistenie***. **Riadenie bezpečnosti** predstavuje manažérsku funkciu ***vedenia ľudí.*** Potvrdzuje sa záväzok pre jednoznačný a aktívny prístup k bezpečnosti prostredníctvom využitia SMB. Zahŕňa organizačné aspekty tvorby SMB a vyžaduje, aby v rámci organizácie boli ustanovené funkcie pre manažérstvo bezpečnosti a s tým súvisiace úlohy a zodpovednosti. Ide o implementáciu SMB a jeho nerušenú prevádzku.

Organizovanie bezpečnosti predstavuje najmä:

a) **inventarizáciu významných aktív a posúdenie ich aktuálnej bezpečnosti,**
b) **uskutočnenie procesu manažérstva rizika** a implementáciu opatrení na modifikáciu rizík, ktoré majú úroveň vyššiu ako prijateľné riziko,
c) **vytvorenie organizačnej štruktúry a implementácia SMB,**
d) **personálne** naplnenie organizačnej štruktúry SMB a príprava bezpečnostných pracovníkov,
e) **delegovanie právomocí a zodpovedností** jednotlivcom a jednotlivým skupinám **za bezpečnosť** a určenie **vzájomných vzťahov medzi nimi,**

f) vyčlenenie zdrojov na činnosť SMB a dosiahnutie bezpečnostných cieľov,
g) zavedenie preventívnych opatrení, napr. prevencia kriminality, predchádzanie incidentom, prevencia porúch, zdravotná prevencia a pod.,
h) zavedenie systémov ochrany, napr. Systém ochrany objektu, Systém požiarnej ochrany, ochrana osobných údajov, OUS atď.,
i) zavedenie systémov manažérstva bezpečnosti pre BOZP, informačnú bezpečnosť, kontinuitu činností, environment, bezpečnostné incidenty a pod.,
j) dosiahnutie pripravenosti na núdzový stav a reakciu,
k) zavedenie bezpečnostnej dokumentácie – vytvorenie potrebných riadiacich a organizačných dokumentov, napr. prevádzkových smerníc, režimových opatrení, smerníc pre strážením, smerníc pre prevádzku technických systémov, smerníc pre zásah, smerníc pre riešenie konfliktných a krízových situácií a pod., s vymedzením úloh, zodpovedností, kompetencií a zásad pre vonkajšiu a vnútornú súčinnosť,
l) organizovanie operatívneho a technického monitoringu vytvoreného SMB,
m) organizovanie logistickej podpory činnosti SMB,
n) operatívne riadenie SMB a manažérstvo zmien. .

Dosiahnutie pripravenosti na núdzový stav a reakciu obsahuje najmä:

a) vymenovanie **koordinátora pre núdzové plánovanie,**
b) zavedenie **havarijných plánov a nácviky** činnosti podľa nich, ak je to vhodné, aj v spolupráci s tretími stranami,
c) vytvorenie **záchrannej služby, havarijného tímu, tímu obnovy**,
d) pravidelné **preskúšavanie prostriedkov výstrahy a varovania**,
e) udržiavanie prostriedkov na zdolávanie havárií, rezervných ochranných prostriedkov, a prostriedkov na evakuáciu **v pohotovostnom stave,**
f) vytvorenie a implementovanie **plánu zastupiteľnosti** pre každú kľúčovú pozíciu,
g) **zabezpečenie, aby zamestnanec, ktorý zastupuje iného pracovníka mal:**
   - **informácie o jeho činnosti** (pracuje na rovnakej pozícií a/alebo všetci zamestnanci na kľúčových pozíciách vypracovávajú podrobné dokumenty, ktoré ukladajú na určených miestach),
   - **adekvátne znalosti a schopnosti** (zabezpečiť napríklad prostredníctvom pravidelných školení zo strany potenciálne zastupovaného pracovníka),
   - v prípade potreby **prístup k dôležitým systémom** s adekvátnymi prístupovými oprávneniami (heslá a prihlasovacie údaje, kópie certifikátov by mali byť uložené na bezpečnom mieste, napr. v trezore),
h) v pracovnej zmluve alebo náplni pracovnej činnosti každého zamestnanca na kľúčovej pozícií zaviazať **viesť dostatočne podrobné zdokumentované informácie** (miera podrobnosti závisí od znalostí osôb, ktoré by v prípade nutnosti zastupovali tohto pracovníka a konkrétnej role zamestnanca vo firme).

Manažérstvo bezpečnostných incidentov

V rámci prevádzkovania SMB a vedenia ľudí je potrebné venovať príslušnú pozornosť **manažérstvu incidentov,** ktoré sa v organizácii vyskytnú, napr. nežiaduce udalosti, podvody, incidenty, nehody a pod. Pri ich riešení je treba postupovať podľa vypracovaných postupov v **Pláne manažérstva incidentov.**

1.b Personálne zaistenie bezpečnosti

Pre personálne zistenie bezpečnosti sa v organizácii vykonáva:

a) **analýza potrieb ľudských zdrojov** v nadväznosti na špecifikáciu pracovných činností (pozícií) v systéme manažérstva bezpečnosti,
b) **vytvorenie štruktúry pracovných miest bezpečnostných pracovníkov** v organizačnej štruktúre,
c) **popis pracovných miest bezpečnostných pracovníkov** v organizačnej štruktúre,
d) **nábor uchádzačov** na potrebné (voľné) pracovné pozície bezpečnostných pracovníkov,
e) **výber a rozmiestňovanie** vhodných pracovníkov z registrovaných uchádzačov na základe personálnej previerky a špecifických kritérií a požiadaviek,
f) **adaptácia bezpečnostných pracovníkov** v novom prostredí,
g) **dosiahnutie a zvyšovanie odbornej spôsobilosti bezpečnostných pracovníkov**,
h) **rozvoj všetkých zamestnancov** pre vytváranie povedomia bezpečnosti v organizácii, so zameraním na vnútroorganizačné **bezpečnostné vzdelávanie a výcvik** (bezpečnosť práce a ochrana zdravia pri práci, požiarna bezpečnosť, ochrana utajovaných skutočností, riešenie incidentov atď.).

Prijímanie zuchádzačov na funkcie bezpečnostných pracovníkov

Ide o etapu personalistiky, v ktorej sa majú vybrať kvalifikovaní pracovníci pre výkon bezpečnostných funkcií na základe kvalifikačných požiadaviek a iných stanovených kritérií. Táto etapa obsahuje:

- ***výber uchádzačov*** o pracovné miesta bezpečnostných pracovníkov,
- ***personálne previerky uchádzačov,***
- ***poučenie*** prijatého zamestnanca o rozsahu jeho oprávnenia, poučenie potvrdiť protokolom s podpisom, kto poučenie vykonal, obsah tohto poučenia a podpis poučeného,
- ***pri odchode zo zamestnania*** odobratie všetkých prístupových oprávnení azmena všetkých hesiel ku všetkým účtom, ku ktorým mal zamestnanec prístup.
- v prípade odchodu zodpovedného pracovníka (najmä v prípade ak bol nedobrovoľný) ***skontrolovať*** všetky dokumenty a systémy IT vzhľadom na prítomnosť neoprávneného software, vytvorenia zadných vrátok a pod.

Školenie a výcvik personálu, dosiahnutie spôsobilosti

V tomto úseku činnosti personalistiky sa vykonáva:

- tvorba ***programov výcviku a školení*** pre školiace štruktúry a všetkých zamestnancov,
- úvodné, pokračujúce a osobitné ***školenia bezpečnostných pracovníkov*** na získanie kvalifikácie pre vykonávanie povinností spojených so SMB,
- ***školenia a výcvik všetkých zamestnancov*** v otázkach bezpečnosti, oboznámenie s bezpečnostnou politikou, zásadami bezpečného použitia mechanických a technických prostriedkov ochrany a režimovými opatreniami,
- spracovanie ***záznamov*** o vykonaných školeniach so zoznamom školených osôb,
- ***dosiahnutie odbornej spôsobilosti*** bezpečnostných pracovníkov,
- ***kontroly odbornej spôsobilosti*** bezpečnostných pracovníkov a zamestnancov, preskúšanie znalostí a praktických zručností,
- ***budovanie povedomia bezpečnosti***, vytváranie ***bezpečnostnej kultúry.***

1.c Prevádzka SMB

Do prevádzky SMB je možné zaradiť najmä:

- **implementáciu organizačnej štruktúry SMB,**
- **prevádzkovanie SMB**

- **vedenie zamestnancov pre dodržiavanie noriem bezpečnosti**,
- **horizontálnu a vertikálnu koordináciu bezpečnostných činností** – dosiahnuť koordinované a zladené úsilie manažmentu, bezpečnostných pracovníkov a zamestnancov v jednotlivých oblastiach bezpečnosti napr. BOZP, bezpečnosť prevádzky a predchádzanie závažným priemyselným haváriám, bezpečnosť životného prostredia, informačná bezpečnosť, bezpečnosť objektov a chránených priestorov, požiarna bezpečnosť a pod.
- **zavedenie operatívneho a technického monitoringu SMB,**
- **zabezpečenie logistickej podpory činnosti SMB**.
- **monitorovanie a preskúmavanie zvyškových a nových rizík** – prípadné prehodnotenie kritérií rizika a opakované procesy manažérstva rizika, ukončené spracovaním Plánu zaobchádzania s rizikami.

Vytvorenie organizačnej štruktúry SMB

V etape organizovania sa na základe Plánu implementácie SMB vytvára a naplňuje jeho organizačná štruktúra, určujú povinnosti a zodpovednosti a vyčleňujú zdroje na činnosť SMB. Táto etapa obsahuje najmä:

- **vytvorenie a naplnenie organizačnej štruktúry** SMB organizácie,
- konkrétne pridelenie **povinností a zodpovedností bezpečnostným pracovníkom**, kto má komu podávať hlásenia, kto je za čo zodpovedný a pod.,
- vytvorenie štruktúry na riešenie krízového riadenia – vymenovanie **koordinátora pre núdzové plánovanie, vytvorenie havarijného tímu,**
- zavedenie štruktúry **manažérstva bezpečnostných incidentov** a postupu ohlasovania bezpečnostných incidentov zamestnancami,
- zavedenie procesu dobrovoľného ohlasovania **bezpečnostných rizík,**
- zavedenie postupu na posúdenie nového vybavenia a zariadení, ktoré súvisia s bezpečnosťou v organizácii, z hľadiska nebezpečenstva/ rizík predtým, ako sú zavedené do prevádzky a postupu na prehodnotenie existujúcich relevantných činností a procesov, ak sa kedykoľvek vyskytnú zmeny týkajúce sa tohto vybavenia alebo zariadení.

Operatívne riadenie (prevádzkovanie) SMB

V priebehu operatívneho riadenia SMB a vedenia ľudí je potrebné:

a) **motivovať bezpečnostných pracovníkov** a vytvárať **systém ich kariér**, zabezpečiť starostlivosť o ich osobnostný a profesijný rast,
b) **hodnotiť bezpečnostných pracovníkov** podľa výsledkov práce a správania (*hodnotenie práce),*
c) **operatívne riadiť činnosť SMB a zamestnancov** pri **dodržiavaní noriem bezpečnosti, odmeňovať** podľa výkonnosti a prínosu pre organizáciu,
d) **monitorovať a preskúmavať zvyškové a nové riziká**, nepretržite prehodnocovať kritériá rizika.
e) **udržiavať komunikáciu bezpečnostných pracovníkov so zamestnancami** o **problematike bezpečnosti:**
   - vytvárať a stimulovať komunikatívne prostredie a priestor pre rozumnú aktivitu a iniciatívu zamestnancov v otázkach bezpečnosti,
   - zoznamovať zamestnancov s bezpečnostnými cieľmi (úlohami) a bezpečnostnou politikou a ich objasňovanie,
   - prideľovať úlohy na dosahovanie bezpečnosti zamestnancom,
   - pripravovať a viesť zamestnancov pre dodržiavanie bezpečnostných noriem, smerníc a stanovených bezpečnostných postupov,
f) **udržiavať vonkajšiu komunikáciu so zainteresovanými účastníkmi,**

g) **motivovať** všetkých zamestnancov na vytváranie **povedomia bezpečnosti a bezpečnostnej kultúry,**
h) **realizovať manažérstvo bezpečnostných incidentov –** zvládanie problémov, eliminácia možnosti výskytu vnútorných páchateľov a pod.

Posudzovanie bezpečnostných rizík

Organizácia musí posudzovať bezpečnostné riziká v pravidelných intervaloch, alebo pri návrhu či výskyte významných zmien, vzhľadom na stanovené kritériá. Organizácia musí uchovávať ***zdokumentované informácie*** o výsledkoch posudzovania bezpečnostných rizík.

Zaobchádzanie s bezpečnostnými rizikami

Organizácia musí implementovať **Plán zaobchádzania s bezpečnostnými rizikami** a uchovávať zdokumentované informácie o výsledkoch zaobchádzania s bezpečnostnými rizikami.

Manažérstvo zmien

Manažérstvo zmien *(manažment zmien* *alebo* ***riadenie zmien)*** je riadiaci proces v organizácii, ktorý sa vyvinul v 60. rokoch 20. storočia a ktorý sa zaoberá vnímaním, komunikáciou, metodikou, organizáciou a vyhodnocovaním prechodu organizácií, skupín v organizácii i jednotlivcov v organizácii zo súčasného stavu do požadovaného budúceho stavu.

Zahŕňa metodiku organizačných procesov manažmentu zmien a zaoberá sa jednotlivými modelmi riadenia organizačných zmien a riadenia systémových zmien, ktoré sa spolu používajú a vychádzajú z pohľadu riadenia ľudských zdrojov v organizácii. Ide najmä o:

a) **krátkodobú zmenu –** týka sa technologického alebo systémového procesu v organizácii, ktorý sa dá vopred naplánovať, definovať jeho výstupy a následky,
b) **dlhodobú zmenu –** týka sa procesu riadenia systémov a organizačnej zmeny, kde sa zmena plánuje na dlhšie obdobie, je potrebné ju riadiť a kontrolovať a výstupy sú definované v určitých zásadách a charakteristikách, následky sú iba odhadované,
c) **strategickú dlhodobú zmenu –** proces organizačnej zmeny, v ktorej hrá dôležitú úlohu predvídanie, vízia, komunikácia a je potrebné prihliadať k organizačnému správaniu sa skupín, jednotlivcov i organizačného okolia, výstupy sú charakterizované zásadami a následky sú iba odhadnuteľné, často nepredvídateľné.

V prípade **zmien v etape prevádzkovania SMB** ide o:

- vytvorenie a udržiavanie ***metodického postupu na identifikovanie a manažérstvo zmien*** v jednotlivých prvkoch bezpečnostného sektora vo vnútri organizácie, ktoré by mohli ovplyvniť dosiahnutie stanovených bezpečnostných cieľov,
- zabezpečenie, aby požadované výkony v oblasti bezpečnosti umožnili ***zníženie alebo modifikáciu bezpečnostných rizík vyplývajúcich zo zmien*** v organizácii, poskytovaní služieb alebo v prevádzkovom prostredí,
- umožnenie, aby sa zaviedli ***metódy na zisťovanie zmien*** systémov alebo činností, ktoré môžu naznačovať, že sa niektorý prvok blíži k bodu, kedy už nebude možné dodržať prijateľné úrovne bezpečnosti, a že boli prijaté nápravné opatrenia,
- pravidelné ***doplňovanie a aktualizovanie bezpečnostnej dokumentácie*** vzhľadom na vykonané zmeny.

6.8 HODNOTENIE VÝKONNOSTI

Organizácia musí určiť čo, ako a kedy má byť sledované, merané, analyzované a vyhodnotené. Súčasťou tohto procesu je tiež interný audit, aby sa zabezpečilo, že systém manažérstva zodpovedá požiadavkám na organizáciu ako rovnako aj normám a je úspešne zavedený a udržiavaný. Posledným krokom v preskúmaní manažmentom je posúdenie, či je systém manažérstva vhodný, primeraný a účinný.

Hodnotenie výkonnosti obsahuje:

1. **Monitorovanie, meranie, analýzy a vyhodnotenie.**
2. **Interný audit.**
3. **Preskúmanie manažmentom.**

Monitorovanie, meranie, analýzy a vyhodnotenie

Monitorovanie a meranie výkonnosti sa musí vykonávať ako rutinná záležitosť, s cieľom:

- odporučiť zlepšenia tam, kde je to potrebné,
- poskytnúť istotu manažérom zaistením bezpečnosti činností v ich oblastiach,
- overiť zhodu s príslušnými časťami svojich systémov manažérstva bezpečnosti.

Monitorovanie a meranie výkonnosti obsahuje:

a) stanovenie **charakteru, rozsahu a časového plánu** vykonávania ***skúšok výkonnosti SMB,***
b) vytvorenie a udržiavanie **prostriedkov na overenie výkonnosti SMB** organizácie – výkonnosť bezpečnosti organizácie musí byť preukázaná vzhľadom na ukazovatele výkonnosti v bezpečnosti a ciele výkonnosti systému SMB v bezpečnosti,
c) preukázanie **účinnosti opatrení na zaobchádzanie s bezpečnostnými rizikami,**
d) analýzu výsledkov merania – hodnotenie SMB,
e) stretnutia s riadiacim orgánom pre bezpečnosť,
f) zabezpečenie, aby **manažment a zamestnanci dodržiavali politiky, postupy, roly a zodpovednosti** v otázkach bezpečnosti.

Organizácia musí v priebehu monitorovania a merania výkonnosti hodnotiť úroveň bezpečnosti a účinnosť SMB a preto **musí určiť:**

a) čo je potrebné sledovať a merať, vrátane procesov bezpečnosti a kontrol,
b) metódy na monitorovanie, meranie, analýzy a hodnotenia, použiteľné na zistenie právoplatných výsledkov (aby boli zvolené metódy považované za platné mali by dávať porovnateľné a reprodukovateľné výsledky),
c) kedy sa má vykonávať monitorovanie a meranie,
d) kto bude monitorovať a merať,
e) kedy musia byť analyzované a vyhodnotené výsledky z monitorovania a merania,
f) kto bude analyzovať a vyhodnocovať tieto výsledky.

Organizácia musí uchovávať príslušné ***zdokumentované informácie*** ako dôkazy o výsledkoch monitorovania a merania.

Interný audit

Audity sú základnou časťou postupu systému manažérstva na kontrolu napĺňania stanovených cieľov a posúdenie zhody so stanovenými normami. Na pomoc pri vykonávaní **kontroly systémov manažérstva** je určená norma STN EN ISO 19011:2011 **Návod na auditovanie systémov manažérstva**, ktorá poskytuje špecifické návody na vonkajšie a vnútorné audity systémov manažérstva.

Táto norma obsahuje návod na auditovanie systémov manažérstva vrátane zásad auditovania, manažérstva programu auditu a vykonávania auditov systému manažérstva a tiež návod na hodnotenie kompetentnosti jednotlivcov zapojených do procesu auditu vrátane osoby, ktorá manažuje program auditu, audítorov a audítorské tímy.

Interný bezpečnostný audit sa podľa tejto normy vykonáva s cieľom:

- overovať stav realizácie Bezpečnostnej politiky, Plánu implementácie SMB, Havarijného plánu, Bezpečnostného plánu na ochranu objektu alebo Projektu na ochranu objektu,
- zisťovať platnosť prijatej bezpečnostnej koncepcie v konkrétnych podmienkach daného bezpečnostného prostredia,
- zisťovať stav implementácie a výkonnosť SMB organizácie,
- hodnotiť výsledky aplikácie opatrení na zaobchádzanie s rizikom,
- zistiť skutočný stav bezpečnosti a zistiť, či sa činnosti na jej dosiahnutie uskutočňujú plánovane a bez podstatných odchýlok,
- overovať spoľahlivosť prevádzky technických prostriedkov ochrany,
- zisťovať dodržiavanie prijatých organizačných a režimových opatrení,
- overovať platnosť organizačne – riadiacich aktov, bezpečnostných, havarijných a zásahových plánov,
- preverovať činnosť zamestnancov pri plnení úloh na udržiavanie bezpečnosti.

Organizácia musí interné audity vykonávať v plánovaných intervaloch, aby poskytli informácie o tom, či SMB:

a) zodpovedá vlastným požiadavkám organizácie na SMB a požiadavkám tejto medzinárodnej normy.

b) je efektívne zavedený a udržiavaný.

Organizácia musí:

a) plánovať, vytvoriť, zaviesť a udržiavať program(y) auditov, vrátane početnosti, metód, zodpovedností, plánovacích požiadaviek a podávania správ – program auditu(ov) musí brať do úvahy význam príslušných procesov a výsledky predchádzajúcich auditov,
b) definovať kritériá auditu a rozsah každého auditu,
c) vybrať audítorov a vykonávať audity, ktoré zaistia objektivitu a nestrannosť procesu auditu,
d) zabezpečiť, aby výsledky auditov boli hlásené príslušným vedúcim pracovníkom,
e) uchovávať zdokumentované informácie ako dôkazy o programe (och) a výsledkoch auditu.

Interné audity môžu obsahovať:

a) prípravu **plánov interných auditov,**

b) prípravu **postupov pre periodický interný audit** *na zistenie bezpečnostných nedostatkov,* ich súčasťou môžu byť aj *postupy na monitorovanie zhody bezpečnostných opatrení s internými predpismi organizácie a s externými právnymi, regulačnými a zmluvnými požiadavkami a na odstraňovanie zistených nezhôd,*

c) vytvorenie a udržiavanie prostriedkov na overenie:

- *že bezpečnosť organizácie je v súlade s bezpečnostnou politikou a bezpečnostnými cieľmi,*
- *účinnosti manažérstva bezpečnostných rizík, čo sa dosiahne sledovaním a meraním výsledkov aktivít,*

d) recenzie protokolov, zhromaždených metrických hodnôt *z vykonávaných previerok a auditov,*

e) posúdenie **úspechov pri plnení bezpečnostných cieľov,**

f) vykonávanie **pravidelného preskúšavania záložných prostriedkov,**

g) precvičovanie krízových plánov, ak je to vhodné, aj v spolupráci s tretími stranami pre posilňovanie pripravenosti na možné ohrozenia bezpečnosti.

Preskúmanie manažmentom

Preskúmanie manažmentom predstavuje opakovanú činnosť manažmentu na posúdenie ***vhodnosti, primeranosti a efektívnosti SMB organizácie.*** Preskúmavanie kvality SMB organizácie sa vykonáva v ***plánovaných intervaloch***, aby sa zabezpečila jeho trvalá vhodnosť, primeranosť a efektívnosť. Odporúčaný interval preskúmania ***jeden rok*** môže byť v špecifických prípadoch predĺžený alebo skrátený so zreteľom na mieru účinnosti a efektívnosti SMB.

Preskúmanie manažmentom musí zahŕňať úvahy o:

a) stave opatrení z predchádzajúcich preskúmaní vedením,
b) zmenách externých a interných súvislostí, ktoré sa týkajú SMB,
c) spätnej väzbe na výkonnosť bezpečnosti, vrátane trendov v:
   1. nezhodách a nápravných opatreniach,
   2. výsledkoch monitorovania a merania,
   3. výsledkoch auditu,
   4. splnenia cieľov bezpečnosti.
d) spätnej väzbe od zainteresovaných účastníkov,
e) výsledkoch posúdenia rizík a stavu plánu zaobchádzania s rizikami,
f) príležitostiach pre trvalé zlepšovanie.

Preskúmanie manažmentom sa vyhodnocuje formou **Správy z preskúmania manažmentom.** Organizácia musí uchovávať zdokumentované informácie ako dôkaz o výsledkoch preskúmania manažmentom. Pretože sa musí preskúmať stav celého SMB, nestačí aby súčasťou súboru informácií pre preskúmanie manažmentom boli iba výsledky z auditov, ale tento súbor musí zahŕňať všetky rozhodujúce oblasti, zdroje, vstupy a výstupy zo všetkých častí, ktoré sú súčasťou prevádzkovaného SMB, politiky a cieľov kvality.

Výstupy preskúmaní manažmentom musia zahŕňať **rozhodnutia** vzťahujúce sa k príležitostiam ***trvalého zlepšovania*** a akýmkoľvek potrebám pre zmeny v SMB. Tieto výstupy nemôžu byť iba konštatovaním stavu, ale ***musia byť prijaté adekvátne opatrenia a potrebné zdroje na odstránenie nezhôd, ale hlavne na zlepšovanie účinnosti a efektívnosti všetkých činností a procesov.***

6.9 ZLEPŠOVANIE

Obsahom tejto etapy je:

1. **Nezhoda a nápravné opatrenia.**
2. **Trvalé zlepšovanie.**

Nezhoda a nápravné opatrenia

Previerky a nápravné opatrenia sú určené na zlepšenie bezpečnostných procesov organizácie, prijatých na odstránenie príčin nezhôd alebo iných nežiaducich situácií. Sú zamerané na systematické **vyšetrovanie základných príčin nezhôd,** v snahe ***zabrániť ich opakovaniu*** (pre nápravné opatrenia), alebo aby sa ***zabránilo ich vzniku*** (preventívna akcia). Pri výskyte nezhody organizácia musí:

a) reagovať na nezhodu a podľa potreby:
   1. prijať opatrenia na riadenie a nápravu nezhody,
   2. riešiť následky.
b) vyhodnotiť potrebné opatrenia na odstránenie príčin nezhody, aby sa znova neopakovala alebo nevyskytla na inom mieste, a to:
   1. preskúmať nezhodu,
   2. určiť príčiny nezhody,
   3. určiť, či existujú podobné nezhody, alebo by mohli nastať,
c) vykonať všetky potrebné opatrenia;
d) posudzovať účinnosť prijatých nápravných opatrení,
e) vykonávať zmeny v SMB, pokiaľ je to nutné.

Nápravná činnosť predstavuje činnosť na odstránenie ***príčiny zistenej nezhody alebo inej neželateľnej situácie*** a zabránenie ich opakovaniu, využíva sa ako nástroj na zlepšovanie. **Náprava** znamená činnosť na ***odstránenie zistenej nezhody***.

Organizácia musí uchovávať zdokumentované informácie ako dôkaz o:

a) povahe nezhôd a prípadných prijatých nápravných opatreniach,
b) výsledky akéhokoľvek nápravného opatrenia.

Trvalé zlepšovanie

Organizácia musí trvale zlepšovať vhodnosť, primeranosť a účinnosť SMB. Zlepšovanie znamená činnosť, ktorá má prostredníctvom využívania politiky kvality, cieľov kvality, zistení z auditov, analýzy údajov, nápravných a preventívnych činností, a preskúmaní manažmentom akýmkoľvek spôsobom zlepšovať SMB organizácie. Zlepšovaniu môžu pomôcť tieto činnosti:

a) vytvorenie a udržiavanie ***metodického postupu pre určenie príčin neštandardnej výkonnosti*** SMB,
b) určenie ***dopadov neštandardnej výkonnosti na prevádzku*** a odstránenie alebo zmiernenie týchto príčin,
c) stanovenie ***nových strategických cieľov*** pre bezpečnosť,
d) ***optimalizácia*** SMB.

6.10 BEZPEČNOSTNÁ DOKUMENTÁCIA

Bezpečnostná dokumentácia predstavuje súbor bezpečnostných dokumentov. Základnými bezpečnostnými dokumentmi sú **Bezpečnostná politika a Systémové bezpečnostné politiky**. Okrem nich sa vytvára ďalšia dokumentácia pre SMB, manažérstvo rizika, jednotlivé bezpečnostné smernice, metodiky a nariadenia vo všetkých podsektoroch a oblastiach bezpečnostného sektora.

Pri stanovení rozsahu bezpečnostnej dokumentácie musí organizácia vychádzať z **platných zákonov a ďalších noriem**, v ktorých je táto dokumentácia stanovená. Všeobecne možno ďalšiu bezpečnostné dokumenty deliť na: plánovacie, technické, prevádzkové, výkazové, informačné a pomocné.

Príkladmi niektorých bezpečnostných dokumentov, ktoré sa majú spracovať môžu byť:

a) Plánovacie bezpečnostné dokumenty:
- Plán implementácie SMB,
- Bezpečnostný plán ochrany objektu,
- Bezpečnostný plán (ochrany prvku kritickej infraštruktúry),
- Plán manažérstva rizika,
- Plán zaobchádzania s rizikami,
- Havarijný plán,
- Plán kontinuity činností,
- Plán manažérstva incidentov
- Krízový plán ochrany objektu,
- Krízové plány a pod.

b) Prevádzkové bezpečnostné dokumenty:
- Prevádzkový poriadok objektu (obsahuje režimové opatrenia),
- Pravidlá na výkon fyzickej ochrany objektu a grafická časť Schéma rozmiestnenia kontrolných (strážnych) stanovíšť,
- Protipožiarne smernice a pod.

c) Výkazové dokumenty (určené pre pracovníkov fyzickej ochrany objektu na vedenie prehľadu o priebehu služby):
- Denný záznam o priebehu služby,
- Záznamy o odovzdaní a prevzatí služby zmeny,
- Záznam o bezpečnostných incidentoch a mimoriadnych udalostiach,
- Záznam o vykonaných zásahoch ,
- Kniha kontrol,
- Kniha návštev organizácie,
- Kniha návštev chráneného priestoru,
- Kniha vjazdu/výjazdu vozidiel,
- Evidencia výdaja kľúčov,
- Ďalšie dokumenty podľa potreby, resp. rozhodnutia vedúceho.

d) Technické dokumenty, napr. Technická dokumentácia objektu,

e) Informačné dokumenty, napr. Kniha hlásení o incidentoch.

6.10.1 Bezpečnostná politika

Vrcholový manažment musí vytvoriť bezpečnostnú politiku, ktorá:

- je vhodná pre účely organizácie,
- poskytuje štruktúru pre nastavenie a dosiahnutie cieľov bezpečnosti,
- obsahuje záväzok splniť príslušné požiadavky.

Bezpečnostná politika vychádza predovšetkým z týchto faktorov:

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

Bezpečnostná politika musí:

- odrážať ***záväzky*** organizácie týkajúce sa bezpečnosti,
- obsahovať jasné prehlásenie o ***zaistení nevyhnutných zdrojov*** pre zavedenie politiky bezpečnosti,
- ***zahŕňať postupy*** bezpečnostných hlásení,
- jasne určovať ***neprijateľné druhy správania*** a musí zahŕňať ***podmienky***, pri ktorých by nebol uplatňovaný disciplinárny postih,
- byť pravidelne ***preskúmavaná,*** aby bolo zaistené, že je stále relevantná a primeraná danej organizácii.
- ***umožňovať normálnu prevádzku*** – ak totiž v záujme bezpečnosti takmer znemožníme rutinné činnosti, pravidlá sa zákonite porušujú.

Bezpečnostná politika musí byť:

- v súlade s medzinárodnými a národnými právnymi požiadavkami,
- podpísaná zodpovednými vedúcimi organizácie,
- stručná a zrozumiteľná,
- so zrejmým súhlasom oznámená celej organizácii a komunikovaná v organizácii,
- dostupná ako zdokumentovaná informácia,
- dostupná zainteresovaným účastníkom, pokiaľ je to vhodné,
- vynútiteľná a kontrolovateľná,
- z hľadiska svojej vhodnosti preskúmavaná v stanovených intervaloch, a keď sa vyskytnú podstatné zmeny, aby bolo zaistené, že je stále relevantná a primeraná danej organizácii.

Správne vytvorená bezpečnostná politika, ktorá je implementovaná do každodenného fungovania organizácie, sa stáva pevným základom funkčného SMB organizácie. Zaručuje istotu manažmentu, že aktíva organizácie sú dostatočne zabezpečené proti poškodeniu alebo zničeniu. S bezpečnostnou politikou musí byť **so zrejmým súhlasom zoznámená celá organizácia.**

Bezpečnostná politika môže mať ***rôzne podoby,*** ide o ***písomný dokument***, ktorý popisuje všeobecné zásady, na ktorých je postavený a prevádzkovaný SMB v organizácii. Bezpečnostná politika sa obvykle spracováva **pod vedením najvyššieho manažmentu** organizácie a **oznamuje sa všetkým zamestnancom organizácie**. Zverejnenie bezpečnostnej politiky je predpokladom pre vznik a rozvoj pozitívnej ***bezpečnostnej kultúry*** v organizácii.

Po vypracovaní bezpečnostnej politiky ***nasleduje vypracovanie jednotlivých bezpečnostných plánov, potom realizačná a overovacia fáza,*** s cieľom neustáleho zlepšovania bezpečnosti.

Politiky určujú **len zásadné pravidlá**, pre konkrétne systémy ***musia byť doplnené zrozumiteľnými bezpečnostnými postupmi*** (smernicami, metodikami). Bezpečnostné politiky neslúžia len pre formálne účely, ale výrazne sprehľadňujú proces manažérstva bezpečnosti. Dobre spracované politiky určujú jasné hranice dovoleného, nahrádzajú nejasné bezpečnostné opatrenia, prakticky riadia prevádzku, prístup k systémom, životný cyklus systémov atď.

Oboznámenie s bezpečnostnou politikou

Rozsah oboznámenia s bezpečnostnou politikou organizácie sa má stanoviť na základe toho, do akej miery alebo k akým aktívam podniku bude mať zamestnanec alebo tretia osoba prístup. Odporúča sa, aby sa zamestnanci a tretie osoby oboznámili s bezpečnostnou politikou a s povinnosťami z nej vyplývajúcimi ***predtým, ako začnú*** pre organizáciu vykonávať požadované úlohy a činnosti. Organizácia má zabezpečiť aj oboznamovanie týchto subjektov o zmenách, ktoré v jej bezpečnostnej politike nastanú v dobe platnosti ich vzťahu s organizáciou.

Školenia pre zamestnancov organizácie na udržanie a zdokonaľovanie ich bezpečnostných návykov, znalostí a zručností sa odporúča vykonávať ***pravidelne,*** s periódami, ktoré si organizácia zvolí primerane k bezpečnostným úlohám a zodpovednosti zamestnancov.

Bezpečnostné postupy pri personálnych zmenách, ako sú ukončenie pracovného pomeru, zmena pozície a zodpovednosti zamestnancov organizácie alebo ukončenie a zmeny zmluvných vzťahov s tretími osobami sa majú týkať najmä riadenia prístupových práv, účtov, držby zariadení, údajov, dokumentov a pod.

Odporúča sa, aby si organizácia vypracovala ***formálne postupy na právne riešenie*** porušenia bezpečnostných opatrení zo strany zamestnancov, ako aj tretích osôb (disciplinárne konania, sankcie v zmluvách a pod.).

Druhy bezpečnostnej politiky

Nástrojom riadenia bezpečnosti je **celková bezpečnostná politika,** ako verejný záväzný dokument, prijatý vedením organizácie, ako vnútorná norma, z ktorej vychádzajú **systémové bezpečnostné politiky.** Aj keď zodpovednosť za bezpečnosť podniku majú manažéri, je nutné, aby odbornú stránku zabezpečovali bezpečnostní manažéri, systémoví špecialisti a pod., ktorí sú realizátormi bezpečnostnej politiky organizácie.

Podľa úrovne, na ktorej sa bezpečnostná politika spracováva sa rozlišuje:

a) Celková bezpečnostná politika organizácie
- základný a východiskový dokument organizácie, ktorá ňou deklaruje svoj záujem na implementáciu bezpečnosti do všetkých sfér činnosti,
- verejný, záväzný dokument prijatý vedením organizácie, ako vnútorná norma má strategický charakter, prijíma sa na dlhšie obdobie (5 – 10 rokov).

b) Systémové bezpečnostné politiky organizácie – vychádzajú z celkovej bezpečnostnej politiky, ktorá vo svojom vymedzení pôsobnosti ***definuje, pre ktoré oblasti je potrebné jednotlivé politiky resp. koncepcie vypracovávať***, majú platnosť zhruba 2 – 5 rokov, môžu to byť **systémové politiky**:
- Politika manažérstva rizika
- Politika BOZP,
- Politika bezpečnosti osôb a majetku v objektoch a chránených priestoroch,
- Politika bezpečnosti pred požiarmi,

- Politika bezpečnosti kontinuity činností (BCM),
- Environmentálna politika (program),
- Politika informačnej bezpečnosti,
- Politika počítačovej bezpečnosti,
- Bezpečnostný projekt podnikateľa – definovanie bezpečnostnej politiky a spôsob jej realizácie v oblasti OUS (personálnej bezpečnosti, administratívnej bezpečnosti, objektovej a fyzickej bezpečnosti, šifrovej ochrany informácií a bezpečnosti technických prostriedkov).
- Politiky bezpečnosti v iných oblastiach.

Obsah bezpečnostnej politiky je uvedený vo viacerých učebniciach bezpečnostného manažmentu *(Hofreiter, 2002 a Mesároš, Reitšpís, Križovský, 2010)*. Mierne odlišný obsah má bezpečnostná politika uvedená v Manuáli ICAO pre riadenie bezpečnosti. Možný obsah bezpečnostnej politiky zahŕňa podstatné časti z týchto uvedených publikácií. Je tu však uvedený ako návod, každá organizácia vo svojej bezpečnostnej politike uvedie to, čo je pre jej bezpečnosť dôležité.

Možný obsah bezpečnostnej politiky organizácie:

1. **Programové vyhlásenie**.
2. **Záväzok vedenia k zodpovednosti za zachovanie bezpečnosti:**
   a) vyhlásenie vedenia o podpore bezpečnostnej politiky podniku a úlohy vedenia podniku pri zaisťovaní bezpečnosti a integrity,
   b) súlad bezpečnostnej politiky podniku so všeobecne záväznými právnymi predpismi, s vnútornými predpismi podniku a jeho zmluvnými záväzkami.
3. **Zodpovednosť za bezpečnosť:**
   a) definovanie zodpovednosti a kompetencií pracovníkov organizácie,
   b) všeobecné a špecifické zodpovednosti a povinnosti v oblasti bezpečnosti na zaistenie nenarušenia bezpečnosti a integrity.
4. **Analýza súčasného stavu bezpečnosti organizácie:**
   a) charakteristika a účel organizácie,
   b) dislokácia a popis všetkých objektov (infraštruktúry) organizácie,
   c) ***definovanie aktív v objektoch a chránených priestoroch organizácie*** – je potrebné zistiť nakoľko významná je ich ochrana, výhodné je usporiadať ich podľa cennosti,
   d) popis stávajúceho stavu ochrany osôb a majetku,
   e) úroveň manažérstva bezpečnosti a manažérstva rizika,
   f) čiastkový záver k stavu bezpečnosti jednotlivých sektorov bezpečnosti.
5. **Manažérstvo rizika:**
   a) identifikácia nebezpečenstva (odkiaľ hrozí nebezpečenstvo a jeho opodstatnenie),
   b) ***určenie kritérií rizika*** a stanovenie ***metód identifikácie a analýzy rizika***.
6. **Plánovanie bezpečnosti:**
   a) stanovenie ***bezpečnostných cieľov*** organizácie, spôsobov a kritérií ich vyhodnocovania a spôsobov kontroly postupov využívaných na ich dosahovanie,
   b) určenie ***bezpečnostných noriem***,
   c) príprava Plánu implementácie SMB,
   d) určenie zásad havarijného plánovania a riešenia bezpečnostných incidentov, príprava plánov,
   e) určenie, ktoré ďalšie dokumenty na zaistenie bezpečnosti a integrity organizácia vypracuje.
7. **Dosiahnutie a riadenie bezpečnosti:**
   a) vytvorenie Systému manažérstva bezpečnosti organizácie,

b) stanovenie rozsahu, úrovne, spôsobov a postupov zavedenia opatrení na ochranu aktív organizácie a jej sektorov bezpečnosti, časových podmienok a finančných podmienok ich zavedenia,
c) návrh na spôsob dosiahnutia bezpečnostného povedomia v podniku (školenia, osveta).

8. Zaistenie bezpečnosti:

a) zavedenie systému kontroly bezpečnosti organizácie, spôsoby riešenia pri narušení bezpečnosti a rozsah a periodicita vnútorného bezpečnostného auditu organizácie,
b) prostriedky, procesy, postupy a zdroje na preukázanie zhody s bezpečnostnými normami,
c) požadované dôkazy o dosiahnutej úrovni bezpečnosti (napr. výsledky previerky bezpečnosti, bezpečnostné záznamy atď.).

9. Podpora bezpečnosti

a) stanovenie postupov pri revízii bezpečnostnej politiky organizácie, vrátane periodicity pravidelných revízií a dôvodov mimoriadnych revízií bezpečnostnej politiky.
b) zabezpečenie nepretržitého školenia a nácvikov bezpečnosti (napr. nácvik činnosti podľa havarijného plánu) a šírenia hlavných informácií o bezpečnosti v celej organizácii,
c) komunikácia o otázkach bezpečnosti so zainteresovanými účastníkmi.

Možný obsah Programového vyhlásenia

Programové vyhlásenie *(policy statement)* – predstavuje vyhlásenie o celkových cieľoch bezpečnosti v organizácii, určuje všeobecný smer a úsilie pre zvýšenie bezpečnosti.

Možný príklad obsahu programového vyhlásenia:

„Bezpečnosť je na prvom mieste vo všetkých našich činnostiach. Zaviazali sme sa pre vykonávanie, rozvoj a zlepšovanie stratégie, systémov riadenia a postupov, aby zabezpečili, že všetky naše aktivity budú udržiavať najvyššiu výkonnosť v oblasti bezpečnosti všetkých činností a spĺňať národné a medzinárodné štandardy.

Naším cieľom je:

- *vytvoriť a zaviesť bezpečnostnú kultúru do všetkých činností, ktorá uznáva význam a hodnotu efektívneho riadenia bezpečnosti za všetkých okolností a potvrdzuje, že bezpečnosť je prvoradá,*
- *jasne vymedziť pre všetkých pracovníkov povinnosti a zodpovednosti za vývoj, zavedenie a dodržiavanie stratégie bezpečnosti,*
- *modifikovať riziká spojené s činnosťami až na dosiahnuteľnú alebo uskutočniteľnú úroveň,*
- *zabezpečiť, aby externe dodávané systémy a služby, ktoré majú vplyv na bezpečnosť činností, spĺňali príslušné bezpečnostné normy,*
- *aktívne rozvíjať a zlepšovať bezpečnostné postupy v organizácii, aby zodpovedali svetových štandardom,*
- *dodržiavať právne a regulačné požiadavky a normy,*
- *zabezpečiť, aby celému personálu boli poskytované primerané a vhodné informácie o bezpečnosti a odborná príprava na dosiahnutie kompetencií v otázkach bezpečnosti a prideľovať im iba úlohy porovnateľné s ich schopnosťami,*
- *zabezpečiť dostatočný počet kvalifikovaných a vyškolených pracovníkov na realizovanie bezpečnostnej stratégie a politiky,*
- *zaviesť a merať výkonnosť v oblasti bezpečnosti vo vzťahu k reálnym cieľom,*
- *dosiahnuť najvyššiu úroveň bezpečnostných noriem a výkonov vo všetkých činnostiach,*
- *nepretržite zlepšovať bezpečnosť prevádzky,*
- *hodnotiť výkonnosť v oblasti bezpečnosti a zabezpečiť prijímanie príslušných opatrení".*

6.10.2 Plán implementácie Systému manažérstva bezpečnosti

Úspešné manažérstvo bezpečnosti vyžaduje jasne definované plánovacie procesy a postupy. Dobrý **Plán implementácie SMB** (niekde ako Realizačný plán) povedie organizáciu smerom k dosiahnutiu svojich cieľov v oblasti bezpečnosti. Plán predstavuje nástroj pre praktické uplatňovanie základných bezpečnostných zásad definovaných v bezpečnostnej politike organizácie.

Rovnako ako v praktikách všeobecného manažmentu, začína činnosť SMB starostlivým a podrobným plánovaním. Rozsah Plánu implementácie SMB sa vzťahuje na všetky súčasti SMB, vrátane organizačnej štruktúry, procesov, prostriedkov a postupov manažérstva bezpečnosti. Okrem toho plán výslovne rieši koordináciu medzi SMB organizácie a SMB iných organizácií, s ktorými sa organizácia musí prepojiť v priebehu svojich činností.

Proces plánovania by mal využiť možnosti a zdroje organizácie pre manažérstvo bezpečnosti (vrátane skúseností, vedomostí, procesov, postupov riadenia a pod.). Plánovacie činnosti bude riadiť bezpečnostný manažér organizácie a pre zvýšenie úrovne plánovania sa môžu využiť aj líniovi manažéri na kľúčových pozíciách. Vykonávací Plán implementácie SMB musí byť **schválený vrcholovým vedením organizácie.**

Plán implementácie SMB, založený na podrobných výsledkoch procesov diferenčných analýz, sa pripravuje na vyplnenie jednotlivých etáp, ktoré tvoria prvky štruktúry SMB. Je to realistická stratégia pre implementáciu SMB, ktorá bude v organizácii podporovať účinné a efektívne dosiahnutie bezpečnostných cieľov. Popisuje, ako organizácia dosiahne svoje bezpečnostné ciele a ako spozná nové alebo upravené bezpečnostné požiadavky a regulátory. Plán implementácie SMB nemusí byť súhrnný alebo neúmerne podrobný, ale má poskytnúť základnú orientáciu na spoznanie celkových cieľov stanovených v štruktúre SMB, na vytvorenie a zavedenie integrovaného komplexného SMB pre celú organizáciu.

Plány môžu mať rôzne úrovne podrobností, zvyčajne sa používajú dve úrovne:

- **jednoročný plán** s podrobnými detailmi (spracovaný na týždennej báze),
- **trojročný plán,** kde sú znázornené celkové míľniky a aktivity, ale nie podrobne.

