BEZPEČNOSTNÝ MANAŽMENT

BEZPEČNOSŤ A MANAŽÉRSTVO RIZIKA

1. časť

BEZPEČNOSŤ

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

OBSAH

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

POUŽITÉ SKRATKY

- **AIDS** *(Acquired Immune Deficiency Syndrome*) – Syndróm získanej imunitnej nedostatočnosti.
- **BS** *(British Standards)* – Britské normy.
- **CENTO** *(Central Treaty Organization)* – Organizácia vzájomnej bezpečnosti 1955-1979 – Turecko, Irán, Pakistan a Veľká Británia.
- **CO –** Civilná ochrana.
- **CSS** *(Critical Security Studies)* **–** Kritické bezpečnostné štúdie.
- **EÚ** – Európska únia.
- **ES** – Európske spoločenstvo.
- **GMO** – Geneticky modifikovaný organizmus.
- **G 20** – skupina najväčších ekonomík sveta predstavovaná ministrami financií a guvernérmi centrálnych bánk, t. j. členmi 19 štátov a Jednotného vnútorného trhu Európskej únie.
- **HIV** *(Human Immunodeficiency Virus)* – Vírus ľudskej imunitnej nedostatočnosti.
- **IEC** (*International Electrotechnical Commission)* – Medzinárodná elektrotechnická komisia.
- **ICAO** *(International Civil Aviation Organisation)* – Medzinárodná organizácia pre civilné letectvo.
- **IKT** – Informačné a komunikačné technológie.
- **IS** – Informačné systémy.
- **ISO** *(International Organization for Standardization)* – Medzinárodná organizácia pre normalizáciu.
- **KĽDR** – Kórejská ľudovodemokratická republika.
- **MZP** – Mechanické zábranné prostriedky.
- **MŽP** – Ministerstvo životného prostredia.
- **NAFTA** *(North American Free Trade Agreement)* – Severoamerická dohoda o voľnom obchode, obchodná dohoda spájajúca Kanadu, Spojené štáty americké a Mexiko do zóny voľného obchodu.
- **NATO** *(North Atlantic Treaty Organization*) – Severoatlantická aliancia
- **OBSE** *(Organization for Security and Co-operation in Europe, skrátene OSCE)* – Organizácia pre bezpečnosť a spoluprácu v Európe.
- **OECD** *(Organisation for Economic Co-operation and Development)* – Organizácia pre hospodársku spoluprácu a rozvoj.
- **OSN** *(United Nations Organisation, skrátene UNO)* – Organizácia spojených národov.
- **OUS** – Ochrana utajovaných skutočností.
- **SBS** – Súkromná bezpečnostná služba.
- **SEATO** *(South East Asia Treaty Organization)* – Organizácia zmluvy pre juhovýchodnú Áziu.
- **SLEX** – Elektronický krátky slovník slovenského jazyka.
- **SMS** *(Short message service)* – Krátka textová správa, esemeska.
- **SR** – Slovenská republika.
- **STN** – Slovenská technická norma.
- **TZP** – Technické zabezpečovacie prostriedky.
- **UNDP** *(United Nations Development Programm)* – Rozvojový program OSN.
- **UNHCR** *(United Nations High Commissioner for Refugees)* – Úrad Vysokého komisára OSN pre utečencov.
- **WB** *(World Bank)* – Svetová banka.
- **WTO** (*World Trade Organization)* – Svetová obchodná organizácia.
- **ZSSR** – Zväz sovietskych socialistických republík.

Motto: Človek je súčasťou prírody a je na nej životne závislý.

1 ÚVOD

Potreba bezpečia, istoty patrí spoločne s fyziologickými potrebami už oddávna medzi najsilnejšie pociťované ľudské potreby. Ľudia od samého počiatku vnímali svoje postavenie v prostredí **zápasu dobra** (bezpečnosť, istota) **a zla** (nebezpečenstvo pre život a majetok človeka), pričom **vnímali dva aspekty bezpečnosti:**

1. ako ochranu pred nebezpečenstvami **prírodnej povahy** (prírodné živly, dravá zver atď.),
2. spojený s javmi **spoločenskej povahy** (násilie) – ktorý má na spoločnosť väčší dopad.

Protipólom bezpečnosti je vo všetkých oblastiach života **nebezpečnosť, nebezpečenstvo,** ktoré môže spôsobiť rôzne **negatívne udalosti**. Tieto nebezpečné udalosti majú vo väčšine prípadov za následok rôzne **škody,** ujmy na ***životoch a zdraví osôb, majetku a na životnom prostredí.***

Ľudské vedomosti, vedecký, technický a technologický pokrok na jednej strane odhaľujú človeku nové dimenzie, na druhej strane vyvolávajú, prípadne priamo so sebou prinášajú, rad nebezpečenstiev a ohrození jeho samotnej existencie. Preto aj doterajší rozvoj spoločnosti, techniky a technológií bol spojený s nárastom množstva bezpečnostných hrozieb a menil aj vnímanie pocitu ľudskej bezpečnosti. Donedávna bola bezpečnosť rozpracovaná najmä vo vojenskej a vojensko-politickej teórii, v súčasnosti je potreba bezpečia a istoty človeka zameraná najmä na osobnú (individuálnu) bezpečnosť a ekonomickú istotu.

Z hľadiska **osobnej bezpečnosti** človeka sa prejavuje najmä potreba:

- ***istoty bezpečnosti*** – tradičnej potreby vyhnúť sa násiliu, agresii a inému ohrozeniu (bolesti, stresu, úzkosti, strachu, chladu atď.),
- ***sociálnej a právnej istoty*** – ochrana zdravia, morálna a fyziologická istota, istota rodiny, potreba mieru a pokoja, stability, poriadku, práva, ochrany, nádeje a viery, dôvery, informácií a orientácie,
- ***ekonomickej istoty*** – do popredia vystupujú istota zamestnania, istota príjmu a prístupu k zdrojom, potreba sebestačnosti, potreba vlastníctva a hromadenia majetku.

Okrem bezpečnosti osôb sa prejavujú aj nové formy bezpečnosti a značne sa zvýšilo množstvo subjektov s významnými aktívami, ktoré je potrebné chrániť – **referenčné objekty**. Okrem individuálnej bezpečnosti narástla dôležitosť ***medzinárodnej a vonkajšej národnej bezpečnosti***. Zvýšila sa úloha ochrany ***vnútornej bezpečnosti a poriadku v štáte,*** s dôrazom na ochranu občanov a majetku. Pre narastajúce rasové, náboženské, etnické, sociálne, majetkové, kultúrne a iné riziká sa pozornosť v zvýšenej miere zameriava aj na ***skupinovú bezpečnosť'***.

Okrem štátu patria medzi referenčné objekty ***mestá, obce, organizácie, rôzne druhy objektov a životné prostredie,*** pre ktoré má bezpečnosť vysoký význam**.** Každá organizácia, ktorá chce byť úspešná, musí byť pripravená ochraňovať všetky aktíva, ktoré pre ňu predstavujú a vytvárajú hodnoty. Pre organizácie, ktoré potrebujú zostať efektívne a konkurencieschopné, sa ochrana pracovníkov, informácií, technológií, alebo iného majetku stáva nevyhnutnou súčasťou života. Na zachovanie bezpečnosti musia rešpektovať rôzne zákony, regulačné predpisy a nariadenia, ktoré vyjadrujú záujem štátu chrániť celospoločenské hodnoty, ktoré môžu byť činnosťou alebo produktmi organizácie ohrozené.

Cieľom prvej časti učebnice Bezpečnostný manažment – Bezpečnosť je poskytnúť základné údaje o teórii bezpečnosti, vývoji bezpečnostných štúdií, referenčných objektoch,

a bezpečnostnom sektore v organizáciách, v ktorom je podľa ich zamerania množstvo oblastí bezpečnosti. Štruktúra učebnice je zameraná na zodpovedanie nasledujúcich otázok:

- **AKÉ** sú **definície, vlastnosti a zásady bezpečnosti**?
- **ČO** je **referenčný objekt**? – základný prvok bezpečnosti, chránená hodnota.
- **KOHO** a **ČO chrániť**? – aktíva.
- **AKÉ druhy bezpečnosti** sú zamerané na ochranu osôb, majetku a životného prostredia v organizáciách?

Na základe uvedených otázok sa v jednotlivých kapitolách riešia problémy:

- **Základy bezpečnosti –** prístupy k vymedzeniu pojmu bezpečnosť, definície bezpečnosti, vlastnosti bezpečnosti, bezpečnosť v spoločenských a technických systémoch, úroveň bezpečnosti, zásady bezpečnosti organizácie.
- **Vývoj bezpečnostných štúdií –** vývoj chápania pojmu bezpečnosť, tradičné a kritické bezpečnostné štúdie, paradigmy a základné roviny bezpečnosti, bezpečnostný koncept „ľudskej bezpečnosti“, dimenzie a sektory bezpečnosti z pohľadu Kodanskej školy, referenčný objekt.
- **Manažment aktív –** právne normy, definícia, proces manažérstva aktív, správa aktív, inventarizácia a klasifikácia aktív, pridelenie zodpovednosti za aktíva.,
- **Bezpečnostný sektor organizácie** a jeho zložky – BOZP, bezpečnosť prevádzky, predchádzanie závažným priemyselným haváriám, informačná bezpečnosť, fyzická bezpečnosť osôb a majetku **v rôznych objektoch**.

Pri tvorbe publikácie boli využité výsledky vedeckovýskumnej a publikačnej činnosti Katedry bezpečnostného manažmentu Fakulty bezpečnostného inžinierstva Žilinskej univerzity v Žiline a právne normy pre bezpečnostný manažment a manažérstvo bezpečnosti.

Publikácia je určená pre študentov študijného programu Bezpečnostný manažment, môže sa využiť aj v iných študijných programoch na Fakulte bezpečnostného inžinierstva, ale aj na komerčné potreby.

2 BEZPEČNOSŤ

Bezpečnosť (z lat. *sēcūritās)* je už oddávna jednou z najsilnejšie pociťovaných ľudských potrieb. V Maslowovej teórii hierarchie potrieb je ***bezpečnosť a istota*** začlenená na druhé miesto za fyziologické potreby. Okrem nich sú v nej *spoločenské potreby, potreba úcty a uznania, potreba sebarealizácie.*

Bezpečnosť je nevyhnutnou požiadavkou pre existenciu života na Zemi, v prírode i spoločnosti. Je životným záujmom občanov, sociálnych skupín, štátov a medzinárodného spoločenstva – ľudské dejiny sú preto späté s hľadaním ciest, spôsobov a foriem zabezpečenia medzinárodnej, vnútornej aj vonkajšej bezpečnosti.

Bezpečnosť má základný význam pre fungovanie štátu, jeho inštitúcií a organizácií i existenciu človeka ako indivídua. Pre súčasnú spoločnosť je charakteristické, že sa na jednej strane znížila hrozba rozsiahleho alebo regionálneho ozbrojeného konfliktu, na druhej strane sa vo zvýšenej miere prejavuje strata pocitu bezpečnosti a nárast fenoménu násilia. Vnímanie zhoršovania stavu bezpečnosti sa prejavuje najmä v neistote či:

- bude garantovaná ***ochrana zdravia a života človeka***,
- bude zaistená ***bezpečnosť majetku***,
- bude garantovaná ***ochrana životného prostredia***,
- bude zaistená ***kontinuita hlavných i podporných činností v organizácii***,
- bude vždy dostatok ***informácií*** pre dennodenné rozhodovanie a zabezpečená ich ochrana.

Pre optimálny vývoj v daných vonkajších i vnútorných podmienkach je nevyhnutná **r o v n o v á h a** v prírode a spoločnosti. Všeobecne platí, že v systémoch **každý dej, jav, prípadne proces** prebieha v ***štandardných podmienkach spôsobom, ktorý je možné s určitou pravdepodobnosťou predvídať a popísať, prípadne, ktorý je priamo plánovaný***. V uvedených prípadoch možno vo všetkých oblastiach života (v prírode i spoločnosti) hovoriť o:

B E Z P E Č N O S T I

Podľa Šimáka je každý rovnovážny stav charakterizovaný radom parametrov, pričom podstatná zmena niektorého z nich môže zapríčiniť stratu stability rovnovážneho stavu *(Šimák, 2004).*

Strata stability rovnovážnych stavov:

- *je prirodzeným javom, ktorý je súčasťou evolučného vývoja sveta,*
- *dá sa do značnej miery eliminovať rôznymi preventívnymi nástrojmi,*
- *v prevažnej väčšine prípadov jej však nie je možné zabrániť.*

Stratu stability rovnovážneho stavu je možné členiť na dva základné typy:

- **mäkká strata stability** – ustáleným režimom sa stáva periodický režim, ktorý sa *len málo líši od rovnovážneho stavu*,
- **tvrdá strata stability** – náhodné zmeny parametrov a poruchy vychýlia systém natoľko, že sa *úplne naruší stabilita, dochádza k jej strate, systém opúšťa rovnovážny stav skokom a prechádza na iný režim vývoja*.

Každá činnosť, dej alebo jav prebiehajúci v prírode i v spoločnosti sa môže teda v konkrétnych podmienkach stať nekontrolovateľný a spôsobiť ujmy. Je nevyhnutné pochopiť, v čom je podstata týchto nežiaducich zmien. Ak človek pochopí ich príčiny, môže hľadať cesty eliminovania rizík, ako aj príznakov a odstrániť tieto negatívne javy ešte pred ich negatívnym pôsobením na systém.

2.1 PRÍSTUPY K VYMEDZENIU POJMU BEZPEČNOSŤ

V súčasnosti sú známe mnohé pokusy o objasnenie obsahu a významu pojmu bezpečnosť. Jej definície nachádzame v monografiách, slovníkoch, vedeckých a odborných článkoch, zákonoch, technických normách a pod. Pojem bezpečnosť inak vysvetľujú sociológovia, inak ekonómovia, právnici, politológovia, ekológovia, vojaci či technici.

Podľa **IS/ISO/IEC Guide 51:2005** – Bezpečnostné aspekty, pokyny pre ich začlenenie do noriem – pojem **bezpečnosť** znamená ***neprítomnosť neprijateľného rizika*** *(safety – freedom from unacceptable risk).*

Korzeniowski definuje bezpečnosť ako *určitý objektívny stav, ktorý spočíva v neprítomnosti ohrozenia, ktorý subjektívne cítia (vnímajú) jedinci alebo skupiny (Korzeniowski 2005, 2007, 2008).* Význam pojmu bezpečnosť určuje tromi atribútmi: *subjekt so svojimi schopnosťami aktivity; stav – objektívna situácia spočívajúca v chýbajúcom ohrození; subjektívny pocit.* Bezpečnosť ako predmet výskumu má multilaterálnu (mnohostrannú) povahu a je niečím viac, než súhrnom neprítomnosti ohrozenia *(Korzeniowski, 2013).*

Dinesh Mohan, jeden z popredných svetových odborníkov na otázky bezpečnosti prevádzky a ľudskej tolerancie voči zraneniam definuje bezpečnosť ako *stav, v ktorom sú ohrozenia a podmienky vedúce k fyzickým, psychickým, psychologickým alebo materiálnym úrazom kontrolované kvôli zachovaniu zdravia a dobrého sebavedomia osôb i celého spoločenstva (Mohan, 2003).*

Ryszard Zięba ukazuje dve poňatia chápania termínu „bezpečnosť“. Úzke poňatie, ktoré Joseph S. Nye nazýva *negatívnym (Nye, 1989),* vníma bezpečnosť ako *neprítomnosť ohrozenia* a sústreďuje sa na analýzu pôsobenia subjektu pre ochranu pred ohrozeniami jeho podstatných vnútorných hodnôt. Bezpečnosť je tu definovaná v protiklade k ohrozeniu. Druhé, *pozitívne poňatie,* pozoruje formovanie istoty prežitia, vlastnenia a slobody rozvoja subjektu. *Tu je bezpečnosť definovaná z hľadiska schopnosti kreatívnej aktivity subjektu (Zieba, 2004).*

Šimák a kol. uvádzajú v spracovanom Terminologickom slovníku krízového manažmentu, že bezpečnosť je *stav spoločenského, prírodného, technického, technologického systému alebo iného systému, ktorý v konkrétnych vnútorných a vonkajších podmienkach umožňuje plnenie stanovených funkcií a ich rozvoj v záujme človeka a spoločnosti.*

Viktor Porada definuje stav bezpečnosti ako *systém navzájom súvisiacich a do rôznej miery vplyvných činiteľov a ich vlastností, ktoré ovplyvňujú vznik, vývoj a následky spoločenských javov, ktoré majú negatívny vplyv na zdravie, život a všetky ďalšie hodnoty v konkrétnej spoločnosti (sociálny systém, sloboda, viera, majetok a pod.) (Porada, 2003).*

Filozof **W. Tulibacki** považuje bezpečnosť za konfiguráciu situácií, udalostí, skutočností a stavov, ktoré záležia alebo nezáležia odľudí. „*Tak chápaná bezpečnosť predchádza iným hodnotám, tiež je jednou zo základných hodnôt a plní inštrumentálnu rolu pre vznik a existenciu materiálnych a duchovných hodnôt*“ *(Tulibacki, 1999).*

Pre **W. I. Jaročkina** je bezpečnosť „*stav ochrany osoby, spoločnosti, štátu pred vonkajšími a vnútornými nebezpečenstvami a ohrozeniami, ktorý spočíva v aktivite ľudí, spoločnosti, štátu, svetovej spolupráce národov pre odhalenie, zabránenie, oslabenie, odstránenie (likvidáciu) a odrazenie nebezpečenstva a ohrození schopných ich zničiť, pripraviť o základné materiálne a duchovné hodnoty, urobiť neprípustnú (objektívne a subjektívne) škodu, zavrieť cestu pre život a rozvoj“ (Jaročkin, 2000).*

V. K. Senčagov definuje bezpečnosť ako *schopnosť života akéhokoľvek biologického objektu (Senčagov, 2015).*

V Rusku je kategória „bezpečnosti“ prítomná v právnom systéme Federácie, kde sa vychádza z toho, že „*bezpečnosť je stav ochrany životne dôležitých záujmov osoby, spoločnosti a štátu pred vnútornými a vonkajšími ohrozeniami*“.

Kovács *(2008)* uvádza, že bezpečnosť je pojem ***ťažko merateľný,*** preto ju môžeme iba vymedzovať pojmami:

- **negatívna bezpečnosť** – existencia relevantnej hrozby,
- **pozitívna bezpečnosť** – zabezpečená eliminácia existujúcich hrozieb.

2.1.1 Prehľad prístupov k bezpečnosti

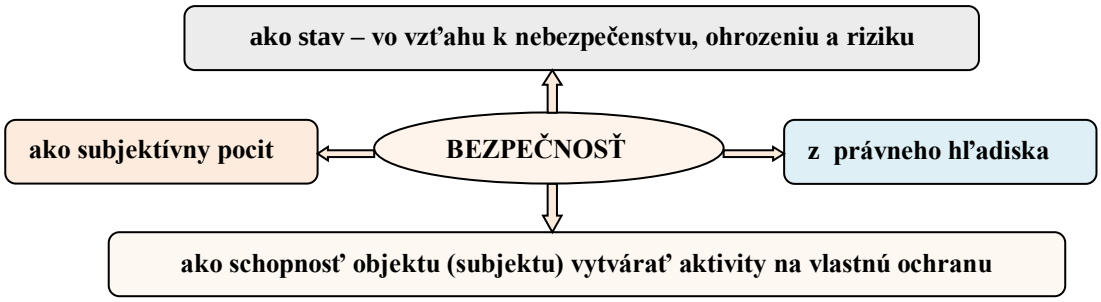
Podľa toho, ako je v definíciách vnímaná podstata a význam bezpečnosti, môžeme **jednotlivé prístupy k bezpečnosti** kategorizovať podľa obr. 1.

a) Ako stav vo vzťahu k nebezpečenstvu, ohrozeniu a riziku:
- kategória, v ktorej sa chápe ***bezpečnosť ako prípustná miera nebezpečenstva (ohrozenia)***.
- vo svojom absolútnom význame je vyjadrením ***neprítomnosti (neexistencie) bezpečnostných rizík s úrovňou vyššou ako prijateľné riziko,***
- stav, v ktorom sú ***riziká odstránené alebo znížené na prijateľnú mieru***.

b) Ako subjektívny pocit – pri ktorom sa daný ***objekt necíti byť ohrozený*** z hľadiska svojich oprávnených záujmov.

c) Ako schopnosť objektu (subjektu) vytvárať aktivity na vlastnú ochranu:
- ***schopnosť objektu, javu, procesu chrániť svoju podstatu*** a základnú charakteristiku v podmienkach cieľavedome zameranej, rozvratnej a deštruktívnej činnosti či už zvonka, alebo zvnútra objektu.
- ako ***rozhodujúca podmienka (garant) existencie jedinca (občana), sociálnej skupiny, štátu,*** ktorá umožňuje chrániť a rozmnožovať ich materiálne a duchovné bohatstvo.

d) Z právneho hľadiska – ***súhrn spoločenských vzťahov, ktoré upravujú právne normy*** a ktoré chránia práva a oprávnené záujmy jednotlivcov, sociálnych skupín, organizácií, štátu a životného prostredia.



Obr. 1 Prístupy k bezpečnosti

Pri rešpektovaní rôznych prístupov k definovaniu bezpečnosti možno konštatovať, že **bezpečnosť (byť v bezpečí)** v súhrne znamená stav:

- **neprítomnosti** (neexistencie) **bezpečnostných rizík s úrovňou vyššou ako prijateľné riziko,**
- **odolnosti proti bezpečnostnému riziku, schopnosti čeliť mu,**

- **ochrany pred bezpečnostným rizikom – súhrn opatrení na ochranu životných záujmov všetkých subjektov (objektov) bezpečnosti,**
- **schopnosti rýchlo obnoviť svoju činnosť, čím je zachovaná funkčná spôsobilosť,**
- **rešpektovania bezpečnostných právnych noriem.**

Takto štruktúrovaná definícia bezpečnosti sa vzťahuje na všetky zraniteľné a cenné aktíva:

- **osoby, spoločnosti, národy,**
- **iné živé tvory,**
- **hmotný majetok,**
- **nehmotný majetok,**
- **schopnosť vykonávať určité činnosti.**

2.2 DEFINÍCIE POJMU BEZPEČNOSŤ

Rôzny výklad pojmu bezpečnosť sa vyskytuje aj v niektorých bezpečnostných právnych normách a vydaných slovníkoch.

2.2.1 Ústavný zákon č. 227/2002 Z. z. o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu

V tomto zákone je **bezpečnosť** definovaná ako: ***stav,*** *v ktorom je zachovávaný mier a bezpečnosť štátu, jeho demokratický poriadok a zvrchovanosť, územná celistvosť a nedotknuteľnosť hraníc štátu, základné práva a slobody a v ktorom sú* ***chránené životy a zdravie osôb, majetok a životné prostredie.***

2.2.2 Bezpečnostná stratégia Slovenskej republiky

V Bezpečnostnej stratégii Slovenskej republiky (ďalej len SR) z roku 2005 je bezpečnosť charakterizovaná:

- **Bezpečnosť občana a štátu** je možné dosiahnuť len v stabilnom bezpečnostnom prostredí s možným predvídateľným vývojom, takéto prostredie sa vytvára pevným ukotvením SR v systéme medzinárodných noriem a inštitúcií, ktoré slúžia na vytvorenie stabilného a transparentného prostredia a na zvýšenie dôvery v medzinárodných vzťahoch.
- **Bezpečnosť SR** je zviazaná s bezpečnosťou štátov v euroatlantickej oblasti a závisí od globálnej bezpečnosti.
- **Úroveň našej bezpečnosti** odráža našu schopnosť spolupracovať a zapájať sa do riešenia konfliktov za našimi hranicami tam, kde je zdroj hrozby a nestability.
- **Bezpečnosť SR** sa nestotožňuje len s územnou obranou. SR je odhodlaná v zmysle solidarity a v spolupráci s medzinárodným spoločenstvom angažovať sa na zaručovaní bezpečnosti a stability a zmierňovaní následkov kríz iných štátov a národov.

2.2.3 Terminologický slovník bezpečnostného manažmentu

Vo výkladovom slovníku „Terminológia bezpečnostného manažmentu“ je **bezpečnosť** definovaná ako: bezstarostnosť, bezpečnosť, istota, záruka, ale aj duševný pokoj, ochrana, zabezpečenie, určitosť, nespornosť – znamená **stav,** ***v ktorom je zachovaná vnútorná bezpečnosť a poriadok, demokratické základy štátu, jeho suverenita a integrita a je chránené životné prostredie*.**

a) Bezpečnosť vo význame vnútornej bezpečnosti môžeme chápať ako:
   - ***súhrn spoločenských vzťahov,*** ktoré upravuje právo a ktoré chránia práva a oprávnené záujmy fyzických a právnických osôb, záujmy spoločnosti a ústavné zriadenie republiky;
   - ***faktický stav*** (úroveň), ako sa tieto vzťahy chránia;
   - *kategóriu,* v ktorej sa chápe bezpečnosť ako ***prípustná miera nebezpečenstva*.**

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

c) Bezpečnosť je tiež definovaná z týchto hľadísk:
   - *stav bezpečia;*
   - *stav ochrany pred nebezpečenstvom, bezpečie;*

- *ochrana (safeguarding) štátu, organizácie, osoby a pod.; pred nebezpečenstvom (danger), špionážou, krádežami;*
- *nezávislosť, oslobodenie od pochybnosti; dôvera; istota;*
- *nezávislosť od dozoru (ochrany), od úzkosti, znepokojenia, obáv; pocit slobody; nezávislosť od nebezpečenstva;*
- *vlastnosť byť bezpečne stabilný, pevný, stály; stabilita; pevnosť, ustálenosť, istota;*
- *niečo, čo zabezpečuje bezpečnosť, neporušiteľnosť, nedotknuteľnosť (safe); ochrana (protection), ochrana (guard),* obrana *(defence);* a pod.

d) Okrem definovania existencie bezpečnosti ako určitého stavu, existuje aj **vnímanie bezpečnosti**, v dôsledku ktorého môže byť definovaný stav:
- *objektívnej bezpečnosti, daný absenciou ohrozenia, alebo*
- *subjektívnej bezpečnosti, ako dôsledok absencie vnímania ohrozenia.*

e) Bezpečie znamená:
- *pocit bezpečia pred zranením, úrazom, nemať pocit nebezpečenstva;*
- *záchrana, ochrana pred rizikom a nebezpečenstvom;*
- *prostriedok na zachovanie bezpečia, sebaochrana pred nebezpečenstvom a pod.*

2.2.4 Elektronický krátky slovník slovenského jazyka

Elektronický krátky slovník slovenského jazyka (SLEX 99) uvádza tieto významy:

a) Bezpečnosť:

1. istota; ochrana; zabezpečenie: *osobná bezpečnosť; bezpečnosť práce; bezpečnosť jazdy; systém kolektívnej bezpečnosti; bezpečnosť štátu;*

2. policajné orgány, polícia; policajný úrad: *oznámiť niečo bezpečnosti;*

b) Bezpečný:

1. majúci pocit bezpečia, poskytujúci ochranu pred nebezpečenstvom: *bezpečný úkryt; byť na bezpečnom mieste:*
- neohrozený, istý: *cítiť sa bezpečný; utečenci boli v lese bezpeční, neohrození, zaistiť bezpečný presun tovaru;*
- nepochybný, zaručený, istý: *bezpečný dôkaz;*
- istý: *cítila sa doma bezpečná, istá;*
- spoľahlivý, zaručený (z hľadiska bezpečia): *schovať vec na spoľahlivom, zaručenom mieste;*
- zabezpečený, zaistený: *zabezpečený, zaistený úkryt.*

2. isto: zaručujúc ochranu pred nebezpečenstvom, bez pocitu ohrozenia; nevyvolávajúc pocit ohrozenia; nevyvolávajúc pocit nebezpečenstva:
- iste, bezpečne, neohrozene: *medzi priateľmi sa cítil isto, bezpečne;*
- spoľahlivo: *stroj pracuje isto, spoľahlivo, bezpečne;*

c) Bezpečne: *bezpečne skryť; bezpečne uložené peniaze; bezpečne pristáť; bezpečne viesť;*

d) Bezpečnostný: *bezpečnostné opatrenia; bezpečnostné zariadenie; bezpečnostný referent;*

e) Bezpečie: *bezpečné miesto: byť v bezpečí, dostať sa do bezpečia.*

2.2.5 Krátky slovník slovenského jazyka

Bezpečnosť:

1. istota, bezstarostnosť: *osobná bezpečnosť, bezpečnosť a hygiena práce, bezpečnosť jazdy;*
2. zabezpečenie, ochrana poriadku, pokoja, mieru: *verejná, štátna bezpečnosť; orgány národnej bezpečnosti; politicky kolektívna bezpečnosť – zmluva o kolektívnej bezpečnosti;*

2.2.6 Bezpečnosť v anglickom jazyku

V slovenskom i nemeckom *(Sicherheit)* jazyku sa na rozdiel od angloamericky hovoriaceho prostredia používa len jeden pojem „bezpečnosť“ oproti ich:

a) „**Security**“ – bezpečnosť, tiež nazývaná spoločenská bezpečnosť *(Social Safety)* alebo verejná bezpečnosť *(Public Safety),* znamená riziko ublíženia v dôsledku úmyselných trestných činov, ako je ohrozenie osobnej bezpečnosti napadnutím *(Asault),* lúpežné vlámanie *(Burglary)* alebo vandalizmus (*Angriffs Sicherheit* – bezpečnosť pred napadnutím). Vzhľadom na otázky morálky má bezpečnosť *(Security)* pre väčšinu ľudí väčší význam než skutočné bezpečie *(Safety).* Napríklad smrť spôsobená vraždou sa považuje za horšiu ako smrť pri autonehode, aj keď v mnohých krajinách sú úmrtia v doprave častejšie než vraždy. Bezpečnosť znamená teda stupeň odolnosti proti, alebo ochranu pred poškodením *(Harm).*To sa vzťahuje na všetky zraniteľné a cenné aktíva, ako sú osoby, obydlia, spoločnosti, štát alebo organizácie.

b) „**Safety**“

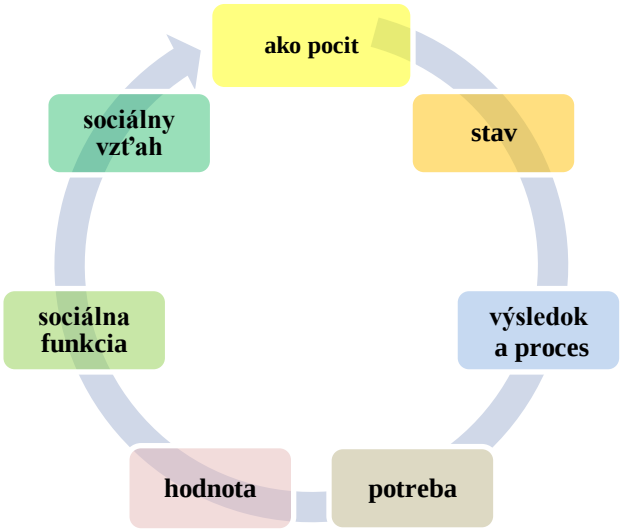
- stav bytia v „bezpečí“ *(Safe, fr. sauf),* spoľahlivosti, istoty, bez rizika, stav chránený pred fyzickým, sociálnym, duchovným, finančným, politickým, emocionálnym, pracovným, psychologickým, výchovným alebo iným druhom následkov zo zlyhania, poškodenia, chyby, poruchy, úrazu alebo inej udalosti, ktorá môže byť považovaná za nežiaducu *(Betriebs Sicherheit* – bezpečnosť prevádzky, ochrana podniku),
- riadenie zisteného rizika na dosiahnutie jeho prijateľnej úrovne, ochrana pred udalosťami alebo vystavením niečomu, čo môže spôsobiť zdravotnícke alebo ekonomické straty (zaobchádzanie s rizikom), zahŕňa ochranu ľudí a majetku.

Pojem Safety má dva mierne odlišné významy bezpečnosti, napr. bezpečnosť domu môže znamenať schopnosť budovy chrániť pred vonkajšími udalosťami, ktoré môžu spôsobiť škody (ako je počasie, vniknutie do domu a pod.), alebo môže znamenať, že jeho vnútorné zariadenia (napr. spotrebiče, schodištia a pod.) sú bezpečné (nie sú nebezpečné alebo škodlivé) pre svojich obyvateľov.

2.3 VLASTNOSTI BEZPEČNOSTI

Pri charakterizovaní pojmu bezpečnosť sa prejavujú niektoré jej osobitosti, relativita a rozdielnosť. Na posudzovanie bezpečnosti možno použiť charakteristiky podľa obr. 2 (*Hofreiter, 2006)*:

1. **Bezpečnosť ako pocit – *objektívna a subjektívna stránka bezpečnosti.***
2. **Bezpečnosť definovaná ako stav – *relativita bezpečnosti.***
3. **Bezpečnosť ako výsledok a proces – *užšie a širšie ponímanie bezpečnosti.***
4. **Bezpečnosť ako potreba.**
5. **Bezpečnosť ako hodnota.**
6. **Bezpečnosť ako sociálna funkcia.**
7. **Bezpečnosť ako sociálny vzťah.**



Obr. 2 Vlastnosti bezpečnosti

2.3.1 Bezpečnosť ako pocit – objektívna a subjektívna stránka bezpečnosti

Potreba istoty a bezpečnosti patrí medzi základné potreby, ktoré vytvárajú podmienky na spokojný život človeka a celej spoločnosti. Človek je súčasťou bezpečnosti v pozícii poznávajúceho a konajúceho subjektu. Definície pojmu bezpečnosť sa koncentrujú na jeho objektívne a subjektívne aspekty. **Bezpečnosť** má teda charakter subjektovo-objektívneho vzťahu, v rámci ktorého rozoznávame jeho ***objektívnu aj subjektívnu stránku.*** Okrem toho má bezpečnosť svoj ***vnútorný a vonkajší rozmer*** *(Šimák, 2006).*

Podľa Korzeniowského objektívny stav bez ohrozenia, ktorý je pociťovaný subjektívne, znamená, že bezpečnosť znamená objektívny alebo subjektívny stav. Objektívne charakteristiky stavu rozhodujú o účinkoch konania človeka. Spojka alebo v tomto prípade znamená, že bezpečnosť znamená ***iba objektívny stav, alebo len subjektívny stav, alebo objektívny a subjektívny stav spolu*** *(Korzeniowski, 2013):*

- **Objektívny** – existujúci nezávisle od akéhokoľvek vedomia, nezávislý od poznávajúceho subjektu. Existujúci nezávisle od vedomia, čo neznamená, že človek neovplyvňuje túto existenciu. Práve naopak, správanie sa človeka mení objektívny stav, aj keď toto správanie je spôsobené subjektívnymi informáciami.

- **Subjektívny** – závisí od vnútorných vlastností poznávajúceho subjektu, a nie odvlastností skúmaného subjektu, podmienený zážitkami a názormi daného človeka (subjektu).

Z logickej analýzy vzťahu objektívny – subjektívny vyplývajú štyri možné situácie uvedené v tabuľke 1.

Tab. 1 Objektívna a subjektívna stránka bezpečnosti

	Stav (situácia)	**Charakteristika stavu (situácie)**
1	**Stav bezpečnosti**	• *ohrozenie je objektívne, reálne* a • ohrozený subjekt si to uvedomuje a dokáže znížiť riziko.
2	**Falošná bezpečnosť**	• *ohrozenie je objektívne, reálne* a • ohrozený subjekt o tom nevie, neuvedomuje si toto riziko.
3	**Stav ohrozenia**	• *ohrozenie je objektívne, reálne* a • ohrozený subjekt si ho uvedomuje, ale nemá možnosť, alebo nevie ako znížiť riziko.
4	**Falošné ohrozenie**	• *objektívne ohrozenie neexistuje*, ale • subjekt má falošné povedomie, predstavu ohrozenia, ktoré sa v skutočnosti nevyskytuje, • následkom čoho reaguje tak, že zbytočne míňa energiu a zdroje (obsesia).

Existuje niekoľko rôznych možností, ako môže človek reagovať na existujúce a vnímané nebezpečenstvo:

1. odstrániť nebezpečenstvo (zdroj rizika),
2. vyhnúť sa nebezpečenstvu,
3. ignorovať nebezpečenstvo a prijať riziko,
4. rezignovať na svoju ochranu a podľahnúť nebezpečnosti.

Bezpečnosť má svoj vonkajší a vnútorný rozmer:

a) Vonkajšia bezpečnosť je založená na úrovni a charaktere vonkajšieho rizika a na druhej strane na pôsobení rôznych ochranných prvkov spoločenského života (vojenských, politických, ekonomických atď.). Spočíva teda v pripravenosti a schopnosti subjektu pôsobiť voči iným objektom, ktoré ovplyvňujú jeho bezpečnosť zvonka a v kvalitách objektov schopných podieľať sa na zabezpečení bezpečnosti (danosti, vlastnosti a možnosti rôznych bezpečnostných systémov, či inštitúcií).

b) Vnútorná bezpečnosť je založená na interpretácii vlastného stavu subjektu a schopnosti znižovať vnútorné riziká, ktoré ho môžu ohroziť. Spočíva teda v pripravenosti a schopnosti subjektu aktivizovať sa pre jeho zachovanie.

2.3.2 Bezpečnosť definovaná ako stav – relativita bezpečnosti

Stav (situácia) je prívlastkom, ktorý je možné popísať vzhľadom na to, že:

- vždy je časový úsek, v ktorom stav (situácia) začína a má svoj koniec, v skutočnosti každý stav je určený krajnými hodnotami začiatku a konca,
- každý subjekt (objekt) v danom časovom úseku má nejakú charakteristiku,
- medzi subjektmi (objektmi) vznikajú určité vzťahy,
- v stabilnom stave charakteristiky subjektov (objektov) majú stále hodnoty.

Bezpečnosť je ***pojem stupňujúci sa medzi absolútnou bezpečnosťou a totálnym nebezpečenstvom,*** podobne ako pravda medzi absolútnou pravdou a absolútnou nepravdou.

Keďže bezpečnosť je funkciou mnohých ohrození, tak môžeme dosiahnuť len jej určitú úroveň:

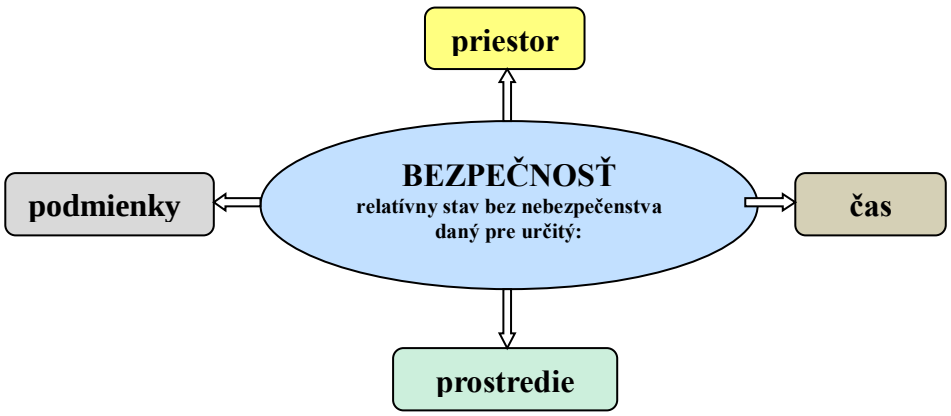
- keď prevažuje pravdepodobnosť zachovania existencie života a vývoja, hovoríme, že subjekt je (skôr) bezpečný,
- keď prevláda ohrozenie, hovoríme, že subjekt (objekt) je (skôr) ohrozený.

Samozrejme, že v dôsledku vlastného (alebo cudzieho) konania, zameraného na zmenu druhu a sily ohrozenia, môže subjekt zmeniť úroveň vlastnej bezpečnosti. Hodnota bezpečnosti teda nie je trvalou veličinou, ale sa mení, jednak v priestore, ale najmä v čase. Vplyvom vonkajších i vnútorných činiteľov, ktoré môžu mať najrôznejšiu povahu, má bezpečnosť kolísavú úroveň – buď sa bezpečnosť ***zvyšuje***, buď ***klesá***, alebo dočasne ***zostáva bez zmien.***

Bezpečnosť definovaná ako stav znamená jej relativitu.

Relativita bezpečnosti znamená, že *v komplexných systémoch nie je možné riziká úplne vylúčiť,* bezpečnosť sa podľa obr. 3 preto všeobecne môže chápať iba ako:

- **relatívny stav** bez nebezpečenstva,
- ktorý je daný len pre **určitý priestor, čas a určité prostredie,**
- alebo existuje za **určitých podmienok.**



Obr. 3 Relativita bezpečnosti

Veľkosť ohrozenia závisí od mnohých faktorov a hodnotí sa podľa rozličných subjektívnych a kultúrnych hodnôt. V extrémnom prípade môžu všetky bezpečnostné opatrenia stroskotať pre javy, ktoré sa nedajú ovplyvniť alebo predvídať, napr. dopad meteoritu. Bezpečnosť preto neznamená, že riziká sú úplne vylúčené, ale len, že sú v dostatočnej miere nepravdepodobné.

2.3.3 Bezpečnosť ako výsledok a proces – užšie a širšie ponímanie bezpečnosti

V užšom ponímaní sa bezpečnosť chápe ako ***funkčná sféra, oblasť činnosti, či ako bezpečnostná politika.*** Toto užšie poňatie je dynamické, teda videné ako proces: Zahŕňa cyklus manažérstva bezpečnosti a vzťahuje sa k vedomej a riadenej činnosti konkrétnych subjektov a inštitúcií. Najvšeobecnejšie sa charakterizuje ako absencia, neprítomnosť nebezpečenstva alebo ohrozenia. Takto ponímaná bezpečnosť nemôže byť iná, než ***relatívna.***

V širšom ponímaní sa bezpečnosť chápe ako ***všeobecný atribút*** (podstatná, základná charakteristická vlastnosť). Bezpečnosť ako atribút, s určitou mierou či hodnotou, môže byť pripísaná takmer čomukoľvek, napr.: *bezpečná vzdialenosť, bezpečný zdroj informácií, bezpečné dodávky surovín.* Takto chápaná bezpečnosť je synonymom pre stabilitu, poriadok,

určitosť, spoľahlivosť, rovnovážny stav, existenciu subjektu bez hrozieb, stav a pocit istoty, zabezpečenosť, bezproblémový stav. Ide o proces, v ktorom ide o odvrátenie, oslabenie alebo elimináciu hrozieb vyplývajúcich z bezpečnostného prostredia – ***realistický prístup k bezpečnosti.***

Hodnota (miera) bezpečnosti človeka, sociálnej skupiny, štátu (objektov) bude vždy *výsledkom interakcie vonkajších a vnútorných bezpečnostných rizík a ochranných (obranných) vlastností, schopností a možností subjektu (objektu) ako nositeľa bezpečnosti.*

Vo vzťahu k akémukoľvek subjektu možno pojem bezpečnosť vymedziť ako „stav, keď sú na najnižšiu možnú mieru eliminované hrozby pre objekt (s jeho záujmami)". Platí pri tom, že objekt je na elimináciu súčasných i potenciálnych hrozieb efektívne vybavený a je ochotný pri utváraní vlastnej bezpečnosti spolupracovať.

2.3.4 Bezpečnosť ako potreba

Bezpečnosť ako potreba znamená:

- pocit nedostatku niečoho, čo je nevyhnutné pre život a rozvoj jedinca vzhľadom na biologické, spoločenské a kultúrne zretele,
- špecifický stav organizmu spôsobený nedostatkom niečoho, čo je preňho dôležité, niekedy aj bezpodmienečné pre jeho existenciu, rozvoj a normálne fungovanie,
- je významným motivujúcim, mobilizujúcim faktorom, ktorý sa významne prejaví najmä v mimoriadnych a krízových situáciách, v čase ohrozenia bezpečnosti človeka a iných sociálnych subjektov.

2.3.5 Bezpečnosť ako hodnota

Bezpečnosť má podstatný význam ako pre fungovanie štátu, tak aj pre existenciu človeka ako indivídua. Bezpečnosť nadobúda formu vnútornej hodnoty a realizuje sa v individuálnom i spoločenskom vedomí. Charakteristické je, že táto hodnota má univerzálny charakter a je vo svojej podstate uznávaná všetkými ľuďmi, nezávisle od ich rasy, národnosti, pohlavia, veku či sociálneho statusu. Hodnota bezpečnosti sa však mení tak, ako sa mení situácia. Maslow uvádza, že najvyššiu hodnotu má vždy tá potreba, ktorej deficit pociťuje človek najviac. Pritom platia zásady:

- v dobe mieru, v blahobyte, počas pokoja a dostatku hodnota bezpečnosti klesá,
- keď sa objavia sociálne nepokoje, bieda, vojny, teroristické útoky, narastá kriminalita, hodnota a potreba bezpečnosti prudko narastá (ochota vynaložiť väčšie náklady na bezpečnosť, dokonca pristúpiť na obmedzenie niektorých ľudských práv).

2.3.6 Bezpečnosť ako sociálna funkcia a sociálny vzťah

Bezpečnosť ako sociálna funkcia – z hľadiska funkčného prístupu zaistenie bezpečnosti predstavuje súhrn politických, hospodárskych, vojenských, sociálnych a iných opatrení a nástrojov:

- na zaručenie a ochranu národného záujmu pred vnútornými a vonkajšími rizikami a ohrozeniami,
- na zaručenie stáleho progresívneho rozvoja života občana, sociálnych skupín a štátu,
- na ochranu života, slobody a majetku občana a štátu,
- na ochranu životného prostredia.

Bezpečnosť ako sociálny vzťah – je charakterizovaný vzájomnou dôverou, vzťahmi bez agresívnych a nepriateľských aktivít. Aby sa upevnili vzťahy bezpečnosti, aby bola garantovaná ich stabilita a neporušiteľnosť, boli medzi ľuďmi, národmi a štátmi prijaté ***normy***

a princípy bezpečnosti vo vzájomných vzťahoch, ktoré existujú vo forme zákonov, spoločenských noriem, bilaterálnych a multilaterálnych zmlúv. Na zaistenie bezpečnosti vznikli také inštitúcie ako armáda, polícia, rôzne druhy bezpečnostných a záchranných služieb.

2.3.7 Ďalšie vlastnosti bezpečnosti

Bezpečnosť sa vyznačuje aj inými vlastnosťami:

- bezpečnosť je celistvým stavom subjektu (objektu), má **nedeliteľný charakter,** ktorý súvisí vždy s jeho systémovými väzbami,
- bezpečnosť obvykle **nie je v priestore rozložená rovnomerne,** ale rôzne prvky systému (podsystémy) môžu mať rôzny stav bezpečnosti, systém je potom natoľko bezpečný, nakoľko je bezpečný jeho ***najmenej bezpečný podsystém,***
- veľkosť ohrozenia chránených záujmov subjektu (objektu) vyjadruje **úroveň bezpečnosti,** ktorá je aj v usporiadanom systéme závislá od všetkých prvkov systému,
- požadovaná **úroveň bezpečnosti** je výrazom individuálne nastavenej hodnoty veľkosti akceptovateľného rizika.

2.3.8 Bezpečnosť ako vzťah

V bežnej i odbornej praxi sa výraz ***bezpečnosť*** používa vo vzťahu k určitej ***oblasti, chránenému subjektu alebo rizikám,*** ktoré im hrozia.

Tab. 2 Možný obsah a štruktúra pojmu bezpečnosť (zdroj: Reitšpís, 2004)

AKÁ ?	KOHO ? ČOHO ?	PRED AKÝMI RIZIKAMI ?
• vnútorná • politická • vojenská • technologická • ekonomická • surovinová • ekologická • biologická • informačná • genetická	• planéty, kontinentu, regiónu • štátu • sociálnej skupiny • občana • objektu • organizácie, podniku • mesta (obce) • systému • procesu	• sociálnej povahy • prírodnej povahy • technologickej povahy

Záver k vlastnostiam bezpečnosti: Bezpečnosť treba chápať ako trvalý, cyklický a nepretržitý proces reagovania na riziká vyplývajúce z okolia (z bezpečnostného prostredia) objektu (subjektu) alebo z objektu (subjektu) samého. Je to proces, umožňujúci nepretržite realizovať opatrenia na zaistenie ochrany osôb, majetku a životného prostredia, a to vždy v ľubovoľných podmienkach a situáciách.

Platí, že subjekt (objekt) bude tým bezpečnejší, čím budú vyššie jeho:

- schopnosti ***včas identifikovať bezpečnostné riziká*** a
- možnosti trvalo ***ochraňovať svoje aktíva*** (životné záujmy) pred neustále sa meniacimi (vyvíjajúcimi sa) bezpečnostnými rizikami najrôznejšej povahy.

2.4 ROZPORY

Herakleitos – *„len vďaka* ***kontrastu*** *sa všetky veci vytvárajú či dospievajú k zániku“.*

Engels – *„pokiaľ uvažujeme veci ako stávajúce v pokoji a neživé, každú pre seba, vedľa seba a po sebe, nenarazíme u nich samozrejme na žiadne rozpory, ale úplne inak to dopadá, keď uvažujeme veci v ich pohybe, v ich zmene, v ich živote,* ***v ich pôsobení na seba navzájom****“.*

G. W. F. Hegel – *„****vzájomné pôsobenie*** *je pravá konečná príčina vecí“.*

Rôzne filozofie, pokiaľ nejaký vývoj uznávali, hľadali obvykle iba jeho vonkajšie zdroje, ležiace mimo veci či javu a zvonku na ne pôsobiace. Zatiaľ čo materialisti pátrali po hmotnej, idealisti predpokladali ideovú hmotnú silu. Nikdy ich nenašli, a preto si ich museli vymýšľať. A pritom je to jednoduché.

Hybnou silou sveta je jeho ***rozpornosť, ktorá ho udržiava v neustálom pohybe.***

Hlavnú hybnú silu všetkého vo vesmíre musíme hľadať vo vnútri podstaty všetkých vecí a javov.

Vec môže byť **objektívne existujúci stav**:

- všetko, čo existuje mimo človeka, abstraktný alebo aj konkrétny jav: *vzťah vecí k človeku,*
- konkrétny predmet, vnímateľný zmyslami, predmet slúžiaci človeku, osobný majetok a pod.: *vníma veci okolo seba, cenná vec, pobaliť si svoje veci,*
- fakt, skutočnosť, skutok, udalosť: *vážna vec, hlavná vec, nepríjemná vec,*
- problém, otázka, záležitosť, (akýkoľvek) výsledok práce: *to je vážna vec, tvoja vec, prišiel v úradnej veci,*
- vo filozofii: časť materiálneho sveta, ktorá má relatívne samostatnú existenciu, predmet, objekt,
- v práve: hmotný predmet alebo ovládateľná prírodná sila slúžiaca potrebám ľudí, spor, záležitosť sporu.

Jav, *fenomén* alebo *úkaz* je všetko, čo sa vníma zmyslovo, je to ***súhrn vonkajších premenlivých, zmyslami vnímaných vlastností.*** Javy sú najdôležitejšími znakmi procesov, ktoré prebiehajú vo svete. Jav, ktorý sa nemení v určitom časovom úseku, sa nazýva **stav.** Javom môže byť všetko, čo je možné zmyslami pozorovať: skutočnosť, fakt, realita, udalosti, procesy, vlastnosti.

Zdroj vývoja je vo vnútri sveta, v jeho vnútorných rozporoch. Filozofický **zákon o jednote a boji protikladov**, ktorý to formuluje, sa nazýva tiež ***zákonom rozporu***. Tento zákon objavuje príčiny vývoja, vyjadruje zdroj pohybu a vývoja (samopohybu a samovývoja) prírody a spoločnosti, je aj všeobecným zákonom poznania. Vychádza z poznania, že **všetko v prírode, spoločnosti i v myslení** je vlastne ***rozporné, protichodné, vzájomne proti sebe stojace a bojujúce.***

Každá vec a jav je **jednotou protikladnosti a protirečivosti**. Neustále striedanie sa (boj protikladov) je ***hybnou silou, dynamikou vývoja.***

V bežnom vedomí sa **jednota** považuje za stav, za vzťah dvoch objektov či subjektov. Je to iba jav, ktorého podstatou je nové spojenie zložitých a mnohotvárnych pohybov účastníkov tohto vzťahu. Veci a procesy sa spájajú ***pohybom***. *Spojením vzniká nový pohyb, majúci novú formu, spôsob či smer.* Toto spojenie však nikdy nie je úplné, nemenné a trvalé. Časť pohybu ostáva nespojená, vznikajú nové tendencie pohybu, ale staré nezanikajú. Pretože každá akcia vyvoláva reakciu, medzi spojeným a nespojeným pohybom i jeho starými a novými tendenciami vzniká ***protiklad***.

Jednota znamená nový pohyb, vnútorne protikladný proces, v ktorom protiklady vytvárajú väzbu a súčasne bránia úplnému zlúčeniu pohybov. Každá jednota je vždy **vnútorne rozporná,** vyvíjajúca sa, iba čiastočná a vždy len dočasná. ***Všetko existujúce sa neustále navzájom ovplyvňuje, a tým mení.***

2.4.1 Charakteristika rozporov

Teóriu rozporu najobsiahlejšie pojmovo spracoval G. W. F. Hegel. Dialektický **rozpor** podľa neho nie je prázdnota protikladu medzi kontradiktórnymi pojmami, ale ***jednota protikladného***. Protikladné je to, čo v sebe samom obsahuje svoj protiklad. Podľa Hegela sú všetky veci sami o sebe rozporné, **rozpor *je princíp všetkého samopohybu, koreňom všetkého žijúceho sveta, v ktorom človek žije.*** Jeho život je plný rozporov, sám ich vyvoláva i mení, bojuje s nimi i využíva ich, snaží sa ich odstraňovať, ale tým vyvoláva nové *(Hegel,1986).*

Rozumieť svetu preto znamená rozumieť jeho rozporom. Rozpory však sú často neviditeľné, nezreteľné, mávajú podobu pokoja, prebiehajú príliš rýchlo či príliš pomaly na to, aby sme ich pozorovali. Ak ich chceme poznať, môžeme tak robiť poznávaním pohybov, ktoré rozpor vyvolávajú a ich odrazov, teda pohybov zmenených.

Rozpor je jedna zo základných kategórií, ktorá vyjadruje ***vzájomné pôsobenie dvoch existujúcich protikladov, ktoré sa navzájom podmieňujú, ale zároveň sa vylučujú.*** Rozpor je výrazom jednoty a boja protikladov. Rozlišujú sa dialektické a logické rozpory. **Logický rozpor** existuje v sfére myslenia, **dialektický rozpor** je vlastný všetkým veciam, procesom, systémom objektívnej reality, predstavuje zdroj všetkého pohybu.

Každý pohyb vo svete mení iný pohyb a **každá zmena pohybu vyvoláva rozpor**, ktorý je prejavom tejto súvislosti. Vzniká tým, že sa niektoré pohyby rôzne spájajú, zatiaľ čo iné, ktoré sú súčasťou rovnakého javu, sa nespájajú a pôsobia odlišne či protikladne. Každý jav i ktorákoľvek vec preto v sebe obsahujú **rozpor, ktorý je základom ich ďalšieho pohybu, zmien a vývoja.**

Je to vnútorný vzťah medzi dvomi protichodnými, spojenými a nespojenými pohybmi a z nich vyplývajúcimi vlastnosťami veci či javu, vzťah medzi časťami celku i medzi rôznymi celkami. Oba tieto protiklady existujú závisle od seba, vzájomne sa vylučujú a podmieňujú, ale vždy majú niečo spoločné. Protiklady nemôžu existovať bez seba. Jeden protiklad chce zachovať daný stav, druhý chce jeho negáciu. Existencia veci či javu je výsledkom riešenia tohto rozporu. **Rozpor je vzťahom zmien pôsobiacich rôznym smerom.**

Funkcia rozporov je *konštruktívna i deštruktívna,* rozpor jednotu vytvára, udržiava, mení, ale aj borí.

Rozpory sú vždy *konkrétne.* Nie je možné ich stvoriť, vznikajú sami zmenou pohybu. Nie je možné ich zrušiť, iba meniť pohybom. So zánikom každého rozporu vznikajú rozpory nové. Rozumieť vývoju znamená vidieť pohyb, rozpory, ktoré vyvoláva, a ich následky. Predvídať vývoj znamená predvídať vývoj rozporov.

Každá zmena je *výsledkom rozporu*. Rozpor je vzťahom pohybov, ich konfliktom, stretom, je procesom zmeny pohybov v ich konfliktoch. V rozporoch sú dočasne ukryté, akumulované protismerné pohyby, ktoré nezanikli, iba sa navzájom brzdia, vyvolávajú zdanie pokoja, rovnováhy, ale pri zmene podmienok sa znovu, i keď inak, prejavia. To budí dojem, že rozpory sú zdrojom pohybu, v skutočnosti sú však len príčinou jeho zmien. To nič nemení na tom, že ide o samopohyb ako vlastnosť a spôsob existencie pohybujúcej sa hmoty.

Rozpory sú *vzťahy vyvolané a meniace sa pohybom*, sú stretom, súvislosťou a transformáciou pohybov. V tomto zmysle je i *rozpor zdrojom pohybu, ale nie jeho príčinou*.

Pohyb ako atribút hmoty existuje súčasne s ňou, ako jediný možný spôsob jej existencie, a nemá rovnako ako ona príčinu, je nekonečný, nezničiteľný, nestvoriteľný.

Rozpor je *podstatou boja i súladu*. Rozpory neexistujú sami osebe, vždy sú viazané na vec či jav, v ktorých sú podstatnou súčasťou. Neexistujú veci a javy vnútorne alebo zvonku nerozporné. Všetko existujúce je tvorené bojom protikladov, tento ***boj je absolútny, trvalý, je hybnou silou vývoja.*** Naopak, každý pokoj je vždy len zdanlivý a prechodný. Pri boji protikladov dochádza k negácii jedného protikladu a súčasne k vzniku nových protikladov a rozporov. Vo vývoji je vždy treba hľadať hlavné, podstatné: protiklady a určujúce stránky rozporov.

Rozpor je *všeobecnou vlastnosťou hmoty a pohybu.* Žiadny rozpor nikdy nie je jediný. Vo vnútri veci či javu ich vždy pôsobí viac. Existujú ***rozpory hlavné,*** ktoré sú nositeľom tendencie vývoja, a ***rozpory vedľajšie***. Základné rozpory pôsobia po celú dobu trvania javu ako takého, vedľajšie rozpory môžu vznikať a zanikať, bez zmeny podstaty javu. Ak sa vedľajšie rozpory stávajú hlavnými, vedie to k zmene javu. Rozpory nie sú nemenné, vyvíjajú sa nasledujúcim postupom:

- **Rozdiel** – univerzálna vlastnosť hmoty, ktorej jednotlivé časti nie sú nikdy úplne totožné, sú vždy niečím rovnaké a súčasne odlišné. Je to počiatočné štádium, podmienka formovania rozporu, vzniká odlišným pohybom častí či jednotlivých stránok vo vnútri celku od samého počiatku jeho existencie. Nemení podstatu javu, je jeho súčasťou.
- **Protiklad** – protismerný pohyb orientovaný k budúcemu stretu, ku ktorému ešte nedochádza, prípadne možnosť takého pohybu vyplýva z podmienok.
- **Rozpor** – ďalšia fáza, kedy sa už pohyby stretli, bráni jeden druhému, vzájomne sa zadržujú, uvádzajú sa do dočasného zdanlivého pokoja alebo menia svoj smer či formu. Jeho zvláštnym druhom je ***antagonismus.***
- **Odraz – *vyústenie a riešenie rozporu***, zmena pohybu, ktorý je syntézou, novou formou pohybov predchádzajúcich. Žiadny pohyb navyše tu nevznikol, žiadny nezanikol, iba sa zmenili pohyby doterajšie. Výsledkom môže byť i ***kvalitatívne vyššia forma pohybu, ktorá obsahuje formy nižšie a vzťahy medzi nimi, alebo naopak rozpad pohybu vyššieho v nižšiu formu.***

Rozpory sú *následkom i príčinou zmien pohybu*. Rozpory majú rôzne formy závislé od prostredia, v ktorom sa prejavujú. Sú rozdielne v hmote neorganickej, organickej a sociálne organizovanej – teda v spoločnosti, ale aj vo vedomí, ktoré je produktom hmoty. Každej forme pohybu zodpovedajú rôzne formy rozporov. Čím sú veci a javy zložitejšie, tím zložitejšie v nich prebiehajú rozpory. V neorganickej prírode sú rozpory skryté, ale nikto ich neskrýva. V spoločnosti sú rozpory tiež skryté, ale navyše sú ľuďmi často zámerne zastierané, popierané, vyvracané, navonok zakrývané rozpormi inými, menej dôležitými. Rozpory môžu byť ľuďmi aj zdôrazňované, absolutizované, býva zatajovaný ich skutočný význam, za hlavné môžu byť vydávané rozpory vedľajšie a naopak, preto sa rozpory v spoločnosti ťažšie hľadajú. Tým skôr, že hľadajúci je vždy v týchto rozporoch osobne zainteresovaný a obvykle sa vedome či nevedome stotožňuje s niektorým protikladom.

Rozpor je *príčinou existencie i zániku javu*. Rozpory nie sú len vo vnútri vecí a javov, ale tiež medzi nimi navonok. Vonkajšie rozpory sú vlastne vnútornými rozpormi nekonečne štruktúrovaného celku. Medzi vonkajšími a vnútornými rozpormi existuje dialektická jednota. Podobne je to so všetkými ďalšími rozpormi:

- **vnútorné rozpory** sú rozhodujúce, určujúce, sú hlavným zdrojom vývoja javu;
- **vonkajšie rozpory** ovplyvňujú rozpory vnútorné, môžu do nich prerastať a až vtedy, keď sa tak stane, keď ovplyvnia vnútorné rozpory, sa môžu stať rozhodujúcimi;

- **hlavné rozpory** sú reakciou na spojenie pohybov vo vnútri jednoty v danej situácii, ktorá sa však mení, a tým sa mení aj dôležitosť rozporov;
- **vedľajšie rozpory** vznikajú z rôzneho pôsobenia pohybov dočasne nespojených;
- **podstatné a nepodstatné rozpory** sa odlišujú podľa toho, ako sa dotýkajú podstaty javov;
- **nutné a náhodné sú rozpory** podľa miery svojej zákonitosti;
- **skutočné rozpory** sú vždy doplňované rozpormi možnými, pre ktoré ešte neboli naplnené všetky podmienky;
- **rozpory vo vnútri obsahu** sú vždy spojené rozpormi vo vnútri formy a medzi formou i obsahom;
- **rozpory v štruktúrovaných javoch** prebiehajú v rôznych rovinách a navzájom sa ovplyvňujú;
- **rozpory v spoločenských procesoch** sú navyše vždy objektívne a subjektívne, racionálne i emotívne;
- **v myslení** navyše poznáme i tzv. rozpory logické, ktoré sú iba rozdielom či protikladom poznatkov a skutočným rozporom sa stávajú iba vtedy, keď vstupujú do toho istého myšlienkového pohybu, teda do sporu.

Výsledkom rozporu je *zmena pohybu, teda odraz*. Všetky veci a javy sa vyznačujú rozpormi, sú jednotou protikladných stránok a tendencií, ktoré sa navzájom stretávajú a popierajú. Boj vnútorných protikladov vo veciach a javoch je príčinou ich zmeny, je zdrojom vývoja a vedie k zániku starého a vzniku nového. Rozpor vo veciach a javoch je vnútorný, podstatný a nutný vzťah, ktorý je zdrojom ich **samovývoja**.

2.4.2 Najdôležitejšie súčasné rozpory

Pojem rozpor sa vyjadruje prostredníctvom mnohých synoným. Podľa Synonymického slovníka slovenčiny *(2004*) r**ozpor znamená** stretnutie nezhodných názorov alebo záujmov, má význam aj ako:

- **spor**: vyriešiť rozpory, spory rokovaním,
- **nezhoda** (nedostatok zhody; *opačne.* zhoda): záujmové nezhody,
- **nesúlad** (nedostatok súladu; *opačne* súlad): nesúlad v manželstve,
- **konflikt**: dostať sa s niekým do konfliktu,
- **kolízia** (skríženie, prekrývanie sa niečoho): kolízia záujmov a povinností,
- **roztržka**, knižne **rozbroj** (prerušenie stykov pre rozpory): vyvolať roztržku,
- **rozbroj,** knižne **rozopra**: rodinná rozopra,
- **zápletka**: diplomatická zápletka,
- **protiklad** (hlboký rozpor): boj protikladov,
- **protirečenie, kontradikcia**: v jeho prejave je plno protirečení,
- **antagonizmus** (nezmieriteľné protirečenie): spoločenský antagonizmus,
- **nesúhlas**: nesúhlas vo výpočtoch,
- **konfrontácia** (nezhoda v názoroch): konfrontácie medzi politikmi,
- **kontroverzia**: došlo medzi nimi ku kontroverzii.

Medzi základné rozpory patria rozpory uvedené v tabuľke 3 *(Šimák, 2006)*.

Tab. 3 Základné rozpory (zdroj Šimák, 2006)

ROZPORY			
Človek a príroda	***Človek a technológie***	***Človek a ľudské spoločenstvo***	***Ľudské spoločenstvá navzájom***

Rozpory medzi človekom a prírodou

Ľudia pretvárajú prírodu, často deštrukčným spôsobom, prispôsobujú ju svojim potrebám, pričom pôsobia nepriaznivo na jej chod a v konečnom dôsledku aj na vlastnú existenciu. Rozpory medzi ľudskými aktivitami a prírodou so sebou prinášajú množstvo **príležitostí,** ale aj **nebezpečenstiev.**

Otázka životného prostredia je v dnešnej dobe je asi najväčším spoločenským problémom. Jadrové elektrárne, freóny, havárie ropných tankerov a vlakov, výrub lesov, zabíjanie zvierat, výstavba, ale aj odhadzovanie odpadkov, to sú len niektoré z problémov. Dochádza ku globálnemu otepľovaniu, ľadovce sa topia a tým sa zvyšuje hladina vodných tokov, ktoré zaplavujú najnižšie položené miesta na svete, vytvára sa ozónová diera, výrubom lesov prichádzame každodenne o tisícky litrov kyslíka prepotrebného pre náš život. Mnohonásobné zvyšovanie intenzity čerpania prírodných zdrojov spôsobujú zjavné i skryté konflikty a boj o ovládnutie energetických a vodných zdrojov obývateľného územia.