Plán má byť aktualizovaný na polročnom základe. Odporúča sa využívať metódu, pri ktorej sa plánujú všetky denné aktivity v najbližších troch mesiacoch.

Plán, fázy, míľniky a výstupy

Podrobný plán zahŕňa celý rad informácií, vrátane doby trvania jednotlivých **fáz** a v rámci každej fázy zahŕňa **činnosti,** ktoré je potrebné vykonať. Navyše, **vzťah medzi činnosťami/ fázami a míľnikmi** v ňom musia byť uvedené, takže je jasné, kedy bude každý míľnik dosiahnutý a ktoré činnosti sa musia vykonať pred dosiahnutím míľnika, aby mohlo byť vyhlásené jeho dosiahnutie.

Podobne ako míľniky, aktivity atď., musia byť naplánované rôzne **výstupy** – v tejto súvislosti je dôležité zdôrazniť, že výstupy sa vzťahujú k činnosti a míľnik umožňuje overenie, že z projektu vznikli určité výstupy.

Nasledovná štruktúra Plánu implementácie SMB je spracovaná s využitím Manuálu manažérstva bezpečnosti medzinárodnej civilnej leteckej organizácie Doc 9859 AN/460.

Model implementácie SMB podľa ICAO (obr. 17)

Politika a ciele bezpečnosti

1.1 Prihlásenie sa vrcholového manažmentu k vytvoreniu SMB a ich zodpovednosť.
1.2 Zodpovednosti manažmentu za bezpečnosť.
1.3 Určenie kľúčového personálu vo vzťahu k bezpečnosti.
1.4 Plán implementácie SMB.
1.5 Dokumentácia.

Identifikácia nebezpečenstiev a manažérstvo rizika

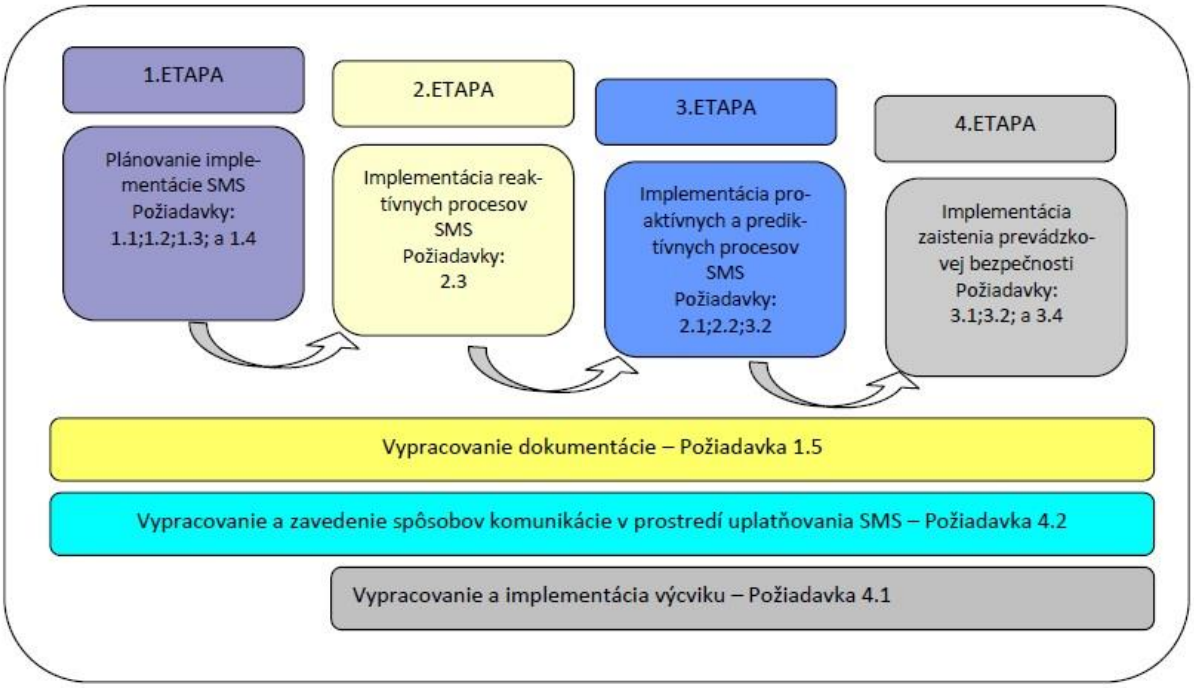
2.1 Proces identifikácie nebezpečenstiev.
2.2 Posudzovanie rizika a proces jeho modifikácie.
2.3 Interné vyšetrovanie bezpečnosti.

Zaistenie bezpečnosti

3.1 Monitorovanie a meranie výkonnosti bezpečnosti.
3.2 Audity a previerky bezpečnosti.
3.3 Manažment zmien.
3.4 Priebežné zlepšovanie systému bezpečnosti.

Presadzovanie bezpečnosti

4.1 Výcvik a vzdelávanie.
4.2 Komunikácia v prostredí uplatňovania bezpečnosti.



Obr. 17 Model implementácie SMB podľa ICAO

ZÁKLADNÁ ŠTRUKTÚRA PLÁNU IMPLEMENTÁCIE SMB

1. Bezpečnostné plánovanie a ciele bezpečnosti.
2. Bezpečnostná politika.
3. Bezpečnostné role a zodpovednosti.
4. Popis systému.
5. Diferenčná analýza.
6. Procesy identifikácie rizík.
7. Procesy manažérstva rizík.
8. Meranie stavu bezpečnosti.
9. Bezpečnostné školenia.
10. Komunikácia o bezpečnosti.
11. Koordinácia s tretími stranami.
12. Preskúmanie vedením (výkonov v oblasti bezpečnosti).

PLÁN IMPLEMENTÁCIE SMB

FÁZA 1

BEZPEČNOSTNÁ POLITIKA A CIELE

Táto fáza by mala plánovať umožniť vytvorenie SMB a jeho integrovanie do pracovných činností organizácie.

1. BEZPEČNOSTNÁ POLITIKA A CIELE

Bezpečnostná politika ukazuje princípy, procesy a metódy SMB na dosahovanie požadovaného výsledku bezpečnosti. Politika ustanovuje záväzok vrcholového manažmentu na dosahovanie a neustále zlepšovanie bezpečnosti vo všetkých aspektoch činnosti organizácie. Vrcholový manažment vytvára opatrenia a vedie organizáciu na dosahovanie rozsiahlych bezpečnostných cieľov.

a) Záväzok manažmentu pre implementáciu SMB:

- Identifikovanie bezpečnostných cieľov organizácie – ciele ako presné a skutočné prvky musia byť potvrdzované (v rôznych fázach) a spojené s indikátormi bezpečnostnej výkonnosti a výkonnostných cieľov bezpečnosti.
- Vývoj bezpečnostnej politiky, ktorý obsahuje aspoň nasledujúce body:
  - dosiahnutie najvyšších bezpečnostných noriem,
  - dodržiavanie všetkých platných právnych požiadaviek, medzinárodných noriem a najefektívnejších postupov,
  - poskytnutie primeraných ľudských a finančných zdrojov,
  - presadzovanie bezpečnosti ako jednej z primárnych zodpovedností všetkých manažérov,
  - zaistenie, že politika je prevzatá, realizovaná a zachovávaná na všetkých úrovniach, určenie časového rozvrhu pre zavedenie procesov SMB medzi jednotlivými úrovňami riadenia organizácie.

b) Stanovenie očakávanej úrovne SMB vedením a jeho využitie zo strany zainteresovaných účastníkov na ich pracoviskách:

- záznam požiadaviek na SMB do zmluvného procesu,
- stanovenie požiadaviek na SMS v dokumentácii.

c) Bezpečnostná komunikácia:

- komunikácia pre využívanie bezpečnostnej politiky všetkými zamestnancami,

- zavedenie komunikačných prostriedkov pre komunikáciu otázok súvisiacich s bezpečnosťou, ktoré by mohli zahŕňať: bezpečnostné zásady a postupy, spravodajcu, bulletiny, web stránky.

2. NÁVRH ŠTRUKTÚRY SYSTÉMU A DIFERENČNÁ ANALÝZA

a) Stanovenie pravidiel pre popis systému a interakcie jeho jednotlivých zložiek:

- zváženie požiadaviek na zabezpečenie činnosti systému ľuďmi,
- hardvérové komponenty systému,
- softvérové komponenty systému,
- prostredie organizácie,
- systém interakcie s inými systémami,
- dodávateľský a nakúpený tovar a služby.

b) Vykonanie diferenčnej analýzy štyroch zložiek a trinástich prvkov v rámci SMS:

1. Bezpečnostná politika a ciele

1.1 Záväzok a zodpovednosť manažmentu.
1.2 Zodpovednosť manažérov za bezpečnosť.
1.3 Vymenovanie kľúčových bezpečnostných pracovníkov.
1.4 Koordinácia plánovania reakcie na mimoriadne udalosti.
1.5 Dokumentácia.

2. Manažérstvo bezpečnostných rizík

2.1 Proces identifikácie rizika.
2.2 Proces posudzovania a zmierňovania rizika.

3. Zaistenie bezpečnosti

3.1 Sledovanie a meranie výkonnosti bezpečnosti.
3.2 Riadenie zmien.
3.3 Neustále zlepšovanie SMB.

4. Podpora bezpečnosti

4.1 Školenie a vzdelávanie.
4.2 Bezpečnosť komunikácie.

c) Identifikovanie potenciálnych problémov pri implementácii, vypracovanie plánov pre riešenie výzvy (t. j. posúdenie rizík plánu)

Z výsledkov diferenčnej analýzy by realizačný tím mal vytvoriť štruktúru SMB a určiť zodpovednosti kľúčových pracovníkov za bezpečnosť.

3. VYTVORENIE ORGANIZAČNEJ ŠTRUKTÚRY SMB

a) Tím plánovania implementácie navrhne štruktúru SMB a zodpovednosť kľúčových zamestnancov za bezpečnosť:

- **Vrcholový manažment** – úroveň organizácie:
  - poradenstvo vrcholového manažmentu o otázkach bezpečnosti,
  - pomoc líniovým manažérom,
  - dohľad nad systémami identifikácie rizík.
- **Bezpečnostný manažér** – zodpovednosti:
  - individuálna zodpovednosť a ústredná zložka pre vývoj a udržiavanie efektívneho SMB,
  - určenie funkcií bezpečnostných pracovníkov a kritérií pre výber,
- **Riadiaci orgán bezpečnosti** (Bezpečnostný výbor alebo rada):
  - vysoká úroveň orgánu, strategické bezpečnostné funkcie,

b) Schválenie plánu implementácie SMB a počiatočný výcvik:

- vytvorenie návrhu plánu implementácie SMB,
- určenie nákladov spojených s odbornou prípravou a plánovaním implementácie,
- návrh rozpočtu pre implementáciu SMB,
- schválenie pôvodného rozpočtu pre plán implementácie SMB,
- podpis vykonávacieho plánu implementácie SMB zodpovedným vedúcim.

c) Školenie:

- predstavenie koncepcie SMB pre všetky úrovne zamestnancov, dodávateľov a subdodávateľov,
- spresnenie, kto má byť vyškolený, určenie, kto potrebuje ďalšie fázy školenia,
- spracovanie školiacej a výcvikovej dokumentácie,
- vytvorenie harmonogramu školenia všetkých zamestnancov,
- určenie fáz školenia – systém prípravy tímov reakcie na incidenty, plánovanie vzdelávania a dosiahnutie pripravenosti, plánovanie metodiky nácvikov, špecifické prípravné praktické nácviky,
- nácviky spôsobu reakcie na mimoriadne situácie – priemyselné havárie, bezpečnostné incidenty, vonkajšie nebezpečnstvá, teroristický útok, postupy pri evakuácii, extrémne počasie, lekárska pohotovosť
- určenie nákladov spojených s odbornou prípravou.

4. KOORDINÁCIA PLÁNOVANIA REAKCIE NA NÚDZOVÉ SITUÁCIE

a) Vnútorná koordinácia:

- zavedenie tímu pre havarijné plánovanie,
- vymenovanie koordinátora pre havarijné plánovanie,
- odkaz na postupy riešenia na príslušnom mieste a iné.

b) Externá koordinácia:

- zavedenie záchranných služieb.

5. DOKUMENTÁCIA

a) Vytvorenie pracoviska na umiestnenie všetkej bezpečnostnej dokumentácie v organizácii

VYHODNOTENIE FÁZE 1

Časová os: 1-6 mesiacov, záleží na zložitosti organizácie.

Výstupy:

- Bezpečnostné ciele organizácie schválené zodpovedným výkonným orgánom.
- Bezpečnostná politika podpísaná zodpovedným výkonným orgánom.
- Bezpečnostná politika rozšírená v rámci celej organizácie.
- Organizačná štruktúra SMB zavedená.
- Zápisy o zodpovednosti za bezpečnosť založené.
- Plán implementácie SMB a počiatočného vzdelávania schválený.
- Havarijný plán zavedený.

Míľniky:

- Predloženie návrhu bezpečnostnej politiky.
- Dodanie výsledkov diferenčnej analýzy (popis aktuálneho stavu, stanovenie cieľov (cieľového stavu) a spôsobov ich dosiahnutia.
- Návrh organizačnej štruktúry SMB, vrátane pridelenia finančných prostriedkov a termínov pre procesy medzi jednotlivými vrstvami riadenia SMB organizácie.
- Návrh rozpočtu pre procesy manažérstva bezpečnosti.

FÁZA 2

MANAŽÉRSTVO BEZPEČNOSTNÝCH RIZÍK

(Reaktívne procesy)

Reaktívne riadenie znamená reakciu na zmenu alebo krízu po tom, čo nastane s malým, až žiadnym očakávaním. Reaktívne riadenie sa vyznačuje nedostatkom plánovania.

Prostriedky zhromažďovania a zaznamenávania, ktoré uvádzajú a vytvárajú spätnú väzbu o **nebezpečenstve a rizikách v činnosti organizácie** podľa výsledkov diferenčnej analýzy:

a) Určenie podoby **intervenčného nástroja,** ktorý sa používa **pre zber reaktívnych informácií.**

b) Rozhodnutie, ktoré **systémy hlásenia** bude potrebné zaviesť v organizácii:
- povinný systém hlásenia,
- dobrovoľné systémy podávania správ,
- dôverné systémy podávania správ.

c) Určenie, aká **matica rizík** sa bude používať (tradičná alebo vlastnoručne vytvorená):
- vlastné matice rizík vyhovujú zložitej organizácii,
- vytvorenie matice rizík na formulároch z predpisov a / alebo z nácvikov.

d) Určenie úrovne kritérií rizík (úrovne neprijateľné, prijateľné alebo prípustné).

e) Zaznamenávanie a písomné oznámenie týchto požiadaviek dodávateľom a subdodávateľom,

f) Identifikovanie procesu riadenia / zodpovednosti za realizáciu stratégií:
- bude potrebná databáza na zaznamenanie reaktívnych dát do formulára?
- kto bude udržiavať archivovanie / databázu?
- kto bude analyzovať dáta pre budúci vývoj?
- ako budú oznámené trendy vývoja?
- vytvorenie stratégie na riadenie a zmiernenie rizík (pre reaktívne procesy).

g) Vybudovanie registra bezpečnosti (prehľad bezpečnostnej dokumentácie).

h) Zhromažďovanie informácií pre ukazovatele výkonu v oblasti bezpečnosti.

i) Príprava inštruktorov.

j) Príprava vedúcich.

k) Príprava pracovníkov prvej línie.

l) Poskytovanie priebežného koučovania a poradenstva vedúcimi orgánmi pre personál prvej línie.

VYHODNOTENIE FÁZE 2

Časová os: x až y mesiacov, záleží na zložitosti organizácie

Výstupy:
- Systém hlásení (pre reaktívne procesy) zavedený.
- Bezpečnostný register vytvorený.

Míľniky:
- Výber matice na posúdenie rizík pre reaktívne procesy.
- Zavedenie postupu predkladania bezpečnostných dát v činnosti organizácie do príbuzných kategórií informácií o rizikách.
- Ukončenie školenia o reaktívnych procesoch pre zamestnancov, manažérov a vedúcich pracovníkov bezpečnosti.
- Poskytovanie dôležitých informácií o bezpečnosti v organizácii na základe reakčných procesov.

FÁZA 3

MANAŽÉRSTVO BEZPEČNOSTNÝCH RIZÍK

(Proaktívne a prediktívne procesy)

Proaktívne riadenie znamená myslieť dopredu, predvídať udalosti (ako sú problémy, trhy, trendy, požiadavky zákazníkov) a plánovať zmeny alebo krízy.

a) Určiť formu **intervenčných nástrojov,** ktoré majú byť použité na zber proaktívnych a prediktívnych informácií (napr. dôverné spravodajské systémy, monitorovanie činnosti atď.).
b) Aktualizovanie **smerníc, postupov, hardvéru a softvéru** na podporu proaktívnych a prediktívnych intervenčných nástrojov.
c) Hodnotenie a aktualizácia **politiky zberu informácií (spravodajstva).**
d) Identifikovanie **administratívnych procesov / zodpovednosti za zber informácií:**
   - bude potrebná databáza na zapísanie proaktívnych a prediktívnych dát z formulára?
   - kto bude udržiavať evidenciu / databázu?
   - kto bude analyzovať dáta pre trendy vývoja?
   - ako sa budú trendy vývoja oznamovať?
e) **Školenie bezpečnostných pracovníkov** o špecifických intervenčných nástrojoch na zhromažďovanie informácií.
f) **Určenie úrovne riadenia rizík,** ktoré majú byť zaznamenané (ako vo fáze 2).
g) Použitie **matice rizík** (ako vo fáze 2).
h) Rozvíjanie **stratégie modifikovania a riadenia rizík.**
i) **Inštruktáž** vedúcich a zamestnancov prvej línie o proaktívnych a prediktívnych procesoch.
j) Požiadavky na poskytnutie **písomnej dokumentácie** pre dodávateľov a subdodávateľov.
k) Tvorba **ukazovateľov výkonnosti bezpečnosti a výkonnostných cieľov bezpečnosti**.

VYHODNOTENIE FÁZE 3

Časová os: x až y mesiacov, záleží na zložitosti organizácie,

Výstupy:

- Systém spravodajstva o bezpečnosti (pre proaktívne a prediktívne procesy) zavedený.
- Ukazovatele výkonnosti bezpečnosti a výkonnostné ciele bezpečnosti schválené generálnym riaditeľom.

Míľniky:

- Vytvorenie stratégie riadenia rizika / zmiernenia.
- Hodnotenie ukazovateľov výkonnosti bezpečnosti a výkonnostných cieľov bezpečnosti podľa stanovených noriem.
- Ukončenie školenia zamestnancov, manažérov a vedúcich o proaktívnych a prediktívnych procesoch.
- Zavedenie reaktívnych procesov na oznamovanie dôležitých bezpečnostných informácií v organizácii.

FÁZA 4

ZAISTENIE BEZPEČNOSTI ČINNOSTI A PODPORA BEZPEČNOSTI

Prijateľná úroveň bezpečnosti:

a) **Definovanie ukazovateľov výkonnosti** v oblasti bezpečnosti a **výkonnostných cieľov** bezpečnosti pre **prijateľnú úroveň bezpečnosti** organizácie
b) Stanovenie **požiadaviek na bezpečnosť**, aby boli naplnené ukazovatele výkonnosti v oblasti bezpečnosti a výkonnostné ciele bezpečnosti pre prijateľnú úroveň bezpečnosti
c) Stanovenie **prijateľnej úrovne bezpečnosti** a hlásenie nadriadeným.

Sledovanie a meranie výkonnosti bezpečnosti

Definovanie procesu na overenie výkonnosti bezpečnosti organizácie v porovnaní so schválenými bezpečnostnými politikami a cieľmi:

- správy o bezpečnosti,
- bezpečnostné štúdie,
- hodnotenie bezpečnosti,
- audity,
- prieskumy,
- vnútorné bezpečnostné vyšetrovanie incidentov, ktoré nemusia byť vyšetrované alebo hlásené zložkám bezpečnosti,
- definovanie ukazovateľov výkonnosti v oblasti bezpečnosti a výkonnostných cieľov bezpečnosti pre prijateľnú úroveň bezpečnosti organizácie,
- stanovenie požiadaviek na bezpečnosť, aby boli naplnené ukazovatele výkonu v oblasti bezpečnosti a výkonnostné ciele bezpečnosti pre prijateľnú úroveň bezpečnosti,
- vytvorenie línií zodpovednosti za mieru spoľahlivosti, dostupnosti a / alebo presnosti bezpečnostných požiadaviek.

Manažérstvo zmien

- posúdenie vnútorných a vonkajších zmien,
- identifikovanie vplyvov zmien na zavedené procesy a služby,
- opatrenia na zaistenie súvislého bezpečnostného výkonu SMB.

Neustále zlepšovanie SMB

- dokončené proaktívne vyhodnotenie zariadenia, vybavenia, dokumentácie a postupov prostredníctvom auditov a prieskumov,
- dokončené proaktívne hodnotenie výkonnosti jednotlivcov na overenie plnenia ich bezpečnostných povinností,
- zavedenie postupov pre reaktívne hodnotenie na overenie účinnosti systému riadenia a zmierňovania rizík (nehody, incidenty a vyšetrovanie významných udalostí),
- školenia o zaistení bezpečnosti činností,
- dokumentácia pre zaistenie bezpečnosti činností,
- hlásenie identifikovaných zmien na základe analýzy vývojových trendov rizík,
- aktualizácia smerníc pre bezpečnosť práce,
- doplňovanie Programu bezpečnosti.

Podpora bezpečnosti

Efektívne metódy na podporu bezpečnosti v tejto fáze by okrem iného mali zahŕňať:

- prieskum, hodnotenie a oznamovanie zmien na využitie v SMB a tvorbu noriem,
- využívanie rôznych poučiek a podkladov na podporu zlepšovania SMB,
- určenie spôsobov oznamovania úspechov SMB (napr. po ukončení školenia, predkladanie dokumentácie o trendoch vývoja, zmeny programov súvisiacich s bezpečnosťou atď.)

- kontrola bezpečnostnej politiky vrátane jej oznamovania,
- podpora účasti všetkých pracovníkov na identifikácii rizík.

VYHODNOTENIE FÁZE 4

Časová os: x až y mesiacov, záleží na zložitosti organizácie,

Výstupy:
- Prijateľná úroveň bezpečnosti dosiahnutá a hlásená nadriadeným.
- Upravená stratégia a bezpečnostné postupy schválené generálnym riaditeľom.

Míľniky:
- Schválenie procesov monitorovania a merania bezpečnosti činností a prehodnotenie stratégie a postupov SMB.
- Dokončenie školenia personálu, manažérov a vedúcich o aktívnom zaistení bezpečnosti.

6.10.3 Havarijné plánovanie

Havarijné plánovanie je **súbor opatrení na *zisťovanie, prevenciu, elimináciu a zdolávanie incidentov, nehôd a havárií*** *prírodného, technického, technologického, radiačného, environmentálneho, epidemiologického, epizootického, epifitického charakteru,* vrátane únikov nebezpečných látok do životného prostredia pri ich používaní, preprave a skladovaní.

Havarijné plánovanie je riešené s odvolávaním sa na právne normy Európskej únie s dôrazom na:
- **závažné priemyselné havárie,**
- **jadrové havárie,**
- **havárie v odpadovom hospodárstve,**
- **havárie vo vodnom hospodárstve,**
- **havárie zo znečistenia ovzdušia,**
- **havárie požiarneho charakteru,**
- **havárie informačných a bezpečnostných systémov,**
- **havárie pri preprave nebezpečných látok.**

Hlavné ciele havarijného plánovania zahŕňajú ochranu:
- života a zdravia občanov,
- životného prostredia a kultúrnych hodnôt,
- majetku.

V rámci prevencie závažným priemyselným haváriám je prevádzkovateľ podľa Zákona o prevencii závažných priemyselných havárií a Vyhlášky MŽP SR č. 490/2002 Z. z. o bezpečnostnej správe a o havarijnom pláne povinný vypracovať:
- **Bezpečnostnú správu** (prevádzkovateľ organizácie kategórie B),
- **Havarijný plán,**
- a spolupracovať na vypracúvaní **Plánu ochrany obyvateľstva** podľa Zákona o civilnej ochrane obyvateľstva.

Bezpečnostná správa

Bezpečnostná správa podľa Zákona o prevencii závažných priemyselných havárií a Vyhlášky MŽP SR č. o bezpečnostnej správe a o havarijnom pláne s prihliadnutím na nebezpečenstvá, ktoré organizácia predstavuje, podáva komplexnú charakteristiku organizácie umožňujúcu získať celkovú predstavu o jej zameraní, umiestnení, činnostiach, o reálnych nebezpečenstvách, ako aj o službách, zariadeniach a opatreniach na bezpečnú prevádzku, prevenciu závažných priemyselných havárií a pripravenosť na ich zdolávanie vrátane väzieb me-

dzi jednotlivými časťami organizácie alebo zariadeniami, ich vzájomného ovplyvňovania a vzťahu k okoliu.

Vyhotovenie, členenie a rozsah bezpečnostnej správy má vychádzať zo zložitosti a rizikovosti organizácie a konkrétnych podmienok jej umiestnenia. Bezpečnostná správa musí byť prehľadná a zrozumiteľná.

Bezpečnostná správa obsahuje:

a) základné informácie o organizácii vrátane jej organizačnej štruktúry, riadenia a umiestnenia,
b) opis okolia a životného prostredia,
c) súpis, opis a umiestnenie vybraných nebezpečných látok prítomných v organizácii,
d) opis činností a zariadení v organizácii spojených s rizikom závažnej priemyselnej havárie,
e) opis prevádzkových služieb týkajúcich sa spoľahlivosti prevádzky organizácie, prevencie závažných priemyselných havárií, ako aj pripravenosti na ich zdolávanie,
f) identifikáciu a analýzu zdrojov rizika závažných priemyselných havárií a ich hodnotenie vrátane príslušných bezpečnostných opatrení,
g) informácie o programe prevencie závažných priemyselných havárií a o bezpečnostnom riadiacom systéme, ako aj o opatreniach týkajúcich sa pripravenosti na zdolávanie závažných priemyselných havárií a na obmedzovanie ich následkov vrátane informácií o havarijnom pláne a o podkladoch na vypracovanie plánu ochrany obyvateľstva,
h) zoznam právnických osôb a podnikajúcich fyzických osôb, ktoré sa podieľali na vypracovaní bezpečnostnej správy.

Mapová dokumentácia obsahuje mierku, v ktorej je vyhotovená, a vyznačený sever. Ostatná grafická dokumentácia musí byť vypracovaná a označená tak, aby z nej boli zrejmé jednotlivé rozmery, vzdialenosti, prípadne aj iné dôležité skutočnosti.

Havarijný plán

Havarijný plán je špecifický plánovací dokument obsahujúcich súbor organizačných a technických opatrení a dokumentovaných postupov (typových plánov) potrebných na zdolávanie havárie alebo zmierňovanie jej následkov, má umožniť vlastné fungovanie za krízových situácií, riadny a účinný prechod z normálnej prevádzky do prevádzky v stave núdze a návrat do normálnej prevádzky. Havarijný plán musí byť prehľadný, stručný a zrozumiteľný.

Poslaním havarijného plánu je zabezpečiť:

- ***včasnú a adekvátnu reakciu*** na bezpečnostnú hrozbu závažnej priemyselnej havárie alebo na vzniknutú závažnú priemyselnú haváriu a na jej zdolanie,
- ***vykonanie opatrení*** potrebných na zaistenie bezpečnosti a ochrany života a zdravia ľudí, životného prostredia a majetku pred následkami závažnej priemyselnej havárie a na obmedzenie týchto následkami závažnej priemyselnej havárie a na obmedzenie týchto následkov,
- potrebnú ***informovanosť***zamestnancov, dotknutej verejnosti, ako aj príslušných orgánov a iných subjektov, s ktorých súčinnosťou sa uvažuje,
- umožnenie ***obnovy*** (sanácie) životného prostredia poškodeného závažnou priemyselnou haváriou.

Obsah havarijných plánov, zásady ich vypracúvania, precvičovania a prehodnocovania, ako aj zásady oboznamovania zamestnancov organizácie a ďalších osôb s nimi, rieši Vyhláška MŽP SR č. 490/2002 Z. z. o bezpečnostnej správe a o havarijnom pláne.

Havarijný plán je ucelený súbor písomnej a grafickej dokumentácie, ktorý **sa člení na:**

1. **Všeobecnú časť:**
   a) všeobecné údaje o organizácii a jej okolí,
   b) osobitné údaje o organizácii.
2. **Pohotovostnú časť,**
   a) plán vyrozumenia a zvolania,
   b) zoznam vedúcich zamestnancov, ďalších zamestnancov, útvarov a služieb,
   c) spôsob vyhlásenia poplachu a varovania,
   d) uvedenie a stručný opis nebezpečenstiev,
   e) určenie záchranných a únikových ciest a zhromaždísk pre zamestnancov a iné osoby zdržiavajúce sa s vedomím prevádzkovateľa v areáli organizácie,
   f) určenie miesta na riadenie zdolávania závažnej priemyselnej havárie a základní pre záchranné zložky,
   g) zoznam a potrebné údaje o vybraných nebezpečných látkach prítomných v organizácii,
   h) zoznam, opis a vyznačenie objektov, zariadení, technologických procesov a pracovísk, ktoré vyžadujú na čo možno najdlhší čas neprerušený chod a prítomnosť príslušných zamestnancov i počas závažnej priemyselnej havárie,
   i) zoznam a rozmiestnenie prostriedkov potrebných na zdolávanie závažných priemyselných havárií a obmedzovanie ich následkov,
   j) základné pokyny na bezpečné správanie sa zamestnancov a iných osôb nachádzajúcich sa v areáli organizácie v prípade závažnej priemyselnej havárie.
3. **Operatívnu časť – scenáre** reprezentatívnych druhov závažných priemyselných havárií a súbory scenárov pre jednotlivé reprezentatívne druhy závažných priemyselných havárií, ktoré môžu nastať ako následok aktivácie alebo nezvládnutia nebezpečenstva v organizácii, prípadne v jej okolí.

Grafická dokumentácia havarijného plánu tvorí spolu s písomnou časťou havarijného plánu ucelený súbor. Vyhotovenie a mierka grafickej časti dokumentácie havarijného plánu musí byť primeraná účelu, na ktorý má slúžiť, a musí byť prehľadná, stručná a zrozumiteľná.

Oboznamovanie s havarijným plánom

Prevádzkovateľ zabezpečí v potrebnom rozsahu oboznamovanie s havarijným plánom, prípadne s jeho príslušnými časťami a s aktualizáciou havarijného plánu:

a) všetkých osôb a služieb, ktorým havarijný plán ukladá určité povinnosti, s týmito povinnosťami; podľa potreby overí aj ich spôsobilosť na plnenie týchto povinností,
b) zamestnancov organizácie a zástupcov zamestnancov,
c) vedenia cudzieho podnikateľa, prípadne priamo jeho zamestnancov,
d) prevádzkovateľov susedných organizácií a verejnosť, ktorí by mohli byť dotknutí závažnou priemyselnou haváriou.

Precvičovanie havarijného plánu

Pravidelné precvičovanie jednotlivých situácií podľa havarijného plánu sa plánuje a uskutočňuje tak, aby sa na ňom zúčastnili všetci zamestnanci prevádzkovateľa, ktorých sa týka vrátane zamestnancov cudzieho podnikateľa. Precvičovanie sa uskutočňuje za účasti príslušných podnikových zložiek, ako sú závodný hasičský útvar, závodný hasičský zbor, záchranná služba, jednotka civilnej ochrany, strážna služba, závodná zdravotná služba, a podľa potreby aj za účasti orgánov verejnej správy a iných osôb, s ktorých súčinnosťou sa pri konkrétnom scenári v havarijnom pláne uvažuje.

Interval precvičovania, rozsah a náplň jednotlivých cvičení určí prevádzkovateľ najmä s prihliadnutím na zložitosť a rozsah organizácie, jej umiestnenie a závažnosť rizík. V oznámení plánovaného precvičovania havarijného plánu prevádzkovateľ uvedie termín konania cvičenia, jeho tematiku, čas trvania a subjekty, ktoré sa na ňom majú zúčastniť. Súčasťou dokumentácie havarijného plánovania je aj chronologický záznam o cvičení a rozbor cvičenia vrátane potrebných opatrení vyhotovený prevádzkovateľom.

Plán ochrany obyvateľstva

Plán ochrany obyvateľstva je podľa Zákona o civilnej ochrane obyvateľstva dokument, ktorý obsahuje úlohy, opatrenia a postupy na zabezpečenie ochrany obyvateľstva pre prípad vzniku mimoriadnej udalosti. V Pláne ochrany obyvateľstva sa uvádza **textová časť** a **grafická časť** na mapách v mierkach 1:1440, 1:2880, 1:5000, alebo 1:10000.

Obsahom textovej časti je obvykle:

a) účel plánu ochrany obyvateľstva, rozsah jeho platnosti,
b) závery analýzy územia z hľadiska vzniku možných mimoriadnych udalostí s únikom nebezpečných látok s uvedením následkov na postihnutom území,
c) zámer starostu obce pri realizácii opatrení na zabezpečenie ochrany obyvateľstva,
d) plán prípravy a nácvikov činnosti obce a jeho krízového štábu,
e) úlohy pri realizácii opatrení na zabezpečenie ochrany obyvateľstva:
    1. varovanie obyvateľstva a vyrozumenie osôb, organizácia informačného toku,
    2. monitorovanie územia,
    3. regulácia pohybu osôb a dopravných prostriedkov,
    4. prvá predlekárska pomoc a neodkladná zdravotná starostlivosť,
    5. evakuácia,
    6. hygienická očista,
    7. špeciálna očista terénu, budov a materiálu,
    8. príprava a informovanie obyvateľstva,
    9. individuálna ochrana osôb,
    10. ukrytie osôb,
    11. prehľad možností ohrozenia pre prípad mimoriadnej udalosti spojenej s únikom biologických nebezpečných látok,
f) úlohy pre materiálno – technické a finančné zabezpečenie realizácie prijatých opatrení,
g) metodika činnosti.

6.10.4 Bezpečnostný plán ochrany objektu

Na **ochranu utajovaných skutočností** sa spracováva **Bezpečnostný plán ochrany objektu**, ktorý má stanovenú štruktúru vo Vyhláške NBÚ č. 336/2004 Z. z.

Na **ochranu prvku kritickej infraštruktúry** sa podľa Zákona o kritickej infraštruktúre spracováva **Bezpečnostný plán**, ktorý obsahuje: *popis možných spôsobov narušenia alebo zničenia prvku, zraniteľné miesta prvku a bezpečnostné opatrenia na jeho ochranu.*

Na **ochranu objektov s inými aktívami**, ktoré je treba chrániť sa obvykle spracováva tiež **Bezpečnostný plán ochrany objektu**. Pri spracovaní tohto plánu sa vychádza zo štruktúry Bezpečnostného plánu ochrany objektu s utajovanými skutočnosťami. Spracováva sa po vykonaní procesu manažérstva rizika a nadväzuje na Plán zaobchádzania s rizikami daného objektu.

Bezpečnostný plán ochrany objektu s inými aktívami môže mať potom nasledujúci obsah:

1. **Opis objektu a chránených záujmov:**
   a) umiestnenie a opis objektu:
      - lokalita umiestnenia objektu: obec, mesto, intravilán, extravilán,
      - opis hranice objektu,
      - opis okolia objektu: prehľadnosť, kontrolovateľnosť, prístupové cesty, výskyt zdrojov rizika,
      - typ objektu: podľa určenia (účel, činnosti v objekte atď.), podľa vyhotovenia (stavebno-technické charakteristiky objektu),
      - vnútorné členenie objektu: počet budov alebo podlaží, ak sa objekt skladá z viacerých budov alebo z viacerých podlaží, zóny, opis zón v objekte (ak sú vytvorené).
   b) určenie chránených priestorov v objekte a chránených aktív,
   c) opis vstupov do objektu (brány, dvere, okná, iné priechodné otvory),
   d) zavedené bezpečnostné opatrenia na ochranu objektu a chránených priestorov.
2. **Závery z procesu manažérstva rizika:**
   - vybrané spôsoby zaobchádzania s rizikami na základe posúdenia možných variantov zaobchádzania s rizikami, ktoré vyžadujú zaobchádzanie (v prípade spracovania Plánu zaobchádzania s rizikom sa tento iba priloží),
   - zvyškové riziká.
3. **Implementácia bezpečnostných opatrení:**
   a) spôsob a postupnosť rozmiestnenia mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov.
   b) spôsob zabezpečenia fyzickej ochrany objektu a chránených priestorov (ak bude použitá), najmä:
      - zloženie strážnej jednotky,
      - forma výkonu ochrany,
      - oprávnenia strážnej jednotky (ktoré priestory kontroluje, kde vstupuje, ktoré priestory sú zakázané),
      - podriadenosť jednotky,
      - oprávnenia ku kontrole fyzickej ochrany (kto je oprávnený vykonávať kontrolu strážnej služby),
      - systém spojenia, resp. použitý technický systém kontroly strážnej služby a pod.

Grafická časť plánu sa vypracuje v rozsahu zodpovedajúcom charakteru objektu a zavedených bezpečnostných opatrení a môže obsahovať:

- hranice objektu a chránených priestorov,
- rozmiestnenie prvkov mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov,
- 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 signalizačných prvkov systému kontroly strážnej služby,
- rozmiestnenie prostriedkov protipožiarnej ochrany,
- rozmiestnenie stanovíšť strážnych psov (ak sú),
- 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.

Prevádzkový poriadok objektu

Podľa charakteru objektu (chránených priestorov) sa režimovej ochrany môže spracovať aj **Prevádzkový poriadok objektu** s obsahom:

- 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,
- podmienky pohybu osôb, dopravných prostriedkov v objekte a v chránenom priestore, a to v pracovnom čase a mimopracovnom čase,
- podmienky používania mobilných telefónov, videokamier, fotoaparátov, audiozáznamových zariadení a pod. (*ak je to potrebné*),
- podmienky a spôsob kontroly objektu a chráneného priestoru po opustení pracoviska zamestnancami,
- podmienky používania, prideľovania, označovania, úschovy a evidencie originálov a kópií bezpečnostných kľúčov a médií do zámkov a uzamykateľných systémov,
- podmienky používania, prideľovania, označovania, úschovy a evidencie kódových nastavení a hesiel používaných na prístup do objektov a chránených priestorov,
- podmienky manipulácie s mechanickými zábrannými prostriedkami a technickými zabezpečovacími prostriedkami a podmienky ich používania,
- postup pri narušení objektu a chráneného priestoru alebo pri pokuse o narušenie objektu a chráneného priestoru (*pokus alebo reálne vniknutie narušiteľa do objektu, narušenie verejného poriadku v blízkosti objektu alebo v objekte a pod.*), alebo pri vzniku nebezpečnej situácie (*oznámenie o uložení výbušného nástražného systému, prijatie nebezpečnej zásielky a pod.*),
- postup v prípade vzniku mimoriadnej situácie (*požiar, havária - plyn, voda, elektrické rozvody a pod.*), ktorých súčasťou je aj Plán na ochranu alebo evakuáciu osôb a majetku, spolu s uvedením zodpovedných osôb.

6.11 LITERATÚRA

Alarm security magazín 1/2006. ISSN 1335-504X.

BELAN, Ľ. – MIŠÍK, J. .[2014]: Štruktúra manažérstva rizika. In: Rozvoj Euroregiónu Beskydy VIII [elektronický zdroj] : medzinárodná vedecká konferencia : zborník : Žilina: Žilinská univerzita. ISBN 978-80-554-0966-5.

BELAN, Ľ. – MIŠÍK, J. .[2014]: Aplikácia zásady ALARP pri znižovaní úrovne rizika. In: Riešenie krízových situácií v špecifickom prostredí : medzinárodná vedecká konferencia. Žilina. Žilinská univerzita. ISBN 978-80-554-1021-0.

BELAN, Ľ. – MIŠÍK, J. .[2014]: Riziká v organizácii. In: Rozvoj Euroregiónu Beskydy VIII [elektronický zdroj]: medzinárodná vedecká konferencia : zborník : Žilina. Žilinská univerzita. ISBN 978-80-554-0965-8.

Príloha SL časť 2 (predtým ISO Guide 83 Zameranie noriem pre systémy manažérstva).

STN ISO 9001:2015 Systém manažérstva kvality.

STN ISO 31000:2011 Manažérstvo rizika. Zásady a návod.

7 INTEGROVANÝ MANAŽÉRSKY SYSTÉM

V súčasnosti v organizáciách dochádza k zvýšenému zavádzaniu rôznych systémov manažérstva zo sústavy medzinárodných noriem ISO. Tieto normy sú zamerané najmä do oblastí:

- kvality,
- bezpečnosti *(safety and security),*
- všeobecného manažmentu,
- zdravotníctva,
- životného prostredia a energie,
- priemyslu,
- služieb,
- informačných technológií.

Mnohé organizácie sa snažia o zavedenie a certifikáciu viacerých systémov manažérstva, napr. *systému manažérstva kvality, systému manažérstva bezpečnosti, manažérstva bezpečnosti* niektorých podsektorov bezpečnostného sektora, ako sú *BOZP, environmentálny, informačný či kontinuity činností* a pod.

Ľahké integrovanie a kombinovanie všetkých týchto systémov umožňuje zavedenie prílohy SL, ktorá určuje desať častí (etáp), ktoré musia byť pre všetky systémy manažérstva zhodné. Všetky súčasné a budúce systémy manažérstva podľa nej majú mať **rovnakú štruktúru, jadro textu a spoločné pojmy a definície,** čo umožní organizáciám ich ľahšiu **integráciu a vytvorenie integrovaného manažérskeho systému.**

Integrovaný manažérsky systém (*Integrated Management Systém, IMS)* je veľmi výhodným spôsobom vytvorenia celkového systému riadenia. Vychádza z vízie prieniku implementácie medzinárodných noriem týkajúcich sa manažérstva kvality, environmentálneho manažérstva, manažérstva bezpečnosti a ochrany zdravia pri práci a manažérstva informácií, kapitálu a aktív, do ktorého sú zahrnuté predovšetkým ich ochrana a bezpečnosť.

Hlavným aspektom i predpokladom integrácie je **systém manažérstva kvality**, na ktorý sú nadviazané ***ďalšie manažérske systémy*** založené na procesnom prístupe. **Procesný prístup** manažérskych podsystémov otvára ich schopnosť zlúčiť sa do jediného IMS.

Medzi dôvody na integráciu uvedených systémov manažérstva patria:

- lepšia orientácia v právnych požiadavkách a ich naplnení,
- zníženie administratívnej náročnosti,
- zníženie duplicity, a tým aj šetrenie finančných nákladov,
- zníženie rizík a zvýšenie zisku,
- rovnováha konfliktných záležitostí,
- vylúčenie konfliktných zodpovedností a vzťahov,
- zvýšenie podnikateľských cieľov,
- formalizácia informačného systému,
- harmonizácia a optimalizácia procedúr,
- zlepšenie komunikácie,
- možnosť zavedenia učiacej sa organizácie.

IMS je systém, ktorý organizácia používa na riadenie svojich procesov, aby dosiahla svoje ciele a spravodlivo uspokojila zainteresovaných účastníkov. IMS v sebe kombinuje všetky súvisiace zložky organizácie do jedného systému pre jednoduchšiu správu a prevádzku.

Nejde iba o spojenie samostatných systémov, ale skôr o **ich integrovanie do väzieb tak, že je možné podobné procesy plynule riadiť a vykonávať bez duplikácie**. Pritom je treba mať neustále na zreteli, že ***manažérske zásady*** uvedené v jednotlivých systémoch manažérstva sa neustále ***zbližujú a vyvíjajú***, preto je potrebné ich neustále sledovanie a zapracovávanie do praxe. Spoločnými prvkami pre všetky zložky IMS sú:

- zdroje (ľudia, zariadenia a vybavenie a pod.),
- procesy podľa jednotného postupu z prílohy SL.