Pri hodnotení súčasného sveta musíme brať do úvahy globálne problémy, ktoré sú odrazom vzťahu človeka a spoločnosti k prírodnému prostrediu, vzťahu štátov k prírodným zdrojom, k bezpečnosti života na zemi. Dotýkajú sa životných záujmov všetkých národov, štátov, koalícií (skupín) štátov, a predstavujú ohrozenie bezpečnosti celého ľudstva. Dôsledkom ich neriešenia môže byť zánik ľudskej civilizácie ako takej, vážny regres podmienok života.

Všetky uvedené **nebezpečenstvá** môžu spôsobiť **environmentálne riziká**, ktoré sa prejavujú ako rôzne ***živelné pohromy a katastrofy*** s negatívnymi následkami pre životné prostredie, ľudskú spoločnosť a jej majetok.

Rozpory medzi človekom a technológiami

Technológia predstavuje odbor zaoberajúci sa premenou materiálov na konečné výrobky (statky a služby) za využitia technických a prírodovedeckých poznatkov, a uplatňovaním týchto poznatkov pri zdokonaľovaní výrobných postupov. Zahŕňa zložky: techniku (nástroje, prístroje a pod.), organizáciu, hmotné predpoklady a pod.

Technologické systémy môžu odkazovať na hmotné objekty, používané spoločnosťou, ako sú stroje, hardvér alebo nástroje, ale môže tiež zahŕňať širšie témy, vrátane rôznych systémov, metód organizácie a techniky. Termín sa môže vzťahovať všeobecne, alebo špecificky na konkrétne oblasti, napr. výrobné technológie, stavebné technológie, zdravotnícke technológie atď.

Technologický proces je súbor technických činností určitého druhu potrebných na zhotovenie určitého výrobku (napr. odlievanie, sústruženie, zváranie, ale aj výroba softvéru a pod.). Proces zdokonaľovania techniky a technológie je trvalý a stále dynamickejší a prináša množstvo ***príležitostí.***

Zložitejšia technika a náročnejšie technológie však zvyšujú aj ***nebezpečenstvo***, ako zdroj technických a technologických rizík, ktoré môže spôsobiť ***incidenty, nehody, poruchy, prerušenie činností, havárie a katastrofy,*** s rozsiahlymi negatívnymi následkami pre osoby, majetok (produkciu), ale určitým spôsobom aj na životné prostredie.

Rozpory medzi človekom a ľudským spoločenstvom

Ľudské spoločenstvo je usporiadané spoločenstvo ľudí, ktorí obývajú určité územie, sú spojení výmenou a spoluprácou a riadení svojimi vlastnými inštitúciami. Je to skupina ľudí tvoriaca polouzavretý alebo polootvorený spoločenský systém, v ktorej väčšina vzťahov je v rámci skupiny.

Spoločenský systém je najzložitejší systém zo známych systémov. Je to dynamický systém a zároveň systém s cieľovým správaním, ktorý sa skladá z ľudí, má zložité vnútorné väzby, vyznačuje sa sekundárnou adaptabilitou, má mnohoznačné správanie, učí sa atď. Existujú ***formálne*** spoločenské systémy (oficiálne ustanovené) a ***neformálne*** spoločenské systémy. Základným podsystémom spoločenského systému je človek. Spoločenská podstata spája človeka s ďalšími ľuďmi, pričom sa snaží využiť množstvo ***príležitostí,*** ktoré mu toto spojenie prináša.

Spoločenský proces je proces tvorený sériou vzájomného pôsobenie ľudí na seba alebo série javov existujúcich v organizácii a štruktúre skupín, ktoré menia vzťahy medzi ľuďmi alebo vzťahy medzi jednotlivými súčasťami pospolitosti. V súčasnosti sa v modernej spoločnosti vyskytujú najmä tieto **sociálne rozpory**:

1. **Tradičné sociálne rozpory** – spoločnosť rozdelená na vládnucu a ovládanú časť:
2. **Súčasné sociálne rozpory** – sociálna stratifikácia (rozvrstvenie spoločnosti):
   - horné vrstvy (majetní vlastníci, politici, právnici, umelci, lekári, panovnícky rod),
   - stredné vrstvy (učitelia, kvalifikovaní robotníci, administratíva, technici),
   - dolné vrstvy (trieda chudoby, nekvalifikovaní, sezónni robotníci...),
   - študenti a dôchodcovia (príliš sa s nimi v politike neuvažuje).

Hlavným rozporom modernej spoločnosti je ***rozpor medzi rastúcou produkciou bohatstva a prehlbujúcou sa nerovnomernosťou jeho rozdeľovania a individuálnych príležitostí***. Vláda vytvára systém na čiastočné prerozdeľovanie bohatstva (dane, ktoré prerozdeľuje do zdravotníctva, školstva a pod.). Tento systém jednotlivé sociálne skupiny kritizujú, každá zo svojho hľadiska. Presadzujú sa individuálne postoje a záujmy a rozpory s postojmi niektorých jednotlivcov a skupín sa môžu prehlbovať, čím vzniká ***nebezpečenstvo,*** že ich budú riešiť neprimeraným spôsobom.

Rozpory medzi ľudskými spoločenstvami

Hlavnými činiteľmi, ktoré ovplyvňujú súčasné bezpečnostné prostredie sa stali:

a) Globalizácia so svojimi pozitívnymi i negatívnymi vplyvmi: Vplyvom globalizácie došlo k ekonomickému, informačnému a technologickému prepojeniu štátnych i neštátnych aktérov. Okrem pozitívneho vplyvu, ako je odstránenie bipolarity, hrozby vojenského konfliktu, urýchľovanie ekonomického, technologického, kultúrneho a politického zbližovania subjektov medzinárodných vzťahov, kooperácia a solidarita, globalizácia priniesla so sebou aj javy a procesy, ktoré sa vymykajú kontrole jednotlivých štátov a koalícií. Zvýšili a zostrili sa aj problémy, ktoré už nemajú vplyv len v miestach ich vzniku, ale sa môžu stať, a v mnohých prípadoch sa aj stali, ohrozením aj pre ich pôvodcu a ľudstvo ako celok. Problémy globálnej spoločnosti (globálne problémy ľudstva) sú navzájom veľmi tesne prepojené, veľmi spolu súvisia. Na druhej strane sa zvýšila aj nutnosť hľadať ochranu pred existujúcimi nebezpečenstvami a ohrozeniami.

b) Nerovnomernosť vývoja, spôsobujúca prehlbovanie sociálno-ekonomických rozdielov medzi jednotlivými časťami sveta: Je reálnym faktom, že svet nebol nikdy tak vyspelý ako je v súčasnosti. Vyspelosť krajín „severu", či „západu" je v protiklade so zaostalosťou „juhu", resp. krajín tretieho sveta. Svet nebol nikdy tak bohatý, ako je v súčasnosti, bohatstvo na jednej strane je však konfrontované s nesmiernou chudobou v rôznych častiach sveta. Musíme si uvedomiť, že takmer 3 miliardy ľudí (čo je asi polovica svetovej populácie) žije z menej ako 2 EUR na deň. Na následky hladu a podvýživu zomiera každý rok 45 miliónov ľudí.

c) **Vznik nových bezpečnostných ohrození:** Súčasný svet je charakterizovaný na jednej strane ako bezpečný, pretože sa znížila pravdepodobnosť globálnej raketojadrovej vojny. V súčasnosti sa však predovšetkým zmenil rozsah nevojenských bezpečnostných rizík a ohrození. Ak tieto mali v predchádzajúcich dobách spravidla miestny, regionálny charakter, v súčasnosti dochádza k ich globalizácii, sú menej predvídateľné, nadmieru diverzifikované a robia svet nebezpečným.

d) **Zvyšujúca sa agresivita medzinárodného terorizmu**, z ktorého sa stal nový aktér svetovej politiky na rovnakej úrovni ako štáty, národné ekonomiky, či nevládne organizácie; teroristické skupiny sa stali násilnými nevládnymi organizáciami s globálnym dosahom.

2.5 NARUŠENIE BEZPEČNOSTI

Žijeme v období plnom rozporov, ktoré sa ľudstvo snaží viac – menej úspešne riešiť. Z bezpečnostného hľadiska vo všetkých veciach a javoch je **hlavným rozporom:**

BEZPEČNOSŤ – NEBEZPEČNOSŤ
bezpečne – nebezpečne
bezpečný – nebezpečný

Podľa slovníkov slovenského jazyka **nebezpečný** znamená skrývajúci ***nebezpečenstvo,*** hroziaci ***nebezpečenstvom,*** predstavujúci ***hrozbu*** niečoho zlého, ***ohrozujúci*** niekoho alebo niečo, zapríčiňujúci zlo, nešťastie ap. V uvedených definíciách sa teda vyskytujú pojmy **nebezpečenstvo** a **ohrozenie**, ktoré sú v tesnom spojení s ďalším bezpečnostným pojmom – **rizikom**.

Nebezpečenstvo môže potenciálne spôsobiť rôzne **negatívne udalosti – ohrozenia,** ktoré môžu mať za následok rôzne ujmy. Vzťah medzi veľkosťou **následku *negatívnej udalosti*** a jej **pravdepodobnosťou** predstavuje **úroveň bezpečnostného rizika**.

V prípade, že sa bezpečnostné riziko neriadi, môže vzniknúť **mimoriadna udalosť** alebo **krízová situácia,** vyžadujúca vyhlásenie určitého stupňa **krízového stavu.** V prípade, že sa krízový jav nepodarí zvládnuť, môže prerásť až do tvrdej straty stability – do **krízy**.

NEBEZPEČENSTVO	OHROZENIE	BEZPEČNOSTNÉ RIZIKO
vlastnosť objektu, ktorá môže spôsobiť neočakávanú negatívnu udalosť	***negatívna udalosť pri ktorej je aktivované nebezpečenstvo***	***úroveň rizika sa vyjadruje kombináciou pravdepodobnosti a následku negatívnej udalosti***

MIMORIADNA UDALOSŤ				
živelná pohroma	***havária***	***katastrofa***	***ohrozenie verejného zdravia II. stupňa***	***teroristický útok***

KRÍZOVÁ SITUÁCIA				
vypovedanie vojny	***vojnový stav***	***výnimočný stav***	***núdzový stav***	***mimoriadna situácia***

Obr. 4 Pojmy na vymedzenie úrovne narušenia bezpečnosti

2.5.1 Nebezpečenstvo

Podľa Zákona č.124/2006 Z. z. o bezpečnosti a ochrane zdravia pri práci:

a) nebezpečenstvo je stav alebo vlastnosť faktora pracovného procesu a pracovného prostredia, ktoré môžu poškodiť zdravie zamestnanca,

b) neodstrániteľné nebezpečenstvo je také nebezpečenstvo, ktoré podľa súčasných vedeckých a technických poznatkov nemožno vylúčiť ani obmedziť,

c) nebezpečná udalosť je udalosť, pri ktorej bola ***ohrozená*** bezpečnosť alebo zdravie zamestnanca, ale nedošlo k poškodeniu jeho zdravia.

V technických a technologických procesoch sa pojem **nebezpečenstvo** používa ako základný pojem pri posudzovaní bezpečnosti výrobných systémov alebo technických zariadení.

Ak sa objekty, ľubovoľné činnosti alebo samostatné činnosti – napr. stroje a strojné systémy, materiály, výrobné technológie – vyznačujú tým, že môžu spôsobiť neočakávaný negatívny jav, ide o ***nebezpečenstvo*** alebo ***nebezpečné činnosti***. Stroj je nebezpečný vtedy, keď počas jeho prevádzky môže vzniknúť negatívny jav.

Podľa Zákona č. 261/2002 Z. z. o prevencii závažných priemyselných havárií:

- **nebezpečenstvom** (zdrojom rizika závažnej priemyselnej havárie) je vnútorná vlastnosť vybranej nebezpečnej látky alebo fyzická situácia s potenciálom poškodenia ľudského zdravia, životného prostredia alebo majetku,
- **prítomnosťou vybranej nebezpečnej látky** v podniku je jej skutočná alebo predpokladaná (projektovaná) prítomnosť, vrátane takej vybranej nebezpečnej látky, ktorá môže vzniknúť v prípade straty kontroly nad chemickým procesom alebo v prípade závažnej priemyselnej havárie.

Nebezpečenstvo je teda podstatná vlastnosť, prípadne schopnosť systému (stroj, zariadenie, technológia, materiál, pracovná činnosť a pod.), ktorá môže spôsobiť vznik ***nežiaducej udalosti.*** Počas činnosti alebo existencie objektu môže vzniknúť incident, nehoda alebo mimoriadna udalosť, ktoré predstavujú ***ohrozenie*** zdravia, majetku alebo životného prostredia. **Nebezpečenstvo** je teda ***zdrojom ohrozenia*** *(Sabo, 2010, Šimák, 2006).*

Nebezpečenstvo je vlastnosť objektu, ktorá môže spôsobiť neočakávanú negatívnu udalosť

2.5.2 Ohrozenie

Ohroziť znamená vystaviť veľkému nebezpečenstvu: *ohroziť niekoho na živote, ohroziť mier; ohrozená vlasť.* **Ohrozenie** je ocitanie sa v nebezpečnej, nepriaznivej, ťažkej situácii, vystavenie nebezpečenstvu. **Ohrozenie je udalosť, ktorá je výsledkom aktivovania nebezpečenstva a ktorá môže spôsobiť negatívne (neželané) následky.** Je to pojem, ktorý označuje:

- aktivovanie nebezpečenstva v konkrétnom priestore a čase,
- bezprostredne vnímanú blízkosť ujmy,
- niečo, čo môže spôsobiť ujmu (osoba, vec, jav).

V prípade, že stroje, materiály, technológie alebo pracovné činnosti vyznačujúce sa určitým nebezpečenstvom sa uvedú do činnosti, a ak účinkom vlastnosti spôsobujúcej nebezpečenstvo môže byť vystavený človek (priamo alebo sprostredkovane), možno túto ***udalosť*** kvalifikovať ako **ohrozenie**. Je to tiež schopnosť aktivovania možného nebezpečenstva v konkrétnom priestore a čase, resp. v systéme človek – stroj – prostredie.

Podľa § 3 zákona o bezpečnosti a ochrane zdravia pri práci, **ohrozením je situácia**, ***v ktorej nemožno vylúčiť, že zdravie zamestnanca bude poškodené.*** Hovoríme, že je to „aktívna vlastnosť objektu“. Ohrozenie je viazané k otázke typu *„ako môže dôjsť k ujme?“*

Poškodiť znamená:

- spôsobiť škodu na niečom; pokaziť: *poškodiť stroj, poškodiť si zdravie,*
- spôsobiť niekomu škodu, ublížiť: *sudca poškodil hosťujúce mužstvo, svojím konaním poškodil priateľa, priateľovi,*
- spôsobiť ujmu na zdraví, uškodiť: *mastné jedlo mu poškodilo.*

Poškodenie je možné chápať ako zmenu vlastnosti objektu, alebo priebehu činnosti v dôsledku pôsobenia vonkajších vplyvov, pričom počas tejto zmeny dochádza k degradácii (negatívnej zmene) znižovania funkčnej schopnosti.

Zmena môže byť **iniciovaná** napr. chybou obsluhy alebo poruchou zariadenia. **Škoda** znamená hmotné alebo iné poškodenie (ujma, strata, neprospech, nevýhoda). Je to každá ľubovoľným spôsobom vzniknutá zmena, definovaná počtom usmrtených alebo zranených ľudí, stratou na majetku, počtom stratených pracovných miest, množstvom kontaminovanej zeminy a pod.

Neodstrániteľným ohrozením je také ohrozenie, ktoré podľa súčasných vedeckých a technických poznatkov nemožno vylúčiť ani obmedziť.

Podľa Zákona č. 42/1994 Z. z. o civilnej ochrane obyvateľstva **ohrozenie** je **obdobie, *počas ktorého sa predpokladá nebezpečenstvo vzniku alebo rozšírenia následkov mimoriadnej udalosti.***

V Trestnom zákone sa pojem **ohrozenie** používa v rôznych významoch, napr. všeobecné ohrozenie; ohrozenie obchodného, bankového, poštového, telekomunikačného a daňového tajomstva; ohrozenie pod vplyvom návykovej látky; ohrozenie bezpečnosti vzdušného dopravného prostriedku a lode; ohrozenie a poškodenie životného prostredia; ohrozenie utajovanej skutočnosti; ohrozenie dôvernej skutočnosti a vyhradenej skutočnosti; ohrozenie bojovej pohotovosti; ohrozenie mieru; ohrozenie kultúrnych hodnôt; ohrozenie záujmu chráneného zákonom; ohrozenie spôsobiť trestný čin; ohrozenie devízového hospodárstva.

Na spôsobenie ohrozenia sú potrebné určité vlastnosti prítomné v samotnom subjekte, ktorého sa týkajú, alebo v súvislostiach subjektu s okolím. Toto ohrozenie sa dá charakterizovať kategóriou negatívneho potenciálu chápaného ako schopnosť deštruktívne pôsobiť na systém. Sú to ohrozenia spôsobené *(Korzeniowski, 2008)*:

1. **neživou prírodou** nezávislou od človeka (napr. kozmické objekty, tektonické pohyby, vulkány, tajfúny...),
2. **živými organizmami** (mikroorganizmy, rastliny, živočíchy),
3. **výtvormi človeka** (stavby, stroje, chemické substancie, výbušniny),
4. **človekom a spoločnosťou:**
   - napätie v medziľudských vzťahoch, otrokárstvo, dobyvateľské a náboženské vojny, teror,
   - môžu to byť tiež reálne činnosti iných účastníkov spoločenského života, neužitočné a nebezpečné pre životné záujmy a základné hodnoty daného človeka, skupiny, spoločnosti či ľudstva na celom svete.

Ohrozenie je zdroj možného zranenia alebo poškodenia zdravia, majetku, životného prostredia, potenciálnej škody, straty. Ohrozenie v technických a technologických procesoch znamená napr. ***uvedenie technického objektu do prevádzky bez zohľadnenia jeho nebezpečnej vlastnosti,*** *čím dochádza* ***k ohrozeniu v určitom pracovnom priestore a čase.***

Ohrozenie je udalosť, ktorá je výsledkom aktivovania nebezpečenstva a ktorá môže spôsobiť negatívne (neželané) následky.

V STN ISO 31000:2011 Manažérstvo rizika, Zásady a návod sa na vyjadrenie úrovne rizika pojem ***ohrozenie*** vôbec nepoužíva. Riziko sa charakterizuje odkazom na potenciálne ***udalosti a následky*** alebo na ich kombináciu.

2.5.3 Riziko

Slovo „riziko“ bolo často chápané **iba negatívnym spôsobom**, kde ohrozenie mohlo spôsobiť určité ujmy, vôbec sa neuvažovalo, že riziká, najmä podnikateľské, môžu okrem ujmy priniesť aj ***zisk, ktorý nie je vôbec závislý od ohrozenia ani odzraniteľnosti.***

Z tohto dôvodu bolo potrebné zaviesť určitú normu, ktorá by riziko chápala z negatívnej, ale aj z pozitívnej stránky. Takouto normou bola STN ISO 010381 Manažérstvo rizika z roku 2003, ktorá je v súčasnosti nahradená normou STN ISO 31000:2011 Manažérstvo rizika, zásady a návod.

Podľa normy ISO 31000 a následnej zásadnej revízii terminológie v ISO Guide 73 definícia „rizika“ už nie je: ***„možnosť alebo pravdepodobnosť straty“,*** ale **„účinok neistoty zámerov“**. Slovo **„riziko“** sa teda odkazuje na **pozitívne možnosti, ako aj tie negatívne.**

V STN ISO 31000:2011 *Manažérstvo rizika, zásady a návod* a európskej norme ISO Guide 73:2002 *Medzinárodné štandardy pre riadenie rizika* je definícia:

RIZIKO = ÚČINOK NEISTOTY ZÁMEROV

Prvky rizika sú vysvetlené v tab. 4.

Tab. 4 Prvky rizika

ÚČINOK	• ***pozitívna*** alebo ***negatívna odchýlka od očakávania***, ktorá môže pozitívne alebo negatívne ovplyvňovať **zámery** (ciele).
NEISTOTA	• **(**alebo **nedostatok istoty)** predstavuje stav, či podmienky, ktoré zahŕňajú nedostatok informácií a vedú k neprimeranému či neúplnému poznaniu alebo porozumeniu ***udalosti,*** jej ***následkov*** alebo ***pravdepodobnosti***.
ZÁMER	• **uvážené rozhodnutie niečo dosiahnuť** (úmysel, plán, cieľ, účel, predsavzatie), • môžu mať rozličné aspekty (finančné, zdravotné, bezpečnostné, environmentálne atď.), • môžu sa uplatňovať na rozličných úrovniach (strategická úroveň, v rámci celej organizácie, v rámci projektu, produktu alebo procesu).

Riziko sa charakterizuje odkazom na potenciálne **udalosti** a **následky,** alebo na **ich kombináciu.** Potom sa jeho **úroveň** vyjadruje **kombináciou** ***následkov udalosti*** (vrátane zmien okolností) a súvisiacej ***pravdepodobnosti výskytu udalosti.*** Všetky druhy činností v organizácii sú ovplyvnené **udalosťami,** ktoré môžu mať **pozitívny účinok** – ***príležitosti k zisku***, alebo **negatívny účinok** – ***ohrozenia*** (tab. 5).

Tab. 5 Negatívne a pozitívne udalosti

Negatívne udalosti	• **negatívny účinok** – **ohrozenia** vyplývajúce z ***nebezpečenstva,*** • mieru tohto ohrozenia predstavuje ***bezpečnostné riziko*** (čisté), ktoré má ***vždy za následok ujmu, škodu.***
Pozitívne udalosti	• **pozitívny účinok** – **príležitosti**, vyplývajúce z niektorých vnútorných a vonkajších faktorov, • predstavujú ***podnikateľské riziko*** (špekulatívne), ktoré môže mať za ***následok zisk, v niektorých prípadoch však aj stratu.***

Úroveň rizika alebo **kombinácie rizík** je veľkosť rizika, ktorá sa vyjadruje ako kombinácia:

- **následkov** *(consequences)* ***udalosti*** (zisk alebo ujma).
- **pravdepodobností** *(likelihood)*, že nejaká ***udalosť*** (pozitívna alebo negatívna) nastane.

Charakteristika pravdepodobnosti a následku udalosti je uvedená v tab. 6.

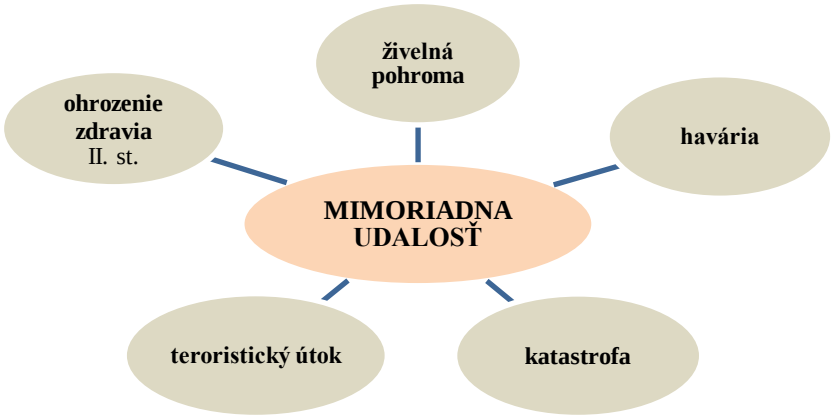
Tab. 6 Pravdepodobnosť a následok udalosti

Pravdepodobnosť	• používa sa v zmysle **predpokladu, že sa niečo stane**, bez ohľadu na to, či sa to meralo alebo objektívne či subjektívne, kvalitatívne či kvantitatívne definovalo, • **vyjadruje sa *všeobecnými výrazmi*** alebo ***matematicky.***
Následok	• **výsledok udalosti**, ktorý ovplyvňuje zámery, • pre negatívnu udalosť predstavuje ***ujmu***, je to neželená kvalitatívna a kvantitatívna zmena predmetu bezpečnosti, zníženie jeho hodnoty alebo jeho úplný zánik (zničenie), • pre pozitívnu udalosť predstavuje ***zisk,*** v niektorých prípadoch však aj ***stratu.***

Úroveň bezpečnostného rizika predstavuje kombináciu pravdepodobnosti vzniku negatívnej udalosti a jej následkov

2.5.4 Mimoriadna udalosť

Mimoriadne udalosti podľa Zákona č. 42/1994 Z. z. o civilnej ochrane obyvateľstva sú uvedené na obr. 5.



Obr. 5 Mimoriadne udalosti

Živelná pohroma

Živelná pohroma je mimoriadna udalosť, pri ktorej dôjde k ***nežiaducemu uvoľneniu kumulovaných energií alebo hmôt v dôsledku nepriaznivého pôsobenia prírodných síl, pri ktorej môžu pôsobiť nebezpečné látky alebo pôsobia ničivé faktory,*** ktoré majú negatívny vplyv na život, zdravie alebo na majetok.

Nebezpečné látky sú prírodné alebo syntetické látky, ktoré svojimi chemickými, fyzikálnymi, toxickými alebo biologickými vlastnosťami samostatne alebo v kombinácii môžu spôsobiť ohrozenie života, zdravia alebo majetku *(Zákon č. 42/1994 Z. z.)*.

Živelnú pohromu môžu spôsobiť nasledujúce prírodné udalosti:

- **atmosférické (poveternostné)** – krupobitie, prietrž mračien, víchrica, tornádo, snehové kalamity, prízemný mráz a rozsiahle námrazy, úder bleskom, sucho, veterná erózia a sedimentácia, tropický cyklón, dezertifikácia (premena obrábanej pôdy na púšť), roztápanie permafrostu (večne zamrznutá pôda),
- **hydrologické** – riečna povodeň, pobrežná záplava, zamokrenie (podmáčanie) územia, vodná erózia a sedimentácia, zasoľovanie pôdy,
- **gravitačné** – zosuv pôdy, skalný prúd, mura (zmývanie zvetranín aj s vegetáciou po prietrži mračien, náhlom oteplení), bahnotok, subsidencia (klesanie územia vplyvom vytláčania vody zo zavodnených horizontov),
- **seizmické** – zemetrasenie, roztopenie sedimentov, cunami,
- **vulkanické** – usadzovanie sopečného popola, dopad sopečných bômb, výron sopečných plynov, lávový prúd, lahar (vulkanický prúd bahna a skál),
- **iné** – prírodný požiar, lavíny.

Najčastejšie živelné pohromy sú povodne, záplavy, prietrže mračien a krupobitia, snehové kalamity, lavíny a rozsiahle námrazy, zosuvy pôdy, zemetrasenia, atmosférické poruchy, kozmické vplyvy, sopečné výbuchy, víchrice, tornáda, búrky apod. Územie postihnuté účinkami živelnej pohromy je charakterizované *(Betuš, 2014):*

- postihnutím veľkého počtu osôb, ktoré sú bez prístrešia a základných životných potrieb, šokované, zranené alebo usmrtené,
- zničením a poškodením budov, priemyselných objektov, mostov,
- narušením dopravy,
- zničením kultúrnych pamiatok a chránených prírodných útvarov,
- miestnymi a plošnými závalmi ulíc,
- poškodením pozemných komunikácií, poškodením rozvodných sietí a ich zariadení,
- vznikom požiarov, zatopením objektov a zaplavením rozsiahlych území,
- postihnutím veľkého počtu zvierat,
- zničením a narušením porastov, lesov a pôdy,
- zhoršením hygienických podmienok, vznikom infekčných ochorení,
- celkovým narušením života, životného prostredia a obmedzením výroby.

Havária

Havária je mimoriadna udalosť, ktorá ***spôsobí odchýlku od ustáleného prevádzkového stavu, v dôsledku čoho dôjde k úniku nebezpečných látok alebo k pôsobeniu iných ničivých faktorov,*** ktoré majú vplyv na život, zdravie alebo na majetok *(Zákon o civilnej ochrane obyvateľstva)*.

Je to ***udalosť***, ktorá vážne ohrozila životy a zdravie osôb, prevádzku, činnosť, prípadne rozvoj organizácie, alebo ktorá spôsobila škodu na majetku organizácie prevyšujúcu stanovenú finančnú hodnotu. V prevádzke organizácie môže dôjsť k zničeniu alebo poškodeniu stroja, dôležitého prístroja, budovy, technologického celku, ľudského zdravia alebo života, k rozsiahlym ekologickým alebo hospodárskym škodám a pod. Zvláštnym prípadom havárie je požiar.

Závažná havária môže byť spojená s únikom ***nebezpečných látok*** toxického, horľavého či výbušného charakteru, rádioaktívnych alebo biologických látok. Haváriami sú dopravné nehody, priemyselné havárie, ekologické havárie a iné havárie (tab. 7) *(Betuš, 2004)*.

Havária ako mimoriadna udalosť vzniká v súvislosti s prevádzkou technických zariadení a budov, používaním, spracovaním a výrobou, skladovaním alebo prepravou nebezpeč-

ných látok, pri manipulovaní s nebezpečným odpadom. Územie postihnuté účinkami havárie je charakterizované postihnutím a ohrozením osôb, ovzdušia, zvierat, terénu, vody a potravín, zhoršením hygienických podmienok, vznikom a šírením infekčných ochorení.

Tab. 7 Havárie (zdroj: Betuš, 2014)

DOPRAVNÉ NEHODY	zvyčajne **nehoda v prevádzke** na **cestných komunikáciách**, ale nehodami sú aj podobné udalosti v ***koľajovej, vodnej*** alebo ***leteckej doprave,***
PRIEMYSELNÉ HAVÁRIE	**nehoda v prevádzke podnikov spracovávajúcich nebezpečné látky** (muničné, chemické, jadrové), ale aj na ***potrubiach*** (vodovod, plynovod, parovod, ropovod, teplovod) alebo ***elektrickej rozvodnej sieti,***
EKOLOGICKÉ HAVÁRIE	**dopravné alebo priemyselné havárie**, ktoré spôsobia *veľké škody na životnom prostredí, prírode, alebo na zdraví väčšieho množstva ľudí,*
INÉ HAVÁRIE	napr. pád výťahu v bytovom dome, prasknutý vodovodný rozvod v byte).

Katastrofa

Katastrofa *(Disaster)* je mimoriadna udalosť**,** pri ktorej dôjde k ***narastaniu ničivých faktorov a ich následnej kumulácii v dôsledku živelnej pohromy a havárie*** *(Zákon o civilnej ochrane obyvateľstva)*. Je to pojem pre náhlu udalosť alebo veľkú nehodu, ktorá spôsobila veľké škody na životoch ľudí, majetku, informáciách, životnom prostredí alebo iných aktívach organizácie.

Katastrofy sú najmä veľké letecké, železničné, lodné a cestné nehody spojené s požiarmi, prípadne s únikom nebezpečných látok, havárie jadrových zariadení, porušenie vodných stavieb. Územie postihnuté účinkami katastrofy je charakterizované postihnutím a ohrozením osôb, ovzdušia, zvierat, terénu, vody a potravín, zhoršením hygienických podmienok, vznikom a šírením infekčných ochorení, celkovým narušením života, výroby a životného prostredia.

Dôležité je katastrofe predísť alebo zmierniť jej následky – to je kľúčovým predmetom manažérstva rizík. Organizácie tiež využívajú poistenie ako nástroj na tlmenie dopadu katastrofy na organizáciu.

Ohrozenie verejného zdravia II. stupňa

Predstavuje ohrozenie verejného zdravia, pri ktorom je potrebné prijať opatrenia pri radiačnej nehode alebo radiačnej havárii, výskyte prenosného ochorenia, podozrení na prenosné ochorenie alebo podozrení na úmrtie na prenosné ochorenie nad predpokladanú úroveň, uvoľnení chemických látok ohrozujúcich život, zdravie, životné prostredie a majetok, alebo úniku mikroorganizmov alebo toxínov z uzavretých priestorov.

Teroristický útok

Predstavuje organizovanú akciu jednotlivca, skupiny osôb alebo organizácie, spravidla militantne orientovanej, zameranú na hrubé a často drastické zastrašovanie obyvateľstva, rôznorodé útoky proti organizáciám, inštitúciám a ich predstaviteľom, objektom, sústavám, zariadeniam, službám a systémom. Ide o napadnutia objektov sústreďujúcich väčšie množstvo osôb, s cieľom spôsobiť straty na životoch, zdraví a majetku, vyvolávať atmosféru neistoty a strachu, vážne ohroziť obyvateľstvo, nútiť vládu alebo medzinárodnú organizáciu konať alebo zdržať sa konania, vážne destabilizovať alebo zničiť základné politické, ústavné, hospodárske

alebo spoločenské zriadenie krajiny alebo medzinárodnej organizácie. Terorizmus a jeho niektoré formy sú popísané v Trestnom zákone.

Na teroristické útoky môžu byť použité konvenčné zbrane a prostriedky obsahujúce chemické, biologické a rádioaktívne látky a materiály. Priestor postihnutý účinkami teroristického útoku je charakterizovaný usmrtením, zranením a ohrozením veľkého počtu osôb, kontaminovaním ovzdušia, vody, potravín a terénu, vznikom paniky postihnutého i nepostihnutého obyvateľstva, vznikom značných materiálových strát a pod.

2.5.5 Krízové javy

Medzi krízové javy je možné zaradiť *ohrozenie, mimoriadnu situáciu, krízovú situáciu, núdzový stav, výnimočný stav, vojnový stav a vojnu* (obr. 6).

Mimoriadna situácia je podľa Zákona o civilnej ochrane obyvateľstva ***obdobie ohrozenia alebo pôsobenia negatívnych následkov mimoriadnej udalosti*** na život, zdravie alebo majetok, ktorá je vyhlásená podľa tohto zákona. Po vyhlásení mimoriadnej situácie sa vykonávajú opatrenia:

- *na záchranu života, zdravia alebo majetku,*
- *na znižovanie rizík ohrozenia,*
- *alebo činnosti nevyhnutné na zamedzenie šírenia a pôsobenia následkov mimoriadnej udalosti.*

Mimoriadnu situáciu vyhlasuje a odvoláva prostredníctvom hromadných informačných prostriedkov obec na území obce v prípade vzniku mimoriadnej udalosti a neodkladne o tom informuje obvodný úrad. Okres ju vyhlasuje na území okresu, kraj na území kraja a vláda na území, ktoré prekračuje územie kraja. Po vyhlásení mimoriadnej situácie sa vykonávajú tieto úlohy a opatrenia:

a) záchranné práce silami a prostriedkami z celého územia, na ktorom bola vyhlásená mimoriadna situácia,
b) evakuácia,
c) núdzové zásobovanie a núdzové ubytovanie alebo
d) použitie základných zložiek a ostatných zložiek integrovaného záchranného systému (IZS).

Krízová situácia v zmysle Ústavného zákona č. 227/2002 Z. z. o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu je **obdobie,** počas ktorého je ***bezprostredne ohrozená alebo narušená bezpečnosť štátu*** a ústavné orgány môžu po splnení podmienok ustanovených v tomto ústavnom zákone na jej riešenie vypovedať ***vojnu,*** vyhlásiť ***vojnový stav*** alebo ***výnimočný stav,*** alebo ***núdzový stav.***

Krízová situácia mimo času vojny a vojnového stavu v zmysle Zákona č. 387/2002 Z. z. o riadení štátu v krízových situáciách mimo času vojny a vojnového stavu je **obdobie,** počas ktorého je ***bezprostredne ohrozená alebo narušená bezpečnosť štátu*** a ústavné orgány môžu po splnení podmienok ustanovených v ústavnom zákone alebo osobitnom zákone na jej riešenie vyhlásiť ***výnimočný stav, núdzový stav*** alebo ***mimoriadnu situáciu.***

Núdzový stav môže vláda vyhlásiť len za podmienky, že došlo, alebo bezprostredne hrozí, že dôjde k ohrozeniu života a zdravia osôb, a to aj v príčinnej súvislosti so vznikom pandémie, životného prostredia alebo k ohrozeniu značných majetkových hodnôt ***v dôsledku živelnej pohromy, katastrofy, priemyselnej, dopravnej alebo inej prevádzkovej havárie***; núdzový stav možno vyhlásiť len na postihnutom alebo na bezprostredne ohrozenom území.

Výnimočný stav môže na návrh vlády vyhlásiť prezident len za podmienky, že došlo alebo bezprostredne hrozí, že dôjde k ***teroristickému útoku, k rozsiahlym pouličným nepokojom spojeným s útokmi na orgány verejnej moci, drancovaním obchodov a skladov alebo s inými hromadnými útokmi na majetok*** alebo dôjde k ***inému hromadnému násilnému protiprávnemu konaniu,*** ktoré svojím rozsahom alebo následkami podstatne ohrozuje alebo narušuje verejný poriadok a bezpečnosť štátu, ak ho nemožno odvrátiť činnosťou orgánov verejnej moci a ak je znemožnené účinné použitie zákonných prostriedkov.

Vojnový stav môže na návrh vlády vyhlásiť prezident len za podmienky, že SR bezprostredne ***hrozí vypovedanie vojny alebo bezprostredne hrozí napadnutie cudzou mocou bez vypovedania vojny.***

Vojnu vypovie prezident na základe rozhodnutia Národnej rady SR len za podmienky, že SR je napadnutá cudzou mocou, ktorá jej vypovedala vojnu alebo ktorá bez vypovedania vojny narušila jej bezpečnosť, alebo za podmienky, že vypovedaním vojny SR plní záväzky vyplývajúce z členstva v organizácii vzájomnej kolektívnej bezpečnosti alebo z medzinárodnej zmluvy o spoločnej obrane proti napadnutiu.

OHROZENIE
obdobie, počas ktorého ***sa predpokladá nebezpečenstvo vzniku alebo rozšírenia následkov*** **mimoriadnej udalosti**

MIMORIADNA SITUÁCIA
obdobie
ohrozenia alebo pôsobenia negatívnych následkov **mimoriadnej udalosti**

KRÍZOVÁ SITUÁCIA
obdobie, počas ktorého
je bezprostredne ohrozená alebo narušená bezpečnosť štátu

v zmysle Zákona č. 387/2002 Z. z. ústavné orgány môžu **vyhlásiť**:
- ***výnimočný stav***
- ***núdzový stav***
- ***mimoriadnu situáciu***

v zmysle ÚZ č. 227/2002 Z. z. ústavné orgány môžu:
- **vypovedať *vojnu***
- **vyhlásiť *vojnový stav, výnimočný stav, núdzový stav***

Núdzový stav	došlo, alebo bezprostredne hrozí, že dôjde k ohrozeniu života a zdravia osôb, a to aj v príčinnej súvislosti so vznikom pandémie, životného prostredia alebo k ohrozeniu značných majetkových hodnôt	*v dôsledku živelnej pohromy, katastrofy, priemyselnej, dopravnej alebo inej prevádzkovej havárie.*
Výnimočný stav	ohrozenie alebo narušenie verejného poriadku a bezpečnosti štátu, ak ho nemožno odvrátiť činnosťou orgánov verejnej moci a ak je znemožnené účinné použitie zákonných prostriedkov	*v dôsledku teroristického útoku, rozsiahlych pouličných nepokojov spojených s útokmi na orgány verejnej moci, drancovaním obchodov a skladov alebo s inými hromadnými útokmi na majetok* alebo *iných hromadných násilných protiprávnych konaní,*
Vojnový stav	bezprostredne *hrozí vypovedanie vojny alebo bezprostredne hrozí napadnutie cudzou mocou bez vypovedania vojny.*	

Obr. 6 Krízové javy

2.6 ÚROVEŇ BEZPEČNOSTI

„Nemôžete riadiť to, čo nemôžete zmerať“ – P. F. Drucker.

„Meraj všetko, čo je merateľné a nemerateľné urob merateľným“ – Galileo Galilei.

Absolútna bezpečnosť je všeobecne nedosiahnuteľný a veľmi drahý cieľ, preto bol v rizikových odvetviach, napr. leteckej alebo železničnej dopravy prijatý pojem **prípustná bezpečnosť.**

Pojem **prijateľné riziko** opisuje udalosť s pravdepodobnosťou výskytu a následkami prijateľnými pre spoločnosť, čo znamená, že spoločnosť je ochotná prijať riziko alebo môže byť vystavená tomuto riziku, ktoré môže udalosť priniesť. Úlohou bezpečnostných riadiacich orgánov je presadiť očakávania a vnímania spoločnosti do kvalitatívnych alebo kvantitatívnych cieľov úrovne bezpečnosti.

V akomkoľvek systéme je nevyhnutné **stanoviť a merať výkonové parametre,** aby sa mohlo rozhodnúť, ***či systém funguje v súlade s očakávaniami a identifikovať kde je potrebné zasiahnuť',*** aby sa zvýšila efektivita systému a aby boli splnené dané očakávania.

V Príručke manažérstva bezpečnosti Medzinárodnej civilnej organizácie letectva (ICAO) Doc 9859 AN/460 sú uvedené vzťahy medzi požiadavkami ***prijateľnej úrovne bezpečnosti, bezpečnostnými cieľmi a ukazovateľmi výkonu*** v oblasti bezpečnosti takto:

- **Úroveň bezpečnosti** *(Level of Safety)* – úroveň bezpečnosti systému, reprezentujúca kvalitu systému, vyjadrenú prostredníctvom ***indikátorov bezpečnosti.***
- **Prijateľná úroveň bezpečnosti** *(Acceptable Level of Safety, AloS)* – minimálny stupeň/ úroveň bezpečnosti, ktorá musí byť zaistená systémom v praxi. Vyjadruje bezpečnostné ciele stanovené manažmentom organizácie. Požadovaná úroveň bezpečnosti sa dosiahne vtedy, keď pre normálny (štandardný) priebeh činnosti (chod systému) nie je potrebné prijímať špecifické opatrenia. V praxi sa koncept prijateľnej úrovne bezpečnosti vyjadruje dvoma parametrami – **indikátory bezpečnosti** a **ciele bezpečnosti,** a realizuje sa prostredníctvom rôznych bezpečnostných požiadaviek.

2.6.1 Indikátory (ukazovatele) bezpečnosti

Indikátor (z lat. *indicare,* ukazovať) predstavuje pojem „ukazovateľ“, napr. ekonomický ukazovateľ, ukazovateľ vlhkosti a pod. Indikátor je údaj alebo hodnota rôzneho charakteru, vyjadrujúca okamžitý stav alebo úroveň zmeny sledovaného stavu *(Hanušinec, 2000).* Pojem indikátor označuje viditeľný jav, vec, respektíve trend alebo skutočnosť, ktorý indikuje stav alebo stupeň niečoho, indikuje ťažko pozorovateľné spoločenské zmeny, prípadne umožňuje iné javy predvídať. Napr.: pouličné nepokoje sú indikátorom napätia v spoločnosti, vlastníctvo niektorých vecí sa často používa ako indikátor blahobytu.

Indikátory (ukazovatele) bezpečnosti *(Safety Indicators)* sú parametre, ktoré charakterizujú a/alebo znázorňujú úroveň bezpečnosti systému. Sú definované ako ***merateľné prevádzkové premenné,*** ktoré môžu byť využité na popis rozsiahlejšieho javu alebo časti skutočnosti. Indikátory bezpečnosti umožňujú organizácii merať a preukázať dosiahnutie stanovených cieľov, preto by mali byť ľahko merateľné. Môžu sa vhodne využiť pre správne rozhodovanie manažmentu a zodpovedných pracovníkov. Je dôležité, aby sa mohli využiť na spätnú väzbu. Všeobecne platí, že indikátory bezpečnosti sú uvedené ***z hľadiska frekvencie výskytu škodlivej udalosti.*** Základnými vlastnosťami ukazovateľov bezpečnosti sú:

- poskytovanie číselných hodnôt,
- pravidelná aktualizácia,
- každý ukazovateľ pokrýva špecifickú časť bezpečnosti.

Indikátory by mali spĺňať nasledujúce požiadavky:

- indikátor v kvantitatívnej forme vyjadruje taký stav bezpečnostnej situácie, kedy vzniká hrozba alebo jej predpoklady pre bezpečnosť referenčných objektov,
- indikátory majú vysokú citlivosť a variabilitu (premenlivosť), čo umožňuje ich použitie na sledovanie, vyhodnocovanie i predikciu procesov v bezpečnostnom prostredí.

Hodnota indikátora bezpečnosti *(Value of a Safety Indicator)* znamená kvantifikáciu indikátora bezpečnosti. Rozlišujú sa druhy indikátorov uvedené na obr. 7:

Obr. 7 Druhy indikátorov bezpečnosti

Reaktívne indikátory vyjadrujú počet určitých bezpečnostných udalostí za určité obdobie, napr. rast, frekvencia, počet nehôd; rast, frekvencia, počet incidentov, úroveň zhody s právnymi normami a pod. Niektoré skupiny indikátorov po prekonaní kritických hodnôt signalizujú zhoršenie bezpečnostnej situácie v lokálnom prostredí a znázorňujú nie dobrý stav bezpečnostnej situácie. Medzi tieto indikátory patrí napríklad:

- ničenie majetku, automobilov, verejnej infraštruktúry,
- pouličná kriminalita (mravnostná, majetková),
- vandalizmus v uliciach prejavujúci sa rozbíjaním okien, výkladov, dvier, poškodzovaním vonkajších fasád budov,
- útoky na osoby na verejnosti, násilná kriminalita,
- prítomnosť pouličných skupín ľudí, ktorí majú agresívne sklony a narušujú verejný poriadok,
- drogová kriminalita, konzumácia a distribúcia drog na verejných priestranstvách a pod.

Prediktívne indikátory sa zaoberajú monitorovaním prevádzkových procesov so zameraním na ich kritické miesta a postavenie v kauzálnych diagramoch vzhľadom na vrcholové udalosti – potenciálne nehody. V najvyššej rozlišovacej úrovni sa zameriavajú na:

- väzbu manažmentu na bezpečnosť,
- fungovanie bezpečnosti zo strany manažmentu,
- osobné väzby na bezpečnosť,
- vnímanie nebezpečenstva a stupňov prevádzkových rizík,
- dopady požadovaného pracovného tempa prevádzkových činností,
- dôvera vo vyšetrovanie nehôd,
- dopady stresových faktorov spojených s prevádzkovými operáciami,
- efektivita komunikácie o bezpečnosti v rámci organizácie,
- efektivita riadenia krízových situácií,
- efektivita vykonávania bezpečnostného výcviku,
- postoj pracovníkov zodpovedných za bezpečnosť k bezpečnosti a pod.

V systéme BOZP medzi indikátory bezpečnosti patria napr.: smrť, zranenie, choroba, pracovný úraz, choroba z povolania, dĺžka pracovnej neschopnosti, odškodnenie pracovného úrazu a pod.

2.6.2 Ciele bezpečnosti

Ciele bezpečnosti *(Safety Targets)*, niekde aj ***výkonnostné ciele bezpečnosti*** predstavujú konkrétne kvantifikované ciele úrovne bezpečnosti, ktoré sa majú dosiahnuť na zabezpečenie požadovanej (prijateľnej) úrovne bezpečnosti. Stanovujú sa vo fáze plánovania manažérstva bezpečnosti, sú nastavené tak, aby sa dosiahla prijateľná úroveň bezpečnosti, ktorú vrcholový manažment považuje za žiaducu a reálnu. Výkonnostný cieľ v oblasti bezpečnosti sa skladá z ***jedného alebo viacerých ukazovateľov výkonnosti v bezpečnosti***, spolu s požadovanými výsledkami vyjadrenými v týchto ukazovateľoch.

Cieľ požadovanej bezpečnosti môže byť uvedený buď ***v absolútnych alebo relatívnych hodnotách***. Výkonnostné ciele bezpečnosti sa pravidelne ***skúmajú a aktualizujú*** podľa potreby, tieto hodnotenia sa vykonávajú ako súčasť strategického plánovania a zlepšovania bezpečnosti. Príkladom žiaduceho bezpečnostného výsledku v absolútnom vyjadrení je napr. menej než 1 smrteľná nehoda na 1 milión prevádzkových hodín.

Hodnota cieľa bezpečnosti *(Value of a Safety Target)* znamená kvantifikáciu cieľa bezpečnosti.

Hlavným **bezpečnostným cieľom** je kvalitatívne alebo kvantitatívne vyjadrenie, ktoré definuje ašpirácie a strategické ciele organizácie týkajúce sa bezpečnosti prevádzky a poskytovaných služieb.

Porovnanie možných indikátorov a cieľov bezpečnosti je uvedené v tab. 8.

Tab. 8 Porovnanie možných indikátorov a cieľov bezpečnosti

Indikátory bezpečnosti	Ciele bezpečnosti
rast/ frekvencia/ počet smrteľných nehôd	zníženie rastu/ frekvencie/ počtu smrteľných nehôd
rast/ frekvencia/ počet zranení	zníženie rastu/ frekvencie/ počtu zranení
rast/ frekvencia/ počet bezpečnostných incidentov	zníženie rastu/ frekvencie/ počtu bezpečnostných incidentov
rast/ frekvencia/ počet počítačových incidentov	zníženie rastu/ frekvencie/ počtu počítačových incidentov
doba prerušenia činnosti	zníženie doby prerušenia činností
veľkosť škôd spôsobených krádežami	zníženie škôd spôsobených krádežami
vývoj /absencia/zhoda právnych noriem	odstránenie nezhôd právnych noriem
vývoj/ absencia/ zhoda prevádzkových predpisov	odstránenie nezhôd s prevádzkovými predpismi
počet previerok, kontrol a auditov	zvýšenie počtu previerok, kontrol a auditov

2.7 ZÁSADY BEZPEČNOSTI ORGANIZÁCIE

Organizácia a fungovanie systému riadenia (manažérstva) jej bezpečnosti musí zodpovedať zásadám uvedeným na obrázku 8 *(Hofreiter, 2006)*:

Obr. 8 Zásady bezpečnosti organizácie

1 Komplexnosť

Uplatňovanie princípu komplexnosti znamená, že ochrana všetkých aktív organizácie musí byť zabezpečovaná všetkými dostupnými zákonnými prostriedkami, metódami a opatreniami. Komplexnosť ochrany aktív organizácie sa dosahuje použitím technických zabezpečovacích prostriedkov, fyzickej ochrany a režimových opatrení, prípadne i detektívnej služby tak, aby boli pokryté všetky bezpečnostné ohrozenia a všetky zraniteľné miesta. Ak má byť ochrana komplexná, nemôže sa klásť dôraz len na jednu formu ochrany, pretože sa tým zvyšuje zraniteľnosť organizácie. Malo by platiť, že pri výbere prostriedkov ochrany môžu existovať priority, ale nemôže existovať druhoradosť. Zníženie ochranných vlastností ktoréhokoľvek prvku bezpečnostného systému zhorší kvalitu celého bezpečnostného systému.

2 Včasnosť

Princíp včasnosti znamená vytvoriť a udržiavať bezpečnostný systém tak, aby dokázal v predstihu eliminovať bezpečnostné ohrozenia, tzn. pred ich reálnym pôsobením proti aktívam organizácie. Znamená to, že bezpečnostný systém musí plniť preventívnu funkciu – včas odhaliť ohrozenie, odradiť potenciálneho útočníka od úmyslu, resp. zadržať ho pred dosiahnutím chráneného záujmu. V závislosti od kvality realizácie tohto princípu môžu vzniknúť nasledujúce varianty:

a) systém zabezpečujúci predstih pred útočníkom,
b) systém reagujúci so začiatkom útoku,
c) oneskorene reagujúci systém.
d) nereagujúci systém.

3 Nepretržitosť

Nepretržitosť v činnosti bezpečnostného systému znamená, že systém musí byť schopný plniť ochranné a preventívne funkcie počas celého cyklu ochrany, aby potenciálni útočníci nemohli využiť „výpadky“, resp. nefunkčnosť alebo nečinnosť bezpečnostného systému na uskutočnenie útoku.

4 Aktívnosť

Chrániť aktíva organizácie treba s dostatočným stupňom húževnatosti a vytrvalosti, pričom treba využívať všetky dostupné ochranné opatrenia tak, aby boli dostatočne odolné aj voči sofistikovaným profesionálne vedeným a netradičným útokom na chránený záujem. Platí, že ochranca by mal poznať možné scenáre útokov na chránený záujem a bezpečnostný systém vytvoriť tak, aby bol čo najmenej zraniteľný.

5 Centralizované riadenie

V organizácii by mal byť vytvorený funkčný systém bezpečnostného manažmentu, ktorý by zahrňoval všetky úrovne riadenia organizácie. Úloha riadenia bezpečnosti organizácie je nedeliteľnou súčasťou riadiacej práce manažmentu organizácie. Nástrojom riadenia bezpečnosti je celková bezpečnostná politika ako verejný záväzný dokument, prijatý vedením organizácie ako vnútorná norma, z ktorej vychádzajú systémové bezpečnostné politiky (napr. pre ochranu majetku, pre bezpečnosť IT, pre personálnu bezpečnosť, pre krízové a havarijné plánovanie a pod.). Aj keď zodpovednosť za bezpečnosť organizácie majú vrcholoví manažéri, je nutné, aby odbornú stránku zabezpečovali bezpečnostní manažéri, systémoví špecialisti ap., ktorí sú realizátormi bezpečnostnej politiky organizácie.

6 Zákonnosť

Princíp zákonnosti znamená, že všetky opatrenia na ochranu aktív organizácie budú vykonané v súlade s platnými zákonmi a právnymi predpismi.

7 Odôvodnenosť, opodstatnenosť

Ak majú byť opatrenia na ochranu aktív organizácie, musia zodpovedať požadovanému stupňu bezpečnosti aktív vzhľadom na ich možné ohrozenie. Všetky realizované opatrenia by mali zodpovedať pokrytiu identifikovaných ohrození a zraniteľných miest.

8 Efektívnosť

Efektívnosť bezpečnostného systému sa dosahuje tým, že náklady na ochranné opatrenia by nemali byť väčšie, ako očakávané straty v dôsledku pôsobenia bezpečnostných rizík. S čím menšími nákladmi dokážeme účinne chrániť aktíva organizácie, tým je efektívnosť bezpečnostného systému vyššia. Ak bezpečnostný systém nedokáže účinne ochrániť aktíva organizácie, potom budú dôsledky negatívnej udalosti zvýšené aj o náklady, ktoré sme vynaložili na vytvorenie bezpečnostného systému.

9 Profesionalita

Vytvorenie, riadenie a prevádzkovanie bezpečnostného systému je náročná činnosť, ktorú by mali vykonávať špeciálne pripravení, odborne spôsobilí pracovníci, či už zamestnanci organizácie, alebo pracovníci bezpečnostných služieb s príslušnou licenciou.

10 Synergia

Efektívna ochrana aktív organizácie si vyžaduje úzku spoluprácu a súčinnosť ako manažmentu organizácie, jeho pracovníkov, tak aj bezpečnostných služieb, ktoré poskytujú službu organizácie, ale aj Policajného zboru a ďalších zložiek, ktoré sa môžu podieľať na zaisťovaní bezpečnosti organizácie, resp. riešení krízových situácií a havárií.

11 Trvalé zlepšovanie (trvalá inovácia, modernizácia)

Zaisťovanie bezpečnosti organizácie je trvalý proces, ktorý musí reagovať na zmeny vo vonkajšom i vnútornom bezpečnostnom prostredí. Aby bol bezpečnostný systém schopný zaisťovať ochranu aktív organizácie, musí byť vykonávaný jeho pravidelný audit. Ak výsledky auditu preukážu, že bezpečnostný systém nezodpovedá aktuálnym požiadavkám a potrebám zaistenia bezpečnosti aktív organizácie, musí byť inovovaný (modernizovaný). Tiež treba trvalo sledovať a zohľadňovať technické inovácie prostriedkov útoku na aktíva organizácie (napr. v oblasti IT) a včas na ne reagovať (zlepšovaním a zvyšovaním odolnosti ochrany IT).

2.8 LITERATÚRA

ANETTOVÁ, A a kol. [2004]: *Synonymický slovník slovenčiny.* 3. nezm. vyd. Bratislava: Veda 2004. ISBN 80-224-0801-8.

BETUŠ, Ľ. [2014]: *Chráň náš svet, chráň svoj život, pomáhaj ohrozeným*. In: Civilná ochrana 2/2014. ISSN 1335-4094.

Bezpečnostná stratégia Slovenskej republiky 2005.

Doc 9859 AN/460 *Príručka manažérstva bezpečnosti Medzinárodnej civilnej organizácie letectva* (ICAO).

HANUŠIN, J. – HUBA, M. – IRA, V. – KLINEC, I. – PODOBA, J. – SZÖLLÖS, J. [2000]: Výkladový slovník termínov z trvalej udržateľnosti. Bratislava (STUŽ/SR).

HEGEL, G. W. F. [1986] *Logika ako veda.* 1. vyd. Bratislava : Pravda, 1986.

HOFREITER, L. [2004]: *Bezpečnosť, bezpečnostné rizika a ohrozenia.* Žilina: EDIS – vydavateľstvo ŽU. ISBN 80-8070-181-4.

HOFREITER, L. [2006]: *Securitológia.* Liptovský Mikuláš: Akadémia ozbrojených síl. ISBN 80-8040-310-4.

HOFREITER, L. [2006]: *Perspektívy bezpečnostného manažmentu v globálnom prostredí.* In: Security Revue 8. decembra 2006, Žilina: ŽU, FŠI.

IS/ISO/IEC Guide 51:2005 – *Bezpečnostné aspekty, pokyny pre ich začlenenie do noriem.*

JAROČKIN V. I. [2000]: *Sekuritologia – nauka o bezopasnosti žiznedejateľnosti*. Moskva: Os-89.

KORZENIOWSKI, L.F. [2008]: *Sekuritologie v procesu stávání se vědou.* In: Obrana a strategie 1/2008. Univerzita obrany Brno. ISSN 1214-6463.

KORZENIOWSKI L. F. [2005]: *Securitology. The concept of safety*. In: Comunikations, No 3, s. 20-23.

KORZENIOWSKI L.F. [2007]: *Securitologia na początku XXI wieku. „Securitologia/Securitology/Секюритология"* Zeszyty Naukowe European Association for Secu rity, nr. 6. Kraków.

KORZENIOWSKI, L. F. [2013]: *Teoretické a metodologické aspekty výskumu bezpečnosti.* In: Politické vedy. Roč. 16, č. 3. ISSN 1335 – 2741. Fakulta politických vied a medzinárodných vzťahov, UMB Banská Bystrica.

KOVÁCS, G. – DVOŘÁK, B. – PECINA, P. [2008]: *Analýza bezpečnostného prostredia ako podklad pre tvorbu bezpečnostných dokumentov. Podstata frekventovaných pojmov bezpečnostnej problematiky.* In: Zborník seminárnych vystúpení, Bezpečnostná a vojenská stratégia. Ústav strategických a obranných štúdií, UO Brno. ISBN 978-80-7231-622-9.

MASLOW, A. H [1943]: *A Theory of Human Motivation,* Psychological Review, 50.

MIKOLAJ, J. – HOFREITER, L. – MACH, V. – MIHÓK, J. – SELINGER, P. [2004]: *Terminológia bezpečnostného manažmentu. Výkladový slovník,* Žilina; ŽU FŠI.

MOHAN, D. – VARGHESE, M.[2003]: *Injuries in South-East Asia Region: Priorities for Policy and Action,* SAERO, World New Delhi.

NYE J.S. Jr. [1989]: *Problemy badań nad bezpieczeństwem*. „Sprawy Międzynarodowe", nr. 6, s. 51-64.

PORADA V. [2003]: *Teoretický rozbor policejní informace, situace a identifikace policejní činnosti.* Praha: „Bezpečnostní teorie a praxe". Sbornik Policejní akademie ČR.

REITŠPÍS, J. – MESÁROŠ,M. – BARTLOVÁ,I. – ČAHOJOVÁ, Ľ. – HOFREITER,L. –

SELINGER, P. [2004]: *Manažérstvo bezpečnostných rizík*. Žilina: EDIS – vydavateľstvo ŽU. ISBN- 80-8070-328-0.

SABO, M. [2010]: *Bezpečnosť práce.* Bratislava: STU. ISBN 80-227-1540-9.

SENČAGOV, V. K. [2015]: *Ekonomická bezpečnosť Ruska.* BINOM, vedecké laboratórium. ISBN: 978-5-9963-0166-9.

STN ISO 31000:2011 *Manažérstvo rizika, zásady a návod.*

ŠIMÁK, L. [2004]: *Krízový manažment vo verejnej správe.* Žilina: EDIS – vydavateľstvo ŽU. ISBN 80-88829-13-5.

ŠIMÁK, L. [2006]: *Manažment rizík.* Žilina: EDIS – vydavateľstvo ŽU.

Terminologický slovník krízového riadenia a zásady jeho používania, Bezpečnostná rada SR, Bratislava 2005.

Terminologický slovník krízového riadenia. Žilina: EDIS – vydavateľstvo ŽU. 2005. ISBN 80-88829- 75-5.

TULIBACKI W. [1999]: *Etyczne aspekty bezpieczeństwa na pewnych „stałych" cech natury ludzkiej*. In: ROSA R.: (red.) Edukacja dla bezpieczeństwa i pokoju w jednoczącejsię Europie. Siedlce: WSRP.

Ústavný zákon č. 227/2002 Z. z. o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu.

Zákon č. 42/1994 Z. z. *o civilnej ochrane obyvateľstva.*

ZIĘBA R. [2004]: *Instytucjonalizacja bezpieczeństwa europejskiego–koncepcje–struktury–funkcjonowanie.* Warszawa: SCHOLAR.

3 VÝVOJ BEZPEČNOSTNÝCH ŠTÚDIÍ

Chápanie pojmu bezpečnosť prešlo v minulosti (a prechádza aj v súčasnosti) svojím vývojom. Len donedávna bola bezpečnosť vnímaná ako synonymum života bez vojen. Hrôzy a utrpenie pochádzajúce z vojen, tak často vstupujúcich do života ľudí, spôsobovali nielen materiálne strádanie, ale aj nesmierne ľudské obete, či už priame, alebo v dôsledku hladu, chorôb a epidémií, majúcich príčiny vo vojnovom čase. Preto sa aj úsilie osvietených a pokrokových ľudí sústreďovalo na vytvorenie podmienok na mierový život – teda na trvalé zaistenie bezpečnosti.

V období studenej vojny, keď existoval bipolárny svet a ľudstvo čelilo hrozbe možnej globálnej vojny, na oboch póloch rozdeleného sveta bola oprávnená obava z možnej vojenskej invázie, či apokalypsy z dôsledkov raketojadrovej vojny. Otázka bezpečnosti bola spájaná najmä so zamedzením vzniku ničivého vojnového konfliktu medzi dvoma superveľmocami.

Dnes už znamená bezpečnosť oveľa viacej, než len vojenskú silu na odvrátenie vonkajších vojenských ohrození. V súčasnom multipolárnom svete sa bezpečnosť meria v prvom rade nevojenskými prostriedkami a riziká a ohrozenia bezpečnosti sú svojim charakterom prevažne nevojenské. V súčasnosti trápia Európu a Európanov viac než možný globálny vojenský konflikt také riziká a ohrozenia, ako sú *nestabilné politické režimy, nestabilné a nezabezpečené hranice umožňujúce nelegálnu migráciu a pašovanie (zbraní, drog, tovarov a pod.), etnické a náboženské konflikty, nedostatok prírodných zdrojov* a, samozrejme, *organizovaný zločin, terorizmus a kriminalita.*

V súčasnom svete je tiež čoraz ťažšie stanoviť hranicu medzi vonkajšou a vnútornou bezpečnosťou. Odstránenie administratívnych a politických bariér medzi štátmi umožnili nielen voľný pohyb osôb, peňazí a tovarov, ale aj zlepšenie podmienok pre činnosť a pôsobenie organizovaného zločinu. *Zločinecké živly* môžu dnes bez vážnejších prekážok pôsobiť skutočne v nadnárodnom rozsahu. Ani *prírodné katastrofy, priemyselné havárie či šírenie nákazlivých chorôb* nerešpektujú hranice štátov. Vplyvom *globalizácie* nie je žiadna krajina izolovaná od negatívnych javov, ktorých zdroje sa nachádzajú aj v geograficky vzdialenom priestore.

Bezpečnosť dnes nadobúda aj sociálny rozmer a vyžaduje si riešiť také problémy, ako je *nezamestnanosť, chudoba v tretích krajinách, masová migrácia a preľudnenosť v určitých aglomeráciách a závažné zdravotné problémy*. Aj keď sa na problém bezpečnosti môžeme pozerať z rôznych uhlov pohľadu, bezpečnosť je vo svojej podstate nedeliteľná a komplexná. Buď je, alebo nie je. Aby sa človek mohol cítiť bezpečný, musí žiť v bezpečnom svete, ktorý je tvorený priaznivými sociálno-ekonomickými podmienkami, bezpečným domom, mestom, regiónom, bezpečnou krajinou.

Podľa prístupu ku skúmaniu bezpečnosti je možné bezpečnostné štúdie rozdeliť do dvoch kategórií:

1. **tradičné bezpečnostné štúdie,**
2. **kritické bezpečnostné štúdie.**

Tieto uvedené charakteristiky možno nazvať **jadrom koncepcie bezpečnosti** a môžu sa použiť ako východiskový bod pre vypracovanie prehľadu systémových atribútov, ktoré sa objavujú v každej diskusii o bezpečnosti *(Mesjasz, 2006).*

3.1 TRADIČNÉ A KRITICKÉ BEZPEČNOSTNÉ ŠTÚDIE

Tradičné bezpečnostné štúdie

Tradičné bezpečnostné štúdie sú zamerané na ***vojenskú bezpečnosť a štát,*** vychádzajú z teórie realizmu. Bezpečnosť sa vymedzuje v protiklade k nebezpečenstvu, ako neexistencia vonkajších hrozieb, chápe sa ako neexistencia vojen a ozbrojených konfliktov a ich hrozieb. Za hlavný bezpečnostný nástroj sa považuje vojenský potenciál, ktorý je mnohostranne prepojený so štátom. Zvýrazňuje sa konfrontačný charakter zaistenia bezpečnosti, ktorá je spojená najmä s obranou štátu, územia, obyvateľov, hodnôt a so zaistením poriadku, stability, rovnováhy a určitosti.

Bezpečnosť sa tradične považuje za ***schopnosť štátu brániť sa proti vonkajším hrozbám.*** Tradičnú bezpečnosť, často aj ako **národnú bezpečnosť** alebo **bezpečnosť štátu** popisuje filozofia medzinárodnej bezpečnosti už od Vestfálskeho mieru v roku 1648 spolu s vytváraním národných štátov. Napriek tomu, že teórie medzinárodných vzťahov zahŕňali množstvo variantov tradičnej bezpečnosti, od realizmu k liberalizmu, základnou črtou týchto škôl bolo zameranie na pôvodnú koncepciu **národného štátu.**

Tradičný význam bezpečnosti sa odvodzuje od zahraničnej politiky a medzinárodných vzťahov – „vonkajšia bezpečnosť“ alebo „vojenská bezpečnosť“.

Vonkajšia bezpečnosť bola považovaná za atribút situácie štátu, ktorý zodpovedá absencii vojenského vonkajšieho konfliktu. Takýto prístup bol navrhnutý v teórii medzinárodných vzťahov v realizme i neorealizme a môže byť spojený s klasickými bezpečnostnými štúdiami a strategickými štúdiami.

Vojenská bezpečnosť je v realistickom a neskôr aj v neorealistickom prístupe charakterizovaná *vzťahom štátu, regiónu alebo zoskupenia štátov (aliancie) s iným štátom (štátmi), regiónmi, zoskupeniami štátov.* Bezpečnosť je vnímaná ako neprítomnosť ohrozenia, alebo stav, pri ktorom by bolo možné predchádzať výskytu následkov tejto hrozby, alebo by štát (región, aliancia) mohol byť od hrozby izolovaný. V mnohých prípadoch všetky aktivity súvisiace s vojenskými činnosťami zaručujú bezpečnostný kontext v jeho tradičnom zmysle – národnej bezpečnosti.

Tento pocit bezpečnosti môže byť rozšírený o koncept „**vnútornej bezpečnosti“,** t. j. absencia ohrozenia štátneho systému a každodenného života jeho občanov politickými alebo vojenskými narušeniami v rámci hraníc krajiny. Od 11. septembra 2001 sa rozšíril koncept „vnútornej bezpečnosti“ *(Homeland),* ktorý obsahuje ako vonkajšie, tak vnútorné ohrozenia a bol prijatý v novembri 2006 v USA.

Kritické bezpečnostné štúdie

Kritické bezpečnostné štúdie predstavujú jeden z najmladších smerov bezpečnostných štúdií (neorealizmus), vzniknutý v 90. rokoch, ktorý kritizuje dovtedajšie koncepty bezpečnosti a poukazuje na dovtedy zabúdané fakty. V máji 1994 sa v Toronte konala konferencia „Stratégie konfliktu: kritické prístupy k bezpečnostným štúdiám“, na ktorej sa začal používať termín *„**kritické bezpečnostné štúdie** (Critical Security Studies, CSS)“.*

Na túto konferenciu nadviazali autori Keith Kraus a Michael C. Wiliams publikáciou *„Critical Security Studies: Concept and Causes“.* Významným príspevkom k premene tradičných bezpečnostných štúdií smerom k ľudskej bezpečnosti boli práce **Kodanskej školy** (najmä Barry Buzan) a **Školy tzv. tretieho sveta** (napr. Mohamed Ayoob a Amitav Acharya). Obe školy spochybnili štátocentrizmus bezpečnostnej analýzy a prinášajú dva významné aspekty:

- skúmanie rozdielov medzi euroatlantickým prístupom a prístupom autorov tretieho sveta v poňatí bezpečnosti a zdrojov hrozieb,
- poňatie indivídua ako samostatného referenčného objektu.

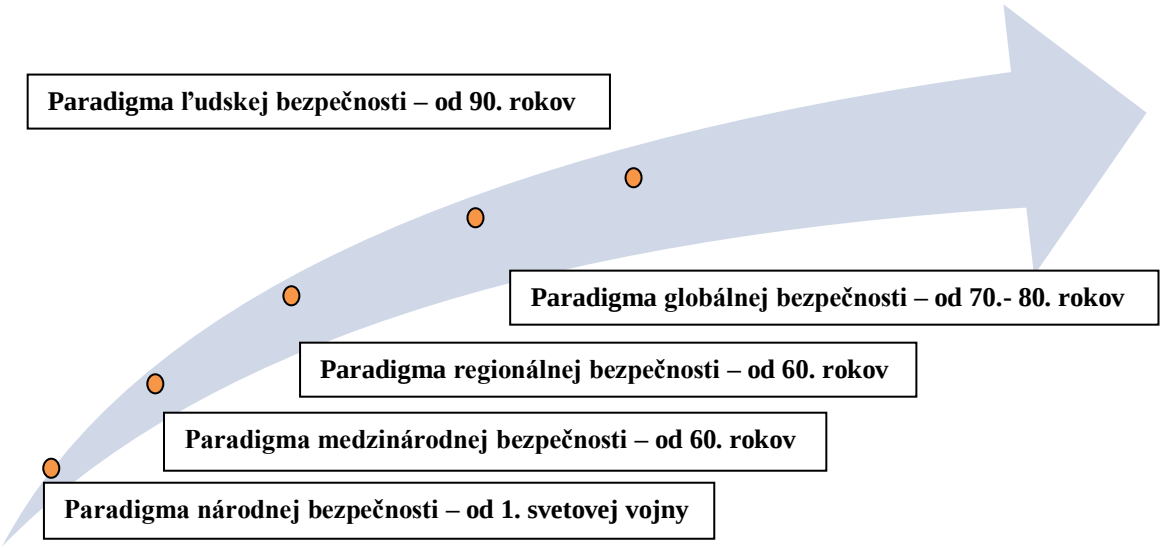
Bezpečnosť v kritických štúdiách prekonáva tradičné zdôrazňovanie vojenského rozmeru bezpečnosti a vojenských hrozieb, posudzuje sa z viacerých aspektov, s väčším dôrazom na iné, než vojenské príčiny napätia, kríz a konfliktov v medzinárodných vzťahoch.

Tradičné vojenské chápanie bezpečnosti sa rozširuje o nové typy hrozieb, ktoré sa analyzujú širším spôsobom a klasifikujú vo viacerých sektoroch, napr. *zhoršovanie životného prostredia, nedostatočný rozvoj a zaostalosť, organizovaný zločin, kriminalita, nedostatok surovín, vrátane potravín a pitnej vody a pod*. Činnosť alebo nečinnosť, či zlyhanie štátu sa môže stať zdrojom hrozieb pre jedinca a sociálnu skupinu i širšie bezpečnostné prostredie.

Teoretici kritických bezpečnostných štúdií sa pýtajú, napr.: „Ako je chránené indivíduum bez štátu (Kurdi, Palestínci…)?“ Podľa nich majú jednotlivci určité práva, ktoré nezávisia od existencie štátu. **Uznaním jednotlivca ako samostatného referenčného objektu bezpečnosti** došlo v roku 1994 k poslednému najradikálnejšiemu rozšíreniu konceptu bezpečnosti – **Human Security.**

3.2 PARADIGMY A ZÁKLADNÉ ROVINY BEZPEČNOSTI

Postupný proces rozširovania konceptu bezpečnosti našiel svoj odraz i v medzinárodných vzťahoch a medzinárodnej politike. V priebehu 20. storočia sa postupne vytvorilo päť paradigiem bezpečnosti: národnej bezpečnosti, medzinárodnej bezpečnosti, regionálnej bezpečnosti, globálnej bezpečnosti, ľudskej bezpečnosti (obr. 9).



Obr. 9 Paradigmy bezpečnosti

3.2.1 Paradigmy bezpečnosti

Paradigma národnej bezpečnosti – Prevládla v medzinárodných vzťahoch po 1. svetovej vojne, predpokladá ohrozenie štátu ostatnými štátmi, snaží sa zachovať vlastnú nezávislosť a suverenitu. Štát je najvyššou hodnotou, ktorá vyžaduje ochranu. Štát a národná bezpečnosť sa nikdy ako referenčný objekt z bezpečnostnej analýzy nestratil. Tradičná bezpečnosť sa snaží brániť štát pred vonkajšou agresiou. Walter Lippmann vysvetlil, že bezpečnosť štátu predstavuje schopnosť štátu potlačiť útok. Využíva odstrašujúce stratégie na zachovanie integrity štátu a ochrany územia od vonkajšieho hrozby *(Lippmann, 1943)*.

Paradigma medzinárodnej bezpečnosti – Vznikla na začiatku 60. rokov v súvislosti s výsledkom Karibskej krízy. Obe veľmoci boli na pokraji jadrovej vojny, kríza ukázala ako ďaleko sú oba štáty ochotné zájsť. Kríza potvrdila vzťah medzi USA a ZSSR, založený na vzájomne zaistenom zničení. Relatívne symetrické existenciálne ohrozenie oboch veľmocí bolo dostatočnou stratégiou na prekonanie jadrovej bezpečnostnej dilemy. Vznik paradigmy medzinárodnej bezpečnosti a jej prijatie v medzinárodných vzťahoch je možné spojiť s nárastom počtu a vplyvu medzinárodných inštitúcií, fungujúcich ako rámec pre realizáciu a kontrolu kooperatívnych stratégií a záujmom o kontrolu šírenia jadrových zbraní (*1963 – Zmluva o zákaze jadrových skúšok s výnimkou skúšok pod zemským povrchom)*. Referenčným objektom ostáva štát.

Paradigma regionálnej bezpečnosti – Vzniká paralelne s medzinárodnou bezpečnosťou, posilnila sa v 2. polovici 50. rokov, kedy sa rad zemí snažil vyviazať zo systémového konfliktu a prehlbovať spoluprácu so susedmi. Paradigma regionálnej bezpečnosti reflektuje napr. teórie bezpečnostných komplexov (B. Buzan). Má dve dimenzie:

1. **teritoriálnu** – vzťahuje sa na konkrétne územie, štáty v danom regióne majú záujem chrániť svoju bezpečnosť pred hrozbami pochádzajúcimi z iných regiónov, napr. EÚ, Africká únia.

2. **funkcionálnu** – vzťahuje sa na konkrétny sektor hrozieb, skupina štátov sa cíti rovnako ohrozená – tieto štáty sa spájajú, aby čelili tejto hrozbe, napr. NATO, CENTO, SEATO.

Paradigma globálnej bezpečnosti – Udalosti v 70. a 80. rokoch potvrdili myšlienku o náraste nepriamych hrozieb (nie je možné určiť konkrétneho pôvodcu ohrozenia), ako sú *globalizácia, vojensko-technologická revolúcia, informačná technológia, terorizmus, nadnárodný organizovaný zločin.* Manifestom paradigmy sa stala Palmeho správa *„Common Security“,* ktorá zdôrazňuje vzájomnú prepojenosť a závislosť (nie nutne symetrickú) všetkých svetových regiónov a všetkých štátov. Zaisťovanie spoločnej bezpečnosti predpokladá akciu všetkých členov systému (prekonáva bezpečnostnú dilemu), zahŕňa nielen zaistenie bezpečnosti štátov, ale i neštátnych aktérov (ľudstvo, biologické druhy, planéta).

Paradigma ľudskej bezpečnosti - Vzniká v 90. rokoch v Programe OSN pre rozvoj (UNDP), podstatou je ***ochrana indivídua, jeho života a práv***. Hlavnými zástancami tohto konceptu boli UNDP, UNHCR, Kanada, Nórsko, hlavnými odporcami boli chudobné štáty svetovej periférie poukazujúce na nedostatok vlastných zdrojov na zaistenie práv jednotlivca. Formovanie tejto paradigmy možno sledovať na pozadí súčasnej diskusie o právach na humanitárnu intervenciu. Táto intervencia narušuje základné a doteraz akceptované pravidlá Vestfálskeho systému (suverenita, teritorialita) štátov a favorizuje indivíduum, ktoré je ohrozené štátom.

3.2.2 Základné roviny bezpečnosti v súčasnosti

V súčasnosti sa pojem bezpečnosť týka celej planéty, kontinentu, regiónu, štátu, sociálnej skupiny, mesta (obce), občana, objektu, podniku, majetku alebo informácií. Z hľadiska úrovne, na ktorej sa bezpečnosť posudzuje, je možné bezpečnosť deliť na *(Ivančík, 2012):*

1. **Medzinárodná bezpečnosť** – taký stav komplexu medzinárodných vzťahov, ktorý jeho subjektom zabezpečuje rovnakú úroveň, bezpečnosť medzinárodného prostredia je vnímaná na najširšej globálnej medzinárodnej úrovni.
2. **Regionálna bezpečnosť** – bezpečnosť regionálnych zoskupení, vnímaná na úrovni rôznych regionálnych zoskupení ako sú napr. EÚ, Africká únia atď.
3. **Národná bezpečnosť** – bezpečnosť štátu, vnímaná tradične na úrovni štátov ako subjektov medzinárodného práva.
4. **Skupinová bezpečnosť** – bezpečnosť vnútroštátnych skupín, vnímaná na úrovni organizovaných skupín v rámci spoločnosti, záujmových skupín alebo politických strán.
5. **Individuálna bezpečnosť** – osobná bezpečnosť, vnímaná na úrovni jednotlivcov (jednotlivých osôb), nie skupín alebo obyvateľstva (obr. 10).

Každá z týchto úrovní bezpečnosti sa dá vnútorne ešte ďalej diferencovať na základe viacerých kritérií (napr. veľkosť aktérov, typy a druhy inštitúcií zaisťujúcich bezpečnosť, spôsob ich riadenia a pod.). Jednotlivé úrovne bezpečnosti sa navzájom podmieňujú, ale rozdielne mechanizmy ich utvárania a fungovania spôsobujú, že väzby medzi nimi a ich vzájomné ovplyvňovanie nie sú priamočiare. Vysoká úroveň bezpečnosti v jednej rovine neznamená automaticky rovnakú úroveň bezpečnosti, či odstránenie bezpečnostných hrozieb aj v ďalších rovinách.

Medzinárodná bezpečnosť

Medzinárodná bezpečnosť *(International Security)* predstavuje bezpečnosť medzinárodného prostredia a bezpečnosť regionálnych zoskupení. Globálne bezpečnostné prostredie je určené teritóriom celého sveta a je limitované rovnováhou politických, ekonomických, diplomatických, bezpečnostných, vojenských, sociálnych, kultúrnych, náboženských, hodnotových, etnických a ekologických vplyvov. Regionálne bezpečnostné prostredie je určené re-

gionálnymi hranicami na geopolitickej mape, ktoré vymedzujú teritória susedných, prípadne aj okolitých štátov. Slovensko existuje v tomto prostredí a jeho bezpečnosť – ako malej krajiny – je vecou stability rozvoja jeho spoločnosti.

Vo všeobecnom encyklopedickom slovníku je medzinárodná bezpečnosť definovaná ako: *„súbor právnych pravidiel, inštitúcií a opatrení v oblasti medzinárodných vzťahov, ktoré majú zaistiť zachovanie medzinárodného mieru a bezpečnosti, pokojný život a rozvoj národov“*. Je to taký stav komplexu medzinárodných vzťahov, ktorý svojím subjektom zabezpečuje rovnakú úroveň národnej bezpečnosti. Utvára sa predovšetkým v interakcii štátov a iných aktérov medzinárodných vzťahov. Nový systém bezpečnosti vo svete, ktorý je založený na medzinárodných vzťahoch, sa formuje od skončenia studenej vojny, je predovšetkým ovplyvnený:

- novým rozdelením sveta, kde dominantné postavenie majú USA, Rusko a Čína ako svetové superveľmoci,
- rastúcim vplyvom niektorých medzinárodných organizácií, ktoré na základe dohôd a medzinárodného práva dokážu riešiť spory medzi štátmi mierovými dohodami (napr. NATO, EÚ, Medzinárodný menový fond a Svetová banka, menej však OSN a OBSE),
- posilňovaním regionálnych mocností (Izrael, Kórea, India, Brazília atď.),
- kontrolou zbraní hromadného ničenia,
- snahou niektorých štátov získať jadrové zbrane (Irán, KĽDR),
- integráciou a dezintegráciou, rastúcim vplyvom niektorých ekonomicky silných štátov,
- lokálnymi zdrojmi napätia,
- nerovnomerným rozdelením bohatstva,
- historickými zmenami v niektorých arabských štátoch, ktoré môžu priniesť ich demokratizáciu alebo islamizáciu (šírenie islamu a moslimskej populácie do sveta),
- narastajúcim nacionalizmom v mnohonárodných štátoch.

Nový význam a nebezpečnejší charakter získavajú také hrozby ako *terorizmus, nelegálne šírenie zbraní hromadného ničenia, extrémizmus, organizovaný zločin, zlyhávajúce štáty, diktátorské režimy v ich vzájomnej previazanosti* atď.

Regionálna bezpečnosť

Organizácia pre bezpečnosť a spoluprácu v Európe OBSE je **najväčšou existujúcou regionálnou bezpečnostnou organizáciou,** ktorá zahŕňa oblasť Európy, Kaukazu, Strednej Ázie a severnej Ameriky. Spoločným cieľom všetkých účastníckych krajín OBSE je na základe vzájomnej spolupráce udržiavať mier a bezpečnosť v geografickom priestore OBSE. Štáty sa zaviazali rešpektovať ľudské práva a základné slobody, demokraciu, princípy právneho štátu a zabezpečiť sociálnu spravodlivosť a ochranu životného prostredia.

Danú organizácia v súčasnosti tvorí 57 účastníckych štátov z Európy, Strednej Ázie a Severnej Ameriky vrátane SR. Organizácia OBSE predstavuje komplexný prístup k bezpečnosti, ktorý zahŕňa politicko-vojenské, ekonomické, environmentálne a rovnako aj ľudskoprávne aspekty. Činnosť OBSE pokrýva širokú škálu otázok súvisiacich s bezpečnosťou, vrátane kontroly zbrojenia, ľudských práv, národnostných menšín, demokratizácie, policajných stratégií, boja proti terorizmu, ekonomických a ekologických aktivít.

Základným dokumentom OBSE je ***Deklarácia zásad riadiacich vzťahy medzi účastníckymi štátmi Konferencie pre bezpečnosť a spoluprácu v Európe*** prijatá v Helsinkách v roku 1975. Túto deklaráciu tvorí 10 princípov:

1. Zvrchovaná rovnosť, rešpektovanie práv vyplývajúcich zo zvrchovanosti.
2. Nepoužitie sily alebo hrozby silou.

3. Neporušiteľnosť hraníc.
4. Územná integrita štátov.
5. Mierové riešenie sporov.
6. Nezasahovanie do vnútorných záležitostí.
7. Rešpektovanie ľudských práv a základných slobôd, vrátane slobody myslenia, svedomia, náboženstva a presvedčenia.
8. Rovnoprávnosť a právo národov na sebaurčenie.
9. Spolupráca medzi štátmi.
10. Svedomité plnenie záväzkov podľa medzinárodného práva.

V snahe dosahovať čo najlepšie výsledky v rámci stanovených cieľov OBSE podporuje nasledujúce aktivity: *Boj proti nezákonnému obchodovaniu; Demokratizácia; Vzdelávanie; Ľudské práva; Práva menšín; Tolerancia a nediskriminácia.*

OBSE má rozsiahly prístup k ***politicko-vojenskej dimenzii bezpečnosti***, prostredníctvom ktorej sa snažia dosahovať stanovené ciele v tejto oblasti. Dosiahnutiu týchto cieľov napomáhajú nasledujúce aktivity: *Správa hraníc; Boj proti terorizmu; Kontrola zbrojenia; Vojenská reforma; Polícia; Prevencia konfliktov.*

Národná bezpečnosť – bezpečnosť štátu

Ústavný zákon č. 227/2002 Z. z. o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu udáva bezpečnosť štátu ako stav, v ktorom sú zachovávané:

- mier, zvrchovanosť, územná celistvosť a nedotknuteľnosť hraníc,
- fungovanie, stabilita a rozvoj štátu,
- vnútorný demokratický poriadok, základné práva a slobody občanov,
- ochrana životov a zdravia osôb, majetku a životného prostredia.

Vonkajšia bezpečnosť štátu má základnú úlohu zabezpečiť samostatne a v koalícii štátnu zvrchovanosť a územnú celistvosť SR.

Vnútorná bezpečnosť štátu znamená taký stav usporiadania a poriadku v krajine, aby v nej mohla bezchybne fungovať demokratická spoločnosť. Je to stav, v ktorom sú na minimálnu mieru eliminované ohrozenia štátu a jeho záujmy zvnútra a štát má vytvorené dostatočné právne prostredie, inštitúcie, zdroje, sily, prostriedky a mechanizmy na riešenie možných krízových situácií. Je to tiež spoločnosťou akceptovaná úroveň demokracie, ekonomickej prosperity, ochrany občanov a uplatňovania právnych noriem, ktorých zabezpečovanie je jednou zo základných funkcií štátu. Pojem bezpečnosť (vo význame vnútornej bezpečnosti) môžeme chápať ako:

- súhrn spoločenských vzťahov, ktoré upravuje právo a ktoré chránia práva a oprávnené záujmy fyzických a právnických osôb, záujmy spoločnosti a ústavné zriadenie republiky,
- faktický stav (úroveň), ako sa tieto vzťahy chránia,
- kategóriu, v ktorej sa chápe bezpečnosť.

Verejný poriadok predstavuje takú úroveň spoločenských vzťahov vznikajúcich a prejavujúcich sa v správaní ľudí prevažne na verejnosti a regulovaných sociálnymi normami, ktoré sú podľa charakteru miesta, času a verejnej mienky nevyhnutnou podmienkou pre fungovanie verejnej správy, činnosť právnických a podnikajúcich fyzických osôb, pre život občanov, v súlade so zásadami stanovenými právnym poriadkom, ale aj s názormi spoločnosti na správanie ľudí.

Skupinová bezpečnosť – bezpečnosť vnútroštátnych skupín

Skupinová bezpečnosť je spojená najmä s interakciou sociálnych skupín medzi sebou, ale aj s ďalšími subjektmi pôsobiacimi v bezpečnostnej oblasti. Rôzne konfliktné prvky napätia, ktoré sa môžu stať aj bezpečnostnými problémami, môžu vytvárať rozdiely rasové, náboženské, etnické, sociálne, majetkové, kultúrne a iné. Novým zdrojom bezpečnostných hrozieb sa na začiatku 21. storočia stávajú aktivity skupín etnického a konfesionálneho charakteru, ktoré sa nachádzajú na teritóriách viacerých štátov a snažia sa spájať.

Individuálna bezpečnosť

Osobná (individuálna) bezpečnosť *(Personnel Security)* je stav, ako pociťuje ohrozenie svojej existencie a rozvoja jednotlivec. Bezpečnosť osoby sa môže chápať ako:

- ***fyzická bezpečnosť*** – predstavuje bezprostrednú telesnú neporušenosť a neprítomnosť ohrozenia,
- ***ekonomická bezpečnosť*** – trvalé zabezpečenie základov existencie, ktoré zaistia budúcnosť osoby.

Podľa Maslowovej hierarchie ľudských potrieb po naplnení fyziologických potrieb potrebuje človek pocit istoty: istota zamestnania, istota príjmu a prístupu k zdrojom, fyzická bezpečnosť – ochrana pred násilím a agresiou, morálna a fyziologická istota, istota rodiny, istota zdravia. Bezpečnosť pre ľudí neznamená len objektívny stav bez nebezpečenstva a rizika, ako napr. chránené ubytovanie so zaistením zásobovania všetkými potrebami, ale aj subjektívny pocit bezpečia, bez ohľadu na to, či takýto stav existuje. Toto platí pre jednotlivé osoby, ale aj pre celé skupiny obyvateľov.

Najdôležitejšie prvky pre dosiahnutie bezpečnosti jednotlivcov tvoria: *ľudské a občianske práva, sociálno-ekonomické podmienky existencie a rozvoj indivíduí.*

Ak sa na úroveň uvedených podmienok neprihliada alebo sa podceňujú, predstavujú ľudské práva iba formálnu záležitosť, ktorá reálne neprispieva k zaisteniu bezpečnosti.

3.3 KONCEPCIA ĽUDSKEJ BEZPEČNOSTI

Výstupom diskusie o ľudskej bezpečnosti bol produkt ***aproximácie (priblíženia) faktorov na konci studenej vojny.*** Tieto odmietli dominanciu neorealistickej paradigmy sústredenia sa štátov na „vzájomne zaručené zničenie“ a ***vojenskú bezpečnosť*** a heslovite aktivovali vznik ***širšieho poňatia bezpečnosti.*** Stále rýchlejšie tempo globalizácie, zlyhanie liberálneho budovania štátu prostredníctvom nástrojov washingtonského konsenzu, zníženie hrozby jadrovej vojny medzi veľmocami, exponenciálny rast v šírení a upevňovaní demokratizácie a medzinárodných noriem v oblasti ľudských práv otvorili priestor, v ktorom by mohli byť preskúmané aj „vývoj“ aj „koncepcie“ bezpečnosti.

V rovnakom čase sa zvýšil počet vnútorných násilných konfliktov v Afrike, Ázii a Európe (Balkán, Gruzínsko, Ukrajina), ktoré mali za následok koncepcie národnej a medzinárodnej bezpečnosti a neodrážali výzvy nového bezpečnostného prostredia po studenej vojne, zlyhanie neoliberálnych modelov rozvoja generovať rast, najmä v Afrike, alebo sa zaoberať s následkami komplexných nových hrozieb (ako je HIV/AIDS a zmena klímy), posilnili pocit, že medzinárodné inštitúcie a štáty neboli organizované na riešenie týchto problémov integrovaným spôsobom.

Hlavné možné ukazovatele pohybu smerom k individuálnemu poňatiu bezpečnosti ležia v prvom rade vo vývoji medzinárodnej spoločnosti, úvahách o právach jednotlivcov oproti potenciálnym hrozbám zo štátov. Najviditeľnejšie základy analýzy sú Charta OSN, Deklarácia OSN o ľudských právach (1948) a jej sprievodné záväzky (1966) a dohovory, týkajúce sa konkrétnych zločinov (napr. genocída) a práv jednotlivých skupín (napr. ženy, rasové skupiny a utečenci) *(MacFarlane* a *Yuen Foong Khong, 2006).*

Rozvojový program OSN definoval v roku 1990 **ľudský rozvoj ako proces rozširovania ľudských možností.** V zásade môžu byť tieto možnosti nekonečné a môžu sa meniť v čase. Primárnym cieľom rozvoja je vytvoriť také prostredie, ktoré umožní ľuďom vychutnávať zdravý, dlhý a tvorivý život. Rozvoj má predovšetkým vytvoriť možnosti, ktoré umožnia zvýšiť schopnosti ľudí tak, aby mali príležitosť žiť taký život, aký si sami cenia. Základnými predpokladmi pre to sú: ***dlhý a zdravý život, prístup k vzdelaniu, prístup k prostriedkom, ktoré umožnia prežiť dôstojný život a príležitosť aktívne sa zapájať sa do života spoločenstva.*** Pokiaľ nie sú tieto základné možnosti k dispozícii, veľa ďalších príležitostí ostane nedostupných.

3.3.1 Bezpečnostný koncept „ľudskej bezpečnosti“

Bezpečnostný koncept „ľudskej bezpečnosti“ vznikol v rámci Rozvojového programu OSN *(United Nations Development Programme, UNDP)* v súvislosti so Správou o rozvoji spoločnosti *(Human Development Report)* z roku 1994, ktorú vypracoval Dr. Mahbub ul Haq (pakistanský ekonóm). Koncept bol pôvodne zameraný na ochranu dvoch základných slobôd definovaných v preambule Všeobecnej deklarácie ľudských práv:

- **oslobodenie od strachu,**
- **oslobodenie od nedostatku**.

Postupne sa tento koncept stal doktrínou sprevádzajúcou zahraničnú politiku a podporu medzinárodného rozvoja, ako aj politickým nástrojom OSN.

Bývalý generálny tajomník OSN Kofi Annan v predslove k „Ľudskej bezpečnosti a novej diplomacii“ pri popise čo je ľudská bezpečnosť píše: *„Počas studenej vojny definície bezpečnosti boli zamerané takmer výhradne z hľadiska vojenskej sily a rovnováhy. Dnes vie-*

me, že bezpečnosť znamená oveľa viac ako absencia konfliktu. Máme tiež väčšie uznanie pre nevojenské zdroje konfliktu. Vieme, že trvalý mier vyžaduje širšie vízie, ktorá zahŕňa oblasti, ako je vzdelávanie a zdravotníctvo, demokracia a ľudské práva, ochrana proti zhoršovaniu životného prostredia a šírenie smrtiacich zbraní. Vieme, že nemôžeme byť bezpeční uprostred hladovania, že nemôžeme budovať mier bez zmierňovania chudoby, a že nemôžeme budovať slobodu na základoch nespravodlivosti. Toto sú piliere toho, čo teraz rozumieme ako koncepcie zamerané na ľudí – ľudskej bezpečnosti – ktoré sú vzájomne prepojené a vzájomne sa posilňujú".

Podľa Mahbub ul Haqa, **ľudský rozvoj** je výsledkom komplexného procesu, ktorý zahŕňa sociálne, ekonomické, demografické, politické a kultúrne faktory. Základným cieľom rozvoja je rozšíriť možnosti ľudí. Ľudia si vo všeobecnosti cenia úspechy, ktoré nie sú priamo spojené s výškou príjmu či s ekonomickým rastom, ako napr.: *ľahší prístup k vzdelaniu, lepšia výživa a zdravotnícka starostlivosť, zaistené živobytie, ochrana pred zločinom a násilím, voľný čas, politická a kultúrna sloboda a možnosť aktívnej účasti na živote spoločnosti (Mahbub ul Haq, 1994).*

Rozvojové ciele OSN pre ďalšie tisícročie, stanovené v roku 2000, sa pokúsili kodifikovať rozsah ľudskej bezpečnosti a realizovať jej merateľnosť. V súčasnosti sa Human Security dostala do každodenného slovníka vládnych úradníkov, vojenských a nevládnych pracovníkov, humanitárnych pracovníkov a politikov. Dôležitosť ochrany ľudskej bytosti pre medzinárodnú bezpečnosť je teraz uznávaná, ale jej implementácia sa ukazuje ako veľmi ťažká.

Základnou myšlienkou tohto konceptu je fakt, že v centre záujmu všetkých bezpečnostných iniciatív je človek. Dôvodom, ktorý v súčasnosti prevažuje misku váh na stranu mäkkej bezpečnosti je fakt, že mäkké hrozby voči bezpečnosti (hlad, nedostatok pitnej vody, choroby) zabijú každoročne milióny ľudí, o mnoho viac, ako toľko diskutované tvrdé bezpečnostné hrozby.

Na rozdiel od tradičného chápania bezpečnosti sa na bezpečnosť nenazerá v súvislosti s vojnou medzi štátmi, ako v prípade národnej bezpečnosti, kde je povinnosťou jednotlivcov voči svojej vláde zabíjať, alebo byť zabitý. Naopak, v tomto prípade sú jednotlivci (alebo všeobecne ľudia) v centre záujmu, analýz a politiky a štáty sú kolektívnym nástrojom na ochranu ľudského života a zabezpečenie ľudského blahobytu.

Základom je teda bezpečnosť ľudí voči hrozbám pre ich osobnú bezpečnosť a život. Podľa definície Oxfordskej univerzity „*cieľom ľudskej bezpečnosti je ochrániť základné životné potreby všetkých ľudí od všadeprítomných závažných hrozieb spôsobom, ktorý umožní dlhodobé naplnenie ich existencie*".

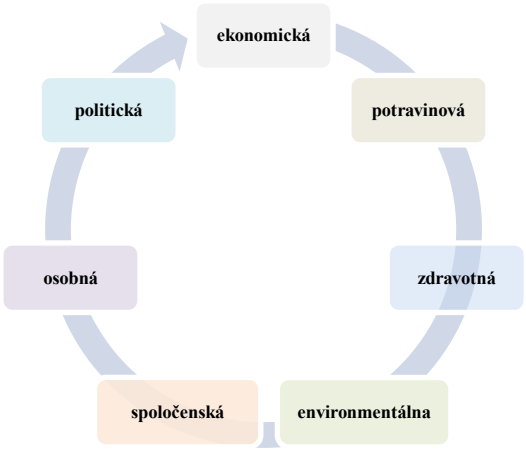
Definíciu Human Security, ktorá svojím spôsobom prepojuje široké i úzke poňatie, spracoval aj Taylor Owen: „*Ľudská bezpečnosť znamená ochranu minima nutného pre život každého človeka pred kritickými a agresívnymi hrozbami spojenými s ekonomickou situáciou, osobnou bezpečnosťou, politickým prostredím, výživou, zdravím a životným prostredím človeka*".

Tento nový prístup zdôraznil, že poňatie bezpečnosti sa musí zmeniť dvomi základnými spôsobmi:

- dôraz na bezpečnosť územia transformovať na primárny dôraz na bezpečnosť ľudí,
- posunúť sa od bezpečnosti cez vojenský potenciál k bezpečnosti cez udržateľný ľudský rozvoj.

V Správe o rozvoji spoločnosti z roku 1994 sa definuje, že oblasť globálnej bezpečnosti sa musí rozšíriť a zahrnúť ohrozenia v siedmich sektoroch (oblastiach) bezpečnosti, kto-

ré sú znázornené na obr. 10: *ekonomickej, potravinovej, zdravotnej, environmentálnej, spoločenskej, osobnej a politickej*.



Obr. 10 Oblasti bezpečnosti podľa Human Security

Ekonomická bezpečnosť – stav, v ktorom ekonomika objektu, ktorého bezpečnosť má byť zaistená (štátu, aliancie štátov, podniku, podnikateľských subjektov a pod.) nie je vystavená rizikám a ohrozeniam, ktoré by mohli výrazne znížiť (alebo už znižujú) jej výkonnosť, potrebnú na plnenie základných funkcií a dosahovanie cieľov. Predstavuje najmä zaistený základný príjem pre jednotlivca, zvyčajne za produktívnu a lukratívnu prácu alebo ako sociálne zabezpečenie. Hlavnými hrozbami sú *ekonomická nezamestnanosť a pretrvávajúca chudoba, ktoré vyvolávajú politické napätie a etnické násilie.*

Potravinová bezpečnosť – stav, v ktorom je zabezpečená výroba, obchod, preprava a skladovanie potravín v druhoch a množstvách, ktoré zabezpečujú plynulé zásobovanie obyvateľstva. Vyžaduje, aby všetci ľudia za každých okolností mali fyzický a ekonomický prístup k základným potravinám. Podľa OSN celková dostupnosť potravín nie je problémom, častejším problémom je zlá distribúcia potravín a nedostatok kúpnej sily. Hlavnými hrozbami sú *hlad vo svete, nedostatok základných potravín v niektorých krajinách.*

Zdravotná bezpečnosť – bezpečnosť zdravia má za cieľ zaručiť minimálnu ochranu pred chorobou a nezdravým životným štýlom. V rozvojových krajinách hlavnými príčinami úmrtí boli tradičné choroby, kým v priemyselných krajinách hlavným problémom boli choroby obehovej sústavy. Hlavnými hrozbami sú *smrteľné infekčné choroby, HIV/AIDS, materská úmrtnosť, podvýživa, nebezpečné potraviny a nedostatočná zdravotná starostlivosť.* Patrí sem aj *biologická bezpečnosť* – riadenie rizika, ktoré predstavujú geneticky modifikované organizmy (GMO) pre ekonomiku, životné prostredie a zdravie ľudí, prostredníctvom vylúčenia, tlmenia, adaptácie, kontroly – ochrany a eradikácie (ničenie choroboplodných organizmov); zahŕňa bezpečný prenos, narábanie a využívanie živých organizmov, ktoré sú výsledkom biotechnológií a mohli by negatívne ovplyvniť biodiverzitu.

Environmentálna bezpečnosť – stav, v ktorom ľudská spoločnosť a ekologický systém na seba pôsobia trvalo udržateľným spôsobom, jednotlivci majú dostatočný prístup ku všetkým prírodným zdrojom a existujú mechanizmy na zvládanie kríz a konfliktov priamo či nepriamo spojených so životným prostredím. V tomto stave sú minimalizované riziká a ohrozenia spojené so životným prostredím a spôsobené prírodnými alebo antropologickými silami alebo procesmi vyvolanými antropologickými silami. Podstatou je chrániť ľudí pred krátkodobým a dlhodobým pustošením prírody, umelými hrozbami a zhoršovaním životného prostredia. V rozvojových krajinách je *nedostatočný prístup k čistým vodným zdrojom* jednou

z najväčších ekologických hrozieb. V priemyselných krajinách jednou z hlavných hrozieb je *znečistenie ovzdušia, globálne otepľovanie.* Hlavnými hrozbami sú *environmentálna degradácia lokálnych ekosystémov i globálneho systému, vyčerpanie prírodných zdrojov, nedostatok čistej vody, degradácia pôdy, najrôznejšie znečistenie, prírodné katastrofy.*

Osobná bezpečnosť – zameriava na ochranu ľudí pred fyzickým násilím, či už štátnym alebo od iných štátov, pred násilnými jednotlivcami a inými aktérmi, pred domácim násilím alebo zneužívaním detí. Najväčším zdrojom obáv je zločin – najmä násilné trestné činy. Hlavnými hrozbami sú *fyzické násilie a mučenie vo vojne, kriminalita – osobitne násilná, domáce násilie, nútená detská práca, užívanie drog* a pod.

Spoločenská bezpečnosť – má za cieľ chrániť ľudí pred narušením tradičných vzťahov a hodnôt. Ohrozené sú tradičné spoločenstvá, najmä etnické menšinové skupiny, tieto etnické konflikty sa vyskytujú skoro v polovici štátov sveta. Hlavnými hrozbami sú *etnické, náboženské či iné napätie* založené na báze rozdielnych identít, ohrozené je prežitie tradičných kultúr a etnických skupín a tiež ich fyzická bezpečnosť.

Politická bezpečnosť – týka sa toho, či ľudia žijú v spoločnosti, ktorá ctí ich základné ľudské práva. Podľa prieskumu, ktorý uskutočnila organizácia Amnesty International, politické represie, systematické mučenie, zlé zaobchádzanie alebo únosy sa stále praktizujú v 110 krajinách. Porušovanie ľudských práv je najčastejšie v období politických nepokojov. Hlavnými hrozbami sú *politický nátlak a potlačovanie ľudských, občianskych a politických práv.*

3.3.2 Ďalšie koncepcie ľudskej bezpečnosti

V teórii ľudskej bezpečnosti sa dostáva stále viac pozornosti od kľúčových globálnych rozvojových inštitúcií, ako je Svetová banka. Tadjbakhsh, okrem iného, odvodil z vývoja ľudskej bezpečnosti v medzinárodných organizáciách záver, že koncept bol rozpracovaný a od roku 1994 výrazne zmenený, aby bol vhodný pre záujmy organizácií *(Tadjbakhsh, 2007).*

Tomuto konceptu je často vytýkaná prílišná neurčitosť, neohraničenosť – všetko, čo narušuje fyzický a duševný blahobyt človeka, je konceptom Human Security považované za hrozbu. Požiadavku na zúženie či „zaostrenie“ konceptu možno považovať za oprávnenú a užitočnú – Human Security by bolo zamerané na také javy, ktoré predstavujú ohrozenie života a základných životných potrieb človeka.

Sedem kategórií hrozieb z Rozvojového programu OSN získava primeranú celosvetovú pozornosť a zdroje. Napriek tomu sa prejavuje snaha realizovať túto agendu ľudskej bezpečnosti vznikom dvoch hlavných myšlienkových smerov, ako najlepšie zabezpečiť praktickú bezpečnosť človeka – „Oslobodenie od strachu“ a „Oslobodenie od nedostatku“.

Oslobodenie od strachu – Táto škola sa snaží obmedziť prax Human Security na ochranu osôb pred násilným konfliktom a zároveň uznáva, že tieto násilné hrozby sú silne spojené s chudobou a nedostatočnou kapacitou štátu. Tento prístup tvrdí, že obmedzenie zamerania na násilie je realistický prístup k ľudskej bezpečnosti. Pomoc pri mimoriadnych udalostiach, predchádzanie konfliktom a ich riešenie, budovanie mieru sú hlavnými problémami tohto prístupu.

Oslobodenie od nedostatku – Škola presadzuje holistický prístup k dosiahnutiu ľudskej bezpečnosti a tvrdí, že agenda hrozby by mala byť rozšírená, aby zahŕňala hlad, choroby, prírodné katastrofy, pretože sú neoddeliteľné pri riešení koreňov ľudskej neistoty a usmrtia oveľa viac ľudí ako vojny, genocídy a terorizmus a ich kombinácie. Na rozdiel od „oslobodenia od strachu“ sa rozširuje zameranie okrem násilia na dôraz na rozvoj a bezpečnostné ciele.

Napriek rozdielom možno považovať, že sa tieto dva prístupy k ľudskej bezpečnosti skôr dopĺňajú, než sú v rozpore. Výrazy v tomto zmysle zahŕňajú aj tieto názory:

- **Franklin D. Roosevelt** v prejave v roku 1941 (Štyri slobody), charakterizoval *slobodu od nedostatku* ako tretiu a *slobodu od strachu* ako štvrtú základnú univerzálnu slobodu.
- **Vláda Japonska** považuje *oslobodenie od strachu* a *slobodu od nedostatku* za rovnocenné vo vývoji zahraničnej politiky Japonska.
- **Surin Pitsuwan,** generálny tajomník ASUAN, na základe teoretikov, ako Hobbes, Locke, Rousseau a Houmy vyvodil, že „*ľudská bezpečnosť je primárnym cieľom na začiatku organizovania štátu*". Vyvodil záver, že *Správa o ľudskom rozvoji* z roku 1994 oživila tento koncept, a naznačuje, že autori z roku 1994 mohli využiť prejav Franklina Roosevelta bez toho, aby ho doslovne citovali *(Pitsuwan, 2007).*

Aj keď *sloboda od strachu* a *sloboda od nedostatku* sa najviac vzťahujú na praktické kategórie ľudskej bezpečnosti, narastá počet ďalších alternatívnych myšlienok ako najlepšie riešiť ľudskú bezpečnosť v praxi. Medzi ne patria teórie:

- **G. King a C. Murray** sa snažia zúžiť ľudskú bezpečnosť definovaním „*očakávania rokov života, bez zažitia stavu všeobecnej chudoby"*. V ich definícii, „všeobecná chudoba" znamená „klesnutie pod kritické hranice v ľubovoľnej oblasti blahobytu" a v rovnakom článku dávajú stručný prehľad kategórií „domény blahobytu". Tento súbor definícií je podobný ako „sloboda od nedostatku", ale má konkrétnejšie zameranie na niektoré hodnotové systémy.
- **Caroline Thomas** *(2000)* si všíma, že bezpečnosť ľudí opisuje „*stav bytia*", ktorý predstavujú základné materiálne potreby, ľudská dôstojnosť, vrátane zmysluplnej účasti na živote spoločnosti a aktívnu a vecnú predstavu o demokracii od miestnej až po globálnu úroveň.
- **Roland Paris** *(2001)* argumentuje, že je mnoho spôsobov, ako definovať „ľudskú bezpečnosť", sú príbuzné s určitým súborom hodnôt a strácajú neutrálnu pozíciu. Odporúča, aby sa ľudská bezpečnosť považovala za kategóriu výskumu. Uvádza maticu 2x2 pre objasnenie oblastí bezpečnostných štúdií.
- **Sabina Alkire** *(2003)* sa odlišne od týchto prístupov snaží zúžiť a špecifikovať ciele ľudskej bezpečnosti, posunuje myšlienku ešte o krok ďalej ako „*ochrániť podstatné jadro všetkých ľudských životov pred kritických všadeprítomnými hrozbami, bez narušenia dlhodobých ľudských želaní*". V koncepte navrhne „životné jadro", ochranu minimálneho alebo hlavného súboru základných funkcií pre prežitie, existenciu a dôstojnosť a všetky inštitúcie by mali minimálne a záväzne chrániť toto jadro pred akýmkoľvek zásahom.
- **Lyal S. Sunga** *(2009)* argumentoval, že koncept ľudskej bezpečnosti, ktorý je plne zavedený medzinárodným právom v oblasti ľudských práv, medzinárodného humanitárneho práva, medzinárodného trestného práva a medzinárodného utečeneckého práva a ktorý berie do úvahy príslušné medzinárodné právne normy zakazujúce použitie sily v medzinárodných vzťahoch, sa pravdepodobne ukáže cennejším v medzinárodnej právnej teórii a praxi v dlhodobom horizonte, než koncept ľudskej bezpečnosti, ktorý nespĺňa tieto podmienky, pretože tieto oblasti práva predstavujú skôr objektivizovanú politickú vôľu štátov, než subjektívnu predpojatosť učencov.

3.4 BEZPEČNOSŤ Z POHĽADU KODANSKEJ ŠKOLY

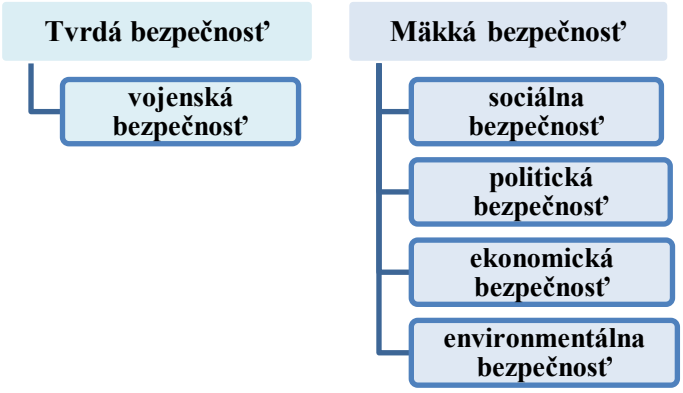
Kodanská škola bezpečnostných štúdií nadviazala na tradíciu teórie medzinárodných vzťahov sociálneho konštruktivizmu. Jej teórie vznikli v rámci **Inštitútu pre výskum mieru v Kodani** a jej zakladateľmi sú **Barry Buzan** a **Ole Waever,** medzi ďalších predstaviteľov školy patria **Jaap deWilde, M. Keltrup a P. Lemaitre.** Ich agenda bola najlepšie objasnená v spoločnom diele: *Bezpečnosť: Nový rámec pre analýzu (1998).*

Základom tejto agendy a hlavným prínosom školy je ***koncept bezpečnostných sektorov, regionálnych bezpečnostných komplexov a sekuritizácie***. Medzi základné pojmy, ktoré priniesla agenda Kodanskej školy možno zaradiť **pojmy:**

- **Bezpečnostní aktéri (referenčné objekty)** – pojem bezpečnosť sa vzťahuje priamo na konkrétny subjekt alebo subjekty, ktoré usilujú o jej dosiahnutie – teda ***aktérov bezpečnosti***. Kodanská škola nazýva týchto aktérov **r e f e r e n č n ý m i o b j e k t m i.** Týmito aktérmi môžu byť *jedinci, skupiny, spoločenstvá, štáty, aliancie, medzinárodné organizácie alebo medzinárodné spoločenstvo.*
- **Sekuritizáciu** je možné považovať za radikálnejšiu formu politizácie. Je to do istej miery subjektívny proces. Buzan pojem vysvetľuje ako „*vyzdvihovanie určitej témy, ktorá tak začína byť chápaná ako existenčná hrozba, žiada si mimoriadne opatrenia a ospravedlňuje konanie vybočujúce zo štandardných mantinelov politických procedúr*“.
- **Aktéri sekuritizácie** – *sú to aktéri, ktorí rozbiehajú proces sekuritizácie tým, že prehlasujú niečo za existenčne ohrozené,* v prípade štátu to môžu byť *vládne elity.*
- **Funkcionálni aktéri** – *sú to aktéri, ktorí urýchľujú bezpečnostnú dynamiku vzťahov.*
- **Bezpečnostné sektory** – *pohľady na medzinárodný systém, ktoré stavajú do popredia jeden konkrétny aspekt vzťahov a interakcií medzi jeho jednotkami (Buzan a kol., 2003).*

Kodanská škola rozdelila bezpečnosť na päť sektorov – *vojenský, ekonomický, politický, sociálny a environmentálny* a vytvorila teoretický nástroj na analýzu bezpečnostnej politiky. Jej predstaviteľom sa podarilo definovať bezpečnosť širšie bez toho, aby popreli úlohu tvrdej bezpečnosti.

Jednou z možností, ako možno nazerať na fenomén bezpečnosti, je z pohľadu jej **dimenzií.** V zásade najjednoduchšie a najčastejšie rozlíšenie je uvedené na obr. 11.



Obr. 11 Dimenzie bezpečnosti

Tvrdá bezpečnosť *(Hard Security)* – do 90. rokov 20. storočia bol hlavným aktérom bezpečnosti predovšetkým „štát“ a bezpečnosť štátu bola považovaná za životný záujem štátu. Takéto chápanie bezpečnosti môžeme označiť ako ***klasické, alebo tradičné, negatívne a užšie chápanie bezpečnosti.*** Bezpečnosť bola spojená výlučne s vojenskými aspektmi a otázkami

medzinárodného práva, bezpečnostná politika bola realizovaná prostredníctvom ozbrojených síl a bezpečnostných zložiek. Patrí sem jeden sektor bezpečnosti: *vojenská bezpečnosť*.

Mäkká bezpečnosť *(Soft Security)* – s pádom bipolarity sa stratila aj bezprostredná hrozba nukleárneho konfliktu, ale čoskoro sa objavilo veľké množstvo nových (staronových) bezpečnostných hrozieb. Do centra záujmu sa dostali asymetrické hrozby, terorizmus, ekonomické, energetické a humanitárne krízy a ekologické katastrofy. Patria sem nasledujúce sektory bezpečnosti: ***sociálna bezpečnosť', politická bezpečnosť', ekonomická bezpečnosť', environmentálna bezpečnosť'***.

3.4.1 Vojenská bezpečnosť

Vojenský sektor je už tradične veľmi úzko spojený s bezpečnosťou. Aj keď po skončení studenej vojny, odstránení bipolarity a zmenách v globálnom bezpečnostnom prostredí sa riziko priameho vojenského ohrozenia vyplývajúceho z celosvetového vojnového konfliktu takmer vytratilo a nevojenské bezpečnostné hrozby postupne prevažujú nad vojenskými, vo vojenskom sektore štát stále zostáva centrálnym bezpečnostným aktérom. Je to totiž práve štát, ktorý si v tomto sektore bezpečnosti nárokuje svoje právo na prežitie, pokiaľ sa cíti ohrozený.

Napriek tomu, že pravdepodobnosť vzniku globálneho vojnového konfliktu je v súčasnosti veľmi nízka a vojenský útok na krajiny NATO alebo EÚ je veľmi nepravdepodobný, naďalej vzniká vo svete množstvo lokálnych a regionálnych konfliktov, ktoré môžu negatívne ovplyvniť vývoj globálneho bezpečnostného prostredia, a preto si vyžadujú, aby štáty naďalej udržiavali svoje ozbrojené sily a používali ich, alebo mali ich pripravené na použitie v prípade ohrozenia štátu a jeho obyvateľov, resp. jeho záujmov.

Postavenie štátu v tomto sektore bezpečnosti bude aj naďalej prvoradé a štát bude aj napriek súčasným tendenciám vždy štát na prvom mieste v zaistení bezpečnosti a obrany svojej nezávislosti, územnej celistvosti, integrity a suverenity, v zaistení bezpečnosti a ochrany svojich občanov, a v neposlednom rade aj svojich záujmov *(Ivančík, 2012)*.

Vonkajšia bezpečnosť štátu má základnú úlohu zabezpečiť samostatne alebo v koalícii štátnu zvrchovanosť a územnú celistvosť SR. Bezpečnosť je tradične zameraná na obranu územnej integrity štátu, na úrovni regionálneho a subregionálneho bezpečnostného prostredia.

V rámci vojenského sektora sú za hlavné bezpečnostné hrozby považované ***vojenské hrozby,*** ostatné hrozby a riziká sú prehliadané, alebo len druhoradé. Aktérmi bezpečnosti v súčasnosti môžu byť:

- štáty ako najdôležitejší referenčný objekt,
- medzinárodné aliancie, regionálne organizácie, prípadne medzinárodné spoločenstvo,
- jednotky v rámci štátu (národy, kmene), náboženstvá, spoločnosť, opozičné skupiny (napríklad separatistické hnutia, povstalci, národy žijúce v diaspóre či organizovaný zločin).

V strednodobom časovom výhľade nie je známa proti SR žiadna bezpečnostná hrozba vojenského charakteru (ozbrojený konflikt akéhokoľvek rozsahu). V dlhodobom časovom výhľade možno predpokladať pretrvávanie starých a vznik nových ohnísk napätia v regiónoch juhovýchodne a východne od SR (Ukrajina, Balkán). Rozhodujúca časť hrozieb bude pochádzať zo vzdialenejšieho bezpečnostného prostredia, predovšetkým vo forme asymetrických hrozieb (najmä terorizmus). Ich odstránenie bude vyžadovať včasné a efektívne použitie síl a prostriedkov SR a jej spojencov vrátane vojenských kapacít a spôsobilostí.

Členstvom v NATO, EÚ a rozložením vojenskej sily vo svete sa SR dostáva do pozície, keď svoje ozbrojené sily používa v rámci koaličných síl. Súčasná vojenská politika SR

vychádza z predpokladu, že armáda nemá ubrániť celú krajinu, ale je skôr budovaná so schopnosťou čiastkového úderu a vojnového nasadenia v rámci koalície.

3.4.2 Sociálna bezpečnosť

Sociálny (spoločenský) sektor bezpečnosti súvisí predovšetkým so ***skupinovou identitou,*** ktorá bola v minulosti výrazne obchádzaná. V tomto sektore taktiež zohráva najdôležitejšiu úlohu štát. Pod identitou spoločnosti chápe spoločenská bezpečnosť identitu osôb, skupiny, etnických skupín a národov, ktoré spoločne tvoria spoločnosť na určitom vymedzenom území. Kľúčom k spoločnosti je súbor ideí a zvyklostí, ktoré identifikujú jednotlivcov ako členov spoločenskej skupiny.

Referenčné objekty sociálneho (spoločenského) sektora tvoria predovšetkým entity a skupiny, ktoré majú spoločného menovateľa – identitu, ktorá sa stáva ohrozenou, môžu to byť:

- národy, národnostné menšiny, etnické skupiny, civilizácia, rasy,
- náboženské systémy,
- región, obec,
- triedna príslušnosť,
- rodinní príslušníci.

Sú to teda akékoľvek malé alebo väčšie skupiny, ktoré sa spolčujú na základe kolektívnej súdržnosti a lojality, ktorú považujú za ohrozenú a hodnú ochrany. Sem môžeme zaraďovať napríklad nielen nacionálne skupiny vo vnútri štátu, ale aj rôzne transnacionálne skupiny naprieč viacerými štátmi ako antiglobalisti, neofašisti alebo environmentalisti za predpokladu, že myslia a konajú ako jedna skupina. Práve spolčovanie na základe nacionálnej identity je pre štát najväčšou hrozbou, pretože môže smerovať k požiadavke sebaurčenia, čo vždy podkopáva územnú integritu štátu, alebo môže dochádzať k podkopávaniu stability štátu prostredníctvom skupín nárokujúcich si nadštandardné výhody (rómske obyvateľstvo).

Z globálneho pohľadu sa za **najväčšie problémy** v tomto sektore považujú:

- polarizácia bohatý Sever a chudobný Juh, spojená s migráciou, chorobami a organizovaným zločinom,
- globalizácia.

Za **hlavné hrozby** sa považuje:

- migrácia (presun obyvateľstva),
- horizontálne súperenie (súperenie medzi minimálne dvoma spoločnosťami – napríklad menšiny v rámci štátov, menšie krajiny sa obávajú kultúrneho vplyvu väčších susedov, stret civilizácií, etnické, náboženské či iné napätie založené na báze rozdielnych identít),
- vertikálne súperenie (problémy týkajúce sa politickej integrácie či fragmentácie),
- nezamestnanosť,
- úbytok obyvateľstva,
- genocída,
- epidémie,
- kriminalita a organizovaný zločin.

3.4.3 Politická bezpečnosť

Základom politickej bezpečnosti je organizačná stabilita spoločenského usporiadania, zameraná na ochranu politických inštitúcií štátu, na ich stabilitu a kontinuitu. Kľúčový význam z bezpečnostného hľadiska má demokratické zriadenie. V politickom sektore je referenčným objektom štát a ide o hrozby, ktoré smerujú proti jeho suverenite, politickému usporia-

daniu a ideologickým základom. Postupne sa referenčnými objektmi stávajú subjekty nadnárodnej povahy (EÚ). Predmetom politickej bezpečnosti je ohrozenie legitimity alebo uznania politických jednotiek, štruktúry, procesov alebo inštitúcií.

Referenčné objekty v tomto sektore sú:
- štát, ako politická organizácia (hlavný aktér),
- nadštátne útvary (OSN, EÚ, NATO),
- spoločenské skupiny so silnými politickými inštitúciami (národnostné menšiny),
- medzinárodné hnutia (cirkvi, ideové politické hnutia), prípadne medzinárodné právo,
- medzinárodné organizácie.

Hrozbami pre politickú bezpečnosť sú:
- existenčné ohrozenie idei, na ktorej politické inštitúcie stoja (hlavná hrozba),
- ohrozenie stability politického poriadku, politickej ideológie, vládnej štruktúry alebo suverenity,
- ohrozenie suverenity štátu zvnútra či zvonka,
- národy alebo národnostné menšiny (Kurdi v Turecku, Albánci v Srbsku, Macedónsku),
- ideológia či náboženstvo,
- nacionalizmus,
- prílišná integrácia, pretože v rámci nej môže byť ohrozená suverenita štátu,
- odmietnutie, spochybnenie, porušenie medzinárodnej zmluvy, alebo spochybňovanie medzinárodného spoločenstva.

Kodanská škola považuje politický sektor zároveň za súčasť každého z ostatných sektorov, pretože proces sekuritizácie prebieha práve prostredníctvom politického rozhodovania. Aj napriek prepojenosti všetkých sektorov a oblastí je možné i v tomto sektore vymedziť základné zdroje ohrozenia, ktoré predstavujú zdroje zraniteľnosti štátu. V tomto sektore bezpečnosti sa stávajú predmetom ohrozenia najmä suverenita, štátna ideológia, politický systém a štátne inštitúcie *(Ivančík, 2012)*.

3.4.4 Ekonomická bezpečnosť

Ekonomický sektor nepredstavuje úplne nový prístup k bezpečnosti, pretože už liberálno-idealistická koncepcia presadzovala ekonomické nástroje ako jedny z najdôležitejších nástrojov ovplyvňovania bezpečnosti a blahobytu obyvateľstva štátov. Stabilné národné hospodárstvo, fungujúce výrobné, obchodné a finančné vzťahy, fungujúca a výkonná národná ekonomika sú dôležitými faktormi rozvoja štátu, ktoré výrazne ovplyvňujú i bezpečnosť štátu.

Súčasná integrácia štátov do nadnárodných ekonomických zoskupení predstavuje budovanie kooperácie štátov založené na ekonomickom princípe. Na druhej strane však prináša i bezpečnostné záruky a stabilizáciu, pretože krajiny, ktoré spolupracujú v ekonomickej oblasti, majú za cieľ túto spoluprácu prehlbovať a nie ju rôznymi spormi alebo konfliktami podkopávať, pretože ich základným zámerom je vytvorenie stability a prosperity. Zároveň je ich cieľom dosiahnuť takú úroveň ekonomickej bezpečnosti, pri ktorej sú v rámci ekonomických vzťahov uspokojované potreby jednotlivcov aj spoločnosti.

Ekonomická bezpečnosť *(Economic Security)* predstavuje stav, v ktorom ekonomika objektu, ktorého bezpečnosť má byť zaistená (štátu, aliancie štátov, podniku, podnikateľských subjektov ap.), nie je vystavená rizikám a ohrozeniam, ktoré by mohli výrazne znížiť (alebo už znižujú) jej výkonnosť, potrebnú na plnenie základných funkcií a dosahovanie cieľov.

Hlavnými atribútmi ekonomickej bezpečnosti sú:
- diverzifikácia a zaistenie stabilných dodávok energetických a prírodných zdrojov,

- prístup k finančným zdrojom a investíciám, menová a finančná stabilita,
- prístup na svetové trhy, stabilita finančných trhov,
- rozvinutá infraštruktúra,
- kvalifikované ľudské zdroje,
- integrácia do regionálnych i svetových ekonomických a hospodárskych štruktúr,
- konkurencieschopnosť a výkonnosť, ktorá je nevyhnutná na zaistenie bezpečnostných kapacít a sociálnej súdržnosti,
- prevencia kríz globálneho rozsahu.

Medzi **hlavných aktérov** ekonomickej bezpečnosti patria:

- jednotlivci,
- štáty (národné hospodárstva),
- firmy, nadnárodné monopoly,
- medzivládne organizácie (WTO, NAFTA, EÚ, WB),
- trh, finančný systém, banky.

Hrozbami pre ekonomickú bezpečnosť sú:

- systémové krízy, ktoré môžu ohroziť celý medzinárodný ekonomický systém,
- pre národné hospodárstvo zánik veľkých podnikov, strata konkurencieschopnosti v medzinárodnom prostredí, štrajky,
- blokáda (napr. Kuba, Irán, KĽDR),
- sankcie (napr. Rusko v súčasnosti),
- nedostatok energetických zdrojov,
- pre jednotlivcov naplnenie základných ľudských potrieb (dostatok potravy, pitnej vody, obydlie).

3.4.5 Environmentálna bezpečnosť

Environmentálny sektor v minulosti nebol priamou súčasťou klasických bezpečnostných prístupov. Environmentálna agenda bezpečnosti sa dostala do užšieho záujmu až prijatím Deklarácie OSN o životnom prostredí na Konferencii OSN o životnom prostredí v Štokholme v roku 1972, ktorá znamenala prelom v chápaní vplyvu životného prostredia na bezpečnosť. Práve táto konferencia vyčlenila globálne environmentálne problémy a prostredníctvom regiónov i pre nich vyplývajúce ohrozenia, ktoré boli transformované ako priority do Environmentálneho programu OSN. Posledné výskumy v oblasti bezpečnosti dokazujú, že bezpečnosť a stabilita environmentálneho prostredia sú predovšetkým otázkou nadnárodnej kooperácie, pretože sú dôležitými aspektmi mieru, bezpečnosti štátov a stability spoločnosti.

Environmentálna bezpečnosť *(Environmental Security)* predstavuje bezpečnosť životného prostredia ako stav, v ktorom ľudská spoločnosť a ekologický systém na seba pôsobia trvalo udržateľným spôsobom, jednotlivci majú dostatočný prístup ku všetkým prírodným zdrojom a existujú mechanizmy na zvládanie kríz a konfliktov priamo či nepriamo spojených so životným prostredím.

V tomto stave sú minimalizované riziká a ohrozenia spojené so životným prostredím a spôsobené prírodnými alebo antropologickými silami alebo procesmi vyvolanými antropologickými silami.

Aktérom bezpečnosti v tomto sektore je predovšetkým životné prostredie, zachovanie biosféry a ekosystémov.

Referenčnými objektmi môžu byť:

- štáty ohrozené nedostatkom zdrojov, rozširovaním púšte, nárastom hladiny oceánov,
- rôzne spoločenstvá,
- jedinci.

Hrozby v tomto sektore sa dajú zaradiť do troch skupín:

- prírodné hrozby,
- hrozby zapríčinené ľudskou činnosťou, ktoré možno považovať za existenčné hrozby,
- hrozby, ktoré nie sú existenčným ohrozením ľudstva.

Sú to teda hrozby ako prírodné katastrofy (zemetrasenia, vlny cunami, sopky), degradácia životného prostredia, globálne otepľovanie, nedostatok energetických alebo prírodných zdrojov. Z hľadiska antropocentrického poňatia je preto legitímne, že hrozby z degradácie životného prostredia sa môžu ľahko premeniť na hrozby klasické: vojny, násilie, rozvrat. SR môžu ohrozovať predovšetkým klimatické zmeny a výrazne narušený hydrologický režim (nedostatok vody).

Počas niekoľkých nasledujúcich desaťročí nastane úbytok pôdy, vyčerpávanie prírodných nerastných surovín ako ropa, uhlie a zemný plyn, ktoré budú využívané predovšetkým na uspokojenie rastúcej spotreby ľudstva. Samozrejme dostatok potravín, ale aj čistý vzduch a najmä pitná voda budú suroviny, ktoré budú na základe prognóz demografického vývoja ľudstva v nasledujúcich rokoch čoraz vzácnejšie, a preto môžu spôsobiť problémy zásadného charakteru z hľadiska bezpečnosti.

Tieto problémy budú testovať tradičné chápanie hraníc, štátnej bezpečnosti, pretože miestny lokálny konflikt o prírodné zdroje môže prerásť do regionálneho alebo až globálneho boja o vlastníctvo nedostatkových zdrojov. Najväčšie problémy spojené s environmentálnym prostredím predstavujú environmentálna degradácia, predovšetkým prílišné vyčerpávanie prírodných zdrojov a s ním súvisiace poškodzovanie životného prostredia a environmentálny nedostatok.

3.4.6 Ďalšie sektory bezpečnosti

Pretože súčasné vývojové tendencie ukazujú potrebu rozšírenia sektorov bezpečnosti, je možné k vyššie uvedeným doplniť aj ďalšie dva sektory, ktoré je možné dnes považovať za rovnocenné, a to sektory: ***informačný, energetický.*** Okrem vyššie uvedených sektorov, je vzhľadom na aktuálny vývoj vo svete, ako aj akademické a politické diskusie, možné uvažovať aj o ďalších sektoroch bezpečnosti, napríklad ***technologickom*** **a** ***infraštruktúrnom sektore bezpečnosti,*** týkajúcom sa najmä zaistenia bezpečnosti kritickej infraštruktúry, alebo ***kultúrnom sektore bezpečnosti*** (zatiaľ najmenej zmapovanom), týkajúcom sa zaistenia bezpečnosti v prípade problémov a napätia vyplývajúceho z dotyku rôznych a/alebo rozdielnych kultúr *(Ivančík, 2012)*.

Informačný sektor bezpečnosti

Informačný sektor je jedným z najdynamickejšie sa rozvíjajúcich sektorov spoločnosti za posledných desať rokov. Klasické bezpečnostné prístupy sa týmto smerom nikdy neuberali a do popredia záujmu sa informačný sektor dostal až začiatkom 90. rokov 20. storočia. Rozvoj internetu a moderných počítačových, komunikačných a informačných technológií sa premietol nielen do oblasti súkromnej a ekonomickej sféry, ale čoraz viac zasahuje aj do štátnej a verejnej správy štátu, a tiež do oblastí vojenstva a bezpečnosti.