Na základe podnikovej stratégie, definovanej politiky, cieľov a programov na ich dosahovanie, predstavuje IMS dobrovoľný nástroj uplatňovania efektívneho, jednotného, systémového a procesného manažmentu organizácií najmä v oblastiach:

- zvyšovania a neustáleho zlepšovania ***kvality*** vyrábaných výrobkov resp. poskytovaných služieb – **ISO 9001:2015 Systém manažérstva kvality**.
- dodržiavania ***bezpečnosti a ochrany zdravia pri práci*** – **OHSAS 18001:2009 Systém manažérstva BOZP – Požiadavky**, od októbra 2016 ju nahradí norma **ISO 45001:2016 Systémy manažérstva BOZP – Požiadavky.**
- komplexnej starostlivosti o ***životné prostredie,*** riadenia environmentálnych aspektov, minimalizovania environmentálnych vplyvov a zlepšovania environmentálneho správania a environmentálneho profilu – **ISO 14001:2005 Environmentálny manažérsky systém**, od septembra 2016 ju nahradí **ISO 14001:2016 Environmentálny manažérsky systém –. Požiadavky a návod.**
- ***informačnej bezpečnosti*** – **ISO 27001:2013 Systémy manažérstva informačnej bezpečnosti – Bezpečnostné techniky.**

Okrem uvedených systémov manažérstva je množstvo ďalších manažérskych systémov, uvedených na http://www.iso.org/iso/mss-list, ktoré môžu organizácie do svojho IMS postupne zaraďovať, najmä:

- **ISO 22301:2012 Systém manažérstva kontinuity činnosti – Požiadavky.**
- **ISO 22313:2012 Systém manažérstva kontinuity činnosti – Návod.**
- ISO 18788:2015 Systém manažérstva poskytovania služieb súkromnej bezpečnosti – Požiadavky a návod.
- ISO/AWI TS 18482 Systém manažérstva bezpečnosti – Návod – Posúdenie rizika podvodu a zneužitia.
- ISO/DIS 34001.3 Systém manažérstva bezpečnosti – Riadenie a prostriedky ochrany pred podvodmi.
- ISO 39001:2012 Systém manažérstva bezpečnosti cestnej premávky. Požiadavky a návod.
- ISO 22000:2006 Systém manažérstva bezpečnosti potravín – špecifikovanie *požiadaviek na manažment bezpečnosti potravín.*
- ISO 26000:2010 Manažérstvo spoločenskej zodpovednosti – *poradenstvo sociálnej zodpovednosti*.
- ISO 55000:2014 Manažérstvo aktív – Prehľad, zásady a terminológia.
- ISO 55001:2014 Manažérske systémy – Manažérstvo aktív – Požiadavky.
- ISO 55002:2014 Manažérske systémy – Manažérstvo aktív – Návod.
- ISO 41000 Integrovaný manažérsky systém – Facility manažment. Požiadavky a návod.
- ISO 50001:2011 Systém manažérstva energie – špecifikuje úlohy na *zriadenie, udržiavanie a zlepšovanie systému energetického manažmentu.*

7.1 SYSTÉM MANAŽÉRSTVA KVALITY

Najčastejším motívom zavádzania systému manažérstva kvality je požiadavka zákazníka – odberateľa alebo zadávateľa výberového konania. Zavedenie systému riadenia kvality prinesie zvýšenie efektivity riadenia, zlepšenie organizácie, zvýšenie morálky v spoločnosti a hlavne skvalitnenie výroby a uspokojovanie vašich zákazníkov – t. j. v konečnom dôsledku vyšší zisk a podiel na trhu.

Normy ISO pre manažérstvo kvality

- **ISO 9000** Systémy manažérstva kvality, Základy a slovník – poskytuje potrebné údaje pre správne pochopenie a uplatňovanie tejto medzinárodnej normy. Tieto zásady nie sú požiadavky samy o sebe, ale tvoria základ požiadaviek stanovených v tejto norme. Náčrt zásad manažérstva kvality je obsiahnutý v prílohe B.
- **STN EN ISO 9001:2009** – Systém manažérstva kvality – univerzálna norma, pokrýva všetky oblasti podnikania, od výrobných činnosti až po poskytovanie služieb. Vďaka tomu je vhodná pre každý typ organizácie. Definuje súbor pravidiel, požiadaviek a postupov na manažment podniku s cieľom zabezpečiť kvalitu výsledného produktu. Manažérstvo kvality sa zaoberá nielen procesmi výroby, vývojom a produktom samotným, ale siaha i do riadenia podniku a snaží sa o vyhodnocovanie vedenia či úspešnosti strategických rozhodnutí.
- **ISO 9004** Riadenie udržateľného úspechu organizácie – prístup k manažérstvu kvality – poskytuje návod pre organizácie, ktoré sa rozhodnú postupovať nad rámec požiadaviek tejto medzinárodnej normy osloviť širšie spektrum tém, ktoré môže viesť k neustálemu zlepšovaniu celkového výkonu organizácie ISO 9004 obsahuje metodiku sebahodnotenia pre organizáciu aby bola schopná zhodnotiť úroveň vyspelosti svojho systému riadenia kvality.

Medzinárodná norma EN ISO 9001:2015

Tento dokument navrhla technická komisia ISO / TC 176, *Manažment kvality a zabezpečenie kvality,* subkomisií SC2, *systémy kvality.* Toto piate vydanie normy ISO 9001 ruší a nahrádza ISO 9001:2008. Predstavuje technickú revíziu v porovnaní s predchádzajúcim vydaním, a to prostredníctvom prijatia revidovaného doložky pre prispôsobenie revidovaných „zásad manažérstva kvality“ a nových konceptov.

Prijatie systému manažérstva kvality by malo byť pre organizáciu strategickým rozhodnutím. Systém manažérstva kvality môže pomôcť organizácii zlepšiť jeho celkový výkon a tvorí neoddeliteľnú súčasť iniciatív trvalo udržateľného rozvoja.

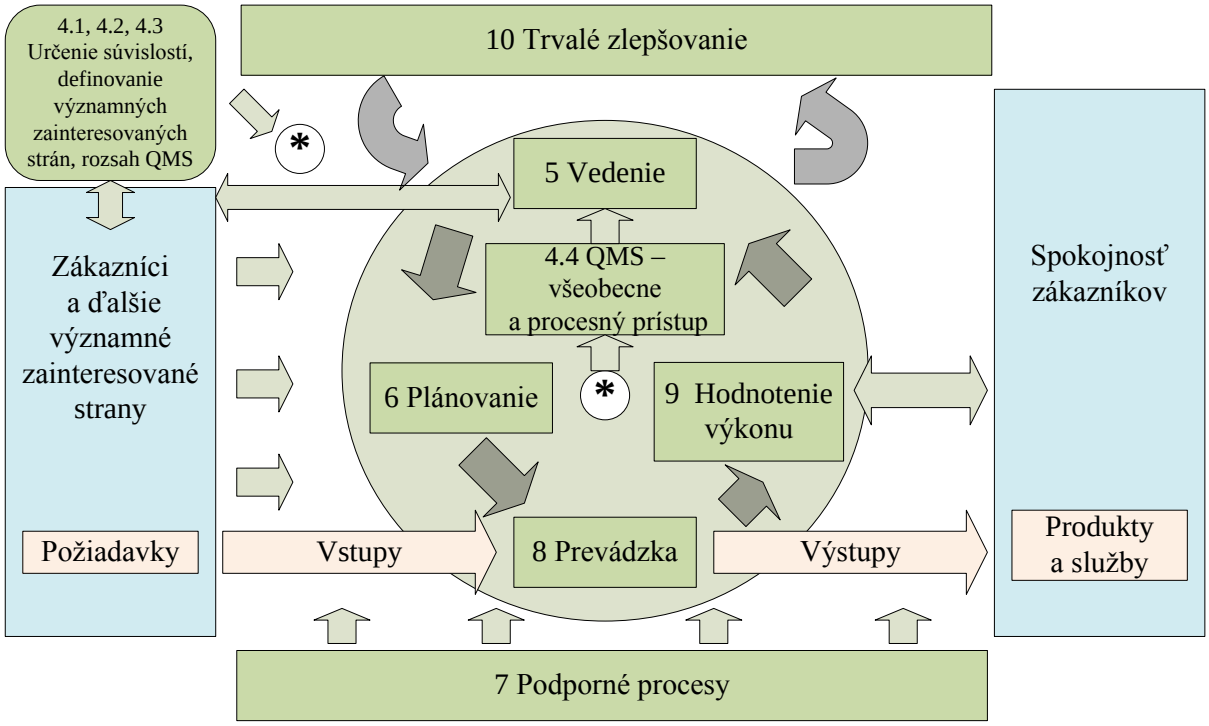
Súvislosti organizácie môžu zahŕňať vnútorné faktory, ako sú organizačná kultúra, a externé faktory, ako sú sociálno-ekonomické podmienky, za ktorých pôsobí; na základe toho všetky požiadavky tejto medzinárodnej normy sú všeobecné, ale spôsoby, v ktorých sú použité sa môžu líšiť od jedného organizácie do druhej.

Táto medzinárodná norma presadzuje prijatie procesného prístupu pri vývoji, uplatňovaní a zlepšovaní účinnosti systému manažérstva kvality, zvýšení spokojnosti zákazníkov tým, že spĺňa ich požiadavky. Procesný prístup platí pre systematickú definíciu a riadenie procesov a ich interakcie za účelom dosiahnutia plánovaných výsledkov v súlade s politikou kvality a strategickým riadením organizácie. Pri použití v rámci systému manažérstva kvality, procesný prístup zabezpečuje:

a) požiadavky na pochopenie organizácie a jej súvislostí,
b) zváženie procesov z hľadiska pridanej hodnoty,
c) dosiahnutie efektívnej výkonnosti procesov,

d) zlepšovanie procesov na základe vyhodnotenia údajov a informácií.

Obr. 18 ilustruje proces väzby medzi zložkami 4-10 tejto medzinárodnej normy. To ukazuje, že zákazníci hrajú významnú úlohu pri stanovení vstupných požiadaviek, ktoré organizácia potrebuje riešiť vo všetkých fázach svojho systému manažérstva kvality. Okrem toho, potreby a očakávania ďalších príslušne zainteresovaných účastníkov by mohli zohrať úlohu pri definovaní týchto požiadaviek. Monitorovanie uspokojenia zákazníka vyžaduje vyhodnocovanie informácií týkajúcich sa vnímania zákazníka o tom, či organizácia plní tieto požiadavky.



Obr. 18 Model procesu systému manažérstva kvality podľa ISO 9001:2015

Riadenie procesov a systému manažérstva ako celku možno dosiahnuť použitím modelu PDCA so zameraním na riziká a prevenciu nežiaducich výsledkov. Model môže byť stručne popísaný nasledujúcim spôsobom:

- **Plánovanie:** stanoviť ciele systému a jeho procesov a zdroje potrebné na dosiahnutie výsledkov v súlade s požiadavkami zákazníkov a politiky organizácie,
- **Vykonanie:** realizovať to, čo bolo naplánované.
- **Kontrola:** sledovať a (v prípade potreby) merať procesy a výsledné produkty a porovnať ich politikou, cieľmi a požiadavkami a podať správy o výsledkoch,
- **Činnosť:** prijať opatrenia na zlepšenie výkonnosti procesov, ak je to potrebné.

7.2 SYSTÉM MANAŽÉRSTVA BOZP

Neoddeliteľnou súčasťou integrovaného manažérskeho systému je manažérstvo bezpečnosti a ochrany zdravia pri práci, ktoré prispieva k naplneniu právnych a ďalších požiadaviek, minimalizácii rizík poškodenia zdravia zamestnancov a zlepšeniu pracovných podmienok. V SR je inštitúciou na propagovanie a presadzovanie zavádzania systémov riadenia BOZP v podnikoch **Národný inšpektorát práce**.

Systém manažérstva BOZP *(Health Safety Management System, HSMS)* je definovaný ako „časť systému manažérstva organizácie ktorý sa používa pri príprave a implementácií politiky BOZP a manažérstve jej rizík BOZP“.

Štruktúra a proces činnosti tohto systému sú podrobnejšie popísané v nasledovných právnych normách:

STN OHSAS 18001:2009 Systémy manažérstva bezpečnosti a ochrany zdravia pri práci. Požiadavky – norma série hodnotenia bezpečnosti a ochrany zdravia *(OHSAS – Occupational Health and Safety Assessment Series)* špecifikuje požiadavky na systém manažérstva bezpečnosti a ochrany zdravia pri práci (BOZP), aby uľahčila organizáciám riadiť vlastné riziká BOZP a zlepšiť vlastnú výkonnosť BOZP.

Norma umožňuje organizáciám vytvoriť **politiku BOZP**, určiť **ciele** a **procesy** na splnenie záväzkov politiky, ktoré ***zohľadnia právne požiadavky a informácie o rizikách*** BOZP. Môžu ju použiť organizácie ktoréhokoľvek typu a veľkosti v rozličných zemepisných, kultúrnych a sociálnych podmienkach. Úspech systému závisí od záväzku všetkých úrovní a funkcií organizácie, najmä vrcholového manažmentu.

Súhrnným cieľom noriem je prispieť a podporiť dobrú prax v BOZP, vrátane samoriadenia tak, aby bola v rovnováhe so sociálnoekonomickými potrebami. Treba poznamenať, že veľa požiadaviek sa môže určiť súbežne alebo sa môžu kedykoľvek revidovať. Normu OHSAS 18001 má v roku 2016 nahradiť norma ISO 45001.

STN OHSAS 18002:2009 Systémy manažérstva bezpečnosti a ochrany zdravia pri práci. Návod na implementáciu OHSAS 18001 – vznikla na základe ohlasu a požiadaviek používateľov preto, aby sa vytvorila konkrétna norma, podľa ktorej by sa posudzovali a certifikovali systémy manažérstva bezpečnosti a ochrany zdravia pri práci. Norma OHSAS 18002 cituje špecifické požiadavky z normy OHSAS 18001 s nasledujúcim relevantným návodom. Číslovanie kapitol normy OHSAS 18002 zodpovedá norme OHSAS 18001.

Norma OHSAS 18002, ktorá je určená na všeobecnú pomoc organizáciám pri tvorbe, zavádzaní alebo zlepšovaní systému manažérstva BOZP, poskytuje pokyny, vysvetľuje základné princípy, a opisuje účel, typické vstupy, procesy a typické výstupy pre každú požiadavku normy OHSAS 18001. Pomáha pochopiť a zaviesť normu OHSAS 18001.

Príručka „Systém riadenia BOZP – návod na zavedenie systému – pravidlá dobrej praxe BOZP“, vydaná Národným inšpektorátom práce v roku 2002 v sebe integruje zásady systému riadenia podľa príručky Medzinárodnej organizácii práce ILO-OSH 2001, medzinárodného štandardu OHSAS 18001 a jeho slovenskej verzie STN OHSAS 18001, britskej normy BS 8800 a ďalších slovenských právnych noriem týkajúcich sa problematiky BOZP.

7.2.1 Štruktúra Systému manažérstva BOZP

Štruktúra Systému manažérstva BOZP je často budovaná ako samostatná a nezávislá na bezpečnostnom manažérovi, v niektorých organizáciách je však bezpečnostnému manažérovi podriadená. V štruktúre je zastúpená ***bezpečnostnotechnická služba*** a ***pracovná zdravotná služba.***

Bezpečnostnotechnická služba

Bezpečnostnotechnická služba vytvára predpoklady na komplexnú starostlivosť o BOZP, napomáha zamestnávateľovi pri riadení BOZP. Zamestnávateľovi poskytuje ***poradenské služby*** v oblasti odborných, metodických, organizačných, kontrolných, koordinačných, vzdelávacích úloh a iných úloh pri ***zaisťovaní bezpečnosti a ochrany zdravia pri práci,*** najmä z hľadiska primeranosti pracovných priestorov a stavieb, pracovných procesov a pracovných postupov, pracovných prostriedkov a iných technických zariadení, pracovného prostredia a ich technického, organizačného a personálneho zabezpečenia.

Bezpečnostnotechnická služba primerane plní úlohy aj ***pracovnej zdravotnej služby*** a v záujme optimalizácie pracovných podmienok ovplyvňuje postoje zamestnávateľa, vedúcich zamestnancov a zamestnancov k bezpečnosti a ochrane zdravia pri práci. Úlohy bezpečnostno-technickej služby môže zamestnávateľ zabezpečiť aj **dodávateľským spôsobom.**

Úlohy bezpečnostnotechnickej služby podľa zákona č. 124/2006 Z. z. vykonáva:

- **bezpečnostný technik,**
- **autorizovaný bezpečnostný technik**
- podľa potreby aj **iný odborník na prevenciu a ochranu v špecifickej oblasti bezpečnosti a ochrany zdravia pri práci.**

Autorizovaný bezpečnostný technik je bezpečnostný technik podľa § 23 zákona, ktorý po absolvovaní najmenej dvoch rokov odbornej praxe bezpečnostného technika po získaní osvedčenia bezpečnostného technika úspešne vykonal skúšku pred skúšobnou komisiou vymenovanou Národným inšpektorátom práce.

Bezpečnostný technik

Úlohou **bezpečnostného technika** je dohliadať na integráciu BOZP v každom procese podnikateľského subjektu, jeho zaradenie z hľadiska funkcie býva do jednej z vyšších, resp. najvyššej hierarchickej úrovne organizácie. Povinnosti bezpečnostného technika možno rozdeliť do nasledovných kategórií:

- stroje, zariadenia a ich inštalácia, materiál a pod.,
- organizácia práce a pracovné postupy,
- dozor a kontrola pracovníkov BOZP,
- školenia BOZP,
- informácie,
- štatistiky,
- pracovné vzťahy a pod.,
- certifikácia systému manažérstva BOZP organizácie,
- spoluprácu so štátnymi orgánmi pri vyšetrovaní pracovných úrazov a spisovaní protokolov,
- sledovanie právnych zmien v oblasti BOZP,
- vedenie dokumentácie a evidencie o stave BOZP.

Bezpečnostný technik je na svojom úseku zodpovedný za:

- vykonávanie kontroly dodržiavania bezpečnostných predpisov a noriem na pracovisku,
- navrhovanie opatrení smerujúcich k odstráneniu zistených nedostatkov,
- tvorbu a aktualizáciu interných smerníc BOZP,
- realizáciu vstupných a priebežných školení zamestnancov v oblasti BOZP,
- vykonávanie kontrol, previerok a bezpečnostných auditov,
- vyšetrovanie pracovných úrazov,
- vedenie dokumentácie a evidencie o stave BOZP,
- hlásenie vykonaných opatrení nadriadenému.

Pracovná zdravotná služba

Pracovná zdravotná služba je definovaná v zákone o bezpečnosti a ochrane zdravia pri práci. Úlohy pracovnej zdravotnej služby plnia ***odborní zdravotnícki pracovníci kvalifikovaní na výkon pracovnej zdravotnej služby.***

Pracovná zdravotná služba u zamestnávateľa najmä:

- zisťuje nebezpečenstvá a hodnotí zdravotné riziká, ktoré ohrozujú zdravie zamestnancov pri práci,
- dohliada na faktory pracovného prostredia a na stav pracovných podmienok, ktoré môžu ovplyvňovať zdravie zamestnancov,
- podporuje prispôsobovanie práce zamestnancom,
- poskytuje poradenstvo zamestnávateľovi i zamestnancom, najmä pri plánovaní a organizácii práce a odpočinku vrátane usporiadania pracovísk a pracovných miest, ďalej pri technológiách a látkach, ktoré sa používajú pri práci a ktoré môžu ohroziť zdravie a taktiež pri ochrane a kladnom ovplyvňovaní zdravia, hygiene, fyziológii a psychológii práce, ergonómii vrátane prostriedkov individuálnej ochrany a kolektívnej ochrany,
- zúčastňuje sa na vypracúvaní programov ochrany a podpory zdravia zamestnancov, na zlepšovaní pracovných podmienok a na vyhodnocovaní nových zariadení a technológií zo zdravotného hľadiska,
- zúčastňuje sa na opatreniach pracovnej rehabilitácie, na rozboroch pracovnej neschopnosti, chorôb z povolania, ochorení súvisiacich s prácou a zdravotných rizík,
- podieľa sa na organizovaní systému prvej pomoci v prípade ohrozenia života alebo zdravia zamestnancov,
- školí zamestnancov na poskytovanie prvej pomoci, spolupracuje pri poskytovaní informácií, výcviku a výchove v oblasti ochrany a kladného ovplyvňovania zdravia, hygieny, fyziológie a psychológie práce a ergonómie,
- dohliada na zdravie zamestnancov v súvislosti s prácou.

Zástupca zamestnancov pre bezpečnosť

Zamestnávateľ je povinný vymenovať jedného zamestnanca alebo viacerých zamestnancov za zástupcov zamestnancov pre bezpečnosť, a to na základe návrhu príslušného odborového orgánu, zamestnaneckej rady alebo voľby zamestnancov, ak u zamestnávateľa nepôsobí odborový orgán alebo zamestnanecká rada. Zamestnanca možno navrhnúť alebo zvoliť za zástupcu zamestnancov pre bezpečnosť len s jeho písomným súhlasom.

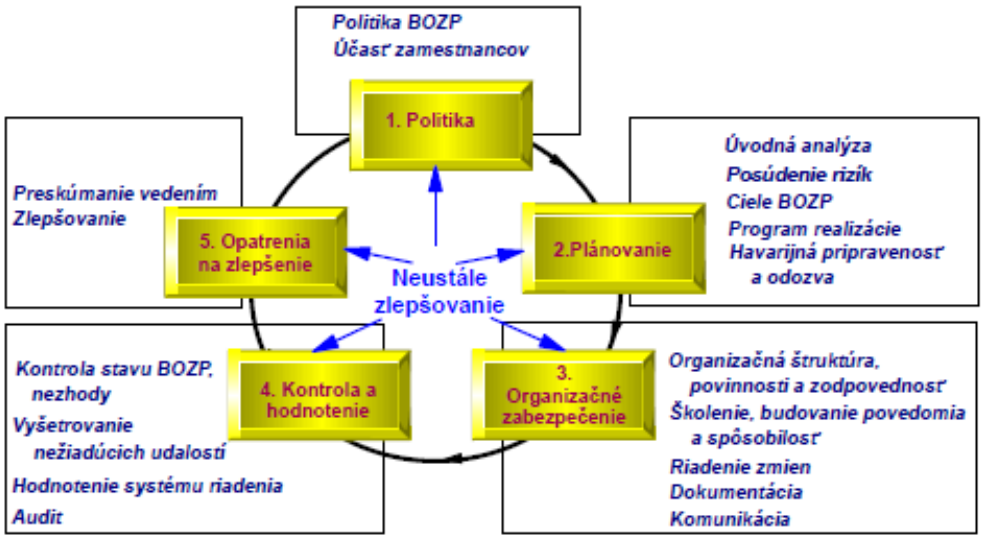
Jeden zástupca zamestnancov pre bezpečnosť u zamestnávateľa, ktorý vykonáva činnosti s vyšším rizikom, pri ktorých môže dôjsť k závažnému poškodeniu zdravia zamestnancov alebo pri ktorých častejšie dochádza k poškodeniu ich zdravia, môže zastupovať najviac 50 zamestnancov. U ostatných zamestnávateľov môže jeden zástupca zamestnancov pre bezpečnosť zastupovať viac ako 50 zamestnancov, ale nie viac ako 100 zamestnancov.

Komisia bezpečnosti a ochrany zdravia pri práci

Zamestnávateľ, ktorý zamestnáva viac ako 100 zamestnancov, zriadi ako svoj poradný orgán komisiu bezpečnosti a ochrany zdravia pri práci, ktorú tvoria zástupcovia zamestnancov pre bezpečnosť a zástupcovia zamestnávateľa, najmä odborníci v danom odbore, pričom nadpolovičnú väčšinu tvoria zástupcovia zamestnancov pre bezpečnosť. Zamestnávateľ je povinný sprístupniť na svojich pracoviskách na obvyklom a voľne prístupnom mieste zoznam zástupcov zamestnancov pre bezpečnosť spolu s uvedením pracoviska, na ktorom pracujú.

7.2.2 Proces manažérstva BOZP

Proces manažérstva BOZP je spracovaný v štruktúre Demingovho cyklu PDCA vo viacerých dokumentoch s miernymi odchýlkami (obr. 19).



Obr. 19 Proces manažérstva BOZP (zdroj Národný inšpektorát práce)

Politika BOZP

Politika BOZP stanovuje koncepciu organizácie v oblasti BOZP. Vrcholové vedenie s výkonnou zodpovednosťou musí stanoviť a schváliť politiku BOZP a zaviazať sa pre jej uplatňovanie v systéme manažérstva BOZP. S politikou BOZP musia byť zoznámení a súhlasiť s ňou všetci zamestnanci. Je to dokument, ktorý prezentuje základné ciele, zámery a stratégiu podniku v oblasti úrazovej prevencie, zlepšovania pracovných podmienok a pracovného prostredia. Politika BOZP:

a) má byť primeraná vzhľadom na povahu a rozsah rizík BOZP organizácie,
b) obsahuje záväzok na prevenciu úrazov a zhoršenia zdravotného stavu a neustále zlepšovanie riadenia a výkonnosti systému manažérstva BOZP,
c) obsahuje záväzok dosiahnuť minimálne zhodu s platnými právnymi predpismi a inými požiadavkami, ku ktorým sa organizácia zaviazala,
d) poskytuje štruktúru pre stanovenie a preskúmanie cieľov BOZP,
e) je zdokumentovaná, implementovaná a udržiavaná,
f) oboznamuje všetkých zamestnancov aby boli informovaní o svojich povinnostiach vo vzťahu k BOZP,
g) je k dispozícii zainteresovaným stranám,
h) pravidelne sa preskúmava, aby sa zabezpečilo, že je stále relevantná a vhodná pre organizáciu.

Účasť zamestnancov

Podľa § 10 Zákona č. 124/2006 Z. z. je zamestnávateľ povinný *umožniť zamestnancom alebo zástupcom zamestnancov pre BOZP zúčastňovať sa na riešení problematiky BOZP a vopred s nimi prerokúvať otázky, ktoré môžu podstatne ovplyvňovať BOZP.*

Zapájanie zamestnancov do otázok BOZP je kľúčovým prvkom systému riadenia BOZP u zamestnávateľa. Aj keď ***za BOZP zodpovedajú v mene zamestnávateľa vedúci zamestnanci***, nemôžu byť úplne úspešní bez aktívnej spolupráce so všetkými zamestnancami.

Zamestnávateľ musí zabezpečiť, aby boli ***všetky otázky týkajúce sa BOZP konzultované a prerokované so zamestnancami a ich zástupcami, aby boli informovaní a školení*** vo všetkých aspektoch BOZP, vrátane núdzových opatrení v súvislosti s ich pracovným zaradením.

Zamestnávateľ musí hrať aktívnu úlohu v podnecovaní a podporovaní spolupráce so zamestnancami, musí hľadať formy motivácie zamestnancov a zabezpečiť, aby zamestnanci a ich zástupcovia pre BOZP mali potrebný časový fond a zdroje umožňujúce ich aktívnu účasť v procese organizácie, plánovania a implementácie, hodnotenia a nápravných opatrení v rámci systému riadenia BOZP. Zamestnávateľ musí podľa potreby zabezpečiť ustanovenie a efektívne fungovanie ***komisie BOZP*** v súlade s celoštátnymi právnymi normami a štandardnými postupmi.

Plánovanie

1. **Úvodná analýza** – podľa potreby posúdiť a zhodnotiť existujúci systém riadenia BOZP organizácie vzhľadom na právne požiadavky a zámery v oblasti BOZP a neustáleho zlepšovania BOZP. V prípade, že neexistuje systém riadenia BOZP alebo ak ide o novovzniknutú organizáciu, úvodné posúdenie by malo slúžiť ako základňa pre zavedenie systému riadenia BOZP.
2. **Manažérstvo rizika** – organizácia je povinná zisťovať nebezpečenstvá a ohrozenia, posudzovať riziko a vypracovať písomný dokument o posudzovaní rizika pri všetkých činnostiach vykonávaných zamestnancami.
3. **Ciele** – pre úspešnú realizáciu politiky BOZP je nevyhnutné zabezpečiť, aby po úvodnej analýze boli na všetkých úrovniach organizácie stanovené ***reálne, merateľné a dosiahnuteľné ciele v oblasti BOZP.***
4. **Program realizácie** – organizácia má spracovať program realizácie podnikovej politiky BOZP, v ktorom stanoví **konkrétny plán úloh** na dosiahnutie stanovených cieľov, spôsob vykonania, kontroly a vyhodnotenia podnikovej stratégie a zámerov na zlepšenie jednotlivých oblastí BOZP.
5. **Havarijná pripravenosť** – Organizácia má **určiť postupy** pre prípad bezprostredného a vážneho ohrozenia života alebo zdravia a aktívne **zabezpečovať prostriedky** a zvládnutie havarijných stavov, mimoriadnych udalostí, nehôd, poškodení zdravia a úrazov.

Organizačné zabezpečenie

1. **Organizačná štruktúra, povinnosti a zodpovednosť** – pre dosiahnutie účinného riadenia BOZP je potrebné, aby bola stanovená jasná ***organizačná štruktúra*** zamestnávateľa. Pre zamestnancov, hlavne vedúcich zamestnancov, majú byť ***definované úlohy, zodpovednosti a právomoci v oblasti BOZP***. Súčasťou štruktúr sú aj ***externé odborné služby*** v tejto oblasti a zabezpečenie zodpovedajúcich zdrojov.
2. **Školenia, spôsobilosť, budovanie povedomia** – vzdelávanie a výcvik zamestnancov je základným princípom bezpečnostných opatrení. Preškolený a kompetentný zamestnanec, ktorý je dostatočne motivovaný dodržiavať zásady BOZP, je predpokladom pre úspešnosť podniku.
3. **Riadenie zmien/operatívne riadenie** – úspešnosť fungovania systému však nie je možná bez zvládnutia ***operatívneho riadenia a efektívneho riadenia zmien.***
4. **Dokumentácia** – dostatočná ***dokumentácia a jej pravidelná aktualizác*****ia** sú kľúčovými prvkami umožňujúcimi zamestnávateľovi zaviesť efektívny, úspešný a primerane zrozumiteľný systém riadenia BOZP.
5. **Komunikácia –** správna komunikácia zabezpečí, ***aby primerané informácie o BOZP boli v organizácii poskytnuté všetkým, ktorí ich potrebujú.***

Kontrola a hodnotenie

1. **Kontrola stavu BOZP** – cieľom kontroly stavu BOZP je ***zabezpečiť systematické vykonávanie predpísaných prehliadok, skúšok, revízií a meraní,*** aby bola sústavne kontrolovaná ***technická spôsobilosť strojov, zariadení, objektov, technológie a bezpečnosť pracovných činností***, aby bola tiež trvale zabezpečená ***kontrola zamestnancov pri dodržiavaní zásad BOZP.***
2. **Vyšetrovanie nežiaducich udalostí** – organizácie majú stanoviť efektívne postupy na ***zisťovanie príčin pracovných úrazov a iných nežiaducich udalostí*** a na systém prijímania opatrení proti opakovaniu sa podobných udalostí.
3. **Kontrola systému riadenia** – okrem klasickej kontroly dodržiavania predpisov a úrovne starostlivosti o BOZP je v systéme riadenia BOZP dôležité tiež zavedenie ***kontroly fungovania a výkonnosti jednotlivých prvkov riadenia.***
4. **Audit** – Audit systému manažérstva BOZP je ***proces, pomocou ktorého organizácie môžu preskúmať a kontinuálne vyhodnocovať efektívnosť svojho systému manažérstva BOZP.*** Vo všeobecnosti audity systému manažérstva BOZP musia brať do úvahy politiku a postupy BOZP, ako aj podmienky a prax na pracovisku.

Opatrenia na zlepšenie

1. **Preskúmavanie vedením** – vrcholový manažment (vedenie organizácie) by mal ***preskúmať činnosť systému riadenia BOZP***, aby overil, či je systém plne zavedený vo všetkých funkciách a činnostiach organizácie a či je naďalej zodpovedajúci na plnenie politiky a dosahovanie cieľov BOZP vyhlásených organizáciou.
2. **Zlepšovanie** – napĺňanie cieľov a zámerov, splnenie úloh a celého programu realizácie podnikovej politiky dáva priestor pre formulovanie nových cieľov na zlepšenie celkovej úrovne BOZP a formulovanie novej stratégie, politiky na kvalitatívne vyššej úrovni.

Posledný krok cyklu je základom na formulovanie nových cieľov podnikovej politiky BOZP na kvalitatívne vyššej úrovni a absolvovanie ďalšieho cyklu. V tom je princíp neustáleho zlepšovania. Zmyslom zavedenia systému riadenia je vykonanie jednotlivých prvkov. Pre systém manažovania BOZP boli vo svete spracované viaceré príručky a normy, ktoré poskytujú návod na zavedenie systému v podniku.

7.2.3 Nová norma pre Systémy manažérstva bezpečnosti a ochrany zdravia pri práci

ISO/CD 45001:2016 Occupational health and safety management systems – Requirements (Systémy manažérstva bezpečnosti a ochrany zdravia pri práci. Požiadavky) – bude využívať spoločne rovnakú štruktúru, definície a hlavný obsah so súčasnými upravenými normami, vychádzajúcimi z prílohy SL, ako sú normy, ktoré sa týkajú systémov manažérstva kvality, životného prostredia, informačnej bezpečnosti a kontinuity podnikateľských činností.

V štruktúre normy sú uvedené všetky časti podľa kap. 6.1. Odlišnosti sú v čiastkových bodoch v častiach 6, 7, 8 a 9 takto:

6 PLÁNOVANIE

6.1 Činnosti, ktoré sa zaoberajú rizikami a príležitosťami:

6.1.1 Všeobecne.

6.1.2 Identifikácia rizika.

6.1.3 Určenie právnych a iných požiadaviek.

6.1.4 Posúdenie rizika.

6.1.5 Plánovanie zmien.

6.1.6 Plánovanie vykonávania ďalších činností.

6.2 Ciele BOZP a plánovanie ich dosiahnutia.

7 PODPORA

7.1 Zdroje.
7.2 Kompetencie.
7.3 Povedomie.
7.4 Informácie, komunikácia, súčinnosť a poradenstvo..
7.5 Zdokumentované informácie.

8 PREVÁDZKA

8.1 Operatívne plánovanie a riadenie:
8.1.1 Všeobecne.
8.1.2 Postupnosť kontroly.
8.2 Manažment zmien.
8.3 Outsourcing.
8.4 Zásobovanie.
8.5 Dodávatelia.
8.2 Havarijná pripravenosť a reakcia.

9 HODNOTENIE VÝKONNOSTI

9.1 Monitorovanie, meranie, analýzy a vyhodnotenie:
9.1.1 Všeobecne.
9.1.2 Hodnotenie a zhoda.
9.2 Interný (vnútorný) audit:
9.2.1 Ciele interného auditu.
9.2.2 Procs interného auditu.
9.3 Preskúmanie manažmentom.

Celkové **zameranie štandardu zostáva rovnaké** s OHSAS 18001, obsahuje však aj niektoré vývojové trendy, príbuzné s novými pravidlami pre vyvíjajúce sa medzinárodné štandardy systému manažérstva. Napríklad, je v nich teraz oveľa väčšie zameranie na súvislosti organizácie, rovnako ako významnejšia úloha pre vrcholový manažment a vedenie.

ISO 45001 trvá na tom, že tieto aspekty BOZP majú byť **začlenené do celkového systému riadenia organizácie** a vyžadujú oveľa **silnejšie zapojenie od jej vedenia**. To bude veľká zmena pre užívateľov, ktorí môžu v súčasnej dobe preniesť zodpovednosť na bezpečnostného manažéra, skôr, ako tieto úlohy začleniť úplne do prevádzky organizácie.

Zavedenie normy prinesie nasledujúce zmeny:

- väčšia flexibilita dokumentu organizácie a štruktúra systému manažérstva BOZP,
- zavedenie pojmu zdokumentované informácie namiesto zdokumentované postupy a záznamy,
- preventívne činnosti už nie sú zahrnuté, celý štandard znamená prevenciu,
- nové zameranie na Súvislosti organizácie,
- pochopenie inetrných a externých problémov,
- zahrnutie zainteresovaných účastníkov,
- strategický prístup k manažérstvu BOZP,
- väčší dôraz na spojenie manažérskych činností v BOZP,
- väčšia zodpovednosť a zdôraznenie významu vrcholového manažmentu,
- väčší dôraz na koncepciu manažérstva rizika,
- právne a iné požiadavky sú viac jednoznačné,
- väčší dôraz na dosiahnutie zhody,
- väčší dôraz na postupné kontroly,
- špecifické zahrnutrie manažmentu zmien,
- väčšie zameranie na sprostredkovanie a outsourcig.

7.3 ENVIRONMENTÁLNY MANAŽÉRSKY SYSTÉM

Medzinárodná organizácia pre normy ISO zostavila v roku 1991 Strategickú poradnú skupinu pre ochranu životného prostredia. Nadväzne na Podnikateľskú chartu trvale udržateľného rozvoja, vydanú Medzinárodnou obchodnou komorou (1991), a Deklaráciu Konferencie Spojených národov o životnom prostredí a rozvoji, konanej v Rio de Janeiro v roku 1992. Skupina pre ochranu životného prostredia definovala potreby vývoja štandardizácie v oblasti ochrany životného prostredia. Súbežne vznikali na národných úrovniach, hlavne v Európe, národné normy, z ktorých britská norma BS 7750:1992 sa postupne stala základom pre certifikáciu EMS v mnohých štátoch Európy.

V rokoch 1993/1994 bola vytvorená samostatná technická komisia ISO/TC 207 pre environmentálne manažérstvo, ktorej úlohou je postupné riešenie a vydávanie medzinárodných technických noriem životného prostredia do noriem radu **ISO 14000** pod skupinovým názvom **Environmentálne manažérstvo.**

V SR bola v decembri 1996 ustanovená pri Slovenskom ústave technickej normalizácie technická normalizačná komisia TK č. 72 s názvom Environmentálne manažérstvo. V priebehu roku 1997 bolo riešených prvých päť noriem radu ISO 14000. Po konečnom schválení Úradom pre normalizáciu, metrológiu a skúšobníctvo, ktoré sa uskutočnilo začiatkom roku 1998, boli zaradené do sústavy STN.

Z hľadiska najprepracovanejších nástrojov vyznačujúcich sa vysokou efektívnosťou sa v súčasnosti pri budovaní a implementovaní EMS odporúča použitie dvoch štandardizovaných nástrojov:

1. **EMS – Systém environmentálneho manažérstva**
   - **STN EN ISO 14001 – Systémy environmentálneho manažérstva. Špecifikácia s návodom na použitie –** základná medzinárodná technická norma špecifikujúca požiadavky na EMS. Nie je pre organizácie záväzná a bola vytvorená tak, aby bola použiteľná v organizáciách akéhokoľvek typu a veľkosti a aby zohľadňovala rôzne geografické, kultúrne a sociálne podmienky. Splnením predpísaných požiadaviek, ktorých zhodu s normou preverí úspešný certifikačný audit, organizácia získa od certifikačnej spoločnosti certifikát, ktorý je zároveň aj dokladom o účinnosti systému.

2. **EMAS – Systém environmentálne orientovaného riadenia a auditu**
   - **Nariadenie Európskeho parlamentu a Rady č. 1221/2009 o dobrovoľnej účasti organizácií v schéme Spoločenstva pre environmentálne manažérstvo a audit EMAS** ***(Environmental Management and Audit Scheme)*** **–** najdôveryhodnejší a najsilnejší nástroj environmentálneho manažérstva na trhu, ktorý pridáva prvky k požiadavkám medzinárodnej normy pre systém environmentálneho manažérstva EN ISO 14001:2004 čím napomáha organizáciám dosahovať kontinuálne zlepšovanie ich environmentálneho správania. Po splnení všetkých požiadaviek nariadenia EPaR č. 1221/2009 a kladnom posúdení žiadosti predloženej príslušnému orgánu pre EMAS je organizácia registrovaná v schéme EMAS a zapísaná do národného a európskeho registra EMAS (Zákon č. 468/2002 Z. z. o systéme environmentálne orientovaného riadenia).

Kým EMS systému ISO ustanoveného v rámci noriem radu 14000 sú globálne najrozšírenejším systémom, systém EMAS je európskou normou implementovanou v rámci politiky životného prostredia EÚ a jej členských štátoch. V SR je najrozšírenejším EMS systém ISO a podiel certifikácie EMAS je v rámci SR zanedbateľný. Rozdiel medzi systémom ISO a systémom EMAS spočíva v tom, že kým ISO je medzinárodnou normou, EMAS je vymedzený právnym predpisom – príslušným nariadením EÚ č. 761/2001 ES.

Implementácia oboch systémov môže mať pre organizácie v strednodobom časovom horizonte významný prínos. Je však náročná a kladie vysoké nároky na administratívu a informovanosť zamestnancov. Preto spravidla organizácie uprednostňujú jeden z uvedených systémov.

Dôvodmi, pre ktoré organizácie v SR uprednostňujú EMS v rámci ISO pred EMAS sú:

- menšia náročnosť na implementáciu a zavedenie tohto systému,
- menej finančne nákladný ako systém EMAS,
- je rozšírenejší a jeho platnosť je globálne rozšírená, čo uľahčuje spoluprácu v širšom priestore, na širšom medzinárodnom trhu,
- nižšie nároky na informačné zabezpečenie.

Komplexný prístup k environmentálnemu manažérstvu, keď je dôraz kladený na ***zníženie dopadov na životné prostredie*** a ***zvýšenie celkovej úrovne kvality vo všetkých etapách výrobne – spracovateľského cyklu na všetkých úrovniach riadenia***, sa nazýva **Komplexné environmentálne manažérstvo kvality** (KEMK).

KEMK je dôležitým prístupom pre implementáciu stratégie dlhodobej udržateľnosti pôsobenia MSP *(Managed service provider – poskytovateľ manažérskych služieb na diaľku)* v súlade so stratégiami ochrany životného prostredia. Pre implementáciu KEMK sú dôležité nasledujúce faktory:

- dôležitým faktorom pre zvýšenie konkurencieschopnosti organizácie sa stávajú ***environmentálne vlastnosti výrobkov a služieb,***
- zabezpečenie konkurencieschopnosti v dlhodobom časovom horizonte bude podmienený ***rozvojom čistejšej produkcie a zavádzaním inovatívnych technológií, s nižšími dopadmi na životné prostredie,***
- ***kultúra a informovanosť verejnosti organizáciou*** speje k nárastu predaja čistejšej produkcie pri zachovaní jej kvality, nárast tejto produkcie je podmienený preferenciami zákazníkov.

V súčasnosti sú z oblasti EMS spracované a začlenené do našej sústavy tieto technické normy:

- STN EN ISO 14001:2005 *Systémy environmentálneho manažérstva. Špecifikácia s návodom na používanie.*
- STN EN ISO 14004:2005/Z1 *Systémy environmentálneho manažérstva. Všeobecné pokyny obsahujúce zásady, systémy a podporné techniky* – je zameraná na systém environmentálneho manažérstva a všeobecné pokyny a techniky na jeho implementáciu, poskytuje návod na vytvorenie, zavedenie, udržiavanie a zlepšovanie systému environmentálneho manažérstva a jeho koordináciu s ďalšími systémami riadenia.
- STN ISO 14005:2012 (83 9005), *Systémy environmentálneho manažérstva. Pokyny na fázovú implementáciu systému environmentálneho manažérstva vrátane použitia hodnotenia environmentálneho správania* – ustanovuje pokyny pre postupné zavádzanie systému ekologického manažmentu, vrátane využívania hodnotenia ekologickosti.
- STN ISO 14006 je určená na použitie v tých organizáciách, ktoré zaviedli EMS podľa ISO 14001 a zároveň napomáha pri integrácii pravidiel a požiadaviek na ekodizajn harmonizovane v súčinnosti s inými systémami riadenia.
- STN ISO 14010-14019 Pokyny pre environmentálny audit.
- STN ISO 14015 Environmentálne posudzovanie miest a organizácií.
- STN EN ISO 14020 – 14029 Environmentálne značky a vyhlásenia. Všeobecné zásady.
- STN EN ISO 14031 Environmentálne manažérstvo. Hodnotenie environmentálneho správania.

- ISO 14040 (14040 až 14049), Environmentálne manažérstvo. Posudzovanie životného cyklu.
- ISO 14050 Environmentálne manažérstvo. Slovník.
- a množstvo ďalších noriem.

Environmentálny manažérsky systém EMS je súčasťou systému celkového riadenia organizácií, ako aj súčasťou KEMK. EMS zriadené a zavedené v súlade so systémom noriem ISO radu 14000 zohľadňujú a zahŕňajú komplexnú organizačnú štruktúru organizácií a aj jednotlivé činnosti a aktivity v celku.

EMS podľa normy ISO 14001 umožňuje organizáciám zavedenie nasledovných postupov a opatrení:
- riadiť, koordinovať a projektovať výrobu a spracovanie výrobkov s nižšími dopadmi na životné prostredie pri znížení produkcie odpadov, efektivity recyklácie a efektívne nakladanie so zdrojmi a so vstupmi výroby,
- monitorovať celý cyklus výroby a spracovania výrobkov a poskytovania služieb a hodnotiť produkty a ich dopady na životné prostredie na základe merateľných a overiteľných indikátorov,
- vytvárať predpoklady pre objektívne preskúmanie možností zavedenia EMS a certifikácie v rámci ISO 14001,
- napomáhať organizáciám pri implementácii ďalších príbuzných technických noriem a systémov.

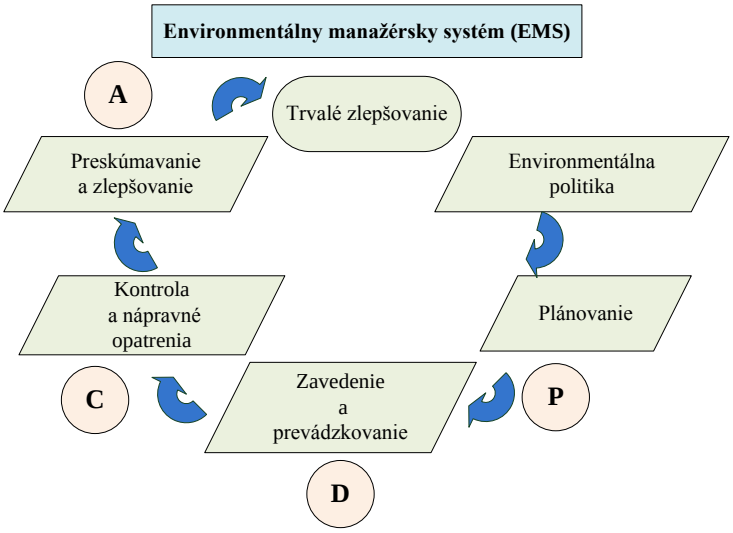
Norma ISO 14001 nešpecifikuje univerzálne úroveň ochrany životného prostredia, pretože tá sa v jednotlivých organizáciách líši a je špecifická pre každú výrobnú alebo obchodnú činnosť, čo často predpokladá zavedenie doplňujúcich systémov a nástrojov súvisiacich s normou ISO 14001. Preto ISO obsahuje ďalšie technické normy týkajúce sa špecifických otázok životného prostredia.

Zámerom ISO 14001 je poskytnúť rámec pre komplexný a strategický prístup pre environmentálnu politiku organizácie, jej plánovanie a rozvoj činností. ISO 14001 tvorí všeobecné požiadavky na systém environmentálneho manažérstva, ktorého filozofiou je vytvorenie jednotného referenčného rámca pre komunikáciu o otázkach ochrany životného prostredia medzi organizáciami a ich zákazníkmi, regulačnými a kontrolnými orgánmi, verejnosťou a ďalšími zainteresovanými účastníkmi.

Rozsah využitia EMS v rámci ISO 14001 závisí od faktorov, ako je environmentálna politika organizácie, povaha jej činností, výrobkov a služieb, pravidlá a miesto kde a za akých podmienok funguje. ISO 14001 špecifikuje požiadavky, ktoré musí EMS spĺňať. Splnenie týchto požiadaviek je podmienené existenciou objektívnych dôkazov, ktoré môžu byť preukázané v rámci nezávislého overenia alebo auditu. Je potrebné preukázať, že systém environmentálneho manažmentu je vedený v súlade s normou ISO. ISO 14001 je možné využiť aj na dosahovanie interných cieľov organizácie.

STN EN ISO 14001:2005 bude platiť len do 31.8.2016, kedy ho nahradí ISO 14001:2016 spracovaný už podľa prílohy SL.

Realizácia EMS v organizácii sa uskutočňuje podľa metodiky PDCA (Demingov cyklus) a možno ju rozložiť do nasledujúcich etáp (obr. 20):



Obr. 20 PDCA cyklus EMS

Zavádzanie EMS

Podstatou zavádzania systému environmentálneho manažérstva v organizácii je postupné vnášanie environmentálnych hľadísk do jej riadiaceho systému na všetkých jeho úrovniach. Pod pojmom organizácie sa pritom rozumie spoločnosť, združenie, firma, podnik, úrad alebo inštitúcia, poprípade ich časť, alebo kombinácia, nech sú zapísané v registri alebo nie, nech sú verejné alebo súkromné, ktoré však majú vlastné funkcie a správu. Oba u nás používané systémy, t. j. ISO 14001 a EMAS majú po revízii EMAS zhodné nároky na vlastný systém riadenia .

Pri zavádzaní EMS sa organizácia riadi týmito zásadami:

- Zaviazať sa k realizácii EMS a definovať svoju environmentálnu politiku.
- Formulovať plán plnenia stanovenej environmentálnej politiky.
- Zaviesť mechanizmy potrebné pre realizáciu environmentálnej politiky.
- Merať, monitorovať a vyhodnocovať svoje správanie k životnému prostrediu, čiže sledovať zmeny svojho environmentálneho profilu.
- Preverovať svoj systém environmentálneho manažmentu za účelom jeho neustáleho zlepšovania.

Prehľad najvýznamnejších zmien zavedením ISO 14001:2016

Termíny a definície. Návrh definuje 33 bežne používaných pojmov namiesto súčasných 20 pojmov normy ISO 14001:2005. Okrem novej terminológie sa menia niektoré súčasné pojmy, čím sa získa iný dôraz a zlepší zrozumiteľnosť. Niektoré nové pojmy zahŕňajú napr. *analýzu životného cyklu, ukazovatele, systém riadenia* sa stáva *systémom environmentálneho manažérstva*.

Pochopenie organizácie a jej súvislostí a **Pochopenie potrieb a očakávania zainteresovaných účastníkov** budú vyžadovať od organizácie identifikovanie problémov a požiadaviek, ktoré môžu mať vplyv na rozsah systému riadenia ochrany životného prostredia. Chápanie a zistené závery by potom mali byť použité pre priamu revíziu systému environmentálneho manažérstva.

Vedenie. Úspech systému environmentálneho manažérstva, alebo akéhokoľvek manažérskeho systému, závisí na odhodlaní vedenia organizácie. Vrcholový manažment je definovaný ako „osoba alebo skupina ľudí, ktorí riadia a kontrolujú organizáciu na najvyššej úrovni.“ K štandardným mandátom musí vrcholový manažment prevziať vedúcu úlohu pri začle-

ňovaní praktík environmentálneho manažmentu do hlavnej stratégie, procesov, a priorít ich organizácie.

Zmeny v požiadavkách pre politiku životného prostredia zahŕňajú nový záväzok povinností týkajúcich sa právnych a iných požiadaviek. Organizácie sú naďalej požadované, aby sa zapojili do „neustáleho zlepšovania" systému. Zásadnou zmenou je, že organizácia by mala byť odhodlaná na „ochranu životného prostredia, vrátane prevencie znečistenia a ďalšie špecifiká v rámci systému".

Prístup založený na riziku. Súčasťou prístupu založeného na posudzovaní rizika zahŕňa určenie významných aspektov a identifikáciu, vrátane príslušných opatrení a dodržiavanie predpisov v rámci systému. Obe tieto činnosti sú podobné predchádzajúcim požiadavkám, ale väčší dôraz je kladený na organizáciu, ktorá určuje svoj vlastný profil rizika. Prístup na základe rizík vyžaduje myslenie na základe rizík a na základe posúdenia rizika, preventívne opatrenia v priebehu vývoja, implementáciu, údržbu a zlepšovanie systému environmentálneho manažérstva.

Podporné procesy. Kompetencie osôb, ktoré môžu mať vplyv na výkonnosť systému manažérstva životného prostredia boli doplnené časťami Povedomie a Komunikácia. Zatiaľ čo tieto klauzuly boli predtým zoskupené pod rovnakými doložkami v ISO 14001:2004, požiadavky sa výrazne nemenia. Podobným spôsobom, boli zdroje a dokumentácia prevzaté z Roly, zodpovednosti a zdroje, dokumentácia a riadenie dokumentov a sú úzko modelované na zmeny už v STN EN ISO 9001:2008.

Prevádzka zahŕňa kontrolu alebo vplyv procesov a služieb spojených s významnými environmentálnymi aspektmi, organizačnými rizikami, a životným cyklom a núdzovou pripravenosťou v „Plánovaní a riadení prevádzky". Plánovanie a riadenie prevádzky predstavuje podstatne odlišné koncepty. „Perspektíva životného cyklu" musí byť požadovaná v oblasti verejného obstarávania organizácie produktov a služieb. Iné úvahy platia pri navrhovaní procesov výroby a služieb.

Hodnotenie výkonu. Použitie kritérií indikátorov výkonnosti a výrazu stav životného prostredia bol predstavený v spojení s definíciou výkonu. Stav životného prostredia je popísaný ako „stav alebo charakteristiky životného prostredia, stanovené v určitom okamihu", s ktorým by mali byť všetci oboznámení.

Preventívna činnosť. Návrh normy neobsahuje špecifické požiadavky pre preventívnu činnosť, pretože jedným z kľúčových účelov Systému manažérstva je pôsobiť ako preventívny nástroj. Na základe toho norma požaduje: „Posúdenie vonkajších a vnútorných záležitostí organizácie, ktoré sú relevantné pre jej účel, a ktoré ovplyvňujú jej schopnosť dosiahnuť zamýšľaný výsledok(y)."

Pojmy **dokument a záznam** nahrádza v celom návrhu termín „zdokumentované informácie." Potreba zdokumentovaných postupov nie je identifikovaná.

Jedným z očakávaných prínosov prijatia štruktúry spoločného systému manažérstva bude
uľahčenie organizáciám implementovať niekoľko systémov riadenia do harmonizovanej, štruktúry účinným spôsobom. To by im malo umožniť zamerať svoju pozornosť na porozumenie, plánovanie a prevádzku ich podnikateľských procesov. Správne navrhnutý a implementovaný systém manažérstva by mal poskytnúť dostatok objektívnych dôkazov o zhode s príslušnými normami, ako aj zodpovedajúce regulačné a zákaznícke požiadavky, na ktoré sa táto organizácia zaviazala.

7.4 SYSTÉM MANAŽÉRSTVA INFORMAČNEJ BEZPEČNOSTI

Úrad pre normalizáciu, metrológiu a skúšobníctvo SR vydal pre systémy manažérstva informačnej bezpečnosti (SMIB) Slovenské technické normy:

- **STN ISO/IEC 27001:2014** (36 9789), Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Požiadavky – táto norma **obsahuje** slovenskú verziu normy ISO/IEC 27001:2013 a **ruší a nahrádza** normu STN ISO/IEC 27001 (36 9789) Informačné technológie: zabezpečovacie techniky: systémy manažérstva informačnej bezpečnosti: požiadavky z októbra 2006 v celom rozsahu.
- **STN ISO/IEC 27000:2014** (36 9789), Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Prehľad a slovník – táto norma **obsahuje** slovenskú verziu normy ISO/IEC 27000: 2012
- **STN ISO/IEC 27002:2014** (36 9784), Informačné technológie. Bezpečnostné metódy. Pravidlá dobrej praxe riadenia informačnej bezpečnosti – táto norma **obsahuje** slovenskú verziu normy ISO/IEC 27002:2013 a **nahrádza** STN ISO/IEC 27002 (36 9787) Informačné technológie: zabezpečovacie techniky: pravidlá dobrej praxe manažérstva informačnej bezpečnosti z októbra 2006 v celom rozsahu.

Základná medzinárodná norma STN ISO/IEC 27001:2014 špecifikuje požiadavky na vytvorenie, zavedenie, údržbu a stále zlepšovanie SMIB v organizácii. Obsahuje aj požiadavky na posúdenie a zaobchádzanie s rizikami informačnej bezpečnosti prispôsobené potrebám organizácie. Požiadavky vymedzené v tejto medzinárodnej norme sú všeobecné a sú určené pre všetky organizácie bez rozdielu typu, veľkosti alebo pôvodu.

SMIB zachováva dôvernosť, integritu a dostupnosť informácií aplikovaním procesu manažérstva rizika a dáva istotu zainteresovaným stranám, že riziká sú primerane riadené. Je súčasťou procesov a celkovej štruktúry riadenia organizácie a je do nich integrovaný. Bezpečnosť informácií sa zvažuje pri návrhu procesov, informačných systémov a opatrení, očakáva sa, že zavedenie SMIB bude nastavené v súlade s potrebami organizácie.

Organizácia zavedením SMIB do svojej štruktúry získa množstvo výhod, napr.

- certifikáciou SMIB sa zvyšuje imidž a osobná prestíž organizácie na trhu, u zákazníkov, dodávateľov, odberateľov a širokej verejnosti, čo prospieva jej dlhodobej stabilite a prosperite,
- SMIB poskytuje zrýchľovanie rastu konkurenčnej schopnosti organizácie a napomáha odstráneniu prístupových bariér k svetovým aj domácim trhom,
- zvýšenie produktivity činnosti pozitívnou efektivitou motivácie, vzdelanosti, monitoringu, kontroly a sankcií o zníženie počtu a následkov rizík a z nich vyplývajúcich incidentov, čím sa redukujú náklady na chyby,
- optimalizácia a zefektívnenie plánovania investícií do IS a IT.

Obsah normy ISO / IEC 27001: 2014

Norma umožňuje, vďaka tomu, že stanovuje jednoznačné požiadavky na systém riadenia, kontrolu zavedenia SMIB a prípadnú certifikáciu, teda nezávislé overenie SMIB tretím (dôveryhodným a akreditovaným) subjektom.

V štruktúre normy sú uvedené všetky časti podľa kap. 6.1. Odlišnosti sú v čiastkových bodoch v častiach 6, a 8 takto:

6. PLÁNOVANIE

6.1 Činnosti, ktoré sa zaoberajú rizikami a príležitosťami.

6.1.1 Všeobecne.

6.1.2 Posúdenie rizika informačnej bezpečnosti.

6.1.3 Zaobchádzanie s rizikami informačnej bezpečnosti.
6.2 Ciele informačnej bezpečnosti a plánovanie ich dosiahnutia.

8 PREVÁDZKA
8.1 Operatívne plánovanie a riadenie.
8.2 Posudzovanie rizík informačnej bezpečnosti.
8.3 Zobchádzanie s rizikami informačnej bezpečnosti.

Najnovší štandard, ISO / IEC 27001: 2014 prináša niektoré zmeny, napr.:

- zrejme najzjavnejšia zmena oproti je **nové usporiadanie dokumentu**, ktoré odráža snahu ISO implementovať v budúcnosti univerzálnu šablónu pre všetky nové normy, cieľom je dosiahnuť kompatibilitu noriem, ktoré sa zaoberajú rôznymi systémami manažérstva (napr. ISO 9001, ISO 14 001, ISO 20000 a pod.).
- **odlišný spôsob stanovenia rozsahu implementácie SMIB**, kým v pôvodnej verzii bolo postačujúce stanoviť hranice procesu a opísať výnimky, nové znenie kladie väčší dôraz na **súvislosti**, teda ***rozsah implementácie navrhuje určiť sprostredkovane, pomocou určenia bezpečnostných cieľov a identifikácie očakávaní všetkých zainteresovaných účastníkov.***
- nové požiadavky na posudzovanie rizík – **prepojenie na normu STN ISO 31000,** ktorá poskytuje zásady a všeobecný návod na manažérstvo rizika:
  - princíp vlastníka aktíva je nahradený princípom ***vlastníka rizika,*** t. j. pre každé identifikované riziko treba určiť, ***kto bude zodpovedný za zaobchádzanie s ním,***
  - odstraňuje sa povinná ***identifikácia hrozieb a zraniteľností aktív*** ako predpoklad pre ***identifikáciu rizika.***
- nezdôrazňuje Demingov cyklus PDCA, užívateľ SMIB môže okrem neho voľne ***použiť akýkoľvek proces manažérstva (zlepšenia)***, ako napr. 6 SIGMA DMAIC.
- kým vo verzii 2005 norma určovala zoznam a názvy jednotlivých dokumentov, nová verzia určuje ***už len obsahovú stránku dokumentácie a zavádza pojem dokumentovaná informácia,*** určenie ***rozsahu a štruktúry dokumentácie je už úlohou a právom organizácie v úmysle zabezpečiť efektivitu SMIB,***
- revidovaný štandard bol napísaný s použitím **novej štruktúry** na vysokej úrovni, ktorá je ***spoločná pre všetky nové normy pre systémy riadenia*** – to umožní, aby ich integrácia bola jednoduchá pri realizácii viac než jedného systému riadenia,
- rozdiely v ***terminológii a niektoré definície*** boli odstránené alebo premiestnené,
- požiadavky na **záväzky vedenia** sú zamerané na **„vedenie“,**
- **preventívne opatrenia** boli nahradené **„opatreniami na riešenie rizík a príležitostí“,**
- požiadavky na **Prehlásenie o aplikovateľnosti SOA** sú podobné, viac je jasné, že je potrebné ***stanoviť kontroly v procese zaobchádzania s rizikom***,
- **kontroly** uvedené v prílohe A (opatrenia na zaobchádzanie s rizikom) boli upravené tak, aby odstránili duplicity a majú viac logické zoskupenie,
- **špecifické kontroly** boli pridané pre kryptografiu a bezpečnosť v dodávateľských vzťahoch,
- väčší dôraz je kladený na **stanovenie cieľov, monitorovanie výkonu a metriky.**

Medzi hlavné aspekty tejto časti normy, ktoré pokrýva, patria:

- harmonizácia s normami manažérstva pre ďalšie systémy riadenia,
- kontinuálne zabezpečenie procesu zlepšovania manažérstva bezpečnosti informácií,
- celopodnikové riadenie,
- zabezpečenie súladu s právnymi a regulačnými predpismi,
- záruky za bezpečnosť informácií,
- zavedenie princípov OECD pre oblasť bezpečnosti informačných systémov a sietí.

7.5 SYSTÉM MANAŽÉRSTVA KONTINUITY ČINNOSTÍ

Kontinuita činností zahŕňa voľne definovaný súbor plánovacích, prípravných a príbuzných činností, ktoré majú zaistiť, aby rozhodujúce podnikateľské funkcie organizácie mohli pokračovať vo svojej činnosti, napriek vážnym incidentom alebo haváriám, ktoré by niektoré činnosti mohli prerušiť, alebo budú obnovené do prevádzkového stavu v rozumne krátkom čase.

Kontinuita činností prispieva ku zvýšeniu odolnosti spoločnosti. Širšie spoločenstvo a dopad spoločenstva, v ktorom sa organizácia nachádza, na túto organizáciu môže vytvoriť potrebu zapojiť do procesov obnovy ďalšie organizácie.

Kontinuita činností zahŕňa tri kľúčové prvky:

1. **Odolnosť:** rozhodujúce podnikateľské funkcie a podporná infraštruktúra sú navrhnuté a vyrobené takým spôsobom, aby ich väčšina porúch nemohla ovplyvniť, napríklad použitím nadbytkov a voľnej kapacity.
2. **Obnova:** budú prijaté opatrenia na opätovné nadobudnutie alebo obnovu rozhodujúcich a menej rozhodujúcich podnikateľských funkcií, ktoré z nejakého dôvodu zlyhali.
3. **Pohotovosť:** organizácia zaistí všeobecnú schopnosť a pripravenosť účinne sa vyrovnať s výskytom akéhokoľvek veľkého incidentu a haváriou, vrátane tých, ktoré neboli, a ani možno nemohli byť predvídané. Príprava na nepredvídanú výnimočnú situáciu predstavuje poslednú inštanciu odpovede v prípade, že opatrenia odolnosti a obnovy sa ukázali v praxi ako nedostatočné.

Pokiaľ nie je realizovaný Plán kontinuity činností, príslušná organizácia čelí pomerne vážnemu ohrozenie alebo narušeniu, ktoré môže viesť k narušeniu realizácie a výsledkov.

Manažérstvo kontinuity činností prevažne patrí do oblasti manažérstva rizika, s niektorými súvisiacimi oblasťami, ako sú zákony, informačná bezpečnosť a zhoda predpisov. Riziko je hlavným hľadiskom odkedy sa kontinuita činností týka podnikových funkcií, prevádzky, zásob, systémov, vzťahov atď., ktoré sú kriticky dôležité pre dosiahnutie prevádzkových cieľov organizácie. Analýza dopadom činností je všeobecne prijímaná ako termín pre manažérstvo rizika pre proces určenia relatívnej dôležitosti alebo kritickosti týchto prvkov a naopak, riadi priority, plánovanie, prípravu a ďalšie aktivity manažérstva kontinuity činností.

Na manažérstvo kontinuity činností sa v organizácii vytvára **Systém manažérstva kontinuity činností**, *(Business continuity management system, BCMS)*. BCMS kladie dôraz na:

- pochopenie potrieb organizácie a nutnosti vytvorenia politiky a cieľov manažérstva kontinuity činností,
- zavedenie kontroly funkčnosti a opatrení pre celkové riadenie schopnosti organizácie zvládať rušivé incidenty,
- monitorovanie a preskúmavanie výkonnosti a efektívnosti BCMS,
- trvalé zlepšovanie založené na objektívnom meraní.

BCMS je charakterizovaný v týchto právnych normách:

- **ISO 22301:2012 Spoločenská bezpečnosť – Systémy manažérstva kontinuity činnosti – Požiadavky** – špecifikuje požiadavky pre plánovanie, vytvorenie, zavedenie, prevádzkovanie, monitorovanie, hodnotenie, udržiavanie a neustále zlepšovanie zavedeného Systému manažérstva kontinuity činností na ochranu pred incidentmi a haváriami, zníženie pravdepodobnosti ich výskytu, prípravu reakcie a obnovu činnosti po ich ničivom pôsobení. Požiadavky uvedené v tejto norme sú všeobecné, môžu byť uplatnené pre všetky organizácie

alebo ich časti, bez ohľadu na druh, veľkosť a charakter. Rozsah uplatňovania týchto požiadaviek závisí na prevádzkových podmienkach a zložitosti organizácie.

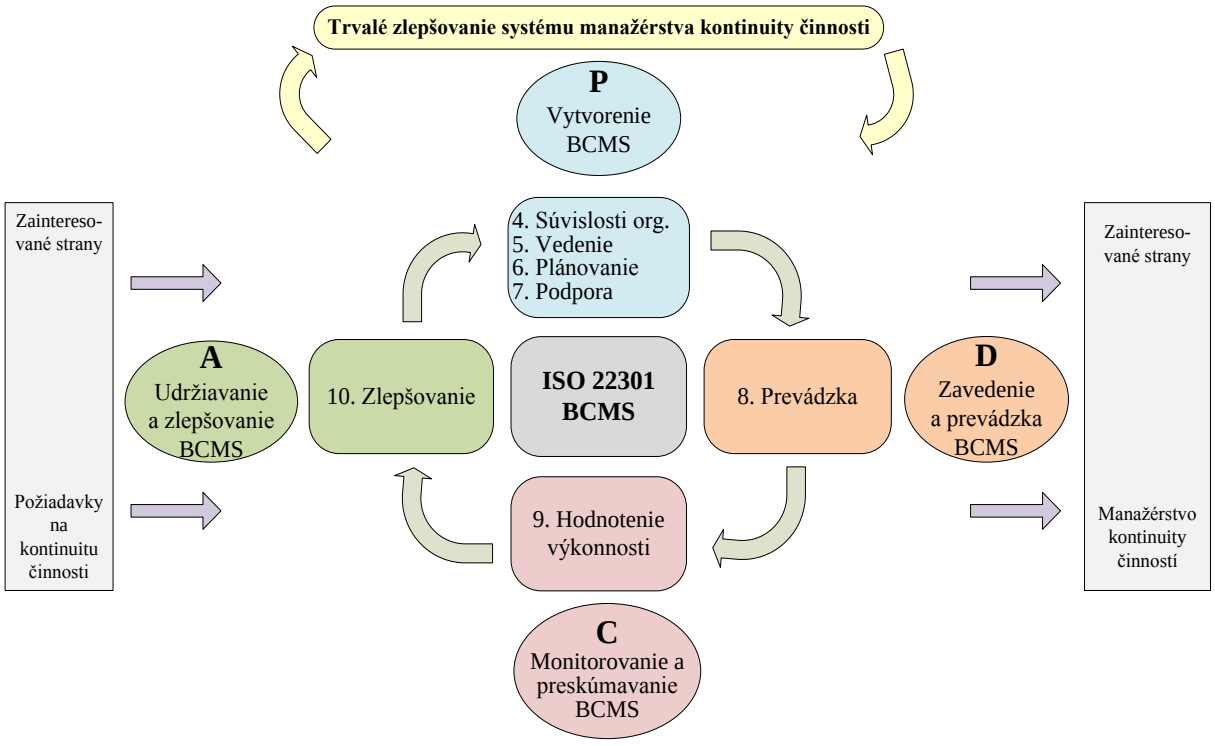
- **ISO 22313:2012 Spoločenská bezpečnosť – Systémy manažérstva kontinuity činnosti – Návod** – poskytuje návod, pokiaľ je to vhodné, na základe požiadaviek stanovených v ISO 22301:2012 a poskytuje odporúčania (mal by) a oprávnenia (môže) vo vzťahu k nim. Zámerom tejto medzinárodnej normy nie je poskytnúť pokyny o všetkých aspektoch kontinuity činností.
- **ISO/IEC 27031:2011 Informačná bezpečnosť – Bezpečnostné techniky – Smernice pre prípravu informačných a komunikačných technológií [IKT] na zabezpečenie kontinuity činností** – popisuje spôsoby a zásady pripravenosti IKT pre kontinuitu činností a poskytuje sústavu metód a procesov na identifikáciu a špecifikáciu všetkých aspektov (napr. kritéria vykonania, schéma a zavedenie), pre zlepšovanie pripravenosti IKT na kontinuitu činností organizácie.

7.5.1 Norma STN EN ISO 22301:2012

ISO 22301 sa vzťahuje na všetky typy a veľkosti organizácií, ktoré si želajú:

- vytvoriť, zaviesť, udržiavať a zlepšovať svoj BCMS,
- zaistiť zhodu s politikou kontinuity činností organizácie,
- preukázanie zhody s ostatnými,
- usilovať o certifikáciu / registráciu svojho BCMS akreditovaným certifikačným orgánom tretej strany alebo
- z vlastného rozhodnutia vydať prehlásenie o zhode s touto medzinárodnou normou.

Táto medzinárodná norma využíva model PDCA na plánovanie vytvorenie, zavedenie, prevádzku, monitorovanie, preskúmavanie, udržiavanie a trvalé zlepšovanie efektívnosti BCMS v organizáciách (obr. 21).



Obr. 21 PDCA model aplikovaný na procesy BCMS

Obr. 21 ilustruje ako BCMS prijíma ako vstupy zainteresovaných účastníkov a požiadavky na manažérstvo kontinuity, a ako prostredníctvom nevyhnutných činností a procesov vytvára výstupy kontinuity (riadenú kontinuitu činností), ktorá tieto požiadavky spĺňa.

7.5.2 Obsah modelu PDCA

Súvislosti organizácie

Určenie vonkajších a vnútorných problémov, ktoré sa týkajú účelu organizácie a ktoré ovplyvňujú jej schopnosť dosiahnuť očakávané výstupy svojho BCMS, ako sú:

- činnosť organizácie, funkcie, služby, produkty, partnerstvo, dodávateľské reťazce, vzťahy so zainteresovanými účastníkmi, a potenciálny dosah nezhôd medzi politikou kontinuity činností, cieľmi organizácie a inými politikami, vrátane celkovej stratégie manažérstva rizika,
- snaha organizácie o manažérstvo rizika,
- potreby a očakávania príslušných zainteresovaných účastníkov;
- príslušné právne, regulačné a ďalšie požiadavky, ku ktorým sa organizácia zaviazala.

Pri stanovení rozsahu BCMS sa berú do úvahy strategické ciele organizácie, hlavné produkty a služby, kritériá rizika a všetky usmernenia, zmluvy alebo záväzky so zainteresovanými účastníkmi.

Vedenie

Vrcholový manažment musí preukázať trvalý záväzok k BCMS. Svojím vedením a jednaním môže manažment vytvoriť prostredie, v ktorom sú plne zapojené rôzne subjekty, a v ktorom môže systém manažérstva účinne fungovať v synergii s cieľmi organizácie. Vrcholový manažment zodpovedá za:

- zaistenie kompatibility BCMS so strategickým riadením organizácie,
- začlenenie požiadaviek BCMS do podnikateľských procesov organizácie,
- poskytnutie potrebných zdrojov pre BCMS,
- oznamovanie významu efektívneho manažérstva kontinuity činností,
- zabezpečenie, že BCMS dosiahne svoje očakávané výsledky,
- usmerňovať a podporovať neustále zlepšovanie,
- stanoviť a oznámiť politiku kontinuity činností,
- zabezpečenie stanovenie cieľov a plánov BCMS,
- zabezpečenie, že zodpovednosti a právomoci pre príslušné role sú priradené.

Významným faktorom pri implementácii BCMS je vymenovanie **osoby zodpovednej za dohľad a riadenie programu BCM** (napr. BC manažér, BC koordinátor, BC analytik, BC konzultant). Celkovú zodpovednosť (BC manažér) sa odporúča prideliť členovi vrcholového manažmentu, čo zaručí, že programu sa bude venovať patričná pozornosť a adekvátna podpora. V malých organizáciách zodpovednosť za riadenie incidentov, manažment kontinuity a manažment obnovy činností podniku môže mať jedna osoba.

Tímy pre BCMS

Väčšie organizácie môžu využiť rôzne fóra (napr. BCM manažérske fórum) a pracovné tímy:

a) Tím výkonného manažmentu (*Executive Management Team*) – rozhoduje hlavne o politike a stratégii BCM, zabezpečuje komunikáciu na úrovni predstavenstva a kontakt s externými organizáciami (napr. médiá, orgány štátnej správy), autorizuje vyvolanie plá-

nov kontinuity činností a plánov obnovy činností a autorizuje rozpočet na riešenie incidentu.

b) Tím manažérstva incidentov v podnikateľských činnostiach (*Incident Management Team*) je zodpovedný hlavne za zaistenie bezpečnosti všetkých zamestnancov, posúdenie škody, vyšetrovanie incidentov a za podporu tímov obnovy. Tímy manažérstva incidentov sa využívajú *len v prípade vyšetrovania bezpečnostného incidentu*. Členovia tímu musia byť skúsení pracovníci v oblasti bezpečnosti a musia byť zastúpené všetky oblasti bezpečnosti.

c) Tímy obnovy majú za úlohu obnovu činností, IKT a zariadení podniku podľa plánov BCM, zabezpečenie vhodných zdrojov na poskytnutie bezpečného a efektívneho pracovného prostredia a preskúmanie, plánovanie a zavedenie opatrení pre návrat do pôvodného stavu v organizácii. Obvykle sa vytvárajú:
- Tímy obnovy infraštruktúry *(Infrastructure Recovery Teams),*
- Tímy obnovy činností *(Business Recovery Teams).*

V niektorých prípadoch môžu byť tieto tímy podporované **ďalšími tímami** so zodpovednosťou napríklad za ***komunikáciu s médiami*** alebo za ***personálne záležitosti***. V prípade akéhokoľvek incidentu by mali existovať **rýchlo účelovo zostaviteľné skupiny zamestnancov** (BCM tímy), ktoré zabezpečia, aby podnik mal potvrdený rozsah a charakter incidentu, prevzal kontrolu nad situáciou, potlačil incident a komunikoval so zainteresovanými účastníkmi.

Úlohy tímov BCMS

Medzi základné úlohy tímu výkonného manažmentu patrí:

a) vyhodnocovať informácie od vedúceho, resp. zástupcu vedúceho IMT, ktorý informuje o situácii po incidente a na základe nich rozhodnúť o zvolaní EMT,
b) zabezpečiť komunikáciu s IMT,
c) spolu s IMT rozhodnúť, či má byť vyvolaný havarijný stav, alebo sú potrebné dodatočné informácie,
d) evidovať záznamy o všetkých kľúčových udalostiach a činnostiach, ktoré sa udiali počas havarijného stavu,
e) počas havarijného stavu udržiavať pravidelnú výmenu aktuálnych informácií s IMT ohľadom kľúčových faktorov:
   - stav personálu: zranenia a problémy s personálom,
   - situácia stavieb: poškodenie, odhadovaná výdrž,
   - služby: ktoré služby sú zasiahnuté,
   - komunikácia: účinky na verejnosť a tlač,
f) kontrola podnikových priorít:
   - časové špecifiká krízovej situácie (napr. mesiac/štvrťrok/koniec roka) a ich následok na priority,
   - súčasné hlavné riešené projekty,
g) potvrdiť stratégiu BCM s IMT,
h) dohodnúť aké informácie môžu byť zverejnené v médiách:
   - komunikovať s vedúcim tímu podnikovej komunikácie,
   - identifikovať hovorcu/hovorcov,
i) autorizovať hlavné výdavky nezahrnuté do rozpočtu, ako napríklad:
   - dočasný prenájom kancelárskych priestorov,
   - neplánované nákupy vybavenia.

Medzi základné úlohy tímu manažmentu incidentov patrí:

a) komunikácia s prvotným kontaktným bodom (napr. helpdesk, bezpečnostná služba, poverení zamestnanci),
b) posúdenie incidentu a jeho dopadov na organizáciu,
c) odporúčanie vyhlásenia havarijného stavu tímu výkonného manažmentu,
d) spolupráca s tímami obnovy, potvrdzovať požiadavky zdrojov potrebných počas špecifických období v rámci fungovania BCM plánov,
e) udržiavanie záznamu o tímových aktivitách/výdavkoch,
f) koordinácia činností:
   - komunikácia so záchrannými službami – spojiť sa so záchrannými službami, zabezpečiť koordináciu medzi IMT a záchrannými službami, spojiť sa s tímami obnovy za účelom prístupu k budovám,
   - zabezpečenie zamestnancov – sledovať zdravotný stav zamestnancov, venovať starostlivosť všetkým, ktorý boli postihnutí incidentom, prípadne ich rodinám, zabezpečenie personálu počas havarijného stavu,
   - presun na alternatívne pracovisko – aktivovanie alternatívneho pracoviska, vydanie inštrukcií na presun, zabezpečenie stravy a dopravy atď.
   - riadenie a komunikácia – zabezpečenie komunikácie medzi členmi tímu manažérstva incidentov a tímami obnovy, zabezpečenie komunikácie so zamestnancami, dodávateľmi, poisťovňami, právnymi zástupcami, majiteľom budovy a médiami (napr. zriadenie horúcej linky),
   - informovanie príslušných tímov o rozsahu škôd na IKT a pravdepodobných časoch obnovy, iniciovanie SLA a riadenie dodávateľov IKT,
   - ochrana aktív a ich záchrana – koordinácia záchranných služieb pri identifikácií a ochrane cenných aktív počas incidentu, vytvorenie inventáru aktív vrátane ich stavu poškodenia a umiestnenia, spolupráca so správcom financií ohľadom vyplácania poistného, zabezpečenie fyzickej ochrany majetku – ochrana perimetra, kontrola vstupu, zabránenie rozkrádania majetku,
   - finančná kontrola – evidovanie všetkých nákladov spojených s incidentom a obnovou,
   - médiá a public relations – kontaktovanie médií, pripraviť krátke a stručné vyhlásenie pre médiá,
   - administratívna podpora.

Plánovanie

Táto rozhodujúce etapa sa týka vytvorenia strategických cieľov a hlavných zásad pre BCMS ako celok. Ciele BCMS sú vyjadrením zámeru organizácie na zaobchádzanie so zistenými rizikami alebo podrobenie sa požiadavkám potrieb organizácie.

Ciele kontinuity činností musia:

- byť v súlade s politikou kontinuity činností,
- brať do úvahy minimálnu úroveň produktov a služieb, ktoré sú pre organizáciu prijateľné na dosiahnutie svojich cieľov,
- merateľné;
- zohľadňovať príslušné požiadavky;
- byť sledované a podľa potreby aktualizované.

Vyššie uvedené tímy a zamestnanci by mali mať vypracované plány a postupy na riadenie incidentov a taktiež plány aktivácie, výkonu, koordinácie a komunikácie o odozve na incident, preto jednotlivci poverení implementáciou BCM do podniku by mali vytvoriť a aktualizovať dokumenty kontinuity činností podniku:

a) Politiku BCM,
b) Analýzu dopadov činností *(Business Impact Analysis),*
c) Plán manažérstva rizika,
d) Plán zaobchádzania s rizikami,
e) Stratégiu BCM,
f) Plány manažérstva incidentov *(Incident Management Plan),*
g) Plány kontinuity činností *(Business Continuity Plan),*
h) Plány obnovy činností *(Business Recovery Plan),*
i) Plán obnovy po havárii *(Disaster Recovery Plan),*
j) Dohody o úrovni poskytovaných služieb *(Service-level agreement, SLA),*
k) Programy pripravenosti *(Awareness Programme),*
l) Programy školení alebo výcviku,
m) Rozvrhy a záznamy o testovaní.

Plán kontinuity činností – zdokumentovaný súbor postupov a informácií, ktoré sú vytvorené a udržiavané na účel ich použitia v prípade vzniku incidentu/havárie na to, aby organizácia naďalej plnila svoje kritické činnosti na prijateľnej, vopred definovanej úrovni.

Plán obnovy po havárii – obsahuje všetky technické a organizačné úlohy potrebné na prevádzku procesov v mieste prevádzky (záložnom mieste) v prípade havárie (katastrofy). Je to podrobný plán akcií, ktoré sa musia vykonať na obnovu všetkých kritických systémov, služieb a zariadení.

Podpora

Každodenný manažérsky efektívny systém manažérstva kontinuity činností spolieha na použitie vhodných zdrojov pre každú úlohu. Medzi ne patrí kvalifikovaný personál s príslušným a preukázateľným školením, podporné služby, uvedomenie a komunikácia. To musí byť podporované vhodne spravovanými dokumentovanými informáciami. Interná i externá komunikácia organizácie sa v tejto oblasti musí brať do úvahy, vrátane formátu, obsahu a správneho načasovania tejto komunikácie. V tomto bode sú uvedené aj požiadavky na zriadenie, aktualizáciu a kontrolu zdokumentovaných informácií.

Prevádzka

Po plánovaní vytvorenia BCMS, musí organizácia tento systém zaviesť do prevádzky. Táto etapa zahŕňa:

a) Analýzu dopadov činností: Táto činnosť umožňuje organizácii identifikovať rozhodujúce procesy, ktoré podporujú jej rozhodujúce produkty a služby, vzájomné vzťahy medzi procesmi a zdroje potrebné na prevádzku procesov minimálne na prijateľnej úrovni.

b) Manažérstvo rizika: ISO 22301 na vykonanie tohto procesu sa odkazuje na normu ISO 31000. Cieľom tejto požiadavky je vytvoriť, zaviesť a udržiavať formálne zdokumentovaný proces posúdenia rizika, v ktorom systematicky identifikuje, analyzuje a vyhodnocuje riziko rušivých incidentov v organizácii.

c) Stratégiu kontinuity činností: Potom, čo požiadavky boli stanovené s využitím BIA a posúdenia rizika, môžu byť vyvinuté stratégie na identifikáciu opatrení, ktoré umožnia organizácii chrániť a obnoviť rozhodujúce činnosti, založené na tolerovaní rizika organizáciou v rámci definovaných cieľov času obnovy. Skúsenosti a osvedčené postupy jasne ukazujú, že včasné vytvorenie stratégie BCM organizácie zabezpečí usporiadané činnosti BCM v súlade s podporou celkovej podnikateľskej stratégie organizácie. Stratégia kontinuity činností môže byť integrálnou súčasťou celkovej podnikateľskej stratégie organizácie.

d) Postupy na zabezpečenie kontinuity činností: Organizácia musí zdokumentovať postupy (vrátane potrebných opatrení) na zaistenie kontinuity činností a manažérstvo rušivých incidentov. Postupy musia:

- zaviesť vhodné protokoly internej a externej komunikácie,
- byť konkrétne, pokiaľ ide o bezprostredné kroky, ktoré majú byť prijaté počas narušenia,
- byť pružné, aby reagovali na nepredvídané riziká a zmeny vnútorných a vonkajších podmienok,
- zamerať sa na dopad udalostí, ktoré by mohli narušiť činnosti,
- byť vypracované na základe uvedených predpokladov a analýzy vzájomných závislostí,
- byť účinné pri minimalizácii následkov prostredníctvom realizácie vhodných zmierňujúcich stratégií.

e) Cvičenia a preskúšanie: zabezpečiť, aby postupy na zabezpečenie kontinuity činností boli v súlade s cieľmi zabezpečenia kontinuity jej podnikania, čo organizácia musí testovať pravidelne. Cvičenia a testovanie sú procesy overovania plánov a postupov kontinuity činností, na to, aby sa zaistili stratégie schopné poskytnúť výslednú reakciu a obnovu v lehotách odsúhlasených vedením.

Hodnotenie výkonnosti

Po implementácii BCMS vyžaduje ISO 22301 trvalé monitorovanie systému, rovnako ako pravidelné hodnotenie pre zlepšenie jeho fungovania:

- sledovanie, do akej miery sú splnené všeobecné a špecifické ciele politiky kontinuity činností organizácie,
- meranie výkonnosti procesov, postupov a funkcií, ktoré chránia svoje prioritné činnosti,
- monitorovanie zhody s touto normou a cieľmi kontinuity činností,
- sledovanie historických dôkazov o nedostatočnej výkonnosti BCMS vykonávaním interných auditov v stanovených intervaloch,
- vyhodnocovanie uvedeného preskúmaním vedením v plánovaných intervaloch.

Zlepšovanie

Trvalé zlepšovanie môže byť definované ako všetky opatrenia prijímané v celej organizácii na zvýšenie účinnosti (dosiahnutie cieľov) a efektivity (pomer optimálne náklady / prínos) bezpečnostných procesov a kontroly, ktoré majú priniesť zvýšený prínos pre organizáciu a jej zainteresovaných účastníkov. Organizácia môže neustále zlepšovať efektivitu systému manažmentu využitím politiky kontinuity činností, cieľov, výsledkov auditov, analýz sledovaných udalostí, nápravných a preventívnych opatrení a manažérskym preskúmaním.

7.6 LITERATÚRA

HRUBEC, J. a kol. [2009]: *Integrovaný manažérsky systém.* Nitra. SPU. ISBN 978-80-552-0231-0.

KOLLÁR, V. – BROKEŠ, P. [2005]: *Environmentálny manažment.* Bratislava : Sprint, 2005. 327 s. ISBN 80-89085-37-7.

Národný inšpektorát práce [2002]: *Systém riadenia bezpečnosti a ochrany zdravia pri práci.* Bratislava.

SOCHA, Ľ. [2010]: *Manažérske systémy integrovaného riadenia*. Ružomberok: VERBUM – vydavateľstvo Katolíckej univerzity v Ružomberku, ISBN 978-80-8084-608-4.

ŠOLC, M. [2010]: *Systémy manažérstva BOZP ako efektívny nástroj riadenia podniku.* Košice. PHF EU 4/2010. ISSN 1336-7137.

8 SYSTÉM MANAŽÉRSTVA INCIDENTOV

Vo filozofickej, prírodovednej, technickej i sociálnej oblasti sa vyskytuje pojem incident (udalosť) v rôznych významoch. V najvšeobecnejšom význame sa pod udalosťami chápe jav, proces, úkaz či skutočnosť *(Požár, 2006)*.

Trochu presnejšie vymedzujú udalosť technické a prírodné vedy, ako osobitný súbor okolností, ako fenomén lokalizovaný v jednotlivom bode časopriestoru. Je to základná výskumná entita v teórii vedy. Najobecnejšie je udalosť definovaná vo filozofii, kde sa chápe ako fenomén, ktorý nasleduje a je spôsobený nejakým predchádzajúcim fenoménom. Pod udalosťou v informatike sa chápe incident v informačnej bezpečnosti, ktorý nastane a spôsobí poruchu alebo výpadok počítačového informačného systému.

Udalosť (incident) je **ľubovoľná zmena v čase na danom objekte** *(Filák, 2006)*. Je to pozorovaná zmena normálneho správania sa systému, životného prostredia, procesu, priebehu práce alebo osoby (zložky). Udalosťami sú ***procesy a javy,*** ktoré prebiehajú za určitých podmienok, v časovom slede jednotlivých činností.

Existujú **tri základné typy udalostí:**

1. **Normálna udalosť** – nemá vplyv na rozhodujúce zložky alebo požiadavky na zmenu riadiacich prvkov pred implementáciou rozhodnutia. Normálne udalosti nevyžadujú účasť vedúcich pracovníkov alebo hlásenia o udalosti.
2. **Vystupňovanie** – narastanie udalosti ovplyvňuje rozhodujúce systémy produkcie alebo vyžaduje vydanie rozhodnutia, ktoré musí následne zmeniť riadiaci proces. Stupňovanie udalosti vyžaduje účasť vedúcich pracovníkov a oznámenie udalosti zainteresovaným účastníkom.
3. **Stav núdze** *(emergency)* – predstavuje bezprostredné riziko pre zdravie, život, majetok alebo životné prostredie. Väčšina núdzových situácií vyžaduje okamžitú reakciu, aby sa zabránilo zhoršeniu situácie, hoci niektoré núdzové situácie nemusí byť možné zmierniť a vedenie môže byť schopné poskytnúť iba zmiernenie následkov. Je to udalosť, ktorá môže:
   a) ovplyvniť zdravie alebo bezpečnosť ľudí,
   b) narušiť základné prvky riadenia rozhodujúcich systémov,
   c) významne ovplyvniť výkon súčastí alebo vplývať na súčasti systémov, čím naruší ich ochranné činnosti alebo ich vplyv na zdravie alebo bezpečnosť osôb,
   d) byť považovaná za stav núdze vyplývajúci z bezpečnostnej politiky alebo z vyhlásenia koordinátora incidentu.

Zatiaľ, čo niektoré núdzové situácie sú evidentné (ako je napríklad prírodná katastrofa, ktorá ohrozuje mnoho životov), rad menších incidentov vyžaduje, aby pozorovateľ (alebo ovplyvnené strany) rozhodol, či sa má kvalifikovať ako núdza. Presná definícia núdze sa mení podľa príslušnosti, zvyčajne ju stanovuje vedenie, ktorého záchranné služby sú zodpovedné za havarijné plánovanie a riadenie.

Incident predstavuje núdzový stav, ak je ***v súlade s jednou alebo viacerými z nasledujúcich podmienok:***

1. predstavuje ***bezprostredné ohrozenie*** života, zdravia, majetku alebo životného prostredia,
2. ***už spôsobil*** stratu života, zdravotné ujmy, škody na majetku, alebo poškodenie životného prostredia,
3. ***má vysokú pravdepodobnosť eskalácie spôsobiť bezprostredné ohrozenie*** života, zdravia, majetku alebo životného prostredia.

8.1 BEZPEČNOSTNÝ INCIDENT

Bezpečnostný incident je proces, ktorý sa pripravuje, vzniká, má svoj priebeh a zaniká a ktorý má za následok **zhoršenie bezpečnostnej situácie**. Bezpečnostné orgány potom riešia vzniknutú situáciu tak, aby sa objasnil relevantný incident *(Požár, 2006)*. Bezpečnostná udalosť je dej, ktorý sa zvyčajne stal v minulosti, ale môže ísť aj o dej, ktorý sa pripravuje, prebieha alebo ktorý sa zatajuje.