Informačné technológie sa svojim širokým spektrom využitia dostali skoro do všetkých oblastí spoločenského života. Možnosti narušenia tohto priestoru neustále narastajú

a predstavujú potenciálne hrozby, s ktorými sa musia vyrovnať takmer všetky subjekty v spoločnosti. Narušenie tejto bezpečnosti môže prebiehať na viacerých úrovniach, od odpočúvania a rušenia signálov telekomunikačných a informačných sietí, až sabotáže informačných tokov, či dokonca kyberterorizmus a iné.

V informačnom sektore bezpečnosti úloha štátu spočíva najmä vo vytvorení inštitucionálneho rámca, ktorý podporuje ochranu a bezpečnosť informácií šírených prostredníctvom komunikačných a informačných sietí. Štát však nemôže byť zodpovedný za ľahkomyseľné a nerozvážne využívanie týchto sústav jednotlivcami alebo firmami, aj keď jeho cieľom by mala byť minimalizácia zneužitia šírených údajov alebo šírenia nelegálnych údajov.

Energetický sektor bezpečnosti

Energetický sektor bezpečnosti je jednou z najdôležitejších oblastí, bez ktorých by štát nedokázal plniť svoje základné funkcie. Predstavuje rovnovážny stav v štáte, kedy je zabezpečený prístup k energetickým zdrojom. Túto oblasť Kodanská škola zaraďovala do ekonomického sektora bezpečnosti, avšak vývojové tendencie vo svete dokazujú jeho opodstatnenie a zvyšovanie jeho významu do budúcnosti.

Energetická bezpečnosť ako samostatný sektor má opodstatnenie aj z toho dôvodu, že je významným indikátorom vzájomnej závislosti štátov, a teda aj vzťahov medzi nimi, ktoré sa môžu v krátkom časovom období výrazne meniť.

Hlavnými zdrojmi ohrozenia v tomto sektore bezpečnosti sú predovšetkým vyčerpateľnosť zdrojov (surovinová bezpečnosť), politická nestabilita a manipulácia, útoky na zdroje a infraštruktúru, priemyselné nehody alebo prírodné katastrofy, rast cien energií, alebo odstavenie dodávok energií. Energetická bezpečnosť by preto mala byť jednou z priorít každého štátu, pričom by mala byť založená na efektívnom zásobovaní energetickými surovinami, ktoré zabezpečujú rozvoj spoločnosti, a zabezpečení diverzifikácie energetických dodávok v rámci predchádzania rôznym výpadkom.

3.5 LITERATÚRA

ACHARYA, A. [1999]: *Reordering Asia: „Cooperative Security or Concept of Powers?“ (Znovuusporiadanie Ázie: Kooperatívna bezpečnosť alebo koncepcia sily?)*

ALKIRE, S. [2003]: *Koncepčný rámec pre ľudskú bezpečnosť*, Centrum pre výskum nerovnosti, ľudskej bezpečnosti, a etnicity, pracovný dokument 2. Londýn:. University of Oxford

AYOOB, M. [1995]: *The Third World Security Predicament: State Making, Regional Conflict and the International System.(Dilema bezpečnosti tretieho sveta: Vývoj štátov, regionálny konflikt, a medzinárodný systém).* In: Boulder, CO: Lynne Rienner Publishers

BUZAN, B. – WAEVER, O. – DE WILDE, J. [1998]: *Security: A New Framework for Analysis.* Boulder CO: Lynne Rienner Publishers

BUZAN, B. – WAEVER, O. – DE WILDE, J. [2005]: *Bezpečnost: Nový rámec pro analýzu.* 1. vyd. Brno: UO, Centrum strategických studií, Současná teorie mezinárodních vztahů. ISBN 80-903333-6-2

HOFREITER, L. [2006]: *Perspektívy bezpečnostného manažmentu v globálnom prostredí.* In: Security Revue. Žilina: Elektronický časopis FŠI ŽU Žilina, 5.12.2006

HOFREITER, L. – ŠIMKO, J. [2007]: *Zdroje a oblasti konfliktov v súčasnom svete.* Liptovský Mikuláš: Akadémia ozbrojených síl. ISBN 978-80-8040-330-0

HUMAN SECURITY CENTRE [2008]: „*Čo je ľudská bezpečnosť*“. 19. apríla 2008 http://www.humansecurityreport.info

IVANČÍK R. [2012]: *Teoreticko-metodologický pohľad na bezpečnosť.* In: Krízový manažment 1/2012, Žilina: FŠI ŽU Žilina,

KING, G. – MURRAY Ch.: *Prehodnotenie Human Security.* Political Science Quarterly, Vol.116, č.4 s. 585-610

KRAUS, K. – WILLIAMS, C. M.[1997]: *Critical Security Studies: Concept and Causes.* Minneapolis: University of Minnesota Press

KUSTROVÁ,M. [2013]: *Základné atribúty potravinovej bezpečnosti*. In: Krízový manažment, vedecko-odborný časopis FŠI ŽU v Žiline, ročník 12, č. 1/2013. ISSN 1336-0019.

LIPPMANN, W. [1943]: *Zahraničná politika USA.* Boston

MACFARLANE, S. N. – FOONG K.Y. [2006]: *Human Security and the UN:* A Critical History. Indiana: Indiana University Press

MADER, M. [2012]: *Úzus tvrdej a mäkkej bezpečnosti (prípadová štúdia Balkán) I.* In: Project ARES, Štúrovo, Banská Bystrica, 3.1.2012, www.projectares.sk

MESJASZ, C. [2006]: *Komplexné štúdie systémov a konceptov bezpečnosti,* Krakovská ekonomická univerzita, Krakov.

PARIS, R. [2001]: *Ľudská bezpečnosť*: *Zmena paradigmy alebo táranie?* Medzinárodná bezpečnosť. 26.2.2001 str. 87-102.

PITSUWAN, S. [2007]: *Regionálna spolupráca pre ľudské bezpečnosti.* Príhovor k Medzinárodnej konferencii o ľudskej bezpečnosti: Október 2007.

PROGRAM OSN PRE ROZVOJ [1994]: *Správa o ľudskom rozvoji*

ROLAND, P. [2001]: *„Ľudská bezpečnosť: Zmena paradigmy alebo táranie?“* Medzinárodná bezpečnosť. 26.2.2001 str. 87-102.

SUNGA, L. S. [2009]: *„Koncepcia ľudskej bezpečnosti: Pridávať čokoľvek hodnotné k medzinárodným právnym teóriám alebo praxi?“* (editoval Marie-Luisa Frick a Andreas Oberprantacher) Ashgate Publishers

ŠKVRNDA F. [2005]: *Vybrané sociologické otázky charakteristiky bezpečnosti v súčasnom svete.* In: ČUKAN K. a kol.: *Mládež a armáda.* Bratislava: MO SR.

TADJBAKHSH, S. [2007]: *Ľudská bezpečnosť v medzinárodných organizáciách: požehnanie alebo pohroma.* Human Security Journal, Volume 4,

THOMAS, C. [2000]: *Globálne vládnutie, rozvoj a ľudská bezpečnosť - výzva chudoby a nerovnosti.* Londýn a Sterling, VA:. Pluto Press

UL HAQ, M. [1994]: *Správa o ľudskom rozvoji* (v rámci Rozvojového programu OSN)

Ústavný zákon 227/2002 Z. z. o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu.

VOLNER, Š. [2012]: *Bezpečnosť, riziká a hrozby v 21. storočí.* 3. dopl. vyd. - Bratislava : Iris, 2012. - 387 s., ISBN 978-80-89256-74-7.

4 REFERENČNÝ OBJEKT A AKTÍVA

Po skončení studenej vojny sa začína presadzovať poňatie bezpečnosti, ktoré rozširuje škálu bezpečnostných javov v týchto aspektoch:

- **Subjekty bezpečnosti** – (referenčné objekty bezpečnosti, aktéri bezpečnosti).
- **Sektory alebo dimenzie bezpečnosti** – oblasti v ktorých vznikajú bezpečnostné problémy.
- **Intenzita alebo prah bezpečnosti** – odkedy sa z nejakého problému či hrozby stáva problém, resp. hrozba špecificky bezpečnostná. Prechádza sa od tradične vnímanej bezpečnosti – tvrdej bezpečnosti (hard security), v ktorej ide o prežitie, moc a silové prostriedky, ku konceptu mäkkej bezpečnosti (soft security). V rámci soft security sa študujú uspokojivé životné podmienky, vyhovujúce životné prostredie, ochrana ľudských práv.

Subjekt bezpečnosti, niektorými opisovaný ako nositeľ, nosič, subjekt, objekt je subjektom situácie, ktorý poznáva následky ohrozenia, prijíma stimuly a reaguje. V politických vedách namiesto subjektu bezpečnosti sa používa termín ***objekt*** (vzťažný objekt), pod ktorým sa myslí štát, sociálne skupiny alebo jednotlivci *(Korzeniowski, 2013)*.

V securitológii sa tiež používa termín **objekt**, aj keď je to nejednoznačný termín a označuje ľubovoľný systém vrátane planéty, štátu, spoločnosti, skupiny, živých organizmov, častí prírodného prostredia, jednoducho všetko, čo je nevyhnutne potrebné na zaistenie ľudského života a čo môže pôsobiť proti ohrozeniam rôzneho charakteru.

Subjektívna bezpečnosť (bezpečnosť objektu) je stav subjektu (objektu), jeho potenciál a možnosti adekvátnej reakcie na hrozby, téma ochrany pred ohrozeniami.

Podľa Kodanskej školy sa pojem **bezpečnosť** tiež 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.***

Referenčným objektom bezpečnosti môže byť: ***medzinárodný systém, medzinárodné organizácie a aliancie, štát, subštátny systém*** *(územné a správne jednotky štátu),* ***nehmotné entity*** *(ľudské práva, princíp demokracie, informácie),* ***sociálna skupina*** *(národ, národnostná menšina, ženy),* ***jedinci****.*

- **vo vojenskom sektore** najdôležitejším referenčným objektom (objektom skúmania) boli a sú *štáty,* ďalej *medzinárodné aliancie, regionálne organizácie,* prípadne *medzinárodné spoločenstvo*, *jednotky v rámci štátu (národy, kmene), náboženstvá, spoločnosť, opozičné skupiny (napr. separatistické hnutia, povstalci, národy žijúce v diaspóre či organizovaný zločin).*
- **v sociálnom sektore** referenčné objekty predstavujú *národy, národnostné menšiny, etnické skupiny, civilizácia, náboženské systémy a rasy.*
- **v politickom sektore** sú referenčnými objektmi *štát ako politická organizácia, nadštátne útvary (EÚ, OSN, NATO), spoločenské skupiny so silnými politickými inštitúciami (národ-*

nostné menšiny), medzinárodné hnutia (cirkvi, ideové politické hnutia), prípadne medzinárodné právo, medzinárodné organizácie.

- **v ekonomickom sektore** sú referenčnými objektmi *jednotlivci, štáty (národné hospodárstva), podniky, spoločnosti, nadnárodné monopoly, banky, medzivládne organizácie (WTO, NAFTA, EÚ, WB), trh či finančný systém.*
- **v environmentálnom sektore** sú referenčnými objektmi *ľudstvo, životné prostredie, zachovanie biosféry a ekosystémov.*

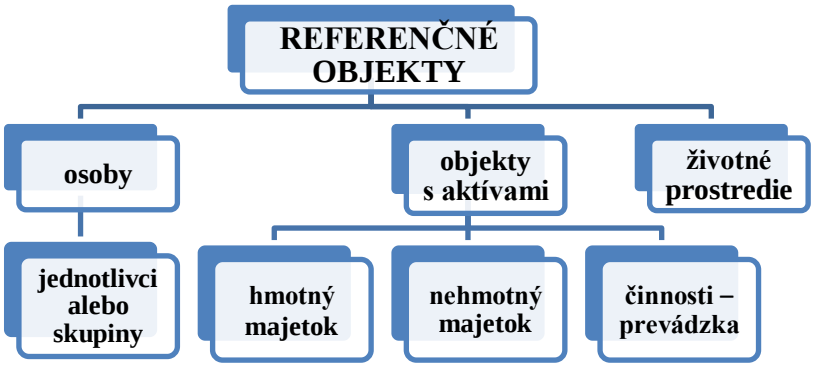
Model Kodanskej bezpečnostnej školy priniesol takúto typológiu referenčných objektov:

- **Globálne medzinárodné systémy** – najširšie konglomeráty vzájomne závislých aktérov a ich vzťahov, napr.: OSN, Globálny ekonomický systém, ekosystém.
- **Medzinárodné subsystémy** – zoskupenie jednotiek, ktoré sa intenzitou väzieb líšia od okolia. Obyčajne sú teritoriálne definované. napr.: NATO, Africká únia.
- **Jednotky** – tradične predovšetkým štáty, ale dnes aj silné nadnárodné korporácie a nevládne organizácie, ich činnosť je takmer nezávislá od moci jednotlivých štátov.
- **Podjednotky –** organizované skupiny vo vnútri jednotiek, záujmové skupiny, formalizované siete, politické strany.
- **Jednotlivci.**

4.1 REFERENČNÝ OBJEKT V BEZPEČNOSTNOM MANAŽMENTE

Referenčné objekty je možné z hľadiska bezpečnostného manažmentu posudzovať z viacerých hľadísk, napr.:

1. **Z hľadiska druhu ohrozených subjektov** (obr. 12):
   - **a) osoby** – jednotlivci alebo skupiny (človek, malá skupina, spoločnosti, ľudstvo),
   - **b) objekty s aktívami**, ktoré obsahujú:
     - hmotný a nehmotný ***majetok***,
     - ***činnosti*** na vytváranie určitých produktov alebo poskytovanie služieb (prevádzka),
   - **c) životné prostredie.**



Obr. 12 Referenčné objekty z hľadiska druhu ohrozených subjektov

2. **Z organizačného hľadiska ohrozených subjektov:**
   a) štátne orgány a organizácie,
   b) jednotky územnej samosprávy – vyššie územné celky, mesto, obec,
   c) výrobné podniky,
   d) nevýrobné podniky poskytujúce služby,
   e) ďalšie organizácie poskytujúce služby,
   f) dobrovoľné ziskové a neziskové organizácie.
3. **Z hľadiska právneho ide o právnické osoby:**
   a) združenia fyzických alebo právnických osôb,
      - občianske združenia, spolky, spoločnosti, zväzy, hnutia a kluby,
      - politické strany a hnutia,
      - cirkvi a náboženské spoločnosti a nimi založené komunity,
      - združenia, ktoré sú zriadené priamo osobitným zákonom,
      - verejnoprospešné organizácie,

   b) účelové združenia majetku – nadácie a štátne fondy,
   c) jednotky územnej samosprávy,
   d) iné subjekty, o ktorých to ustanovuje zákon, napr. Rozhlas a televízia Slovenska.

4.1.1 Osoby ako referenčný objekt

Bezpečnosť jednotlivca (individuálne ohrozenie) spočíva v chýbajúcom ohrození jednotlivej osoby, avšak **bezpečnosť skupinová** sa týka dvoch a viacerých osôb. V trestnom práve ***individuálne ohrozenie*** spočíva vo vystavení riziku jednotlivca alebo menšieho počtu osôb, naopak ***všeobecné ohrozenie*** spočíva v úmyselnom vystavení ľudí nebezpečenstvu smr-

ti alebo ťažkej ujmy na zdraví alebo cudzieho majetku nebezpečenstvu škody veľkého rozsahu.

Všeobecné ohrozenie podľa Trestného zákona spočíva v:

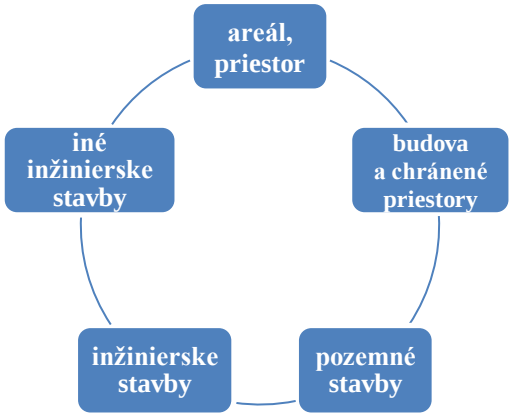
- spôsobení požiaru, povodne, alebo poruchy či havárie prostriedku hromadnej prepravy,
- zavinení škodlivých účinkov výbušnín, plynu, elektriny, rádioaktivity alebo iných podobne nebezpečných látok alebo síl,
- inom podobnom nebezpečnom konaní (všeobecné nebezpečenstvo),
- zvýšení všeobecného nebezpečenstva alebo sťažení jeho odvrátenia alebo zmiernenia.

Všeobecné nebezpečenstvo podľa uvedeného zákona predstavuje:

- poškodzovanie a ohrozovanie prevádzky všeobecne prospešného zariadenia,
- ohrozenie pod vplyvom návykovej látky,
- porušovanie povinnosti pri hrozivej tiesni,
- porušovanie povinností a vyhýbanie sa výkonu povinností za krízovej situácie,
- ohrozenie bezpečnosti vzdušného dopravného prostriedku a lode,
- zavlečenie vzdušného dopravného prostriedku do cudziny,
- nedovolené ozbrojovanie a obchodovanie so zbraňami,
- založenie, zosnovanie a podporovanie zločineckej skupiny alebo teroristickej skupiny,
- nedovolená výroba a držanie jadrových materiálov, rádioaktívnych látok, vysoko rizikových chemických látok a vysoko rizikových biologických agensov a toxínov.

4.1.2 Objekty ako referenčný objekt

Pojem objekt má niekoľko významov, v prvom rade ako **predmet vnímania, myslenia, poznávania,** na druhej strane ako **zariadenie slúžiace nejakému cieľu**. Z druhého hľadiska môže **objekt** predstavovať (obr. 13):



Obr. 13 Objekty

Komplex zariadení slúžiaci istému cieľu, vymedzená časť územia, pozemky so stavbami (areál), výrobná alebo hospodárska jednotka:

- **priestory** *(Premises)*, **areál,** ktorý stavebne a obvykle aj z hľadiska účelu a vlastníckych vzťahov tvorí jeden funkčný celok, zvyčajne zahŕňa viacero budov a priestor medzi nimi, väčšinou býva areál uzavretý (ohradený) a prístup ľudí a vozidiel je možný cez jeden či viac vchodov (východov) či vjazdov, niekedy vybavených aj vrátnicou.

Budova alebo iný stavebne alebo inak ohraničený priestor, v ktorom sa nachádzajú chránené priestory: podľa Zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností **chráneným priestorom** sa rozumie *stavebne alebo inak ohraničený priestor vo vnútri*

objektu, ktorý je určený na ukladanie a manipuláciu s utajovanými skutočnosťami, zodpovedajúci príslušnému stupňu utajenia.

Pozemné stavby *(Zákon č. 50/1976 Zb. o územnom plánovaní a stavebnom poriadku, Stavebný zákon)* – priestorovo sústredené zastrešené budovy vrátane podzemných priestorov, ktoré sú stavebnotechnicky vhodné a určené na ochranu ľudí, zvierat alebo vecí; nemusia mať steny, ale musia mať strechu, podľa účelu sa členia na:

a) bytové budovy: rodinné domy, bytové domy, ďalšie budovy na bývanie, napríklad detské domovy, študentské domovy, domovy dôchodcov a útulky pre bezdomovcov,

b) nebytové budovy:

- hotely, motely, penzióny a ostatné ubytovacie zariadenia na krátkodobé pobyty,
- budovy pre administratívu, správu a na riadenie, pre banky a pošty,
- budovy pre obchod a služby vrátane autoservisov a čerpacích staníc,
- dopravné a telekomunikačné budovy, stanice, hangáre, depá, garáže a kryté parkoviská,
- priemyselné budovy a sklady, nádrže a silá,
- budovy pre kultúru a na verejnú zábavu, pre múzeá, knižnice a galérie,
- budovy pre školstvo, na vzdelávanie a výskum,
- nemocnice, zdravotnícke a sociálne zariadenia,
- kryté budovy pre šport,
- poľnohospodárske budovy a sklady, stajne a maštale,
- budovy a miesta na vykonávanie náboženských aktivít, krematóriá a cintoríny,
- kultúrne pamiatky, ktoré nie sú bytovými budovami,
- ostatné nebytové budovy, napríklad nápravné zariadenia alebo kasárne.

Inžinierske stavby *(Stavebný zákon)* sú:

a) diaľnice, cesty, miestne a účelové komunikácie, nábrežia, chodníky a nekryté parkoviská,
b) železničné, lanové a iné dráhy,
c) vzletové dráhy, pristávacie dráhy a rolovacie dráhy letísk,
d) mosty, nadjazdy, tunely, nadchody a podchody,
e) prístavy, plavebné kanály a komory, úpravy tokov, priehrady a ochranné hrádze, závlahové a melioračné sústavy, rybníky,
f) diaľkové ropovody a plynovody, miestne rozvody plynu,
g) diaľkové a miestne rozvody vody alebo pary, úpravne vody, miestne kanalizácie a čistiarne odpadových vôd,
h) diaľkové a miestne elektronické komunikačné siete a vedenia, telekomunikačné stožiare, transformačné stanice,
i) diaľkové a miestne rozvody elektriny, stožiare, transformačné stanice, televízne káblové rozvody,
j) banské stavby a ťažobné zariadenia,
k) stavby energetických zariadení, plynárne a spaľovne odpadu,
l) stavby na spracovanie a ukladanie jadrového materiálu a rádioaktívneho odpadu,
m) stavby chemických zariadení, rafinérie a koksovne,
n) stavby ťažkého priemyslu, napríklad vysoké pece, valcovne a zlievarne,
o) nekryté športové ihriská, automobilové, motocyklové a bicyklové dráhy, golfové ihriská, lyžiarske trate a vleky,
p) zábavné a oddychové parky, zoologické a botanické záhrady.

Ostatné inžinierske stavby, napríklad skládky odpadu *(Stavebný zákon)*.

4.1.3 Organizácia ako referenčný objekt

Organizácia predstavuje:

- ***združenie (zoskupenie, spolok) osôb alebo inštitúcií majúcich spoločný cieľ, program, spoločné záujmy*** a pod.;
- ***zložka takéhoto združenia:*** *občianske, hospodárske, neziskové, kultúrne, politické, humanitárne, náboženské, športové, medzinárodné, mimovládne, mládežnícke, právnické, vedecké, stavovské, vojenské, zdravotnícke, záujmové organizácie a iné organizácie, spolky a agentúry.*

Okrem štátu a územných a správnych jednotiek verejnej správy možno medzi referenčné objekty z organizačného hľadiska zaradiť aj nasledujúce organizácie:

1. **Výrobné podniky:**
   - **ťažobné:** nerasty – uhlie, ropa, železná ruda, kameň, štrk, piesok, štrkopiesok, priemyselné suroviny,
   - **lesné:** drevo – ťažba a spracovanie dreva, lesníctvo, píly, drevoobrábacie stroje a zariadenia,
   - **poľnohospodárske:** pestovanie potravín a krmovín, ovocinárstvo, živočíšna výroba,
   - **energetické**: energetika, plyn, teplo,
   - **telekomunikačné**: pošta, internet, telefón,
   - **spracovateľské vyrábajúce výrobné prostriedky:** strojárske, elektrotechnické, chemické, textilné, priemyselná technika, zariadenia, diely atď.,
   - **spracovateľské vyrábajúce spotrebné predmety**: obuv, odev, nábytok,
   - **stavebné** – realizujú stavby budov, ciest, železníc, letísk atď.
2. **Nevýrobné podniky poskytujúce služby:**
   - **obchodné a sprostredkovateľské**: nákup a predaj tovarov – obchody, supermarkety, holdingy, trhy,
   - **finančné (finančný sektor):** banky, poisťovne, zmenárne – vedenie účtov, poskytovanie úverov, pôžičiek,
   - **dopravné, prepravné a transportné** – preprava tovaru a osôb,
   - **skladovacie**: sklady,
   - **informačné a komunikačné služby a priemysel,**
   - **stravovacie a ubytovacie:** predaj jedál, ubytovanie, rekreačné strediská, hotely,
   - **cestovného ruchu:** cestovné kancelárie – organizovanie zájazdov, dovoleniek,
   - **remeslá a opravy atď.**
3. **Ďalšie organizácie sektora služieb:**
   - **vzdelávacie a vedeckovýskumné:** školy, univerzity, akadémie, výskumné ústavy, knižnice,
   - **zábava, kultúra a šport:** múzeá, kiná, kongresové centrá, pamätníky, cintoríny, vydavateľstvá, športové strediská, štadióny, kúpaliská,
   - **médiá, informácie a propagácia,**
   - **zdravotnícke a sociálnej starostlivosti:** polikliniky, nemocnice, rehabilitačné strediská, kúpele,
   - **poradenstvo, právne a odborné služby:** súdy, právne poradne, väznice, nápravné ústavy,
   - **verejná správa, politické a náboženské** organizácie: úrady, kostoly, katedrály a pod.

4.1.4 Príklad referenčného objektu

Objekty, medzi ktoré patria priestory organizácií, budovy s chránenými priestormi, bytové a nebytové budovy a inžinierske stavby predstavujú samy osebe určité hodnoty, aktíva, majetok, ktorý je potrebné chrániť. Vo väčšine objektov sú umiestnené ďalšie aktíva (majetok), ktoré pre vlastníka často predstavujú významnú hodnotu a je tiež potrebné ich chrániť. Priestory v objektoch, kde sú tieto ďalšie aktíva uložené sa označujú ako ***chránené priestory***.

Usporiadanie objektov a chránených priestorov je uvedené v nasledujúcom príklade, kde sú v referenčnom objekte, ktorý predstavuje **priestor** (objekt) **výrobného podniku** XY umiestnené **samostatné objekty s chránenými priestormi** (tab. 9).

Tab. 9 Objekty a chránené priestory

Priestor, areál	Objekt	Chránené priestory
priestor (objekt) výrobného podniku	oplotenie	vchody a vjazdy pre osoby, vozidlá a vlakové súpravy; a i.;
	technické zariadenia budov	kanalizácia, vodovod, plynovod, vykurovanie; a i.;
	administratívna budova	kancelárie vrcholových manažérov; tajná spisovňa; učtáreň; trezorová miestnosť; miestnosť so serverom; recepcia, a i.;
	výrobná hala	výrobné linky; sklady nebezpečných látok; sklady náhradných dielov; šatne; a i.;
	skúšobná hala	testovacie miestnosti; a i.;
	sklad vyrobeného tovaru	kancelária s výpočtovou technikou; a i.;
	sklad zásob	nakladacie a vykladacie rampy; sklady nebezpečných látok; a i.
	garáže	boxy pre vozidlá; sklad a čerpadlá PHM; dielne na opravovanie; a i.

Je samozrejmé, že v priestoroch (objektoch) rôznych organizácií sa podľa ich účelu budú nachádzať aj rôzne samostatné objekty so špecifickými chránenými priestormi, v ktorých budú uložené rôzne druhy aktív. Rozdielne objekty a chránené priestory budú v jednotlivých výrobných podnikoch, ale aj v nevýrobných podnikoch poskytujúcich služby, napr. poľnohospodárske podniky a banky. Úplne odlišné budú aj objekty a chránené priestory v jednotlivých organizáciách sektora služieb, ktoré majú podľa svojho účelu veľmi rozdielne zameranie, napr. univerzity a nemocnice.

Podstatné však je, aby vrcholový manažment poznal, kde a aké významné aktíva má vo svojich objektoch umiestnené a ako má zaistenú ich bezpečnosť.

4.2 AKTÍVA

„Najväčší dar je vedieť posúdiť hodnotu vecí“ (François de La Rochefoucauld).

Aktíva *(Assets)* sú podľa ISO 55000:2014 Asset management. Overview, principles and terminology definované ako „***položka, vec alebo osoba, ktorá má potenciálnu alebo skutočnú hodnotu pre organizáciu***“**,** preto sú pre organizáciu **hodnotami**, ktoré treba chrániť. Je to pojem, ktorý označuje ***majetok organizácie či hospodárske prostriedky.***

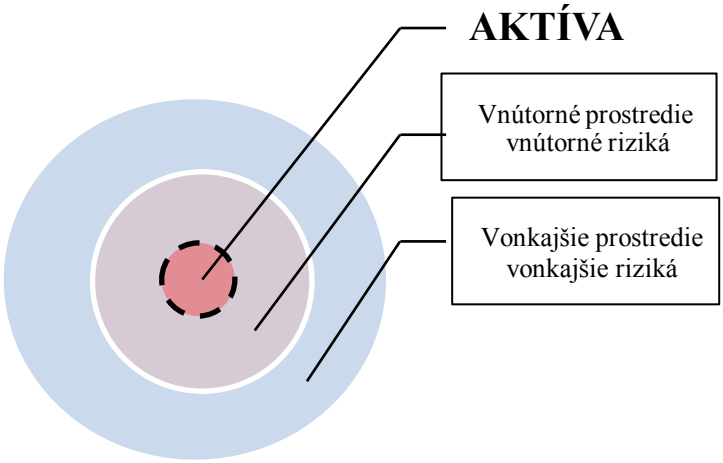
Pod pojmom **majetok** rozumieme ***súhrn všetkých vecí, ktoré niekomu patria***, napr. peňazí, pohľadávok a iných majetkových hodnôt, ktoré patria podnikateľovi a sú určené na podnikanie. Z účtovníckeho hľadiska aktíva predstavujú pre organizáciu ekonomické prostriedky, ktoré sú výsledkom minulých udalostí a od ktorých sa očakáva, že v budúcnosti povedú k zvýšeniu ekonomických úžitkov, predstavujú príležitosti, z ktorých sa pri vhodnom využití dosahuje určitý zisk.

Aktívom organizácie sa rozumie ***objekt, subjekt, služba, štruktúra, vzťah alebo proces,*** ktorého narušením môže organizácia utrpieť stratu. Hodnota aktív sa bude medzi rôznymi organizáciami a ich partnermi v podnikaní líšiť, môže byť hmotná alebo nehmotná, finančná alebo nefinančná.

Aktíva organizácie sú spravidla aj **chráneným záujmom**, musia byť chránené najmä pred úmyselným napadnutím, napr. odcudzením, poškodením, zničením, krádežou informácií a pod. alebo pred iným spôsobom narušenia, napr. živelnou pohromou, požiarom, haváriou.

Každá organizácia, ktorá chce dosiahnuť alebo zvýšiť určitú úroveň bezpečnosti svojich aktív, si musí v rámci bezpečnostnej politiky a bezpečnostných cieľov utvoriť adekvátny názor na ich správu, zhodnotiť ich význam a zaujať postoj pre ich ochranu pred rôznymi druhmi nebezpečenstva, ktoré môžu spôsobiť nežiaduce udalosti – ohrozenia. Tieto negatívne udalosti predstavujú pre organizáciu bezpečnostné riziká, ktoré môžu spôsobiť ujmy na zdraví a životoch osôb, škody na majetku a životnom prostredí.

Najdôležitejším aspektom pre bezpečnosť aktív je ich ochrana pred vonkajšími a vnútornými rizikami (obr. 14).



Obr. 14 Aktíva a riziká organizácie

4.2.1 Druhy aktív

Aktíva je možné deliť podľa rôznych hľadísk.

Podľa doby ich využívania sa aktíva môžu členiť na:

1. **dlhodobý majetok** – investičný majetok (majetok, ktorý sa využíva dlhšie ako 1 rok),
2. **obežný majetok** – obežné aktíva (pôsobí krátkodobo, vo vecnej i peňažnej forme),
3. **ostatné aktíva** – prechodné aktíva.

Podľa formy medzi aktíva patrí:

1. **hmotný majetok** (hmotné aktíva, majetok hmotného charakteru),
2. **nehmotný majetok** (nehmotné aktíva, majetok nehmotného charakteru), napr. dobré meno spoločnosti (goodwill),
3. **finančný majetok** (finančné aktíva), napr. cenné papiere,
4. **pohľadávky**.

Všeobecne možno medzi aktíva zahŕňať:

1. **hmotné aktíva (majetok),**
2. **nehmotné aktíva (majetok),**
3. **schopnosť vykonávať činnosti na tvorbu určitých produktov alebo poskytovanie služieb – podnikateľské činnosti** *(*výrobný proces, služby, obchod, podnikanie, administratíva atď.).

Hmotné aktíva (majetok) tvoria najmä:

a) **ľudské zdroje** – zamestnanci, klienti, návštevy, predplatitelia atď.,
b) **nehnuteľný majetok** – budovy, stavby, infraštruktúra, potrubia a kanalizácia, výrobné a iné zariadenia, pozemky, zásoby atď.,
c) **hnuteľný majetok** – nábytok, kancelárska a komunikačná technika, zariadenie kancelárií atď.,
d) **pracovné nástroje** – mechanické pracovné prostriedky používané pri pracovnej činnosti ako článok, prostredníctvom ktorého človek pôsobí na pracovné predmety, aby ich prispôsobil na uspokojenie svojich potrieb (náradie, prístroje, stroje, sústava strojov, zariadenia na spracovanie odpadu atď.),
e) **pracovné predmety** – to, na čo človek pôsobí svojou prácou,
f) **podporné zariadenia** – technické zariadenia budov (kanalizácia, vodovod, plynovod, vykurovanie); zdroje energií, klimatizačné a vykurovacie zariadenia, osvetlenie, distribučná sieť, dopravné prostriedky, mechanické a technické prostriedky ochrany objektov atď.,
g) **finančné hmotné zdroje:**
   - **vnútorné zdroje**, ktoré podnik vytvára zo zisku (samofinancovanie), z odpisov, z dlhodobých rezerv, z prostriedkov uvoľnených zrýchleným obratom kapitálu,
   - **vonkajšie zdroje**, ktoré podnik získava z vlastných zdrojov, napr. rozšírením základného imania (akcie, podielové listy), alebo z cudzích zdrojov, napr. prostredníctvom rôznych druhov krátkodobých a dlhodobých úverov, emisiou obligácií, využitím lízingu, faktoringu, príp. finančných derivátov,
h) **komponenty informačného systému (IS) a informačných a komunikačných technológií (IKT)** – počítačový hardvér, modemy, smerovače, ústredne, vysielače, prenosové zariadenia, prenosové káble, telefóny, fax, servery, pracovné stanice, tlačiarne, aktívne a pasívne sieťové prvky, diskové polia a knižnice atď.,
i) **nosiče údajov a informácií** – médiá (disky, pásky atď.), papierová dokumentácia (kontrakty, návody, dokumentácia spoločnosti, dokumenty s dôležitými obchodnými údajmi.

j) hospodárske a domáce zvieratá:
- hovädzí dobytok, kone, ošípané, ovce, kozy,
- hydina – kura domáca, kačica domáca, hus domáca, morka domáca, holub domáci, pštros,
- malé kožušinové zvieratá – králik domáci, nutria,
- pes.

Nehmotné aktíva (majetok) tvoria najmä:

a) ľudské schopnosti – duševné vlastníctvo,

b) informácie – údaje a informácie vo všetkých podobách (elektronická, zvuková, video, papierová, archivovaná), vrátane systémovej dokumentácie, bezpečnostných dokumentov, používateľských manuálov, zácvikových materiálov, plánov kontinuity,

c) softvérové aktíva – aplikačný softvér, systémový softvér, vývojové nástroje a utility (pomocné programy),

d) služby – počítačové a komunikačné služby, všeobecne prospešné služby (vykurovanie, osvetlenie, klimatizácia, zabezpečenie dodávky vody a energií),

e) využívané technológie, patenty, licencie, know-how,

f) povesť organizácie – imidž, značka, dobré meno, kredit, goodwill, dobré vzťahy s vlastnými zamestnancami a externými subjektmi.

Činnosti na vytváranie určitých produktov alebo poskytovanie služieb

Činnosti na vytváranie určitých produktov alebo poskytovanie služieb predstavujú najmä **hlavné činnosti – primárne** *(core business)*, ktoré môžu byť charakterizované ako dominantné, funkčné procesy, uskutočňované v objekte (organizácii) jednotlivcom, skupinou jednotlivcov, organizáciou, firmou s cieľom **splnenia základnej primárnej funkcie – *dosiahnutie stanovených cieľov vo výrobe alebo poskytovaní služieb.***

V zásade sú to podnikateľské procesy, ktoré **prinášajú podnikateľským subjektom najvyššiu pridanú hodnotu**. Napr. podnikateľské subjekty vykonávajú vo svojom objekte činnosti pre splnenie základného cieľa organizácie – zisku, preto sú hlavné činnosti pre nich nosné.

Podľa účelu, pre ktorý je podnikateľská organizácia vytvorená, možno medzi hlavné činnosti zaradiť:
- **riadenie,**
- **obstarávanie,**
- **financovanie,**
- **výrobu alebo služby,**
- **skladovanie,**
- **odbyt, marketing,**
- **dopravu,**
- **iné dôležité činnosti.**

V organizáciách sa okrem hlavných činností uskutočňuje aj množstvo činností, ktoré sa vykonávajú pre zaistenie efektívneho fungovania hlavných činností. Predstavujú **podporné činnosti,** ktoré v organizácii zahŕňajú najmä oblasti:
- **manažérstvo bezpečnosti,**
- ***personalistika (riadenie ľudských zdrojov),***
- ***všeobecná administratíva,***
- ***manažérstvo kvality,***
- ***informatika a telekomunikácie,***

- ***investovanie,***
- ***výskum a vývoj,***
- ***manažérstvo aktív (správa majetku),***
- ***prevádzka, údržba a servis objektov a technologických zariadení, revízie a odborné prehliadky,***
- ***verejné obstarávanie,***
- ***energetické zabezpečenie,***
- ***havarijná služba a iné činnosti,***
- ***záručný a pozáručný servis,***
- ***iné podporné činnosti.***

4.2.2 Manažérstvo aktív

Manažérstvo aktív *(Asset Management, AM)* predstavuje určitý systém, ktorý monitoruje a udržiava hodnotu vecí ucelenej jednotky alebo skupiny. Môže sa vzťahovať na hmotné aktíva, ako sú budovy a nehmotné pojmy, ako sú duševné vlastníctvo a povesť.

Je to **systematický proces** ***zavádzania, prevádzky, údržby, využitia a efektívneho usporiadania aktív.*** Znamená stanovenie hodnoty jednotlivých aktív v závislosti od posúdenia dopadov na činnosť organizácie, z ktorých by mohla vyplynúť strata dôveryhodnosti, integrity alebo dostupnosti aktív.

Základnou normou, ktorá špecifikuje požiadavky na integrovaný a účinný systém správy aktív, riadenie majetku – manažment aktív, je v súčasnosti norma ISO 55001:2014 Asset management. Management systems. Requirements (Manažérstvo aktív. Systémy manažérstva. Požiadavky).

Táto norma, zverejnená v januári 2014, nahradila normu PAS 55 Asset Management, na podporu organizácií pre dosiahnutie najlepšieho možného čistého výnosu z aktív, a zároveň na zníženie nákladov na ich vlastníctvo. Hlavný rozdiel je v tom, že PAS 55 sa zameral na hmotné aktíva, ale ISO 55001 zahŕňa všetky druhy finančného, organizačného a hmotného majetku. Normu je možné použiť na všetky druhy aktív a všetky druhy a veľkosti organizácií.

Ďalšie normy týkajúce sa tejto oblasti sú:

- ISO 55000:2014 Asset management. Overview, principles and terminology. (Manažérstvo aktív. Prehľad, zásady a terminológia), poskytuje prehľad o manažérstve aktív, jeho zásadách a názvosloví a očakávaných prínosoch zo zavedenia manažérstva aktív, táto norma môže byť aplikovaná na všetky druhy aktív a všetky druhy a veľkosti organizácií.
- ISO 55002:2014 Asset management. Management systems. Guidelines for the application of ISO 55001 (Manažerstvo aktív. Systémy manažérstva. Návod na aplikáciu ISO 55001), poskytuje návod na realizáciu uvedeného systému.

Pojem Asset management sa chápe rôznymi spôsobmi:

- v ekonomickej terminológii sa používa ako ekvivalent anglického Asset Management, ***manažment aktív,***
- jeho alternatívou je ***riadenie*** alebo ***správa majetku,***
- z hľadiska terminológie kvality sa používa pojem ***manažérstvo aktív***.

Definícia **manažérstva (správy) majetku** podľa špecifikácie PAS 55-1:2008 bola: „*Ide o systematické a koordinované aktivity a praktiky, prostredníctvom ktorých organizácia optimálne a udržateľne* ***riadi svoj majetok a celkový systém, výkonnosť, riziká a náklady počas celého jeho životného cyklu,*** *s cieľom dosiahnutia určeného strategického plánu.“*

Strategický plán je definovaný ako *„celkový dlhodobý a zavedený plán, ktorý vychádza z vízie, smerovania, hodnôt, obchodnej politiky, požiadaviek zainteresovaných strán, cieľov a riadenia rizík organizácie“.*

Podľa ISO 55000:2014 Asset management predstavuje *„**koordinované aktivity organizácie, prostredníctvom ktorých vytvára hodnoty využívaním svojho majetku**“.*

Podľa Európskej federácie národných spoločností údržby (EFNMS) – Asset management prestavuje *„optimálne riadenie **životného cyklu fyzického majetku** s cieľom dosiahnutia stanovených trvalo udržateľných podnikateľských cieľov“.*

Životný cyklus aktíva je obdobie od počiatku do konca existencie aktíva, zahŕňa všetky fázy, ktorými aktívum prešlo. Fázy životného cyklu môže určiť organizácia podľa svojich potrieb. Existuje celý rad noriem a iných publikácií, ktoré sa zaoberajú rozdelením etáp životného cyklu aktív. Životný cyklus aktív sa nemusí nutne zhodovať s dobou, počas ktorej je niekto v organizácii nositeľom ***zodpovednosti za aktíva***.

Manažérstvo aktív spoločnosti prestavuje koordinované aktivity počas ich celého životného cyklu (dlhodobé), súvisiace so stanovenou víziou a cieľom organizácie splniť očakávania zainteresovaných strán (zákazníkov).

Získanie **výstupov** (realizácia cieľov) možno definovať ***ako hodnotu vytvorenú efektívnym využívaním aktív***. Veľkosť tejto hodnoty, teda úspešnosť dosiahnutia stanovených cieľov, je podmienená ***analýzou***, ktorá musí byť v takom rozsahu, aby maximálne obsiahla všetky ***vonkajšie aj vnútorné riziká***, ktoré existujú v prostredí, kde aktíva pôsobia, alebo na ktoré má užívanie aktív počas ich životného cyklu dosah.

Výsledkom tejto analýzy je odhad a vyhodnotenie možných faktorov – **pravdepodobností** ohrozenia strategických cieľov a **závažnosť ich následkov** na zámery spoločnosti – ***posúdenie rizika.*** **Výsledná hodnota tohto rizika *je podkladom pre rozhodovanie manažmentu v otázke investícií,*** pričom treba predchádzať potenciálnym stratám alebo zvažovať rezervy ich zmiernenia. Manažérstvo aktív organizácie je nepretržitý balans medzi očakávaniami a pripravenosťou predchádzať rôznym vplyvom, na ktoré tieto očakávania môžu mať dosah (v negatívnom slova zmysle), alebo ich zmierňovať.

Efektívny manažment aktív umožňuje okrem zvyšovania spokojnosti zákazníkov zvyšovaním výkonnosti a kontroly produktov dodávaných podľa požadovaných štandardov aj:

- zvyšovať výkonnosť v oblasti ***bezpečnosti a ochrany zdravia pri práci a environmentálnej bezpečnosti,***
- zlepšovať ***manažérstvo rizík,***
- zlepšovať reputáciu korporácie – výhody, ktoré môžu byť v podobe dosiahnutia očakávanej hodnoty zainteresovanými stranami, zlepšenie marketingu produktov/služieb, spokojnosť zamestnancov a efektívnejšie a účinnejšie zásobovanie dodávateľmi,
- schopnosť preukázať trvalo udržateľný rozvoj týkajúci sa správy majetku počas jeho životného cyklu.

Z hľadiska bezpečnostného manažmentu je pre **správne manažérstvo (správu) aktív potrebné vykonať:**

- **inventarizáciu aktív** (musíme vedieť **ČO** ideme chrániť),
- **usporiadanie, klasifikáciu aktív** (musíme vedieť **AKÚ HODNOTU** to pre nás má),
- **pridelenie zodpovednosti za aktíva** (**KTO** zodpovedá).

Pre inventarizáciu a klasifikáciu aktív musia byť zavedené zrozumiteľné pravidlá.

Inventarizácia aktív

Organizácia má byť schopná identifikovať svoje aktíva, určiť ich relatívnu hodnotu a dôležitosť. Každé aktívum by malo byť jasne identifikované a jeho **vlastníctvo** a **bezpečnostná klasifikácia** by mali byť odsúhlasené a zdokumentované spolu s jeho **aktuálnym umiestnením.** Na základe týchto informácií môže **zabezpečiť daným aktívam úroveň ochrany zodpovedajúcu ich hodnote a dôležitosti.** Je teda nutné, aby organizácia mala úplný, zrozumiteľný a aktuálny zoznam svojich aktív.

Inventárne zoznamy aktív napomáhajú zabezpečiť uskutočňovanie efektívnej ochrany aktív. Proces zostavenia inventárneho zoznamu aktív je dôležitým aspektom manažérstva rizík. Zoznam aktív musí byť **aktuálny** a **musí odrážať zmeny v štruktúre aktív v takmer reálnom čase**.

Inventárne zoznamy aktív (zásob aktív a ich atribútov) sa obvykle spracovávajú **v kombinácii s počítačovým systémom riadenia údržby.** Všetky aktíva sú tak vzájomne prepojené a sústredené na jednom mieste, pričom môžu byť tieto aktíva pripojené aj do geodatabázy v informačnom systéme, ktorý štandardizuje dáta a umožňuje interoperabilitu, poskytuje užívateľom možnosť znovu ich použiť, koordináciu a možnosť čspoločne používať efektívnym a účinným spôsobom.

Každé aktívum by malo byť jasne identifikované a jeho vlastníctvo a bezpečnostná klasifikácia by mali byť odsúhlasené a zdokumentované spolu s jeho aktuálnym umiestnením. Organizácia má byť schopná identifikovať svoje aktíva, ich relatívnu hodnotu a dôležitosť. Na základe týchto informácií môže **zabezpečiť daným aktívam úroveň ochrany zodpovedajúcu ich hodnote a dôležitosti.** Je teda nutné, aby organizácia mala úplný, zrozumiteľný a aktuálny zoznam svojich aktív.

Inventárne zoznamy aktív napomáhajú zabezpečiť uskutočňovanie efektívnej ochrany aktív. Proces zostavenia inventárneho zoznamu aktív je dôležitým aspektom manažmentu rizík. Zoznam aktív musí byť aktuálny, musí odrážať zmeny v štruktúre aktív v takmer reálnom čase.

Usporiadanie – klasifikácia aktív

Cieľom klasifikácie aktív je určiť jednotnú ***klasifikačnú schému*** pre ich zaradenie do kategórií na základe ich hodnoty a iných kritérií. Klasifikačná schéma určuje kategórie, ktorým budú v prostredí organizácie priradené zodpovedajúce technické a organizačné opatrenia tak, aby bola chránená ich integrita. Za klasifikáciu aktív zodpovedá garant týchto aktív a musí s ňou byť oboznámený každý zamestnanec spoločnosti.

Aktíva sa môžu **zoskupovať** podľa potrieb organizácie. Takéto zoskupovanie aktív môže zahŕňať ***systémy aktív, portfóliá aktív*** alebo ***druhy aktív.*** Základným hľadiskom členenia aktív je ***doba ich upotrebiteľnosti***, príp. ***obťažnosť ich premeny na peňažné prostriedky*** (likvidita).

Príkladom klasifikácie inventárneho majetku môže byť ich rozdelenie na triedy, napr.:

- Trieda IM 1301 Softvér.
- Trieda IM 9701 Drobný hmotný majetok.
- Trieda IM 9702 Drobný nehmotný majetok.

Z hľadiska bezpečnostného manažmentu možno aktíva klasifikovať do nasledujúcich skupín:

- **Chránené aktíva** –v ich prípade narušenie bezpečnosti spôsobí vážne bezpečnostné následky, tieto aktíva vyžadujú vysoký stupeň ochrany.

- **Štandardné aktíva** – v ich prípade narušenie bezpečnosti má dopad len na obmedzenú skupinu používateľov v rámci jednej súčasti, tieto aktíva vyžadujú štandardnú ochranu.
- **Nechránené aktíva** – aktíva, ktoré nemusia byť žiadnym spôsobom chránené. Musia byť prijaté opatrenia na to, aby nemohli ohroziť bezpečnosť chránených aktív. Správca môže odmietnuť poskytovať podporu a zabezpečovať funkčnosť nechránených aktív.
- **Špeciálne aktíva** – aktíva, ktoré svojím charakterom vyžadujú kombináciu vymenovaných stupňov ochrany a prístupových práv. Bezpečnosť týchto aktív musí byť riešená individuálne.

Pridelenie zodpovednosti za aktíva

Pridelenie zodpovednosti za aktíva znamená, že ***každé aktívum musí mať vlastníka*** (garanta), ktorý zaň zodpovedá. Pokiaľ neexistuje vlastník aktíva, môže sa na riadenie jeho bezpečnosti zabudnúť. Nie je dobré, ak vlastníkom všetkých aktív je napr. konateľ spoločnosti (zodpovednosť je neriaditeľná) alebo administrátor systému (zodpovednosť nie je vymožiteľná). Ideálnym vlastníkom je pracovník s dostatočnými kompetenciami (presadenie ochrany) a motiváciou (straty v prípade neplnenia si povinností). Pokiaľ sa aktívum – systém skladá z viacerých samostatných častí (podsystémov, modulov), môže byť garant určený pre každú takúto časť.

Garant zodpovedá za bezpečnosť aktíva a vykonanie náležitých opatrení na jeho ochranu v súlade s riadiacimi dokumentmi bezpečnostnej politiky. Zodpovednosť za implementáciu bezpečnostných opatrení môže byť delegovaná na odborné útvary spoločnosti alebo externých dodávateľov. Garant (vlastník, používateľ) aktív potvrdzuje prevzatie aktív svojím podpisom, napr. Miestny zoznam hmotného majetku (tab. 10).

Tab. 10 Príklad pridelenia zodpovednosti za aktíva

		MIESTNY ZOZNAM HMOTNÉHO MAJETKU		
Útvar: FBI - ŽU		Umiestnenie: kancelária č. 301 Ing. Ján Kompas		Číslo listu: 1
Riadok č.	Inventárne číslo	Názov	Počet ks	Poznámka
1.	90052370	Tlačiareň HP Laser Jet 1150	1	
2.	90072900	Stolička čalúnená drevená	1	
3.	90089240	Regál	1	
4.	90090972	Telef. prístroj OPTI POINT 50	1	
5.	90130970	Počítač PC Desktop AMD Phenom	1	
Materiál odovzdal:		Dátum:	Materiál prevzal:	

Využitie informačných systémov pri správe aktív

Správa aktív predstavuje prevádzkové procesy, ktoré umožňujú ***využitie informačných systémov*** na podporu správy hmotných i nehmotných aktív organizácie. Patrí sem:

- ***Správa hmotných aktív*** – praktické riadenie celého životného cyklu (projektovanie, výstavbu, uvádzanie do prevádzky, prevádzku, údržbu, opravy, úpravy, nahradenie a vyradenie z prevádzky (predaj) hmotných aktív a aktív infraštruktúry, ako sú konštrukcie, výroba a servis zariadení, energie, vody a zariadení na spracovanie odpadov, inžinierske siete, dopravné systémy, budovy a ďalšie hmotné aktíva).

- ***Správa aktív infraštruktúry*** – rozširuje túto problematiku vo vzťahu predovšetkým k verejnému sektoru, službám, majetku a dopravným systémom. Navyše sa v budúcnosti môže odkazovať na prepojenie medzi človekom, stavbami a prírodným prostredím, prostredníctvom spolupráce a rozhodovacích procesov založených na faktoch.
- ***Správa stálych aktív*** – účtovný proces, ktorý sa snaží sledovať dlhodobý majetok na účely finančného účtovníctva.
- ***Správa IT aktív*** – sústava ekonomických praktík, vytvorená spojením finančných, zmluvných a zásobovacích funkcií na podporu riadenia životného cyklu a strategického rozhodovania o IT prostredí.
- ***Digitálna správa aktív*** – forma digitálneho spravovania aktív.

4.3 LITERATÚRA

BUZAN, B. – WAEVER, O. – DE WILDE, J. [1998]: *Security: A New Framework for Analysis.* Boulder CO: Lynne Rienner Publishers.

BUZAN, B. – WAEVER, O. – DE WILDE, J. [2005]: *Bezpečnost: Nový rámec pro analýzu.* 1. vyd. Brno: UO, Centrum strategických studií, Současná teorie mezinárodních vztahů. ISBN 80-903333-6-2.

BS ISO 55001:2014 *Asset management. Management systems. Requirements.*

BS ISO 55000:2014 *Asset management. Overview, principles and terminology.*

BS ISO 55002:2014 *Asset management. Management systems. Guidelines for the application.*

KORZENIOWSKI, L. F. [2013]: *Teoretické a metodologické aspekty výskumu bezpečnosti.* In: Politické vedy. Roč. 16, č. 3. ISSN 1335 – 2741. Fakulta politických vied a medzinárodných vzťahov, UMB Banská Bystrica.

PAČAIOVÁ H. [2005]: *Asset management – riadenie majetku na báze posudzovania rizík.* In: ATP Journal 19.8.2014.

PAS 55-1: 2008 *Asset Management. Part 1: Specification for the optimized management of physical assets.* BSI.

5 BEZPEČNOSTNÝ SEKTOR

Bezpečnosť referenčného objektu možno dosiahnuť len pri ***sústavnom a efektívnom využívaní všetkých zdrojov, ktoré umožnia jeho stabilné fungovanie v súčasnosti a stály rozvoj v budúcnosti.***

Na dosiahnutie **stavu bezpečnosti** sa musia v organizácii vytvoriť podmienky pre zavedenie:

- právnych bezpečnostných noriem a dosiahnutie zhody s vnútornými bezpečnostnými normami,
- opatrení na ochranu životných záujmov všetkých objektov bezpečnosti – ochranu osôb, majetku a životného prostredia.

V organizáciách, ktoré predstavujú referenčný objekt sa z funkčného hľadiska uskutočňuje veľké množstvo ***hlavných a podporných činností,*** ktoré vrcholovému manažmentu pri správnom riadení umožňujú dosahovať stanovené ciele.

Hlavné a podporné činnosti, uvedené v kapitole 3.2.1 sa nevyskytujú vo všetkých organizáciách v rovnakom rozsahu. Niektoré špecifické činnosti sa uplatňujú len v určitých organizáciách (napr. výroba), mnohé z nich sa však vyskytujú prakticky v každej organizácii. Medzi tie činnosti, ktorým musí vrcholový manažment každej organizácie venovať zvýšenú pozornosť patrí aj:

MANAŽÉRSTVO BEZPEČNOSTI

Manažérstvo bezpečnosti predstavuje činnosť vrcholového manažmentu a bezpečnostných manažérov (riadiaca zložka) zameranú na nepretržité udržiavanie bezpečnosti v organizácii, s cieľom dosiahnuť taký **stav bezpečnosti**, pri ktorom:

- sú odstránené riziká alebo znížené na prijateľnú úroveň a bezpečnosť predstavuje prípustnú mieru nebezpečenstva (ohrozenia),
- ohrozenie je objektívne, reálne a ohrozený subjekt si to uvedomuje a dokáže znížiť riziko (stav bezpečnosti),
- organizácia má schopnosť rýchlo obnoviť svoju činnosť, čím zachovať funkčnú spôsobilosť.

Manažérstvo bezpečnosti teda veľmi úzko súvisí s ***manažérstvom rizík*** a je zamerané na vytvorenie alebo trvalé zabezpečenie takých podmienok, ktoré pomôžu predchádzať alebo znížiť identifikované riziká a vyhnúť sa incidentom, s využitím rôznych ***štandardov, smerníc, prostriedkov, metód, postupov a nástrojov ochrany.***

Najvyššiu **zodpovednosť za bezpečnosť** má prirodzene vlastník, štatutárny orgán a najvyšší manažment (top manažment) organizácie. Zodpovednosť za dodržiavanie bezpečnostných smerníc a režimových opatrení majú aj všetci línioví manažéri od najnižšieho po najvyšší stupeň.

Priamu zodpovednosť za manažérstvo bezpečnosti má vo veľkých a stredných organizáciách **bezpečnostný manažér** – CSO. V rade väčších organizácií existuje profesia manažéra informačnej bezpečnosti – CISO (v našich podmienkach ***správca informačnej siete*** alebo ***bezpečnostný správca informačnej siete***), zameraná výhradne na informačnú bezpečnosť. Veľké organizácie alebo organizácie podnikajúce v rizikovom prostredí (napríklad banky, poisťovne) môžu mať ešte ďalších špecialistov manažérstva bezpečnosti. Ďalší bezpečnostní pracovníci sú zaradení vo všetkých zložkách bezpečnostného sektora.

V malých organizáciách je zodpovednosť za manažérstvo bezpečnosti koncentrovaná na úrovni **štatutárneho orgánu,** pretože nie je efektívne zamestnávať špecializovaného manažéra bezpečnosti na plný úväzok.

Každá organizácia je však zodpovedná za určenie funkcionárov bezpečnosti a splnenie požiadaviek bezpečnosti stanovených v právnych normách. Ide napr. najmä o:

- fyzickú bezpečnosť osôb – osobný strážca – bodyguard,
- bezpečnosť a ochranu zdravia – autorizovaný bezpečnostný technik, bezpečnostný technik, preventívne a ochranné služby,
- požiarnu bezpečnosť – technik požiarnej ochrany, špecialista požiarnej ochrany, členovia protipožiarnej hliadky, príslušníci závodného hasičského útvaru alebo zboru,
- ochranu utajovaných a citlivých informácií – bezpečnostný zamestnanec, správca informačného systému, bezpečnostný správca informačného systému,
- havarijnú činnosť – havarijný technik, špecialista na prevenciu závažných priemyselných havárií, členovia záchrannej služby,
- a ďalšie oblasti bezpečnosti, pre ktoré sú stanovené príslušné zákony, normy a smernice.

5.1 CHARAKTERISTIKA BEZPEČNOSTNÉHO SEKTORA

Každá organizácia (prevádzkovateľ) si podľa svojho poslania, vízií a účelu na úspešné dosahovanie stanovených cieľov vytvára **organizačnú štruktúru**. Jadro organizačnej štruktúry predstavuje základné prostredie pre vykonávanie všetkých hlavných a podporných činností a procesov, ktoré sú v organizácii zastúpené. Základný organizačný rámec uľahčuje úspech plnenia povinností zamestnancami organizácie, ktorí pracujú pod dohľadom zodpovedných manažérov.

Štruktúra organizácie má byť podľa Senewalda *(2011)* vytvorená podľa určitej logickej schémy, ktorá zahrnie nielen všetky primárne (hlavné) oblasti alebo činnosti, ale aj všetky sekundárne (podporné) oblasti alebo činnosti. Každá uvedená oblasť hlavných a podporných činností tvorí samostatnú časť (úsek) celej organizácie. Podľa Slovníka cudzích slov úsek, časť, diel nejakého väčšieho celku (ekonomického, územného, stavebného a pod.) sa nazýva **sektor.**

Na základe jednotlivých činností môžeme teda organizačnú štruktúru organizácie členiť na jednotlivé sektory, napr.: výrobný, finančný, investičný, marketingový, dopravný, personálny, administratívny, informačný, výskumu a vývoja, údržby, servisu a revízií, energetický, služieb a pod.

V národnom hospodárstve sú známe najmä sektory:

- primárny – suroviny, prvovýroba,
- sekundárny – výroba a priemysel, spracovateľský a výrobný sektor,
- terciálny – služby,
- znalostný – kvartérny sektor ekonomiky založený na poznatkoch, zahŕňa najmä vedu a výskum,
- súkromný – založený na ziskovom princípe,
- verejný – špecifická súčasť ekonomiky, poskytovanie verejných služieb, nie je založený na ziskovom princípe.

Bezpečnostný sektor SR je možné definovať ako súhrn jednotlivých komponentov bezpečnostnej štruktúry štátu, fungovanie ktorých má byť založené na kompletnej bezpečnostnej politike štátu. Podľa Výboru pre rozvojovú pomoc OECD sú súčasťou bezpečnostného orgánu mocenské inštitúcie, relevantné civilné orgány a súbor ich vzájomných vzťahov, ktorými sa zaisťuje riadenie a kontrola. Patria sem:

a) *štátne inštitúcie* s legitímnym mandátom zaisťovať bezpečnosť štátu a obyvateľstva pred akýmkoľvek aktom násilia: *ozbrojené sily, polícia, spravodajské služby a ďalšie orgány spojené s výkonnou mocou*.
b) volené a ustanovené autority, zodpovedné za riadenie a kontrolu mocenských inštitúcií:
   - užšie chápanie – mocenské inštitúcie štátu, vládne orgány riadenia, parlamentné orgány kontroly,
   - širšie chápanie – navyše zahŕňa aj súdy a orgány spravodlivosti, relevantné mimovládne organizácie, médiá, špecifických aktérov (súkromné bezpečnostné služby, polovojenské milície, ďalšie neštátne organizácie podobného charakteru) *(Samson, Korba, 2006).*

Veľmi dôležitú podpornú činnosť predstavuje **manažérstvo bezpečnosti organizácie,** ktoré má v každej organizácii zasahovať do všetkých činností, ktoré sa v nej vykonávajú. Rozsah bezpečnostných opatrení sa odvíja najmä od veľkosti a zložitosti organizácie, preto oblasti, na ktoré sa zameriavajú, budú rôzne, najmä v závislosti od zamerania organizácie. Dôležitosť týchto bezpečnostných činností a opatrení je však vo všetkých oblastiach činností organizácie rozhodujúca.

Každá organizácia musí teda v organizačnej štruktúre okrem vytvorenia pracovných miest na manažérstvo svojich hlavných a podporných činností pamätať aj na vytvorenie štruktúry pre pracovníkov, ktorí budú sledovať a riadiť jej bezpečnosť – **štruktúru bezpečnostných pracovníkov**. Z hľadiska organizácie môžeme **manažérstvo bezpečnosti** považovať za veľmi dôležitú časť (úsek) jej celkových činností a štruktúru bezpečnostných pracovníkov za časť jej celkovej štruktúry, ktorú môžeme nazvať:

BEZPEČNOSTNÝ SEKTOR ORGANIZÁCIE

5.1.1 Bezpečnostný sektor organizácie

Bezpečnostný sektor tvorí ***súhrn jednotlivých komponentov bezpečnostnej štruktúry organizácie, fungovanie ktorých má byť založené na jej kompletnej bezpečnostnej politike.*** Predstavujú ho špeciálne vytvorené subjekty bezpečnosti alebo súbory subjektov (oblasti), ktorých hlavným **cieľom** je dosiahnutie, zaistenie a upevňovanie trvalej celkovej ***bezpečnosti osôb, majetku a životného prostredia*** v organizácii.

Bezpečnostný sektor organizácie sa odkazuje na štruktúry, procesy, hodnoty a postoje, ktoré rozhodujú o podobe (forme) bezpečnosti a spôsoboch jej dosahovania. Zahŕňa všetky odvetvia ľudskej činnosti, ktorých podstatou je dosiahnutie a udržiavanie bezpečnosti, teda poskytovanie práce, vedomostí, finančných prostriedkov, infraštruktúry, výrobkov alebo ich vzájomnej kombinácie.

Jednotlivé súčasti bezpečnostného sektora zasahujú prakticky do všetkých ***hlavných i podporných činností*** organizácie, kde je potrebné chrániť významné aktíva. Bezpečnosť pre jednotlivé súčasti bezpečnostného sektora je zakotvená v právnych bezpečnostných normách, ktoré musí spĺňať každá právnická i podnikajúca fyzická osoba.

Súčasti bezpečnostného sektora organizácie vystupujú ako aspekty **komplexne poníamej bezpečnosti organizácie** (komplexná bezpečnosť organizácie = súčet úrovní bezpečnosti jednotlivých podsektorov, oblastí a zložiek bezpečnostného sektora organizácie). Úroveň komplexnej bezpečnosti organizácie závisí od miery integrácie jednotlivých podsektorov, oblastí a zložiek bezpečnostného sektora organizácie.

Rozsah a štruktúra bezpečnostného sektora bude v jednotlivých organizáciách odlišná, v závislosti od ich zamerania, veľkosti a štruktúry. Jadrom bezpečnostného sektora organizácie a jeho jednotlivých subsystémov je bezpečnostný systém – **Systém manažérstva bezpečnosti organizácie.** Bezpečnostný sektor organizácie je možné **podľa subjektov ochrany** rozdeliť na niekoľko **podsektorov,** ktoré sa obvykle v rôznej intenzite vyskytujú vo všetkých druhoch organizácií**:**

1. **Bezpečnosť osôb a majetku.**
2. **Bezpečnosť životného prostredia (environmentálna bezpečnosť).**
3. **Bezpečnosť podnikania (podnikateľská bezpečnosť).**

Oblasti podsektora Bezpečnosť osôb a majetku

Bezpečnosť osôb a majetku je najširším **podsektorom bezpečnostného sektora organizácie**. Ide v ňom o bezpečnosť všetkých aktív organizácie, ktorá je závislá najmä od bezpečnostných rizík (úmyselného napadnutia alebo náhodných), teda o:

- fyzickú bezpečnosť jednotlivcov i skupín, a ich bezpečnosť v pracovnom či vnútornom prostredí organizácie,
- bezpečnosť hmotného i nehmotného majetku (teda aj informácií a informačných systémov) v objektoch organizácie,

- bezpečnosť a nepretržitosť činností, ktoré zveľaďujú majetok organizácie (výrobných činností, nevýrobných činností na poskytovanie služieb alebo iných činností na poskytovanie služieb).