Bezpečnostný incident:

- nejaká **neštandardná, alebo nepríjemná bezpečnostná udalosť, ktorá vedie k narušeniu pravidiel bezpečnosti v organizácii,**
- **vzniká** ako následok **zlyhania bezpečnostných opatrení, alebo porušenia bezpečnostnej politiky,**
- je to **udalosť, ktorá môže viesť k strate alebo narušeniu činností organizácie, služby alebo jej určitej funkcie.**

Ak sa incident nezvládne, môže sa vystupňovať do **prerušenia činnosti, poruchy, nehody, havárie, katastrofy alebo krízy** *(Mikolaj, 2004).*

Podľa ISO 22301:2012 *Spoločenská bezpečnosť – Systémy manažérstva kontinuity činnosti – Požiadavky,* **incident** je **situácia, ktorá spôsobuje alebo môže spôsobiť:**

- **prerušenie činností,**
- **škodu,**
- **krízovú situáciu,**
- alebo **krízu.**

Incidenty sú udalosti, ktoré sú najmenej nebezpečné, ale zároveň si vyžadujú určite rovnaké množstvo pozornosti, ako každá iná udalosť. Incidenty sú asi najpočetnejšie udalosti a zároveň asi aj najviac ignorované.

Bezpečnostný incident môže vzniknúť v ktorejkoľvek oblasti prevádzky, od budov, cez informačné technológie až po právne záležitosti. Bez efektívneho manažérstva incidentu môže incident rýchlo narušiť prevádzkové činnosti, informačnú bezpečnosť, informačné systémy, poškodiť zamestnancov či zákazníkov a ďalšie životne dôležité funkcie organizácie.

Organizácia má preto povinnosť **aktívne riadiť závažné incidenty** na ochranu jej zákazníkov, zamestnancov, dodávateľov a podporovateľov, majetku, značky, povesti, ziskov a podporu kontinuity všetkých efektívnych činností. Nevyhnutnou podmienkou pre splnenie tejto povinnosti je schopnosť rýchlo a účinne reagovať na každý závažný incident alebo krízu. Táto činnosť sa v bezpečnostnej teórii uvádza pod pojmom ***„manažérstvo incidentu“***.

8.1.1 Základné pojmy

Termín **incident** vo význame **„nebezpečná udalosť“** zahŕňa pojmy:

- **nehoda** *(Accident),*
- **incident** *(Incident)* v zmysle určitej nežiaducej príhody alebo udalosti,
- **skoronehoda** *(Near Miss),*
- **nebezpečná udalosť** *(Dangerous Occurrence).*

Následkom niektorej nebezpečnej udalosti môže byť aj:

- **porucha,**
- **prerušenie činnosti.**

Udalosťami s vyšším stupňom nebezpečenstva sú:

- **mimoriadne udalosti**,
- **krízové situácie,**
- **kríza**.

Incident

Incident je cudzie slovo, označujúce **nepríjemnú udalosť, príhodu.** V bežnom živote je často chápané ako:

- nehoda (väčšinou) bez významných následkov, vzniknutá na základe ľudského pochybenia a ovplyvňujúca bezpečnosť,
- táto nehoda by však mohla byť natoľko závažná, že je potrebné sa z nej poučiť a predchádzať jej, napr. letecký incident,
- často sa slovom incident označuje tiež exces (výstrelok, výtržnosť) niektorého človeka alebo skupiny ľudí, väčšinou mediálne známych, napr. speváčka Janet Jackson a jej incident na finále Super Bowlu v roku 2004.

V politike sa týmto slovom často označuje:

- nehoda bezpečnostného charakteru, ktorá vyvolá vyhrotenie politického napätia medzi dvoma štátmi, napr. aféra U-2 (zostrelenie amerického výzvedného lietadla U-2 nad územím bývalého Sovietskeho zväzu v máji 1960), Kubánska raketová kríza v októbri 1962,
- krátkodobý skratový akt násilia, bleskový ozbrojený útok (po ktorom väčšinou nasleduje stiahnutie), často vedený ako silové riešenie vyhrotenej politickej situácie, napr. incident vo Scapa Flow (potopenie nemeckého vojnového loďstva v júni 1919).

Incident sa z hľadiska manažérstva bezpečnosti zvyčajne vzťahuje k **nečakanej nežiaducej udalosti, zvyčajne menšej nepríjemnej príhode, ktorá nespôsobila zranenie alebo poškodenie tentoraz, ale mala na to potenciál**.

Je to akákoľvek situácia, ktorá nečakane vzniká na pracovisku, ktorá má potenciál spôsobiť zranenie, škody či ublíženie. Incidenty predstavujú situácie, ktoré majú potenciál spôsobiť ujmu osoby alebo poškodenia zariadenia alebo majetku, napr. prevádzkovanie zariadenia bez využitia potrebnej stráže alebo osobných ochranných pomôcok.

Je to akákoľvek ***udalosť iná než nehoda***, ktorá je spojená s prevádzkou a ovplyvňuje, alebo by mohla ovplyvniť plynulosť a bezpečnosť prevádzky. Incident má širší význam a môže sa použiť ako pre ***náhody,*** tak aj na ***úmyselné činnosti,*** napr. zločiny.

Závažný (nebezpečný) incident (Serious Incident) je definovaný ako nejaká udalosť, ktorá zahŕňa okolnosti ukazujúce na vysokú pravdepodobnosť havárie a ktorá ohrozuje zdravie a bezpečnosť osôb alebo prevádzku či povesť organizácie.

Závažný incident, ktorý vyžaduje vyšetrovanie a musí sa hlásiť, je definovaný ako incident vo vzťahu k zdravotníckej starostlivosti, ktorý má niektorý z nasledovných následkov (*Serious Incident Framework, 2015)*:

- neočakávaná alebo náhodná smrť jedného alebo viac pacientov, zamestnancov, návštevníkov alebo verejnosti,
- vážne zranenie jedného alebo viac pacientov, zamestnancov, návštevníkov, verejnosti, alebo prípad vyžadujúci zásah na záchranu života, vážny chirurgický/ lekársky zásah, úraz s trvalými následkami alebo skrátenie pravdepodobnej dĺžky života, alebo má za následok dlhodobé bolesti či psychologickú traumu,
- udalosti, ktoré zabraňujú alebo môžu zabrániť organizácii poskytovať zdravotnícku starostlivosť, napr. aktuálna alebo potenciálna strata zdravotníckych informácií, poškodenie majetku, povesti či životného prostredia, zlyhanie IKT,

- neopodstatnené tvrdenie o zneužívaní,
- nepriaznivé mediálne pôsobenie alebo verejný záujem o organizáciu.

Nehoda

Nehoda *(Accident)* je **nečakaná, nepredvídaná, nežiaduca udalosť alebo sled udalostí,** ktoré **prerušia dokončenie činnosti**, a ktoré **môžu (ale nemusia) spôsobiť zranenie alebo škody na majetku**. Nehoda sa používa na opis udalostí, ktoré sa dejú ***neúmyselne,*** inými slovami, ***náhodne.***

Zločiny nemožno hodnotiť ako nehody, pretože patria do trestnej činnosti, napríklad v prípade krádeže má lupič v úmysle niečo ukradnúť, nie je to náhoda. Medzi **fyzikálne nehody** patria napr. nechcené kolízie alebo pády, zranenia dotykom o niečo ostré, horúce alebo elektrické napätie, použitie jedu, dopravná nehoda na poľadovici. *Nefyzikálne nehody* sú napr. nechcené odhalenie tajomstva, zabudnutie na dôležité stretnutie a iné. Nehody pri výkone práce alebo vyplývajúce z nej sa nazývajú ***pracovné úrazy***, vo voľnom čase sa stávajú predovšetkým ***športové úrazy.***

Aj keď slovo „nehoda“, môže znamenať niečo, čo je mimo našu kontrolu, v skutočnosti je možné väčšine nehôd predísť, ak ľudia jednoducho sledujú pokyny pre bezpečnosť a ochranu zdravia na ich pracovisku.

Skoronehoda

Skoronehoda *(Near Miss)* je termín pre **neplánované udalosti, ktoré by mohli spôsobiť ujmu, ale nespôsobili ju.** Je to udalosť, pri ktorej nedošlo k žiadnej škode na majetku ani zraneniu, ale kde, keby sa odvíjala len trochu inak (časovo alebo priestorovo), ku škode alebo zraneniu by došlo. Len šťastné prerušenie reťaze udalostí zabránilo zranenie, nešťastie alebo poškodenie; inými slovami, nešťastie však bolo veľmi blízko. Aj keď na uvedenú udalosť sa bežne používa označenie *„ľudská chyba“*, aj *„chybný proces alebo systém“* môžu trvalo umožňovať škody, a je potrebné sa zamerať na ich zlepšenie. Iné známe termíny pre tieto udalosti sú *„únik o vlások“,* alebo *„v prípade pohybujúcich sa objektov“, „blízko kolízie“, „v blízkosti úderu“* alebo *„dar“*.

Nebezpečná udalosť

Nebezpečná udalosť *(Dangerous Occurrence)* predstavuje niečo, čo sa **stane, s následkom zranenia alebo iného poškodenia**, ktoré **nepodlieha povinnosti hlásenia**, ale čo mohlo vážnejšie zranenie či poškodenie spôsobiť. Prehľady nebezpečných udalostí, ktoré je **potrebné hlásiť** sú spracované v jednotlivých oblastiach bezpečnosti, napr. BOZP, nebezpečné látky a pod. **Následkom niektorej nebezpečnej udalosti** môže byť: ***prerušenie činnosti, porucha.***

Porucha

Porucha *(Fault)* je **nepriaznivá, škodlivá zmena normálneho stavu alebo chyba** na úrovni komponentov, vybavenia, alebo subsystému, **čo môže viesť k ich zlyhaniu a neplneniu požadovanej funkcie.** Následkom poruchy môže byť **zastavenie alebo obmedzenie činností**, pri čom vznikne škoda v určitom finančnom rozpätí. Daná udalosť vždy predstavuje pre organizáciu stratu.

Porucha je udalosť, ktorá už nastala a je nutné riešiť ju ex post, podľa konkrétnej situácie. Poruchám možno predchádzať prostredníctvom preventívnych opatrení. Dôležitou súčasťou manažérstva rizík je poruchy predvídať a vopred sa na ich výskyt pripravovať.

Prerušenie činnosti

Prerušenie činnosti (*Business Interruption*) možno chápať ako akúkoľvek **očakávanú alebo neočakávanú udalosť,** ktorá **je príčinou narušenia normálneho priebehu činností. Činnosti** predstavujú prácu alebo úlohy pozostávajúce z jedného alebo viacerých prvkov, vykonávaných zvyčajne na jednom mieste. Činnosti transformujú zdroje alebo vstupné údaje do požadovaných tovarov, služieb alebo výsledkov, ktoré predstavujú hodnotu pre zákazníkov. Dve alebo viac prepojených činností predstavujú ***proces*** a všeobecne rozdeľujú sa do štyroch základných kategórií: spracovanie, kontrola, preprava, uloženie.**Možné stupňovanie následkov bezpečnostného incidentu**

Udalosťami s **vyšším stupňom nebezpečenstva** pre organizáciu sú **mimoriadne udalosti**, ktoré môžu nastať, keď sa incident a jeho stupňovanie nedá zastaviť. Pokiaľ sa uvedené mimoriadne udalosti nepodarí zvládnuť, môžu vyústiť do ***krízovej situácie***, prípadne do vyhlásenia niektorého z ***krízových stavov.***

Medzi **mimoriadne udalosti** patria: ***živelná pohroma, havária, katastrofa, ohrozenie verejného zdravia II. stupňa a teroristický útok.***

Medzi **krízové situácie** patria:

- podľa Ústavného zákonač. 227/2002 Z. z. o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu: ***núdzový stav, výnimočný stav, vyhlásenie vojnového stavu a vypovedanie vojny,***
- podľa Zákona č. 238/2002 Z. z. o riadení štátu v krízových situáciách mimo času vojny a vojnového stavu: ***mimoriadna situácia, núdzový stav a výnimočný stav.***

8.1.2 Klasifikácia a druhy bezpečnostných incidentov

Každý 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.

Špecifikácia, resp. konkrétne určenie o aký druh incidentu ide, ovplyvňuje vznik konkrétneho druhu a zabezpečenie špecifických činností bezpečnostných orgánov, ktoré sú do týchto činností nasadené. Klasifikáciu incidentov možno vykonávať **podľa rôznych kritérií**.

Medzi najvýznamnejšie určujúce kritériá patrí:

a) právne posúdenie danej udalosti – škodová udalosť, priestupok, trestný čin,
b) zavinenie danej udalosti – úmyselné zavinenie, zavinenie z nedbanlivosti, prírodné katastrofy,
c) spôsobenie následku (ujmy) – škoda, ublíženie na zdraví, usmrtenie, poškodenie cudzích práv danou udalosťou a pod.

Úrovne incidentov

Každá organizácia (spoločnosť) si podľa svojich podmienok môže stanoviť vlastné stupne úrovní incidentov. Všeobecné stupne nie sú pevne stanovené, napr. environmentálne incidenty sa zaraďujú do 5 stupňov, ***malý, obmedzený, vážny, veľmi vážny a katastrofický***.

V literatúre sa uvádzajú rôzne kritéria na stanovenie závažnosti incidentov, napr.:

- **jednotlivé stupne závažnosti:** nízka, stredná, vysoká, kritická,
- **podľa množstva postihnutých užívateľov:** jeden alebo niekoľko málo užívateľov, celá pobočka, celý región, celá spoločnosť,

- **podľa úrovne manažmentu, ktorý sa bude incidentom zaoberať:** referent, nižší manažment, stredný manažment, vrcholový manažment,
- **podľa toho, kto musí byť s incidentom zoznámený:** jeden alebo niekoľko málo zamestnancov spoločnosti, všetci zamestnanci spoločnosti, okrem vlastných zamestnancov aj osoby mimo spoločnosti, okrem vlastných zamestnancov aj verejnosť,
- **podľa úrovne odbornosti:** prvá úroveň podpory, správca systému, bezpečnostný expert, bezpečnostná firma.

Spoločnosť Prince's Trust pre manažérstvo incidentov rozlišuje tri úrovne incidentov, ***vysoká*** (červená), ***stredná*** (oranžová), ***nízka*** (žltá).

a) Vysoká úroveň incidentu:
- incident majúci za následok smrť, ťažké ublíženie na zdraví alebo viacnásobné straty na životoch ako následok činnosti organizácie, vrátane akcií dodávateľských partnerov,
- incidenty zahŕňajúce násilné alebo iné závažné trestné činy,
- incidenty spojené so zneužívaním alebo potenciálnym zneužívaním mládeže,
- incidenty (napr. požiar, povodeň, výbuch), ktoré spôsobia uzavretie pracoviska organizácie po dlhšiu dobu ako jeden týždeň,
- incidenty spojené s terorizmom alebo riziká, ktoré priamo ovplyvňujú prevádzku,
- incidenty, ktoré by mohli prilákať záujem celoštátnej tlače,
- významné straty alebo vyzradenie citlivých osobných údajov.

Na tieto prípady bude priamo dohliadať vrcholový manažment. Prvoradá úloha **vedúceho manažéra incidentov (koordinátora incidentov)** je ***hlásiť incident nadriadenému vo vrcholovom manažmente.***

b) Stredná úroveň incidentu:
- incidenty majúce za následok zranenia vplyvom činností organizácie, vrátane akcií dodávateľských partnerov,
- incidenty týkajúce sa pokusu o samovraždu,
- incidenty, ktoré vedú k uzavretiu pracoviska organizácie po dobu kratšiu ako jeden týždeň,
- incidenty, ktoré by mohli prilákať záujem miestnej tlače.

Pri týchto incidentoch bude **vedúci manažér incidentov v prípade potreby** navrhovať vhodných zamestnancov na riešenie incidentu a ***hlásiť incident nadriadenému vo vrcholovom manažmente.*** V prípade možnosti stupňovania incidentu do vyššej úrovne je potrebné incident dôkladne preskúmavať.

c) Nízka úroveň incidentu:
- všetky ďalšie prípady a skoronehody, ktoré predstavujú príležitosti poučenia pre posilnenie dôvery,
- incidenty, ktoré pravdepodobne neprilákajú záujem tlače.

Tieto prípady budú zahrnuté ako nehody a incidenty ***do zoznamov a hlásení*** a nebudú vyžadovať činnosť Tímu manažérstva incidentov. Zamestnanci, ktorých sa incident dotýka, sa musia podporiť pri riešení incidentu. Ak to bude potrebné, môže sa vyžiadať pomoc od špecialistov.

8.2 PROCES MANAŽÉRSTVA BEZPEČNOSTNÝCH INCIDENTOV

Manažérstvo incidentu *(Incident Management)* je termín, charakterizujúci činnosti organizácie pri:

- predchádzaní incidentu,
- identifikovaní incidentu,
- analýze a regulovaní nebezpečenstva, aby sa zabránilo jeho opakovanému výskytu v budúcnosti,
- vyvodení dôsledkov pre budúcu činnosť.

Manažérstvo incidentu je súhrn procesov súvisiacich s detekciou, hlásením a posudzovaním incidentu, následnou odozvou a so zaobchádzaním a poučením sa z neho *(ISO/IEC 27000:2009)*. **Cieľom manažérstva incidentu je čo najskôr obnoviť činnosť organizácie.**

Manažérstvo bezpečnostného incidentu sa týka detekcie a reakcie na bezpečnostné incidenty a s nimi súvisiacich komunikačných plánov na ohlasovanie a informovanie, vrátane určenia úloh a zodpovednosti.

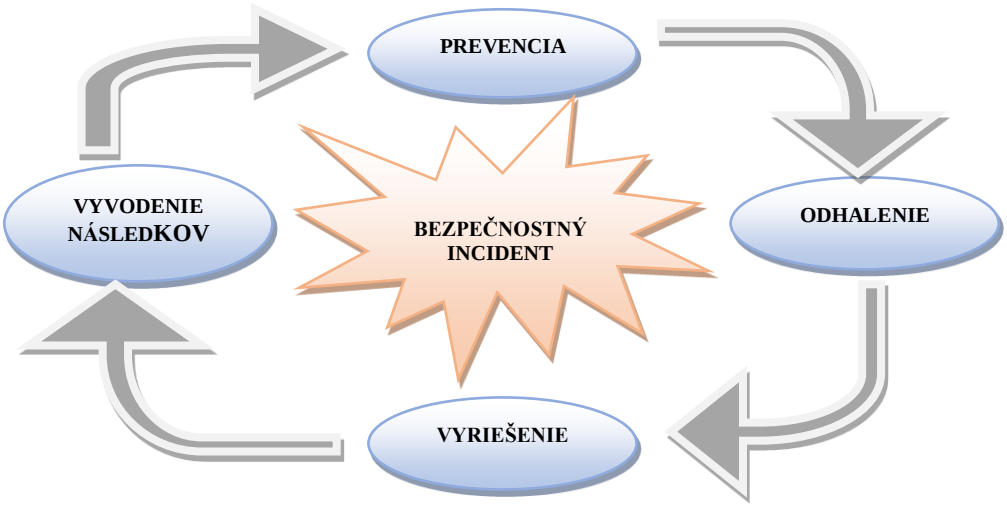
Organizačné štandardy a postupy manažérstva bezpečnostných incidentov sa majú týkať zisťovania bezpečnostných incidentov a reakcií na vzniknuté incidenty, ako aj zabezpečenia prevencie pred vznikom alebo opakovaním bezpečnostných incidentov. Monitorovacie a kontrolné postupy majú byť schopné odhaliť nielen zrealizované narušenia, ale aj pokusy o narušenie bezpečnosti.

K dôvodom na vyšetrovanie incidentu na pracovisku patria:

- najdôležitejšie je ***zistiť príčinu incidentu a zabrániť podobným incidentom v budúcnosti,***
- splniť všetky právne požiadavky,
- overiť súlad s platnými bezpečnostnými predpismi,
- zistiť ***náklady na incident,***
- spracovať nároky na odškodnenie zamestnancov.

Incidenty, ktoré nespôsobili zranenia alebo škody na majetku by sa mali vyšetriť na určenie nebezpečenstiev, ktoré je treba odstrániť. Rovnaké zásady platia pre rýchle vyšetrovanie menšieho incidentu a na viac formálne vyšetrovanie nebezpečných udalostí.

Životný cyklus bezpečnostného incidentu je uvedený na obr. 22.



Obr. 22 Životný cyklus bezpečnostného incidentu (zdroj Staša, 2003)

Životný cyklus bezpečnostného incidentu

1. **Prevencia**
   - Príprava na incident.
2. **Odhalenie**
   - **2.1 Zistenie a registrácia incidentu:**
     a) Identifikácia:
        - zistenie,
        - hlásenie o vzniku nehody určenej osobe v rámci organizácie,
        - poskytnutie prvej pomoci a lekárskej starostlivosti pre poškodené osoby a zabránenie ďalšiemu zraneniu alebo škode,

     b) registrácia – Záznam zistenej alebo hlásenej udalosti v systéme.
   - **2.2 Klasifikácia a prvotná podpora:**
     a) kategorizácia – udalosti sú rozdelené do kategórií podľa priority,
     b) stanovenie priorít – incident stanovuje priority pre lepšie využitie zdrojov a času podporného personálu.
3. **Vyriešenie:**
   - **3.1 Vyšetrovanie a diagnostika:**
     a) diagnostika – odhalí všetky príznaky incidentu,
     b) eskalácia – povinnosť podpory od iných organizačných jednotiek,
     c) vyšetrovanie a popis druhu – ak nie je nájdené žiadne riešenie z minulosti, incident sa preskúma a nájde príčina:
        - identifikovanie príčin,
        - Správa o vyšetrovaní incidentu.
   - **3.2 Vyriešenie a obnova** – ihneď, ako sa nájde riešenie, je incident vyriešený:
     a) vypracovanie plánu pre prijatie nápravných opatrení,
     b) vykonávanie plánu,
     c) obnova poškodeného systému,
     d) vyhodnotenie účinnosti nápravných opatrení.
   - **3.3 Uzavretie incidentu:**
     a) výpočet vzniknutej škody,
     b) uvedenie koncového stavu incidentu do záznamu o incidente.
   - **3.4 Vlastníctvo, monitorovanie, sledovanie a komunikácia:**
     - sledovanie priebehu a výsledku riešenia incidentu.
4. **Vyvodenie následkov:**
   a) starostlivosť o tých, ktorí sú ovplyvnení incidentom,
   b) aktualizácia Plánov reakcie na incident a dodatočné zabezpečenie systému,
   c) vykonanie zmien pre neustále zlepšovanie,
   d) poučenie do budúcnosti.

8.3 PREVENCIA – PRÍPRAVA NA INCIDENT

V priebehu implementácie SMB do organizácie sa uskutočňuje aj príprava na riešenie incidentov. **Bezpečnostný manažér, vedúci manažér incidentu (koordinátor incidentov) a tímy na manažérstvo incidentu:**

- vypracujú postupy na riešenie incidentov v **Pláne manažérstva incidentu** *(Incident Management Plan),*
- spracujú **Metodiky (smernice) na vyšetrovanie bezpečnostných incidentov,**
- uskutočňujú **vzdelávanie** zamestnancov a osobitne členov tímov na riešenie incidentu o postupe pri manažérstve incidentu.

Pre úspešné zvládnutie riešenia bezpečnostných incidentov treba:

- mať ***definované postupy pre činnosť v prípade vzniku*** (objavenia sa) bezpečnostného incidentu,
- mať vypracované ***postupy na riešenie*** najpravdepodobnejších bezpečnostných incidentov,
- každý bezpečnostný incident ***analyzovať,*** pričom sa zamerať na analýzu časových a priestorových charakteristík príčin jeho vzniku, na spôsob jeho prejavov, pôsobenia a negatívnych následkov,
- 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*** na 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.

Plán manažérstva incidentu podľa ISO 22301:2012 *Spoločenská bezpečnosť – Systémy manažérstva kontinuity činnosti – Požiadavky* predstavuje jasne definovaný a zdokumentovaný plán činností pre použitie v dobe incidentu, typicky zahŕňajúci rozhodujúce personálne zdroje, služby a činnosti potrebné pre realizáciu procesu manažérstva incidentu. Tento plán:

- podrobne opisuje, ako incident vyriešiť, po návrat do normálnej prevádzky,
- poskytuje informácie o štruktúre Tímu manažérstva incidentu,
- uvádza kritériá pre obnovenie kontinuity prevádzky a požiadavky na zdroje,
- popisuje manažérstvo incidentu, všetky potrebné pohyby personálu a rozhodujúce postupy.

Plán manažérstva incidentu môže obsahovať:

- účel Tímu manažérstva incidentu, povinnosti a odborné plány na jeho podporu,
- kategórie incidentov,
- možné stupňovanie a úrovne závažnosti incidentov,
- ako sa zaoberať s incidentom, hláseným dodávateľskými partnermi alebo havarijnou službou,
- priority reakcií na incident,
- otázky, ktoré musí riešiť Tím manažérstva incidentu,
- vedenie záznamov o incidente,
- preskúmanie po vyriešení incidentu,
- doplnenie správ o incidente.

S Plánom manažérstva incidentu sa musia ***zoznámiť všetci zamestnanci***. V prípade incidentu by si mal každý zapojený zamestnanec ***zaznamenávať svoje zapojenie do incidentu*** do organizáciou vopred pripravených ***formulárov.***

Všetci zamestnanci by mali mať ***kontaktné údaje*** na svojho nadriadeného a svojich podriadených, aby mohli v prípade potreby využiť telefonické spojenie na kontaktovanie všetkých zamestnancov.

Všeobecná štruktúra plánu nie je pevne stanovená, v spoločnosti Prince's Trust obsahuje **Plán manažérstva incidentu** nasledujúce údaje:

1. Všeobecné údaje:

1.1 Úvod:
- všeobecne o incidentoch v organizácii,
- hlavné kontaktné telefónne čísla.

1.2 Účel plánu.

1.3 Miestne kontaktné telefónne čísla tiesňového volania.

1.4 Povinnosti všetkých zamestnancov.

2. Tím manažérstva incidentu – účel, zodpovednosť a odborné plány:

2.1 Účel.

2.2 Povinnosti Tímu manažérstva incidentu:
- určenie cieľov na minimalizovanie dopadu na prevádzku,
- hlásenie príslušných incidentov nadriadenému,
- vytvorenie vlastných postupov na riešenie incidentu a jeho následkov,
- schválenie **Plánu komunikácie** s komunikačným strediskom organizácie,
- monitorovanie incidentu a v prípade potreby prehodnotenie priradených úrovní incidentu,
- pôsobenie v úlohe ***hlavného kontaktného miesta*** pre manažérstvo incidentu.

2.3 Podporné odborné plány a pomocné programy:
- **Program na riešenie incidentov BOZP,**
- **Plán obnovy IT po havárii,**
- **Plán kontinuity činností** (Business Continuity Plan).

3. Určenie kategórií úrovní pre manažérstvo incidentu.

4. Spôsob hlásenia incidentu dodávateľskými partnermi a havarijnými službami.

5. Priority pre reakcie na incident:
- ***Bezpečnosť života a zdravia*** – absolútnou prioritou je bezpečnosť všetkých osôb, ktoré sú alebo môžu byť zapojené do incidentu.
- ***Obnovenie a udržiavanie poskytovania služieb*** – v priebehu alebo po incidente je typické, že sa dosahuje len znížená úroveň poskytovania služieb, preto je potrebné umožniť obnovu kompletných služieb a aktívne riadenie následkov zníženej prevádzky.
- ***Ochrana a zlepšenie povesti organizácie*** – ochrana značky a dobrého mena spoločnosti.
- ***Prevencia pred ďalším rizikom alebo poškodením organizácie*** – proaktívna odpoveď na incident, pri hľadaní potenciálnych rizík v blízkej budúcnosti.

6. Externá komunikácia v priebehu incidentu – hlásenia a plán komunikácie.

7. Otázky, ktoré má riešiť Tím manažérstva incidentu.
Zatiaľ čo presná skladba programu činnosti tímu bude diktovaná charakterom incidentu, mal by riešiť nasledujúce otázky:

- Správy o incidente – počiatočné posúdenie udalosti a všetky ďalšie relevantné informácie. Informácie sú často obmedzené v ranej fáze udalosti, takže je dôležité rozlišovať medzi *tým, čo je známe* a *tým, čo sa predpokladá.*
- Analýza možného/ skutočného dopadu – vyhodnotiť dostupné informácie a porovnať názory všetkých dôležitých funkcionárov, cieľom je vytvoriť spoločný tímový pohľad na udalosti.
- Plán činnosti – definovať a určiť priority činností, identifikácia všetkých potrebných zdrojov na celoštátnej a miestnej úrovni, súhlas s prístupom ku koordinácii a podpore následných aktivít.
- Komunikácia – odvolanie sa na Plán komunikácie.
- Hlásenia – schválenie požiadaviek na podávanie správ o životnom cykle incidentu a prideľovanie úloh zodpovedajúcim spôsobom.

8. Vedenie záznamov.

9. Preskúmanie po incidente.

10. Ohlasovanie, monitorovanie a hodnotenie politiky.

Smernica (metodika) **na vyšetrovanie bezpečnostných incidentov**

Smernica na vyšetrovanie nehody má poskytovať jasné a stručné pokyny, čo robiť a kedy to urobiť. Vytvára sa skôr, než dôjde k incidentu, spresňuje zodpovednosti tých, ktorí sa zapoja do procesu vyšetrovania, napr. môže obsahovať oznámenie incidentu, v reakcii na vyšetrovanie a pod.

Smernica by minimálne mala obsahovať postupy, ktoré určujú:

- kto by mal byť informovaný o incidente,
- kto je oprávnený oznámiť incident vonkajším organizáciám (hasiči, polícia a pod.),
- kto je určený na vyšetrovanie,
- potrebné školenia pre vyšetrovateľov incidentov,
- kto prijíma a postupuje správy o vyšetrovaní,
- časový plán na vykonávanie opatrení pre zníženie nebezpečenstva.

8.4 ODHALENIE INCIDENTU

Identifikácia a hlásenie incidentu

Po zistení akéhokoľvek incidentu je potrebné:

- podať správu o jeho vzniku určenej osobe v rámci organizácie,
- iniciovať poskytnutie prvej pomoci a lekárskej starostlivosti pre poškodené osoby,
- zabrániť ďalšiemu zraneniu alebo rozširovaniu škody.

Program na ohlasovanie incidentu je podstatným prvkom riešenia incidentu. Od všetkých zamestnancov organizácie aj tretích osôb sa má vyžadovať, aby si všímali a hlásili informácie a okolnosti o možnom narušení bezpečnosti a zraniteľnosti prevádzky a služieb. Každý zamestnanec, ktorý objaví, usvedčí alebo pozná páchateľa, nebezpečenstvo alebo neoprávnený postup alebo situáciu, alebo priestupok proti bezpečnostným pravidlám, má túto vec hneď oznámiť príslušným orgánom. Včasné vykazovanie krádeže, straty alebo poškodenia majetku, nedovolenej manipulácie alebo nepovoleného prezradenia informácií sú dôležité informácie.

Včasné hlásenie zvyšuje možnosť, že sa majetok získa späť, minimalizujú škody a postihne páchateľ. **Incident môže byť ohlasovaný** *telefonicky, hlasovou poštou, osobne, písomne, faxom, emailom, automaticky monitorovacím softvérom* alebo môže byť zaznamenaný priamo *používateľom, ktorý má prístup do systému na zaznamenávanie incidentov.*

V priebehu hlásenia incidentu je potrebné hlásiť:

- Čo sa stalo/deje (reálny popis).
- Kde a kedy udalosť nastala.
- Kto bol zapojený (ak sa to dá preukázať).
- Došlo k zraneniu osôb alebo poškodeniu jednotlivcov alebo majetku?

Registrácia incidentu

Všetky zistené alebo hlásené incidenty by mali byť **zaregistrované** spôsobom, ktorý dovoľuje vyhľadávanie a analyzovanie dôležitých informácií. Zamestnanci manažmentu incidentov by mali mať prístup do databázy, v ktorej sú uložené informácie o:

- technických špecialistoch,
- predchádzajúcich incidentoch,
- súvisiacich problémoch a známych chybách,
- náhradných pracovných postupoch,
- kontrolných zoznamoch, ktoré napomáhajú pri obnove činností *(ISO/IEC 20000-1:2011).*

Všetky incidenty musia byť dôkladne zaznamenané, najmä musia byť zaznamenané všetky relevantné informácie o incidente, aby pomohli k jeho vyriešeniu.

Každý zaznamenaný incident by mal obsahovať informácie uvedené v tab. 3.

Všetky informácie o incidente sa ukladajú na bezpečnom mieste s riadeným prístupom pre analýzu a spracovanie opatrení a prípadné použitie informácií v pracovno-právnom alebo trestno-právnom procese.

Tab. 3 Záznam o incidente (možný vzor)

Referenčné číslo		Kategorizáciu incidentu	
Dátum a čas zaznamenania		Naliehavosť incidentu	
Meno osoby, ktorá incident zaznamenala		Popis príznakov incidentu	
Spôsob ohlásenia		Stav incidentu	
Kontakt na užívateľa na danej lokalite		Dopad incidentu	
Meno riešiteľskej skupiny alebo riešiteľa		Priorita incidentu	
		Súvisiace problémy	
Kategória uzavretia		Riešiteľské aktivity	
Dátum a čas uzavretia incidentu		Dátum a čas vyriešenia	

Klasifikácia incidentu

Počiatočné zaznamenanie musí obsahovať aj informáciu o kategorizácii incidentu pre štatistické účely. **Klasifikácia incidentov** je dôležitá, umožňuje stanoviť prioritu riešenia a prípadne ďalšie vzťahy, ktoré môžu byť použité pri porovnávaní s databázou známych chýb. Množstvo nástrojov umožňuje aj viacúrovňovú kategorizáciu incidentov.

Možným spôsobom kategorizácie je ***klasifikácia incidentov podľa zdroja,*** ktorým môže byť:

- človek – úmyselné, neúmyselné incidenty,
- technické či technologické zariadenie (stroj),
- nebezpečné látky – s chemickými, fyzikálnymi, toxikologickými alebo biologickými vlastnosťami,
- živelné pohromy – vnútorné (požiar), vonkajšie (víchrica).

Ďalším dôležitým aspektom je **stanovenie priority incidentu**, ktorá sa využíva pri určení **relatívnej dôležitosti incidentu**. Je založená na ***dopade a závažnosti*** a zvykne identifikovať ***čas,*** ktorý si činnosti vyžadujú. **Dopad** predstavuje ***mieru vplyvu incidentu, problému alebo zmeny na procesy v organizácii***, často sa zakladá na tom, ako budú ovplyvnené úrovne služieb. Na druhej strane **naliehavosť** je ***miera, ktorá vyjadruje dobu potrebnú pre incident, problém alebo zmenu*** (napr. vysoko významný incident môže mať nízku naliehavosť, ak sa dopad neprejaví do konca finančného roka).

8.5 RIEŠENIE INCIDENTU

Vyšetrovanie *(investigations)* incidentu predstavuje činnosti, ktorých cieľom je ***ukončiť prebiehajúci incident a/alebo minimalizovať škody,*** ktoré by uvedeným incidentom mohli byť spôsobené. Interné vyšetrovanie nehôd a incidentov poskytuje organizácii spätný obraz o fungovaní opatrení na kontrolu rizík a súvisiacich postupov systému manažérstva bezpečnosti. Z toho dôvodu sa majú systematicky vyšetrovať nielen zjavné príčiny, ale aj skryté príčiny.

V priebehu riešenia incidentu sa uskutočňuje:

a) diagnostika incidentu,
b) eskalácia incidentu,
c) objasňovanie incidentu,
d) vyriešenie incidentu a obnova,
e) tvorba záverov z riešenia incidentu,
f) uzavretie incidentu.

Diagnostika incidentu

Po *určení priority a klasifikovaní incidentu* je snaha incident **vyriešiť na prvej úrovni manažérstva incidentu** (miesto prvého kontaktu).

Problém je obvykle identifikovaný bežným zamestnancom a to napríklad nefunkčnosťou stroja alebo zariadenia, resp. odopretím požadovanej služby (napr. zlyhanie softvérovej aplikácie, pripojenie na internet). Nasleduje šetrenie a pokusy o vyriešenie problému **miestom prvého kontaktu.**

V úvode sa vykoná **diagnostika incidentu** a hľadá sa jeho riešenie. Vo väčšine prípadov sa na to využívajú dané postupy, kedy operátor pomocou otázok diagnostikuje problém. Pri diagnostike by mali byť zodpovedané otázky: **kto, čo, kedy, kde, prečo, ako.**

Diagnostika incidentu znamená:

- ***odhaliť podstatu a príčiny incidentu,***
- určiť jeho ***druh a úroveň,***
- ***a odhadnúť, akým spôsobom sa bude riešiť,*** najmä vtedy, keď nie je jasne špecifikovaný problém.

Fakty by mali byť jasne odlíšené od názorov a dedukcií a oboje by malo byť prezentované jasne a v logických súvislostiach. V priebehu diagnostiky sa k incidentu dopĺňajú ďalšie dôležité informácie.

Na záver diagnostikovania incidentu na mieste prvého kontaktu môžu nastať nasledujúce **varianty:**

- **riešenie je k dispozícii** – aplikuje sa, zaznamená a incident je vyriešený.
- **riešenie nie je dostupné** – manažment sa pokúsi vyhľadať riešenie v databáze známych problémov, pri nájdení riešenia sa toto riešenie aplikuje, zaznamená a incident je vyriešený.
- **diagnostika nebola úspešná** – incident je potrebné ***eskalovať (stupňovať).***

Eskalácia incidentu

Pokiaľ táto aktivita nevedie k úspechu v požadovanom čase, ***je potrebné problém eskalovať – riešiť na vyššom stupni.*** Existujú dva typy eskalácie, funkčná eskalácia a hierarchická eskalácia.

- **Funkčná eskalácia** presúva riešenie incidentu, problému alebo zmeny na ***odborný technický tím,*** ktorý je v rámci organizácie na vyššom stupni odbornej znalosti.

- **Hierarchická eskalácia** je naproti tomu proces informovania alebo zapojenia ***viacerých nadriadených úrovní odborného manažmentu*** pri riešení eskalácie.

Oba typy eskalácie je možné vykonávať manuálne alebo zavedením automatickej eskalácie. Automatická eskalácia je väčšinou vedená na základe prekročenia časového limitu pre riešenie incidentu, preto je v tomto prípade nutné zaznamenávať i čas strávený nad jeho riešením. Rovnako je podmienená vlastníctvom vhodného softvérového nástroja, ktorý automatizáciu umožňuje. Podporné riešiteľské skupiny incident podrobne preskúmajú a vykonajú potrebnú diagnostiku incidentu.

Z pohľadu riešenia incidentu je ***niekedy problém rozlíšiť***, kedy sa riešenie ***bežného poruchového stavu*** mení na riešenie **havarijného stavu.** Postupným hlásením sa informácia dostane až **k osobe, ktorá je oprávnená vyhlásiť *havarijný stav*** (napr. tím výkonného manažmentu, pod vedením manažéra BCM).

V prípade havarijného stavu sa striktne postupuje ***podľa plánov BCM*** (fáza obnovy). Samotné rozhodnutie o vyhlásení havarijného stavu nie je pre danú zodpovednú osobu ľahkou záležitosťou, nakoľko so sebou prináša nemalé finančné náklady. Havarijný stav je vhodné obvykle vyhlásiť ak:

- je zrejmé, že oprava štandardnými postupmi o značný čas prekročí cieľovú dobu obnovy *(Recovery Time Objective),*
- z času vymedzeného na cieľovú dobu obnovy zostáva už len toľko, koľko je potrebné na obnovu podľa spracovaných a otestovaných plánov.

Krízovým riadením (*Crisis Management*) možno chápať proces, ktorým organizácia riadi širší dopad akéhokoľvek incidentu, až do doby, pokiaľ nie je pod kontrolou, alebo zvládnutý bez ďalšieho dopadu na organizáciu, alebo pokiaľ nie je aktivovaný plán kontinuity činností.

Objasňovanie incidentu

Ak sa v minulosti nevyskytlo žiadne podobné riešenie, incident sa **preskúma a nájde jeho príčina.** Na objasnenie incidentu sa môže využiť:

a) Všeobecné vyšetrovanie incidentov – typické pre väčšinu vyšetrovaných incidentov, ktoré sa vyskytujú na pracovisku. Vedúci alebo bezpečnostný manažér, môže hľadať ***príčiny incidentu*** a vypracuje ***správu o incidente***. Postupy pre tento spôsob vyšetrovania nehôd sú typicky všeobecné a zisťované údaje sú obmedzené na informácie požadované vo formulári na vyšetrovanie incidentov.

b) Špeciálne vyšetrovanie incidentov – vyžaduje osobitné vedomosti a kvalifikovaných vyšetrovateľov. Špeciálne vyšetrovanie je nevyhnutné pre určité typy incidentov, vrátane nehôd motorových vozidiel, požiarov a výbuchov. Špeciálne vyšetrovanie vyžaduje osobitné pomôcky, nástroje a postupy.

Medzi **spôsoby vyšetrovania incidentov** patria:

a) vyšetrovanie na základe minulých udalostí – využíva údaje o incidentoch, ktoré sa stali v minulosti, takto sa vykonáva väčšina vyšetrovaní na pracovisku.

b) štatistické vyšetrovanie – využívajú sa štatistické informácie zhromaždené v priebehu času na zistenie príčin a rozvíjanie preventívnych opatrení. Štatistické zisťovania využívajú matematické postupy, ktoré identifikujú príčiny nehody z hľadiska štatistickej pravdepodobnosti.

c) vyšetrovanie veľkých strát – podrobné vyšetrovania nehody, ktorá vyústila do väčšej straty na životoch, financií, alebo škôd na majetku než je obvyklé. Príklady vyšetrovania veľkých strát sú veľké priemyselné požiare, výbuchy v továrni a letecké nehody.

d) systémy vyšetrovania – Systémy vyšetrovania využívajú systémový prístup na identifikáciu príčinných faktorov. Existuje celý rad dostupných systémov vyšetrovacích techník, vrátane *Analýzy hlavných príčin, Analýzy stromu porúch (FTA) a Analýzy príčin a následkov (FMEA).*

Medzi **štandardizované opatrenia na to, kedy a ako sa má vyšetrovanie vykonávať**, patria:

- postupy oznamovania interných a externých nehôd a incidentov a podávanie správ o nich,
- postupy, formáty a prístupy k vyšetrovaniu (napr. protokol z miesta incidentu), prípadne členené podľa povahy incidentu (napr. ekologické havárie, úrazy zamestnancov, preprava nebezpečných tovarov),
- postupy podávania práv a dokumentovania zistení, záverov a odporúčaní,
- postupy prehodnocovania opatrení na kontrolu rizík po nehode alebo incidente a zabezpečenie realizácie odporúčaní a preventívnych alebo nápravných činností s cieľom zamedziť opakovanému výskytu.

Vyšetrovatelia incidentu

Účinné vyšetrovanie vyžaduje **metodický, štruktúrovaný postup *získavania informácií, ich triedenia a analýzy.*** Vyšetrovanie by mal vykonávať niekto so skúsenosťami s podobným incidentom, ktorý pozná techniky vyšetrovania, so znalosťou pracovných procesov, postupov, osôb a pracovných vzťahov a prostredia a konkrétnej situácie.

Vyšetrovanie nehody je dobrým spôsobom, ako **zapojiť zamestnancov** do otázok bezpečnosti a ochrany zdravia pri práci. To dodá nielen doplňujúci pohľad na problematiku a všeobecnejšom poňatí, ale v očiach zamestnancov to zdôveryhodní vyšetrovanie. Zapojenie zamestnancov tiež obohatí daných zamestnancov tým, že ich vzdeláva o možnostiach potenciálnych rizík – táto skúsenosť väčšinou prispeje, že začnú brať vážnejšie otázky bezpečnosti a ochrany zdravia pri práci, čím sa posilní bezpečnostná kultúra v celej spoločnosti.

Vyšetrovateľom incidentu by mal byť **vedúci pracoviska či práce**, kde k incidentu došlo, **ďalšími členmi vyšetrovacieho tímu** môžu byť:

- ***zamestnanci so znalosťou práce (odborní špecialisti),***
- ***vedúci pracovníci úsekov, ktorých sa incident dotýka,***
- ***bezpečnostný technik,***
- ***zástupca vedenia BOZP,***
- ***zástupca odborového zväzu,***
- prípadne aj ***zamestnanci so skúsenosťami pri vyšetrovaní, vonkajší expert, zástupca miestnej správy.***

Vo väčšine prípadov by mal pomôcť preskúmať udalosť **nadriadený funkcionár. Útvar bezpečnosti** a alebo **osoba zodpovedná za túto oblasť** by mali ***participovať na vyšetrovaní*** alebo sa aspoň dôkladne sa zoznámiť s poznatkami vyšetrovateľov a ich odporúčaniami. Nikto by nemal vyšetrovať incident ***bez zodpovedajúceho školenia a výcviku***. Pri vyšetrovaní ***vyšetrovatelia spolupracujú s právnikom organizácie a policajnými zložkami.***

V rozsiahlej, štruktúrovanej organizácii je na riešenie incidentu obvykle určený **Manažér incidentu *(koordinátor),*** ktorý využíva **Tím manažérstva incidentu** *(Incident Management Team)* alebo **Tím reakcie na incident** *(Incident Response Team).*

Tím manažérstva incidentu je vytvorený na ***riešenie incidentov vysokej a strednej úrovne,*** ktoré ovplyvňujú dôležité činnosti (prevádzku). Tieto tímy sa určujú vopred, alebo v priebehu nebezpenej udalosti, majú miesto vo vedení ISMB. Na riešenie ***závažných inci-***

dentov (trestné činy, vážne zranenie, usmrtenie) sa prizývajú **orgány činné v trestnom konaní.**

Vyšetrovanie incidentu vykonávajú buď ***interní vyšetrovatelia*** alebo si organizácia najíma ***externú špecializovanú firmu***, ktorá vykoná ***analýzu*** alebo ***ucelený forenzný audit.*** V niektorých prípadoch sa pri riešení incidentu môže vykonávať ***audit.*** Audit je intenzívnejší, aj keď prakticky je rozdiel medzi oboma spôsobmi veľmi malý.

Na vyšetrovanie priestupkov alebo trestných činov sa využíva najmä **forenzná analýza.** Je to pojem pre hĺbkovú analýzu, vyšetrovanie, ktorého účelom je objektívne určiť a zdokumentovať vinníkov, dôvody, priebeh a následky nejakého bezpečnostného incidentu alebo porušenie práva štátu alebo pravidiel organizácie.

Forenzná analýza vyšetruje priestupok alebo trestný čin – preukazuje ***kto, ako a kedy niečo zavinil.*** Často súvisí so súdnym dokazovaním, najmä v trestných záležitostiach. Zahŕňa využitie širokého spektra vyšetrovacích technológií a postupov a metód. Forenzní špecialisti zhromažďujú rôzne typy informácií, preto pracujú ako s elektronickými zariadeniami, tak klasickým spôsobom s informáciami na papieri. Forenzná analýza sa používa v celom rade odborov, od kriminalistiky až po interné vyšetrovanie incidentov vo vnútri organizácie.

Vyriešenie incidentu a obnova

Ihneď, ako sa nájde riešenie, je incident vyriešený. Existuje viac spôsobov, ako rýchlo reagovať na bezpečnostný incident:

a) Okamžitá reakcia – pri zranení osôb alebo na zastavenie útoku, ***cieľom*** je *predísť zraneniam a/alebo prevencia ďalšieho útoku.*

b) Potreba rýchlej reakcie (v najbližších niekoľkých hodinách alebo dokonca dňoch), aby sa zabránilo vzniku prípadného nového bezpečnostného incidentu, ***ciele*** stanovia zodpovedné osoby alebo tím manažérstva incidentu so zameraním na *obnovenie potrebnej istoty tých, ktorí sú ovplyvnení incidentom.*

c) Nadväzné opatrenia (v niekoľkých dňoch alebo týždňoch, alebo dokonca mesiacoch). Keď sa situácia stabilizovala, nemusí byť potrebná okamžitá alebo rýchla reakcia. Po každom bezpečnostnom incidente, ktorý si vyžiadal okamžitú alebo rýchlu reakciu sa však vyžaduje **následná reakcia**, s cieľom obnoviť alebo preskúmať pracovné prostredie.

Následné akcie/reakcie budú prebiehať prostredníctvom bežných rozhodovacích procesov organizácie, s cieľom ***obnoviť bezpečné pracovné prostredie navonok, rovnako ako pretvoriť vnútorné organizačné postupy a zlepšiť následné reakcie na bezpečnostné incidenty***.

Každá reakcia má tiež brať do úvahy **bezpečnosť a ochranu iných ľudí alebo organizácií alebo inštitúcií, s ktorou majú pracovný vzťah.**

V období obnovy sa vykonávajú nasledujúce opatrenia:

a) vypracovanie plánu na prijatie nápravných opatrení,
b) vykonávanie plánu,
c) obnova poškodeného systému,
d) vyhodnotenie účinnosti nápravných opatrení.

Závery z vyšetrovania incidentu

Organizácia musí vytvoriť a udržiavať postupy pre zaznamenávanie, vyšetrovanie a analyzovanie incidentu s cieľom:

a) ***určiť podstatné nedostatky***, ktoré by mohli zapríčiniť alebo prispievať k výskytu incidentov,

b) určiť príležitosti na ***preventívne opatrenie,***
c) určiť potrebu ***nápravného opatrenia,***
d) určiť príležitosti na ***trvalé zlepšovanie,***
e) ***komunikovať*** o výsledkoch takéhoto vyšetrovania.

Preventívna činnosť predstavuje činnosť na odstránenie ***príčiny potenciálnej nezhody alebo inej potenciálnej neželateľnej situácie***. Podstatou **prevencie** je vyvolávanie priaznivých a predchádzanie nepriaznivým javom. Z toho vyplýva, že preventívne pôsobenie musí:

- vychádzať z analýzy javu, ktorému treba predchádzať,
- pristupovať k analyzovanému javu z hodnotiaceho hľadiska podľa kritéria javu k integrite a optimálnemu fungovaniu príslušného systému,
- orientovať sa do budúcnosti, z toho dôvodu je spájaná s prognózovaním pravdepodobnosti výskytu príslušného javu,
- pôsobiť zámerne z aspektu cieľov, výberu foriem a metód pôsobenia.

Preventívnym opatrením je ***opatrenie, ktoré sa prijme ako reakcia na udalosť,*** konanie alebo opomenutie, spôsobujúce bezprostrednú hrozbu škody a ktorého účelom je takejto škode predísť alebo ju minimalizovať. Odporúčané preventívne opatrenia majú za úlohu predchádzať incidentom. Mali by zabezpečiť, že bude veľmi nepravdepodobné, alebo dokonca nemožné, aby sa incident opakoval. Napríklad analýza bezpečnosti pracovného postupu by mala byť v súvislosti s hlásením zrevidovaná a zamestnanci znovu vyškolení v rozsahu, ktorý plne zodpovedá odporúčaniam v správe o vyšetrovaní.

Nápravná činnosť predstavuje činnosť na odstránenie ***príčiny zistenej nezhody alebo inej neželateľnej situácie.*** **Náprava** znamená činnosť na odstránenie zistenej nezhody. **Nápravné opatrenie** je akcia alebo kombinácia akcií, vrátane opatrení na zmiernenie následkov alebo dočasných opatrení, ktorých účelom je ***obnova, alebo nahradenie poškodených činností alebo zabezpečenie rovnocennej náhrady za tieto činnosti***. Primárnou nápravou sú nápravné opatrenia, ktorými sa dosiahne obnova činnosti do základného stavu alebo do takmer základného stavu.

Uzavretie incidentu

Po prijatí opatrení na obnovu po incidente je potrebné zistiť veľkosť vzniknutých škôd a riešiť spôsob ich nahradenia. Vyšetrovanie sa musí vykonať v určenom čase. Výsledky z vyšetrovania incidentov sa musia zdokumentovať a udržiavať.

Po zapísaní koncového stavu incidentu do **Záznamu o incidente** je ***incident uzavretý***.

Záverečná správa o vyšetrovaní incidentu obsahuje v jednotnej forme najdôležitejšie údaje a informácie o výsledkoch vyšetrenia príčin incidentu. Správa musí ukázať spôsoby, ako urobiť pracovný postup bezpečným za akýchkoľvek okolností, teda aj v prípade nejakej nepredvídateľnej udalosti. Zvažovanie nákladov alebo technickej obťažnosti v tomto štádiu ešte nie je na mieste.

Po splnení tohto účelu by informácie získané z hlásení mali byť použité na aktualizáciu a revíziu zoznamu rizík a programu prevencie rizík a ich riadenia. Základné príčiny identifikované v správe sa musia analyzovať z hľadiska ich vplyvu na všetky ostatné činnosti a postupy.

Správa o vyšetrovaní incidentu obvykle obsahuje:

A. Úvod – uvedie sa názov (meno) prevádzkovateľa, adresa.

B. Informatívny prehľad:

- stručná a výstižná charakteristika miesta a okolnosti incidentu, dátum incidentu, informácie o zistení a oznámení udalosti,
- zloženie komisie, priebeh vyšetrovania a vypracovania záverečnej správy,
- meno a funkcia osôb predkladajúcich záverečnú správu,
- dátum predloženia Správy o vyšetrovaní incidentu.

C. Hlavná časť správy:

1. Odborné vyšetrovanie incidentu:

a) Pracovisko – postup prác a okolnosti vedúce k incidentu, miesto a čas incidentu.
b) Zranenie osôb – meno, priezvisko, funkcia zranených osôb podľa lekárskej správy, v prípade smrteľného zranenia sa uvedú osoby, ktoré zomreli na priame následky zranenia pri incidente.
c) Svedkovia incidentu.
d) Popis priebehu incidentu – čo sa stalo, vrátane sledu udalostí predchádzajúcich udalosti.
e) Škody – stručný popis priamych škôd, zničenia, prípadne bez poškodenia.
f) Ďalšie škody – v prípade poškodenia iných objektov a zariadení.
g) Popis ďalších súvislostí súvisiacich s incidentom.
h) Výsledky odborného preskúmania – stručné výsledky prípadných testov, skúšok, expertíz.

2. Analýza:

a) rozbor skutočností rozhodujúcich pre určenie záveru a stanovenia príčin incidentu.
b) zo sledu udalostí zistiť, ktoré udalosti boli rozhodujúce v tomto incidente, analýza týchto udalostí môže pomáhať pri určovaní faktorov alebo príčin incidentu.
c) vyhlásenie o príčinách – všetky nebezpečné podmienky, akty, alebo postupy, ktoré akýmkoľvek spôsobom prispeli k incidentu.

3. Závery – text záveru z jednotlivých častí v chronologickom poradí vyšetrovania a stanovia sa všetky príčiny incidentu a prípadne sa rozvedú aj spolupôsobiace okolnosti zistené v celom priebehu vyšetrovania.

4. Opatrenia na zvýšenie bezpečnosti:

a) nápravné opatrenia, ktoré boli prijaté na odstránenie zistených nedostatkov.
b) odporúčané opatrenia na zvýšenie bezpečnosti, aby k podobným incidentom nedochádzalo.

5. Prílohy – záverečná správa sa doplní všetkými údajmi a informáciami, predovšetkým fotografickými a grafickými, ktoré prispejú k plnej zrozumiteľnosti a správnemu pochopeniu jednotlivých častí správy.

Trvalé zlepšovanie

Organizácia musí trvalo zlepšovať efektívnosť systému manažérstva incidentov prostredníctvom využívania:

a) politiky systému manažérstva incidentov,
b) cieľov systému manažérstva incidentov,
c) výsledkov auditu,
d) analýzy údajov,
e) nápravných a preventívnych opatrení,
f) preskúmania manažmentom.

8.6 LITERATÚRA

FILÁK, A. a kol. [2006]: *Základy teorie policejně bezpečnostní činnosti II.* Praha: Police History.

KALUŽA, F. [2011]: *Manažment incidentov informačnej bezpečnosti.* In: Security Revue. Elektronický časopis. Žilina: ŽU, FŠI.

MIKOLAJ, J. – HOFREITER, L. – MACH, V. – MIHÓK, J. – SELINGER, P. [2004]: *Terminológia bezpečnostného manažmentu. Výkladový slovník,* Žilina; ŽU FŠI.

POŽÁR, J. [2006]: *Bezpečnostní situace a identifikace.* In.: Filák, A. a kol.: Základy teorie policejně bezpečnostní činnosti II. Praha : Police History.

SARNOVSKÝ, M. – FURDÍK, K. – ŠKOLOVÁ, E. [2011]: *Riadenie IT prostredia.* Technická univerzita v Košiciach.

STAŠA, P. [2003]: *Prevence a zvládaní bezpečnostních incidentů*. In: IT system 6/2003 Dostupné na: http://www.systemonline.cz/clanky/prevence-a-zvladani-bezpecnostnich-incidentu.htm.

STN EN ISO 9001:2009, *Systém manažérstva kvality.*

9 SYSTÉM OCHRANY PRIESTORU (OBJEKTU)

Ochrana predstavuje **starostlivosť o odvrátenie nebezpečenstva alebo škodlivých vplyvov**, vo význame:

- ***zabezpečenie, zábezpeka:*** ochrana, zabezpečenie, zábezpeka pred povodňou, požiarom,
- ***prevencia (ochrana predchádzaním):*** ochrana pred chorobami, prevencia chorôb.

V druhom význame **ochrana** predstavuje ***prostriedok (osobu, zariadenie a pod.) na chránenie:*** spoľahlivá ochrana, vziať niekoho do ochrany, byť pod ochranou, záštitou.

Protection (ochrana) – v anglickom jazyku mnohovýznamové slovo znamená: akt ochrany alebo stav zabezpečenia; vec, osobu alebo skupinu, ktorá chráni; patronát; poistenie; dokument, ktorý zaisťuje bezpečnosť pred poškodením, oneskorením, alebo iným ohrozením pre osoby alebo majetok.

Safeguard (zabezpečenie, ochrana) predstavuje niečo, čo poskytuje ochranu pred možnou stratou, poškodením atď.

Ochrana v súčasných terminologických slovníkoch predstavuje:

- súhrn opatrení na odvrátenie alebo zmiernenie škodlivých vplyvov a následkov mimoriadnych udalostí a krízových situácií (terminologický slovník bezpečnostného manažmentu),
- súhrn systémových opatrení, činností a prostriedkov na prevenciu a odstránenie následkov súčasných a potenciálnych vnútorných i vonkajších rizík občanov i materiálnych a duchovných hodnôt (terminologický slovník krízového manažmentu).

Z uvedených odlišných definícií možno vytvoriť novú, súhrnnú definíciu: „**Ochrana predstavuje súhrn síl, prostriedkov opatrení a činností systému** na prevenciu a zabezpečenie pred súčasnými i potenciálnymi vonkajšími a vnútornými bezpečnostnými rizikami a na obmedzenie ich následkov“.

Cieľom ochrany v organizácii je:

- použitím režimových bezpečnostných opatrení, procesov (činností) manažérstva bezpečnosti, síl fyzickej ochrany a mechanických a technických ochranných prostriedkov **predchádzať a zabrániť** realizácii možných bezpečnostných rizík vonkajšieho a vnútorného prostredia, schopných spôsobiť ujmy všetkým aktívam (osobám, objektom a chráneným priestorom, informáciám, informačným a komunikačným technológiám, prevádzke alebo životnému prostrediu),
- v prípade, že došlo k aktívnej realizácii rizika, **minimalizovať jeho následky.**

Základom ochrany je **prevencia.**

Ochranu môžeme charakterizovať aj ako **pasívny spôsob odrazenia útoku.**

9.1 OCHRANA PRIESTORU (OBJEKTU)

Pod pojmom priestory možno chápať:

- ***priestory organizácií,*** napr. podniku, závodu, školy, univerzity, nemocnice, železničnej stanice, nákupné centrum a pod.,
- ***areál –*** vymedzená časť územia, napr. pozemky so stavbami, areál výstaviska, areál rekreačného zariadenia, revír (oblasť vymedzená na istú činnosť), rezervácia (chránená oblasť) a pod.
- ***prevádzkareň*** – miesto, dielňa na výrobnú alebo inú hospodársku činnosť,
- ***samostatné objekty***, napr. dom s pozemkom,
- ***vnútorné priestory budov,*** napr. miestnosti, schodiská, terasy, balkóny, výťahy a pod.

V praxi bezpečnostného manažmentu sa uvedené priestory obvykle nazývajú **objekty a chránené priestory.** V nasledujúcich častiach učebnice sa na charakterizovanie ochrany priestoru a objektu bude používať pojem ***ochrana objektu***

Termín **ochrana objektu** nie je v súčasných právnych predpisoch definovaný jednotným spôsobom.

V Zákone č 215/2004 Z. z. o ochrane utajovaných skutočností sa uvádza termín – **ochrana objektov a chránených priestorov** – ktorá sa zabezpečuje mechanickými zábrannými prostriedkami, technickými zabezpečovacími prostriedkami, fyzickou ochranou, režimovými opatreniami a ich vzájomnou kombináciou v súlade s bezpečnostným štandardom fyzickej bezpečnosti a objektovej bezpečnosti.

Vo Vyhláške NBÚ č. 336/2004 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti sa uvádzajú oddelene:

- **ochrana objektu,** ktorá sa zabezpečuje *vybranými* mechanickými zábrannými prostriedkami a technickými zabezpečovacími prostriedkami,
- **ochrana chráneného priestoru určeného na ukladanie utajovaných skutočností,** ktorá sa zabezpečuje *všetkými* tu uvedenými mechanickými zábrannými prostriedkami a technickými zabezpečovacími prostriedkami.

V Zákone č. 45/2011 Z. z. o kritickej infraštruktúre sa na **ochranu prvku kritickej infraštruktúry** uvádzajú ako bezpečnostné opatrenia najmä mechanické zábranné prostriedky, technické zabezpečovacie prostriedky, bezpečnostné prvky informačných systémov, fyzická ochrana, organizačné opatrenia, kontrolné opatrenia a ich vzájomná kombinácia.

V Zákone č. 541/2004 Z. z. o mierovom využívaní jadrovej energie (atómový zákon) je uvedený tiež pojem **fyzická ochrana.**

Vo Výkladovom slovníku bezpečnostného manažmentu sa pod pojmom **ochrana objektu** chápe ***súhrn bezpečnostných, technických i režimových opatrení***, ktoré vedú k prekazeniu **nepriateľskej činnosti proti *objektu či osobám*** nachádzajúcich sa v chránenom objekte. Cieľom je zabrániť útoku na osoby či majetok *(Mikolaj a kol., 2004).*

Podľa Falisovej **ochranou objektu** je ***bezpečnostné opatrenie na zabránenie neoprávnenému prístupu nepovolaných osôb do objektu a zabránenie útokom na majetok.*** To znamená predchádzanie krádežiam a poškodzovaniu majetku, úniku utajovaných skutočností a vzniku mimoriadnych udalostí *(Falisová, 1997).*

V anglicky hovoriacich krajinách sa systém ochrany najčastejšie označuje ako systém **fyzickej ochrany** *(Physical Protection System).* Ide o systém, ktorý **integruje ľudí, prostriedky a postupy *na ochranu osôb a majetku pred širokým rozsahom bezpečnostných rizík***, napr. pred násilnou činnosťou (krádež), ohňom, haváriou, špionážou, sabotážou, zniče-

ním a napadnutím. Vytvára sa na prevenciu, ochranu a reakciu na krádež, sabotáž, škodlivú činnosť alebo iné útoky.

Obsah všetkých uvedených definícii je, napriek niektorým odlišnostiam, v podstate rovnaký, preto sa pre zjednotenie budú v ďalšej časti učebnice uvádzať pojmy „**ochrana objektu“** a **„systém ochrany objektu“**. Tým sa myslí priestor organizácie, objekt spoločne s chránenými priestormi, ale aj prvok kritickej infraštruktúry.

Zameranie ochrany je závislé od charakteru priestoru (objektu), ktorý je treba chrániť. V predajni sa napr. ochrana týka najmä krádeží alebo nepoctivosti zamestnancov (drobné krádeže, sprenevera, podvod). Všeobecný súbor kategórií, ktoré majú byť chránené zahŕňa:

- osobnú bezpečnosť osôb v organizácii, napr. zamestnancov a zákazníkov,
- hmotný majetok, napr. v podniku vybavenie, hotové výrobky, hotovosť, cenné papiere,
- nehmotný majetok, napr. utajované informácie rôznych stupňov, či komerčné informácie súkromnej organizácie (výrobné tajomstvo),

Rozdiel medzi systémom ochrany a verejnými bezpečnostnými službami ako sú polícia a hasičské jednotky je v uplatňovaní pasívnych a preventívnych opatrení.

Vo väčšine objektov existujú štyri typy fyzických cieľov na ktoré sa môže zameriavať úmyselná násilná činnosť páchateľov:

- **osoby** – zamestnanci, fyzická ochrana (strážni), návštevníci,
- **majetok** – aktíva, súhrn všetkých vecí, ktoré niekomu patria: hotovosť, zásoby, vybavenie, informačný systém, utajované skutočnosti a pod.,
- **infraštruktúra** – ***budovy*** (sklady, garáže, predajné miesta, administratívna budova, výrobné haly a pod.), ***technické zariadenia budov*** (kanalizácia, vodovod, plynovod, vykurovanie).
- **životné prostredie** – skládky, znečistenie vodných zdrojov a pod.

Ochrana objektov môže byť **jednoduchá,** napr. zamknuté dvere alebo **zložitá,** napr. viac vrstiev prekážok, ozbrojená bezpečnostná služba, či umiestnenie strážnice. Bezpečnostné opatrenia nevyhnutne vyžadujú náklady a v skutočnosti nikdy nemôžu byť dokonalé alebo kompletné – môžu zvýšiť bezpečnosť, ale nemôžu úplne vylúčiť riziko.

Vzhľadom na to, že tieto opatrenia sú nedokonalé, silné ochranné zabezpečenie uplatňuje **zásadu ochrany do hĺbky** pomocou ***vhodných kombinácií prekrývania*** a ***dodatočných kontrol.*** Ochrana objektu sa realizuje použitím **viacerých vrstiev** navzájom prepojených ochranných systémov, najmä použitím *fyzickej ochrany, mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov, režimových opatrení a ochrany pred požiarmi, technickými a inými haváriami a živelnými pohromami*.

Ochrana objektov sa jednoznačne netýka iba ochrany pred ľuďmi. V praxi je často potrebné aktívne brániť územie proti narušiteľom z živočíšnej ríše. Súčasné spôsoby ochrany sa neustále zdokonaľujú, pretože technológia sa neustále vyvíja spolu s rizikami. Ochranné opatrenia, ktoré boli v minulosti považované za dostatočné, bývajú v súčasnosti často nepostačujúce, pretože dochádza k stálemu pokroku vo vedomostiach a schopnostiach útočníkov. V súčasnosti existuje veľké množstvo firiem, ktoré ponúkajú ***integrované systémy ochrany objektov a priestorov***.

9.1.1 Systém ochrany objektu

Podľa Zákona o ochrane utajovaných skutočností **fyzická bezpečnosť a objektová bezpečnosť** predstavuje systém opatrení, určených na ***ochranu utajovaných skutočností*** pred nepovolanými osobami a pred neoprávnenou manipuláciou **v objektoch a chránených priestoroch,** ***ktoré sú určené na ukladanie a manipuláciu s utajovanými skutočnosťami, s rôznym stupňom utajenia*****.**

Zásady fyzickej bezpečnosti a objektovej bezpečnosti uvedené v tomto zákone majú okrem **ochrany objektov a chránených priestorov s uloženými utajovanými skutočnosťami** svoj **význam** aj pri ***ochrane priestorov,*** v ktorých ***sú uložené všetky ďalšie aktíva organizácie***.

Tieto zásady sa primerane vzťahujú aj na **ochranu všetkých aktív v objektoch a priestoroch**, tzn. na ochranu **osôb a majetku** pred akoukoľvek ujmou, spôsobenou predovšetkým **násilným napadnutím** (napr. krádeže, vandalizmus, teroristické útoky, špionáž), ktoré môže mať za následok škody na majetku alebo poškodenie zdravia a života osôb.

Systém ochrany objektu sa vytvára s cieľom pripraviť bezpečnostné opatrenia na:

- ***zabránenie neoprávneného prístupu nepovolaných osôb*** (narušiteľov) do objektov a priestorov organizácií, k jej zariadeniam, vybaveniu, zdrojom a všetkým ďalším hodnotám, ktoré sú v nich umiestnené,
- ***ochranu osôb a majetku*** pred ublížením alebo inou ujmou (špionáž, krádež, teroristický útok).

V **systéme ochrany objektu** je potrebné rozlišovať:

- ***ochranu pred úmyselným konaním človeka,***
- ***ochranu pred náhodnými bezpečnostnými rizikami****, ako sú živelné pohromy (zemetrasenia, tornáda alebo záplavy), havárie (požiar alebo elektrická porucha), riziká BOZP* a pod.

- Medzi konštrukciou uvedených druhov ochrany objektu je významný rozdiel, pretože na rozdiel od ľudských páchateľov, **náhodné bezpečnostné udalosti** podliehajú určitým zákonitostiam a dajú sa v mnohých prípadoch vysvetliť a predvídať. Naopak, **ľudský páchateľ** má možnosť: rozhodnúť sa či zaútočí, môže sa prispôsobiť a prípadne prekonať aj ochranné opatrenia. V ďalšej časti sa bude riešiť len ochrana objektu pred úmyselným konaním človeka.

Účinný **systém ochrany objektu pred úmyselným konaním človeka** má poskytnúť adekvátnu ***ochranu proti každému riziku, na všetkých možných smeroch postupu narušiteľa*** (nad, pod, okolo, priamo).

Štruktúru systému ochrany objektu tvoria:

1. **Ľudské zdroje.**
2. **Režimové opatrenia na ochranu objektu.**
3. **Prostriedky ochrany.**

Ľudské zdroje, ktoré sa podieľajú na ochrane objektu tvoria:

a) **manažéri v riadiacom orgáne bezpečnosti,** zameraní na ochranu objektov,
b) **manažéri,** zodpovední za jednotlivé objekty,
c) **bezpečnostný manažér,**
d) **príslušníci centrálneho útvaru bezpečnosti,** zameraní na ochranu objektov,
e) **facility manažér,**
f) **fyzická ochrana** (z vlastných alebo prenajatých zamestnancov):
   - vedúci výkonu fyzickej ochrany,

- vedúci objektu fyzickej ochrany,
- vedúci zmeny fyzickej ochrany,
- pracovníci fyzickej ochrany, strážni, ktorí vykonávajú stráženie a hliadkovanie,
- pracovník fyzickej ochrany (ochranca dôležitej osoby v objekte),
- operátor strediska registrácie poplachov (pult centralizovanej ochrany),
- členovia zásahovej skupiny.

Prostriedky ochrany objektu podľa Vyhlášky NBÚ č. 336/2004 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti predstavujú:

1. **Mechanické zábranné prostriedky** (MZP):
   a) **bezpečnostné úschovné objekty,**
   b) **uzamykacie systémy a ich súčasti,**
   c) **dvere a ich súčasti,**
   d) **mreže,**
   e) **bezpečnostné fólie,**
   f) **okná,**
   g) **zasklenia.**
2. **Technické zabezpečovacie prostriedky** (TZP):
   a) **systémy na kontrolu vstupov do objektov a systémy slúžiace na elektronické preukazovanie totožnosti a oprávnenosti osôb,**
   b) **elektrické zabezpečovacie systémy (poplachové systémy na hlásenie narušenia),**
   c) **kamerová zostava v rámci uzatvoreného televízneho okruhu,**
   d) **tiesňové systémy,**
   e) **zariadenia na detekciu látok a predmetov,**
   f) **zariadenia fyzického ničenia nosičov informácií.**

Druhy a charakteristika **mechanických zábranných prostriedkov** sú v plnom rozsahu uvedené v učebnici:

- MACH,V. [2010]: *Bezpečnostné systémy. Mechanické bezpečnostné prostriedky*. Žilina. EDIS - vydavateľstvo ŽU v Žiline. ISBN: 978-80-9704-106-9

Druhy a charakteristika **technických zabezpečovacích prostriedkov** sú v plnom rozsahu uvedené v učebniciach:

- VEĽAS, A. [2010]: *Elektrické zabezpečovacie systémy.* Žilina. EDIS - vydavateľstvo ŽU v Žiline, ISBN 978-80-554-0224-6.
- LOVEČEK, T. – NAGY, P. [2008]: *Bezpečnostné systémy. Kamerové bezpečnostné systémy.* Žilina. EDIS- vydavateľstvo ŽU v Žiline . ISBN 978-80-807-0893-1.
- LOVEČEK,T., REIŠPÍS, J. [2012]: *Projektovanie a hodnotenie systémov ochrany objektov.* Žilina: EDIS, vydavateľstvo ŽU v Žiline. ISBN: 978-80-554-0457-8
- LOVEČEK, T. – VEĽAS, A. – ĎUROVEC, M. [2015]: *Bezpečnostné systémy. Poplachové systémy.* Žilina: EDIS- vydavateľstvo ŽU v Žiline .

9.2 FUNKCIE OCHRANY OBJEKTU

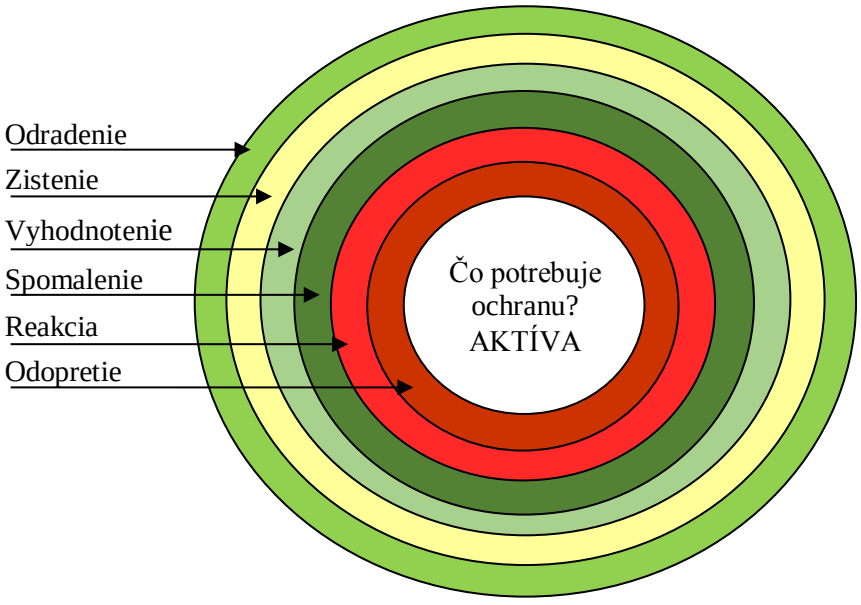
Systém ochrany objektu pred násilným napadnutím sa plánuje podľa princípu lúpania cibule *(onion-peeling principle)* nazývaný 4 D:
D eter – odradenie, odstrašenie,
D etect – zistenie, detekcia, odhalenie,
D elay – oneskorenie, spomalenie, zdržanie,
D efeat – zmarenie, prekazenie.

Hlavné funkcie, ktoré potom plní Systém ochrany objektu sú uvedené v tab. 4.

Tab. 4 Hlavné funkcie Systému ochrany objektu

Detect - zistenie	**Delay – oneskorenie**	**Response – reakcia, odozva**
• detekcia narušenia • prenos poplachového signálu • vyhodnotenie narušenia • kontrola vstupu	• pasívne fyzické prekážky • aktívne prekážky – fyzická ochrana,	**a. prerušenie** • vyžiadanie zákroku síl reakcie • zákrok síl reakcie **b. zneškodnenie**

Kibbey *(2004)* uvádza, že ochrana objektov pred násilným napadnutím má plniť nasledujúce funkcie (obr.23):
1. **Odradenie (odstrašenie)** potenciálnych narušiteľov *(deterrence)*,
2. **Zistenie** vniknutia a monitorovanie narušiteľa *(detection)*,
3. **Vyhodnotenie** zistených údajov *(assessment)*,
4. **Spomalenie, oneskorenie, zdržanie** narušiteľa *(delay)*,
5. **Reakcia, odozva** *(response)*,
6. **Odopretie, odmietnutie** *(denial)*.



Obr. 23 Funkcie Systému ochrany objektu (zdroj Kibbey, 2004)

Odradenie

Zavedenie systému ochrany objektu vníma potenciálny narušiteľ ako psychologickú prekážku. Odradenie potenciálnych narušiteľov znamená preventívnu činnosť na vyvolanie obavy z možných následkov z pohľadu činiteľov potenciálneho napadnutia. Cieľom metód odradenia je presvedčiť potenciálnych útočníkov, že úspešný útok je nepravdepodobný vzhľadom na silnú obranu. Ak narušiteľ zistí, že môže byť pristihnutý, orientuje sa pravdepodobne na iný cieľ.

Funkciu odradenia plnia hlavne viditeľné, masívne mechanické zábranné prostriedky, strážne psy, pracovníci strážnej služby, viditeľne umiestnené prvky elektrických zabezpečovacích i kamerových systémov *(Hofreiter, 2013).* Systém ochrany musí pôsobiť proti osobám konajúcich násilnú alebo inú nežiaducu činnosť proti objektu svojimi vonkajšími viditeľnými znakmi, ako je: oplotenie, osvetlenie, kamery, aktivity fyzickej ochrany, varovné nápisy a označenia, legenda v mieste a pod.

Na zvýšenie účinku je možné:

- **Zviditeľniť niektoré prvky ochrany** – výstražné označenie, obchádzky hliadok, dobré osvetlenie.
- **Podporovať prejavy vysokej úrovne bezpečnosti** – pravidelné bezpečnostné nácviky, ktoré ukazujú páchateľovi dobrú pripravenosť a vybavenie na riešenie takýchto situácií a v publikáciách poukazovať na vysokú úroveň bezpečnosti v zariadení.
- **Zverejniť a presadzovať tvrdé tresty za pokus o krádež alebo sabotáž** – zverejňovať informácie o tých, ktorí boli potrestaní za porušenie bezpečnostných pravidiel a systému, ktorý podporuje vysokú bezpečnosť.

Zistenie

Zistenie vniknutia a monitorovanie narušiteľa znamená ***odhalenie a oznámenie,*** že došlo k vniknutiu alebo pokusu o vniknutie. To zahŕňa zistenie skrytého alebo zjavného vniknutia do zariadenia nasledovným postupom:

1. Snímač reaguje na podnety a **zistí narušenie.**
2. **Informácie zo snímača sa prenášajú na zobrazenie.**
3. Človek **vyhodnotí** informácie a rozhodne, či ide o narušenie (detekcia bez hodnotenia nie je považovaná za detekciu).

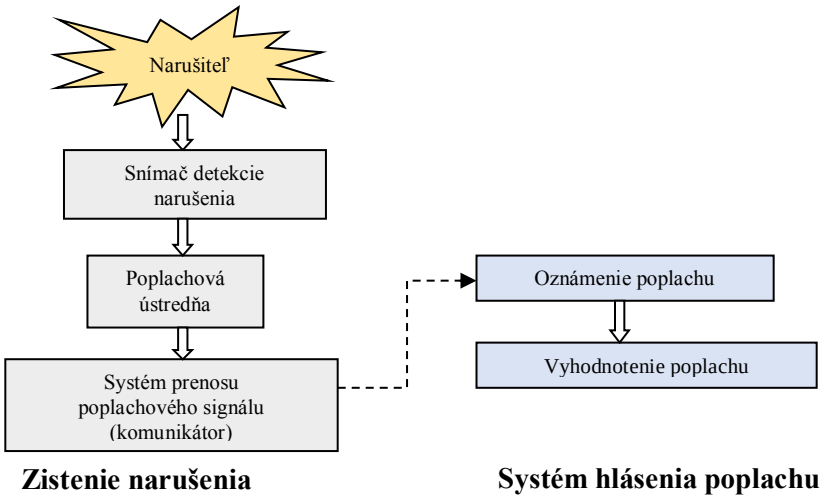
Schopnosť zisťovania osobným pozorovaním sa zvyšuje využitím technológií, čím sa v podstate dá zistiť vniknutie v ktoromkoľvek mieste. Poplachové systémy pracujú v tandeme s fyzickými bariérami, mechanickými systémami a fyzickou ochranou, slúžia na spustenie reakcie, keď boli porušené tieto iné formy zabezpečenia. Používajú sa rôzne **snímače,** napr. ***vonkajšie obvodové senzory, dverové senzory, kontaktné senzory, snímače pohybu, detektory rozbitia skla*** a pod.

V súčasnosti sa na trhu zvyšuje počet vonkajších a vnútorných senzorov pre zistenie narušenia. Sú navrhnuté tak, aby reagovali na špecifické podnety, a sú klasifikované podľa rôznych hľadísk. Odporúčané postupy pre zisťovanie sú:

- K zisteniu musí dôjsť čo najskôr (pred oneskorením), aby sa mohlo reagovať a prerušiť činnosť páchateľa.
- Systémy na zisťovanie musia byť správne inštalované a integrované.
- Konštrukcia systému zisťovania by mala zahŕňať doplnkové technológie tak, aby páchateľ mohol byť zistený rôznymi metódami.
- Detekčný systém by mal mať odolnosť proti rušeniu a falošným poplachom, s vysokou pravdepodobnosťou zistenia.

- Systém by mal byť projektovaný na zisťovanie zásahov páchateľa.
- Systém by mal byť spoľahlivý a odolný pre životné prostredie.
- Systém by mal byť ošetrovaný a jeho údržba overená testovaním.
- Detekčný systém musí byť kombinovaný s dobrým systémom ***hodnotenia*** (nie zistenie bez vyhodnotenia).

Postup zistenia a hlásenia narušenia je uvedený na obr. 24.



Obr. 24 Postup zistenia a hlásenia narušenia

Vyhodnotenie

Vyhodnotenie údajov predstavuje **posúdenie narušenia osobou** bezprostredne na mieste alebo prostredníctvom technológií – obyčajne prostredníctvom ***priemyselnej televízie*** (CCTV). Vyhodnotenie či ide o narušenie osobou, zvieraťom, vtákom alebo poveternostnými vplyvmi je potrebné na určenie oprávnenosti poplachu a zodpovedajúcej reakcie.

Spomalenie

Spomalenie alebo oneskorenie, zdržanie, prekazenie znamená v zásade prevenciu pokusom o prienik. Ide o schopnosť fyzických alebo psychických prekážok obmedziť pohyb a spomaliť postup narušiteľa. Účelom oneskorenia je poskytnúť dostatočný čas silám reakcie na reakciu a prerušenie jeho činnosti.

Osvedčené postupy spomalenia:

- vyvážené využitie technických prostriedkov a / alebo ochranných síl personálu,
- rozmiestnenie prvkov fyzickej ochrany na spomalenie, menej nákladné je umiestniť ich pri nebezpečenstve krádeže bližšie, pri nebezpečenstve sabotáže ďalej od chráneného prvku,
- prvky spomalenia umiestniť na základe zraniteľnosti definovanej pri identifikácii rizík,
- viac technológií na spomalenie páchateľa je potrebné využiť pri ochrane dôležitých aktív,
- prvky na spomalenie začleniť do dizajnu zariadenia tak, aby neboli nápadné,
- overenie veľkosti spomalenia sa môže vykonať testovaním alebo simuláciou a modelovaním,
- systém spomalenia umiestniť na možné smery vniknutia páchateľa, čo umožní, aby sily reakcie efektívnejšie prerušili jeho činnosť,
- pred spomalením je treba vždy zistiť páchateľa, spomalenie nie je účinné, kým nie je zistený páchateľ, pretože časy na spomalenie sú obmedzené.

Na spomalenie sa podľa tab. 5 okrem síl fyzickej ochrany vo väčšom rozsahu využívajú **vonkajšie technické prostriedky, *špeciálne vyrábané na tento účel***, medzi ktoré patria:

- ***mechanické zábranné prostriedky obvodovej ochrany,***
- ***poplachové prvky obvodovej (perimetrickej) ochrany***

Tab. 5 Charakteristika prvkov spomalenia

Sily fyzickej ochrany – stráže	Prekážky	Disponibilné prekážky
• flexibilné, • vyžadujú trvalé prevádzkové náklady, • závisia na počte strážnych, • sú schopné komunikovať a dohodnúť sa.	**Trvalé vlastnosti:** • dajú sa prekonať, • komerčne dostupné, • slabé proti výbušninám. **Prevádzkové vlastnosti:** • obmedzujú výhľad.	**Možnosť napojenia:** • možnosť rýchleho nasadenia, • maximalizácia oneskorenia, • „akoby“ závislé na hrozbe.

Reakcia

Reakcia, odpoveď znamená iniciovanie vhodnej ***reakcie*** na narušenie. Funkciu reakcie musí zahŕňať každý účinný systém ochrany objektov. Funkciu reakcie, resp. odpovede plní zásahová jednotka fyzickej ochrany v objekte. Zásahová jednotka ***súkromnej bezpečnostnej služby*** môže v súlade s oprávneniami obmedziť útočníka na slobode, naopak zásahová jednotka ***policajného zboru*** môže útočníka zadržať. V prípade vplyvu iných druhov nebezpečnestva sa reakciou rozumie ***zásah jednotky hasičského a záchranného zboru, jednotiek civilnej ochrany, pyrotechnikov, zdravotnej záchrannej služby*** a pod. *(Hofreiter, 2013).*

Významy pojmov „reakcia“ alebo „sily reakcie“ sú v jednotlivých krajinách odlišné a líši sa aj ich chápanie v jednotlivých zariadeniach. Časť, alebo všetky sily reakcie môžu byť umiestnené mimo objektu, môžu ich tvoriť vlastné kvalifikované tímy reakcie alebo príslušníci SBS. Bez ohľadu na rozdiely v prístupe, musia sily reakcie zabrániť páchateľovi dosiahnuť svoj cieľ. Sila reakcie musí pôsobiť na jednoznačnom právnom základe. Funkcia reakcie zahŕňa: ***reakciu personálu, núdzové plánovanie, komunikáciu a prerušenie.***

Núdzové plánovanie znamená tvorbu postupov na zisťovanie potenciálnych páchateľov, reakciu na rôzne nebezpečné udalosti, komunikovanie s externými organizáciami a určenie, aké veľké strážne sily možno použiť v rôznych situáciách. Hneď po identifikovaní potenciálnych cieľov bezpečnosti, môžu bezpečnostní pracovníci vyhodnotiť pravdepodobné trasy vniknutia páchateľov a rozvíjať taktické plány na riešenie rôznych rizík pre zariadenia a stanovenie plánov stráženia a trasy strážnej hliadky. Postupy a plány strážnej činnosti v prípade napadnutia by mal byť dobre zavedené v praxi prostredníctvom pravidelných cvičení. Ak je plán hotový, mali by sa pripraviť a uskutočniť spoločné nácviky reakcie na napadnutie.

Komunikácia je dôležitou súčasťou funkcie reakcie, pretože na rozdiel od všetkých ostatných funkcií systému ochrany je reakcia silne závislá na správnej komunikácii medzi celým zodpovedajúcim personálom. Informácie musia byť odovzdané prostredníctvom tejto siete rýchlo a presne. Ide o informácie o možných napadnutiach a inštrukcie pre nasadenie. Najbežnejší spôsob komunikácie síl reakcie je otvorenou rečou, bez šifrovania alebo kódovania, využitím malých prenosných vysielačiek alebo mobilu.

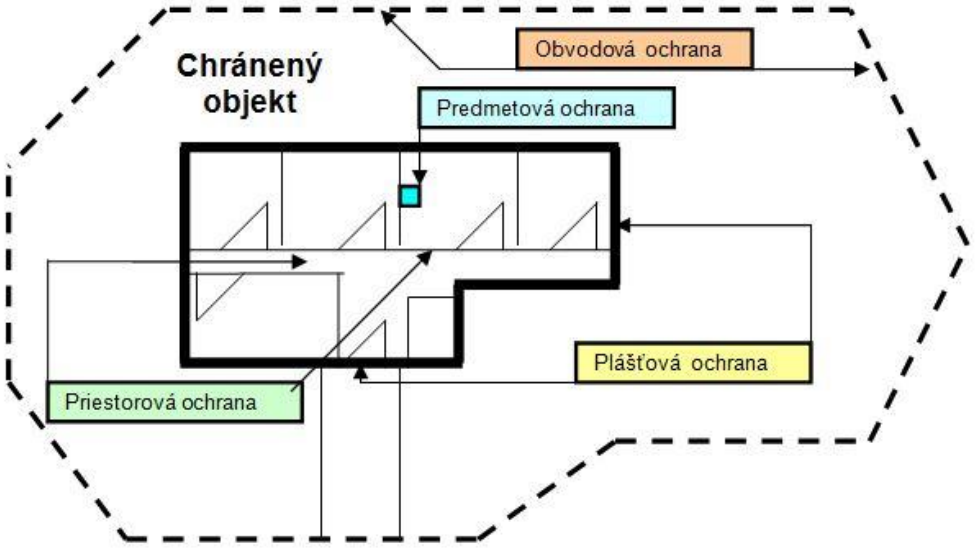
Prerušenie je poslednou časťou funkcie reakcie. Znamená úspešný zásah síl reakcie na mieste narušenia páchateľom. Pravdepodobnosť úspešného prerušenia môže byť zvýšená využitím známych, chránených ciest.

Odmietnutie znamená ***schopnosť postaviť sa proti alebo negovať účinky narušenia*** – skutočného alebo predstieraného pôsobenia. Odmietnutie je definitívna a posledná šanca, ako prekaziť činnosť protivníka.

9.3 VRSTVY OCHRANY OBJEKTU

Vrstvy ochrany objektu pred úmyselným napadnutím podľa obr. 25 tvoria *(Mach, 2012):*

1. **Obvodová ochrana.**
2. **Plášťová ochrana.**
3. **Priestorová ochrana.**
4. **Predmetová ochrana.**



Obr. 25 Vrstvy (zóny) ochrany objektu (zdroj Mach, 2012)

9.3.1 Obvodová ochrana

Obvodová ochrana *(perimetrická)* ***zaisťuje bezpečnosť*** okolo chráneného objektu a ***signalizuje narušenie*** obvodu objektu.