Na základe uvedených aktivít na ochranu aktív všeobecne medzi kľúčové **oblasti podsektora bezpečnosť osôb a majetku v organizáciách** patria najmä:

a) Fyzická bezpečnosť,
b) Požiarna bezpečnosť,
c) Bezpečnosť práce,
d) Bezpečnosť prevádzky (činností na tvorbu produktov alebo poskytovanie služieb),
e) Informačná bezpečnosť – bezpečnosť a ochrana utajovaných skutočností nad rámec osobných údajov, v zmysle ochrany zákonom alebo zmluvne chránených či cenných informácií,
f) Počítačová bezpečnosť (Bezpečnosť informačných a komunikačných technológií) – v zmysle použitia a nastavení hardvéru a softvéru, vrátane špeciálnych prostriedkov (napr. ochrana, či nasadenie sledovania a odpočúvania),
g) Bezpečnosť a ochrana vnútorného poriadku,
h) Ďalšie možné oblasti bezpečnosti organizácie.

Okrem uvedených oblastí, ktoré sa vyskytujú prakticky vo všetkých organizáciách, existujú v podsektore bezpečnosti osôb a majetku aj oblasti bezpečnosti, ktoré sa vyskytujú len **v určitých špecifických organizáciách a objektoch,** napr.:

- **bezpečnosť kritickej infraštruktúry** – ochrana objektov v sektoroch a prvkoch kritickej infraštruktúry pred úmyselným fyzickým napadnutím,
- **bezpečnosť jadrových zariadení** – ochrana jadrových zariadení a ich okolia pred náhodnými jadrovými haváriami.

Oblasti podsektora Podnikateľská bezpečnosť

Z hľadiska podnikateľskej činnosti sa v organizáciách vyskytuje aj množstvo **oblastí podsektora podnikateľskej bezpečnosti**, ktoré sú závislé od podnikateľských rizík, napr.:

- **ekonomická bezpečnosť,**
- **finančná bezpečnosť,**
- **bezpečnosť produkcie,**
- **projektová bezpečnosť,**
- **ochrana proti podvodom a zneužitiu** *(Fraud management),*
- a **ďalšie oblasti bezpečnosti podnikateľskej činnosti**.

Jednotlivé **oblasti** podsektorov bezpečnostného sektora organizácie je možné ďalej deliť na **zložky bezpečnosti** (dole označené písmenami). Niektoré zložky bezpečnosti sú tvorené samostatnými **prvkami bezpečnosti** (označené bodkami).

5.1.2 Zložky v oblastiach podsektora Bezpečnosť osôb a majetku

Uvedené základné oblasti podsektora bezpečnosť osôb a majetku obvykle obsahujú:

1. Fyzická bezpečnosť:
a) ***fyzická bezpečnosť osôb*** – ochrana *osôb* pred úmyselným fyzickým a nefyzickým napadnutím:
- fyzická ochrana dôležitých osôb,
- bezpečnosť zamestnancov pred fyzickým a nefyzickým násilím,
- bezpečnosť zamestnancov pred diskrimináciou.

b) ***fyzická bezpečnosť objektov*** – ochrana *objektov a majetku v nich*, iného než sú utajované skutočnosti, pred úmyselným fyzickým napadnutím:
- fyzická bezpečnosť priestorov organizácie,
- fyzická bezpečnosť objektu,
- facility manažment.

c) ***bezpečnosť objektov kritickej infraštruktúry*** – ochrana *špecifických objektov kritickej infraštruktúry* pred úmyselným fyzickým napadnutím:
- bezpečnosť objektov osobitnej dôležitosti,
- bezpečnosť ďalších dôležitých objektov.

2. Protipožiarna bezpečnosť – ochrana *osôb, objektov, majetku a prevádzky* pred úmyselným alebo náhodným požiarom:

a) požiarna ochrana,

b) protipožiarna bezpečnosť stavieb.

3. Bezpečnosť práce:

a) bezpečnosť práce,

b) bezpečnosť technických zariadení,
- technická bezpečnosť technických zariadení,
- pracovná bezpečnosť technických zariadení,
- prevádzková (funkčná) spoľahlivosť technických zariadení.

c) bezpečnosť pracovného prostredia a pracovných podmienok (hygiena práce).

4. Bezpečnosť prevádzky (činností na tvorbu produktov alebo poskytovanie služieb):

a) bezpečnosť technických zariadení,

b) bezpečnosť kontinuity činností – ochrana *kľúčových výrobných a nevýrobných činností* na tvorbu produktov alebo poskytovanie služieb, ktoré prerušením pre poruchu alebo haváriu môžu spôsobiť značné straty,

c) prevencia závažných priemyselných havárií – ochrana *prevádzky priemyselných podnikov s nebezpečnými látkami* a ich okolia pred náhodnými priemyselnými haváriami,

d) jadrová bezpečnosť – ochrana prevádzky jadrových zariadení a ich okolia pred náhodnými jadrovými haváriami.

5. Informačná bezpečnosť:

a) ochrana utajovaných skutočností **–** ochrana ***informácií v akejkoľvek forme*** (elektronické, fyzické a iné) pred úmyselným alebo náhodným napadnutím či zneužitím:
- fyzická bezpečnosť a objektová bezpečnosť – ochrana *utajovaných skutočností v objektoch a chránených priestoroch* pred nepovolanými osobami a pred neoprávnenou manipuláciou,
- administratívna bezpečnosť – ochrana *utajovaných skutočností pri ich tvorbe, príjme, evidencii, preprave, ukladaní, rozmnožovaní, vyraďovaní a uchovávaní alebo pri inej manipulácii,*
- personálna bezpečnosť – ochrana *utajovaných skutočnosti elimináciou hrozieb spôsobených zamestnancami,* ktorí sa s nimi môžu v určenom rozsahu oboznamovať,
- priemyselná bezpečnosť – ochrana *utajovaných skutočností, ktoré boli postúpené, alebo ktoré vznikli u právnickej osoby alebo podnikajúcej fyzickej osoby,*
- bezpečnosť technických prostriedkov – ochrana *utajovaných skutočností,* ktoré sa tvoria, spracúvajú, prenášajú, ukladajú alebo archivujú *na technických prostriedkoch,*
- šifrová ochrana informácií – systém na zabezpečenie ochrany utajovaných skutočností kryptografickými metódami a prostriedkami šifrovej ochrany informácií.

b) bezpečnosť informačných systémov **–** ochrana *utajovaných skutočností v informačných systémoch:*

- bezpečnosť informačných systémov verejnej správy,
- bezpečnosť informačných systémov poskytovateľov elektronických služieb,
- trestnoprávna zodpovednosť za porušenie bezpečnosti informačných systémov.

c) ***bezpečnosť dôležitých informácií*** – ochrana *dôležitých informácií v dokumentoch a informačných systémoch:*
- ochrana osobných údajov,
- ochrana obchodného tajomstva,
- ochrana bankového tajomstva,
- ochrana listového tajomstva,
- ochrana autorských práv,
- ochrana pred odpočúvaním,
- ochrana súkromia pred nevyžiadanými správami,
- ochrana súkromia pred neoprávneným použitím informačno-technických prostriedkov,
- elektronický podpis a elektronická pečať.

6. **Počítačová bezpečnosť (Bezpečnosť IKT)** – ochrana *informačných a telekomunikačných technológií* pred úmyselným alebo náhodným poškodením:
   - fyzická bezpečnosť,
   - počítačová bezpečnosť,
   - komunikačná bezpečnosť,
   - bezpečnosť dát,
   - režimová bezpečnosť,
   - personálna bezpečnosť.

7. **Bezpečnosť a ochrana vnútorného poriadku:**
   a) ochrana vnútorného poriadku v zmysle organizačných dokumentov a režimových opatrení,
   b) manažérstvo bezpečnostných incidentov.

Charakteristika jednotlivých oblastí a zložiek bezpečnostného sektora je uvedená v nasledujúcich kapitolách učebnice.

5.2 LITERATÚRA

DUFINEC, I. [2011]: *Manažérstvo bezpečnosti podniku.* In: IDEEX s.r.o. News. Košice 7.3.2011.

GAŠPIERIK, L. – REITŠPIES, J., – SELINGER, P. [2011]: : *Bezpečnosť podniku – významný činiteľ súčasnosti.* In: Krízový manažment, vedecko-odborný časopis FŠI ŽU v Žiline, ročník 10, č. 1/2011. ISSN 1336-0019

KORMANCOVÁ, G. [2007]: *Bezpečnosť podniku*. In: Krízový manažment. Roč. 6, č. 2 (2007), s. 62-65. - ISSN 1336-0019.

MESÁROŠ, M. – HRÁDOCKÝ, L. – DUFINEC, I. – KRIŽOVSKÝ, S.[2007]: *Podnikové manažérstvo.* VŠBM Košice, 2007, str. 115. ISBN 978-80-89282-15-9

SAMSON, I. – KORBA, M. [2003]: *Reforma bezpečnostného sektora. Skúsenosti SR.* Bratislava. Projekt v rámci grantovej schémy MZV SR ev. č. 9/2006. Výskumné centrum pre zahraničnú politiku, n. o.

SENNEWALD, CH. A. [2011]: *Effective Security Management.* 5. vydanie. Elsevier Science. ISBN-13-9780123820136.

6 FYZICKÁ BEZPEČNOSŤ

Fyzická bezpečnosť má za cieľ zabrániť úmyselnému napadnutiu osôb či majetku a obmedziť potenciálne škody a zranenia, ktoré môžu byť týmto napadnutím spôsobené. Tvorí ju:

- Fyzická bezpečnosť osôb.
- Fyzická bezpečnosť objektov.
- Bezpečnosť objektov kritickej infraštruktúry.

6.1 FYZICKÁ BEZPEČNOSŤ OSÔB

Osobná bezpečnosť je základným nárokom zaručeným podľa Všeobecnej deklarácie ľudských práv prijatej v Paríži na zasadnutí Valného zhromaždenia OSN v roku 1948. V Slovenskej republike je právo na ochranu osobnosti zaručené každému, pričom predmetom ochrany osobnosti človeka je podľa § 11 ***Občianskeho zákonníka*** najmä život a zdravie, občianska česť a ľudská dôstojnosť, súkromie, rodinný život, meno, dobrá povesť a prejavy osobnej povahy. Toto právo je zaručené už na ústavnej úrovni ***Listinou základných práv a slobôd*** a je spresnené zákonom. Okrem všeobecnej ochrany prostredníctvom občianskeho zákonníka, sú to napr. *Zákon o ochrane osobných údajov, Trestný zákonník, Zákonník práce.*

Policajné štatistiky a Čierna kronika neustále upozorňujú na množstvo prípadov prepadnutia obchodov, herní, bánk, vozidiel prevážajúcich finančnú hotovosť alebo iné cennosti. V značnej miere sa vyskytujú lúpežného prepadnutia, znásilnenia a iné kriminálne útoky na osoby, bez ohľadu na ich postavenie. Spoločenská bezpečnosť je teda neustále narušovaná a spoločnosť hľadá možnosti, ako sa čo najlepšie chrániť.

6.1.1 Zameranie fyzickej bezpečnosti osôb

Fyzická bezpečnosť osôb môže byť narušená rôznymi personálnymi bezpečnostnými incidentmi, ktoré znamenajú ***fyzické narušenie osobnej bezpečnosti***, napr. napadnutie; lúpež; ublíženie na zdraví; usmrtenie; útok na verejného činiteľa; útok na orgán verejnej moci; branie rukojemníkov; teroristický útok; písomné zasielanie potenciálne nebezpečných látok, napr. „biely prášok“; prenasledovanie a napadnutia; ale v niektorých prípadoch aj diskriminácia, sexuálne obťažovanie; sexuálne násilie a zneužívanie a znásilnenie.

Fyzická ochrana osôb je v organizácii zameraná najmä na ochranu:

a) zamestnancov pred fyzickým násilím a diskrimináciou,

b) hlavných predstaviteľov manažmentu organizácie (môže zahŕňať aj prehliadku zameranú na odhalenie odpočúvacích zariadení a sledovanie osôb – detektívna služba),

c) klientov pri:
   - obchodných rokovaniach, dražbách, aukciách,
   - preprave finančných hotovostí a iných cenností,
   - sprevádzaní pri služobných cestách,
   - poskytnutí autoservisu s vodičom vrátane osobnej ochrany,
   - vytváraní a aktivovaní podporného tímu na osobnú ochranu.

d) osôb pri preprave finančných hotovostí a iných cenností – bezpečnosť prepravy cenností predstavuje komplex činností zameraných na odvrátenie alebo zmenšenie rizík, resp. prejavov hrozby bezpečnostných incidentov, ktoré by sa mohli vyskytnúť v priebehu prepravy cenností.

Zatiaľ čo ochrana zamestnancov pred hrozbou násilia na pracovisku a pred diskrimináciou je väčšinou záležitosť interpersonálnych vzťahov a incidenty v tejto oblasti riešia najmä líniovíi vedúci, **ochranu hlavných predstaviteľov manažmentu** (Bodyguarding) **a ochranu klientov** riešia ***bezpečnostní pracovníci.***

Fyzická ochrana osôb *(Bodyguarding)* sa rovnako, ako aj fyzická ochrana majetku v organizáciách, zvyčajne zabezpečuje príležitostným *prenajímaním príslušníkov súkromných bezpečnostných služieb*, ktorí, okrem iného, podľa Zákona o súkromnej bezpečnosti vykonávajú strážnu službu formou:

a) ochrany majetku na verejne prístupnom mieste,
b) ochrany majetku na inom než verejne prístupnom mieste,
c) ochrany osoby,
d) ochrany majetku a osoby pri preprave,
e) ochrany prepravy majetku a osoby,
f) zabezpečovania poriadku na mieste zhromažďovania osôb,
g) prevádzkovania zabezpečovacieho systému alebo poplachového systému, prevádzkovania ich častí, vyhodnocovania narušenia chráneného objektu alebo chráneného miesta,
h) vypracúvania plánu ochrany alebo
i) monitorovania činnosti osoby v uzavretom priestore alebo na uzavretom mieste.

6.1.2 Bezpečnosť zamestnancov pred fyzickým násilím

Násilie je patologickou formou agresie, ktorej cieľom je úmyselné použitie či hrozba použitím fyzickej sily alebo moci proti sebe, inej osobe, proti skupine či komunite, a to sily (moci), ktorá má, alebo s vysokou pravdepodobnosťou bude mať za následok poranenie, smrť, psychickú ujmu, poruchu vývoja či osobnosti. To je však iba jedno z možných poňatí definície násilí.

Násilie predstavuje veľmi zložitý fenomén, zahŕňajúci širokú škálu prejavov a etiologických príčin, takže jeho jednotná a ucelená definícia neexistuje. Násilie možno deliť podľa radu kritérií (napr. podľa spôsobu vykonania, príčin vzniku, dĺžky trvania, aktérov i obetí, následkov pre účastníkov, očakávania či neočakávania vzniku a pod.)

Rovnako ako neexistuje jednotná definícia násilia, neexistuje ani jednotná teória jeho podmienenosti. Všeobecne sa rozlišujú vplyvy vrodené (biologické) a vplyvy prostredia (sociálne, ktoré sú prevažne výsledkom učenia). V posledných rokoch sa vedci už zhodujú v tom, že biologické a sociálne faktory pôsobí spoločne a zároveň sa navzájom ovplyvňujú.

Násilie na pracovisku zahŕňa rôzne fyzické a verbálne útoky, takéto situácie zahŕňajú, ale nie sú obmedzené na:

- obmedzovanie osobnej slobody, ohováranie, vydieranie, donútenie, hrubý nátlak, poškodzovanie cudzích práv,
- obmedzovanie slobody vyznania, porušovanie slobody združovania a zhromažďovania,
- zneužitie právomoci, korupcia, úplatkárstvo, úžera, vydieranie,
- neoprávnené nakladanie s osobnými údajmi.

6.1.3 Bezpečnosť zamestnancov pred diskrimináciou

Okrem zodpovednosti za bezpečnosť a ochranu zdravia pracovníkov pri práci sú organizácie zodpovedné aj za situácie, keď sú zamestnanci pod hrozbou diskriminácie a násilia, v súvislosti s plnením ich povinností alebo v dôsledku iných okolností, ktorým sú vystavené.

Diskriminácia je také konanie, keď sa v tej istej situácii zaobchádza s jedným človekom (skupinou ľudí, organizáciou, krajinou, skupinou krajín) inak než s iným človekom (skupinou ľudí, organizáciou, krajinou, skupinou krajín) na základe jeho odlišnosti napr. rasového alebo etnického pôvodu, vierovyznania, veku, rodu, pohlavia, alebo sexuálnej orientácie, pričom rozhodovanie o tom, či došlo alebo nedošlo ku diskriminácii, sa uskutočňuje na základe toho, či existuje príčinná súvislosť medzi znevýhodnením a použitím kritéria pre rozlišovanie. Diskriminácia je v moderných demokratických spoločnostiach považovaná za neprípustnú a minimálne jej vyššie vymedzené formy sú v súčasnosti zakazované zákonmi a medzinárodnými zmluvami.

Diskriminácia predstavuje nerovnaké zaobchádzanie podkopávajúce a spochybňujúce dôstojnosť človeka. Zákaz diskriminácie teda automaticky neznamená rovnaké zaobchádzanie. V istých prípadoch práve formálne rovnaké zaobchádzanie sa môže stať ponižujúcim a teda diskriminujúcim (v tomto poňatí slovo „*diskriminácia*“ nadobúda oproti zúženému chápaniu slova v zmysle „*rozlišovanie*“ nový význam: „*znevýhodňovanie*“).

Diskriminačné dôvody vychádzajú z negatívnych vlastností diskriminovaných osôb iba vo výnimočných prípadoch. Aj nevedomosť a nepozornosť voči iným sa môžu stať príčinou neúmyselnej diskriminácie. Príčinami najčastejšie bývajú:

- osobnostné problémy diskriminujúcich (komplexy menejcennosti, podceňovanie iných pre zvyšovanie vlastného sebavedomia, znižovanie agresivity po duševných traumách týmto spôsobom, autoritatívnosť…),
- socializácia diskriminujúcich ľudí (prevládajúci názor na vlastnú subkultúru, kultúrna identita, spoločenské postavenie…),
- stereotypy (zúžené predstavy o iných),
- predsudky (ideológiou vštepené, negatívne hodnotenia s emocionálnou zložkou),
- právny rámec, ktorý diskrimináciu umožňuje.

Diskriminácia ľudí môže mať množstvo najrozmanitejších dôvodov, ako napr.:

- rasový alebo etnický pôvod, národnosť, štátne občianstvo,
- jazyk,
- rodinný stav, povinnosť k rodine,
- vierovyznanie,
- sociálny pôvod, majetok,
- vek – väčšinou sa vyskytuje v pracovnoprávnych vzťahoch,
- rod/ pohlavie, tzv. rodová diskriminácia, napr. nižšie platy žien na tých istých pracovných pozíciách ako muži,
- sexuálna orientácia,
- politická príslušnosť, členstvo v politických či odborových organizáciách,
- zdravotné postihnutie,
- ďalšie dôvody, môžu vyplývať z akéhokoľvek predsudku (napr. výška v cm, krása, sexuálna príťažlivosť, temperament, zajakavosť, výslovnosť…).

Za diskrimináciu z dôvodu:

a) ***pohlavia*** sa považuje aj diskriminácia z dôvodu tehotenstva alebo materstva, ako aj diskriminácia z dôvodu pohlavnej alebo rodovej identifikácie,

b) ***rasového pôvodu, národnostného alebo etnického pôvodu*** sa považuje aj diskriminácia z dôvodu vzťahu k osobe určitého rasového pôvodu, národnostného alebo etnického pôvodu,

c) ***náboženského vyznania alebo viery*** sa považuje aj diskriminácia z dôvodu vzťahu k osobe určitého náboženského vyznania alebo viery a aj diskriminácia fyzickej osoby bez náboženského vyznania,
d) ***zdravotného postihnutia*** sa považuje každé obmedzovanie, rozlišovanie či znevýhodňovanie ľudí so zdravotným postihnutím, ktoré vyúsťuje do znemožnenia užívania ich práv v politickej, hospodárskej, sociálnej, kultúrnej, či občianskej oblasti na rovnakom základe s ostatnými.

Antidiskriminačné právo EÚ (napr. Európska antidiskriminačná smernica 2000/78/ES, ktorou sa stanovuje všeobecný rámec pre rovné zaobchádzanie v zamestnaní a povolaní) rozlišuje:

a) **priamu diskrimináciu** – správanie, pri ktorom sa s určitou osobou na základe určitého diskriminačného dôvodu zachádza menej priaznivo ako sa zachádza s inou osobou v porovnateľnej situácii,
b) **nepriamu (skrytú) diskrimináciu** – správanie, keď zdanlivo neutrálne rozhodnutie, rozlišovanie alebo postup znevýhodňuje či zvýhodňuje fyzickú osobu voči inej na základe rozlišovania podľa vymedzených diskriminačných dôvodov, napr. v prípade zdravotnej diskriminácie sem patrí neprijatie nevyhnutných opatrení, aby zdravotne postihnutá osoba mala rovnaké šance ako nediskriminovaná osoba,
c) **pokyn na diskrimináciu** – je spojený so zneužitím podriadeného postavenia druhej osoby na diskrimináciu inej osoby (príkladom je príkaz zamestnancovi na diskriminačné správanie). Páchateľom diskriminácie je ten, kto vydal príkaz, dokonca i v prípade, že ku diskriminačnému správaniu zo strany podriadenej osoby nedošlo.
d) **navádzanie na diskrimináciu** – presvedčovanie, utvrdzovanie alebo podnecovanie druhej osoby, aby diskriminovala tretiu osobu. V tomto prípade osoba, ktorá navádza a tá, ktorú navádza na diskriminačné správanie sa, nie sú v podriadenom postavení.
e) **prenasledovanie (neoprávnený postih)** – je nepriaznivé zaobchádzanie ako odveta za to, že obeť si uplatnila práva na ochranu pred diskrimináciou, môže pochádzať od osoby, voči ktorej diskriminácii sa obeť bránila, ale i od jej „spojencov“. Neoprávnený postih je také konanie alebo opomenutie, ktoré je pre osobu, ktorej sa týka, nepriaznivé a priamo súvisí:
   - s domáhaním sa právnej ochrany pred diskrimináciou vo svojom mene alebo v mene inej osoby alebo
   - s podaním svedeckej výpovede, vysvetlenia alebo súvisí s inou účasťou tejto osoby v konaní vo veciach súvisiacich s porušením zásady rovnakého zaobchádzania,
   - so sťažnosťou namietajúcou porušenie zásady rovnakého zaobchádzania.

Často sa vyskytuje i pojem **pozitívna diskriminácia** alebo tiež afirmatívna akcia, resp. vyrovnávacie opatrenie. Pojem by sa dal opísať ako *zvýhodňovanie diskriminovaných* alebo *zvýhodňovanie znevýhodnených*. Príkladom by mohol byť predpis o určitých výhodách garantovaných invalidom pri hľadaní si práce.

Slovensko prijalo tzv. **Antidiskriminačný zákon** č. 365/2004 Z. z., ktorý vychádza z antidiskriminačných smerníc Európskej únie (smernica Rady Európy 2000/43/ES, smernica Rady Európy č. 2000/78/ES). Tento zákon rieši problematiku diskriminácie predovšetkým v oblasti sociálneho zabezpečenia, zdravotnej starostlivosti, vzdelávania, pracovnoprávnych vzťahov a poskytovania tovarov a služieb a ukladá povinnosť dodržiavať zásadu rovnakého zaobchádzania. Okrem neho sa diskrimináciou zaoberá viacero odvetvových zákonov.

Zásada rovnakého zaobchádzania sa uplatňuje len v spojení s právami osôb ustanovenými osobitnými zákonmi najmä v oblastiach:

a) ***prístupu k zamestnaniu, povolaniu, inej zárobkovej činnosti alebo funkcii,*** vrátane požiadaviek pri prijímaní do zamestnania a podmienok a spôsobu uskutočňovania výberu do zamestnania,

b) ***výkonu zamestnania a podmienok výkonu práce v zamestnaní*** vrátane odmeňovania, funkčného postupu v zamestnaní a prepúšťania,

c) ***prístupu k odbornému vzdelávaniu***, ďalšiemu odbornému vzdelávaniu a účasti na programoch aktívnych opatrení na trhu práce vrátane prístupu k poradenstvu pre výber zamestnania a zmenu zamestnania (ďalej len „odborné vzdelávanie“) alebo

d) ***členstva a pôsobenia v organizácii zamestnancov, organizácii zamestnávateľov a v organizáciách združujúcich osoby určitých profesií*** vrátane poskytovania výhod, ktoré tieto organizácie svojim členom poskytujú.

Ku konkrétnemu riešeniu diskriminácie možno použiť nasledujúce prostriedky: zmierne riešenie sporu (mimosúdne vyjednávanie, mediácia); podnety kontrolným orgánom; medializácia; súdna ochrana.

6.2 FYZICKÁ BEZPEČNOSŤ OBJEKTOV

V praxi bezpečnostného manažmentu sa **pod pojmom objekt môžu rozumieť:**

- **priestory** *(premises)***, areál,** ktorý stavebne a obvykle aj z hľadiska účelu a vlastníckych vzťahov tvorí jeden funkčný celok, zvyčajne zahŕňa ***viac budov a priestory medzi nimi***, napr. priestory podniku, univerzity a pod.,
- **budova alebo iný stavebne alebo inak ohraničený priestor,** v ktorom sa nachádzajú ***chránené priestory s utajovanými skutočnosťami,***
- **budova alebo iný stavebne alebo inak ohraničený priestor,** v ktorom sa nachádzajú ***chránené priestory s inými druhmi aktív,***
- **bytové budovy:** rodinné domy, bytové domy, ďalšie budovy na bývanie, napríklad detské domovy, študentské domovy, domovy dôchodcov a útulky pre bezdomovcov,
- **nebytové budovy** určené na rôzne účely, s rôznou veľkosťou,
- **inžinierske stavby**, ktoré často nie sú tvorené budovami a môžu byť zaradené aj medzi prvky kritickej infraštruktúry.

Pre všetky uvedené objekty platia rovnaké pravidlá zachovania bezpečnosti, rozlišujú sa iba v rozsahu prijímaných opatrení. Zásady **bezpečnosti objektov** XY *(Physical Security)* alebo **bezpečnosti priestorov** *XY (Premises Security)* vychádzajú zo zásad **fyzickej bezpečnosti a objektovej bezpečnosti**, ktoré sú podľa Vyhlášky NBÚ č. 336/2004 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti špecificky zamerané na ***objekty a chránené priestory s uloženými utajovanými skutočnosťami.***

Zásady fyzickej bezpečnosti a objektovej bezpečnosti sa vo všetkých objektoch aplikujú primerane aj na ***ochranu ďalších aktív organizácie***. Ide o ***aktíva*** uložené v chránených priestoroch, ale aj o ***infraštruktúru,*** pre ktoré sa bezpečnosť zabezpečuje podľa rovnakých zásad. Dôležitá je aj ochrana ***technického zariadenia budov***, do ktorého sa zaraďuje kanalizácia, vodovod, plynovod a vykurovanie.

Infraštruktúra organizácie predstavuje systém vybavenia, zariadenia a služieb nevyhnutných na jej prevádzku. Bezpečnosť jednotlivých prvkov infraštruktúry je teda veľmi dôležitá pre celú činnosť organizácie a musí jej byť venovaná patričná pozornosť. Infraštruktúru organizácie možno rozdeliť na vonkajšiu a vnútornú.

Vonkajšia infraštruktúra pôsobí nezávisle od organizácie, v popise úrovne jej bezpečnosti sa obvykle uvádza:

- zásobovanie surovinami,
- dodávka potravín a vody,
- systém poskytovania zdravotníckej služby,
- systém dodávky elektriny, plynu, PHM,
- automobilová a železničná dopravná sieť,
- okolité objekty (budovy, zariadenia, vodné toky atď.),
- bezpečnostné zbory a služby v regióne,
- informačné a komunikačné systémy a služby,
- bankový sektor a iné finančné ústavy,
- orgány štátnej správy a samosprávy,
- zložky integrovaného záchranného systému.

Vnútorná infraštruktúra môže byť riadená a ovplyvniteľná organizáciou, závisí od veľkosti organizácie, produktov, ktoré sa vyrábajú, alebo služieb, ktoré organizácia ponúka. V popise úrovne bezpečnosti vnútornej štruktúry organizácie sa obvykle uvádza:

- stavebná a konštrukčná úroveň budov a zariadení,

- mechanické a elektrické zabezpečovacie systémy,
- energetické rozvody,
- informačné a komunikačné systémy,
- fyzická a objektová ochrana objektov a chránených priestorov.

V Analýze tendencií vývoja vnútornej bezpečnosti SR a z nej vyplývajúcich rizík a ohrození SR spracovanej Sekciou krízového manažmentu a civilnej ochrany Ministerstva vnútra SR v roku 2010 sú uvedené definície:

- **Bezpečnosť chráneného objektu** – je kvalifikovaná úroveň ***fyzickej, technickej alebo funkčnej bezpečnosti*** chráneného objektu, jeho integrity a funkcií, stav, kedy chránenému objektu reálne nehrozí žiadne nebezpečenstvo a jeho fyzická alebo technická bezpečnosť, sebarealizácia, funkcie, podstata a určené činnosti prebiehajú spôsobom (sú v stave) postavenia, určenia alebo poslania.
- **Porucha bezpečnosti chráneného objektu** – je kvalifikovaná úroveň ***potenciálneho ohrozenia alebo chyby v systéme (úrovni) bezpečnosti*** chráneného objektu, stav, kedy bezpečnosť alebo výkon funkcií alebo účel chráneného objektu alebo jeho hodnota, podstata (integrita) sú reálne ohrozené, hrozí alebo vzniká porucha, krízový stav, priamo na chránenom objekte alebo porucha systému ochrany alebo subjektu zabezpečujúceho ochranu, pričom následok (škoda) ešte nastať nemusel.
- **Útok na objekt** – je ***bezprostredné ohrozenie bezpečnosti chráneného objektu***, najmä ***priama bojová akcia, teroristický útok, priamo alebo bezprostredne prebiehajúca násilná trestná činnosť alebo iné protiprávne konanie,*** smerujúce proti bezpečnosti chráneného objektu alebo subjektu zabezpečujúceho ochranu, s cieľom získať chránený objekt alebo jeho časť do moci útočníka, pod jeho kontrolu, eliminácia alebo poškodenie chráneného objektu alebo získanie politického, ekonomického alebo iného prospechu alebo spôsobenie inej ujmy alebo škody.

Medzi riziká úmyselného ohrozenia bezpečnosti chráneného objektu patria najmä lúpež, ozbrojená lúpež, vandalizmus, krádeže aktív vlámaním alebo zamestnancami, násilie proti personálu, vniknutie do informačného systému, narušenie poplachového systému, podozrivá poštová zásielka, špionáž, vyhrážanie bombou, teroristický útok.

Bezpečnosť objektov je realizovaná prostredníctvom bezpečnostných opatrení, ktoré sú uvedené na obr. 15.

Obr. 15 Bezpečnosť objektov

6.3 BEZPEČNOSŤ PRVKOV KRITICKEJ INFRAŠTRUKTÚRY

Smernica Rady 2008/114/ES definuje kritickú infraštruktúru ako zložku, systém alebo ich časť, ktorá je nevyhnutná na zachovanie základných funkcií spoločnosti, zdravia, ochrany, bezpečnosti, kvality života obyvateľov z ekonomického a sociálneho hľadiska, a ktorej narušenie alebo zničenie by malo závažné dôsledky v členskom štáte z dôvodu nemožnosti zachovať tieto funkcie.

Kritická infraštruktúra je podľa Zákona č. 45/2011 Z. z. o kritickej infraštruktúre súčasť infraštruktúry a predstavuje systém, ktorý sa člení na sektory a prvky.

Sektorom kritickej infraštruktúry je časť kritickej infraštruktúry, do ktorej sa zaraďujú prvky kritickej infraštruktúry. Sektor môže obsahovať jeden alebo viac podsektorov kritickej infraštruktúry.

Prvkom kritickej infraštruktúry je najmä ***inžinierska stavba, služba vo verejnom záujme a informačný systém v sektore kritickej infraštruktúry,*** ktorých narušenie alebo zničenie by malo podľa sektorových kritérií a prierezových kritérií ***závažné nepriaznivé dôsledky na uskutočňovanie hospodárskej a sociálnej funkcie štátu, a tým na kvalitu života obyvateľov z hľadiska ochrany ich života, zdravia, bezpečnosti, majetku, ako aj životného prostredia.***

Toto zničenie alebo znefunkčnenie môže nastať z dôvodu *veľkej prírodnej alebo technologickej katastrofy, teroristického útoku, extrémnych vplyvov počasia, či z ďalších dôvodov.* Zničenie alebo znefunkčnenie kritickej infraštruktúry by znamenalo veľké straty na životoch a majetku, morálne škody, alebo by viedlo k dezorganizácii spoločnosti.

Do kritickej infraštruktúry patria najmä:

- ***objekty osobitnej dôležitosti,***
- ***ďalšie dôležité objekty,***
- ***vybrané informačné a komunikačné prostriedky,***
- ***zariadenia na výrobu a zásobovanie vodou, elektrickou energiou, ropou a zemným plynom,***
- ***ďalšie časti majetku štátu a podnikateľských právnických a fyzických osôb*** určené vládou SR, alebo iným kompetentným orgánom štátnej správy, ktoré sú nevyhnutné na zvládnutie krízových situácií, ochranu obyvateľstva a majetku, na zaistenie minimálneho chodu ekonomiky a správy štátu, ako aj jeho vonkajšej a vnútornej bezpečnosti a ktoré treba špeciálne ochraňovať.

Sú to zariadenia, služby a informačné systémy životne dôležité pre obyvateľov a riadenie štátu, ktorých strata funkčnosti alebo zničenie môže ohroziť bezpečnostné záujmy štátu *(Šimák a kol., 2012).*

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

Podľa Zákona č. 319/2002 Z. z. o obrane SR:

- **objekty osobitnej dôležitosti** sú strategické objekty obrannej infraštruktúry, ktorých poškodenie alebo zničenie obmedzí zabezpečenie obrany štátu,
- **ďalšie dôležité objekty** sú objekty obrannej infraštruktúry, ktorých poškodenie alebo zničenie obmedzí činnosť ozbrojených síl alebo chod hospodárstva Slovenskej republiky.

Zničenie alebo znefunkčnenie objektov môže nastať z dôvodu *veľkej prírodnej alebo technologickej katastrofy, teroristického útoku, extrémnych vplyvov počasia, či z ďalších dôvodov*. Zničenie alebo znefunkčnenie kritickej infraštruktúry by znamenalo veľké straty na životoch a majetku, morálne škody, alebo by viedlo k dezorganizácii spoločnosti.

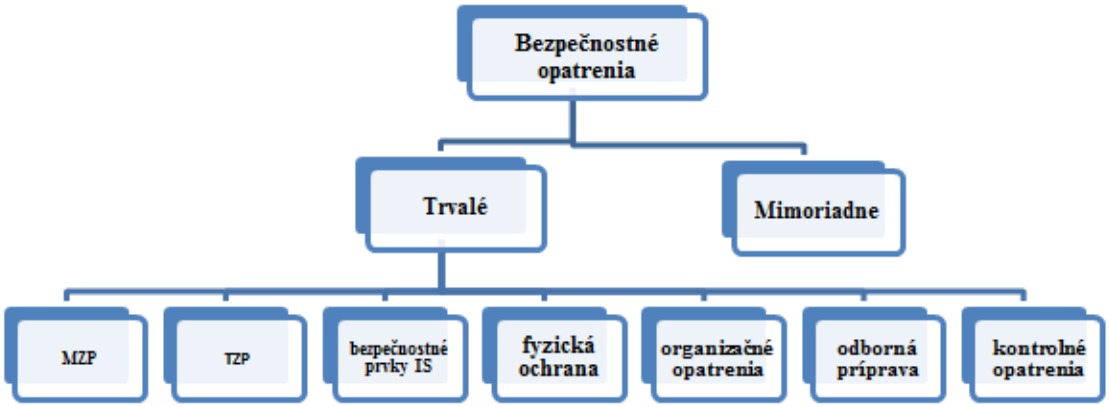
Ochrana prvkov kritickej infraštruktúry

Ochrana prvku kritickej infraštruktúry predstavuje zabezpečenie jeho funkčnosti, integrity a kontinuity činnosti, s cieľom predísť, odvrátiť alebo zmierniť hrozbu jeho narušenia alebo zničenia. V rámci organizácie sa chápe ako súhrn činností, mechanizmov, síl, prostriedkov a opatrení na:

- prevenciu pred rizikovými faktormi,
- odvrátenie útoku na prvok kritickej infraštruktúry,
- zabránenie negatívnym vonkajším alebo vnútorným vplyvom ohrozujúcim existenciu, stabilitu a fungovanie prvku kritickej infraštruktúry,
- odstránenie následkov.

Na ochranu prvku kritickej infraštruktúry sa určujú bezpečnostné opatrenia. Ich rozsah sa stanovuje na základe posúdenia hrozby narušenia alebo zničenia prvku.

Bezpečnostné opatrenia na ochranu prvku sa členia podľa obr 16 na:



Obr. 16 Bezpečnostné opatrenia na ochranu prvku kritickej infraštruktúry

Trvalé bezpečnostné opatrenia sú investície a postupy na zabezpečenie ochrany prvku, a to:

a) mechanické zábranné prostriedky,
b) technické zabezpečovacie prostriedky,
c) bezpečnostné prvky informačných systémov,
d) organizačné opatrenia s dôrazom na postup pri vyrozumení a varovaní, ako aj na krízové riadenie,
e) odborná príprava osôb, ktoré zabezpečujú ochranu prvku,
f) kontrolné opatrenia na dodržiavanie trvalých bezpečnostných opatrení.

Mimoriadne bezpečnostné opatrenia sú opatrenia, ktoré sa uplatňujú v závislosti od intenzity hrozby narušenia alebo zničenia prvku.

Mechanické zábranné prostriedky sú podľa Zákona o kritickej infraštruktúre prostriedky:

1. obvodovej ochrany, najmä pevná bariéra, brána, závora a turniket,
2. plášťovej ochrany, najmä dvere, mreža, bezpečnostné sklo a bezpečnostná zámka,
3. predmetovej ochrany, najmä komorový trezor a komerčný úschovný objekt.

Technickými zabezpečovacími prostriedkami sú najmä:

a) systém na kontrolu vstupu,
b) elektronický zabezpečovací systém,
c) kamerový systém,
d) elektrická požiarna signalizácia,
e) zariadenie na detekciu látok a predmetov,
f) zariadenie proti odpočúvaniu,
g) zariadenie na fyzické ničenie nosičov informácií.

Na ochranu prvku kritickej infraštruktúry sa spracováva ***bezpečnostný plán***, v niektorých prípadoch aj ***havarijný plán*** (Zákon o kritickej infraštruktúre).

Bezpečnostný plán prevádzkovateľa prvku kritickej infraštruktúry obsahuje:

- popis možných spôsobov hrozby narušenia alebo zničenia prvku,
- zraniteľné miesta prvku a bezpečnostné opatrenia na jeho ochranu.

Prevádzkovateľ je povinný oboznámiť svojich zamestnancov v nevyhnutnom rozsahu s bezpečnostným plánom a precvičiť podľa bezpečnostného plánu aspoň raz za tri roky modelovú situáciu hrozby narušenia alebo zničenia prvku.

Postup pri vypracúvaní bezpečnostného plánu:

1. Určujú sa **dôležité zariadenia prvku.**
2. Vyhodnocuje sa **riziko narušenia alebo zničenia jednotlivých zariadení prvku**, ich zraniteľné miesta, predpokladané následky ich narušenia alebo zničenia na funkčnosť, integritu a kontinuitu činnosti prvku.
3. Vyberú sa **hlavné bezpečnostné opatrenia na ochranu prvku,** ktoré sa členia na:
   a) trvalé bezpečnostné opatrenia,
   b) mimoriadne bezpečnostné opatrenia.
4. Určujú sa **hlavné bezpečnostné opatrenia** na ochranu prvku.
5. Bezpečnostný plán sa počas jeho tvorby **konzultuje** s orgánmi, ktorých súčinnosť sa predpokladá pri ochrane prvku.

6.4 FACILITY MANAŽMENT

Facility manažment (FM) je integrovaný multidisciplinárny, interdisciplinárny odbor, ktorý sa zaoberá **riadením podporných činností organizácie.** Norma STN/EN 15221 Facility management definuje FM takto: *„integrácia činností v rámci organizácie na zabezpečenie a rozvoj dohodnutých služieb, ktoré podporujú a zvyšujú efektivitu vlastných základných činností organizácie“*. Je to metóda vzájomného harmonizovania zamestnancov, pracovných činností a pracovného prostredia, ktoré v sebe zahŕňa princípy obchodnej administratívy, architektúry, humanitných a technických vied.

Organizácia vo svojom stavebnom objekte uskutočňuje:

a) Hlavné činnosti – primárne *(core business)* – môžu byť charakterizované ako dominantné, funkčné procesy, uskutočňované v stavebnom objekte jednotlivcom, skupinou jednotlivcov, organizáciou, firmou s cieľom splniť základnú primárnu funkciu. Napr. podnikateľské subjekty vykonávajú v stavebnom objekte činnosti s cieľom splniť základný cieľ organizácie – zisk. Hlavná činnosť je pre nich nosná. V zásade sú to procesy, ktoré prinášajú podnikateľským subjektom najvyššiu pridanú hodnotu.

b) Podporné činnosti – sekundárne – ak cieľom manažmentu organizácie je maximálna efektívnosť hlavnej činnosti, tak strategickým cieľom FM je riadenie podporných činností s cieľom zaistiť ich efektívne fungovanie *(Vyskočil, Štrup, 2003)*.

Podporné činnosti v organizácii zahŕňajú najmä oblasti:

- ***správa majetku,***
- ***bezpečnosť, zdravie, ochrana*** – BOZP na ochranu pracovníkov a podnikania, kontrola najmä technického vybavenia, ochranu osôb môže mať na starosti iný útvar,
- ***požiarna ochrana*** – kontrolná činnosť požiarnym technikom, údržba, revízie a skúšky všetkých požiarnych bezpečnostných zariadení a systémov, vedenie evidencie a dodržiavanie predpisov,
- ***ochrana životného prostredia,***
- ***plánovanie kontinuity činnosti*** – všetky organizácie by mali mať plán kontinuity činností, aby sa mohli rýchlo zotaviť v prípade požiaru alebo závažnej poruchy,
- ***riadenie nehnuteľnosti*** – budova môže byť vo vlastníctve osoby užívajúcej nehnuteľnosť alebo prenajatá, prenajaté nehnuteľností budú predmetom pravidelného nájomného hodnotenia,
- ***administratíva nehnuteľností,***
- ***riadenie prevádzky budovy*** – zodpovednosť za každodenný chod budovy, vykonávané internými alebo externými pracovníkmi (bežné problémy ako veľké teplo alebo zima, osvetlenie, zaseknutá kopírka, rozliate tekutiny, problémy s automatom, ale aj rezervácia zasadacích miestností, parkovacích miest a mnoho ďalších služieb),
- ***prevádzka, údržba a servis*** objektu a technologických zariadení – údržba, preskúšanie a revízne plány majú zabezpečiť, že zariadenie funguje bezpečne a efektívne, s cieľom maximalizovať životnosť zariadení a znížiť riziko porúch,
- ***verejné obstarávanie,***
- ***prideľovanie priestorov*** – v mnohých organizáciách, sa často mení rozmiestnenie kancelárií,
- ***upratovanie*** – obvykle mimo pracovného času, ale je možné stanoviť v pracovnej dobe čas na čistenie toaliet, doplňovanie spotrebného materiálu (toaletný papier, mydlo atď.), odhŕ-

ňanie snehu, upratovanie sa plánuje ako séria „pravidelných“ úloh: denné, týždenné, mesačné atď.

- ***stravovanie,***
- ***energetický manažment,***
- ***informatika a telekomunikácie,***
- ***riadenie kvality,***
- ***záručný a pozáručný servis*** – zastupovanie klientov pri rokovaní s tretími osobami,
- ***revízie, odborné technické prehliadky*** – zabezpečenie revízií podľa platných vyhlášok a noriem (napr. elektrozariadenie, výťahy, spotrebiče a pod.),
- ***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,
- ***vedenie kľúčového hospodárstva*** – evidencia kľúčového hospodárstva, systém generálneho kľúča.

Facility management nie je teda len správa budov, ale je to komplex podporných činností vychádzajúcich z optimalizovania prevádzkových nákladov na kvalitné zabezpečenie, plánovanie a riadenie všetkých procesov, činností a služieb, ktoré priamo nesúvisia s kľúčovými aktivitami danej firmy, no sú nevyhnutné na jej fungovanie a existenciu, pričom jeho hlavným cieľom je vytvoriť optimálne podmienky pre existujúce ekonomické ciele danej spoločnosti. Súbor týchto služieb pre danú organizáciu je väčšinou poskytovaný z vonkajších zdrojov tzv. outsourcingom, ktorý poskytuje spoločnosť zaoberajúca sa Facility managementom.

Pojem outsourcing – vznikol spojením skratiek anglických slov **out**sidere **sourc**e us**ing** = využívanie vonkajších zdrojov *(Somorová, 2006).*

Prvá spoločnosť FM – National (NFMA) vznikla v máji 1980 v USA. O rok neskôr sa z tejto organizácie stala International Facility Management Association (IFMA). Európa sa s pojmom facility management stretáva až na začiatku 90. rokov (Veľká Británia, Škandinávske krajiny, Francúzsko a Benelux). V roku 1998 sa pridalo Maďarsko, Česká republika bola za člena IFMA prijatá v roku 2000. Na Slovensku vznikla v roku 2009 Slovenská asociácia facility managementu (SAFM) ako nezávislé neziskové združenie.

Podľa organizácie IFMA možno FM definovať ako *„metódu, ako v organizáciách vzájomne zladiť pracovníkov, pracovné činnosti a pracovné prostredie, ktoré v sebe zahŕňa princípy obchodnej administratívy, architektúry, humanitných a technických vied.“*

STN EN 15221 Facility management ho definuje takto: *facility management predstavuje integráciu činností v rámci organizácie s cieľom zabezpečenia a rozvoja dohodnutých služieb, ktoré podporujú a zvyšujú efektivitu vlastných základných činností (Somorová, 2006).*

Cieľom FM je „posilniť tie procesy v organizácii, pomocou ktorých pracovníci na svojich pracoviskách podávajú najlepšie výkony a v konečnom dôsledku pozitívne prispejú k ekonomickému rastu a celkovému úspechu organizácie“ *(Vyskočil, Štrup, 2003).*

Z definície IFMA vyplýva, že FM je sústredený do troch oblastí :

a) Oblasti, týkajúcej sa **pracovníkov,** t. j. ľudských zdrojov a sociologických aspektov: schopnosti pracovníkov v procese FM a sledovanie a analýza potrieb pracovníkov, ktorí vykonávajú hlavnú činnosť.
b) Oblasti **pracovnej činnosti**, t. j. oblasti výkonov a financovania: know-how hlavných činností a ich väzieb a know-how ich optimálnej podpory.

c) Oblasti **pracovného prostredia**, t. j. architektúry a inžinieringu: sledovanie a analýza potrieb pracovísk, optimálne dispozície a väzby, technické zázemie.

Na dosiahnutie požadovanej kvality služieb by podľa STN EN 15221-1 Facility management – Termíny a definície poskytovateľ mal pôsobiť v strategickej, taktickej a prevádzkovej úrovni *(Somorová 2008):*

- ***v strategickej úrovni,*** kde organizácia definuje dlhodobé ciele, by mala byť definovaná aj stratégia facility manažmentu, ktorá by mala byť zhodná so stratégiou organizácie. Dôležitou súčasťou stratégie firmy v nadväznosti na služby FM je vypracovanie Dohody o úrovni služieb *(SLAs – Service level agreements)* a Kľúčových výkonnostných identifikátorov *(KPIs – Key performance indicators).*
- ***taktická úroveň*** predstavuje strednodobú implementáciu strategických cieľov organizácie. V nej by mali byť prenesené strategické ciele facility managementu na taktickú úroveň, ako i presná definícia SLAs a KPIs (vykonanie služieb, ich kvalita, riziko).
- ***v prevádzkovej úrovni*** prebieha dodávanie služieb v súlade s požiadavkami klienta v zmysle podpísanej zmluvy, ktorej súčasťou by mala byť SLAs, ďalej monitorovanie a kontrolovanie procesov dodávania služieb FM (KPIs).

Norma STN EN 15221-1 Termíny a definície definuje tzv. **„tvrdé služby“** (FM služby vzťahujúce sa na priestor a infraštruktúru) a **„mäkké služby“** (FM služby vzťahujúce sa na ľudí a organizácie). Rozsah služieb FM je štruktúrovaný do dvoch sekcií v zmysle požiadaviek klienta. V norme sú definované ako:

a) požiadavky spojené s priestorom a infraštruktúrou:
- požiadavka na priestor,
- požiadavka na technickú infraštruktúru,
- požiadavka na čistenie (upratovanie),
- požiadavka súvisiaca s vonkajším priestorom,
- požiadavka súvisiaca s pracoviskom,
- požiadavka spojená s priestorom a infraštruktúrou.

b) požiadavky spojené s pracovníkmi a organizáciou:
- požiadavka na zdravie, bezpečnosť a ochranu,
- požiadavka na stravovanie,
- požiadavka na informácie a komunikáciu,
- požiadavky na logistiku,
- požiadavka na integrované riadenie, poradenstvo a administratívnu podporu,
- špecifické požiadavky organizácie.

Norma na požiadavku priestoru uvádza strategické plánovanie a riadenie priestoru, návrh a výstavbu, prenájom a riadenie obsadenosti, správu a údržbu budov, renováciu a prestavbu atď.

Pre technickú infraštruktúru sú to požiadavky na technické vybavenie budovy (technickú infraštruktúru), ktoré sa uspokojujú službami zabezpečujúcimi príjemnú klímu, svetlo/tieň, elektrický prúd, vodu a plyn. Príkladmi služieb, ktoré zodpovedajú týmto potrebám, sú správa médií a energií, prevádzka a údržba technickej infraštruktúry (TZB), svetelné hospodárstvo atď.

Štvrtá časť európskej normy prEN 15221-4 Kategorizácia, klasifikácia a štruktúry vo FM poskytuje systémové usporiadanie produktov FM v nadväznosti na ich členenie podľa prvej časti normy 15221-1 s kódovaním jednotlivých produktov FM, a to spôsobom kategorizácie, klasifikácie a použitím štruktúr, ktoré sú uvedené v tab. 11.

Tab. 11 Kategorizácia produktov facility managementu

Facility Management – Integrácia procesov na *strategickej úrovni*	
1000	**Priestor & Infraštruktúra – integrácia procesov na *taktickej a prevádzkovej úrovni***
1100	Vnútorný priestor
1200	Vonkajší priestor
1300	Upratovanie
1400	Pracovný priestor
1900	Špecifické – základné aktivity
2000	**Ľudia & Organizácia – integrácia procesov na *taktickej prevádzkovej úrovni***
2100	Zdravie, ochrana, bezpečnosť HSSE
2300	Informačné a komunikačné technológie
2400	Logistika
2500	Podpora prevádzky
2900	Špecifiká – organizácia
9000	***Horizontálne alebo centrálne funkcie***

Podporné činnosti sú zabezpečované službami, ktoré sú v norme STN EN 15221-1 definované ako „služby facility manažmentu – podporné zabezpečenie základných činností spoločnosti, dodávané interným alebo externým poskytovateľom“. Kvalitné fungovanie všetkých podporných činností je podmieňujúcim faktorom zabezpečenia dosiahnutia efektívnosti základnej činnosti organizácie. Efektívnosť podporných činností by mal zaisťovať FM tak, aby boli:

- nákladovo optimálne,
- právne a formálne regulárne,
- ekologicky a energeticky efektívne,
- zodpovedajúce štandardom organizácie *(Vyskočil, Štrup, 2003).*

Základy FM v Európe stanovuje EÚ norma, u nás označovaná STN EN 15221 „Facility management“, ktorú tvoria:

1. **STN EN 15 221-1: Facility management: Termíny a definície** – vymedzuje oblasť facility manažmentu, približuje základné pojmy a definície. Norma definuje tzv. „tvrdé služby“ (FM služby vzťahujúce sa k priestoru a infraštruktúre) a „mäkké služby“ (FM služby vzťahujúce sa k ľuďom a organizácii). Cieľom normy je:
   a) zlepšiť komunikáciu medzi stranami dopytu a ponuky,
   b) zlepšiť efektivitu primárnych procesov a procesov facility managementu,
   c) kvalitatívne zlepšiť výstup.
2. **STN EN 15 221-2: Facility management: Návod na prípravu dohôd o facility managemente** – pomáha s prípravou FM zmlúv, kde základným predpokladom je zmluva medzi klientom a FM poskytovateľom a poskytnutie súboru FM služieb (nie zmluva na jednotlivé FM služby).
3. **STN EN 15221-3: Kvalita vo facility managemente** nadväzuje na jestvujúce normy EN 15221-1 a 15221-2 a na normy kvality ISO 9000. Cieľom tejto časti je poskytnúť návod, ako dosiahnuť, zlepšiť a merať kvalitu služieb facility managementu.
4. **STN EN 15221-4: Kategorizácia, klasifikácia a štruktúry vo facility managemente** – kategorizácia a štruktúra produktov/služieb facility managementu ako i klasifikačný systém vytvárajú predpoklady pre dosiahnutie zabezpečenia efektívnych služieb facility managamantu, a tým aj zefektívnenie podnikania.

5. **STN EN 15221-5: Návod na procesy vo facility managemente** poskytuje návod na analýzu procesov s cieľom mať jasný obraz o organizácii klienta a jeho základných činnostiach ako základ pre vývoj strategického facility managementu. Analýza slúži ako základ pre všetky dôležité rozhodnutia pri špecifikácii úrovne služieb a ich kvality, výber modelu a prípadnej prípravy správnej kategórie dohody o vykonaní služieb.
6. **STN EN 15221-6: Meranie plôch a priestorov vo facility managemente** poskytuje štruktúru s jasnými termínmi, definíciami a princípmi pre meranie podlažných plôch a priestorov v budove. Potrebnosť tejto časti normy je daná faktom, že mnoho krajín EÚ používalo rôzne pravidlá a definície pre ocenenie plôch a priestorov budov. Výsledkom boli údaje, ktoré boli neporovnateľné.

Slovenský ústav technickej normalizácie SÚTN, ktorý je členom CEN pre tvorbu noriem v rámci EÚ, rozhodol o prevzatí schválených noriem prekladom**.**

6.5 LITERATÚRA

DVOŘÁK, Z. – LUSKOVÁ, M. [2011]: *Základný výskum v oblasti kritickej infraštruktúry,* In: Krízový manažment 1/2011, Vedecko-odborný časopis Fakulty špeciálneho inžinierstva Žilinskej univerzity v Žiline, 2011, ISSN 1336-0019, s.47-51.

HOFREITER, L. a kol. [2013]: *Ochrana objektov kritickej dopravnej infraštruktúry,* 1.vyd. Žilina: EDIS – vydavateľstvo ŽU. ISBN 978-80-554-0803-3.

JASENOVEC, J. – DVOŘÁK, Z. [2012]: *Možnosti definovania kritickosti infraštruktúry.* In: Civilná ochrana : revue pre civilnú ochranu obyvateľstva. ISSN 1335-4094. Roč. 14, č. 2 (2012), s. 46-49.

KLUČKA, J. [2012]: *Kritická infraštruktúra a bezpečnosť.* In: Bezpečnostní management a společnost, 2012, str.110 (článok 619-623), ISBN 978-80-7231-871-1.

LOVEČEK, T. – VACULÍK, J. – KITTEL, L. [2012]: *Qualitative approach to evaluation of critical infrastructure security systems.* In: European journal of security and safety [elektronický zdroj]. - ISSN 1338-6131. - 2012. - Vol. 1, no. 1 (2012), online, s.1-11. - http://www.esecportal.eu/journal/index.php/ejss/article/view/3/2.

SEIDL, M. – ŠIMÁK, L. [2012]: *Protection of critical infrastructure.* In: Logistics and transport, No 1(14)/2012, Wroclaw, ISSN 1734-2015, s. 81-102.

Sekcia krízového manažmentu a civilnej ochrany MV SR [2010]: *Analýza tendencií vývoja vnútornej bezpečnosti SR a z nej vyplývajúcich rizík a ohrození.*

Smernica Rady 2008/114/ES z 8. decembra 2008 o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu.

SOMOROVÁ, V. [2006]: *Facility management – metóda efektívneho spravovania budov.* Vydavateľstvo STU Bratislava 2006. ISBN 80-227-2445-9.

SOMOROVÁ, V. [2008]: *STN EN 15221 Facility management*. In: magazín Správa budov.

VIDRIKOVÁ, D.: *Ochrana prvkov kritickej infraštruktúry v cestnej doprave,* In: Logistický monitor, september 2011, ISSN 1336-5851, 7 s.

VYSKOČIL, V. – ŠTRUP, O. [2003]: *Podpůrné procesy a snižování režijních nákladu (Facility management).* Professional Publishing 2003. ISBN 80-86419-45-2.

ŠIMÁK, L. a kol. [2012]: Ochrana kritickej infraštruktúry v sektore doprava (vedecká monografia - separát), 1.vyd. Žilina: EDIS – vydavateľstvo ŽU. ISBN 978-80-554-0625-1.

7 PROTIPOŽIARNA BEZPEČNOSŤ

Protipožiarnu bezpečnosť upravuje najmä Zákon č. 314/2001 Z. z. o ochrane pred požiarmi v znení neskorších predpisov a Vyhláška MV SR č. 121/2002 Z. z. o požiarnej prevencii.

Zákon o ochrane pred požiarmi upravuje:

a) **podmienky na ochranu života a zdravia fyzických osôb, majetku a životného prostredia pred požiarmi,**
b) ustanovuje pôsobnosť orgánov štátnej správy a obcí na úseku ochrany pred požiarmi a hasičských jednotiek pri vykonávaní záchranných prác pri požiaroch, živelných pohromách a iných mimoriadnych udalostiach,
c) povinnosti ústredných orgánov štátnej správy a ďalších ústredných orgánov, obcí, právnických osôb, fyzických osôb – podnikateľov a fyzických osôb na úseku ochrany pred požiarmi,
d) požiadavky na odbornú prípravu a odbornú spôsobilosť na výkon činností na úseku ochrany pred požiarmi,
e) výkon štátnej správy na úseku ochrany pred požiarmi,
f) **druhy hasičských jednotiek,** ich zriaďovanie a povinnosti pri zdolávaní požiarov a vykonávaní záchranných prác pri živelných pohromách a iných mimoriadnych udalostiach,
g) poskytovanie pomoci pri zdolávaní požiarov,
h) úlohy Dobrovoľnej požiarnej ochrany SR a iných občianskych združení na úseku ochrany pred požiarmi,
i) sankcie za porušovanie povinností vyplývajúcich z predpisov o ochrane pred požiarmi.

Zákon o ochrane pred požiarmi definuje:

a) požiar je každé nežiaduce horenie, pri ktorom vznikajú škody na majetku, životnom prostredí alebo ktorého následkom je usmrtená alebo zranená fyzická osoba, alebo uhynuté zviera; požiar je tiež nežiaduce horenie, pri ktorom sú ohrozené životy alebo zdravie fyzických osôb, zvieratá, majetok alebo životné prostredie,
b) 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 a požiarne uzávery,
c) preventívna protipožiarna prehliadka je súhrn úkonov vykonávaných právnickými osobami a fyzickými osobami – podnikateľmi v rámci vnútornej kontroly, zameraných na dodržiavanie predpisov o ochrane pred požiarmi,
d) hasičská stanica je budova s technickým zariadením určená na zabezpečenie stálej služby hasičskej jednotky, umiestnenie hasičskej techniky, vecných prostriedkov a na vykonávanie odbornej prípravy a výcviku,
e) hasičská zbrojnica je budova, ktorá je zvyčajne bez personálu a slúži na uskladnenie technických zariadení, hasičskej techniky a vecných prostriedkov na ochranu pred požiarmi,
f) zásah je súbor činností zameraných na zdolávanie požiarov a vykonávanie záchranných prác pri živelných pohromách a iných mimoriadnych udalostiach na účely záchrany osôb, zvierat a majetku alebo ochrany životného prostredia,
g) objekt je stavba alebo súbor stavieb, zariadení a priestorov, ktoré sa užívajú na účel, na ktorý boli určené.

Vyhláška MV SR o požiarnej prevencii definuje:

1. **Činnosti so zvýšeným nebezpečenstvom vzniku požiaru** sú činnosti, ktoré vytvárajú zvýšené riziko možnosti vzniku požiaru pri výrobe, spracúvaní, používaní alebo pri skladovaní horľavých látok, najmä:
   a) prevádzkovanie, odstavovanie a spúšťanie výroby v technologických zariadeniach obsahujúcich horľavé látky,
   b) údržba a opravy technických a technologických zariadení obsahujúcich horľavé látky a odstraňovanie ich poruchových stavov,
   c) zváranie, tepelné delenie a ďalšie spôsoby spracúvania kovov, pri ktorých sa používa zváracie, brúsiace alebo iskriace zariadenie nezávisle od stupňa automatizácie na miestach s možnosťou vzniku požiaru alebo výbuchu,
   d) lepenie horľavých podlahových a strešných krytín, obkladov stien a stropov pomocou ohňa, elektrotepelných spotrebičov a zariadení alebo horľavých lepidiel a odstraňovanie starých náterov pomocou tepelných spotrebičov a zariadení,
   e) nevyhnutná manipulácia s otvoreným ohňom na miestach s možnosťou vzniku požiaru,
   f) spaľovanie horľavých látok na voľnom priestranstve,
   g) zber obilnín, ich pozberová úprava a skladovanie objemových krmovín a slamy.
2. **Miesta so zvýšeným nebezpečenstvom vzniku požiaru** sú miesta, v ktorých sa nachádzajú horľavé látky za takých podmienok, že vytvárajú zvýšené riziko možnosti vzniku požiaru. K týmto miestam patria najmä priestory, v ktorých sa:
   a) používajú, spracúvajú alebo skladujú za bežných prevádzkových podmienok pevné horľavé látky, ktoré svojou veľkosťou, formou, množstvom a podmienkami uloženia podstatne zvyšujú intenzitu a šírenie požiaru; na stavebné konštrukcie z horľavých látok a na horľavé predmety tvoriace zariadenia miestností sa toto ustanovenie nevzťahuje,
   b) vyrábajú, používajú, spracúvajú alebo skladujú prevzdušnené alebo suché steblové horľavé látky,
   c) usadzuje pri výrobe alebo pri manipulácii horľavý prach v súvislej vrstve schopnej šíriť požiar alebo pri výrobe, prípadne pri manipulácii vzniká horľavý prach v takej miere, že je trvalo v ovzduší a vznik výbušnej koncentrácie nemožno vylúčiť,
   d) vyrábajú, používajú, spracúvajú, prečerpávajú, dopravujú alebo skladujú horľavé kvapaliny,
   e) vyrábajú, používajú, spracúvajú, prečerpávajú, dopravujú alebo skladujú horľavé plyny alebo horenie podporujúce plyny,
   f) vyrábajú, spracúvajú alebo skladujú výbušniny alebo horľavé toxické látky,
   g) používajú látky, ktoré sa pri styku so vzduchom alebo s vodou, alebo vzájomne medzi sebou môžu vznietiť alebo môžu uvoľniť horľavé pary alebo plyny, ktoré môžu v zmesi so vzduchom vytvoriť výbušnú zmes,
   h) používa pri výrobe, používaní alebo pri spracúvaní horľavých látok otvorený oheň.
3. **Miesta s možnosťou vzniku požiaru alebo výbuchu** sú miesta, v ktorých sa vyskytujú horľavé látky, výrobky alebo výbušniny, a miesta, v ktorých sa môže vyskytnúť ich výbušná koncentrácia.
4. **Čas zvýšeného nebezpečenstva vzniku požiaru** je obdobie, ktoré vyhlási okresné riaditeľstvo Hasičského a záchranného zboru pre celé územie okresu alebo časť územia okresu. Dôvodom na vyhlásenie času zvýšeného nebezpečenstva vzniku požiaru je najmä:
   a) suché a teplé počasie trvajúce najmenej päť po sebe nasledujúcich dní alebo
   b) zvýšený výskyt požiarov lesa alebo trávnatých porastov v priebehu troch po sebe nasledujúcich dní, alebo

c) ak požiarne nebezpečenstvo v lesoch na príslušnom území dosiahlo aspoň stupeň vysoké požiarne nebezpečenstvo v lesoch podľa stanovenia stupňa požiarneho nebezpečenstva v lesoch Slovenským hydrometeorologickým ústavom.

Právne normy, ktoré upravujú **ochranu pred požiarmi** sú pomerne rozsiahle, patria sem najmä:.

- Zákon č. 314/2001 Z. z. o ochrane pred požiarmi v znení neskorších predpisov.
- Zákon č. 315/2001 Z. z. o hasičskom a záchrannom zbore v znení neskorších predpisov.
- Vyhláška MV SR č. 121/2002 Z. z. o požiarnej prevencií v znení neskorších predpisov.
- Vyhláška MV SR č. 123/2002 Z. z., ktorou sa ustanovuje katalóg činností v hasičskom a záchrannom zbore.
- Vyhláška MV SR č. 611/2006 Z. z. o hasičských jednotkách.
- Vyhláška MV SR č. 719/2002 Z. z., ktorou sa ustanovujú vlastnosti, podmienky prevádzkovania a zabezpečenie pravidelnej kontroly prenosných hasiacich prístrojov a pojazdných hasiacich prístrojov.
- Vyhláška MV SR č. 726/2002 Z. z., ktorou sa ustanovujú vlastnosti elektrickej požiarnej signalizácie, podmienky jej prevádzkovania a zabezpečenia jej pravidelnej kontroly.
- Vyhláška MV SR č. 55/2002 Z. z., ktorou sa určujú sídla a územné obvody krajských riaditeľstiev Hasičského a záchranného zboru, okresných riaditeľstiev Hasičského a záchranného zboru a sídla hasičských staníc v znení neskorších predpisov.
- Vyhláška MV SR č. 258/2007 Z. z., o požiadavkách na protipožiarnu bezpečnosť pri skladovaní, ukladaní a pri manipulácii s tuhými horľavými látkami.
- Vyhláška MV SR č. 124/2000 Z. z., ktorou sa ustanovujú zásady požiarnej bezpečnosti pri činnostiach s horľavými plynmi a horenie podporujúcimi plynmi.
- Vyhláška MV SR č. 478/2008 Z. z. o vlastnostiach, konkrétnych podmienkach prevádzkovania a zabezpečenia pravidelnej kontroly požiarneho uzáveru.
- Vyhláška MV SR č. 142/2004 Z. z. o protipožiarnej bezpečnosti pri výstavbe a pri užívaní prevádzkarne a iných priestorov, v ktorých sa vykonáva povrchová úprava výrobkov náterovými látkami.
- Vyhláška MV SR č. 401/2007 Z. z o technických podmienkach a požiadavkách na protipožiarnu bezpečnosť pri inštalácii a prevádzkovaní palivového spotrebiča, elektrotepelného spotrebiča a zariadenia ústredného vykurovania a pri výstavbe a používaní komína a dymovodu a o lehotách ich čistenia a vykonávania kontrol.
- Vyhláška MV SR č. 96/2004 Z. z., ktorou sa ustanovujú zásady protipožiarnej bezpečnosti pri manipulácii a skladovaní horľavých kvapalín, ťažkých vykurovacích olejov a rastlinných a živočíšnych tukov a olejov.
- Vyhláška MV SR č. 94/2004 Z. z, ktorou sa ustanovujú technické požiadavky na protipožiarnu bezpečnosť pri výstavbe a pri užívaní stavieb v znení neskorších predpisov.
- Vyhláška MV SR č. 699/2004 Z. z. o zabezpečení stavieb vodou na hasenie požiarov v znení neskorších predpisov.