Obvod objektu *(perimeter)* môže byť vymedzený prírodnou (vodné toky) alebo umelou hranicou (plot, stena a iné). V závislosti od typu zariadenia môže obvodová ochrana zahŕňať *chodníky, cesty, parkoviská, zariadenia mimo múrov objektu, predsieň, alebo dvere kancelárie.* Obvodové bezpečnostné normy sa týkajú oblastí mimo zariadenia.

Cieľom ochrany objektu je presvedčiť možných útočníkov, že pravdepodobná cena útoku prekračuje hodnotu, na ktorú má smerovať útok, napr. že následky prerušenia útoku môžu prevyšovať zisk. Možnosti ochrany objektu zvýši kombinácia niekoľkých vrstiev bezpečnostných opatrení.

Prvá vrstva ochrany objektov ***je určená na prevenciu napadnutia*** prostredníctvom ***úpravy okolia na odradenie (odstrašenie) možných útočníkov***. Takmer vždy sa využívajú vonkajšie technické prostriedky, *špeciálne vyrábané na tento účel*, medzi ktoré patria:

- ***mechanické zábranné prostriedky obvodovej ochrany,***
- ***poplachové prvky obvodovej (perimetrickej) ochrany.***

Mechanické zábranné prostriedky obvodovej ochrany

Ide o mechanické zábranné prostriedky, ktoré sú zriadené mimo vlastného chráneného objektu (budovy) na okolitej voľnej ploche. Obvykle priamo vizuálne charakterizujú hranicu pozemku, ktorý patrí k budove, a tak vytvárajú **právnu hranicu.** Väčšinou sa používa oplote-

nie alebo ohradenie okolitého pozemku vrátane bránok, brán, závor, priepustov, ktoré obmedzujú alebo zabraňujú prístupu nežiaducich osôb na chránené územie. Tieto mechanické prekážky môžu byť podľa stupňa zaistenia doplnené o detekčné a monitorovacie systémy.

Mechanické zábranné prostriedky obvodovej ochrany je možné rozdeliť do šiestich základných skupín *(Gymerská, 2003)*: ***klasické drôtené oplotenie; bezpečnostné oplotenie; vysoko bezpečnostné oplotenie; vrcholové zábrany; prekážky proti podhrabaniu; vstupy, vjazdy a iné vstupné jednotky.***

Najčastejšie sa využívajú prostriedky, špeciálne vyrábané na tento účel, napr.: ***výstražné znamenia alebo ohrady, návestné závory, návestné obmedzovače, bezpečnostné osvetlenie priestorov, fyzické bariéry a priekopy, rôzne druhy oplotenia, vyhradené miesta vstupu, vjazdy a vstupy do chráneného priestoru – brány, bránky, turnikety, bezpečnostné priepusty, závory, klincové bariéry, zastavovacie pásy*** a pod.

Poplachové prvky obvodovej ochrany

Prvky obvodovej ochrany zabezpečujú signalizáciu pri násilnom vniknutí cez okno, dvere alebo pozemok do stráženého priestoru: Sú to snímače, ktoré chránia, resp. signalizujú narušenie vonkajšej časti rozľahlých objektov, komplexov budov alebo tovární na samostatnom pozemku. Konštrukcia vonkajších snímačov zodpovedá vonkajšiemu prostrediu, tak sa samozrejme odlišuje od častí zabezpečovacieho systému, ktoré sú umiestnené vnútri budovy. Vzhľadom na dimenzie vonkajších priestorov sa odlišujú od snímačov pre vnútorné použitie najmä v dosahu. Ak sú funkčné dosahy vnútorných snímačov rádovo 10 metrov, pri vonkajších ide rádovo o 100 metrov.

Všeobecne sa rozlišujú tieto hlavné detekčné systémy:

a) detekčný systém plota – ide buď o senzory integrované v plote alebo namontované na plote (spínač inštalovaný vrchnej tretine plota – chráni pred prelezením, ťažný spínač, ku ktorému vedú odporové drôty napojené na vyhodnocovaciu elektroniku natiahnuté na plote – proti prestrihnutiu, vodiče svetelných vĺn v pletive – proti prelezeniu, senzory zvuku telesa, senzory otrasov vibrácie) plotov,

b) zemné detekčné systémy – Ide o tlakové senzory, seizmické senzory (geofóny), zakopané koaxiálne káblové detektory,

c) systém elektrického poľa – je zložený z elektródového plota, vysielača a prijímača. Ak prenikne osoba do elektrického poľa medzi vysielacím a prijímacím drôtom a zemou, zmení sa kapacita, čo spôsobí vyhlásenie poplachu.

Na ochranu plotov možno využiť *nízkofrekvenčný kábel, infrazávory, mikrovlnné závory, zemné káble a tlakové hadice.*

9.3.2 Plášťová ochrana

Plášťová ochrana ***zabraňuje akémukoľvek narušeniu plášťa objektu a jeho všetkých otvorových výplní a signalizuje narušenie plášťa objektu.*** Ide o **vnútorné bezpečnostné prvky** – ***mechanické, elektronické a procesné riadenie prístupu.***

Plášť objektu tvoria ***stavebné prvky budov*** a ***otvorové výplne.*** **Plášťová ochrana** je zameraná predovšetkým na stavebné otvory budovy (dvere, okná atď.) pred vniknutím páchateľa *(Mach, 2012).* Vstupné bezpečnostné štandardy, ktoré sa vzťahujú na bezpečnostné otázky týkajúce sa vstupu do zariadení, riešia:

a) riadenie vstupu a výstupu zamestnancov a návštev,
b) riadenie príjmu a expedície (pošty, zásielok, tovaru, materiálu,...),
c) riadenie vjazdu a výjazdu dopravných prostriedkov (automobil, vlak, loď),
d) ochranu vchodov a východov proti vstupu nepovolaných osôb.

Mechanické zábranné prostriedky plášťovej ochrany a priestorovej ochrany

Základnými zabezpečovacími prvkami plášťovej ochrany sú ***mechanické zábranné systémy,*** ktorých úlohou je sťažiť a prakticky znemožniť vniknutie páchateľa do chráneného priestoru v objekte, poprípade ho odradiť od tejto činnosti. **Mechanická ochranná vrstva** obsahuje ***brány, dvere, zámky a kľúče.*** Pri veľkom počte používateľov sú kľúče problémom, stávajú sa neovládateľné.

Stavebné prvky budov sú dôležitými prvkami mechanickej plášťovej ochrany objektov, medzi, ktoré patria: ***múry, podlahy, stropy a strechy budov.*** Ich mechanická odolnosť proti prielomu je závislá od použitého materiálu, jeho pevnosti, hrúbke a vlastnom vyhotovení. Z hľadiska kvalitného zaistenia plášťovej ochrany objektu je potrebné zamerať pozornosť predovšetkým na:

a) vonkajšie obvodové múry budov, stropy a podlahy, ktoré tvoria ich vonkajšiu hranicu,
b) strechy prízemných budov, najmä stavieb, kde strecha je súčasne stropom objektu.
c) ľahké stavby – ohraničujúce skorej priestor, ktorých pasívna bezpečnosť je veľmi nízka a sú pre kvalitné bezpečnostné zaistenie nevhodné (sádrokartón, priečky z dutých tehál, betónové múry hrúbky do 50 mm, pórobetónové murivo a pod.),
d) pevné stavebné konštrukcie, ktoré majú vzhľadom na použité stavebné materiály a hrúbku, veľkú odporovú odolnosť.

Otvorové výplne sú výplne stavebných otvorov (dvere, okná, vikier) v plášti budovy, bez ktorých objekt nemôže byť. Otvorové výplne sa dajú rozdeliť na: ***vstupné otvorové výplne; okná a balkónové dvere; mreže, rolety a žalúzie.*** Tieto otvorové výplne predstavujú stále potenciálne nebezpečenstvo, lebo bez kvalitného zaistenia sa relatívne ľahko prekonávajú.

Mreže sú klasickým spôsobom ochrany najmä zasklených otvorových výplní a plôch. Mreže sa ***rozlišujú z hľadiska ukotvenia, otvárania, umiestnenia ovládania a materiálu.***

Najznámejšími a najviac používanými mechanickými prvkami bezpečnostných systémov sú **uzamykacie prvky**. Ich základom je ***zámok*** – technické zariadenie k dočasnému spojovaniu, uzatváraniu alebo zaisťovaniu pohyblivých častí zábranných mechanizmov.

Doplnkové mechanizmy tvoria prvky a zariadenia, ktoré dopĺňajú pasívnu bezpečnosť vstupných otvorových výplni z hľadiska ich pasívnej bezpečnosti. Aplikácia týchto mechanizmov môže byť samostatná podľa jednotlivých druhov a typov alebo ich vzájomnou kombináciou podľa účelu využívania vstupných dverí za účelom chráneného záujmu. Doplnkové mechanizmy tvoria:

a) Prídavné zámky – doplnkové uzamykacie zariadenia dverového zapusteného zámku, ktorý rozširuje uzamykací systém dverí.
b) Bariérové závory – svojou konštrukciou a umiestnením podstatne zvyšujú pasívnu bezpečnosť dverí, a to predovšetkým proti ich násilnému vyrazeniu a vysadeniu zo závesov.
c) Zábrany proti násilnému vyrazeniu dverí – z hľadiska pasívnej bezpečnosti dverí sú dôležitým prvkom, nakoľko závesy sú kritickým miestom dverových krídel.
d) Poistné retiazky dverí – zariadenia umožňujúce potvorenie dverí na definovanú vzdialenosť a v tejto polohe dvere zaistiť tak, aby nedošlo k násilnému vniknutiu nepovolanej osoby, prípadne napadnutiu osoby.
e) Dverové zarážky – sú určené na vymedzenie vzdialenosti pri otvorení dverí. Upevňujú sa na vnútornú spodnú časť dverí.
f) Dverové priezory – dôležité z hľadiska vizuálneho pozorovania priestoru pred dverami a zistenia osôb dožadujúcich sa otvorenia dverí.

Poplachové prvky plášťovej ochrany

Stále častejšie sa pristupuje k **elektronickému riadeniu vstupu**, ktoré je vhodné aj pre veľkú skupinu používateľov, kontroluje časy vstupu a výstupu, dátumy a miesta vstupu jednotlivcov. Prvky plášťovej ochrany sú určené na stráženie otvárania alebo na kontrolu priestupov plášťa budovy, t. j. okien, brán a dverí. Patria sem najmä:

a) **detektory pohybu, zvuku, rozbitia skla,**
b) magnetické, mechanické, vibračné, drôtové **snímače,**
c) poplachové **fólie** a poplachové **sklá,**
d) **rozperné tyče.**
e) **osobné tiesňové hlásiče,**
f) **prvky poplachovej prenosovej cesty,**
g) **výstupná signalizácia,**
h) **rôzne druhy kamerových (CCTV) systémov,**
i) **systémy kontroly *vstupu a dochádzky a iné.***

Inou formou riadenia prístupu je **využitie režimových opatrení *na riadenie prístupov*** do zakázaných priestorov. Príkladom je ***rozmiestnenie bezpečnostného personálu*** na určené miesta vstupu. Režimové opatrenia sa na riadenie vstupu sú obvykle spojené s mechanickým a elektronickým riadením vstupu. Vyššia vrstva mechanického/elektronického riadenia vstupu sa dosiahne v spojení s kľúčovým systémom riadenia.

Rozsah prostriedkov sa určí po zvážení finančných možností a kritického stavu položiek a oblastí, ktoré majú byť chránené, zraniteľnosti objektov a ceny bezpečnostných opatrení nutných na zníženie pravdepodobnosti napadnutia. Cena bezpečnostných opatrení by nemala presahovať peňažnú hodnotu položky alebo oblasti, ktorá má byť chránená, ak to nevyžaduje jej kritický stav alebo národná bezpečnosť.

9.3.3 Priestorová ochrana

Priestorová ochrana sa poníma ako ***vnútorná ochrana objektov***, ktorá zabezpečuje vnútorné priestory chráneného záujmu v objekte. Ťažiskom priestorovej ochrany sú ***obytné miestnosti budov a centrálne body – schodištia, haly, spojovacie chodby a vnútorné komunikačné uzly.*** Zabezpečuje ochranu priestoru vnútri chráneného objektu (komunikačné priestory, miestnosti s koncentráciou hmotných alebo duševných hodnôt) a signalizuje javy s charakterom nebezpečenstva v chránenom priestore.

Táto oblasť sa týka sekundárnej úrovne kontroly ľudí alebo predmetov, ktoré sa dostali do vnútra zariadenia. Vnútorná bezpečnosť sa dosahuje ***odlíšením zamestnancov od návštevníkov, sledovaním bezpečnej prevádzky, prípravou havarijných plánov, pohotovosťou na riešenie priemyselných a environmentálnych havárií a hasenie požiarov.***

Prvky priestorovej ochrany objektu tvoria najmä ***poplachové prvky priestorovej ochrany,*** v menšej miere ***mechanické zábranné prostriedky.*** Tieto prvky sa dajú využiť i v priestore medzi perimetrom a plášťom objektu.

Poplachové prvky priestorovej ochrany

Poplachové prvky priestorovej ochrany majú za úlohu chrániť vnútorné priestory budov indikovaním pohybu objektov v priestore v čase stráženia – signalizujú javy spojené s vniknutím narušiteľa do vnútorných priestorov chráneného objektu. Ťažiskom sú centrálne body budovy – schodiská, chodby, spojovacie chodby, vnútorné komunikačné uzly. Poplachové prvky priestorovej ochrany sú ako alternatíva alebo doplnenie k v súčasnosti najlepšej forme stráženia – plášťovej ochrane. Základné delenie je na snímače pasívne a snímače aktívne.

a) pasívne snímače – pri zisťovaní charakteristických rysov napadnutia iba registrujú fyzikálne zmeny vo svojom okolí,

b) aktívne snímače – pri zisťovaní charakteristických rysov napadnutia vytvárajú svoje pracovné prostredie aktívnym pôsobením na svoje okolie a detegujú zmenu takto vytvoreného fyzikálneho prostredia.

V praxi sa využívajú **snímače pohybu:**

a) pasívne infračervené snímače (PIR),
b) aktívne ultrazvukové snímače (US),
c) aktívne mikrovlnné snímače (MW),
d) duálne – kombinované snímače (PIR – US, PIR – MW).

Niektoré snímače majú vyššiu úroveň bezpečnosti na základe **ochrany pred zakrytím alebo zaslepením pohybového detektora,** zväčša cez deň, v čase, keď je bezpečnostný systém vypnutý (tzv. antimasking). Táto funkcia je aktívna aj v dobe pokoja objektu a je určená na indikáciu zakrytia snímača. Tieto snímače sa montujú do verejne prístupných priestorov, kde je riziko sabotáže systému s cieľom pripraviť si objekt na vlámanie v stave stráženia.

Stredisko registrácie poplachov – pult centralizovanej ochrany

Stredisko registrácie poplachov – pult centralizovanej ochrany (*Alarm Receiving Centre SRP-PCO)* je **komplex technických zariadení a práce obslužných pracovníkov**: ***operátorov, zásahových pracovníkov, technikov, správcov databáz.*** Ide o špecializované pracovisko s celodennou prevádzkou so zvláštnym režimom, vybavené technológiou centrálneho vyhodnocovania monitorovaných objektov.

Jeho základnou úlohou je **prijímať signály** z monitorovaných objektov a **v prípade vyhlásenia narušenia, prepadu, sabotáže a iných poplachových signálov** zabezpečiť ***vyslanie zásahovej jednotky, zabezpečenie objektu a vykonanie ďalších úloh v zmysle dohody s klientom a platných právnych noriem.***

Pri vyhlásení poplachu je k objektu vysielaná zásahová motorizovaná hliadka, ktorá vykoná okamžité preverenie signálu a opatrenia podľa § 44 ods. 5 Zákona č. 579/2002 Z. z. SRP-PCO umožňuje prijímať signál prostredníctvom **vysielačky, telefónneho komunikátora**, **IP komunikátora,** poprípade kombinovane, čo zvyšuje bezpečnosť prenosu signálu a zároveň minimalizuje možnosť použitia ľahko dostupných rušičiek GSM signálu. Každý prijatý signál je možné presne lokalizovať tak, aby bolo už pri jeho spracovaní jasné, z ktorej miestnosti, priestoru, alebo zariadenia bol vyslaný.

PCO sú obvykle koncipované dvoma spôsobmi – ako úplne autonómne systémy a ako systémy integrované do PC.

1. **Autonómne systémy –** autonómny PCO je konštruovaný tak, že je schopný plnohodnotnej prevádzky bez ďalších prístrojov a zariadení. Obyčajne je vybavený displejom a tlačiarňou. Jeho súčasťou je napájací zdroj so zálohovacím akumulátorom. K systému sa pripojuje počítač, ktorý umožňuje komfortnejšiu obsluhu s radom doplnkových funkcií, medzi ktoré patrí napr. zobrazovanie nákresov (schém) pripojených objektov, mapiek okolia, prístupových trás apod. Výhodou tohto systému je, že v prípade výpadku elektrického napájania alebo poruchy PC je PCO schopné prijímať poplachové signály z chránených objektov.
2. **Systémy integrované do PC –** sú konštruované tak, že na pevnom disku je nainštalovaný špecializovaná software. To znamená, že takýto PCO pre svoju prevádzku potrebujú celú kapacitu PC a je nevyhnutné, aby fungovali všetky prvky (časti) osobného počítača. V prípade poruchy pevného disku, na ktorom je nainštalovaný software, to znamená totálny výpadok funkcií PCO. Rovnaký dopad by mali aj poruchy softwarového charakteru.

PCO musí byť schopný prijímať správy o poplachu z napojených objektov a spoľahlivo ich vyhodnotiť. PCO/SRP využívajú na prenos poplachových správ:

- priame linky (buď vyhradené z inej siete alebo pevné – na tento účel inštalované),
- účastnícke linky telefónnych sietí,
- bezdrôtový prenos.

S využitím SRP-PCO možno vykonávať služby:

- diaľkový monitoring EZS (elektronickou zabezpečovacou signalizáciou),
- diaľkový monitoring CCTV (kamerovým systémom),
- kontrola stavu objektov výjazdovou jednotkou,
- zaistenie páchateľa výjazdovou jednotkou,
- kontrola pohybu osôb (zamestnancov) v objekte,
- monitoring uzamykania objektu (kontrola elektronického zakódovania objektu v dohodnutom čase),
- zaistenie objektu proti vzniku ďalších škôd,
- služba TIESEŇ – rýchle privolanie pomoci,
- stráženie automobilov pomocou systému GPS.

Okrem narušenia objektu je možné na SRP-PCO prijímať aj iné signály, ako napríklad stav záložných akumulátorov, výpadok elektrickej energie, sabotáž a narušenie vysielacieho zariadenia, únik plynu, požiar.

Z hľadiska **mechanických zábranných prostriedkov** ide predovšetkým o vnútorné stavebné otvory – ***vnútorné dvere, špeciálne vnútorné okná*** atď. *(Mach, 2012).*

Prednosťou priestorovej ochrany sú nižšie náklady na inštaláciu a montáž ako pri ostatných druhoch ochrany, pretože magnetické kontakty a detektory na ochranu sklenených plôch sú náročnejšie na správne umiestnenie a nastavenie ako detektory pohybu.

9.3.4 Predmetová ochrana

Predmetová ochrana zabezpečuje ochranu predmetov v chránenom objekte, ochranu informácií a iných aktív uložených v úschovných zariadeniach v jednotlivých chránených priestoroch objektu. Zabezpečuje priestory či úschovné miesta, kde sú uložené chránené informácie, cenné predmety a financie pred odcudzením a neoprávnenou manipuláciou s nimi a signalizuje napadnutie alebo neoprávnenú manipuláciu s chráneným predmetom. Okrem mechanickej prielomovej odolnosti týchto zariadení sa požaduje aj ich požiarna odolnosť.

Medzi prostriedky predmetovej ochrany patria:

a) mechanické zábranné prostriedky predmetovej ochrany,

b) poplachové systémy.

Mechanické zábranné prostriedky predmetovej ochrany sa v niektorých prípadoch nazývajú aj úschovnými objektmi. Na rozdelenie úschovných objektov je možné použiť celý rad kritérií. Podľa veľkosti sa delia na skriňové a trezorové s určením na bezpečnostnú odolnosť proti vlámaniu a ohňovzdornosť. Najvšeobecnejšie rozdelenie úschovných objektov je z hľadiska ich účelu a konštrukcie na:

1. **Komerčné úschovné objekty –** patria k najpoužívanejším, majú relatívne nízku pasívnu bezpečnosť oproti trezorovým zariadeniam, sú najviac využívané v podnikoch, inštitúciách, obchodoch, ale aj v domácnostiach, zahŕňajú zostávajúce druhy úschovných objektov, od pokladničky po ťažké skriňové trezory. Pracovne ich môžeme rozdeliť na:
   a) ***skriňové trezory*** – úschovný objekt, ktorý chráni svoj obsah proti vlámaniu a ktorý v uzatvorenom stave má dĺžku jednej vnútornej strany menšiu alebo rovnajúcu sa 1 m.

b) ***ohňovzdorné skrine*** – sú vyrobené z oceľových a nehorľavých materiálov, majú dvojplášťovú konštrukciu, medzi plášťami je ohňovzdorná výplň (vydržia 60 až 120 min), sú skrine na ochranu papierových materiálov, pre dátové médiá a kombinované z bezpečnostnou triedou,

c) ***účelové trezory*** – vstavané trezory, trezory na zbrane, vhadzovacie trezory, nočné trezory,

d) ***oceľové a kartotékové skrine*** – ich bezpečnostná úroveň je nízka, v kanceláriách ako skrine na dokumenty, sú jednoplášťové,

e) ***príručná pokladnička*** – bezpečnostná úroveň veľmi nízka, používa sa na krátkodobú úschovu pseňazí, cenín a dokumentov, sú jednoplášťové, s hrúbkou 2-3 mm.

2. Bezpečnostné úschovné objekty, trezory – sú určené na odkladanie a ochranu peňazí, šperkov, drahocenností, cenných papierov pred poškodením, zničením i odcudzením:

a) Prenosné trezory.

b) Komorové trezory sú pevným stavebným celkom budov, ktoré sú riešené buď samostatne vnútri objektu, alebo sú súčasťou a väčšinou bývajú budované súčasne so stavbou budovy v podzemí, najlepšie v jej strede. Komorové trezory sú riešené ako:

- **monolitické komorové trezory** – vznikajú priamo pri stavbe uložením a spracovaním betónovej zmesi so statickou a špeciálnou bezpečnostnou výstužou do požadovaného tvaru,
- **panelové komorové trezory** – sa montujú priamo na stavbe z príslušných priemyslovo vyrobených prvkov stavebnej sústavy,
- **kombinované komorové trezory** – využitie oboch predchádzajúcich technológií.

Z **poplachových systémov** ide najmä o **systémy na identifikáciu osôb (autentizácia)** – ***elektrické systémy sledovania.*** Pre predmetovú ochranu je možné využiť prvky určené pôvodne pre iný druh ochrany ako: ***magnetické kontakty, PIR detektory, MW detektory, infračervené závory, seizmické detektory, kapacitné detektory***.

Bezpečnostné kamery môžu byť často ako odstrašujúci prostriedok, ale ich skutočný výkon vychádza z overenia incidentu a rozboru predchádzajúcej činnosti. Napríklad, alarmy sa vytvárajú tam, kde sú kamery, kamera by mohla overovať alarm. V prípade, že kamera zachytila útočníka, záznam ho môže vyhodnotiť. Kamerové monitorovanie je jednoduchý prostriedok na získavanie dôkazov pre analýzu v neskoršom čase.

9.3.5 Bezpečnostný audit systému ochrany objektu pred úmyselným napadnutím

Aj najlepšie plánované bezpečnostné systémy a bezpečnostné postupy stratia svoju účinnosť, keď nie sú nepretržite monitorované. Pravidelné bezpečnostné previerky sa majú vykonávať v intervale stanovenom vrcholovým vedením, ktoré by malo tiež stanoviť kritériá, kedy by sa mali vykonávať ďalšie neplánované bezpečnostné audity, napr. pri zmene miesta, nových rizikách, predpokladaných stratách alebo skutočných stratách atď. Výsledky bezpečnostného auditu sa musia hlásiť späť vrcholovému vedeniu. Bezpečnostné audity môžu zahŕňať široký súbor oblastí, najrozšírenejšie sa vykonáva audit v týchto zložkách:

1. Fyzické usporiadanie budov organizácie a okolitých priestorov:

- Rozmiestnenie aktív zvyšuje alebo znižuje bezpečnosť pred možnými spôsobmi útoku alebo prístupu?
- Umožňuje charakter terénu ukrytie alebo poskytuje možnosti prístupu cez strechy alebo iné prístupové miesta?
- Koľko vstupov je do budovy? Sú tieto vstupy monitorované?
- Prechádzajú všetky osoby, ktoré vstupujú alebo vychádzajú z objektu kontrolným miestom?

2. **Osvetlenie:**
   - Osvetlenie, aby stráže, zamestnanci alebo iní videli miesta možného ukrytia alebo na prístupy, je dostatočné?
   - Nie sú prístupové miesta zle viditeľné pre slabé osvetlenie?
3. **Poplachové zariadenia** – vrátane požiaru, narušenia, sabotáže, pohybu:
   - Sú dvere, okná, dvere, turnikety vybavené prostriedkami na monitorovanie výstupu a vniknutiu?
   - Sú prostriedky monitorovania schopné určiť, kto prichádza do týchto priestorov?
   - Je priestor monitorovaný na vznik ohňa alebo výskyt dymu? Môže tento systém upozorniť miestny hasičský útvar?
   - V prípade násilného vniknutia, koho poplachový systém informuje? Je to sledované treťou stranou alebo zamestnancami?
4. **Fyzické prekážky** - vrátane plotov, betónových zábran, spomaľovacích pásov, brán:
   - Sú ploty dosť vysoké na zníženie možnosti neoprávnenému prístupu k majetku? Je plot pravidelne kontrolovaný zamestnancami (diery, poškodenie alebo prístupové miesta)?
   - Sú umiestnené betónové zábrany, aby nedošlo k poškodeniu budov alebo prístupových miest vozidlami?
   - Sú spomaľovacie pásy inštalované a schopné zabrániť neoprávnenému vstupu do chránených oblastí okolo majetku? Parkoviská, nakladacie rampy, miesta odberu.
   - Sú brány bezpečné a fungujú správne?
   - Je vstup do týchto priestorov chránený bránami, alebo je voľný pohyb vozidiel povolený vo vnútri i mimo priestory?
5. **Prístupové miesta** – vrátane dverí, brán, turniketov, okien, nakladacích rámp, výťahov a schodísk:
   - Sú dvere a brány v dobrom stave? Fungujú správne a uzatvárajú priestory?
   - Fungujú turnikety správne a vyžadujú potrebné doklady?
   - Sú okná zabezpečené, keď sú otvorené?
   - Ak sú v objekte umiestnené veľké tabule skla, sú potiahnuté bezpečnostnou fóliou, aby sa zabránilo násilnému vniknutiu?
   - Nakladacie priestory a dvere k nim fungujú správne, a sú zabezpečené, keď sa nepoužívajú?
   - Sú výťahy a schodiská kontrolované denne alebo po hodinách bezpečnostnou službou?
6. **Fyzická ochrana:**
   - Využíva organizácia fyzickú ochranu?
   - Overujú strážni osoby prichádzajúce do priestorov? Ako ich overujú? Osobné doklady, preverovanie príslušnosti, kontrola vozidiel, zapisovanie mien a iných informácií?
   - Kontrolujú stráže prístup k miestam, ktoré oddeľujú majetok? Dvere, okná, výťahy, schodiská, nákladné rampy, bezpečnostné oblasti?
   - Majú stráže kompletné kontrolné zoznamy, podľa ktorých overujú totožnosť, alebo kontrolujú podľa pokynov?
7. **Kamerové systémy:**
   - Sú obvod budovy a priestory s aktívami dostatočne pokryté kamerami?
   - Dokážu kamery automaticky prejsť z denného na nočný režim alebo slabé osvetlenie?
   - Sú stavebné vchody a východy monitorované kamerami?
   - Sú schodiská a ďalšie prístupové miesta monitorované kamerami?
   - Kamery monitorujú 24 hodín denne alebo len preskúmavajú činnosť keď došlo k incidentu?
8. **Systémy kontroly vstupu** – vrátane zámkov, bezdotykových kariet, kódovaných alebo šifrovaných zámkov a iných metód kontroly:
   - Sú zámky a zaisťovacie zariadenia v dobrom stave a pracujú správne?

- Majú ešte predchádzajúci zamestnanci kľúče/prístupové karty do budovy?
- Predchádzajúcim zamestnancom/končiacim zamestnancom sa odoberajú práva prístupu k majetku?
- Ako často sa menia prístupové kódy?

9. **Spôsoby narušenia komunikácie** zistené počas bezpečnostného auditu u osôb zodpovedných za bezpečnosť organizácie, vrátane – miestne poplachové zariadenia/osvetlenie, telefón, e-mail, textové správy atď:
   - Ako je bezpečnostný personál informovaný o narušení v oblasti bezpečnosti a neoprávneného prístupu? Strážou, miestnymi poplachovými zariadeniami, monitorovacími poplachovými zariadeniami, telefónom?
   - Má bezpečnostný personál poznať postupy organizácie pre oznamovanie udalostí manažmentu iným kľúčovým zamestnancom?

Vykonanie bezpečnostného auditu v pravidelných intervaloch pomôže organizácii minimalizovať straty a zvýšiť bezpečnosť zamestnancov a zákazníkov. Po každom audite bude organizácia stále menej zraniteľná, zníži sa počet krádeží vonkajšími i vnútornými páchateľmi.

Čokoľvek, čo možno urobiť, aby sa znížila možnosť vzniku týchto udalosti bude mať vplyv na efektivitu organizácie. Bezpečnostný audit zaberie minimum času a bude mať trvalé účinky na zvýšenie bezpečnosti.

9.4 REŽIMOVÉ OPATRENIA NA OCHRANU OBJEKTU

Režimovú ochranu tvorí súhrn administratívne–organizačných opatrení na zabezpečenie chránených záujmov a hodnôt. Tvorí ju systém poriadku a režimu, jeho zabezpečenie a pravidelná kontrola.

Režimové opatrenia na ochranu objektu predstavujú postupy pre efektívne uplatňovanie systému ochrany objektu, ktoré určujú:

a) podmienky ***vstupu osôb a vjazdu dopravných prostriedkov*** do objektu a podmienky ***výstupu osôb a výjazdu dopravných prostriedkov*** z objektu,
b) podmienky ***pohybu osôb, dopravných prostriedkov v objekte*** a to v pracovnom čase a mimopracovnom čase,
c) určujúce podmienky ***používania mobilných telefónov, videokamier, fotoaparátov, audio záznamových zariadení*** a pod.,
d) podmienky ***ochrany priestorov*** kde sú uložené významné aktíva,
e) podmienky a spôsob ***kontroly objektu po opustení pracoviska*** zamestnancami, ktoré zabezpečia že nedôjde k neoprávnenej činnosti,
f) opatrenia na ***ochranu rokovacích miestností***,
g) podmienky používania, prideľovania, označovania, úschovy a evidencie originálov a kópií ***bezpečnostných kľúčov a médií*** do zámkov a uzamykateľných systémov,
h) podmienky používania, prideľovania, označovania, úschovy a evidencie ***kódových nastavení a hesiel používaných pre prístup do objektov***,
i) podmienky manipulácie s ***mechanickými zábrannými prostriedkami a technickými zabezpečovacími prostriedkami*** a podmienky ich používania,
j) ***postup pri narušení objektu*** alebo pri pokuse o narušenie objektu,
k) postup v prípade ***vzniku mimoriadnej situácie***, ktorých súčasťou je aj plán na ochranu a evakuáciu spolu s uvedením zodpovedných osôb; ak bezprostredne hrozí vznik mimoriadnej situácie alebo ak mimoriadna situácia už nastala, je vedúci oprávnený povoliť vstup do objektu osobám zabezpečujúcim alebo vykonávajúcim záchranné akcie; v takých prípadoch pred vykonaním záchrannej akcie, v jej priebehu a bezprostredne po jej skončení musia byť prijaté opatrenia, ktoré zabránia neoprávneným činnostiam.

Režimové opatrenia pre vstup a pobyt v objektoch, môžu byť stanovené nasledovne:

1. Zamestnanci pri vstupe do objektov sú povinní na požiadanie zamestnancov na vrátnici predložiť tieto doklady:
   a) služobný preukaz u zamestnancov poverených výkonom kontroly,
   b) personálnu identifikačnú kartu, resp. preukaz totožnosti zamestnancov,
   c) preukaz totožnosti u cudzích návštevníkov,
   d) služobný preukaz u príslušníkov policajného zboru.
2. Schváleným návštevám je povereným pracovníkom pridelený preukaz návštevníka, musia sa zapísať do knihy návštev, ako aj čas príchodu a odchodu.
3. V dňoch pracovného pokoja, vo sviatky, soboty a nedele môže byť možný prístup na pracovisko len konkrétnou bránou alebo vstupom. Vstup môže byť umožnený tým zamestnancom, ktorí majú povolený vstup na pracovisko.
4. Pohyb vozidiel organizácie môže byť obmedzený časovo. Výjazd môže byť povolený len na základe príkazu na cestu. Vjazd a výjazd môže byť možný iba vodičom a ostatní cestujúci sú povinný prejsť cez vrátnicu a preukázať sa identifikačnou kartou.
5. Motorové vozidlá dodávateľských organizácií môžu mať vjazd povolený len na základe zaevidovania žiadosti do systému organizácie.

6. Materiálový a expedičný režim stanoví postup pri príjme, uskladňovaní, výdaji a pohybe materiálu, chráni sa ním majetok pred rozkrádaním, poškodzovaním a znehodnocovaním.
7. Poverený pracovník strážnej služby môže skontrolovať obsah príručných tašiek pri príchode a odchode vlastných zamestnancov, zamestnancov dodávateľských organizácií a návštev.
8. Pri dovoze materiálu, člen bezpečnostnej služby prevezme súpis materiálu, označí ho pečiatkou, dátumom a svojim podpisom. Pri dovoze materiálu musí byť odovzdaný súpis materiálu. Zamestnanec bezpečnostnej služby skontroluje súpis materiálu a porovná ho so skutočne dovážaným materiálom alebo tovarom.

Prevádzkový režim zabezpečuje plynulosť a bezpečnosť prevádzky a činnosti pri mimoriadnych udalostiach.

Kľúčový režim prevádzky stanoví ***označovanie, prideľovanie, odovzdávanie kľúčov, spôsob ich použitia, výroba náhradných kľúčov, výmena zámkov v dôležitých častiach objektu a pod.***

a) náhradné kľúče od všetkých miestností na pracoviskách musia byť uložené v uzamykateľných skrinkách na vrátniciach objektov,
b) zamestnankyne – upratovačky svoje kľúče od miestností po skončení pracovnej doby uložia na vrátniciach príslušných objektov,
c) každý zamestnanec je povinný pred odchodom z pracoviska služobné pomôcky a zverené predmety uschovať a zabezpečiť proti krádeži uzamknutím, prípadne zapečatením.
d) v prípade straty kľúčov od dôležitých miestností (skladov, pokladní, trezorov a pod.), je potrebné vymeniť zámky, u trezorov celé uzamykacie mechanizmy.

9.5 FYZICKÁ OCHRANA OBJEKTU

Podľa ustanovenia § 2 Zákona o súkromnej bezpečnosti **druhmi bezpečnostnej služby** sú:

a) strážna služba,
b) profesionálna cezhraničná preprava eurovej hotovosti cestnou dopravou,
c) detektívna služba,
d) odborná príprava a poradenstvo.

Strážna služba na zabezpečenie ochrany objektov sa vytvára z vlastných zamestnancov alebo prenajatej SBS. Podľa § 3 uvedeného zákona sa pod pojmom **strážna služba** rozumie:

a) ochrana **majetku** na verejne prístupnom mieste,
b) ochrana **majetku** na inom než verejne prístupnom mieste,
c) ochrana **osoby,**
d) ochrana **majetku a osoby pri preprave**,
e) ochrana **prepravy majetku a osoby**,
f) **zabezpečovanie poriadku** na mieste zhromažďovania osôb,
g) prevádzkovanie **zabezpečovacieho systému** alebo **poplachového systému**, prevádzkovanie ich častí, **vyhodnocovanie narušenia chráneného objektu alebo chráneného miesta,**
h) vypracúvanie **plánu ochrany** alebo
i) **monitorovanie činnosti osoby v uzavretom priestore alebo na uzavretom mieste**.

Podľa **Zák. č. 473/2005** Z. z. o súkromnej bezpečnosti, § 8, písm. b) sa pod **fyzickou ochranou** rozumie:

1. **Obchôdzka** - priamy výkon činností uvedených v § 3 písm. a), b) a f) striedavým premiestňovaním sa osoby poverenej výkonom fyzickej ochrany v tom istom chránenom objekte alebo na tom istom chránenom mieste,
2. **Stráženie** - priamy výkon služby prítomnosťou osoby poverenej výkonom fyzickej ochrany na strážnom stanovisku v chránenom objekte, na chránenom mieste alebo pri chránenej osobe, alebo pri chránenom majetku, kde tieto činnosti má vykonávať, v činnostiach uvedených v:
   - § 2 ods. 1 písm. b) - profesionálna cezhraničná preprava eurovej hotovosti cestnou dopravou,
   - § 3 písm. a) až f) a i):
     a) ochrana majetku na verejne prístupnom mieste,
     b) ochrana majetku na inom než verejne prístupnom mieste,
     c) ochrana osoby,
     d) ochrana majetku a osoby pri preprave,
     e) ochrana prepravy majetku a osoby,
     f) zabezpečovanie poriadku na mieste zhromažďovania osôb,
     i) monitorovanie činnosti osoby v uzavretom priestore alebo na uzavretom mieste.
3. **Prevádzkovanie zabezpečovacieho systému alebo poplachového systému,**
4. **Priame riadenie a kontrola týchto činností.**

Zabezpečovacím systémom je sústava **elektrických, elektronických, mechanických alebo iných súčiastok,** tvoriacich ***pevne zabudovanú prekážku***, ktorú nemožno prekonať bez odborných znalostí alebo použitia sily, zabraňujúcu:

- ***vstupu*** osoby alebo zvieraťa do chráneného objektu alebo na chránené miesto alebo ***výstupu*** z nich,

- alebo ***vjazdu*** dopravného prostriedku do chráneného objektu alebo na chránené miesto alebo ***výjazdu*** z nich.

Poplachovým systémom je sústava **elektrických, elektronických, mechanických alebo iných súčiastok,** tvoriacich ***predmet pevne zabudovaný*** na chránenom objekte alebo na chránenom mieste, alebo v chránenom objekte, ktorý v súlade so zákonom a s inými všeobecne záväznými právnymi predpismi, vyvolá ***svetelný, zvukový alebo iný signál***:

- po neoprávnenom zásahu **na** chránenom objekte alebo **na** chránenom mieste,
- alebo po neoprávnenom zásahu **do** chráneného objektu alebo **do** chráneného miesta,
- alebo konaním osoby **v** chránenom objekte alebo **na** chránenom mieste.

Poplachové systémy samy o sebe nie sú ochranou v pravom slova zmysle – okrem odstrašujúceho účinku páchateľom v ničom nezabránia, majú však dve základné úlohy:

- **podporovať mechanické zábranné systémy** – t. j. dodať informáciu o narušení a umožniť fyzickej ochrane (zásahovej jednotke) včas zasiahnuť,
- **zvyšovať efektívnosť fyzickej ochrany**, použitím poplachových systémov sa znižuje počet strážnych pri ochrane objektu.

Vecným bezpečnostným prostriedkom je **vec vrátane zvieraťa**, ktorá je určená na to, aby sa použila ako ***zbraň alebo vec*** na zastavenie, prípadne obmedzenie pohybu osoby, zvieraťa alebo vozidla alebo na obmedzenie funkcie iného technického zariadenia.

Iným technickým prostriedkom je **stroj** alebo **prístroj,** ktorý sa používa na plnenie úloh fyzickej ochrany, pátrania, odbornej prípravy a poradenstva.

Fyzická ochrana objektu môže byť, predovšetkým **mimo pracovného času,** zabezpečená aj **kontrolou hranice objektu *použitím elektrického zabezpečovacieho systému s vyvedením výstupného signálu na stanovište stáleho výkonu služby fyzickej ochrany.***

Zásahom je činnosť osoby poverenej výkonom fyzickej ochrany alebo pátrania, pri ktorej sa zasahuje do práv a slobôd inej osoby.

Medzi základné úlohy fyzickej ochrany patrí :

- **kontrola osôb** a ich **batožiny** pri vstupe alebo pri odchode z objektu a **požadovanie predloženia príslušných dokladov,**
- **kontrola vjazdu a výjazdu vozidiel,** ich **nákladu, príslušných dokladov**,
- **vyzvanie podozrivej osoby v objekte na preukázanie totožnosti** a oprávnenia vstupu do objektu,
- **požadovanie vysvetlenia** od každého nepovolaného v objekte organizácie,
- **predvedenie na miesto** určené vnútornými smernicami, každého, kto nemôže svoju totožnosť preukázať, kto poškodzuje majetok, porušuje predpisy, ohrozuje zdravie a život,
- **odobranie veci** dôvodne podozrivej z odcudzenia alebo možnosti zneužitia,
- vykonávanie **kontroly priestorov v určených hodinách.**
- **udržiavanie poriadku,** podávanie informácií, hlásenie nehody, úrazu, neobvyklej udalosti,
- a inej neobvyklej okolnosti, ktorá má vzťah k stráženému objektu.

- **Pracovníci fyzickej ochrany** v rozsahu stanovenom vnútornými smernicami zabraňujú rozkrádaniu, strate, zneužitiu, poškodeniu, prípadne zničeniu majetku a neoprávnenému vstupu osôb alebo vjazdu dopravných prostriedkov, do objektu organizácie**.** Osoby vykonávajúce fyzickú ochranu musia byť ***vycvičené a vybavené komunikačnými prostriedkami.***

Fyzickú ochranu priestoru, objektu, predmetov a iných chránených záujmov môžu vykonávať

- príslušníci ozbrojených síl,

- ozbrojených bezpečnostných zborov,
- trvalo prítomní ozbrojení zamestnanci,
- zamestnanci súkromných bezpečnostných služieb,
- pracovníci dočasne poverení ochranou majetku a iné osoby, ktorým táto povinnosť vyplýva z funkčného zaradenia,
- vyškolení zamestnanci prevádzkovateľa objektu alebo určení vlastní zamestnanci,
- pracovníci, ktorým boli úlohy stanovené inou právnou normou, napr. strážnici, vrátnici, hliadková služba, lesná stráž, poľovná stráž, vodná stráž.

Fyzická ochrana objektu (strážna služba) musí byť organizovaná a vykonávaná tak, aby:

- na jej výkon boli určené ***osoby so zodpovedajúcim stupňom preverenia, fyzicky zdatné a odborne pripravené,***
- pôsobila ako ***prostriedok na odradenie narušiteľa objektu***(chráneného priestoru),
- jednotka vykonávajúca strážnu službu bola ***schopná vykonať včasný zásah v mieste narušenia systému ochrany utajovaných skutočností alebo iných aktív,***
- bolo ***minimalizované riziko,*** že sa príslušníci strážnej (zasahujúcej) jednotky zoznámia s utajovanými skutočnosťami, na ktoré nemajú oprávnenie.

Fyzickú ochranu alebo pátranie môže vykonávať len osoba, ktorá:

- dosiahla vek 19 rokov,
- je spôsobilá na právne úkony v plnom rozsahu,
- je bezúhonná, spoľahlivá, zdravotne spôsobilá,
- a je držiteľom preukazu odbornej spôsobilosti.