Protipožiarna bezpečnosť stavieb

Protipožiarna bezpečnosť stavieb predstavuje schopnosť stavebných objektov zabrániť stratám na životoch a zdraví osôb a stratám na majetku v prípade požiaru. Každá právnická osoba a fyzická osoba podnikateľ má povinnosti na úseku ochrany pred požiarmi podľa § 4 písmeno k) Zákona č. 314/2001 Z. z. o ochrane pred požiarmi v znení neskorších predpisov zabezpečiť, aby sa pri vypracúvaní projektovej dokumentácie stavieb a ich užívaní riešili a dodržiavali požiadavky protipožiarnej bezpečnosti stavieb.

Stavebný objekt z hľadiska protipožiarnej bezpečnosti musí:

- zabezpečiť na určitý čas požadovanú stabilitu a nosnosť,
- umožniť bezpečnú evakuáciu osôb,
- umožniť odvod tepla a splodín horenia,
- zabrániť šíreniu požiaru medzi požiarnymi úsekmi v stavbe, alebo na inú stavbu,
- umožniť účinný a bezpečný zásah hasičskej jednotke.

Protipožiarna bezpečnosť stavieb sa dosahuje urbanistickým riešením, dispozičným riešením, konštrukčným riešením, materiálovým riešením a požiarnymi bezpečnostnými opatreniami.

7.1 LITERATÚRA

Ochrana pred požiarmi a protipožiarna bezpečnosť: (aktualizované predpisy). Bratislava: Epos, 2006. ISBN 80-8057-672-6.

OSVALD, A. [2005]: *Ochrana pred požiarmi.* Zvolen. Technická univerzita, ISBN 80-22 81-493-8.

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.

8 BEZPEČNOSŤ PRÁCE

Jedným zo základných ľudských práv, ktoré sú zakotvené v Listine základných ľudských práv a slobôd, je právo na **ochranu zdravia** a uspokojivé **pracovné podmienky** *(Sabo, 2010)*.

Príčin, ktoré vedú k ohrozeniu zdravia pri práci je viac. Niektoré tkvejú v samotnom ***charaktere práce,*** a preto im nemožno v pracovnom procese úplne zabrániť, ale zväčša ich spôsobuje ***ľudský činiteľ*** a jeho konanie, resp. jeho nečinnosť. Preto sa musí v protiúrazovej a v protihavarijnej prevencii pri všetkých činnostiach človeka venovať ustavičná pozornosť výchove zamestnancov k bezpečnosti práce, ale najmä k osvojovaniu zásad bezpečnosti práce.

V súčasnosti sa vo vyspelých krajinách považuje organizácia a riadenie v oblasti bezpečnosti práce za neoddeliteľnú súčasť organizovania a riadenia výrobných a pracovných procesov. Porucha, havária, požiar zariadenia (objektu), či úraz alebo iné poškodenie zdravia zamestnanca sa považuje za následok nezvládnutia riadenia výrobného alebo pracovného procesu zamestnávateľom.

Porucha vo vzťahoch človeka techniky a pracovného prostredia môže vyústiť do nehody, ktorou sa spravidla rozumie jednorazová nepredvídaná udalosť s následkom poškodenia zdravia alebo smrti človeka. Príčiny, ktoré spôsobujú vznik nehody, sa v podstate dajú rozdeliť do dvoch základných skupín:

- **objektívne príčiny**, spôsobené ***technikou,***
- **subjektívne** príčiny, spôsobené ***človekom***, t. j. predpokladá sa, že nehoda vznikne v interakcii človeka, techniky a pracovného prostredia.

Bezpečnosť práce je ***stav pracoviska***, na ktorom je vysoká miera istoty, že pri dodržaní pravidiel (požiadavky predpisov pre bezpečnosť práce, hygienu, technologické a pracovné postupy a pod.) uplatňovaných pre príslušné pracovisko a pracovný proces a bez pôsobenia nepredvídateľných vonkajších vplyvov bude vylúčený alebo znížený vznik ohrozenia zdravia alebo života osôb či poškodenia alebo zničenia ich majetku. Bezpečnosť práce v organizácii znamená úzku ***spojitosť bezpečnosti a ochrany zdravia pri práci s bezpečnosťou prevádzky.***

Človek na všetkých stupňoch svojho vývoja používa a rozvíja techniku vždy v konkrétnych podmienkach a vzťahoch, pričom je rozhodujúce pracovné prostredie a interakcia človeka a techniky v pracovnom procese. V súlade s modernými teóriami vied o práci, ktorých platnosť prax náležite potvrdila, je **systém ľudskej práce** tvorený v jednote jej troch základných podsystémov, teda v jednote funkcií ***človeka, technických prostriedkov*** a ***pracovného prostredia.***

Systém bezpečnosti práce v organizácii potom tvorí subsystém:

1. **Bezpečnosť a ochrana zdravia pri práci:**
   a) **bezpečnosť práce,**
   b) **ochrana zdravia pri práci,**
2. **Bezpečnosť technických zariadení,**
3. **Bezpečnosť pracovného prostredia a pracovných podmienok (hygiena práce).**

Základnou podmienkou primeranej úrovne bezpečnosti práce je vnútorná vyváženosť stavu a vývoja jej subsystémov, teda bezpečnosti pri práci, bezpečnosti technických zariadení a bezpečnosti pracovného prostredia.

Ak niektorý z uvedených subsystémov nedosahuje vyžadovanú úroveň, je nevyhnutné, aby ostatné subsystémy, ale najmenej jeden z nich, zvýšenou účinnosťou zachoval rovnocennú úroveň bezpečnosti práce celého systému. Týmto spôsobom sa môže dosiahnuť primeraná úroveň bezpečnosti práce, napr. osobnými ochrannými pracovnými prostriedkami, ktoré svojím barierovým pôsobením znižujú, prípadne odstraňujú pôsobenie zdraviu škodlivých faktorov, avšak tieto prostriedky okrem svojej ochrannej funkcie obvykle sťažujú interakciu človeka s nástrojmi, pracovnými predmetmi a materiálom, sťažujú interpersonálnu komunikáciu a vo všeobecnosti pôsobia obťažujúco.

Bezpečnosť práce, ochrana človeka v pracovnom procese a na pracovisku, zachovanie života a zdravia a práceschopnosti človeka, ochrana životného a pracovného prostredia, ochrana majetku a iných ekonomických hodnôt si vyžaduje vytvorenie a udržiavanie ***systému legislatívnych, sociálnych, ekonomických, organizačných, technických, výchovných, vzdelávacích, zdravotných a hygienických opatrení.***

Legislatívne opatrenia predstavujú tvorbu, vydávanie a aktualizáciu zákonov, vyhlášok, predpisov a noriem a patria k rozhodujúcim funkciám štátu. Súčasťou právnej nadstavby musí byť aj sústava zákonov, nariadení vlády SR, vyhlášok, predpisov a noriem určujúcich požiadavky bezpečnosti práce, ktoré možno determinovať ako tzv. „***bezpečnostné predpisy***“. Za bezpečnostný predpis sa považuje každý predpis, obsahujúci záväzné ustanovenia (zákazy, príkazy, pokyny, limity, parametre, kritériá, postupy a pod.), ktoré majú za cieľ zaistenie bezpečnosti práce.

Hlavným právnym dokumentom určujúcim univerzálne povinnosti v oblasti bezpečnosti práce je Zákon č. 124/2006 Z. z. o bezpečnosti a ochrane zdravia pri práci a o zmene a doplnení niektorých zákonov. Ďalej sú to:

- Ústava Slovenskej republiky, čl. 36,
- Listina Základných práv a slobôd,
- Zákonník práce, § 147,
- Zákon č. 355/2007 Z. z. o ochrane, podpore a rozvoji verejného zdravia v platnom znení,
- Zákon č. 125/2006 Z. z. o inšpekcii práce a o zmene a doplnení zákona č. 82/2005 Z. z. o nelegálnej práci a nelegálnom zamestnávaní,
- Nariadenie vlády SR č. 387/2006 Z. z. o požiadavkách na zaistenie bezpečnostného a zdravotného označenia pri práci,
- Nariadenie vlády SR č. 356/2006 Z. z. o ochrane zdravia zamestnancov pred rizikami súvisiacimi s expozíciou karcinogénnym a mutagénnym faktorom pri práci,
- Nariadenie vlády SR č. 391/2006 Z. z. o minimálnych bezpečnostných a zdravotných požiadavkách na pracovisko,
- Nariadenie vlády SR č. 392/2006 Z. z. o minimálnych bezpečnostných a zdravotných požiadavkách pri používaní pracovných prostriedkov,
- Nariadenie vlády SR č. 393/2006 Z. z. o minimálnych požiadavkách na zaistenie bezpečnosti a ochrany zdravia pri práci vo výbušnom prostredí,
- Nariadenie vlády SR č. 395/2006 Z. z. o minimálnych požiadavkách na poskytovanie a používanie osobných ochranných pracovných prostriedkov,
- Ďalšie právne normy.

Sociálne opatrenia predstavujú súhrn opatrení, resp. činností štátu, podnikateľských subjektov, resp. zamestnávateľov zameraných na sústavné zlepšovanie podmienok bezpečnosti práce, na udržiavanie a podporu všestranného rozvoja zamestnancov. Sociálne opatrenia sa realizujú prostredníctvom ***pracovnoprávnych opatrení, sociálnym zabezpečením*** pri chorobe a pri pracovnom úraze, budovaním ***objektov sociálnej starostlivosti*** a pod.

Ekonomické opatrenia sú opatrenia, ktoré sledujú využitie ***ekonomických nástrojov*** v prospech ***zvyšovania úrovne bezpečnosti práce.*** Za optimálnych podmienok by sústava ekonomických nástrojov mala pôsobiť na zamestnávateľov tak, aby starostlivosť o bezpečnosť práce bola pre zamestnávateľov a ich zamestnancov výhodnejšia ako porušovanie predpisov bezpečnosti práce, či nedôslednosť pri plnení ich požiadaviek. Ekonomické nástroje pôsobiace v sústave riadenia hospodárskych subjektov sú orientované na zvyšovanie efektívnosti výroby, znižovanie energetickej a materiálovej náročnosti a pod. Pri takejto orientácii sústavy ekonomických nástrojov je ich vplyv na tvorbu podmienok bezpečnosti práce v podstate sekundárny a môže byť pozitívny i negatívny. Jednou z foriem takto pôsobiacich ekonomických nástrojov je ustanovenie inštitútu osobitného ***úrazového poistenia.***

Organizačné opatrenia možno rozdeliť do troch zásadných skupín.

1. **Tvorba potrebných organizačných dokumentov bezpečnosti práce** na všetkých stupňoch riadenia podnikateľských subjektov, napr. ***organizačný poriadok, pracovný poriadok*** atď. V záujme plnenia úloh podnikateľského subjektu na úseku bezpečnosti práce musí tento vypracovať aj ďalšie potrebné dokumenty, napr. ***politiku bezpečnosti prace, inštitút bezpečnostného technika, plány ozdravných opatrení, protihavarijné plány*** a pod.
2. **Vytvorenie potrebných personálnych predpokladov** na výkon všetkých činností na úseku bezpečnosti práce.
3. **Vytvorenie nevyhnutných materiálnych predpokladov** pre oblasť bezpečnosti práce.

Výchovné a vzdelávacie opatrenia sú obsiahnuté v starostlivosti zamestnávateľa o ***výchovu a vzdelávanie svojich zamestnancov***. Výchova k bezpečností práce je špecifický druh výchovy zameraný na vytváranie uvedomelého vzťahu zamestnancov k bezpečnosti práce, ale predovšetkým k ochrane vlastného zdravia a zdravia spolupracovníkov. V základnom členení v podmienkach podnikateľských subjektov môžeme **školenia** rozdeliť na ***vstupné a opakované.***

Vstupné školenia o bezpečnosti práce sa vykonávajú pri nástupe nových zamestnancov alebo pri preradení zamestnancov na inú kvalitatívne odlišnú prácu ešte pred samotným vykonávaním pracovných úloh. Ich cieľom je získať všetky potrebné vedomosti a návyky, ktoré umožnia predísť vzniku nežiaducich udalostí v pracovnom procese a následnému možnému poškodeniu zdravia, vzhľadom na charakter a podmienky práce, ktorú zamestnanec bude vykonávať.

Opakované školenia sa vykonávajú plánovite, systematicky a diferencovane podľa rizikovosti vykonávanej práce a ich cieľom je regenerovanie predtým získaných vedomostí a ich doplnenie o nové aktuálne informácie.

Z hľadiska štruktúry súboru školených osôb možno školenia deliť do štyroch základných skupín:

1. **Školenia vedúcich zamestnancov** o základných zákonných opatreniach, cieľom je osvojiť si zo strany vedúcich zamestnancov potrebné základné informácie súvisiace s bezpečnosťou práce na nimi riadenom úseku.
2. **Školenia špecializovaných zamestnancov pre bezpečnosť práce,** ako sú ***bezpečnostní technici, skúšobní technici technických zariadení, špecialisti pre škodliviny*** a pod., sú predmetom osobitnej oblasti vzdelávania.
3. **Školenia zamestnancov odborných profesií,** u ktorých sú bezpečnostnými predpismi vyžadované predpísané kvalifikačné požiadavky:
   - zamestnanci ***vykonávajúci odborné a technicky náročné práce*** (elektrotechnici, zvárači, viazači bremien a pod.),
   - zamestnanci ***obsluhujúci určené technické zariadenia*** (tlakové, plynové, zdvíhacie dopravné zariadenia a pod.).

4. **Školenia ostatných zamestnancov** vykonávajúcich rôzne profesie (remeselníkov, robotníkov, pracovníkov administratívy a pod.), ktorí sú pri práci v interakcii s pracovnými a výrobnými prostriedkami vystavení pôsobeniu škodlivých faktorov práce, resp. pracovného procesu. Osobitne výhodnou súčasťou tohto školenia je ***praktická príprava zamestnancov na mieste výkonu práce,*** vrátane nácviku odvracania následkov možných rizikových situácií.

Organizácia bezpečnosti práce v podmienkach vyspelej civilizovanej spoločnosti sa stala neoddeliteľnou súčasťou organizácie práce a je dôležitým funkčným nástrojom zvyšovania kultúry postavenia človeka v pracovnom procese. Úlohy bezpečnosti práce nemožno v štruktúre práce redukovať len na faktory technické a organizačné, pretože pri pracovných operáciách vykonávaných technickými prostriedkami sa radí **faktor psychiky človeka** medzi rozhodujúce nástroje riadenia pracovného procesu.

Človek sa vyznačuje dvoma určujúcimi oblasťami psychickej regulácie pracovného procesu:

1. operácie s informáciami v danom systéme práce, ktoré sú základným predpokladom funkcií človeka v systéme práce. Informačné a komunikačné funkcie sú podriaďované potrebám systému človeka, techniky a pracovného prostredia a
2. spätné väzby, na základe ktorých človek ovplyvňuje systém práce a prijíma informácie o realizácii jednotlivých akcií. Hlavná úloha pôsobenia človeka spätnými väzbami na systém práce spočíva v signalizácii (oznamovaní) výsledného efektu výstupných činností človeka na jeho vstupné činnosti pre prípadnú korekciu riadenia pracovných procesov.

Na správanie človeka v pracovnom procese nepochybne rušivo pôsobia aj **faktory netechnického charakteru,** ako napr. monotónna práca, mikroklimatické podmienky a rôzne iné zdraviu škodlivé faktory vznikajúce v pracovnom procese.

Človek je v pracovnom procese ovplyvňovaný aj **psychickými a sociálnymi činiteľmi**, a to najmä psychickou atmosférou prejavujúcou sa najmä v psychologických a sociálnych vzťahoch na pracovisku, či v pracovnom procese. V zjednodušených súvislostiach sú sociálne a psychologické väzby vertikálne, napr. vzťahy medzi vedúcim zamestnancom a zamestnancom, alebo horizontálne, napr. vzťahy medzi jednotlivými zamestnancami v pracovnom kolektíve. Narušené sociálne a psychologické vzťahy na pracovisku prejavujúce sa v podobe nekonštruktívnych sporov medzi jednotlivcami vedú prirodzene aj k takým poruchám v správaní človeka pri práci, ktoré môžu spôsobiť nehodu s následným možným pracovným úrazom.

Technické faktory a s nimi súvisiace faktory pracovného prostredia pôsobia **menej negatívne** na bezpečnosť človeka ako faktory **sociálne a psychologické.**

Spôsobilosť človeka na prácu (práceschopnosť) sa prejavuje v troch fázach, vo všetkých troch fázach sa zistilo, že o spoľahlivosti správania človeka v pracovnom procese rozhodujú vo veľkej miere sociálne a psychologické faktory.

Prvú fázu práceschopnosti človeka, tzv. „***zapracovanie***“, možno charakterizovať ako obdobie „hromadenia pracovných potenciálov", v ktorej sa uskutočňuje funkčná prestavba a ustaľovanie dynamického stereotypu človeka. Táto fáza je charakterizovaná veľkým počtom chýb pri vykonávaní pracovných operácií, čo znamená, že spoľahlivosť človeka v pracovnom procese je veľmi malá. Rýchlosť zapracovania je determinovaná sociálnymi a psychologickými vzťahmi a tieto vzťahy ovplyvňujú pripravenosť človeka na prácu.

Druhú fázu práceschopnosti človeka možno charakterizovať ako obdobie „***stabilizácie dynamického stereotypu***“ a činnosť človeka nadobúda harmonickú jednotu a celistvosť. Prestavba pracovných funkcií zladením rytmu a tempa nie je závislá len od psychologických faktorov pracovného procesu. Stálosť a spoľahlivosť vykonávania pracovných operácií sa v stereotype činností zlaďuje so sociálnymi a psychologickými vzťahmi v pracovnej skupine, ktoré určujú aj rytmus a tempo pracovných operácií.

Tretia fáza práceschopnosti človeka je charakterizovaná ako obdobie „***poklesu spoľahlivosti a efektívnosti výkonu práce***“, ubúda práceschopnosť a narastá únava. Narastanie únavy je dôsledkom premien najmä funkčného stavu centrálnej nervovej sústavy. Ak podstatnými v týchto zmenách sú procesy útlmu, tak potom sociálne a psychologické vzťahy v pracovnej skupine môžu byť významným stimulujúcim faktorom práce.

Faktory, ktoré rozhodujú o spoľahlivosti práce človeka, sú dané druhom pracovných operácií, pripravenosťou nervového systému a psychickou vybavenosťou človeka. Tieto faktory sú determinované sociálnymi a psychologickými vzťahmi v pracovnej skupine a významnou mierou určujú spoľahlivosť človeka vo všetkých troch fázach jeho práceschopnosti.

8.1 ZLOŽKY SYSTÉMU BEZPEČNOSTI PRÁCE

8.1.1 Bezpečnosť a ochrana zdravia pri práci

Bezpečnosť a ochrana zdravia pri práci (BOZP) je oblasť manažérstva zameraná na bezpečnosť a ochranu zdravia ľudí v priebehu pracovného procesu. **Starostlivosť o BOZP** je nezastupiteľnou ***povinnosťou a zodpovednosťou zamestnávateľa a všetkých vedúcich pracovníkov.***

Najrozsiahlejšiu časť pracovného práva EÚ tvorí problematika BOZP. Medzinárodná organizácia práce *(International Labour Organization, ILO)* prijala komplexný **Dohovor o bezpečnosti a ochrane zdravia pri práci a pracovnom prostredí.**

Základom je **Smernica Rady ES č. 89/391/EHS o opatreniach na zlepšenie BOZP zamestnancov**. Právne normy pre BOZP upravujú práva a povinnosti zamestnávateľov, štátneho dozoru, práva a povinnosti zamestnancov a ostatných orgánov spoločenskej kontroly. Prioritnou zásadou BOZP je dôraz na prevenciu.

BOZP *zahŕňa všetky stránky ochrany zamestnancov súvisiace s prácou* – napríklad fyzickú a psychickú pohodu, sociálnu ochranu, pracovné podmienky, pracovné vzťahy, hygienické podmienky, sociálne vybavenie pracovísk.

BOZP predstavuje aj **stav pracovných podmienok *eliminujúcich vplyv nebezpečných a škodlivých faktorov pracovného procesu alebo prostredia na zamestnancov*.** V praxi je celý systém bezpečnosti a ochrany zdravia pri práci zameraný nielen na zamedzenie poškodenia zdravia pracujúcich, ale aj na podporu zdravia zamestnancov, zvyšovanie alebo regeneráciu úrovne zdravia pri práci a podporu práceschopnosti a pohody pri práci, tak aby to zodpovedalo prijateľným štandardom.

Bezpečnosť a ochrana zdravia pri práci zahŕňa v sebe dve funkcie, ktorými sú:

a) bezpečnosť práce – čiastková kategória bezpečnosti práce, ktorá sleduje vylúčenie alebo zníženie ohrozenia osôb pri práci, spravidla je orientovaná na konkrétnu pracovnú činnosť, miesto, či pracovisko, predstavuje ***súbor preventívnych opatrení na predchádzanie pracovným úrazom.***

b) ochrana zdravia pri práci – ***súbor preventívnych opatrení na predchádzanie vzniku chorôb z povolania, profesionálnych otráv a iných poškodení zdravia z práce,*** v mnohom sa prekrýva s hygienou práce.

V ďalších odsekoch sú uvedené niektoré z**ákladné pojmy z bezpečnosti a hygieny práce** *(Lorko, Lajčinová, 2009).*

Cieľom BOZP je **vytvoriť bezpečné a zdravé pracovné prostredie,** preto sa zameriava na systematické vyhľadávanie a vyhodnocovanie ***rizík pri práci,*** nech ide o samotné pracovisko, ergonómiu, pracovné nástroje, zariadenia, prostriedky a pomôcky (osobné ochranné pracovné prostriedky) alebo o hygienu pracovného prostredia.

Podniková politika BOZP je podniková stratégia v oblasti bezpečnosti a ochrany zdravia pri práci. Vyjadruje postoj vedenia podniku k starostlivosti o bezpečnosť a zdravie zamestnancov a základné zámery a smery pôsobenia organizácie v tejto oblasti. Má obsahovať komplexné riešenie skutočných problémov podniku a zaisťovať ochranu zdravia všetkých zamestnancov. Základným cieľom politiky BOZP má byť – v súlade so základnými povinnosťami zamestnávateľa v tejto oblasti – stále zlepšovanie pracovných podmienok a úrovne BOZP vyvolané zvýšením výkonnosti systému riadenia BOZP.

Bezpečnosť je vlastnosť objektu neohrozovať osoby ani okolie. **Nebezpečenstvo** je stav alebo vlastnosť faktora pracovného procesu a pracovného prostredia, ktoré môžu poško-

diť zdravie zamestnanca. **Neodstrániteľné nebezpečenstvo (ohrozenie)** je také nebezpečenstvo (ohrozenie), ktoré podľa súčasných vedeckých a technických poznatkov nemožno vylúčiť ani obmedziť. **Nebezpečná udalosť** je udalosť, pri ktorej bola ohrozená bezpečnosť alebo zdravie zamestnanca, ale nedošlo k poškodeniu jeho zdravia.

Bezpečnosť a hygiena práce (ochrana zdravia pri práci) bolo by vhodné chápať komplexne, ako dve stránky toho istého problému. Poškodením zdravia je každý pracovný úraz, choroba z povolania i otrava, ide o poškodenie zdravia, stratu práceschopnosti. Teda ak bezpečnosti pri práci necháme pôvodný význam, hygiene práce (ochrane zdravia pri práci) možno prisúdiť strategickú cieľovú funkciu.

Zdravotné a hygienické opatrenia, orientované v prospech bezpečnosti práce ako súčasť jej systému, majú najmä ***preventívnu funkciu***. Významným preventívnym zdravotníckym opatrením je posudzovanie zdravotnej spôsobilosti zamestnanca pred nástupom do práce alebo pri preradení na inú prácu. Je nevyhnutné posudzovať zdravotnú spôsobilosť vo vzťahu k rizikám vykonávanej práce, či činnosti. Zodpovedným posúdením zdravotnej spôsobilosti sa zabezpečí optimálny súlad medzi zdravotným stavom zamestnanca, jeho celkovou dispozíciou a špecifickými požiadavkami práce, a to nielen z anatomického a fyziologického hľadiska, ale aj psychofyziologickej pripravenosti.

Vykonávanie **preventívnych periodických zdravotných prehliadok** je súčasťou zdravotníckych opatrení na pracoviskách, kde sú zamestnanci vystavení expozícii zdraviu škodlivých faktorov. Ich cieľom je zistiť, či pôsobenie zdraviu škodlivých faktorov nezanechalo na zdraví postihnutých zamestnancov patologické zmeny.

Do sústavy zdravotníckych opatrení patrí aj určovanie ***osobitných režimov práce*** pri činnostiach, kde sa vyskytujú zdraviu škodlivé faktory, ktoré nie je možné eliminovať bezpečnostnými opatreniami, napr. osobnými ochrannými pracovnými prostriedkami.

Ochrana zdravia pri práci predstavuje ***systém opatrení vyplývajúcich z právnych predpisov, organizačných opatrení, technických opatrení, zdravotníckych opatrení a sociálnych opatrení*** zameraných na utváranie pracovných podmienok zaisťujúcich BOZP, zachovanie zdravia a pracovnej schopnosti zamestnanca, ochrana práce je neoddeliteľnou súčasťou pracovnoprávnych vzťahov.

Zákon č. 124/2006 Z. z. o bezpečnosti a ochrane zdravia pri práci a o zmene a doplnení niektorých zákonov ustanovuje všeobecné zásady **prevencie** a základné podmienky na **zaistenie bezpečnosti a ochrany zdravia pri práci** a na vylúčenie rizík a faktorov podmieňujúcich vznik pracovných úrazov, chorôb z povolania a iných poškodení zdravia z práce.

Prevencia je systém opatrení plánovaných a vykonávaných vo všetkých oblastiach činnosti zamestnávateľa, ktoré sú zamerané na vylúčenie alebo obmedzenie rizika a faktorov podmieňujúcich vznik pracovných úrazov, chorôb z povolania a iných poškodení zdravia z práce, a určenie postupu v prípade bezprostredného a vážneho ohrozenia života alebo zdravia zamestnanca.

Zamestnávateľ je povinný uplatňovať všeobecné zásady prevencie pri vykonávaní opatrení nevyhnutných na zaistenie bezpečnosti a ochrany zdravia pri práci vrátane zabezpečovania informácií, vzdelávania a organizácie práce a prostriedkov.

Všeobecné **zásady prevencie** podľa Zákona č. 124/2006 Z.z. o bezpečnosti a ochrane zdravia pri práci sú nasledujúce:

a) vylúčenie nebezpečenstva a z neho vyplývajúceho rizika,
b) posudzovanie rizika, ktoré nemožno vylúčiť, najmä pri výbere a počas používania pracovných prostriedkov, materiálov, látok a pracovných postupov,

c) vykonávanie opatrení na odstránenie nebezpečenstiev v mieste ich vzniku,
d) uprednostňovanie kolektívnych ochranných opatrení pred individuálnymi ochrannými opatreniami,
e) nahrádzanie prác, pri ktorých je riziko poškodenia zdravia, bezpečnými prácami alebo prácami, pri ktorých je menšie riziko poškodenia zdravia,
f) prispôsobovanie práce schopnostiam zamestnanca a technickému pokroku,
g) zohľadňovanie ľudských schopností, vlastností a možností najmä pri navrhovaní pracoviska, výbere pracovného prostriedku, pracovných postupov a výrobných postupov s cieľom vylúčiť alebo zmierniť účinky škodlivých faktorov práce, namáhavej práce a jednotvárnej práce na zdravie zamestnanca,
h) plánovanie a vykonávanie politiky prevencie zavádzaním bezpečných pracovných prostriedkov, technológií a metód organizácie práce, skvalitňovaním pracovných podmienok vzhľadom na faktory pracovného prostredia a prostredníctvom sociálnych opatrení,
i) vydávanie pokynov na zaistenie bezpečnosti a ochrany zdravia pri práci.

Zamestnávateľ je okrem prevencie povinný vykonávať opatrenia nevyhnutné na zaistenie bezpečnosti a ochrany zdravia pri práci riadne a včas tak, aby sa splnil ich účel, a zabezpečovať, aby tieto opatrenia boli použiteľné a zamestnancovi prístupné.

Špecifikácia OHSAS 18001 ***(****Occupational Health and Safety Assessment Specification****)*** je rad noriem pre hodnotenie a posudzovanie **ochrany zdravia a bezpečnosti práce,** ktorej predmetom je pomôcť organizáciám vytvárať **politiku zdravia a bezpečnosti práce** s cieľom ochranu zdravia a bezpečnosť práce zlepšovať. Je to dokument pre posudzovanie BOZP, ktorý nie je priamo súčasťou skupiny medzinárodných štandardov vydávaných ISO, ale svojím charakterom a dopadom je im podobná.

Zavedenie normy pomáha zlepšovať systém bezpečnosti práce a ochrany zdravia pri práci na všetkých úrovniach organizácie. Pomáha systematicky obmedzovať pracovné riziká, ktoré môžu ohroziť bezpečnosť a zdravie všetkých osôb ovplyvňovaných činnosťami, výrobkami alebo službami organizácie. Nepriamo tým pomáha obmedziť výskyt chorôb z povolania a pracovných úrazov, minimalizovať náklady spojené s nehodami a tým zvyšovať **výkonnosť organizácie.**

Zároveň je pomocou certifikátu OHSAS 18001 možné preukázať splnenie zákonnej povinnosti v oblasti bezpečnosti práce. Norma je použiteľná vo všetkých sektoroch bezpečnosti.

Medzi prínosy dobrej úrovne BOZP možno zaradiť:
- nižšie náklady na úrazy,
- riadené výdaje na poistenie,
- motivácia a oddanosť zamestnancov,
- produktivita,
- podniková sociálna zodpovednosť,
- získanie a udržanie zákazníkov,
- dôvera investora,
- hodnota značky a dôvera v ňu.

8.1.2 Bezpečnosť technických zariadení

Významné miesto v zložitom súbore opatrení bezpečnosti práce majú opatrenia na zaistenie **bezpečnosti technických zariadení, technológií a objektov.** Uvedené opatrenia riešia najmä ***technickú bezpečnosť a prevádzkovú spoľahlivosť technických zariadení***, avšak do tohto súboru opatrení sa organicky začleňuje aj ***bezpečnosť prevádzkových objektov.***

Systém je vecne i priestorovo ohraničený objekt tvoriaci relatívne samostatný súbor.

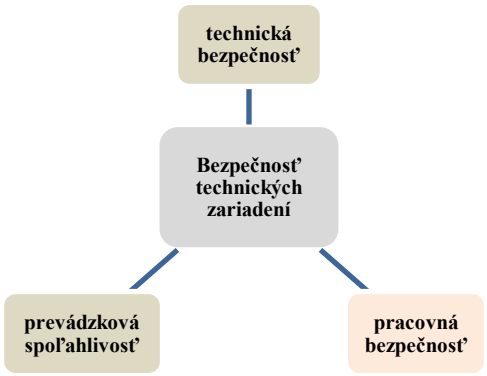
Technický systém je súhrnný pojem, ktorým sú označované rôzne ***technické objekty a zariadenia,*** napr. stroj alebo iné technologické zariadenie, technologický súbor, výrobný objekt, sústava operácií vytvárajúca výrobnú činnosť a pod. Technický systém je väčšinou vytváraný ako komplexný celok, vrátane prvkov, ktoré zabezpečujú riadenie jeho funkcií, preto integrálnou **súčasťou technického systému** je systém riadenia jeho pôsobenia na okolie, teda ***systém riadenia technického procesu,*** ktorý technický objekt (systém) zabezpečuje.

Americký sociológ Rogers špecifikuje „**bezpečnosť systému**“ ako ***pravdepodobnosť, že v systéme nedôjde v čase predpokladanej doby života, pri dodržaní predpokladaných podmienok prevádzky, k žiadnej nežiaducej udalosti,*** ktorá by mohla mať za následok poškodenie zdravia alebo ohrozenie života osôb, prípadne poškodenie alebo zničenie systému a prerušenie prevádzky *(Hatina, 2000).*

Bezpečnosť technického zariadenia je stav technického zariadenia a spôsob jeho používania, pri ktorom nie je ohrozená bezpečnosť a zdravie zamestnanca; bezpečnosť technického zariadenia je neoddeliteľnou súčasťou bezpečnosti a ochrany zdravia pri práci. *(Zákon o bezpečnosti a ochrane zdravia pri práci).*

Bezpečnosť označujú normy ako neprítomnosť neakceptovateľného rizika, pričom **bezpečnosť technických zariadení** je možné charakterizovať ako:

a) technickú bezpečnosť technických zariadení,
b) pracovnú bezpečnosť technických zariadení,
c) prevádzkovú (funkčnú) spoľahlivosť technických zariadení.



Obr. 17 Systém bezpečnosti technických zariadení

Technická bezpečnosť technických zariadení – úroveň technickej bezpečnosti závisí od kvality použitých materiálov, výrobných a pracovných operácií, medzioperačných kontrol, bezpečnostného výstroja a súboru skúšobných úkonov dokumentujúceho vyžadovanú kvalitu výrobku (technického zariadenia). V procese tvorby technickej bezpečnosti technického zariadenia sa vytvára jej kvalita, predstavujúca podstatnú časť celkovej kvality výrobku (technického zariadenia).

Pracovná bezpečnosť technických zariadení – vlastnosť ***neohrozovať ľudské zdravie, majetok alebo životné prostredie*** pri plnení funkcie, na ktorú boli predurčené, v stanovej dobe a za stanovených podmienok. Závisí od vytvorenia podmienok pre ich bezpečnú prevádzku, vypracovania miestnych pravidiel bezpečnej prevádzky, kvalifikácie obsluhy a pravidelnej preventívnej údržby. S otázkou vykonávania preventívnej údržby súvisí ***plánovité vykonávanie skúšok, kontrol a prehliadok technického zariadenia,*** ktorých kladné výsledky sú potvrdením jeho spôsobilosti pre ďalšiu prevádzku.

Prevádzková (funkčná) spoľahlivosť technických zariadení – Ide najmä o ***spoľahlivosť ich bezpečnostných zariadení***, výrazne sa podieľa na tvorbe ich celkovej kvality. Ide najmä o spoľahlivosť bezpečnostného výstroja a ďalších komponentov technického zariadenia, ktorých spoľahlivosť priamo podmieňuje celkovú bezpečnosť zariadenia.

Priama **podmienenosť spoľahlivosti a bezpečnosti** je osobitne významná pri zariadeniach, ktoré sú bezpečnostným výstrojom výrobných systémov, a svojou spoľahlivosťou určujú úroveň bezpečnosti prevádzky systému *(Sabo, 2010)*. Preto je potrebné pri komplexnom posudzovaní bezpečnosti technického zariadenia zohľadniť ako jedno z kritérií aj jeho prevádzkovú spoľahlivosť.

Spoľahlivosť technického zariadenia je **pravdepodobnosť, že činnosť zariadenia** bude *počas určenej doby* a *v daných prevádzkových podmienkach primeraná účelu zariadenia.* Je to všeobecná vlastnosť prvku, vyjadrovaná zostavou čiastkových ukazovateľov a charakteristík, ktorých výklad a definícia sú predmetom normovania. Každý ukazovateľ je možné vyjadriť väzbami medzi čiastkovými vlastnosťami prvku a im zodpovedajúcimi veličinami a ukazovateľmi. Väzby medzi vlastnosťami, ukazovateľmi a veličinami prvkov majú systémovú previazanosť.

Ukazovatele spoľahlivosti sú:

- **pravdepodobnosť,** že isté zariadenie vydrží bez poruchy určitú dobu,
- **primeraná činnosť** – určiť kritérium jasne špecifikujúce, čo je uspokojivá činnosť,
- **doba funkčnosti** – časový interval, v ktorom možno očakávať istý funkčný stav,
- **prevádzkové podmienky** – napr. teplota, tlak, vlhkosť, vibrácia atď.,
- **bezporuchovosť** – schopnosť plniť nepretržite požadované funkcie počas stanoveného času a za stanovených podmienok,
- **životnosť** – schopnosť plniť požadované funkcie do dosiahnutia určeného stavu pri stanovenom systéme údržby a opráv,
- **opraviteľnosť** – spôsobilosť na zisťovanie príčin vzniku porúch a odstraňovania ich následkov opravou,
- **skladovateľnosť** – schopnosť zachovávať prevádzkyschopný stav po dobu skladovania a prepravy.

Vyhláška Ministerstva práce, sociálnych vecí a rodiny SR č. 508/2009 Z. z., ktorou sa ustanovujú podrobnosti na zaistenie bezpečnosti a ochrany zdravia pri práci s technickými zariadeniami tlakovými, zdvíhacími, elektrickými a plynovými a ktorou sa ustanovujú technické zariadenia, ktoré sa považujú za vyhradené technické zariadenia ustanovuje:

a) podrobnosti na zaistenie bezpečnosti a ochrany zdravia pri práci a podrobnosti o odbornej spôsobilosti na výkon niektorých pracovných činností a na obsluhu niektorých technických zariadení,
b) technické zariadenia, ktoré sa považujú za vyhradené technické zariadenia.

Táto vyhláška sa vzťahuje na technické zariadenia ***tlakové, zdvíhacie, elektrické a plynové a ich časti***. Podľa miery ohrozenia sú zadelené do skupín: A – s vysokou mierou ohro-

zenia, B – s vyššou mierou ohrozenia, C – s nižšou mierou ohrozenia. Technické zariadenia skupín A, B sa považujú za vyhradené technické zariadenia.

Vyhradené technické zariadenia sú osobitné technické zariadenia, ktoré vzhľadom na ich charakter a rozsah používania predstavujú ***zvýšené riziko*** *poškodenia zdravia a života osôb a zvýšené riziko škôd na majetku.* Vyžadujú mimoriadne opatrenia bezpečnosti práce pri ich prevádzke.

Opatrenia na zaistenie bezpečnosti technických zariadení majú významné miesto v zložitom súbore opatrení bezpečnosti organizácie. Uvedené opatrenia riešia najmä *technickú bezpečnosť a prevádzkovú spoľahlivosť technických zariadení,* avšak do tohto súboru opatrení sa organicky začleňuje aj *bezpečnosť prevádzkových objektov*. V cykle prípravy, tvorby a prevádzky technických zariadení sa ťažisko ich bezpečnostnej prevencie stáva aktuálnym v štádiu ich prípravy a tvorby.

Primárne nebezpečenstvá v prevádzke technických zariadení majú v prevažnej miere pôvod v **projekčnej a konštrukčnej dokumentácii** v dôsledku nerešpektovania požiadaviek bezpečnostných predpisov. Pri tvorbe projektovej a konštrukčnej dokumentácie technických zariadení, resp. objektov, treba dôsledne rešpektovať požiadavky bezpečnostných predpisov, v ktorých ide predovšetkým o to, **aby zariadenia a objekty boli:**

- **bezpečné** – aby pri normálnej prevádzke technických zariadení nevznikali ohrozenia pre osoby a veci, teda aby technické zariadenia neboli zdrojmi škôd na zdraví či majetku,
- **trvanlivé** – aby pri ich projekcii, či konštrukcii boli navrhnuté materiály schopné v určenom čase prevádzky odolávať vplyvom pracovného prostredia a pracovných podmienok, pre ktoré sú technické zariadenia určené, bez toho, aby sa neprípustne zhoršili ich vlastnosti, resp. narušila funkcia zariadenia,
- **usporiadané** – aby vyhovovali účelu, pre ktorý sú určené a vyrobené, umožňovali vykonávanie riadnej obsluhy, údržby, skúšok a kontrol technických zariadení, aby sa poruchy vyskytovali v čo najmenšom rozsahu a aby umožňovali ich ľahkú identifikáciu, aby umožňovali dobrú orientáciu pri práci, resp. mali prehľadne usporiadané ovládacie a regulačné prvky, správne fungovali a v daných podmienkach pracovali spoľahlivo,
- **chránené pred vplyvom iných zariadení** – aby boli umiestnené tak, že nie sú vystavené škodlivému pôsobeniu iných zariadení, prípadne aby boli odolné proti škodlivému pôsobeniu iných zariadení,
- **škodlivo neovplyvňovali iné zariadenia** – aby svojou činnosťou nežiaducim spôsobom neovplyvňovali funkciu a prevádzku iných zariadení.

Overovanie plnenia požiadaviek bezpečnosti technických zariadení vykonávané v zmysle § 14 Zákona č. 124/2006 Z. z. zahŕňa:

- overovanie odbornej spôsobilosti zamestnávateľa na odborné prehliadky a odborné skúšky a opravy vyhradeného technického zariadenia podľa právnych predpisov na zaistenie bezpečnosti a ochrany zdravia pri práci, na plnenie tlakovej nádoby na dopravu plynov vrátane plnenia nádrží motorového vozidla plynom a vydávanie oprávnení na tieto činnosti,
- vykonávanie prehliadky, riadenie a vyhodnocovanie alebo vykonávanie úradnej skúšky a inej skúšky podľa právnych predpisov na zaistenie bezpečnosti a ochrany zdravia pri práci na vyhradených technických zariadeniach vrátane označenia vyhradeného technického zariadenia a vydávanie príslušných dokladov,
- overovanie odborných vedomostí fyzickej osoby na vykonávanie skúšky, odborných prehliadok a odborných skúšok, opráv a obsluhy vyhradeného technického zariadenia podľa právnych predpisov na zaistenie bezpečnosti a ochrany zdravia pri práci a vydávanie osvedčenia alebo preukazu na tieto činnosti,

- posudzovanie, či technické zariadenia, materiál, projektová dokumentácia stavieb s technickým zariadením a jej zmeny, dokumentácia technických zariadení a technológií spĺňajú požiadavky bezpečnosti a ochrany zdravia pri práci a vydávanie odborného stanoviska.

Plnenie požiadaviek bezpečnosti technických zariadení overuje oprávnená právnická osoba len na základe oprávnenia vydaného Národným inšpektorátom práce.

8.1.3 Bezpečnosť pracovného prostredia a pracovných podmienok

Bezpečnosťou pracovného prostredia a pracovných podmienok sa zaoberá hygiena práce. **Hygiena práce** je zameraná na posudzovaním práce a jej vplyvu na zdravie zamestnanca, je to ***prevencia proti vzniku chorôb z povolania***. Jej cieľom je zachovanie zdravia a odstránenie všetkých možností jeho poškodenia pri plnení pracovných úloh a podpora všetkých užitočných vplyvov na zdravie pracovníka.

Základnou činnosťou odboru hygieny práce v rámci štátneho zdravotného dozoru je kontrola plnenia zákonných povinností v oblasti ochrany zdravia pri práci, čo sú najmä požiadavky na **usporiadanie pracovísk.**

Pracovisko je miesto určené na výkon práce zamestnancov (zamestnanca) a akékoľvek iné miesto v priestoroch zamestnávateľa, ku ktorému má zamestnanec počas svojej práce prístup. Je to priestor, v ktorom sú situované pracovné prostriedky a predmety, s ktorými zamestnanec alebo zamestnanci prichádzajú do styku pri plnení pracovných povinností. Na pracovisku je obvykle viac rovnakých či rôznych pracovných miest.

Požiadavky na usporiadanie pracovísk zahŕňajú najmä:

- zaistenie vyhovujúcich mikroklimatických podmienok na pracovisku, ako sú intenzita, farba a smer osvetlenia, cirkulácia vzduchu (vetranie), teplotné pomery a pod.,
- dodržiavanie hygienických limitov pre fyzikálne faktory (hluk, vibrácie, prach v pracovnom prostredí),
- dodržiavanie zásad pre práce s biologickými činiteľmi a chemickými škodlivinami,
- dodržanie limitov pre fyzickú záťaž, naplnenie ergonomických požiadaviek pre pracovné miesto a pracovisko,
- vybavenie pracovísk sanitárnymi a pomocnými zariadeniami, zásobovanie pracovísk vodou, ale i zaistenie podnikovej preventívnej starostlivosti.

V súvislosti s tým je hodnotené pôsobenie fyzikálnych faktorov, napr. hluku, vibrácií, neionizujúceho žiarenia, mikroklimatických podmienok, chemických faktorov (chemické škodliviny), biologických faktorov (baktérie, vírusy) v pracovnom prostredí na zdravotný stav pracovníkov a posudzované technické, organizačné a náhradné opatrenia, vykonané zamestnávateľom na zníženie pôsobenia rizikových faktorov pracovného prostredia.

V zmysle § 31 Zákona č. 355/2007 Z. z. o ochrane, podpore a rozvoji verejného zdravia v znení neskorších predpisov podľa úrovne a charakteru faktorov práce a pracovného prostredia, ktoré môžu ovplyvniť zdravie zamestnancov, hodnotenia zdravotných rizík a na základe zmien zdravotného stavu zamestnancov sa práce zaraďujú do ***štyroch kategórií. Rizikovou prácou*** je práca zaradená do tretej a štvrtej kategórie.

O zaradení práce do tretej kategórie a štvrtej kategórie, o zmene alebo vyradení práce z tretej kategórie a štvrtej kategórie rozhoduje príslušný orgán verejného zdravotníctva na základe návrhu zamestnávateľa, fyzickej osoby - podnikateľa, ktorý nezamestnáva iné fyzické osoby, alebo z vlastného podnetu.

8.2 LITERATÚRA

BOGDANOVSKÁ, G. [2009]: *Nová norma pre systémy manažérstva bezpečnosti a ochrany zdravia pri práci.* In: Security Revue. Elektronický časopis FŠI, Žilina, ŽU 13.2.2009

BOJNANSKÝ, M. [2006]: *Bezpečnosť a ochrana zdravia pri práci v praxi.* Nová práca, spol. s. r. o**.** EAN: 978-80-8892-963-5.

HATINA, T. [2000]: *Bezpečnosť a ochrana zdravia pri práci.* Bratislava: Euronion, s.r.o., 2000. ISBN 80-8898-410-6.

HATINA, T. a kol. [2006]: *Terminologický slovník bezpečnosti a ochrany zdravia pri práci Inštitút pre výskum práce a rodiny. Bratislava 2006.*

LORKO, M. – LAJČINOVÁ, R. [2009]: *Bezpečnosť a hygiena pri práci.* FVT TU v Košiciach, Prešov.

MRENICA, M. – SUJOVÁ, E. [2008]: *Bezpečnosť technických systémov*. Zvolen: ES TU vo Zvolene,

SABO, M. [2010]: *Bezpečnosť práce.* Bratislava: STU. ISBN 80-227-1540-9.

STN EN 12100:2010 *Bezpečnosť strojov. Všeobecné zásady konštruovania strojov. Posudzovanie a znižovanie rizika.*

ŠUKALOVÁ, M. [2011]: *Manažment bezpečnosti práce.* Žilina: EDIS – vydavateľstvo ŽU. ISBN:978-80-5540-403-5.

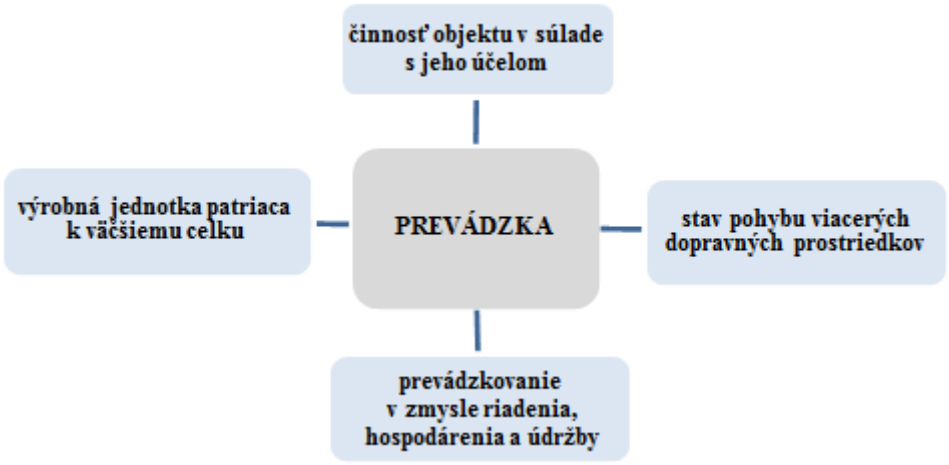
TOMÁŠ, J. [2001]: *Bezpečnosť strojov.* Nitra. SPU, 2001.

TOMEK, M. – SEIDL, M. – ŠEFČÍK, V. [2010]: *Bezpečnosť a ochrana ľudí v pracovnom procese.* Žilina: EDIS vydavateľstvo ŽU. ISBN: 978-80-5540-243-7.

9 BEZPEČNOSŤ PREVÁDZKY

Pojem **„prevádzka“** má viac významov, podľa toho, kvôli čomu sa organizuje môže znamenať napr.:

1. **činnosť, chod, fungovanie objektu v súlade s jeho účelom**, napr.:
   - technické zariadenia (stroje, prístroje, motory, motorové vozidlá, ropovody, plynovody, elektrické rozvody a pod.),
   - inštitúcie, organizácie, zariadenia (podniky, spoločnosti, závody, opravovne, obchody, školy, ústavy, štadióny, lanovky, vleky, klziská a pod.).
2. **stav pohybu viacerých dopravných prostriedkov – dopravná prevádzka** (letecká, železničná, cestná, plavebná).
3. **výrobná jednotka patriaca k väčšiemu celku** – časť nejakého závodu, firmy, podniku, továrne, obchodné jednotky, kultúrne inštitúcie a pod., obdobné slová sú *úsek, sekcia* a *sektor* (*výrobná prevádzka, hutnícka prevádzka, priemyselná prevádzka, obchodná prevádzka, poľnohospodárska prevádzka* a pod.).
4. **prevádzkovanie v zmysle riadenia, hospodárenia a údržby** *(prevádzka podniku, prevádzka firmy)*.



Obr. 18 Významy pojmu prevádzka

Každá z uvedených druhov činností má svoje špecifiká, v závislosti od účelu prevádzky a cieľov, ktoré sa v prevádzke majú dosiahnuť. Všetky druhy prevádzky však spoločne vyžadujú ***bezporuchové a neohrozené fungovanie***, aby sa tieto ciele mohli dosiahnuť ***bez prerušovania kontinuity jednotlivých činností***.

9.1 OBLASTI BEZPEČNOSTI PREVÁDZKY

Bezpečnosť je všeobecne charakterizovaná ako vlastnosť objektu, t. j. stroja, technológie, činnosti, neohrozovať ani osoby, a ani okolie. Analýzy používané na posúdenie **celkovej bezpečnosti organizácie** (objektu) zohľadňujú tak aspekty ***bezpečnosti práce,*** ako aj ***bezpečnosti technických zariadení.***

Bezpečnosť prevádzky znamená proces vytvárania politík a postupov a zavádzanie kontrol, zachovanie dôverných informácií, týkajúcich sa schopnosti a zraniteľnosti organizácie. To sa vykonáva identifikáciou, kontrolou a ochranou týchto záujmov spojených s integritou a nerušeným výkonom zariadenia.

Kľúčovými prvkami bezpečnosti prevádzky sú **pracovníci** – vyškolení bezpečnostným personálom pre vlastnú ochranu a presadzovanie bezpečnostných postupov a zásad, ktorými sa riadia objekty alebo výrobné činnosti a zavedené politiky a postupy. Zásady a postupy majú zaviesť kontroly, aby sa zabránilo neoprávnenému prístupu do zariadení, zneužitiu priestorov a obchodných aktív, či už prostredníctvom nedbanlivosti, úmyselného spáchania trestného činu alebo inej vonkajšej hrozby.

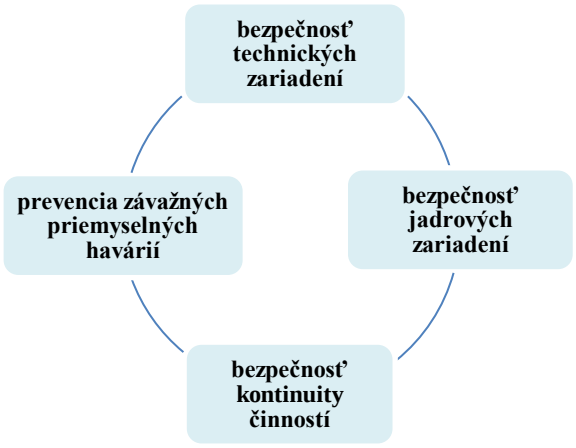
Široko významový pojem **bezpečnosť prevádzky organizácie** je najčastejšie zameraný do oblasti techniky a technológií, priemyslu, energetiky, kde sa vyskytujú termíny:

a) bezpečnosť technických zariadení, uvedená v kapitole 8.2,

b) prevencia závažných priemyselných havárií – *ochrana prevádzky priemyselných podnikov s nebezpečnými látkami* a ich okolia pred náhodnými priemyselnými haváriami a plánovanie ***reakcie na ne,***

c) bezpečnosť jadrových zariadení – *ochrana prevádzky jadrových zariadení a ich okolia pred náhodnými javmi,*

d) bezpečnosť kontinuity činností – *ochrana kľúčových výrobných a nevýrobných činností (podnikateľských)* na tvorbu produktov alebo poskytovanie služieb, prerušenie ktorých (pre poruchu alebo haváriu) môže spôsobiť značné straty.



Obr. 19 Oblasti bezpečnosti prevádzky

9.2 PREVENCIA ZÁVAŽNÝCH PRIEMYSELNÝCH HAVÁRIÍ

Rozvoj priemyselnej výroby, zavádzanie nových technológií, používanie stále väčšieho množstva nových látok prináša so sebou značné riziká, s možnosťou vzniku priemyselných havárií. Za posledných 30 rokov história priniesla množstvo priemyselných havárií s následkami pre život, zdravie a majetok ľudí alebo pre životné prostredie – príčinami havárií bola predovšetkým ***nevhodná manipulácia s nebezpečnými látkami, zanedbanie technologických postupov*** alebo ***zlyhanie ľudského faktora.***

V SR sa vyrába, spracováva, používa, manipuluje a skladuje veľké množstvo toxických, horľavých a výbušných látok, v značných množstvách sú tieto látky prepravované po cestách, železniciach, vodných tokoch alebo potrubím. Inými slovami, značná časť infraštruktúry vyrába, skladuje a používa v technologických procesoch chemické látky a prípravky ako výsledné produkty, medziprodukty alebo konečné produkty procesov.

Celkové množstvá uvedených látok sú značné. Zvláštnosťou je skutočnosť, že nebezpečné látky sú koncentrované v rôznych lokalitách, najčastejšie vo veľkých priemyselných aglomeráciách. Na niektorých miestach sa nachádza i niekoľko skupín nebezpečných látok pohromade a sú uskladnené vo veľkých množstvách.

9.2.1 Havárie

Porucha je poškodenie technického zariadenia, ktoré spôsobilo zastavenie alebo obmedzenie prevádzky, pri čom vznikla škoda v stanovenom finančnom rozpätí.

Havária je udalosť, ktorá vážne ohrozila životy a zdravie osôb, prevádzku, činnosť, prípadne rozvoj organizácie, alebo ktorá spôsobila škodu na majetku organizácie prevyšujúcu stanovenú finančnú hodnotu *(Zákon o civilnej ochrane obyvateľstva)*.

Podľa Zákona č. 261/2002 Z. z. o prevencii závažných priemyselných havárií:

- **Prítomnosťou vybranej nebezpečnej látky** v podniku je jej skutočná alebo predpokladaná (projektovaná) prítomnosť, vrátane takej vybranej nebezpečnej látky, ktorá môže vzniknúť v prípade straty kontroly nad chemickým procesom alebo v prípade závažnej priemyselnej havárie.
- **Nebezpečenstvom** (zdrojom rizika závažnej priemyselnej havárie) je vnútorná vlastnosť vybranej nebezpečnej látky alebo fyzická situácia s potenciálom poškodenia ľudského zdravia, životného prostredia alebo majetku.
- **Rizikom závažnej priemyselnej havárie** je pravdepodobnosť vzniku závažnej priemyselnej havárie a rozsah (závažnosť) jej možných následkov, ktoré môžu nastať počas určitého obdobia alebo za určitých okolností.
- ***Závažná priemyselná havária*** je udalosť, akou je najmä ***nadmerná emisia, požiar alebo výbuch*** s prítomnosťou jednej alebo viacerých vybraných nebezpečných látok, vyplývajúca z nekontrolovateľného vývoja v prevádzke ktoréhokoľvek z podnikov, na ktoré sa vzťahuje tento zákon a ktorá vedie bezprostredne alebo následne k vážnemu poškodeniu alebo ohrozeniu života alebo zdravia ľudí, životného prostredia alebo majetku v rámci podniku alebo mimo neho.
- **Prevenciou závažnej priemyselnej havárie** je súbor organizačných, riadiacich, personálnych, výchovných, technických, technologických a materiálnych opatrení na zabránenie vzniku závažnej priemyselnej havárie.
- **Bezpečnostnou správou** je dokumentácia obsahujúca technické, riadiace a prevádzkové informácie o nebezpečenstvách a rizikách podniku kategórie B a o opatreniach na ich vylúčenie alebo zníženie.

- Podniky sa **kategorizujú** (kategórie A, B) podľa celkového množstva vybraných nebezpečných látok, ktoré sú prítomné v podniku. Medzi základné povinnosti prevádzkovateľov podnikov, v ktorých sa nachádzajú vybrané nebezpečné látky, patrí: *preveriť celkové množstvo vybraných nebezpečných látok v podniku a následne zaradiť podnik do príslušnej kategórie a podať oznámenie o zaradení podniku na príslušný úrad životného prostredia.*

Objektmi následkov havárií sú:

- ľudia, rastliny a živočíchy,
- pôda, voda, vzduch a prírodné prostredie ako celok,
- všetky predchádzajúce prvky alebo ich kombinácie,
- hmotné statky a kultúrne dedičstvo, vrátane historických pamiatok.

Príklady havárií sú uvedené na obr. 20 *(Betuš, 2014)*:

Obr. 20 Havárie

Medzi priemyselné havárie patria:

- havária jadrového zariadenia,
- výbuch v muničnej továrni,
- požiar v chemickej továrni,
- úniky toxických látok v dôsledku mimoriadnych udalostí,
- výbuchy plynov a pár horľavých kvapalín,
- havárie plynovodu, ropovodu, teplovodu, parovodu, elektrických sietí,
- rozsiahle poruchy v energetických sieťach, popadané stĺpy elektrickej rozvodnej siete.

Ekologické havárie predstavujú také dopravné či priemyselné havárie, ktoré spôsobia veľké škody na životnom prostredí, prírode, alebo na životoch a zdraví, napr.:

- výbuch jadrového reaktora,
- únik veľkého množstva jedovatých látok do ovzdušia,
- otrava rýb v rieke či inom vodnom zdroji únikom toxických látok z chemickej či poľnohospodárskej výroby,
- havárie ropných tankerov na mori spojené s únikom veľkého množstva ropy do mora,
- požiare horľavých látok v technologických procesoch, skladoch horľavých látok, čerpacích staniciach, skladoch plastických hmôt, skladoch pesticídov.

Dopravné nehody a havárie sú nepredvídané kolízie jedného alebo viacerých dopravných prostriedkov, pri ktorých dôjde k škode na majetku, alebo ohrozeniu života, zdravia a k zraneniu. Obvykle sa termínom dopravná nehoda (havária) označuje nehoda v prevádzke na cestných komunikáciách, nehodami sú aj mimoriadne udalosti v železničnej, vodnej alebo leteckej doprave.

- Pri **motorových vozidlách** osobných a nákladných sa hovorí o *automobilovej nehode (havárii)*, čo je najčastejší typ dopravnej nehody.

- Na **vodných cestách** môže ísť o: *stroskotanie* alebo *potopenie lode, zrážku s iným plavidlom, požiar na palube* a pod.
- V **leteckej doprave** sa hovorí o: *leteckej havárii, katastrofe*, často spojenej s *pádom lietadla a jeho totálnou deštrukciou* spojenou so zlyhaním pozemného personálu, alebo posádky či navigácie alebo technickou, technologickou chybou lietadla.
- Pri **železničnej dopravnej nehode, havárii** je pozornosť venovaná hlavne *železničným nešťastiam a iným závažným haváriám, spojeným s únikom nebezpečných prepravovaných látok, požiarom nákladného vlaku, ďalej sú to zrážky električiek, trolejbusov, dopravné nehody lanoviek, havárie v tuneloch, havárie spojené s narušením statiky mostov.*
- Pri **visutých lanovkách, výťahoch, eskalátoroch a iných dopravných zariadeniach, najmä zdvíhacích**, má tragické následky *odtrhnutie a pád*.

Medzi havárie, ktorým je potrebné venovať osobitnú pozornosť sa radia:

- závažné priemyselné havárie,
- jadrové havárie a mimoriadne udalosti s ionizujúcim žiarením,
- havárie informačných a bezpečnostných systémov,
- havárie vo vojenských zariadeniach,
- havárie vodohospodárskych diel a vodných zdrojov,
- havárie pri preprave nebezpečných vecí a tovarov,
- náhodné uvoľnenie geneticky modifikovaných organizmov,
- havárie spôsobené činnosťami v morskom prostredí vrátane prieskumu alebo využívania morského dna,
- úniky ropy alebo iných škodlivých a nebezpečných látok.

9.2.2 Právne normy v oblasti závažných priemyselných havárií

V našich podmienkach bola v minulosti problematika prevencie závažných priemyselných havárií riešená len nesystematicky a niektoré opatrenia boli roztrúsené v rôznych zákonoch a právnych normách, ako napr. v zákonníku práce, v zákone o ochrane zdravia ľudí atď. V rámci krajín európskej únie je prevencia závažných priemyselných havárií upravená rôznymi smernicami, rozhodnutiami, nariadeniami a dohovorom:

- **Smernica Rady 82/501/EHS** o veľkých havarijných nebezpečenstvách určitých priemyselných činností (SEVESO I).
- **Smernica Rady 96/82/ES** o kontrole nebezpečenstiev veľkých havárií s prítomnosťou nebezpečných látok (SEVESO II), ktorá je zameraná nielen na prevenciu veľkých havárií, ale aj na obmedzenie ich následkov pre človeka a životné prostredie.
- **Rozhodnutie Komisie 1999/314/ES** týkajúce sa dotazníka, ktorý sa vzťahuje na smernicu Rady 96/82/ES o kontrole nebezpečenstiev veľkých havárií s prítomnosťou nebezpečných látok.
- **Smernica Európskeho parlamentu a Rady 2003/105/ES** dopĺňajúca Smernicu Rady 96/82/ES.
- **Smernica Európskeho parlamentu a Rady 2012/18/EÚ o kontrole nebezpečenstiev závažných havárií s prítomnosťou nebezpečných látok**, s účinnosťou od 13. 8. 2012, ktorou sa mení a dopĺňa a následne ruší smernica 96/82/ES.
- **Nariadenie (ES) č. 1272/2008 o klasifikácii, označovaní a balení látok a zmesí** (KOB, CLP) – SEVESO III. Smernica SEVESO II sa týmto s účinnosťou od 1. júna 2015 zrušuje.
- **Dohovor Európskej hospodárskej komisie OSN o cezhraničných účinkoch priemyselných havárií**. Cieľom dohovoru je v záujme trvalo udržateľného rozvoja a na základe princípov medzinárodného práva a zvyklostí zabezpečiť koncepčnú a systematickú činnosť zmluvných strán na úseku prevencie priemyselných havárií, ktoré môžu mať cezhraničné

účinky, pripravenosť na takéto havárie a zdolávanie priemyselných havárií vrátane obmedzovania ich účinkov na ľudí, životné prostredie a majetok.

Dokument SEVESO je pomenovaný podľa talianskeho mesta, kde po výbuchu chemickej továrne v roku 1976 unikol dioxín, čo spôsobilo hromadnú otravu obyvateľstva. Mesto Seveso sa tak stalo synonymom ekologickej hrozby. Vzhľadom na ďalšie závažné priemyselné havárie (pretrhnutie hrádze banského odkaliska v rumunskom Baia Mare, následkom ktorého sa zamorila kyanidmi rieka Tisa, výbuch továrne na pyrotechniku v holandskom Enschede, výbuch v podniku na výrobu hnojív vo francúzskom Toulouse) vznikla požiadavka Európskej Rady na novelizáciu danej smernice.

Oblasť *závažných priemyselných havárií s prítomnosťou nebezpečných chemických látok* upravuje aj **Dohovor Medzinárodnej organizácie práce č. 174 o prevencii veľkých priemyselných nehôd.**

V SR danú problematiku komplexne rieši Zákon č. 261/2002 Z. z. o prevencii závažných priemyselných havárií a vykonávacie predpisy:

- Vyhláška MŽP SR č. 489/2002 Z. z., ktorou sa vykonávajú niektoré ustanovenia Zákona o prevencii závažných priemyselných havárií v znení neskorších predpisov.
- Vyhláška MŽP SR č. 490/2002 Z. z. o bezpečnostnej správe a havarijnom pláne.
- Zákon č. 245/2003 Z. z. o integrovanej prevencii a kontrole znečisťovania životného prostredia v platnom znení.

Zákon č. 261/2002 Z. z. o prevencii závažných priemyselných havárií stanovuje podmienky a postup pri prevencii závažných priemyselných havárií v podnikoch s prítomnosťou vybraných nebezpečných látok a pripravenosť na ich zdolávanie, a na obmedzovanie ich následkov na život a zdravie ľudí, životné prostredie a majetok v prípade ich vzniku. Uvádza kategórie podnikov podľa celkového množstva vybraných nebezpečných látok, ktoré sú prítomné v podniku a v prílohe 1 uvádza kategórie vybraných nebezpečných látok (chemických látok alebo chemických prípravkov).

Základnou **povinnosťou prevádzkovateľa** je prijať všetky opatrenia potrebné na prevenciu závažných priemyselných havárií a v prípade vzniku takej havárie alebo jej bezprostrednej hrozby opatrenia potrebné na jej zdolanie a obmedzenie jej následkov na život a zdravie ľudí, životné prostredie a majetok. Je povinný:

- oznámiť **zaradenie podniku** do kategórie A alebo B,
- zriadiť **informačný systém prevencie** závažných priemyselných havárií,
- zabezpečiť identifikáciu, analýzu a hodnotenie **rizika**,
- vypracovať **program prevencie** závažných priemyselných havárií a zabezpečiť jeho uplatňovanie,
- v podniku kategórie B zaviesť v rámci celkového riadiaceho systému ucelený bezpečnostný riadiaci systém, vypracovať **bezpečnostnú správu** a zabezpečiť jej uplatňovanie v činnosti a riadení podniku,
- ustanoviť **odborne spôsobilú osobu** (havarijný technik, špecialista na prevenciu závažných priemyselných havárií),
- zabezpečiť potrebnú kvalifikáciu, periodické **školenie a výcvik zamestnancov** podniku vrátane potrebného overenia znalostí, vybavenia potrebnými osobnými ochrannými pracovnými prostriedkami, prístrojmi, náradím a nástrojmi,
- pred začatím prevádzky podniku alebo zariadenia vypracovať **havarijný plán**.
- spolupracovať na vypracúvaní **plánu ochrany obyvateľstva,**

- mať alebo zabezpečiť **prostriedky, prístroje a nástroje** potrebné na včasné rozpoznanie havarijných stavov, na výstrahu a varovanie, vyrozumenie a zvolanie príslušných subjektov, na zdolávanie závažných priemyselných havárií a na obmedzovanie ich následkov,
- zabezpečiť vo svojom podniku organizačne, materiálne a personálne vybavenú **záchrannú službu** zloženú z odborne spôsobilých a vycvičených profesionálnych alebo dobrovoľných členov,
- obvyklým spôsobom a podľa potreby aj opakovane **informovať verejnosť**, ktorá môže byť dotknutá závažnou priemyselnou haváriou,
- **oznámiť** závažnú priemyselnú haváriu okresnému úradu, ministerstvu a ministerstvu vnútra.

Vyhláška MŽP SR č. 489/2002 Z. z. ustanovuje podrobnosti o:

a) náležitostiach **oznámenia o zaradení podniku,**
b) **hodnotení rizika** závažných priemyselných havárií vrátane predbežného odhadu rizika vzniku závažných priemyselných havárií,
c) obsahu a spracúvaní **programu prevencie** závažných priemyselných havárií a o **bezpečnostnom riadiacom systéme,**
d) **odborne spôsobilých osobách**, o ich úlohách, odbornej príprave a o overovaní ich odbornej spôsobilosti vrátane náležitostí osvedčení o odbornej spôsobilosti a o ich vydávaní, o obsahu a vedení zoznamu odborne spôsobilých osôb, ako aj o pečiatke špecialistu na prevenciu závažných priemyselných havárií, jej vzore, úhrade za jej vydanie a o jej používaní,
e) obsahu a vykonávaní **školenia a výcviku zamestnancov** podnikov kategórie A i kategórie B,
f) **autorizácii právnických osôb a fyzických osôb – podnikateľov** na vykonávanie činností podľa § 14 ods. 2 zákona a o vedení zoznamu autorizovaných osôb,
g) obsahu **informácie pre verejnosť,**
h) spôsobe plnenia **oznamovacej povinnosti** a o písomných správach a informáciách podľa § 24 zákona.

9.2.3 Boj proti závažným priemyselným haváriám

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

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

Pritom však treba podotknúť, že:

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

   zabráni premene tohto stavu ohrozenia (tzv. skoronehoda – near miss) na závažnú haváriu a tým aj zabezpečí buď úplné alebo aspoň podstatné zníženie následkov na ľudí, životné

prostredie a majetok (vrátane obmedzenia potreby, zníženia nákladov i času na prípadnú sanáciu).

Pripravenosť na zdolávanie závažných priemyselných havárií

Prevádzkovateľ je povinný:

- pred začatím prevádzky podniku alebo zariadenia vypracovať **havarijný plán,**
- predložiť orgánu, ktorý vypracúva plán ochrany obyvateľstva podľa osobitného predpisu, požadované **podklady** a na požiadanie tohto orgánu spolupracovať na vypracúvaní **plánu ochrany obyvateľstva** v záujme potrebnej previazanosti havarijného plánu a plánu ochrany obyvateľstva,
- mať alebo zabezpečiť **prostriedky, prístroje a nástroje** potrebné na včasné rozpoznanie havarijných stavov, na výstrahu a varovanie, vyrozumenie a zvolanie príslušných subjektov, na zdolávanie závažných priemyselných havárií a na obmedzovanie ich následkov,
- zabezpečiť vo svojom podniku organizačne, materiálne a personálne vybavenú službu (**záchranná služba)** zloženú z odborne spôsobilých a vycvičených profesionálnych alebo dobrovoľných členov.

Havarijný plán – účelom havarijného plánu je zabezpečenie včasnej a adekvátnej reakcie na závažnú haváriu alebo jej bezprostrednú hrozbu v záujme ochrany životov a majetku občanov a štátu a na vylúčenie, resp. čo najväčšie obmedzenie účinkov (následkov) závažnej havárie na životné prostredie. Pri vypracúvaní havarijného plánu prevádzkovateľ vychádza najmä z výsledkov ***hodnotenia rizika***. Havarijný plán musí byť zostavený tak, aby zabezpečoval:

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

Havarijný plán obsahuje najmä:

a) potrebné **údaje o podniku**, jeho zariadeniach a činnostiach, mená a funkcie osôb, ktorým sa v ňom ukladajú určité povinnosti, ako aj názvy príslušných orgánov a iných subjektov, s ktorých súčinnosťou sa uvažuje,
b) **mechanizmy na výstrahu a varovanie ohrozených osôb**, ako aj na vyrozumenie a zvolanie osôb, príslušných orgánov a iných subjektov zúčastnených na zdolávaní závažnej priemyselnej havárie a na obmedzovaní jej následkov,
c) **scenáre reprezentatívnych druhov závažných priemyselných havárií** a súbory scenárov pre reprezentatívne druhy závažných priemyselných havárií a opatrení na ich efektívne zdolanie a obmedzenie ich následkov vrátane určenia zón ohrozenia, opisu potrebného materiálneho, personálneho a iného vybavenia a použiteľných prostriedkov,
d) opatrenia na zabezpečenie **evakuácie** alebo iného spôsobu ochrany ohrozených osôb alebo majetku,
e) opatrenia na zabezpečenie potrebnej **súčinnosti s akciami príslušných orgánov** a iných subjektov na území podniku a podľa potreby aj mimo neho,
f) spôsob **školenia a výcviku** podnikových útvarov a služieb a jednotlivých zamestnancov o činnostiach, ktoré sa od nich očakávajú, vrátane potrebnej súčinnosti s príslušnými orgánmi a inými subjektmi.

Do oblasti pôsobnosti **havarijného manažmentu** (*Failure Management*) budú patriť také situácie, ako: ***prevádzkové havárie, priemyselné havárie, živelné pohromy.***

9.2.4 Prostriedky na zdolávanie závažných priemyselných havárií

Prostriedkami na zdolávanie závažných priemyselných havárií a na obmedzovanie ich následkov sa rozumejú najmä prostriedky na:

a) **kontrolu, meranie a riadenie technologického procesu a signalizáciu** závažných odchýlok, vrátane prípadnej automatickej korekcie tohto stavu,
b) **ochranu zamestnancov a ďalších osôb** zdržiavajúcich sa s vedomím prevádzkovateľa v areáli podniku, ktoré môžu byť ohrozené závažnou priemyselnou haváriou,
c) **obmedzenie rozširovania závažnej priemyselnej havárie** už v počiatočných štádiách, ako aj na zmenšenie jej rozsahu a obmedzenie jej následkov pre podnik a jeho okolie,
d) **zdolanie závažnej priemyselnej havárie** vrátane prostriedkov a zariadení na ochranu osôb zúčastnených na jej zdolávaní, na zisťovanie a vymedzovanie zón ohrozenia a na potrebný monitoring.

Z evidencie a dokumentácie prostriedkov musí vyplývať najmä:

a) ktoré prostriedky a v akom množstve sa nachádzajú priamo v príslušnom zariadení či už ako priama súčasť technologického zariadenia, riadiaceho centra alebo ako pohotovostná rezerva,
b) ktoré prostriedky a v akom množstve sa nachádzajú v havarijnom sklade alebo v inom osobitnom sklade v rámci podniku,
c) účel, na aký môžu byť prostriedky použité, a právomoc a zodpovednosť za riadne využívanie týchto prostriedkov,
d) zodpovednosť za udržiavanie prostriedkov vo funkčnom a bezpečnom stave vrátane potrebných kontrol, preskúšania, kalibrácie a údržby,
e) stav a pohyb zásob prostriedkov vrátane účelu ich použitia a doplnenia.

Záchranná služba

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

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

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

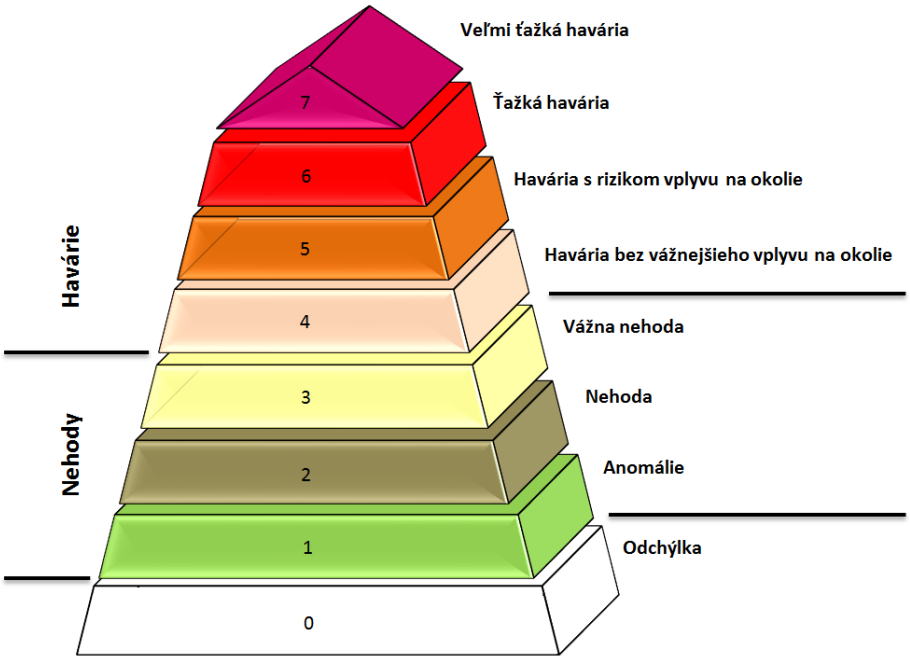
Na zvládanie závažných priemyselných havárií je možné využiť aj viazaných živnostníkov – ***havarijného technika***, alebo ***špecialistu na prevenciu závažných priemyselných havárií***, ktorí musia mať osvedčenie o odbornej spôsobilosti, vydané MŽP SR. Špecialistovi na prevenciu závažných priemyselných havárií vydá ministerstvo za úhradu aj pečiatku špecialistu na prevenciu závažných priemyselných havárií.

9.3 JADROVÁ BEZPEČNOSŤ

Jadrová bezpečnosť predstavuje stav a schopnosť jadrového zariadenia alebo prepravného zariadenia a ich obsluhy zabrániť nekontrolovanému rozvoju štiepnej reťazovej reakcie alebo nedovolenému úniku rádioaktívnych látok alebo ionizujúceho žiarenia do pracovného prostredia alebo do životného prostredia a obmedzovať následky nehôd a havárií jadrových zariadení alebo následky udalostí pri preprave rádioaktívnych materiálov.

Jadrovým zariadením je **súbor stavebných objektov a technologických zariadení**:

1. ktorých súčasťou je jadrový reaktor alebo jadrové reaktory,
2. na výrobu alebo spracovanie jadrových materiálov alebo skladovanie jadrových materiálov s množstvom väčším ako jeden efektívny kg,
3. na spracovanie, úpravu alebo skladovanie rádioaktívnych odpadov,
4. na ukladanie rádioaktívnych odpadov z jadrových zariadení, inštitucionálnych rádioaktívnych odpadov alebo vyhoretého jadrového paliva; za jadrové zariadenie sa nepovažujú kontajnery a kryty, v ktorých sa jadrový materiál používa ako tieniaci materiál na rádioaktívne žiariče, ani priestory, v ktorých sa tieto kontajnery a kryty skladujú.



Obr. 21 Medzinárodná stupnica jadrových udalostí (zdroj Betuš, 2014)

Pri využívaní jadrovej energie sa musí dosiahnuť taká úroveň jadrovej bezpečnosti, spoľahlivosti, bezpečnosti a ochrany zdravia pri práci a bezpečnosti technických zariadení, ochrany zdravia pred ionizujúcim žiarením, fyzickej ochrany, havarijnej pripravenosti a ochrany pred požiarmi, aby riziko ohrozenia života, zdravia, pracovného alebo životného prostredia bolo podľa dostupných znalostí také nízke, aké možno rozumne dosiahnuť, pričom nesmú byť prekročené limity ožiarenia.

Bezpečnosť a najmä jadrová bezpečnosť je prioritou pri každej našej činnosti, je neustále monitorovaná a hodnotená odstupňovaným prístupom, prostredníctvom pravidelných samohodnotení vykonávaných jednotlivými útvarmi, resp. elektrárňami a nezávislých hodnotení realizovaných útvarom bezpečnosti (NOS), previerkami WANO (World Association of

Nuclear Operators), misiami OSART z MAAE (Medzinárodná Agentúra pre Atómovú Energiu) a verifikačnými misiami Európskej komisie.

Útvar nezávislého hodnotenia jadrovej bezpečnosti – NOS (Nuclear Oversight) hodnotí výkonnosť slovenských elektrární najmä na základe hlavných prevádzkových výkonnostných ukazovateľov, kritérií a cieľov WANO. Poslaním NOS je identifikovať možné oblasti na trvalé zlepšovanie bezpečnosti, v čom mu pomáha aj medzinárodný Poradný výbor jadrovej bezpečnosti – NSAC (Nuclear Safety Advisory Committee), ktorý hodnotí na základe skúseností prevádzkovateľov jadrových elektrární vo svete nezávisle úroveň jadrovej bezpečnosti v SE, a.s. a navrhuje vedeniu odporúčania pre jej neustále zvyšovanie. Členovia NSAC taktiež poskytujú svoje rady generálnemu riaditeľovi, riaditeľovi úseku výroby, ako aj ďalším vedúcim zamestnancom zodpovedným za bezpečnú prevádzku jadrových zariadení.

V SR podrobnosti o bezpečnosti jadrových zariadení riešia:

- Zákon č. 541/2004 Z. z. o mierovom využívaní jadrovej energie (atómový zákon) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- Zákon č. 238/2006 Z. z. o Národnom jadrovom fonde na vyraďovanie jadrových zariadení a na nakladanie s vyhoretým jadrovým palivom a rádioaktívnymi odpadmi (zákon o jadrovom fonde) a o zmene a doplnení niektorých zákonov,
- Vyhláška ÚJD SR č. 51/2006 Z. z., ktorou sa ustanovujú podrobnosti o požiadavkách na zabezpečenie fyzickej ochrany,
- Vyhláška ÚJD SR č. 48/2006 Z. z., ktorou sa ustanovujú podrobnosti o spôsobe ohlasovania prevádzkových udalostí a udalostí pri preprave a podrobnosti o zisťovaní ich príčin,
- Vyhláška ÚJD SR č. 55/2006 Z. z. o podrobnostiach v havarijnom plánovaní pre prípad nehody alebo havárie,
- Vyhláška ÚJD SR č. 57/2006 Z. z. ktorou sa ustanovujú podrobnosti o požiadavkách pri preprave rádioaktívnych materiálov.

9.3.1 Prevencia jadrových havárií

Havarijné plánovanie je súbor opatrení a postupov na zisťovanie a zdolávanie nehôd alebo havárií na jadrových zariadeniach a na zisťovanie a zmierňovanie a odstraňovanie následkov úniku rádioaktívnych látok do životného prostredia pri nakladaní s jadrovými materiálmi, s rádioaktívnymi odpadmi alebo s vyhoretým jadrovým palivom a pri preprave rádioaktívnych materiálov.

Havarijné plány sa delia na:

a) **Predbežný vnútorný havarijný plán**, ktorý obsahuje plánované opatrenia na území jadrového zariadenia alebo viacerých jadrových zariadení počas jeho alebo ich výstavby,
b) **Vnútorný havarijný plán,** ktorý obsahuje plánované opatrenia na území jadrového zariadenia alebo viacerých jadrových zariadení, ktoré prevádzkuje jeden držiteľ povolenia, a väzbu na Plán ochrany obyvateľstva a popisuje:
   - systém klasifikácie udalosti,
   - postup hodnotenia,
   - reakcie na havárie a zodpovednosť určených pracovníkov v jej priebehu,
   - systém vyrozumenia a varovania obyvateľstva a personálu JZ,
   - ochranné opatrenia a spôsob ich zavedenia,
   - plán zdravotníckych opatrení,
   - zásady obnovy,
   - spolupracujúce externé organizácie a orgány,
   - systém prípravy personálu a členov organizácie havarijnej odozvy,
   - spôsob osvety a informovania verejnosti.

c) **Plán ochrany obyvateľstva krajov v oblasti ohrozenia** – obsahuje opatrenia na ochranu obyvateľstva, zdravia, majetku a životného prostredia v oblasti ohrozenia v prípade rizika úniku rádioaktívnych látok alebo ich úniku do okolia jadrového zariadenia a väzbu na vnútorný havarijný plán.
d) **Havarijný dopravný poriadok** – spracováva sa na účely prepravy a dopravy jadrového paliva a obsahuje opatrenia v prípade úniku rádioaktívnych látok alebo ich úniku do okolia v súvislosti s prepravou rádioaktívnych látok alebo odpadov. Spracovávajú ich:
   - prevádzkovateľ jadrového zariadenia – preprava po komunikáciách v jeho správe,
   - železničný prepravcovia – na prepravu po tratiach ŽSR.

Obr. 22 Havarijné plánovanie

9.3.2 Fyzická ochrana jadrových zariadení

Podrobnosti o požiadavkách na zabezpečenie fyzickej ochrany jadrových zariadení ustanovuje Vyhláška ÚJD SR č. 51/2006 Z. z.

Fyzickou ochranou jadrových zariadení sa rozumie súbor technických, režimových alebo organizačných opatrení potrebných na zabránenie a zistenie neoprávnených činností s jadrovými zariadeniami, jadrovými materiálmi, špeciálnymi materiálmi a zariadeniami, pri nakladaní s rádioaktívnymi odpadmi, vyhoretým jadrovým palivom, pri preprave rádioaktívnych materiálov, ako aj neoprávneného vniknutia do jadrového zariadenia a vykonania sabotáže.

Účelom systému fyzickej ochrany jadrových zariadení je zabezpečiť:

a) prístup do stráženého priestoru, chráneného priestoru a vnútorného priestoru len osobám alebo vozidlám, ktorým bolo vydané povolenie na vstup alebo na vjazd do vymedzeného priestoru,
b) aby osoby oprávnene vstupujúce do stráženého priestoru, chráneného priestoru a vnútorného priestoru nezneužili toto povolenie na neoprávnenú činnosť,
c) kombináciou elektronického zabezpečovacieho systému a mechanických zábranných prostriedkov včasnú detekciu narušiteľov a spomalenie ich postupu, a tak umožniť zásahovej jednotke zastaviť ich ešte pred neoprávnenou činnosťou.

Stavebné objekty a technologické systémy jadrových zariadení, jadrové materiály alebo rádioaktívne odpady zaradené do:

- **I. kategórie** sa umiestňujú do **vnútorného priestoru,**
- **II. kategórie** sa umiestňujú do **chráneného priestoru,**
- **III. kategórie** sa umiestňujú do **stráženého priestoru.**

Stráženým priestorom je priestor, ktorého obvod je ohraničený mechanickými zábrannými prostriedkami, ak je to uvedené v predbežnom pláne fyzickej ochrany aj elektronickým zabezpečovacím systémom.

Chráneným priestorom je priestor vnútri stráženého priestoru, ktorého obvod je ohraničený mechanickými zábrannými prostriedkami vybavenými elektronickým zabezpečovacím systémom.

Vnútorným priestorom je priestor v budove alebo v miestnosti nachádzajúcej sa vnútri chráneného priestoru, ktorej steny tvoria mechanické zábranné prostriedky, a je vybavený elektronickým zabezpečovacím systémom,

Riadiace centrum sa umiestňuje vnútri stráženého priestoru v budove, ktorej steny, dvere, prípadne okná sú odolné proti prestreleniu. Riadiace centrum sa umiestňuje tak, aby z vonkajšej strany stráženého priestoru nebolo možné sledovať činnosť obsluhy vnútri riadiaceho centra. Zariadenie riadiaceho centra sa nepretržite obsluhuje.

Bariéry stráženého priestoru, chráneného priestoru a vnútorného priestoru sa konštruujú tak, aby ich nebolo možné neoprávnene prekonať v čase kratšom, ako je čas potrebný na spoľahlivé spozorovanie narušiteľa priemyselnou televíziou alebo členmi ochrany. Tieto bariéry sa osvetľujú tak, aby určení členovia ochrany mohli priamo alebo priemyselnou televíziou spoľahlivo spozorovať ich prekonávanie.

Predbežný plán fyzickej ochrany obsahuje:

a) súbor údajov charakterizujúci možné ohrozenie jadrových zariadení, jadrových materiálov alebo rádioaktívnych odpadov v čase prípravy projektu fyzickej ochrany s prihliadnutím na možné zhoršenie bezpečnostnej situácie počas predpokladanej prevádzky jadrového zariadenia, a to počet narušiteľov, ich výzbroj, výcvik, použitý dopravný prostriedok a motiváciu,
b) zhodnotenie lokality stavby a miestnych podmienok z hľadiska fyzickej ochrany,
c) predbežné zhodnotenie rizík z neoprávnených činností,
d) analýzu možností neoprávnených činností a zhodnotenie ich následkov,
e) zaradenie jadrového zariadenia a jadrových materiálov do jednotlivých kategórií,
f) dokumentáciu o zabezpečovaní kvality projektovania a realizácie fyzickej ochrany,
g) analýzu funkcie fyzickej ochrany počas výstavby, uvádzania do prevádzky, prevádzky a vyraďovania jadrového zariadenia a prípadných prevádzkových udalostí,
h) opis opatrení fyzickej ochrany v priebehu výstavby jadrového zariadenia.

Plán fyzickej ochrany obsahuje:

a) zmeny pôvodného konštrukčného riešenia obsiahnutého v predbežnom pláne fyzickej ochrany s preukázaním, že tieto neznížia úroveň fyzickej ochrany,
b) zhodnotenie výsledkov skúšok fyzickej ochrany,
c) režimové opatrenia,
d) spôsob ochrany a kontroly osôb a vjazdov dopravných prostriedkov,
e) opis údržby a prevádzkových kontrol,
f) opatrenia týkajúce sa obmedzenia prevádzky jadrového zariadenia pri pokuse o neoprávnenú činnosť alebo pri narušení fyzickej ochrany,
g) limity a podmienky systému fyzickej ochrany.

9.4 MANAŽÉRSTVO KONTINUITY ČINNOSTÍ

Kontinuita činností *(Business Continuity*) organizácie je ***strategická spôsobilosť organizácie plánovať a reagovať na incidenty a prerušenie činností s cieľom udržať prevádzku podniku na prijateľnej, vopred stanovenej úrovni***.

Činnosťou sa môže chápať ***proces alebo súbor procesov***, realizovaných organizáciou, **ktorého výstupom je:**

- **jeden alebo viacero produktov,**
- **alebo poskytovanie jednej alebo viacerých služieb**.

Kontinuita (nepretržitá súvislosť, neprerušenosť, plynulosť, nepretržitosť) činností zahŕňa voľne definovaný ***súbor plánovacích, prípravných a súvisiacich aktivít,*** ktoré majú zabezpečiť, že:

- **kritické činnosti** organizácie ***budú fungovať*** navzdory vážnym incidentom alebo mimoriadnym udalostiam, ktoré by ich mohli prerušiť,
- alebo ***budú obnovené*** do prevádzkového stavu v primerane krátkom čase.

Kontinuita činností zahŕňa tri kľúčové prvky:

1. **Odolnosť**: kritické činnosti a podporná infraštruktúra sú navrhnuté a vyrobené takým spôsobom, že nebudú podstatne ovplyvnené väčšinou porúch, napríklad prostredníctvom využitia zálohovania a voľných kapacít;
2. **Obnova**: sú prijaté opatrenia na obnovenie alebo rekonštrukciu kritických a menej kritických činností, ktoré z nejakého dôvodu zlyhajú;
3. **Pohotovosť**: organizácia vytvorí všeobecnú schopnosť a pripravenosť na účinné zvládnutie ktorýchkoľvek významnejších incidentov a havárií, ktoré sa vyskytnú, vrátane tých, ktoré neboli, a asi ani nemohli byť predvídané. Opatrenia pohotovosti predstavujú poslednú možnosť reakcie v prípade, že opatrenia na odolnosť a obnovu sa v praxi ukázali ako nedostatočné.

Základom kontinuity činností sú ***normy, vývoj programu*** a podporné ***politiky, pokyny a postupy*** potrebné na *zaistenie pokračovania činností organizácie bez prerušenia, bez ohľadu na nepriaznivé okolnosti alebo udalosti*.

Celý návrh systému, jeho implementácia, podpora a údržba musia byť založené na týchto základoch, aby bola nejaká nádej na dosiahnutie kontinuity činnosti, obnovu po havárii, alebo v niektorých prípadoch, podporu systému.

Celá koncepcia kontinuity činnosti je založená na ***identifikácii všetkých činností*** v rámci organizácie a ***priradení zodpovedajúcej úrovne dôležitosti*** jednotlivých činností na dosahovanie hlavných cieľov organizácie.

Analýza vplyvu jednotlivých činností je základným nástrojom na získavanie týchto informácií, určenia kritického stavu, bodu obnovy cieľov a dobu obnovy cieľov, a je teda súčasťou základu kontinuity činností. Túto analýzu je možné využiť na identifikáciu rozsahu a doby vplyvu narušenia danej činnosti na rôznych úrovniach organizácie. Napr. sa môže skúmať vplyv narušenia prevádzkových, funkčných a strategických činností organizácie. Pomocou tejto analýzy sa môžu posúdiť nielen súčasné aktivity, ale aj účinok prerušenia na významnejšie zmeny činnosti, zavádzanie nového výrobku alebo služby.

Väčšina noriem vyžaduje, aby analýza vplyvu činností bola preskúmaná v definovaných intervaloch vhodných pre každú organizáciu a vždy pri nasledujúcich situáciách:

- významné zmeny vnútorných podnikových procesov, umiestnenia alebo technológie,

- významné zmeny vo vonkajšom podnikateľskom prostredí, napríklad na trhu alebo zmeny právnych predpisov.

Manažérstvo kontinuity činností *(Business Continuity Management – BCM)* predstavuje proces podporovaný vedením organizácie, pri ktorom sa ***identifikujú*** potenciálne dopady udalostí ohrozujúcich činnosť organizácie a ktorého ***cieľom*** je vytvoriť také postupy a prostredie, ktoré umožní správnou reakciou zabezpečiť ***kontinuitu a obnovu kritických procesov a činností*** organizácie na vopred stanovenú úroveň v prípade ich narušenia alebo straty.

Manažérstvo kontinuity činností, na **rozdiel od predchádzania závažným haváriám v priemyselných odvetviach,** predstavuje v ktorejkoľvek organizácii proces, ktorý rieši ***narušenie kontinuity*** vo všetkých druhoch ***hlavných a podporných činností*** vplyvom vážnych incidentov alebo mimoriadnych udalostí.

Na manažérstvo kontinuity činností sa v organizáciách vytvára **Systém manažérstva kontinuity činností** – *Business Continuity Management System – SBCM, ktorý bude charakterizovaný v druhom diele učebnice.*

Na riešenie manažérstva kontinuity činností sú v súčasnosti zavedené **normy:**

- **ISO 22301:2012 Spoločenská bezpečnosť – Systémy manažérstva kontinuity činnosti – Požiadavky** – špecifikuje požiadavky na plánovanie, vytvorenie, zavedenie, prevádzkovanie, monitorovanie, hodnotenie, udržiavanie a neustále zlepšovanie zavedeného Systému manažérstva kontinuity činností na ochranu pred incidentmi, 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 praktické poradenstvo týkajúce sa manažérstva kontinuity činností.
- **ISO / IEC 27031:2011, Informačná bezpečnosť – Bezpečnostné techniky – Pokyny pre prípravu IKT na zabezpečenie kontinuity činnosti.**

9.5 LITERATÚRA

BETUŠ, Ľ. [2014]: *Chráň náš svet, chráň svoj život, pomáhaj ohrozeným*. In: Civilná ochrana 2/2014. ISSN 1335-4094.

MARKOŠ, J. – LABOVSKÁ, Z. [2013]: *Reaktorové inžinierstvo I,* Vydavateľstvo STU, Bratislava, ISBN: 978-80-227-4056-2.

SHARP, J. [2009]: *Jak postupovat při řízení kontinuity činností. Praha : překlad a interpretace pro Risk Analysis Consultants, 2009.* ISBN 978-80-254-3992 - 0.

ŠOUČÍKOVÁ, Ľ. a spol. [2005]: *Závažné priemyselné havárie a ich následky.* Žilina: Žilinská univerzita, FŠI. ISBN 80-8070-467-8.

10 POČÍTAČOVÁ BEZPEČNOSŤ

Informačné a komunikačné technológie skr. **IKT** (*Information and Communication(s) Technology, ICT)* sú technológie, ktoré umožňujú elektronicky zaznamenávať, uchovávať, vyhľadávať, spracovávať, prenášať a šíriť informácie. Ide teda o kombináciu informačnej technológie (techniky) a komunikačnej technológie (techniky).

Informačnú technológiu alebo informačné technológie možno definovať ako systémy, zariadenia, komponenty a softvér, ktoré sú potrebné na zabezpečenie vyhľadávania, spracovania a ukladania informácií vo všetkých centrách ľudskej činnosti (domov, úrad, továreň atď.), a ktorých použitie vo všeobecnosti vyžaduje použitie elektroniky alebo podobnej technológie *(ISO/IEC 38500:2008 – Corporate governance and information technology).*

Termín informačná technika sa používa buď ako synonymum termínu informačná technológia alebo sa (správnejšie) obmedzuje na „fyzickú“ (organizačnú, výpočtovú, reprografickú a prípadne aj telekomunikačnú) techniku používanú pri práci s informáciami *(Paulička, 2002).*

Počítačová bezpečnosť (Bezpečnosť informačných a komunikačných technológií) je **oblasť vedy o počítačoch** *(computer science)*, ktorá sa zaoberá ***odhaľovaním a eliminovaním rizík spojených s používaním počítača.***

V zmysle informatizácie sa počítačová bezpečnosť definuje ako *„schopnosť siete alebo informačného systému ako celku odolať s určitou úrovňou spoľahlivosti náhodným udalostiam, alebo nezákonnému, alebo zákernému konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu a dôvernosť uchovávaných alebo prenášaných údajov a súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a systémov“ (Bíro, 2008).*

Narušenie bezpečnosti môže zahŕňať čokoľvek – počnúc poškodením vzhľadu webovej stránky, cez napadnutie počítača, resp. systému škodlivým softvérom, zlyhanie zamestnanca, ktorý neúmyselne prezradí svoje heslo, bývalého zamestnanca, ktorý sabotuje zákaznícku databázu až po priemyselných špiónov, ktorí zistia, koľko tovaru si zakúpil váš najlepší zákazník v minulom mesiaci. Vo všeobecnosti, najväčšiu časť tvoria krádeže, zneužitia a neoprávnené manipulácie s informáciami (teda údajmi).

Keďže spoločnosť speje k stále významnejšiemu využívaniu IKT v každodennom živote, význam informačnej bezpečnosti a jej dodržiavania úmerne narastá. Informačná bezpečnosť má veľký záber a pokrýva široké spektrum problematík, pričom s rozvojom IKT sa vynárajú stále ďalšie oblasti, ktoré sem patria a naopak zanikajú niektoré staré, aj keď v porovnateľne menšom meradle.

Cieľom počítačovej bezpečnosti je zabezpečiť:

- ochranu pred neoprávneným manipulovaním so zariadeniami počítačového systému,
- ochranu pred neoprávnenou manipuláciou s dátami, ochrana narušenia celistvosti, dôvernosti a dostupnosti,
- ochranu pred nelegálnou tvorbou kópií dát,
- bezpečnú komunikáciu a prenos dát,
- bezpečné uloženie dát.

Systémová ochrana utajovaných skutočností stupňa Dôverné a vyšších stupňov spracúvaných na technických prostriedkoch sa zabezpečuje ***systémovými prostriedkami s odporúčaným bezpečnostným nastavením.***

Medzi **bezpečnostne posudzované systémové prostriedky** patria najmä:

a) operačné systémy, ich jednotlivé verzie a modifikácie,
b) databázové systémy,
c) produkty na správu a prevádzku počítačových sietí,
d) produkty na správu a prevádzku elektronickej pošty,
e) firewally a špeciálne systémové bezpečnostné produkty,
f) iné funkčne špecializované systémové produkty určené na tvorbu, spracovanie, prenos alebo na uchovávanie utajovaných skutočností.

Počítačová bezpečnosť sa dosahuje aplikovaním bezpečnostných opatrení z oblasti ***počítačovej a komunikačnej, kryptografickej a emisnej bezpečnosti*** na ochranu utajovaných skutočností spracovávaných, uchovávaných, zobrazovaných alebo prenášaných ***v komunikačných, informačných a iných elektronických systémoch*** proti náhodnej, nedbanlivostnej alebo úmyselnej strate dôvernosti, integrity alebo dostupnosti, ako aj proti strate integrity a dostupnosti samotných systémov, a opatreniami zamedzujúcimi popretie vykonanej operácie, resp. služby.

Informačná istota znamená zaistenie, že dáta sa nestratia, keď nastanú kritické problémy, ako sú: *prírodné kalamity, zlyhávanie počítača alebo serveru, fyzická krádež alebo iný prípad, kedy sa môžu údaje stratiť*. Od doby, keď je väčšina informácií uložená v počítačoch, zaisťujú ich odborníci na bezpečnosť IT. Jeden z najbežnejších spôsobov zaistenia informácií je ich zálohovanie.

Počítačová bezpečnosť zahŕňa (*Sarnovský, 2015*):

- fyzickú bezpečnosť,
- bezpečnosť technického a programového vybavenia,
- komunikačnú bezpečnosť,
- bezpečnosť dát,
- režimovú bezpečnosť,
- personálnu bezpečnosť.

Fyzická bezpečnosť *(Physical Security, PHYSEC)* predstavuje pôsobenie hrozieb na hmotné aktíva potrebné na prevádzkovanie informačného systému. Ide o:

- ochranu informačného systému a jeho častí proti neoprávnenému vniknutiu osôb – prevencia a detekcia neoprávneného vniknutia,
- spôsoby zničenia už nepotrebných informácií alebo už nepotrebných médií s informáciami (archivačných médií, tlačových a iných výstupov informačného systému),
- ochranu proti požiaru, vode,
- plánovanie prevencie havárií systému a riešenie krízových situácií (tzv. krízový manažment).

Bezpečnosť technického a programového vybavenia *(Computer Security, COMPUSEC)* zahŕňa hrozby na hmotné aj nehmotné aktíva potrebné na spracovanie informácií, v praxi sa ďalej delí na:

- ***bezpečnosť technického vybavenia*** – výber a spoľahlivosť týchto prostriedkov, zabezpečenie ich okamžitého servisu, kontrola prístupu k týmto prostriedkom, ich ochrana pred elektrostatickou elektrinou a elektromagnetickým vyžarovaním.
- ***bezpečnosť programového vybavenia*** – vyladenie operačného systému takým spôsobom, aby bol skutočným filtrom prístupu k informáciám uloženým v IS – t. j. aby bola zabezpečená kontrola prístupu, identifikácia a autentizácia užívateľov, rozdelenie právomocí.

Komunikačná bezpečnosť *(Communications Security, COMSEC)* vyžaduje eliminovanie hrozby pre hmotné i nehmotné aktíva nevyhnutné pre komunikáciu. Zahŕňa technické vybavenie, i všeobecné štruktúry (napr. definície komunikačných protokolov). Ide teda o ochranu komunikácií medzi jednotlivými časťami informačného systému a to nielen z hľadiska výpočtovej techniky, ale aj z hľadiska prenosu faxových správ alebo telefonických rozhovorov.

Bezpečnosť dát alebo **informačná bezpečnosť** *(Information Security, INFOSEC)* predstavuje ***ochranu dát v súboroch a databázach a citlivých dát.*** Zahŕňa pôsobenie hrozieb na nehmotné aktíva, nevyhnutné pre fungovanie IS z hľadiska organizačného spracovania informácie. Tu treba zohľadniť najmä citlivosť, životnosť, platnosť dát a pod. Niekedy sa označuje ako ***technická bezpečnosť informačného systému*** *(Technical Security).* Bezpečnosť dát znamená:

- ochranu dát v súboroch a v databázach proti chybám, vírusom,
- ochranu citlivých dát prostriedkami autorizácie a riadenia prístupu k dátam.

Režimová bezpečnosť *(Procedural Security)* predstavuje komplex administratívnych opatrení a systém kontrol na zaistenie bezpečnosti informačného systému znamená:

- určenie spôsobov, postupov a procedúr vstupu a pohybu osôb v objekte (priestore) a ich evidenciu,
- výber osôb pre činnosť na citlivých úsekoch,
- definovanie oprávnených a zakázaných činností v informačnom systéme,
- použitie šifrovej ochrany,
- označovanie a evidenciu médií a postup pri ich ničení,
- bezpečné zálohovanie dát,
- vedenie užívateľských účtov,
- postup prihlásenia sa do IS a odhlásenia,
- metodika nastavenia užívateľských práv v IS,
- spôsoby ukončenia práce v IS,
- spôsob testovania požadovaných bezpečnostných parametrov atď.

Personálna bezpečnosť *(Personnel Security, PERSEC)* predstavuje ochranu počítačových systémov ***pred neoprávnenými pracovníkmi***, zaoberá sa predovšetkým *elimináciou hrozieb spôsobených ľudským faktorom*, rieši ochranu pracovníkov ako súčasti informačného systému a ochranu IS pred dôsledkami udalostí spôsobených nekorektným jednaním pracovníkov – eliminácia hrozieb spôsobených ľudským faktorom.

Zabezpečenie počítačového systému spočíva v ***zabezpečení počítačového systému pred útokom hackerov, škodlivých programov*** (vírusy, červy, trójske kone, spyware, adware a pod.). Do tejto časti patrí aj ***zaškolenie zamestnancov***, aby sa správali v súlade s počítačovou bezpečnosťou a dodržiavali etiketu na sieti.

Zabezpečenie fyzického prístupu spočíva v ***zabránení prístupu nepovolaných osôb k častiam počítačového systému.*** Na toto zabezpečenie sa používajú bezpečnostné prvky ako:

- *pridelenie rozdielnych práv zamestnancom,*
- *elektronické zámky,*
- *poplašné zariadenia,*
- *kamerové systémy,*
- *autorizačné systémy chránené heslami, čipovými kartami a pod.,*
- *autentizačné systémy na snímanie odtlačkov prstov, dlane, krvného riečiska, očnej dúhovky, rozpoznania hlasu a pod.,*

- *auditové systémy na sledovanie a zaznamenávanie určitých akcií zamestnancov (vstup zamestnanca do miestnosti, prihlásenie sa do systému, kopírovanie údajov a pod.).*

Zabezpečenie informácií spočíva v ***bezpečnom zálohovaní dát.*** Záloha dát by mala byť vytvorená tak, aby ju neohrozil útočník ani prírodná živelná pohroma (požiar, záplavy, pád lietadla). Zálohované dáta je tiež potrebné chrániť proti neoprávnenej manipulácii použitím vhodného šifrovacieho systému.

Ekonomické a právne zabezpečenie spočíva v ***správnej motivácii a postihu zamestnancov.***

OCHRANA PRED POČÍTAČOVOU KRIMINALITOU

Počítačová kriminalita sú trestné činy zamerané proti počítačom, ako aj trestné činy páchané pomocou počítača. Ide o nelegálne, nemorálne a neoprávnené konanie, ktoré zahŕňa zneužitie údajov získaných prostredníctvom výpočtovej techniky alebo ich zmenu. Počítače v podstate neumožňujú páchať nový typ trestnej činnosti, iba poskytujú novú technológiu a nové spôsoby na páchanie už známych trestných činov ako je sabotáž, krádež, zneužitie, neoprávnené užívanie cudzej veci, vydieranie alebo špionáž.

Európske krajiny považujú túto formu trestnej činnosti za jednu z globálnych hrozieb a jedným z nástrojov na jej potieranie je **Dohovor o počítačovej kriminalite** z 23.11.2001. SR tento dohovor ratifikovala v roku 2007.

Najvýraznejšími prejavmi počítačovej kriminality sú:

1. **Útok na počítač, program, údaje, komunikačné zariadenie** – z hľadiska rozsahu najväčších škôd pravdepodobne najväčší podiel patrí *nelegálnej tvorbe a predaju autorsky chráneného programového vybavenia* v počítačovom slangu označovaná ako Warez.
2. **Neoprávnené užívanie počítača alebo komunikačného zariadenia** *(na vlastnú zárobkovú činnosť.*
3. **Neoprávnený prístup k údajom, získanie utajovaných informácií (počítačová špionáž) alebo iných informácií o osobách, činnosti a pod.** – v súvislosti s týmto trestným činom môže byť aj súbežný trestný čin ako napr. *vydieranie, nekalá súťaž, ohrozenie hospodárskeho tajomstva, vyzvedačstvo, ohrozenie štátneho tajomstva*.
4. **Krádež počítača, programu, údajov, komunikačného zariadenia.**
5. **Zmena v programoch a údajoch (okrajovo i v technickom zapojení počítača resp. komunikačného zariadenia.**
6. **Zneužívanie počítačových prostriedkov na páchanie inej trestnej činnosti** – napr. zostavy v skladoch, tržby, nemocenské poistenie, stavy pracovníkov, stav účtov a pod., patria sem aj krádeže motorových vozidiel, falšovanie technickej dokumentácie, priekupníctvo, daňové podvody, falšovanie a pozmeňovanie cenín, úradných listín a dokladov, dokonca aj peňazí.
7. **Podvody páchané v súvislosti s výpočtovou technikou** – využitie omylu niekoho vo svoj prospech.
8. **Šírenie poplašných správ** – tieto správy sú v počítačovom slangu označovaná ako Hoax.

Používanie, šírenie a vytváranie prostriedkov na odstránenie ochranných prvkov určených na chránenie autorských diel alebo používanie a šírenie takto upravených autorských diel, s ktorými sa nakladá v rozpore s autorským právom je najviac rozšírenou trestnou činnosťou. Takéto prostriedky sa v počítačovom slangu nazývajú **Warez.** Ľudia, zaobchádzajúci s týmito prostriedkami, bývajú označovaní ako ***softvéroví piráti.***

Neoprávnené vniknutie do systému je ďalšou rozšírenou trestnou činnosťou. Človek zaoberajúci sa touto činnosťou sa v počítačovom slangu nazýva ***hacker.*** Najčastejšie metódy na prienik do systému sú:

- **útok hrubou silou** – spočíva vo vyskúšaní všetkých možných kombinácií znakov,
- **slovníkový útok** – spočíva v skúšaní všetkých slov daného jazyka,
- **odpočúvanie sieťovej komunikácie** – heslo sa dá veľmi jednoducho získať odpočúvaním nezabezpečených komunikačných liniek,
- **využitie neukončeného spojenia** – útočník môže využiť zabudnutie odhlásenia zo systému.
- **zadné vrátka** – útočník zostrojí program nazývaný Backdoor (zadné vrátka), ktorý mu umožní pripojiť sa do systému bez nutnosti poznať správne používateľské meno a heslo, tento program rozšíri pomocou počítačového červa alebo trójskeho koňa,
- **odchytenie hesla** – útočník zostrojí program nazývaný Keylogger, ktorý zaznamenáva stlačené klávesy a takto získané údaje mu odosiela prostredníctvom Internetu, tento program rozšíri pomocou počítačového červa alebo trójskeho koňa.

Bankové krádeže uskutočnené pomocou počítača sú zatiaľ u nás zriedkavé no vo svete sa začínajú čoraz viac vyskytovať, známe sú nasledujúce tri typy krádeží:

- **Phishing** – správy, ktoré vás pod určitou zámienkou nabádajú ku zmene osobných údajov.
- **Pharming** – presmerovanie názvu www. stránky na inú adresu (možná strata úspor).
- **Spoofing** – všetky metódy, ktoré používajú hackeri na zmenu totožnosti odosielaných správ.

Možnosti ochrany proti útokom sa môžu rozdeliť na tri skupiny:

- **prevencia**: ochrana pred hrozbami – uvedomiť si bezpečnostné nedostatky siete a vytvoriť krízový plán pre prípad útoku, určiť postupnosť potrebných krokov a zodpovednosti.
- **detekcia**: odhalenie neoprávnenej činnosti a slabého miesta v systéme – vytvoriť prostriedky a stanoviť kritériá pre detekciu útoku, vytvoriť postupy a algoritmy pre prípad veľkého objemu dátovej komunikácie.
- **náprava**: odstránenie slabého miesta v systéme – zaistiť schopnosť odhaliť rozsah útoku, identifikovať zdroje útoku, zablokovať fungovanie z týchto zdrojov a posunúť dostatočné informácie o útoku k ďalším právnym krokom.

Ochrana pred počítačovou kriminalitou zahŕňa dve základné zložky: *prevenciu a represiu* (tab. 12).

Tab. 12 Ochrana pred počítačovou kriminalitou

PREVENCIA	REPRESIA
• **psychologická prevencia** – zavádzanie opatrení, ktoré pomáhajú vytvárať povedomie o nemorálnosti a neprijateľnosti právom zakázaných činov, • **technologická prevencia** – zabezpečenie, ide o vytváranie novších programov a systémov na ochranu pred trestnými činmi páchanými pomocou počítačov.	• rieši ju **polícia a súdy**, ide o vyšetrovanie správnych deliktov, priestupkov a trestných činov a tiež ukladanie sankcií, ktoré sú stanovené zákonom, • práca represívnych zložiek v oblasti počítačovej kriminality je náročná, a to nielen po technologickej stránke, ale aj zo strany dokazovania protiprávneho konania.

V súčasnosti medzi odborníkmi prevláda názor, že dokonalá ochrana v oblasti počítačovej kriminality neexistuje. V dôsledku toho je ochrana proti počítačovej kriminalite podporovaná aj zákonnými obmedzeniami. Typickým prípadom je autorský zákon, ktorý zakazuje užívateľom prekonávať alebo obchádzať ochranu, a to aj v prípade, ak je ochrana nedokonalá.

Riešenie počítačových bezpečnostných incidentov

Bezpečnostný incident na informačnom systéme je úmyselné využitie zraniteľnosti na spôsobenie škody alebo straty na aktívach informačného systému alebo neúmyselné vykonanie akcie, ktorej výsledkom je škoda na aktívach, ďalej je to akékoľvek narušenie bezpečnosti informačných systémov a sietí subjektu, ako aj akékoľvek porušenie bezpečnostnej politiky a súvisiacich pravidiel.

Ministerstvo financií SR zriadilo **Computer Security Incident Response Team Slovakia – CSIRT.SK** s cieľom zabezpečiť primeranú úroveň ochrany národnej informačnej a komunikačnej infraštruktúry – NIKI a kritickej informačnej infraštruktúry. Tím zabezpečuje služby spojené so zvládnutím bezpečnostných incidentov, odstraňovaním ich následkov a následnou obnovou činnosti informačných systémov v spolupráci s vlastníkmi a prevádzkovateľmi NIKI, telekomunikačnými operátormi, poskytovateľmi internetových služieb (ISP) a inými štátnymi orgánmi (napr. polícia, vyšetrovatelia, súdy), podieľa sa na budovaní a rozširovaní poznania verejnosti vo vybraných oblastiach informačnej bezpečnosti, aktívne kooperuje so zahraničnými organizáciami a reprezentuje SR v oblasti informačnej bezpečnosti na medzinárodnej úrovni.

10.1 LITERATÚRA

BÍRO, P. [2008]: *Informačná bezpečnosť*. In: Informatizácia.sk, Ministerstvo financií SR.

ČABÁK, P. [2013]: *Právna úprava spamu (nevyžiadanej pošty).* In: Právo v kultúre, Konferencia Národného centra práva duševného vlastníctva 28.-29.11.2013. Košice.

DOSEDĚL, T. [2004]: *Počítačová bezpečnost a ochrana dat.* Computer Press, 2004 ISBN: 80-2510-106-1.

MATĚJKA, M. [2002]: *Počítačová kriminalita,* Computer Press Praha, ISBN 80-7226-419-2 (brož.), 106 s.

PAULIČKA, I., [2002]: *Všeobecný encyklopedický slovník* (4 zväzky A-F, G-L, M-R a S-Ž), Ottovo nakladatelství Cesty, Praha.

SARNOVSKÝ, M. [2015]: *Riadenie IT Prostredia*. Technická univerzita v Košiciach.

11 INFORMAČNÁ BEZPEČNOSŤ

V polovici 70. rokov minulého storočia nastali výrazné zmeny, keď najdôležitejším zdrojom a motorom hospodárskeho rozvoja prestávajú byť hmotné zdroje (energia, vyrobené produkty), ale stávajú sa ním **informácie, znalosti a nové technológie.** Hlboké zmeny, ktoré v súčasnosti prebiehajú v globálnej spoločnosti sa považujú za známky prechodu k **informačnej spoločnosti.** Podstatná časť ľudí prechádza od práce priamo vo výrobe k práci úzko spojenej s využitím **informatiky** a **informačných technológií**.

Informačná spoločnosť je prostredím, v ktorom ***informácie majú prvoradý význam,*** je to **spoločnosť, *v ktorej informatika, počítače a mikroelektronika určujú a premeňujú celý spoločenský systém,*** vystupujú ako prostriedok vytvorenia nových spoločenských, nadtriednych a nadnárodných štruktúr a zásadným spôsobom menia mechanizmy spoločenského vývoja. Jej nástup urýchľujú možnosti nových **informačných a komunikačných technológií.**

Informačnú spoločnosť možno charakterizovať aj ako **spoločnosť, v ktorej sú informácie prostredníctvom moderných informačných a komunikačných technológií intenzívne využívané na jej všestranný rozvoj,** používa ich vo veľkej miere na:

- stimuláciu ekonomického rastu, najmä na rozvoj obchodu a služieb,
- uľahčenie a skvalitnenie života občanov (vzdelávanie, kultúra, zdravotníctvo, prístup k úradom,
- rozvoj informačného priemyslu (tvorba informácie, prenos a odovzdávanie používateľom, výroba hardvéru a softvéru na spracovanie informácií).

Informácie sú životne dôležité pre všetky organizácie, ***patria k ich najdôležitejším konkurenčným aktívam***. Informácie sa stávajú ***tovarom s vysokou trhovou hodnotou***. Ich nedotknuteľnosť podmieňuje budúce úspechy a mnohokrát je otázkou prežitia. Ochrana ekonomických a technologických záujmov existuje v každej spoločnosti a v súčasnosti jej potreba ešte narastá.

Najväčšou obavou spoločností i verejných inštitúcií zostáva hrozba straty dát a riziko úniku informácií. Popri tom stále stúpa obava podnikových IT profesionálov z napadnutia škodlivým softvérom. K ďalším vážnym hrozbám patria neúmyselné úniky dát cez zamestnancov firiem, alebo naopak sabotáž, teda zámerné vynesenie informácií zo spoločnosti.

Informačná bezpečnosť je podľa medzinárodnej normy ISO/IEC 27001 ochrana informácie pred širokým spektrom hrozieb, ktorej cieľom je:

- **zaistenie kontinuity prevádzky,**
- **minimalizácia strát a**
- **maximalizácia návratnosti investícií.**

Informačná bezpečnosť znamená ochranu ***informácií*** a ***informačných a telekomunikačných technológií.*** Je to všeobecný termín pre akúkoľvek formu informácií (elektronické, fyzické a iné). V súčasnej dobe sa zameriava prevažne na informácie v digitálnej podobe, v plnom rozsahu však zahŕňa nielen digitálnu, ale aj ich analógovú alebo fyzickú podobu.

Zabezpečovanie informácií je interdisciplinárne a okrem informatiky čerpá z rôznych odborov, vrátane manažmentu, účtovníctva, vyšetrovania podvodov, forenznej vedy, systémového inžinierstva, bezpečnostného inžinierstva a kriminológie.

Informačná bezpečnosť má veľký záber a pokrýva široké spektrum problematík, pričom s rozvojom IKT sa vynárajú stále ďalšie oblasti, ktoré sem patria a naopak zanikajú niektoré staré, aj keď v porovnateľne menšom meradle.

Informačná bezpečnosť je len jedna a je rozhodne odporúčané, aby sa pri jej zavádzaní a dodržiavaní myslelo na všetky jej aspekty, nezávisle od toho, či sa chránia špecifické typy informácií alebo systémov, alebo tie úplné všeobecné. Informačná bezpečnosť je inak povedané aj vyváženie rizík výhodami v podobe vykonávania činnosti elektronicky. Keďže spoločnosť speje k stále významnejšiemu využívaniu IKT v každodennom živote, význam informačnej bezpečnosti a jej dodržiavania úmerne narastá.

Riadenie a hlavné dokumenty informačnej bezpečnosti

Na Slovensku majú informačnú bezpečnosť na starosti rôzne orgány:

- **Národný bezpečnostný úrad** (NBÚ) zastrešuje ***ochranu utajovaných skutočností,***
- **Ministerstvo financií** (MF) **spravuje** ***ochranu všetkých ostatných údajov (tzv. neutajovaných),***
- **Ministerstvo kultúry** (MK) rieši ***ochrana digitálnych autorských práv,***
- **Úrad na ochranu osobných údajov** (ÚOOÚ) spravuje ***ochranu osobných údajov.***

Súčasný právny poriadok SR síce obsahuje viacero právnych noriem, ktoré riešia čiastkové problémy, a tak pokrývajú špecifické oblasti informačnej bezpečnosti, ale jednotný, všeobecný právny predpis pre informačnú bezpečnosť digitálneho priestoru v slovenských právnych normách chýba. Absencia takého zákona sa prejavuje napríklad v:

- nejednotnosti terminológie,
- nedostatočnom používaní bezpečnostných štandardov,
- prekrývajúcich sa kompetenciách štátnych orgánov,
- neúplnosti pokrytia informačnej bezpečnosti právnymi predpismi a kompetenciami.

Návrh právneho zámeru zákona o informačnej bezpečnosti je koncipovaný v súlade so stavom a vývojom informačných a komunikačných technológií, reflektuje zmeny v organizácii štátnej správy a územnej samosprávy a zohľadňuje smernice a odporúčania Európskej únie, medzi ktoré patria:

a) Návrh smernice Európskeho parlamentu a Rady o opatreniach na zabezpečenie vysokej úrovne bezpečnosti sietí a informácií v Únii (2013).
   - Zavedenie minimálnej úrovne bezpečnosti sietí a informácií v členských štátoch, a tým zvýšenie celkovej úrovne pripravenosti a reakcie na incidenty.
   - Zlepšenie spolupráce v oblasti bezpečnosti sietí a informácií na úrovni EÚ v záujme efektívneho boja proti cezhraničným počítačovým incidentom a hrozbám.
   - Vytvorenie kultúry riadenia rizika a zlepšenie výmeny informácií medzi súkromným a verejným sektorom.

b) Stratégia pre kybernetickú bezpečnosť EÚ.

c) Smernice a nariadenia EÚ/EK.

Hlavným dokumentom, ktorý sa zaoberá oblasťou informačnej bezpečnosti v SR, je **Národná stratégia pre informačnú bezpečnosť SR**, ktorú 27.8.2008 schválila Vláda SR (Uznesenie Vlády SR č. 570/2008 Z. z.). Dokument má tri základné úrovne:

1. Prvá úroveň popisuje **strategické ciele** SR v informačnej bezpečnosti, ktoré majú dlhodobý charakter a pokrývajú všetky dôležité problémy.
2. Druhá úroveň je zameraná na **popis strategických priorít**.
3. Tretia úroveň definuje **najdôležitejšie problémy**, ktoré sú premietnuté do kľúčových úloh.

Obsahom stratégie sú aj východiská, kompetenčné rozloženie právomocí, návrh smerovania, priorít a krokov na dosiahnutie cieľa. Súčasťou dokumentu je aj základný popis jednotlivých úloh s cieľom zabezpečiť ochranu digitálneho priestoru Slovenska v rozsahu neuta-

jovaných informácií. Z hľadiska práce s informáciami sem patria najmä únik informácií, neoprávnené použitie informácií a narušenie integrity údajov.

K stratégii bol vypracovaný **Akčný plán na roky 2008 až 2013,** ktorý bol 19.1.2010 schválený vládou SR *(Uznesenie Vlády SR č. 46/2010 Z. z.).*

Strategickými cieľmi v oblasti informačnej bezpečnosti podľa neho sú:

a) **prevencia** – zaistenie adekvátnej ochrany digitálneho priestoru SR, aby sa v maximálnej možnej miere predchádzalo bezpečnostným incidentom v ňom,
b) **pripravenosť** – zaistenie schopnosti efektívne reagovať na bezpečnostné incidenty, minimalizovať ich dosah a čas potrebný na obnovu činnosti informačných a komunikačných systémov po bezpečnostných incidentoch,
c) **udržateľnosť** – dosiahnutie, udržiavanie a rozširovanie kompetencie SR v oblasti informačnej bezpečnosti.

Pre dosiahnutie stanovených strategických cieľov je potrebné doriešiť právne normy, kompetencie, technicko-organizačné a finančné záležitosti, hierarchiu a spôsob riadenia, vzdelávanie a mnoho ďalších problémov. Národná stratégia pre informačnú bezpečnosť definuje sedem **základných strategických priorít**, ktorými sú:

- ochrana ľudských práv a slobôd v súvislosti s využívaním Národnej informačnej a komunikačnej infraštruktúry (NIKI),
- budovanie povedomia a kompetentnosti v informačnej bezpečnosti,
- vytváranie bezpečného prostredia,
- zefektívnenie riadenia informačnej bezpečnosti,
- zaistenie dostatočnej ochrany štátnej IKI a IKI podporujúcej kritickú infraštruktúru štátu,
- národná a medzinárodná spolupráca,
- rozširovanie národných kompetencií.

Okrem týchto dvoch noriem medzi **ďalšie východiskové dokumenty pre návrh zákona o informačnej bezpečnosti patria:**

- Zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci (Zákon o e-Governmente).
- Budovanie povedomia a kompetentnosti v oblasti informačnej bezpečnosti – Návrh systému vzdelávania v oblasti informačnej bezpečnosti v SR, uznesenie vlády SR č. 391/2009 Z. z.
- Zriadenie jednotky pre riešenie počítačových incidentov CSIRT.SK (MF SR / Data Centrum), uznesenie vlády SR č. 479/2008 Z. z.
- Legislatívny zámer zákona o informačnej bezpečnosti, Uznesenie Vlády SR č. 136/2010 Z. z.

Pripravovaný zákon o informačnej bezpečnosti má riešiť dva okruhy problémov:

- zaistenie ochrany pre informačné systémy verejnej správy,
- vytvorenie všeobecného právneho rámca pre ochranu celého digitálneho priestoru SR.

Cieľom Zákona o informačnej bezpečnosti má byť vytvorenie uceleného, koordinovaného a efektívneho systému ochrany informačných systémov verejnej správy SR. Keďže informačné systémy verejnej správy sú súčasťou širšieho digitálneho priestoru, ktorého značná časť je v súkromných rukách, zákon vytvára podmienky na zvyšovanie úrovne informačnej bezpečnosti v celom digitálnom priestore SR prostredníctvom štandardizácie informačnej bezpečnosti.

Riešenie informačnej bezpečnosti

Riešenie informačnej bezpečnosti je prierezovou disciplínou, ktorá zasahuje do všetkých častí informačných technológií a všetkých systémov, ktoré klient využíva. Cieľom riešenia je stanoviť pravidlá a následne zabezpečiť ich dodržiavanie, prípadne si ich u užívateľov aj vynútiť. Medzi **špecifické oblasti informačnej bezpečnosti** v SR možno na základe právnych predpisov zaradiť:

1. **Ochrana utajovaných skutočností**
   a) Administratívna bezpečnosť.
   b) Personálna bezpečnosť.
   c) Priemyselná bezpečnosť.
   d) Bezpečnosť technických prostriedkov.
   e) Šifrová ochrana informácií.
   f) Fyzická bezpečnosť a objektová bezpečnosť.
2. **Bezpečnosť informačných systémov**
   a) Bezpečnosť informačných systémov verejnej správy.
   b) Bezpečnosť informačných systémov poskytovateľov elektronických služieb.
   c) Trestnoprávna zodpovednosť za porušenie bezpečnosti informačných systémov.
3. **Ochrana dôležitých informácií**
   a) Ochrana osobných údajov.
   b) Ochrana obchodného tajomstva.
   c) Ochrana bankového tajomstva.
   d) Ochrana listového tajomstva.
   e) Ochrana autorských práv.
   f) Ochrana pred odpočúvaním.
   g) Ochrana súkromia pred nevyžiadanými správami.
   h) Ochrana súkromia pred neoprávneným použitím informačno-technických prostriedkov.
   i) Elektronický podpis a elektronická pečať.

11.1 BEZPEČNOSŤ INFORMAČNÝCH SYSTÉMOV VEREJNEJ SPRÁVY

Bezpečnosť informačných systémov verejnej správy riešia:

- Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov.
- Zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (Zákon o e-Governmente).
- Výnos Ministerstva financií SR č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy.
- Metodický pokyn Ministerstva financií SR č. MF/23579/2011-165 k výnosu Ministerstva financií SR z 9. júna 2010 č. 312/2010-132 Z. z. o štandardoch pre informačné systémy verejnej správy – do vydania nového metodického pokynu platný v nezmenených častiach aj pre výnos č. 55/2014 Z. z.

Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov upravuje:

a) práva a povinnosti povinných osôb v oblasti vytvárania, prevádzkovania, využívania a rozvoja informačných systémov verejnej správy,
b) základné podmienky na zabezpečenie integrovateľnosti a bezpečnosti informačných systémov verejnej správy,
c) postup pri vydávaní elektronického odpisu údajov z informačných systémov verejnej správy a výstupu z informačných systémov verejnej správy.

Informačným systémom *(Information System, IS)* je funkčný celok zabezpečujúci cieľavedomú a systematickú informačnú činnosť prostredníctvom ***technických prostriedkov*** a ***programových prostriedkov***, ktoré sú súčasťou informačného systému alebo ktoré informačnému systému poskytuje iný informačný systém. Informačným systémom sa rozumie *jeden alebo viac počítačov, ich programové vybavenie, periférne zariadenia, procesy alebo prostriedky, ktoré tvoria celok schopný vykonávať zber, tvorbu, spracovanie, ukladanie, zobrazenie a prenos utajovaných skutočností.*

V informačných systémoch spracúvajúcich utajované skutočnosti stupňov utajenia **Dôverné, Tajné a Prísne tajné** sa musí zabezpečiť nepretržité vedenie kontrolného záznamu o činnosti informačného systému a jeho zložiek s možnosťou jeho sledovania, spätného preskúmania, ako aj stanovenia zodpovednosti konkrétneho používateľa za ním vykonané aktivity v informačnom systéme.

- **Informačný systém verejnej správy** – definuje sa ako informačný systém v pôsobnosti povinnej osoby ako správcu informačného systému verejnej správy podporujúci služby verejnej správy, služby vo verejnom záujme a verejné služby.
- **Informačná činnosť** – získavanie, zhromažďovanie, spracúvanie, sprístupňovanie, poskytovanie, prenos, ukladanie, archivácia a likvidácia údajov.
- **Koncepcia** – dokument vypracovaný správcom, ktorý spravuje informačné systémy verejnej správy, definuje najmä ciele, organizačné, technické a technologické nástroje a architektúru informačných systémov verejnej správy.
- **Štandard** – súbor pravidiel spojených s vytváraním, rozvojom a využívaním informačných systémov verejnej správy, ktorý obsahuje charakteristiky, metódy, postupy a podmienky, najmä pokiaľ ide o bezpečnosť a integrovateľnosť s inými informačnými systémami. Štandardy musia byť otvorené a technologicky neutrálne.
- **Povinná osoba** – zodpovedá za vytváranie, správu a rozvoj informačného systému verejnej správy povinná osoba, ktorá je správcom a zabezpečuje výkon verejnej správy na určenom úseku verejnej správy podľa predpisov.