Vedúci výkonu fyzickej ochrany (manažér bezpečnostnej služby):

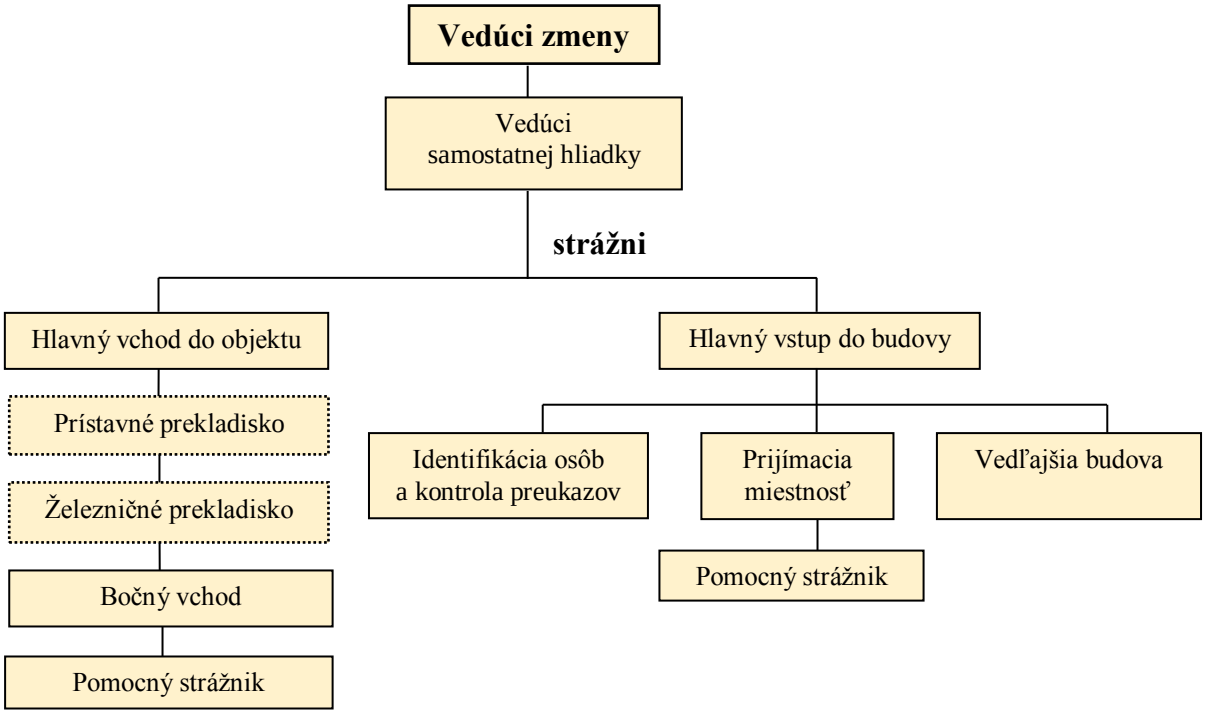
a) Vykonáva tieto typické činnosti:
- riadi, koordinuje, motivuje a hodnotí pracovníkov strážnej služby,
- plánuje týždenné zmeny,
- zaškoľuje novoprijatých zamestnancov,
- vyhľadáva a navrhuje školenia, tréningy a kurzy pre podriadených zamestnancov,
- kontroluje pracovníkov strážnej služby pomocou elektronického kontrolného čipového systému, videozáznamov a pod.
- kontroluje dochádzku podriadených zamestnancov,
- podieľa sa na výbere a prepúšťaní zamestnancov,
- rieši neštandardné situácie na pracovisku.

b) Určuje:
- pravidlá na výkon fyzickej ochrany
- reakčný čas fyzickej ochrany na poplachový signál tak, aby bol kratší, ako čas potrebný na prekonanie realizovaných opatrení na ochranu utajovaných skutočností,
- intervaly preverovania reakcie fyzickej ochrany na poplachové signály (preverovanie sa musí vykonať najmenej raz za rok).

- **Pracovník bezpečnostnej služby** vykonáva tieto typické činnosti:
- zabezpečuje *ochranu fyzických osôb a súkromného majetku,*
- vykonáva *pravidelné obchôdzky* okolo zvereného objektu a priľahlých priestorov,
- vykonáva *obchôdzky v prípade signalizovaného narušenia* chráneného priestoru,
- *monitoruje objekt a priľahlé priestory* pomocou bezpečnostného kamerového systému,
- zisťuje a zaznamenáva *totožnosti osôb,*

- *kontroluje osoby pri vstupe do objektu*, vykonáva pravidelné alebo náhodné osobné prehliadky pri podozrení na prítomnosť nebezpečných a nepovolených predmetov,
- *kontroluje osoby pri opúšťaní objektu,* vykonáva pravidelné alebo náhodné osobné prehliadky pri podozrení z krádeže alebo sprenevery majetku,
- používa hmaty, chvaty a iné donucovacie prostriedky v prípade potreby,
- spolupracuje so zložkami polície, hasičského a záchranného zboru,
- poskytuje pomoc a poradenstvo verejnosti.

Fyzická ochrana objektov sa obvykle vykonáva nepretržite v trojzmennej prevádzke. Podľa Sennewalda jedna zmena môže obsahovať zloženie podľa obr. 26.



Obr. 26 Príklad rozdelenia pracovníkov fyzickej ochrany jednej zmeny

Dokumentácia na výkon fyzickej ochrany

Na výkon fyzickej ochrany objektu sa spracovávajú:

a) Pravidlá na výkon fyzickej ochrany objektu

b) Grafická časť Pravidiel na výkon služby fyzickej ochrany objektu a chráneného priestoru – **Schéma rozmiestnenia kontrolných (strážnych) stanovíšť**,

c) Výkazová dokumentácia určená pre pracovníkov fyzickej ochrany objektu na vedenie prehľadu o priebehu služby:

- denný záznam o priebehu služby,
- záznamy o odovzdaní a prevzatí služby zmeny,
- záznam o bezpečnostných incidentoch a mimoriadnych udalostiach,
- záznam o vykonaných zásahoch ,
- kniha kontrol,
- kniha návštev,
- kniha vjazdu/výjazdu vozidiel,
- evidencia výdaja kľúčov,
- ďalšie dokumenty podľa potreby, resp. rozhodnutia vedúceho.

d) Pomocná dokumentácia, napr.:

- 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 Policajný zbor, Hasičský a záchranný zbor, 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.

Pravidlá na výkon fyzickej ochrany

Pravidlá na výkon fyzickej ochrany objektu a chráneného priestoru pre pracovnú i mimopracovnú dobu môžu obsahovať:

- **spôsob zabezpečenia fyzickej ochrany objektu a chráneného priestoru,** najmä: kto vykonáva fyzickú ochranu, ako je označená, ako je vyzbrojená, aké pomôcky má k dispozícii.
- **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 a pod.).
- **určenie počtu osôb zabezpečujúcich fyzickú ochranu**: koľko príslušníkov má zmena fyzickej ochrany,
- **spôsob kontroly osôb pri vstupe a výstupe a dopravných prostriedkov pri vjazde a výjazde**: spôsob kontroly vstupu osôb, vlastných zamestnancov, dodávateľov, návštev a pod., spôsob kontroly vjazdu a výjazdu dopravných prostriedkov, kontrola dovážaného, vyvážaného materiálu,
- **spôsob vykonávania náhodných prehliadok:** kto oprávňuje k vykonávaniu náhodných prehliadok, ako sa vykonávajú, ako sa dokumentujú ap.
- **spôsob vykonávania obchôdzok:** trasy obchôdzok, periodicita obchôdzok, úlohy pri obchôdzke, čo sa kontroluje, záznamy o výsledkoch obchôdzok ap.
- **spôsob reakcie na poplachové hlásenia technických prostriedkov**: kde je vyvedená signalizácia EZS a kde sú umiestnené monitory CCTV, činnosť pri prevzatí signálu poplach z chránených priestorov, v pracovnej dobe, v mimopracovnej dobe, činnosť pri prevzatí núdzového signálu (PANIC), reakcia na kamerový systém, činnosť pri zistení nepovolanej osoby
- **činnosť pri riešení krízových situácií:** uvedú sa povinnosti a úlohy pre pracovníkov fyzickej ochrany podľa opatrení rozpracovaných v krízovom pláne
- **spôsob kontroly výkonu fyzickej ochrany**: kto je oprávnený kontrolovať výkon služby, rozsah kontroly podľa oprávnenia.

Grafická časť **Pravidiel na výkon fyzickej ochrany** sa môže spracovať napr. formou **Schémy rozmiestnenia kontrolných (strážnych) stanovíšť**, do ktorej 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.
-

9.6 LITERATÚRA

FALISOVÁ, B. [1997]: *Prostriedky technickej ochrany objektov*. Bratislava: ISBN 80-8054-0455-4.

GYMERSKÁ, J. [2003]: *Mechanické prostriedky a systémy technickej ochrany objektov,* Bratislava: APZ.

HOFREITER, L. a kol. [2013]: *Ochrana objektov kritickej dopravnej infraštruktúry*. Žilina: EDIS, ŽU Žilina. ISBN 978-80-554-0803-3.

KIBBEY, R. [2004]: *Understanding Security Basics: A Tutorial on Security Concepts and Technology*. 8th National Biosafety Symposium, Atlanta, Georgia.

LOVEČEK, T. – NAGY, P. [2008]: *Bezpečnostné systémy. Kamerové bezpečnostné systémy.* Žilina. EDIS. ISBN 978-80-807-0893-1.

LOVEČEK, T. – REITŠPÍS, J. [2011]: *Projektovanie a hodnotenie systémov ochrany objektov ŽU v Žiline.* Žilina: FŠI ŽU,2011 ISBN 978-80-554-0457-8.

LOVEČEK, T. – VEĽAS, A. – ĎUROVEC, M. [2015]: *Bezpečnostné systémy. Poplachové systémy.* Žilina. EDIS.

MACH, V. [2010]: *Bezpečnostné systémy – Mechanické bezpečnostné prostriedky*, Košice, Multiprint,2010.

MACH, V. [2012]: *Zisťovanie prielomovej odolnosti mechanických zábranných prostriedkov obvodovej a predmetovej ochrany*. In: Physical Security. 5.10.2012. Žilina: ŽU Žilina: Fakulta špeciálneho inžinierstva.

MIKOLAJ, J. – HOFREITER, L. – MACH, V. – MIHÓK, J. – SELINGER, P. [2004]: *Terminológia bezpečnostného manažmentu. Výkladový slovník,* Žilina; ŽU FŠI.

SENNEWALD, Ch. A. [2003]: *Effective Security Management. Fourth edition.* Elsevier-Science (USA), ISBN 0-7506-7454-7.

VEĽAS, A. [2010]: *Elektrické zabezpečovacie systémy.* Žilina. EDIS, ISBN 978-80-554-0224-6.

ZÁBOJNÍKOVÁ, I. – VIDRIKOVÁ, D. [2010]: *Ochrana objektu, bezpečnostný projekt vybranej firmy*. Žilina: ŽU Žilina: Fakulta špeciálneho inžinierstva.

10 POŽIARNA OCHRANA

Za požiarnu ochranu sú podľa Zákona o ochrane pred požiarmi zodpovední najmä:

- ústredné orgány štátnej správy a ďalšie ústredné orgány,
- obce,
- právnické osoby a fyzické osoby – podnikatelia,
- fyzické osoby na úseku ochrany pred požiarmi.

Právnická osoba a podnikajúca fyzická osoba na ochranu pred požiarmi musí:

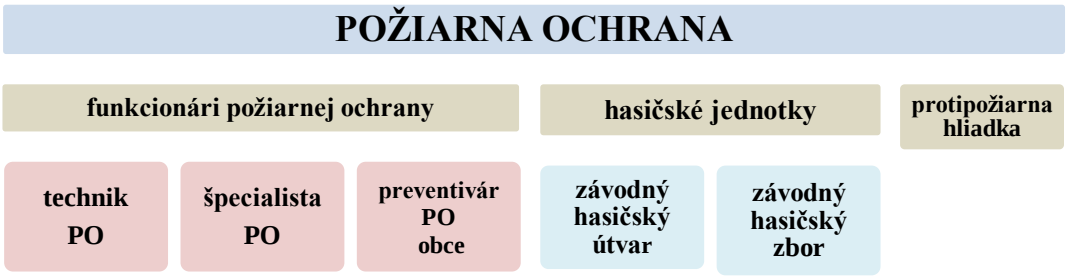
- zabezpečiť v objektoch a v priestoroch vykonávanie **preventívnych protipožiarnych prehliadok a odstraňovať zistené nedostatky,**
- obstarávať a inštalovať **vhodné druhy požiarnotechnických zariadení** – zariadenia na dodávku vody na hasenie požiarov, ďalšie hasiace látky, hasičskú techniku, vecné prostriedky ochrany pred požiarmi, požiarne a evakuačné výťahy, núdzové osvetlenie, technické vybavenie únikových ciest, prostriedky na vyhlásenie požiarneho poplachu, vhodné druhy požiarnotechnických zariadení, prevádzkovať ich v akcieschopnom stave, zabezpečovať vykonávanie ich kontroly a údržby osobou s odbornou spôsobilosťou, ak tak ustanovuje tento zákon, viesť a uchovávať dokumenty o ich prevádzkovaní; vlastnosti a podmienky prevádzkovania zariadenia na dodávku vody na hasenie požiarov, hasičskej techniky, vecných prostriedkov ochrany pred požiarmi, požiarnych výťahov, evakuačných výťahov, technického vybavenia únikových ciest, prostriedkov na vyhlásenie požiarneho poplachu, požiarnotechnických zariadení vrátane podmienok akcieschopnosti, obsah kontroly vrátane lehôt, rozsah údržby, spôsob vedenia dokumentácie o ich prevádzkovaní, vzory dokladov o údržbe a kontrole týchto zariadení ustanoví všeobecne záväzný právny predpis, ktorý vydá ministerstvo,
- označovať a udržiavať trvale voľné **únikové cesty, únikové východy a zásahové cesty, nástupné plochy a prístup k nim,** ako aj **prístup** k uzáverom rozvodných zariadení elektrickej energie, plynu, vody, požiarnotechnickým zariadeniam, zariadeniam na vyhlásenie požiarneho poplachu, požiarnym vodovodom a zdrojom vody na hasenie požiarov,
- strpieť umiestnenie **signalizačného zariadenia** alebo **poplachového zariadenia** určeného na účely ochrany pred požiarmi za primeranú náhradu,
- **udržiavať zdroje vody** na hasenie požiarov v takom stave, aby bola zabezpečená možnosť jej čerpania,
- vykonať **najmenej raz za rok cvičný požiarny poplach** v objektoch právnickej osoby a podnikajúcej fyzickej osoby, v ktorých nie sú jednoduché podmienky na evakuáciu osôb;
- zriadiť a vybaviť potrebný počet **ohlasovní požiarov,**
- spracovať na základe rozhodnutia krajského riaditeľstva HaZZ analýzu nebezpečenstva vzniku požiaru vo svojich objektoch a priestoroch, a na jej základe zriadiť **hasičskú jednotku**, ak tak rozhodlo krajské riaditeľstvo,
- zriaďovať **protipožiarne hliadky** a zabezpečiť plnenie ich úloh a odbornú prípravu; druhy protipožiarnych hliadok, ich úlohy, obsah a rozsah odbornej prípravy a lehoty jej vykonávania ustanoví všeobecne záväzný právny predpis, ktorý vydá ministerstvo vnútra,
- **oznámiť každý požiar,** ktorý vznikol v objektoch, priestoroch alebo na veciach v jej vlastníctve, správe alebo v užívaní príslušnému okresnému riaditeľstvu HaZZ,
- určiť **funkcionárov požiarnej ochrany**.

10.1 SYSTÉM POŽIARNEJ OCHRANY

Štruktúru systému požiarnej ochrany v organizáciách tvoria najmä:

- funkcionári požiarnej ochrany,
- požiarne jednotky (útvar, zbor),
- protipožiarna hliadka,
- požiarnotechnické zariadenia,
- zdroje vody,
- zariadenia na detekciu a signalizáciu,
- hasičská stanica alebo hasičská zbrojnica,
- ohlasovne požiarov,
- dokumentácia požiarnej ochrany.

Orgány požiarnej ochrany v organizácii sú uvedené na obr. 27



Obr. 27 Orgány požiarnej ochrany v organizácii

Právnická osoba a podnikajúca fyzická osoba je povinná zabezpečovať **pravidelné školenie a overovanie vedomostí** o ochrane pred požiarmi zamestnancov a osôb, ktoré sa s vedomím právnickej osoby alebo podnikajúcej fyzickej osoby zdržujú v jej objektoch;

Požiarnotechnické zariadenia sú:

- hasiace prístroje,
- stabilné a polostabilné hasiace zariadenia,
- zariadenia na odvod tepla a splodín horenia,
- elektrická požiarna signalizácia,
- zariadenia na hasenie iskier v pneumatických dopravníkoch,
- požiarne uzávery.

Ohlasovňa požiarov

Právnická osoba alebo podnikajúca fyzická osoba zriaďuje najmenej jednu ohlasovňu požiarov; ak sa člení na organizačné zložky, ktoré majú sídla v inom mieste, zriaďuje ohlasovne požiarov aj v týchto zložkách.

Ak má v objekte sídlo viacero právnických osôb alebo podnikajúcich fyzických osôb, môžu sa títo dohodnúť o zriadení jednej ohlasovne požiarov. Dohoda má písomnú formu a je v nej uvedené, pre koho je spoločná ohlasovňa zriadená a kto zodpovedá za zabezpečenie nepretržitej služby, za jej vybavenie a za uloženie potrebnej dokumentácie.

Ohlasovňa požiarov sa umiestňuje v objekte alebo v priestore, v ktorom je zabezpečená nepretržitá služba najmenej počas prevádzky; označuje sa viditeľne nápisom **Ohlasovňa požiarov.** Ohlasovňa požiarov musí mať spojovacie prostriedky na ohlásenie vzniku požiaru, ako aj zariadenie na vyhlasovanie požiarneho poplachu spôsobom uvedeným v požiarnych poplachových smerniciach.

V ohlasovni požiarov je uložená potrebná dokumentácia všetkých subjektov, pre ktoré je ohlasovňa požiarov zriadená, ktorú tvoria najmä:

- požiarne poplachové smernice,
- požiarne evakuačné plány,
- telefónne čísla štatutárneho zástupcu právnickej osoby a ďalších určených zodpovedných vedúcich zamestnancov alebo podnikajúcej fyzickej osoby a jej zodpovedného zástupcu,
- zoznam právnických osôb a podnikajúcich fyzických osôb vrátane ich telefónnych čísel, ktoré majú sídlo v objekte, pre ktorý je zriadená ohlasovňa požiarov.

Proces požiarnej ochrany v organizácii zahŕňa najmä:

- **analýzu nebezpečenstva vzniku požiaru** v objektoch právnickej osoby a fyzickej osoby – podnikateľa,
- **plánovanie a vykonávanie preventívnych protipožiarnych prehliadok** a odstraňovanie zistených nedostatkov,
- **označovanie a udržiavanie** trvale voľných únikových ciest, únikových východov a zásahových ciest, nástupných plôch a prístupov k nim**,** ako aj prístup k uzáverom rozvodných zariadení,
- obstarávanie a inštalovanie vhodných druhov **požiarnotechnických zariadení**,
- udržiavanie **zdrojov vody** na hasenie požiarov,
- požiarnu **detekciu a signalizáciu**, signalizačné zariadenia alebo poplachové zariadenia,
- zriadenie **hasičskej jednotky**, ak tak rozhodlo krajské riaditeľstvo,
- zriadenie **protipožiarnych hliadok** a zabezpečenie plnenia ich úloh a odbornej prípravy,
- zriadenie a vybavenie potrebného počtu **ohlasovní požiarov,**
- vypracúvanie, vedenie a udržiavanie **dokumentácie ochrany pred požiarmi** v súlade so skutočným stavom,
- vykonávanie **školenia** o ochrane pred požiarmi a odbornej prípravy protipožiarnych hliadok a hasičských jednotiek,
- organizovanie a vyhodnocovanie **cvičných požiarnych poplachov** (najmenej raz za rok),
- určovanie požiadaviek na **protipožiarnu bezpečnosť pri užívaní stavby** a pri zmene v užívaní stavby,
- vypracovanie **dokumentácie o požiarnobezpečnostnej charakteristike užívanej stavby**,
- vypracúvanie riešenia protipožiarnej bezpečnosti v **projektovej dokumentácii stavieb**.

10.1.1 Funkcionári požiarnej ochrany

Funkcionármi požiarnej ochrany sú:

- technik požiarnej ochrany,
- špecialista požiarnej ochrany,
- preventivár požiarnej ochrany obce.

Technikom požiarnej ochrany alebo špecialistom požiarnej ochrany môže byť len fyzická osoba s odbornou spôsobilosťou na výkon činnosti technika požiarnej ochrany. Odborná spôsobilosť je vzdelanie, prax a súhrn teoretických vedomostí, praktických skúseností a znalosť všeobecne záväzných právnych predpisov, ktoré sú potrebné na riadny výkon činnosti. Odbornú spôsobilosť technika požiarnej ochrany alebo špecialistu požiarnej ochrany môže získať len **fyzická osoba s úplným stredným vzdelaním**.

Fyzické osoby s odbornou spôsobilosťou technika požiarnej ochrany alebo špecialistu požiarnej ochrany sa musia podrobiť raz za päť rokov pravidelnému overovaniu odbornej spôsobilosti po absolvovaní ďalšej odbornej prípravy.

Technik požiarnej ochrany

Podľa § 9 ods. 2 Zákona č. 314/2001 Z. z. o ochrane pred požiarmi v znení neskorších predpisov zabezpečuje ústredný orgán, právnická osoba a podnikajúca fyzická osoba prostredníctvom technika požiarnej ochrany plnenie týchto povinností:

a) vykonávanie preventívnych protipožiarnych prehliadok,
b) určovanie miest so zvýšeným nebezpečenstvom vzniku požiaru a počtu členov protipožiarnych hliadok,
c) výchova a vzdelávanie v oblasti ochrany pred požiarmi a odborná príprava protipožiarnych hliadok,
d) odborná poradenská činnosť v oblasti ochrany pred požiarmi,
e) vypracúvanie, vedenie a udržiavanie dokumentácie ochrany pred požiarmi v súlade so skutočným stavom,
f) určovanie požiadaviek na protipožiarnu bezpečnosť pri užívaní stavby a pri zmene v užívaní stavby a vypracovanie dokumentácie o požiarnobezpečnostnej charakteristike užívanej stavby,
g) príprava, organizovanie a vyhodnocovanie cvičných požiarnych poplachov,
h) odborná pomoc pri odstraňovaní nedostatkov vyplývajúcich z protipožiarnych kontrol vykonaných orgánmi štátneho požiarneho dozoru.

Vyššie uvedené činnosti môže technik požiarnej ochrany vykonávať na základe pracovno-právneho vzťahu, dodávateľsky, alebo inou formou. Odbornú spôsobilosť technik požiarnej ochrany preukazuje osvedčením o odbornej spôsobilosti. Odbornú spôsobilosť technika požiarnej ochrany overuje a osvedčenie o odbornej spôsobilosti technika požiarnej ochrany vydáva územne príslušné krajské riaditeľstvo Hasičského a záchranného zboru.

Overenia odbornej spôsobilosti sa môže zúčastniť len fyzická osoba, ktorá absolvovala odbornú prípravu pre technikov požiarnej ochrany vo vymedzenom rozsahu. Odborná príprava sa člení na základnú odbornú prípravu a ďalšiu odbornú prípravu. Základná odborná príprava v rozsahu 120 hodín je určená pre fyzické osoby, ktoré nemajú odbornú spôsobilosť technika požiarnej ochrany. Ďalšia odborná príprava v rozsahu 30 hodín je určená pre fyzické osoby s odbornou spôsobilosťou technika požiarnej ochrany. Overovanie odbornej spôsobilosti technika požiarnej ochrany pozostáva z písomnej časti a ústnej časti.

Špecialista požiarnej ochrany

Podľa § 9 ods. 2 Zákona o ochrane pred požiarmi v znení neskorších predpisov zabezpečuje právnická osoba a podnikajúca fyzická osoba prostredníctvom špecialistu požiarnej ochrany plnenie týchto povinností:

a) vypracúvanie riešenia protipožiarnej bezpečnosti v projektovej dokumentácii stavieb,
b) vykonávanie činností pri posudzovaní zhody výrobkov alebo pri ich certifikácii,
c) riešenie požiadaviek protipožiarnej bezpečnosti pri vývoji nových výrobkov a pri ich používaní,
d) riešenie protipožiarnej bezpečnosti pri umiestňovaní technologických zariadení a riešenie protipožiarnej bezpečnosti výrobkov, ktoré nie sú určenými výrobkami ustanovenými na posudzovanie zhody podľa Zákona č. 264/1999 Z. z. o technických požiadavkách na výrobky a o posudzovaní zhody a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, a posudzovanie materiálov a podmienok na ich bezpečné používanie z hľadiska protipožiarnej bezpečnosti,
e) spracúvanie analýzy nebezpečenstva vzniku požiaru v objektoch právnickej osoby a podnikajúcej fyzickej osoby, ak o tom rozhodlo krajské riaditeľstvo.

Vyššie uvedené činnosti môže špecialista požiarnej ochrany vykonávať na základe pracovno-právneho vzťahu, dodávateľsky, alebo inou formou. Špecialista požiarnej ochrany je povinný osvedčovať pravosť písomností, ktoré vyhotovil pri vykonávaní činností odtlačkom svojej pečiatky a vlastnoručným podpisom.

Odbornú spôsobilosť špecialista požiarnej ochrany preukazuje osvedčením o odbornej spôsobilosti. Overenia odbornej spôsobilosti sa môže zúčastniť len fyzická osoba, ktorá absolvovala odbornú prípravu pre špecialistov požiarnej ochrany vo vymedzenom rozsahu. Odborná príprava sa člení na základnú odbornú prípravu a ďalšiu odbornú prípravu. Základná odborná príprava v rozsahu 160 hodín je určená pre fyzické osoby, ktoré nemajú odbornú spôsobilosť špecialistu požiarnej ochrany.

Ďalšia odborná príprava v rozsahu 40 hodín je určená pre fyzické osoby s odbornou spôsobilosťou špecialistu požiarnej ochrany. Overovanie odbornej spôsobilosti špecialistu požiarnej ochrany pozostáva z písomnej časti, ústnej časti a z obhajoby spracovaného riešenia protipožiarnej bezpečnosti v projektovej dokumentácii stavby, ktoré žiadateľ vopred predloží skúšobnej komisii.

10.1.2 Protipožiarna hliadka

Protipožiarne hliadky sa členia na:

a) protipožiarnu hliadku právnickej osoby alebo podnikajúcej fyzickej osoby,
b) protipožiarnu hliadku pracoviska,
c) protipožiarnu asistenčnú hliadku.

Právnická osoba a podnikajúca fyzická osoba zriaďuje protipožiarnu hliadku:

a) na miestach so zvýšeným nebezpečenstvom vzniku požiaru,
b) v čase zvýšeného nebezpečenstva vzniku požiarov,
c) pri činnostiach spojených so zvýšeným nebezpečenstvom vzniku požiaru,
d) pri podujatiach, na ktorých sa zúčastňuje väčší počet osôb,
e) ak nemá zriadenú hasičskú jednotku a zamestnáva viac ako troch zamestnancov.

Členovia protipožiarnej hliadky dozerajú na dodržiavanie opatrení na zamedzenie vzniku požiaru a vykonávajú nevyhnutné opatrenia na evakuáciu osôb a zdolávanie požiaru. Protipožiarna hliadka dozerá na dodržiavanie predpisov o ochrane pred požiarmi na pracoviskách, v objekte a zistené nedostatky bezodkladne oznamuje príslušnému vedúcemu.

Pri vyhlásení požiarneho poplachu vykonáva nevyhnutné opatrenia, najmä záchranu ohrozených osôb, privolanie pomoci, zdolávanie požiaru a opatrenie na zamedzenie jeho šírenia, predovšetkým zatvorením požiarnych uzáverov, prívodov horľavých látok, odstránením tlakových nádob, vypnutím elektrického prúdu, uzatvorením prívodu plynu a pod.

Členovia protipožiarnej hliadky právnickej osoby sú povinní najmä kontrolovať vybavenosť priestorov hasiacimi zariadeniami, hasiacimi prístrojmi a spojovacími prostriedkami, pričom preverujú ich kompletnosť a prístup k nim, voľnosť únikových ciest, zásahových ciest, východov, prístup k uzáverom rozvodových zariadení energií.

Viac právnických osôb a podnikajúcich fyzických osôb, ktoré sídlia v jednom objekte, môže na základe písomnej dohody zriadiť spoločnú protipožiarnu hliadku. Členovia protipožiarnej hliadky dozerajú na dodržiavanie opatrení na zamedzenie vzniku požiaru a vykonávajú nevyhnutné opatrenia na evakuáciu osôb a zdolávanie požiaru.

10.1.3 Hasičské jednotky

Závodný hasičský útvar

Závodný hasičský útvar zriaďuje podľa Vyhlášky MV SR č. 611/2006 Z. z. o hasičských jednotkách právnická osoba alebo fyzická osoba-podnikateľ na základe rozhodnutia krajského riaditeľstva vtedy, ak:

a) je potrebné vykonať účinný zásah do piatich minút od ohlásenia požiaru ohlasovni požiarov alebo operačnému pracovisku alebo najneskôr do polovice prvej fázy rozvoja požiaru,
b) z analýzy vyplynie potreba zabezpečiť dodávku najmenej 600 l hasiacej látky za minútu vrátane peny alebo použitie halónových hasiacich látok alebo hasiaceho prášku,
c) zabezpečuje sa okrem hasiacich látok aj dodávka vody na ochladzovanie otvorených technologických konštrukcií alebo ďalších objektov a na zabránenie prenosu požiaru na susedné objekty, požiarne úseky alebo priestory,
d) zdolávanie požiaru je zložité a zároveň treba ohrozené osoby evakuovať nielen vybudovanými únikovými cestami, ale aj náhradnými spôsobmi evakuácie, napríklad zásahovou špeciálnou hasičskou technikou, alebo sa vyžaduje dostatočné množstvo špeciálnej hasiacej látky (penotvorný roztok, prášok a podobne),
e) je nevyhnutné vykonávať zásah fyzicky zdatnými, odborne pripravenými a zdravotne spôsobilými zamestnancami hasičskej jednotky a na ochranu ich povrchu tela sú potrebné osobné ochranné pracovné prostriedky na ochranu dýchacích ciest pred účinkami tepelného žiarenia, rádioaktívneho spádu alebo chemických látok a biologických materiálov.

Zamestnanci právnickej osoby alebo podnikajúcej fyzickej osoby zaradení v závodnom hasičskom útvare **vykonávajú činnosti v týchto jednotkách ako svoje zamestnanie**. Zriaďovateľ závodného hasičského útvaru je povinný zabezpečiť vykonávanie služieb zamestnancami tak, aby po prijatí správy ohlasovňou požiaru o potrebe výjazdu na zásah a po nasledujúcom vyhlásení poplachu sa dodržal časový limit výjazdu ***do jednej minúty.***

Závodný hasičský zbor

Závodný hasičský zbor zriaďuje právnická osoba alebo fyzická osoba-podnikateľ na základe rozhodnutia krajského riaditeľstva vtedy, ak:

a) treba vykonať účinný zásah do desiatich minút od ohlásenia požiaru ohlasovni požiarov alebo vykonať zásah na konci prvej fázy rozvoja požiaru,
b) z analýzy vyplynie potreba zabezpečiť zásahovou základnou hasičskou technikou dodávku najmenej 400 l hasiacej látky za minútu,
c) zdolávanie požiaru sa vykonáva v menej zložitých podmienkach a evakuácia ohrozených osôb sa vykonáva po stavebne riešených únikových cestách podľa požiarneho evakuačného plánu so sprievodom člena hasičskej jednotky; na vykonanie zásahu nie je potrebná zásahová špeciálna hasičská technika a vybudované požiarnotechnické zariadenia zabezpečia, že požiar sa nerozšíri na susedné objekty, požiarne úseky alebo priestory,
d) sú v objektoch s vysokým požiarnym rizikom inštalované požiarnotechnické zariadenia (napríklad elektrická požiarna signalizácia a stabilné hasiace zariadenie),
e) na zdolanie požiaru sa nevyžadujú špeciálne druhy hasiacich látok (penotvorný roztok, prášok a podobne) a ani osobné ochranné pracovné prostriedky na ochranu celého povrchu tela,
f) treba vykonať zásah s odborne pripravenými členmi hasičskej jednotky.

O povinnosti zriadiť závodný hasičský zbor môže rozhodnúť aj krajské riaditeľstvo na základe analýzy nebezpečenstva vzniku požiaru v objektoch právnickej osoby a podnikajúcej fyzickej osoby. Krajské riaditeľstvo v rozhodnutí zároveň určí minimálny počet členov a základné materiálno-technické vybavenie závodného hasičského zboru.

Zamestnanci právnickej osoby alebo podnikajúcej fyzickej osoby zaradení v závodnom hasičskom zbore **nevykonávajú činnosti v týchto jednotkách ako svoje zamestnanie.** Zriaďovateľ závodného hasičského zboru je povinný zabezpečiť zvolávanie členov tak, aby po prijatí správy ohlasovňou požiaru o potrebe výjazdu na zásah a po nasledujúcom vyhlásení poplachu sa dodržal časový limit výjazdu ***do piatich minút.***

Štruktúra hasičskej jednotky

Základnou organizačnou zložkou hasičskej jednotky je družstvo. Družstvo tvorí veliteľ a ďalšie tri osoby až osem osôb. Dve alebo tri družstvá jednej zmeny tvoria čatu. Zamestnanci právnickej osoby alebo fyzickej osoby-podnikateľa zaradení do hasičskej jednotky sa zaraďujú do týchto funkcií: *hasič, hasič záchranár, technik-strojník, operátor operačného pracoviska alebo ohlasovne požiarov, hasič záchranár špecialista, veliteľ družstva, technik špecialista odbornej služby, veliteľ čaty, vedúci technik špecialista, veliteľ zmeny, veliteľ stanice, vedúci oddelenia, operačný dôstojník, zástupca veliteľa jednotky, veliteľ jednotky.*

Na nepretržitý príjem hlásení o vzniku požiarov, živelných pohrôm a iných mimoriadnych udalostí sa zriaďuje **ohlasovňa požiarov** v závodnom hasičskom útvare alebo v závodnom hasičskom zbore právnickej osoby alebo podnikajúcej fyzickej osoby, ak sa nezriaďuje **operačné pracovisko Integrovaného záchranného systému**. Závodný hasičský útvar môže zriadiť **operačné pracovisko,** ktoré plní funkciu ohlasovne požiarov.

Nepretržitý výkon služby v závodnom hasičskom útvare sa organizuje na zmeny. Zmenu tvoria zamestnanci zaradení na operačnom pracovisku alebo v ohlasovni požiarov a najmenej jedného družstva. Striedanie zmien sa vykonáva za súčasnej prítomnosti zamestnancov, ktorí službu končia a ktorí do služby nastupujú.

Pri striedaní zmien si zamestnanci vzájomne odovzdávajú nedokončené úlohy, hasičskú techniku, vecné prostriedky hasičskej jednotky a ďalšie prostriedky určené na výkon služby. Zamestnanci vykonávajú službu v zmene podľa organizačného zaradenia určeného rozpisom služieb.

Medzi základné úlohy hasičskej jednotky patrí najmä:

a) záchrana osôb ohrozených požiarom a zdolávanie požiarov,
b) záchrana zvierat a majetku ohrozených požiarom,
c) vykonávanie záchranných prác pri živelných pohromách,
d) poskytovanie pomoci podľa svojich technických možnosti a odbornej kvalifikácie pri bezprostrednom ohrození života pri nehodách a iných mimoriadnych udalostiach,
e) zabezpečovanie akcieschopnosti hasičskej techniky a jej vecných prostriedkov; zriaďuje odborné služby, a to strojnú, protiplynovú a spojovaciu,
f) vykonávanie odbornej prípravy svojich zamestnancov a členov v určenom rozsahu,
g) ohlasovanie bez zbytočného odkladu okresnému riaditeľstvu zásahy pri zdolávaní požiarov a pri vykonávaní záchranných prác počas živelných pohrôm a iných mimoriadnych udalostí,
h) vypracúvanie a vedenie dokumentácie hasičskej jednotky.

Bližšie informácie na úseku ochrany pred požiarmi upravuje Zákon č. 314/2001 Z. z. o ochrane pred požiarmi a vyhláška MV SR č. 611/2006 Z. z. o hasičských jednotkách a interné predpisy.

10.1.4 Dokumentácia požiarnej ochrany

Pre potreby požiarnej ochrany sa vytvárajú:

- požiarny štatút,

- požiarny poriadok pracoviska,
- požiarne poplachové smernice,
- požiarny evakuačný plán,
- požiarna kniha,
- analýza nebezpečenstva vzniku požiaru,
- zoznam objektov a prehľad miest so zvýšeným nebezpečenstvom vzniku požiaru,
- doklady o kontrole požiarnotechnických zariadení a požiarnych vodovodov,
- údaje o požiaroch, príčinách ich vzniku, správy o výsledkoch vykonaných rozborov a o vykonaných opatreniach na úseku ochrany pred požiarmi,
- dokumentácia o školení zamestnancov o ochrane pred požiarmi,
- dokumentácia o odbornej príprave protipožiarnych hliadok,
- dokumentácia o činnosti hasičskej jednotky,
- ďalšie doklady.

Požiarny štatút – základný dokument ochrany pred požiarmi, ktorý vypracováva technik požiarnej ochrany v spolupráci so príslušnými zodpovednými vedúcimi pracovníkmi, a ktorý obsahuje:
- organizačné usporiadanie ochrany pred požiarmi,
- povinnosti jednotlivých organizačných zložiek pri plnení úloh ochrany pred požiarmi,
- povinnosti štatutárneho orgánu na zabezpečenie ochrany pred požiarmi,
- úlohy technika požiarnej ochrany, špecialistu požiarnej ochrany, hasičských jednotiek a protipožiarnych hliadok,
- spôsob a lehoty vykonávania kontrol dodržiavania predpisov, vydaných príkazov, zákazov a pokynov na úseku ochrany pred požiarmi,
- rozsah, lehoty a organizáciu školenia zamestnancov o ochrane pred požiarmi a formy overovania vedomostí,
- rozsah, lehoty a organizáciu odbornej prípravy protipožiarnych hliadok,
- spôsob zabezpečenia ochrany pred požiarmi v mimopracovnom čase, pri činnostiach spojených so zvýšeným nebezpečenstvom vzniku požiaru.

Požiarny poriadok pracoviska – dokument ochrany pre pracoviská so zvýšeným nebezpečenstvom vzniku požiaru, ktorý vypracováva technik požiarnej ochrany v spolupráci so zodpovedným vedúcim pracoviska, a ktorý obsahuje:
- opis technologického postupu a charakteristiku nebezpečenstva vzniku požiaru na pracovisku,
- požiarnotechnické charakteristiky spracúvaných a používaných surovín a materiálov a ich najvyššie prípustné množstvá na pracovisku,
- požiadavky na pracovisko na zabezpečenie ochrany pred požiarmi,
- zoznam miest a zariadení alebo ich častí so zvýšeným nebezpečenstvom vzniku požiaru alebo výbuchu a opatrenia na zamedzenie vzniku a šírenia požiaru,
- osobitné povinnosti zamestnancov.

Požiarne poplachové smernice – dokument vymedzujúci povinnosti zamestnancov v prípade vzniku požiaru, ktorý vypracováva technik požiarnej ochrany, a ktorý obsahuje:
- povinnosti zamestnanca, ktorý spozoruje požiar, spôsob a miesto ohlásenia požiaru,
- spôsob vyhlásenia požiarneho poplachu pre zamestnancov a hasičskú jednotku právnickej osoby alebo podnikajúcej fyzickej osoby,
- povinnosti zamestnancov pri vyhlásení požiarneho poplachu, najmä pokyny o tom, v ktorých prípadoch majú zostať na svojich pracoviskách a v ktorých prípadoch ich majú opustiť, prípadne akým spôsobom sa majú podieľať na zdolávaní požiaru,
- miesto, adresu a číslo telefónu:

– ohlasovne požiarov a hasičských jednotiek,
– pohotovostnej služby elektrárne, plynárne, vodárne, liniek tiesňového volania,
– právnických osôb a fyzických osôb zabezpečujúcich pohotovostné služby.

Požiarny evakuačný plán – dokument upravujúci organizáciu evakuácie osôb, zvierat zo zasiahnutých alebo ohrozených objektov, ktorý vypracováva technik požiarnej ochrany, ktorý obsahuje:

- určenie zamestnancov, ktorí budú riadiť evakuáciu a miesto, z ktorého ju budú riadiť,
- určenie zamestnancov a prostriedkov, pomocou ktorých sa bude evakuácia vykonávať,
- určenie spôsobu evakuácie a ciest na evakuáciu,
- určenie miesta, kde sa evakuované osoby, prípadne zvieratá budú sústreďovať a určenie zodpovedného zamestnanca za kontrolu počtu evakuovaných,
- spôsob zabezpečenia poskytnutia prvej pomoci postihnutým,
- grafické vyznačenie evakuačných ciest v pôdorysoch jednotlivých podlaží objektu.

Požiarna kniha – dokument určený na záznamy o dôležitých skutočnostiach týkajúcich sa ochrany pred požiarmi s dôrazom na:

- vykonané preventívne protipožiarne opatrenia,
- zistené nedostatky,
- spôsob odstránenia zistených nedostatkov,
- vykonané cvičné požiarne poplachy,
- kontrolu dokumentácie ochrany pred požiarmi.

Dokumentácia o odbornej príprave protipožiarnych hliadok: súbor dokumentov, ktorý schvaľuje štatutár subjektu alebo ním poverená osoba:

- tematické plány,
- časový rozvrh odbornej prípravy,
- záznam o vykonaní odbornej prípravy.

Dokumentácia o školení zamestnancov o ochrane pred požiarmi:

- záznam o vykonanom školení,
- výsledky overovania vedomostí vedúcich pracovníkov a osôb zabezpečujúcich ochranu pred požiarmi v mimopracovnej dobe s podpisom predsedu skúšobnej komisie.

Ďalšou oblasťou požiarnej ochrany je **posudzovanie projektovej dokumentácie stavieb** v rámci územného a stavebného konania a nadväzne aj účasť na kolaudačných konaniach. Tam sa preveruje, či realizovaná stavba bola postavená v zmysle požiadaviek schválenej projektovej dokumentácie.

10.2 LITERATÚRA

Ochrana pred požiarmi a protipožiarna bezpečnosť: (aktualizované predpisy). Bratislava: Epos, 2006. ISBN 8080576726.

OSVALD, A. [2005]: *Ochrana pred požiarmi.* Zvolen: Technická univerzita, ISBN 8022 814938.

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

Vyhláška MV SR č. 121/2002 Z. z. o požiarnej prevencii.

Vyhláška MV SR č. 611/2006 Z. z. o hasičských jednotkách.

11 ZÁVER

Učebnica Bezpečnostný manažment – manažérstvo bezpečnosti je vôbec prvou učebnicou v podmienkach SR, zameranou na bezpečnostný manažment z hľadiska všeobecného manažmentu.

Zavádza **novú definíciu bezpečnostného manažmentu**, v ktorej sa vyskytujú nové pojmy: „***manažérstvo bezpečnosti, referenčný objekt*** a ***špecifický druh manažmentu***“. Uvádza a vysvetľuje **významy bezpečnostného manažmentu** a charakterizuje ho z troch **hľadísk:** ***informačného, rozhodovacieho*** a ***funkčného.***

Novým pojmom v učebnici je pojem **„manažérstvo bezpečnosti“**, ktorý však je novým len relatívne, pretože z medzinárodného i národného hľadiska sa všeobecne používa, o čom svedčia štruktúry ***integrovaného manažérskeho systému,*** charakterizované v učebnici, napr. manažérstvo kvality, manažérstvo BOZP, environmentálne manažérstvo a pod.

Na uvedené všeobecné zásady bezpečnostného manažmentu v učebnici nadväzuje **systémový prístup k manažérstvu bezpečnosti,** ktorý sa využíva pri určení ***štruktúry i procesu manažérstva bezpečnosti.***

Proces manažérstva bezpečnosti sa v učebnici rieši podľa najnovších medzinárodných noriem **ISO a prílohy SL**, ktorá zjednocuje štruktúry noriem pre všetky systémy manažérstva, teda aj manažérstva jednotlivých druhov bezpečnosti. V tejto jednotnej štruktúre sú zahrnuté všetky ***manažérske funkcie,*** plánovanie, organizovanie, vedenie i kontrola a dôraz sa kladie aj na ***informačný proces*** a ***rozhodovanie***. Učebnica takto obsahuje najnovšie medzinárodne platné zásady, uplatňované v manažérstve bezpečnosti organizácií.

Učebnica sa zameriava na ***manažérstvo bezpečnosti referenčných objektov***. Nerieši referenčné objekty na národnej a medzinárodnej úrovni, ani všeobecné druhy bezpečnosti podľa Kodanskej školy, či Human Security, sústreďuje sa na štátne a súkromné organizácie a ich objekty. Medzi organizáciami je potrebné chápať aj územné celky a medzi objektmi aj bytové a nebytové domy a inžinierske stavby, ktoré predstavujú určitú hodnotu a potrebujú ochranu.

V učebnici sa veľký význam kladie na **manažérstvo rizika** podľa **STN ISO 31000:2011** Manažérstvo rizika, zásady a návod, ktorá je základom aj pre ***riešenie vonkajších a vnútorných súvislostí*** a ***manažérstva rizika v organizácii*** podľa nových noriem pre systémy manažérstva.

Význam učebnice je aj v tom, že sa nezameriava na technické záležitosti ochrany nejakého objektu, ako doterajšie učebnice, ale na zásady riadiacich činností v manažérstve bezpečnosti, ktoré sú pre budúcich manažérov, pracujúcich v oblasti bezpečnosti, najdôležitejšie. Budúci **bezpečnostní manažéri** majú takto potrebný návod, ktorý môžu využiť vo svojom praktickom pôsobení na akejkoľvek funkcii bezpečnostného manažéra.

prof. Ing. Ľubomír Belan, CSc.

BEZPEČNOSTNÝ MANAŽMENT
Manažérstvo bezpečnosti

Vydala Žilinská univerzita v Žiline, Univerzitná 8215/1, 010 26 Žilina
v edičnom rade VYSOKOŠKOLSKÉ UČEBNICE

Vedecký redaktor prof. Ing. Miloslav Seidl, PhD.

Zodp. red. Ing. Jana Handriková
Tech. red. Mgr. Jana Pauriková
Graf. úprava Ing. Ján Mišík

Vytlačilo EDIS-vydavateľské centrum ŽU,
Univerzitná HB, 010 26 Žilina v roku 2015 ako svoju 4066. publikáciu.
200 strán, 27 obrázkov, 5 tabuliek, AH 18,66, VH 19,16
1. vydanie, náklad 50 CD

ISBN 978-80-554-1163-7

www.edis.uniza.sk

Rukopis v EDIS-vydavateľskom centre ŽU neprešiel jazykovou úpravou.