Povinnými osobami sú:

- Ministerstvá a ostatné ústredné orgány štátnej správy,
- Generálna prokuratúra, Najvyšší kontrolný úrad, Úrad pre dohľad nad zdravotnou starostlivosťou, Úrad na ochranu osobných údajov, Telekomunikačný úrad, Poštový regulačný úrad, Úrad pre reguláciu sieťových odvetví a iné štátne orgány,
- obce a vyššie územné celky,
- Kancelária Národnej rady SR, Kancelária prezidenta SR, Kancelária Ústavného súdu SR, Kancelária Najvyššieho súdu SR, Kancelária Súdnej rady SR, Kancelária verejného ochrancu práv, Ústav pamäti národa, Sociálna poisťovňa, zdravotné poisťovne, Tlačová agentúra SR, Slovenská televízia, Slovenský rozhlas, Rada pre vysielanie a retransmisiu,
- právnické osoby v zriaďovateľskej alebo zakladateľskej pôsobnosti povinných osôb,
- komory regulovaných profesií a komory, na ktoré je prenesený výkon verejnej moci s povinným členstvom,
- fyzické osoby a iné právnické osoby.

Povinné osoby sú povinné:

- vypracovať a aktualizovať koncepciu rozvoja informačných systémov verejnej správy,
- zabezpečovať plynulú, bezpečnú a spoľahlivú prevádzku informačných systémov verejnej správy, ktoré sú v ich správe, vrátane organizačného, odborného a technického zabezpečenia,
- zabezpečovať informačný systém verejnej správy proti zneužitiu,
- sprístupňovať verejnosti údaje z informačných systémov verejnej správy,
- sprístupňovať alebo na požiadanie poskytnúť bezplatne iným povinným osobám údaje z informačných systémov verejnej správy potrebné na ich činnosť,
- prostredníctvom centrálneho metainformačného systému verejnej správy bezodkladne sprístupňovať informácie o informačných systémoch verejnej správy, ktoré prevádzkujú a o poskytovaných elektronických službách verejnej správy,
- prednostne používať integrovanú infraštruktúru určenú na prevádzku informačných systémov verejnej správy, ak to technické možnosti umožňujú,
- poskytovať súčinnosť ministerstvu pri výkone jeho právomocí ustanovených týmto zákonom,
- zabezpečovať, aby bol informačný systém verejnej správy v súlade so štandardmi informačných systémov verejnej správy,
- spravovať príslušné základné registre a zabezpečiť ich zverejnenie,
- poskytovať ministerstvu a Úradu vlády SR prostredníctvom elektronickej služby verejnej správy vybrané údaje určené ministerstvom alebo Úradom vlády SR o informačných systémoch verejnej správy na účely štatistického zisťovania.

Zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci upravuje:

- niektoré informačné systémy pre výkon pôsobnosti orgánov verejnej moci v elektronickej podobe (výkon verejnej moci elektronicky),
- elektronické podanie, elektronický úradný dokument a niektoré podmienky a spôsob výkonu verejnej moci elektronicky a elektronickej komunikácie orgánov verejnej moci navzájom,
- elektronické schránky a elektronické doručovanie,
- identifikáciu osôb a autentifikáciu osôb,
- autorizáciu,
- zaručenú konverziu,

- spôsob vykonania úhrady orgánu verejnej moci,
- referenčné registre.

Na účely tohto zákona sa rozumie:

- **elektronická komunikácia** – prenos elektronických správ elektronickými prostriedkami medzi komunikujúcimi subjektmi,
- **elektronická správa** – logicky usporiadaný dokument, ktorý obsahuje identifikáciu odosielateľa a adresáta a tvorený jedným elektronickým podaním, elektronickým úradným dokumentom alebo prílohou k nim,
- **elektronický dokument** – číselne kódovaná ľubovoľná neprázdna postupnosť znakov zaznamenaných pomocou elektrickým, elektromagnetickým, optických alebo iných fyzikálnych veličín alebo signálov prenášaných alebo spracovávaných pomocou informačno-komunikačných technológií, ktorej interpretáciou na základe formátu elektronického dokumentu možno dosiahnuť vizuálnu podobu zrozumiteľnú pre človeka.

Výnos Ministerstva financií SR č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy ustanovil:

- technické štandardy (technické prostriedky, sieťová infraštruktúra a programové prostriedky),
- štandardy prístupnosti a funkčnosti webových stránok (aplikačné programové vybavenie podľa zákona),
- štandardy použitia súborov (formáty výmeny údajov),
- štandardy názvoslovia elektronických služieb (sieťová infraštruktúra),
- bezpečnostné štandardy (technické prostriedky, sieťová infraštruktúra, programové prostriedky),
- dátové štandardy (údaje, registre a číselníky),
- štandardy elektronických služieb verejnej správy (údaje, registre, číselníky a aplikačné programové vybavenia),
- štandardy projektového riadenia (postupy a podmienky spojené s vytváraním a rozvojom informačných systémov verejnej správy),
- štandardy poskytovania údajov v elektronickom prostredí (databázové prostredie, spoločné moduly, aplikačné programové vybavenie, údaje, registre, číselníky a formáty výmeny údajov),
- štandardy poskytovania cloudcomputingu a využívania cloudových služieb (technické prostriedky a programové vybavenie).

V základných pojmoch okrem iného uvádza:

- **bezpečnostný incident** – akýkoľvek spôsob narušenia bezpečnosti informačných systémov verejnej správy, ako aj akékoľvek porušenie bezpečnostnej politiky povinnej osoby a pravidiel súvisiacich s bezpečnosťou informačných systémov verejnej správy,
- **technické komponenty informačného systému verejnej správy** – tie časti informačného systému a informačno-komunikačné technológie, ktoré nie sú určené na uchovávanie údajov, napr. štruktúrovaná kabeláž, sieťové karty a zdroje,
- **zariadenia informačného systému verejnej správy** – tie časti informačného systému, ktoré môžu uchovávať údaje, napr. pamäťové médiá a počítače vrátane prenosných počítačov.

11.2 BEZPEČNOSŤ IS POSKYTOVATEĽOV ELEKTRONICKÝCH SLUŽIEB

Zákon č. 351/2011 Z. z. o elektronických komunikáciách upravuje:

a) podmienky na poskytovanie elektronických komunikačných sietí a elektronických komunikačných služieb,
b) podmienky na používanie rádiových zariadení,
c) reguláciu elektronických komunikácií,
d) práva a povinnosti podnikov a užívateľov elektronických komunikačných sietí a elektronických komunikačných služieb,
e) ochranu elektronických komunikačných sietí a elektronických komunikačných služieb,
f) efektívne využívanie frekvenčného spektra a čísel,
g) oprávnenia a povinnosti k cudzím nehnuteľnostiam v súvislosti so zriaďovaním a prevádzkovaním elektronických komunikačných sietí,
h) ochranu súkromia a ochranu spracúvania osobných údajov v oblasti elektronických komunikácií,
i) pôsobnosť orgánov štátnej správy v oblasti elektronických komunikácií.

Podľa tohto zákona:

- **Orgány štátnej správy v oblasti elektronických komunikácií** sú Ministerstva dopravy, výstavby a regionálneho rozvoja SR a Telekomunikačný úrad SR.
- **Podnik** je každá osoba, ktorá poskytuje sieť alebo službu, poskytovanie siete alebo v oblasti elektronických komunikácií pre tretiu osobu je podnikaním.
- **Užívateľ** je osoba, ktorá používa alebo požaduje poskytovanie verejnej služby. Za užívateľa sa na účely tohto zákona považuje aj účastník a koncový užívateľ, ak sa ďalej neustanovuje inak.
- **Koncový užívateľ** je osoba, ktorá používa verejnú službu alebo požaduje jej poskytovanie a túto službu ďalej neposkytuje a ani prostredníctvom nej neposkytuje ďalšie služby. Koncovým užívateľom je spotrebiteľ, a ak ide o rozhlasové a televízne programové služby, aj poslucháč a divák.
- **Účastník** je koncový užívateľ, ktorý uzatvoril s podnikom poskytujúcim verejnú službu zmluvu o poskytovaní verejných služieb.
- **Elektronická komunikačná sieť** je funkčne prepojená sústava prenosových systémov, a ak je to potrebné, prepájacích alebo smerovacích zariadení, vrátane sieťových prvkov, ktoré nie sú aktívne, ktoré umožňujú prenos signálov po vedení, rádiovými, optickými alebo inými elektromagnetickými prostriedkami, vrátane družicových sietí, pevných sietí s prepájaním okruhov a s prepájaním paketov, internetu a mobilných pozemských sietí, sietí na rozvod elektrickej energie v rozsahu, v ktorom sa používajú na prenos signálov, sietí pre rozhlasové a televízne vysielanie a káblových distribučných systémov bez ohľadu na druh prenášaných informácií.
- **Verejná sieť** je sieť, ktorá sa úplne alebo prevažne používa na poskytovanie verejných elektronických komunikačných služieb, ktoré podporujú prenos signálov medzi koncovými bodmi siete.
- **Osobitná sieť** je zriadená a prevádzkovaná na vojenské účely iba pre určený okruh osôb; osobitná sieť nie je verejná sieť.
- **Elektronická komunikačná služba** je služba obvykle poskytovaná za úhradu, ktorá spočíva úplne alebo prevažne v prenose signálov v sieťach, vrátane telekomunikačných služieb a prenosových služieb v sieťach používaných na rozhlasové a televízne vysielanie.

- **Verejná služba** je verejne dostupná služba, o ktorej používanie sa môže uchádzať každý záujemca. Verejná telefónna služba je verejná služba na priame alebo nepriame vytváranie a prijímanie národných a medzinárodných volaní prostredníctvom jedného alebo viacerých čísel národného alebo medzinárodného číslovacieho plánu.
- **Univerzálna služba** je minimálny súbor služieb, ktoré sú dostupné v určenej kvalite na celom území SR všetkým koncovým užívateľom bez ohľadu na ich geografickú polohu a za prijateľnú cenu, ktorou je cena prihliadajúca na úroveň spotrebiteľských cien a príjmy obyvateľov.
- **Správa** je informácia, ktorá sa vymieňa alebo prenáša medzi konečným počtom subjektov prostredníctvom verejnej služby; okrem informácie prenášanej ako súčasť rozhlasového alebo televízneho vysielania sieťou, ktorú nemožno priradiť konkrétnemu užívateľovi, ktorý túto informáciu prijíma.
- **Podnik, ktorý poskytuje verejnú sieť alebo službu** je povinný zabezpečiť technicky a organizačne dôvernosť správ a s nimi spojených prevádzkových údajov, ktoré sa prenášajú prostredníctvom jeho verejnej siete a verejných služieb. Zakazuje sa najmä nahrávanie, odpočúvanie, ukladanie správ alebo iné druhy zachytenia alebo sledovania správ a s nimi spojených údajov osobami inými, ako sú užívatelia alebo bez súhlasu dotknutých užívateľov, ak zákon neustanovuje inak. To nebráni technickému ukladaniu údajov, ktoré sú nevyhnutné na prenos správ, bez toho aby bola dotknutá zásada dôvernosti. Podnik nezodpovedá za ochranu prenášaných správ, ak je možnosť ich priameho vypočutia alebo nechráneného získania v mieste vysielania alebo v mieste príjmu.
- **Predmetom telekomunikačného tajomstva** je:
  a) obsah prenášaných správ,
  b) súvisiace údaje komunikujúcich strán, ktorými sú telefónne číslo, obchodné meno a sídlo právnickej osoby, alebo obchodné meno a miesto podnikania fyzickej osoby – podnikateľa alebo osobné údaje fyzickej osoby, ktorými sú meno, priezvisko, titul a adresa trvalého pobytu; predmetom telekomunikačného tajomstva nie sú údaje, ktoré sú zverejnené v telefónnom zozname,
  c) prevádzkové údaje a
  d) lokalizačné údaje.
- **Bezpečnosť a ochrana osobných údajov v prevádzke siete** – podnik je povinný prijať zodpovedajúce technické a organizačné opatrenia na ochranu bezpečnosti svojich sietí, služieb alebo sietí a služieb, ktoré vzhľadom na stav techniky a náklady na realizáciu musia zabezpečiť úroveň bezpečnosti, ktorá je primeraná existujúcemu riziku.
- **Ochrana obchodného tajomstva úradom** – zamestnanci úradu pri všetkých činnostiach sú povinní dodržiavať mlčanlivosť o skutočnostiach tvoriacich predmet obchodného tajomstva, s ktorým sa oboznámili.

Obsah prenášaných informácií je zakázané uchovávať s výnimkou, ak jeho uchovanie predstavuje podstatnú súčasť služby. Ak je z technických dôvodov nutné krátkodobé uchovanie obsahu, podnik je povinný takto uchované informácie po skončení dôvodu ich uchovania bezodkladne zlikvidovať.

Údaje uvedené v zozname účastníkov je podnik oprávnený použiť a spracúvať len na účely poskytovania verejnej telefónnej služby. Akékoľvek iné použitie je dovolené len so súhlasom dotknutého účastníka. Údaje v zozname účastníkov nemožno použiť najmä na zostavovanie elektronických profilov účastníka alebo na zoraďovanie účastníkov do skupín okrem vypracovania a vydania zoznamov účastníkov podľa kategórií prístupu k sieti. Podnik je povinný prijať vhodné technické opatrenia, ktorými znemožní kopírovanie zoznamov účastníkov vydaných v elektronickej forme.

11.3 OCHRANA OSOBNÝCH ÚDAJOV

V druhej polovici 20. storočia došlo k stúpajúcej tendencii záujmu o problematiku ochrany osobných údajov. Tento nárast je spojený hlavne s peňažným tokom a s rozvojom informačných technológií a nutnosťou dátových tokov medzi spolupracujúcimi krajinami, vrátane tokov, ktoré sú uskutočňované prostredníctvom počítačových prenosov osobných údajov.

Na medzinárodnom poli dlho neexistoval žiadny právny akt, ktorý by oblasť ochrany osobných údajov a vôbec osobné údaje pokrýval. V tejto oblasti je iba niekoľko málo právnych aktov, ktoré boli vydané pod hlavičkou Organizácie spojených národov, ktoré sa zaoberajú ochranou osobnosti, respektíve ochranou súkromia, ale čiastočne zasahujú aj do oblasti ochrany osobných údajov. Tieto dokumenty však nemajú ucelený charakter a úprava ochrany osobných údajov v medzinárodnom meradle je tak skôr roztrieštená, ako ucelená.

Na európskej úrovni je snaha o vytvorenie jednotného rámca ochrany osobných údajov a snaha o harmonizáciu právnej úpravy ochrany osobných údajov, a to prostredníctvom právnych predpisov komunitárneho práva EÚ.

Primárne právo predstavuje:

- Zmluva o Európskej únii, čl. 6 a 39,
- Zmluva o fungovaní Európskej únie, čl. 16,
- Charta základných práv Európskej únie, čl. 8.

Smernicu Európskeho parlamentu a Rady č. 95/46/ES z 24.10.1995 o ochrane fyzických osôb pri spracúvaní osobných údajov a voľnom pohybe týchto údajov má nahradiť Návrh nariadenia Európskeho parlamentu a Rady o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (všeobecné nariadenie o ochrane údajov).

Bezpečnosť osobných údajov v SR rieši Zákon č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, ktorý upravuje:

- ochranu práv fyzických osôb pred neoprávneným zasahovaním do ich súkromného života pri spracúvaní ich osobných údajov,
- práva, povinnosti a zodpovednosť pri spracúvaní osobných údajov fyzických osôb,
- postavenie, pôsobnosť a organizáciu Úradu na ochranu osobných údajov SR.

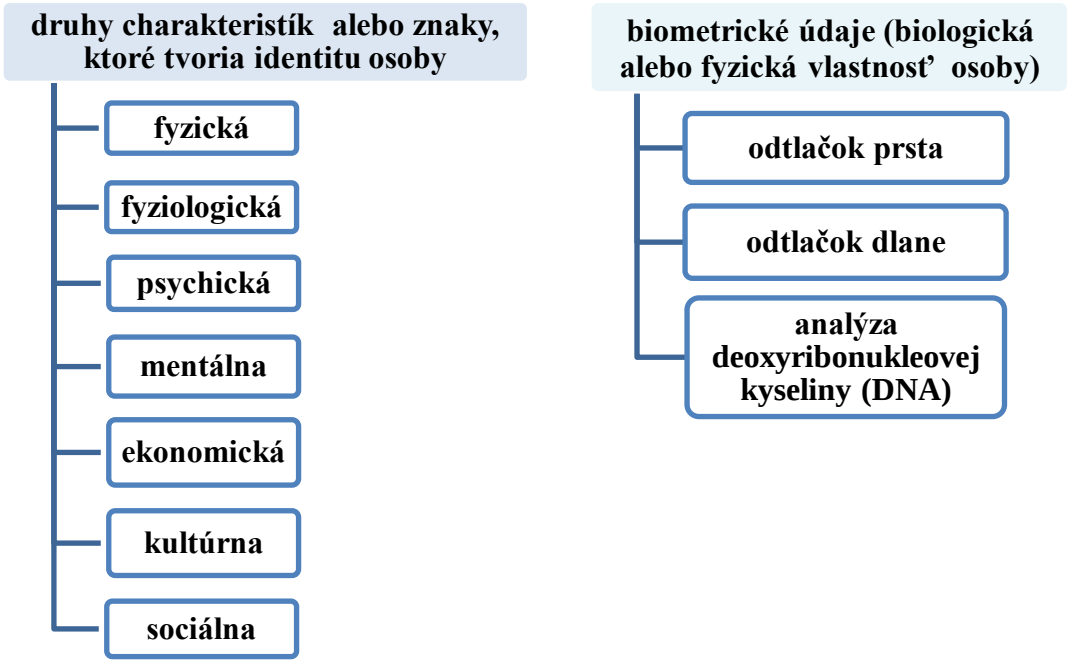
11.3.1 Osobné údaje

Osobnými údajmi sú údaje týkajúce sa určenej alebo určiteľnej fyzickej osoby, pričom takou osobou je osoba, ktorú možno určiť priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora alebo na základe ***jednej či viacerých charakteristík alebo znakov,*** ktoré tvoria jej ***fyzickú, fyziologickú, psychickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu*** (obr. 23).

Medzi osobné údaje patria aj **biometrické údaje**, ktoré sú osobným údajom fyzickej osoby, označujúcim jej biologickú alebo fyziologickú vlastnosť alebo charakteristiku, na základe ktorej je jednoznačne a nezameniteľne určiteľná. Biometrickým údajom je najmä ***odtlačok prsta, odtlačok dlane, analýza deoxyribonukleovej kyseliny (DNA).***

Osobné údaje sú akékoľvek informácie o osobe, pomocou ktorých môže byť identifikovaná, napr.: ***meno, telefónne číslo, e-mailová adresa, dátum narodenia, adresa, číslo sociálneho poistenia alebo iný identifikačný údaj podľa krajiny, číslo účtu, akékoľvek iné informácie o nej, ktoré ju identifikujú alebo pomocou ktorých ju možno identifikovať***. Niektoré osobné údaje sa považujú za citlivé informácie.

Citlivé informácie sú osobné údaje, ktoré informujú o zdraví (napr. sériové číslo používanej zdravotnej pomôcky, dátum vyhotovenia implantátu), rasovom alebo etnickom pôvode, náboženskom alebo filozofickom presvedčení, sexuálnom živote, politickom zmýšľaní, členstve v odborových zväzoch, alebo údaje, ktoré sa týkajú uvedených oblastí.



Obr. 23 Osobné údaje

11.3.2 Spracúvanie osobných údajov

Spracúvanie osobných údajov predstavuje ***vykonávanie operácií alebo súboru operácií s osobnými údajmi,*** najmä ich získavanie, zhromažďovanie, šírenie, zaznamenávanie, usporadúvanie, prepracúvanie a zmena, vyhľadávanie, prehliadanie, preskupovanie, kombinovanie, premiestňovanie, využívanie, uchovávanie, blokovanie, likvidácia, ich cezhraničný prenos, poskytovanie, sprístupňovanie alebo zverejňovanie.

Právnym základom pre získanie osobných údajov môže byť napríklad osobitný zákon (povinnosť, kedy sa nevyžaduje súhlas zamestnanca) alebo súhlas zamestnanca (dobrovoľnosť). Zamestnávateľ má však povinnosť ešte pred získaním osobných údajov zamestnanca oznámiť zamestnancovi svoje identifikačné údaje (túto povinnosť si zamestnávateľ splnil uzatvorením pracovnej zmluvy a tieto informácie nemusí ďalej oznamovať), účel spracúvania osobných údajov, zoznam alebo rozsah osobných údajov, poučenie o dobrovoľnosti alebo povinnosti poskytnúť požadované osobné údaje, tretie strany, ak sa predpokladá alebo je zrejmé, že im budú osobné údaje poskytnuté, prípadne ďalšie informácie podľa Zákona o ochrane osobných údajov.

Osobné údaje možno od zamestnancov získavať a spracovávať len na vymedzený alebo ustanovený účel. Vo vzťahu k zamestnancom je právnym základom spravidla zákonná právna norma. V prípade prihlásenia zamestnanca do registra poistencov je účelom toto prihlásenie. Rozsah a obsah spracovávaných osobných údajov musí zodpovedať účelu ich spracovávania a podmienke nevyhnutnosti dosiahnutia účelu.

Zamestnávateľ je povinný zabezpečiť informačný systém (tvoria ho osobné údaje zamestnancov) primeranými bezpečnostnými opatreniami, a to po technickej a organizačnej stránke, ale aj personálnej stránke.

Informačný systém osobných údajov je informačný systém, v ktorom sa na vopred vymedzený alebo ustanovený účel systematicky spracúva alebo má spracúvať akýkoľvek usporiadaný súbor osobných údajov prístupných podľa určených kritérií, bez ohľadu na to, či ide o informačný systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom alebo geografickom základe; informačným systémom sa na účely tohto zákona rozumie aj súbor osobných údajov, ktoré sú spracúvané alebo pripravené na spracúvanie čiastočne automatizovanými alebo inými ako automatizovanými prostriedkami spracúvania *(§ 4 ods. 3 písm. b) zákona).*

Osobné údaje môže spracúvať len prevádzkovateľ a sprostredkovateľ. Zhromaždené osobné údaje na pôvodne určený účel nemôže prevádzkovateľ spracúvať na iný účel, ktorý je nezlučiteľný s pôvodným účelom spracúvania.

Personálna a mzdová agenda zamestnávateľa je súčasťou jeho registratúry a aj keď skončí napríklad pracovný pomer, osobné údaje, ktoré spracúval, zlikviduje až po uplynutí lehoty ich uchovávania (archivácie). Nie každý dokument (registratúrny záznam) obsahujúci osobné údaje zamestnanca sa môže zlikvidovať. Niektoré zamestnávateľ odovzdá na archiváciu príslušnému štátnemu archívu s regionálnou územnou pôsobnosťou. Dokumenty obsahujúce osobné údaje zamestnanca, ktoré sa neodovzdávajú na archiváciu, musí zamestnávateľ zničiť, aby nebolo možné identifikovať dotknutú osobu (zamestnanca).

11.3.3 Zodpovednosť za bezpečnosť osobných údajov

Za bezpečnosť osobných údajov zodpovedá ***prevádzkovateľ.*** Je povinný chrániť spracúvané osobné údaje pred ich poškodením, zničením, stratou, zmenou, neoprávneným prístupom a sprístupnením, poskytnutím alebo zverejnením, ako aj pred akýmikoľvek inými neprípustnými spôsobmi spracúvania. O osobných údajoch, ktoré spracúva je povinný zachovávať **mlčanlivosť.**

Na tento účel prijme primerané ***technické, organizačné a personálne opatrenia*** zodpovedajúce spôsobu spracúvania osobných údajov, pričom berie do úvahy najmä použiteľné technické prostriedky, dôvernosť a dôležitosť spracúvaných osobných údajov, ako aj rozsah možných rizík, ktoré sú spôsobilé narušiť bezpečnosť alebo funkčnosť informačného systému. Bezpečnostné opatrenia prevádzkovateľ zdokumentuje bezpečnostným projektom alebo bezpečnostnou smernicou.

Bezpečnostný projekt informačného systému s osobnými údajmi musí prevádzkovateľ vypracovať, ak v informačnom systéme prepojenom s verejne prístupnou počítačovou sieťou spracúva osobitné kategórie osobných údajov, alebo informačný systém slúži na zabezpečenie verejného záujmu. Bezpečnostný projekt vymedzuje rozsah a spôsob bezpečnostných opatrení potrebných na eliminovanie a minimalizovanie hrozieb a rizík pôsobiacich na informačný systém z hľadiska narušenia jeho bezpečnosti, spoľahlivosti a funkčnosti.

Obsahuje najmä ***bezpečnostný zámer, analýzu bezpečnosti informačného systému a bezpečnostné smernice.*** Prevádzkovateľ ho vypracúva v súlade s bezpečnostnými štandardmi, právnymi predpismi a medzinárodnými zmluvami, ktorými je SR viazaná.

Bezpečnostnú smernicu prevádzkovateľ vypracúva ak je informačný systém prepojený s verejne prístupnou počítačovou sieťou, ale nespracúva osobitné kategórie osobných údajov, alebo informačný systém spracúva osobitné kategórie osobných údajov, ale nie je prepojený s verejne prístupnou počítačovou sieťou.

Úrad na ochranu osobných údajov SR vykonáva **dozor nad ochranou osobných údajov** a podieľa sa na ochrane základných práv a slobôd fyzických osôb pri spracúvaní ich osobných údajov.

Podľa Zákona č. 351/2011 Z. z. o elektronických komunikáciách sa **ochrana osobných údajov** vzťahuje na účastníkov a užívateľov, ktorí sú fyzickými osobami. Práva a povinnosti prevádzkovateľa, ktorým je podnik, súvisiace s ochranou osobných údajov, ktoré nie sú upravené v tomto zákone, sa spravujú osobitným predpisom.

Podnik je povinný prijať zodpovedajúce technické a organizačné opatrenia na ***ochranu bezpečnosti svojich služieb,*** a ak je to nevyhnutné, aj v súčinnosti s poskytovateľom verejnej siete. Prijaté opatrenia musia zabezpečiť takú úroveň bezpečnosti služieb, ktorá je primeraná existujúcemu riziku vzhľadom na stav techniky a náklady na ich realizáciu.

Podnik, ktorý poskytuje verejné komunikačné služby, môže na účely uzavretia a plnenia zmluvy o poskytovaní verejných služieb, jej zmeny, ukončenia alebo prenesenia čísla, fakturácie, prijímania a evidencie platieb, pohľadávok a postupovania pohľadávok a vypracovania zoznamu účastníkov **získavať a spracúvať údaje účastníkov**, ktorými sú *telefónne číslo, výška neuhradených záväzkov* a:

a) *meno, priezvisko, titul, adresa trvalého pobytu, rodné číslo, číslo občianskeho preukazu alebo iného dokladu totožnosti fyzickej osoby, štátnu príslušnosť,*
b) *obchodné meno, miesto podnikania a identifikačné číslo fyzickej osoby – podnikateľa alebo*
c) *obchodné meno, sídlo a identifikačné číslo právnickej osoby.*

Podnik je povinný informovať účastníka o tom, aké osobné údaje sa získavajú a spracúvajú, na základe akého právneho dôvodu, na aký účel a ako dlho sa budú spracúvať. Táto informácia sa poskytuje najneskôr pri uzavretí zmluvy o poskytovaní verejných služieb.

Bezpečnosť a ochranu osobných údajov okrem uvedeného zákona riešia:

- Smernica Európskeho parlamentu a Rady 95/46/EC z 24. októbra 1995 o ochrane jednotlivcov pri spracúvaní osobných údajov a voľnom pohybe týchto údajov.
- Smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002 týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách).
- Rámcové rozhodnutie Rady 2008/977 SVV z 27. novembra 2008 o ochrane osobných údajov spracúvaných v rámci policajnej a justičnej spolupráce v trestných veciach.
- Dohovor o ochrane jednotlivca pri automatizovanom spracovaní osobných údajov
- Dodatkový protokol k Dohovoru o ochrane jednotlivca pri automatizovanom spracovaní osobných údajov, týkajúci sa orgánov dozoru a cezhraničných tokov údajov.
- Ústavný zákon č. 460/1992 Zb. Ústava SR v znení neskorších predpisov.
- Zákon č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
- Zákon č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov.
- Zákon č. 71/1967 Zb. o správnom konaní (správny poriadok).
- Zákon č. 300/2005 Z. z. trestný zákon v znení neskorších predpisov.
- Vyhláška Úradu na ochranu osobných údajov SR č.164 z 13. júna 2013 o rozsahu a dokumentácii bezpečnostných opatrení.
- Vyhláška Úradu na ochranu osobných údajov SR č.165 z 13. júna 2013 ktorou sa ustanovujú podrobnosti o skúške fyzickej osoby na výkon funkcie zodpovednej osoby.
- Metodické usmernenia Úradu na ochranu osobných údajov SR č.1/2013 k pojmu osobné údaje.

11.4 ĎALŠIE ZLOŽKY OCHRANY DÔLEŽITÝCH INFORMÁCIÍ

11.4.1 Ochrana obchodného tajomstva

Ochranu obchodného tajomstva riešia:

- Zákon č. 22/2004 Z. z. o elektronickom obchode a o zmene a doplnení zákona č. 128/2002 Z. z. o štátnej kontrole vnútorného trhu vo veciach ochrany spotrebiteľa a o zmene a doplnení niektorých zákonov v znení Zákona č. 284/2002 Z. z.
- Zákon 300/2005 Z. z. Trestný zákon, § 265 zneužívanie informácií v obchodnom styku.

Zákon č. 22/2004 Z. z. o elektronickom obchode upravuje:

a) vzťahy medzi poskytovateľom služieb informačnej spoločnosti a ich príjemcom, ktoré vznikajú pri ich komunikácii na diaľku, počas spojenia elektronických zariadení elektronickou komunikačnou sieťou a spočívajú na elektronickom spracovaní, prenose, uchovávaní, vyhľadávaní alebo zhromažďovaní dát vrátane textu, zvuku a obrazu,
b) dohľad nad dodržiavaním zákona,
c) medzinárodnú spoluprácu v elektronickom obchode.

Službou informačnej spoločnosti je služba poskytovaná na diaľku počas spojenia elektronických zariadení elektronickou komunikačnou sieťou spravidla za úhradu na žiadosť príjemcu služby informačnej spoločnosti, najmä komerčná komunikácia, spracovanie, prenos, uchovávanie, vyhľadávanie alebo zhromažďovanie dát a elektronická pošta okrem osobnej elektronickej pošty; službou informačnej spoločnosti nie sú rozhlasové a televízne vysielanie vrátane teletextu, hlasové telefonické služby, telefaxové služby a služby, ktorých obsah vylučuje ich poskytovanie na diaľku.

Komerčnú komunikáciu predstavujú informácie o tovare, službe, podnikateľovi alebo o osobe, ktorá vykonáva povolanie alebo regulované povolanie podľa osobitného zákona, vrátane reklamy, ponuky a predaja tovaru okrem:

1. informácií umožňujúcich priamy styk s poskytovateľom služieb prostredníctvom elektronického zariadenia, najmä o názve domény alebo o adrese elektronickej pošty; doménou sa rozumie symbolická adresa v elektronickej komunikačnej sieti,
2. informácií o tovare, službe, podnikateľovi alebo osobe, ktorá vykonáva povolanie alebo regulované povolanie podľa osobitného zákona, zostavených na iný účel ako na ich reklamu a poskytovaných bezodplatne.

Pod pojmom **komerčné informácie** sa chápu všetky informácie, ktoré sa týkajú hlavnej činnosti podniku, majú určitú trhovú hodnotu a na ich ochrane má podnik záujem. Komerčné informácie sú také informácie, ktoré súvisia s výrobou, technológiou, riadením, financovaním, obchodom, rozvojom a pod. Ochrana komerčných informácií je potrebná, aby konkurencia nezískala prístup k týmto informáciám, čím by získala výhodu, ktorá by v konečnom dôsledku mohla znamenať pre daný podnik stratu.

V právnych normách je definovaný pojem **obchodné tajomstvo** ako *všetky skutočnosti obchodnej, výrobnej alebo technickej povahy súvisiace s podnikom, ktoré majú skutočnú alebo aspoň potenciálnu materiálnu alebo nemateriálnu hodnotu, nie sú v príslušných obchodných kruhoch bežne dostupné, majú byť podľa vôle podnikateľa utajené a podnikateľ zodpovedajúcim spôsobom ich utajenie zabezpečuje.*

Z definície vyplýva, že aby informácia bola považovaná za obchodné tajomstvo, musí spĺňať tieto atribúty:

- nesmie byť utajovanou skutočnosťou podľa zákona o ochrane utajovaných skutočností,
- má vzťah k danému podniku a jeho činnostiam,

- musí mať komerčnú hodnotu alebo zabezpečuje jej vlastníkovi určitú výhodu,
- nesmie byť všeobecné známa alebo prístupná,
- musia byť prijaté opatrenia na jej ochranu.

Za obchodné tajomstvo je možné označiť:

- technológiu výroby (produkcie tovarov), vlastné know-how, patenty a pod.
- databázy, softvér a pod.,
- systém riadenia podniku,
- finančno-ekonomickú situáciu podniku,
- cenovú a obchodnú politiku,
- marketingovú stratégiu,
- zámery reklamných akcií,
- obchodné zámery a stratégie,
- stratégie a programy rozvoja a modernizácie podniku, vrátane vedeckovýskumných programov,
- obchodné a cenové analýzy,
- rokovania o dodávateľsko-odberateľských vzťahoch,
- profesionálno-odborné informácie o zamestnancoch, najmä o vedúcich pracovníkoch a významných špecialistoch,
- mzdovú politiku a systém stimulácie pracovníkov,
- systém ochrany majetku a pod.

Hodnota komerčných informácií, ktoré sú reprezentované v podnikových operáciách, v stratégii výroby, v plánoch a správach zahrnujúcich ich finančné, technické a operačné údaje, sa rovná v podstate hodnote samotného podniku bez hodnoty fyzického majetku. To znamená, že keby sa stratili informácie o tom, ako zabezpečiť fungovanie podniku, reziduálna hodnota tohto podniku by sa rovnala len predajnej cene budov a zariadenia. Existuje množstvo podnikov (podnikateľských subjektov), ktorých skutočná komparatívna hodnota sa rovná hodnote ich autentických know-how alebo ich jedinečnej informačnej bázy.

Najväčšími zdrojmi ohrozenia komerčných informácií sú: vlastní zamestnanci, bývalí zamestnanci, hackeri, komerčné spravodajské služby (priemyselná špionáž), konkurenti.

Ochrana komerčných informácií sa musí zabezpečovať najmä z týchto dôvodov:

- informácie **sú citlivým prostriedkom**, tzn. že získaním komerčných informácií daného podniku získa konkurencia náskok, ušetrí si čas a výdavky na výskum, ktorý by musela vynaložiť na výber správneho rozhodnutia,
- informácie sú **nákladným a rozhodujúcim prostriedkom podnikania**; ak podnik ako jediný vlastní jedinečnú či inovačnú informáciu, môže to byť zárukou jeho úspechu a ziskovosti; na druhej strane, ak stratí výhody dobrej informovanosti, môže stratiť trh, čo môže znamenať i krach celého podniku,
- informácie sú **pominuteľným prostriedkom**, pretože informácie, ktoré boli prezradené (ukradnuté, zverejnené a pod.) sa už nahradiť nedajú; ak sa informácia o obchodnej či technickej stratégii prezradí, jej hodnota sa stráca, nemožno ju nahradiť, lebo jej význam je čisto v jej jedinečnosti pre toho, kto je jej vlastníkom.

Na ochranu komerčných informácií (obchodného tajomstva) sa využívajú rovnaké formy a metódy, ako na ochranu utajovaných skutočností alebo osobných údajov. Ide najmä o využitie: technických zabezpečovacích prostriedkov (MZP, TZP), fyzickej ochrany, režimových opatrení, personálnej bezpečnosti, administratívnej bezpečnosti, opatrení bezpečnosti technických prostriedkov – bezpečnosti IT.

Spôsob výberu bezpečnostných opatrení bude závisieť od hodnoty informácií, resp. veľkosti následkov, ktoré môžu vzniknúť, ak by došlo k prezradeniu alebo úniku komerčných informácií, od veľkosti rizík, ktoré môžu pôsobiť z vonkajšieho a vnútorného prostredia, od zraniteľnosti existujúceho systému ochrany informácií.

11.4.2 Ochrana bankového tajomstva

Ochranu bankového tajomstva rieši:

- Zákon č. 483/2001 Z. z. o bankách a o zmene a doplnení niektorých zákonov,
- Metodické usmernenie Úseku bankového dohľadu Národnej banky Slovenska č. 7/2004 k overeniu bezpečnosti informačného systému banky a pobočky zahraničnej banky.

Bankovou informáciou je informácia týkajúca sa klienta banky, ktorú má banka o ňom a získala ju pri výkone alebo v súvislosti s výkonom bankových činností a ktorá sa poskytuje na základe súhlasu klienta.

Bankové tajomstvo predstavujú všetky informácie a doklady o záležitostiach, týkajúcich sa klienta banky (alebo klienta pobočky zahraničnej banky), ktoré nie sú verejne prístupné, najmä informácie o obchodoch, stavoch na účtoch a stavoch vkladov. Povinnosťou banky alebo zahraničnej pobočky banky je tieto informácie utajovať, chrániť pred vyzradením, poškodením, stratou, odcudzením a pod. Banka alebo pobočka zahraničnej banky môže informácie chránené bankovým tajomstvom poskytnúť tretím osobám len s predchádzajúcim písomných súhlasom dotknutej osoby alebo na jeho písomný pokyn, ak zákon neustanovuje inak.

Klient má právo za úhradu vecných nákladov oboznámiť sa s informáciami, ktoré sú o ňom vedené v databáze banky alebo pobočky zahraničnej banky a na obstaranie výpisu z nej. Za porušenie bankového tajomstva sa nepovažuje poskytovanie informácií v súhrnnej podobe, z ktorých nie je zrejmý názov banky alebo pobočky zahraničnej banky, meno a priezvisko klienta.

Zákon o bankách definuje subjekty, pri ktorých umožňuje banke poskytnúť správu o všetkých záležitostiach, ktoré sú predmetom bankového tajomstva bez súhlasu klienta. Medzi takéto subjekty patria napríklad osoby poverené bankovým dohľadom, audítori pri činnosti ustanovenej zákonom, súdy, orgány činné v trestnom konaní, daňový orgán, colný orgán a pod.

Ďalšími zákonnými výnimkami, pri ktorých môže banka zverejniť informácie o klientovi chránené bankovým tajomstvom súvisia napr. s neplnením si záväzkov klienta voči banke (nesplácanie úveru). V takom prípade je banka oprávnená poskytnúť informácie znalcovi pre ocenenie záväzku klienta, advokátovi alebo komerčnému právnikovi, ktorému udelila písomnú plnú moc na svoje zastupovanie, ostatným bankám a osobe, na ktorú banka postúpila svoju pohľadávku.

Metodické usmernenie Úseku bankového dohľadu Národnej banky Slovenska č. 7/2004 k overeniu bezpečnosti informačného systému banky a pobočky zahraničnej banky v zmysle § 40 ods. 8 a 9 zákona č. 483/2001 Z. z. o bankách v znení neskorších predpisov stanovuje pre banky a pobočky zahraničných bánk:

a) predmet overenia stavu bezpečnosti informačného systému banky, ktorým sú spracúvané a uschovávané bankové údaje, a to z pohľadu zabezpečenia ochrany elektronického spracúvania a uschovávania údajov pred zneužitím, zničením, poškodením, odcudzením alebo stratou,
b) rozsah informácií poskytnutých bankou Národnej banke Slovenska o zabezpečení overenia bezpečnosti informačného systému banky.

Overenie bezpečnosti informačného systému banky je nezávislé, nestranné, nezaujaté a odborné posúdenie bezpečnostných vlastností informačného systému banky z hľadiska zabezpečenia celkovej bezpečnosti informačného systému najmä jeho efektívnosti, kvality a úrovne riadenia bezpečnostných rizík, dôvernosti, integrity, autenticity a dostupnosti informácií a spracúvaných údajov.

Cieľom overenia bezpečnosti informačného systému banky je poskytnúť primeranú istotu:

- či bankou spracúvané a uchovávané údaje sú primerane zabezpečené pred zneužitím, zničením, poškodením, odcudzením, neoprávneným prístupom, zmenou alebo pred stratou,
- celkovú úroveň zaistenia bezpečnosti informačného systému a integrity, dostupnosti, dôvernosti a autenticity údajov z pohľadu domácich právnych noriem a medzinárodne uznávaných štandardov,
- či informačný systém banky spĺňa náležitosti popísané v tomto usmernení a v akom rozsahu,
- či banka chápe bezpečnosť informačného systému ako nepretržitý každodenný proces, ktorý je vecou každého zamestnanca banky.

Podľa tohto metodického usmernenia sú:

a. **aktívom informačnej bezpečnosti** (informačné aktívum) hmotný alebo nehmotný objekt, ktorý sa spolupodieľa na fungovaní a vytváraní informačného systému banky, najmä
   - ***údajové a dokumentačné aktíva,*** najmä – databázy a dátové súbory, údaje a informácie, systémová dokumentácia, používateľské manuály, zácvikové materiály, prevádzkové alebo podporné procedúry, plány kontinuity, dohody o náhradných postupoch používaných v prípade zlyhania poskytovaných služieb alebo systému, archivované informácie,
   - ***softvérové aktíva,*** najmä – aplikačný softvér, systémový softvér, vývojové nástroje a pomocné programy, zdrojové knižnice programov, knižnice vykonateľných programov,
   - ***fyzické aktíva,*** najmä – počítačové vybavenie (procesory, monitory, laptopy, modemy), komunikačné vybavenie (smerovače, faxové prístroje, odkazovače), magnetické médiá (pásky, diskety, pevné disky, kompaktné disky), iné technické vybavenie (napájacie zdroje, klimatizačné jednotky), nábytok,

b. **informačným systémom** hmotné a nehmotné objekty, ktoré sú cielene vyberané alebo vytvorené a vzájomne cielene poprepájané kvôli zberu, výmene, spracovaniu, uchovaniu, generovaniu a distribúcii informácií a údajov vo vopred definovanej štruktúre a čase, a to na výkon rozhodnutí, podporu rozhodovania a informovanosti.

11.4.3 Ochrana listového tajomstva

Ochranu listového tajomstva riešia ustanovenia § 196, § 197, § 198 Trestného zákona a článok 22 Ústavy SR.

Podľa čl. 22 ods. 1 a 2 Ústavy SR listové tajomstvo, tajomstvo dopravovaných správ a iných písomností a ochrana osobných údajov sa zaručujú. Nikto nesmie porušiť listové tajomstvo ani tajomstvo iných písomností a záznamov, či už uchovávaných v súkromí, alebo zasielaných poštou, alebo iným spôsobom; výnimkou sú prípady, ktoré ustanoví zákon. Rovnako sa zaručuje tajomstvo správ podávaných telefónom, telegrafom alebo iným podobným zariadením.

Ochrana sa vzťahuje na správy súkromného, ako aj verejného charakteru, správy obchodné či politické. Predmetom ochrany sú správy zasielané akýmkoľvek spôsobom – v uzavretom liste alebo inej písomnosti, dopravované poštou alebo iným dopravným zariadením,

príp. aj kuriérom. Podľa súčasnej právnej úpravy možno tajomstvo prepravovaných správ obmedziť len v súvislosti s trestným stíhaním. Ak je na objasnenie skutočností závažných pre trestné konanie nevyhnutné zistiť obsah nedoručených telegramov, listov alebo iných zásielok, ktoré pochádzajú od obvineného, alebo sú mu určené, nariadi predseda senátu a v prípravnom konaní prokurátor a vyšetrovateľ, aby mu ich pošta alebo podnik vykonávajúci ich prepravu vydali.

Pozerať listy, e-maily a SMS správy sa teda nesmie, takisto odpočúvať hovory. Pamätá na to aj paragraf 196 Trestného zákona, ktorý hovorí o porušovaní tajomstva prepravovaných správ. V prípade, že sa porušenie tajomstva informácie prenášanej pomocou elektronickej komunikačnej služby dokáže, hrozí väzenie na tri až desať rokov.

11.4.4 Ochrana autorských práv

Autorské právo zabezpečuje autorom výhradné práva na využívanie ich vlastných diel alebo na poskytnutie oprávnenia na ich používanie iným osobám, a tým získanie finančného ohodnotenia. Navyše práva súvisiace s autorským právom zabezpečujú ochranu aj pre výkonných umelcov (napríklad hudobníkov, hercov a výtvarných umelcov), producentov a vysielateľov.

Autorské právo trvá v štátoch EÚ najmenej 70 rokov po autorovej smrti, avšak v niektorých krajinách v rámci angloamerického právneho systému bolo trvanie týchto práv predĺžené až na 90 rokov od autorovej smrti. Keď uplynie doba ochrany autorského práva, dielo sa stáva voľným dielom a na jeho použitie nie je už potrebný žiaden súhlas. Vzhľadom na osobnostné práva autora však autorstvo k dielu bude navždy patriť tej fyzickej osobe, ktorá dielo vytvorila.

Najväčšou obavou vlastníkov autorských práv je porušenie ich práv formou pirátstva a falšovania. Aj súčasné polemiky týkajúce sa napríklad sietí peer-to-peer a preberania súborov sú v podstate o porušovaní autorského práva a pirátstve, keďže v mnohých prípadoch vlastníci autorských práv nedostávajú kompenzáciu za šírenie svojich diel.

Ochranu autorským právam zaručujú ustanovenia Autorského zákona, Občianskeho zákonníka aj ustanovenia Trestného zákona. Pokiaľ bolo do práv autora zasiahnuté alebo hrozí, že jeho práva budú porušené, môže sa autor domáhať nápravy. Predmetom ochrany autorského práva je **dielo**. Ak by išlo o úmyselné porušenie práv, je možné porušiteľa stíhať aj podľa Trestného zákona, pričom podľa závažnosti porušenia mu hrozí trest odňatia slobody až na osem rokov. Každý autor môže urobiť podanie na polícii, pokiaľ má podozrenie, že došlo k neoprávnenému zásahu do jeho práv.

Ak porušením alebo ohrozením práva autora bolo napr. poškodené aj jeho **dobré meno,** alebo atakovaná jeho **česť alebo dôstojnosť**, môže sa autor domáhať aj náhrady nemajetkovej ujmy. Táto môže byť vo forme verejného ospravedlnenia alebo zverejnenia rozsudku v tlači. Pokiaľ by však takýto spôsob nebol vzhľadom na ujmu dostatočný, môže súd priznať aj náhradu v peniazoch.

Autorské právo je na území SR upravené Zákonom č. 618/2003 Z. z. o autorskom práve a právach súvisiacich s autorským právom (autorský zákon). Tento zákon upravuje vzťahy vznikajúce v súvislosti s vytvorením a použitím literárneho a iného umeleckého diela a vedeckého diela, umeleckého výkonu, s výrobou a použitím zvukového záznamu, zvukovo-obrazového záznamu, s vysielaním a použitím rozhlasového vysielania a televízneho vysielania a v súvislosti so zhotovením a použitím databázy tak, aby boli chránené práva a oprávnené záujmy autora, výkonného umelca, výrobcu zvukového záznamu, výrobcu zvukovo-

obrazového záznamu, rozhlasového vysielateľa a televízneho vysielateľa a zhotoviteľa databázy.

Autor, do práva ktorého sa neoprávnene zasiahlo alebo jeho právu hrozí neoprávnený zásah, môže sa domáhať najmä:

1. určenia svojho autorstva,
2. zákazu ohrozenia svojho práva vrátane zákazu opakovania takého ohrozenia, a to aj proti osobe, ktorá sa nepriamo podieľa na ohrození tohto práva,
3. zákazu neoprávneného zásahu do svojho práva, a to aj proti osobe, ktorá sa nepriamo podieľa na neoprávnenom zásahu do tohto práva vrátane zákazu zásahu,
4. poskytnutia informácií o pôvode rozmnoženiny diela alebo napodobeniny diela, o spôsobe a rozsahu jej použitia a o službách porušujúcich právo autora vrátane:
   a) údajov o vlastníkovi, vydavateľovi, výrobcovi, distributérovi, dodávateľovi alebo predajcovi takej rozmnoženiny diela alebo napodobeniny diela alebo o poskytovateľovi služieb,
   b) údajov o vydanom, vyrobenom, dodanom, poskytnutom, prijatom alebo objednanom množstve alebo cene takej rozmnoženiny diela, napodobeniny diela alebo služby.
5. odstránenia následkov zásahu do práva na náklady osoby, ktorá neoprávnene zasiahla alebo hrozila neoprávneným zásahom, a to:
   a) zničením neoprávnene vyhotovenej rozmnoženiny diela alebo napodobeniny diela, jej stiahnutím z obehu alebo z iného použitia alebo
   b) zničením materiálov, nástrojov a pomôcok použitých pri neoprávnenom zásahu alebo hrozbe neoprávneného zásahu, ich stiahnutím z obehu alebo z iného použitia.
6. náhrady ujmy podľa osobitného predpisu,
7. vydania bezdôvodného obohatenia vo výške dvojnásobku odmeny, ktorá je obvyklá za získanie licencie pri obdobných zmluvných podmienkach v čase neoprávneného zásahu do tohto práva.

Autor, ktorý pri výkone povinnej kolektívnej správy svojho majetkového práva k dielu nie je zmluvne zastupovaný príslušnou organizáciou kolektívnej správy, môže sa domáhať vydania odmeny alebo primeranej odmeny, ak sa jeho dielo použilo, alebo vydania náhrady odmeny voči príslušnej organizácii kolektívnej správy alebo inej osobe, ktorá je povinná vytvárať rezervný fond podľa tohto zákona na také účely; tým nie sú dotknuté nároky autora z neoprávneného použitia diela. Nárokov sa okrem autora môže domáhať aj nadobúdateľ výhradnej licencie alebo osoba, ktorá má majetkové právo k dielu alebo jej bol zverený výkon majetkových práv autora.

11.4.5 Ochrana pred odpočúvaním

Cieľom obrannej technickej prehliadky je odhalenie skrytých odpočúvacích prostriedkov, a to aktívnych i neaktívnych v dobe vykonávania prehliadky. Je to komplexná previerka bezpečnosti daného objektu z hľadiska úniku informácií, teda celkové posúdenie objektu, nájdenie odpočúvacieho prostriedku a návrh potrebných opatrení na zamedzenie jeho následnej inštalácie. Technické prehliadky vykonávajú certifikované spoločnosti.

Zadávateľ dostane hneď po ukončení prehliadky ústnu správu o výsledku, potom mu je zaslaná písomná správa s popísaným postupom a jeho výsledky. V správe je tiež vykonané hodnotenie ochrany objektu pred únikom informácií a navrhnuté nové organizačné, režimové a technické opatrenia vedúce k zníženiu rizika.

11.4.6 Ochrana súkromia pred nevyžiadanými správami

Zasielanie nevyžiadanej pošty čo najširšiemu okruhu používateľov internetu je, napriek mnohým opatreniam, stále častým javom. Nevyžiadaná pošta, ktorá je rozosielaná hromadne sa niekedy vysvetľuje a používa aj akronym **S.P.A.M.** – *Self Promotional Advertising Message*.

Vo väčšine prípadov ide o e-mail, ktorý si príjemca vopred nevyžiadal a zvyčajne obsahuje komerčné, marketingové alebo iné prvky obdobného charakteru. Vzhľadom na rýchly vývoj elektronickej komunikácie je bežným trendom nielen rozosielanie nevyžiadaných e-mailov, ale aj SMS, MMS alebo iných správ, ktoré sú zasielané príjemcom bez ich predchádzajúceho súhlasu, resp. vyžiadania. Častými sú aj prípady, kedy spam neobsahuje len marketingové prvky, ale aj rôzny škodlivý softvér, ktorý môže byť aktivovaný už samotným otvorením správy.

Na ochranu súkromia účastníkov elektronickej komunikácie bola prijatá smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002, týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách), ktorá bola už dvakrát zmenená, a to smernicou Európskeho parlamentu a Rady 2006/24/ES z 15. marca 2006 a smernicou Európskeho parlamentu a Rady 2009/136/ES z 25. novembra 2009.

Smernica 2002/58/ES sa v čl.13 venuje výlučne nevyžiadaným správam a v odsekoch 1 a 2 stanovuje, že používanie automatických volacích systémov bez ľudského zásahu (telefónne automaty, faxy alebo elektronická pošta) na účely priamej reklamy môže byť povolené len s **predchádzajúcim súhlasom účastníkov alebo užívateľov**.

V SR sa nevyžiadanej pošte venuje Zákon č. 147/2001 Z. z. o reklame v znení neskorších predpisov. Zákon upravuje, že reklama nesmie zneužívať dôveru spotrebiteľa, nedostatok jeho skúseností alebo vedomostí, reklama sa nesmie šíriť automatickým telefonickým volacím systémom, telefaxom a elektronickou poštou bez predchádzajúceho súhlasu ich užívateľa, ktorý je príjemcom reklamy. Zákon o reklame zároveň stanovuje, že reklama sa nesmie šíriť adresne, ak adresát doručenie reklamy vopred odmieta.

Problematiku nevyžiadanej pošty upravuje aj Zákon č. 22/2004 Z. z. o elektronickom obchode v znení neskorších predpisov, ktorý uvádza, že poskytovateľ služieb nesmie doručovať informácie komerčnej komunikácie elektronickou poštou, ak si ich **príjemca služby vopred nevyžiadal**. Nad dodržiavaním zákona o reklame a zákona o elektronickom obchode vykonáva dohľad Slovenská obchodná inšpekcia.

Dňa 1.11.2011 nadobudol účinnosť Zákon č. 351/2011 Z. z. o elektronických komunikáciách, ktorý definuje pojem **elektronická pošta** v ustanovení § 62 ods. 1, ako ***textovú, hlasovú, zvukovú alebo obrazovú správu zaslanú prostredníctvom verejnej siete,*** ktorú možno uložiť v sieti alebo v koncovom zariadení príjemcu, kým ju príjemca nevyzdvihne.

Zákon o elektronických komunikáciách dovoľuje na účely priameho marketingu volanie alebo používanie automatických volacích a komunikačných systémov bez ľudského zásahu, telefaxu, elektronickej pošty, vrátane služby krátkych správ účastníkovi alebo užívateľovi **len s jeho predchádzajúcim súhlasom**, pričom tento súhlas musí byť preukázateľný. V zákone je formulovaný zákaz zasielania elektronickej pošty, z ktorej **nie je známa totožnosť a adresa odosielateľa**, na ktorú môže príjemca zaslať žiadosť o skončenie zasielania takých správ *(Čabák, 2013)*.

11.4.7 Ochrana súkromia pred neoprávneným použitím informačno-technických prostriedkov

Zákon č. 166/ 2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním) ustanovuje podmienky použitia informačno-technických prostriedkov bez predchádzajúceho súhlasu toho, komu zasahuje do súkromia orgán štátu, ktorý informačno-technický prostriedok používa.

Informačno-technickými prostriedkami na účely tohto zákona sú najmä elektrotechnické, rádiotechnické, fototechnické, optické, mechanické, chemické a iné technické prostriedky a zariadenia, alebo ich súbory používané utajovaným spôsobom pri:

a) vyhľadávaní, otváraní, skúmaní a vyhodnocovaní poštových zásielok a iných dopravovaných zásielok,
b) odpočúvaní a zaznamenávaní v rámci telekomunikačných činností,
c) vyhotovovaní a využívaní obrazových, zvukových alebo iných záznamov.

Informačno-technické prostriedky môže používať Policajný zbor, Slovenská informačná služba, Vojenské spravodajstvo, Zbor väzenskej a justičnej stráže a Colná správa. Informačno-technický prostriedok možno použiť iba vtedy, ak je to v demokratickej spoločnosti nevyhnutné na zabezpečenie bezpečnosti štátu, obranu štátu, predchádzanie a objasňovanie trestnej činnosti alebo na ochranu práv a slobôd iných.

Použitím informačno-technického prostriedku sa môže základné právo alebo sloboda obmedziť len v nevyhnutnom rozsahu a nie dlhšie, ako je to nevyhnutné na dosiahnutie zákonom uznaného cieľa, na ktorý slúži. Informačno-technické prostriedky možno použiť iba na základe predchádzajúceho písomného súhlasu zákonného sudcu len na nevyhnutný čas, najdlhšie však na šesť mesiacov.

11.4.8 Elektronický podpis a elektronická pečať

Elektronický podpis (EP) umožňuje rovnaké postavenie elektronického a papierového dokumentu. Predstavuje alternatívu tradičného ručného podpisu v on-line transakciách. Úlohou EP je potvrdiť, že podpisujúci je skutočne ten, za ktorého sa vydáva a že súhlasí s obsahom podpísaného dokumentu.

Zákon č. 215/ 2002 Z. z. o elektronickom podpise upravuje:

- vzťahy vznikajúce v súvislosti s vyhotovovaním a používaním elektronického podpisu a elektronickej pečate,
- práva a povinnosti fyzických osôb a právnických osôb pri používaní elektronického podpisu a elektronickej pečate,
- hodnovernosť a ochranu elektronických dokumentov podpísaných elektronickým podpisom alebo opatrených elektronickou pečaťou.

V tomto zákone:

- **elektronickým dokumentom** je číselne kódovaný dokument uchovávaný na fyzickom nosiči, prenášaný alebo spracúvaný pomocou technických prostriedkov v elektrickej, magnetickej, optickej alebo inej forme,
- **podpísaným elektronickým dokumentom** je elektronický dokument, pre ktorý bol vyhotovený elektronický podpis alebo elektronická pečať, ak je tento elektronický dokument dostupný spolu s elektronickým podpisom alebo elektronickou pečaťou daného dokumentu.

V styku s orgánmi verejnej moci sa používa *elektronický podpis, zaručený elektronický podpis, elektronická pečať* alebo *zaručená elektronická pečať*.

Elektronický podpis

Elektronický podpis (EP) je technický ekvivalent rukou vytvoreného podpisu. Je to informácia (elektronické údaje), pripojená alebo inak logicky spojená s podpisovaným elektronickým dokumentom, ktorá identifikuje jeho autora (podpisovateľa). Na základe uvedenej vlastnosti je možné elektronicky podpísané dokumenty postaviť na úroveň papierových dokumentov a identifikovať ich autora (odosielateľa). EP sa však nenachádza priamo v dokumente (ale je s ním zviazaný), takže po vytlačení dokumentu sa v ňom podpis nenachádza, a tak stráca platnosť podpísaného dokumentu. EP možno využiť napríklad na podpisovanie elektronických faktúr alebo pri internej firemnej komunikácii. Tento podpis nemusí byť chránený heslom.

Elektronicky podpísaný dokument je možné použiť iba v elektronickej forme. EP je informácia pripojená alebo inak logicky spojená s elektronickým dokumentom, ktorá musí spĺňať tieto požiadavky:

- nemožno ju efektívne vyhotoviť bez znalosti súkromného kľúča a elektronického dokumentu,
- na základe znalosti tejto informácie a verejného kľúča patriaceho k súkromnému kľúču použitému pri jej vyhotovení možno overiť, že elektronický dokument, ku ktorému je pripojená alebo s ním inak logicky spojená, je zhodný s elektronickým dokumentom použitým na jej vyhotovenie.

Zaručený elektronický podpis (ZEP) je taká forma elektronického podpisu, kde totožnosť autora ZEP (podpisovateľa) je jednoznačne a preukázateľne identifikovateľná, pričom právne je postavený na roveň úradne overeného podpisu. Tým sa podpisovateľ vyhne nutnosti osobného kontaktu s tým, kto platnosť podpisu overuje (overovateľom).

Pri použití ZEP hovoríme o otvorených systémoch, teda systémoch, kde sa jednotliví účastníci nemusia osobne poznať. Dôvera v pravosť vytvorených podpisov a bezpečnosť systému nie je odvinutá od osobného kontaktu medzi jednotlivými účastníkmi, ale od pravidiel a noriem, ktoré musia byť dodržané pri všetkých procesoch týkajúcich sa zaručeného elektronického podpisu.

EP a ZEP sa z technického pohľadu nelíšia spôsobom vytvárania a overovania, **líšia sa však úrovňou bezpečnosti**. Dôvera voči EP sa zakladá na spoľahlivosti zariadení a metód, ktoré boli pri jeho vytváraní použité. Požiadavky na bezpečnosť prostredia sú vyššie v prípade ZEP. To sa odráža pri akreditácii – posudzovaní prevádzkových podmienok certifikačných autorít, a rovnako pri certifikácii produktov – posudzovaní bezpečnosti prevádzky zariadení na vytváranie podpisu. Pre EP sú požiadavky na bezpečnosť podstatne nižšie. Tento prístup vyplýva z rozdielneho právneho postavenia EP a ZEP.

ZEP musí spĺňať podmienky ako EP a zároveň:

- je vyhotovený pomocou ***súkromného kľúča***, ktorý je určený na vyhotovenie ZEP; súkromný kľúč je uložený na bezpečnom zariadení na vyhotovenie EP, ktoré je certifikované úradom,
- možno ho vyhotoviť len s použitím bezpečného zariadenia na vyhotovovanie EP,
- spôsob jeho vyhotovovania umožňuje spoľahlivo určiť, ktorá fyzická osoba ZEP vyhotovila,
- na ***verejný kľúč*** patriaci k súkromnému kľúču použitému na vyhotovenie ZEP je vydaný kvalifikovaný certifikát.

Občan, ktorý sa rozhodne používať ZEP, potrebuje na to, aby mohol elektronicky podpisovať nasledujúce prostriedky:

- kvalifikovaný certifikát,
- certifikované zariadenie na uloženie podpisového kľúča – špeciálny USB kľúč, tzv. token,
- certifikovanú podpisovú aplikáciu.

Prvé dva z vyššie uvedených prostriedkov získa občan v ľubovoľnej Akreditovanej certifikačnej autorite. V súčasnosti je na Slovensku viacero autorít, z ktorých najznámejšie a najčastejšie využívanými sú Prvá slovenská certifikačná autorita (PSCA), Certifikačná autorita VÚB (CA VÚB), Certifikačná autorita Dôvera (CA Dôvera) a ďašie.

ZEP je plnohodnotnou náhradou vlastnoručného podpisu, a ak je doplnený **časovou pečiatkou**, je ***ekvivalentom notársky overeného podpisu***. Má preto využitie najmä pri komunikácii so štátnou správou. ZEP dokumentu zabezpečuje:

- **autenticitu** – možno overiť pôvodnosť (identitu subjektu, ktorému patrí EP),
- **integritu** – možno preukázať, že po podpísaní nedošlo k žiadnej zmene, súbor nie je úmyselne alebo neúmyselne poškodený,
- **nepopierateľnosť** – autor nemôže tvrdiť, že podpísaný elektronický dokument nevytvoril (napr. nemôže sa zriecť vytvorenia a odoslania výhražného listu).

Rozdiel medzi EP a ZEP je podobný rozdielu medzi úradne neovereným a overeným vlastnoručným podpisom.

Podpisovateľ vyhotoví EP elektronického dokumentu tak, že na základe svojho súkromného kľúča a elektronického dokumentu vyhotoví nový údaj.

Súkromným kľúčom je tajná informácia, ktorá slúži na vyhotovenie EP elektronického dokumentu alebo elektronickej pečate elektronického dokumentu.

Verejným kľúčom je informácia dostupná overovateľovi, ktorá slúži na overenie správnosti EP alebo elektronickej pečate vyhotovenej pomocou súkromného kľúča patriaceho k danému verejnému kľúču.

Bezpečným zariadením na vyhotovenie EP je prostriedok na vyhotovenie EP, ktorý spĺňa požiadavky zákona a slúži na vyhotovenie ZEP.

Prostriedkom na overenie EP je technické zariadenie alebo programové vybavenie, alebo algoritmy, alebo ich kombinácia, prostredníctvom ktorých môže overovateľ na základe podpísaného elektronického dokumentu a verejného kľúča patriaceho k súkromnému kľúču, ktorý bol použitý na vyhotovenie EP, overiť správnosť elektronického podpisu (obr. 24).

Elektronická pečať

Elektronická pečať je informácia pripojená alebo inak logicky spojená s elektronickým dokumentom, ktorá musí spĺňať tieto požiadavky:

- nemožno ju efektívne vyhotoviť bez znalosti súkromného kľúča a elektronického dokumentu,
- možno na základe znalosti tejto informácie a verejného kľúča patriaceho k súkromnému kľúču použitému pri jej vyhotovení overiť, že elektronický dokument, ku ktorému je pripojená alebo s ním inak logicky spojená, je zhodný s elektronickým dokumentom použitým na jej vyhotovenie,
- obsahuje údaj, ktorý identifikuje pôvodcu pečate.

Zaručená elektronická pečať je elektronická pečať, ktorá musí spĺňať podmienky podľa predchádzajúceho odseku a zároveň:

- je vyhotovená pomocou súkromného kľúča, ktorý je určený výlučne na vyhotovenie zaručenej elektronickej pečate,
- možno ju vyhotoviť len s použitím bezpečného zariadenia na vyhotovovanie elektronickej pečate,
- spôsob jej vyhotovovania umožňuje spoľahlivo určiť, ktorej právnickej osobe alebo orgánu verejnej moci patrí informačný systém, ktorý zaručenú elektronickú pečať vyhotovil,
- na verejný kľúč patriaci k súkromnému kľúču použitému na vyhotovenie zaručenej elektronickej pečate je vydaný kvalifikovaný systémový certifikát.

Časová pečiatka sa používa na preukázanie toho, že elektronický dokument bol vyhotovený v určitom presnom čase. Zdrojom tohto časového údaja je server akreditovanej certifikačnej autority.

Pôvodca pečate vyhotoví elektronickú pečať elektronického dokumentu tak, že na základe svojho súkromného kľúča a elektronického dokumentu vyhotoví nový údaj, vyhotovenie elektronickej pečate prebieha výlučne automatizovaným spôsobom prostredníctvom informačného systému.

Prostriedkom na vyhotovenie EP (elektronickej pečate) je technické zariadenie alebo programové vybavenie, alebo algoritmy, alebo ich kombinácia, prostredníctvom ktorých môže podpisovateľ (pôvodca pečate) na základe elektronického dokumentu a súkromného kľúča podpisovateľa (pôvodcu pečate) vyhotoviť EP elektronického dokumentu (elektronickú pečať elektronického dokumentu).

Prostriedkom na vyhotovenie časovej pečiatky je technické zariadenie a programové vybavenie, ktoré spĺňa požiadavky tohto zákona a prostredníctvom ktorého možno na základe časového údaja, elektronického dokumentu a na tento účel určeného súkromného kľúča vyhotoviť časovú pečiatku daného elektronického dokumentu.

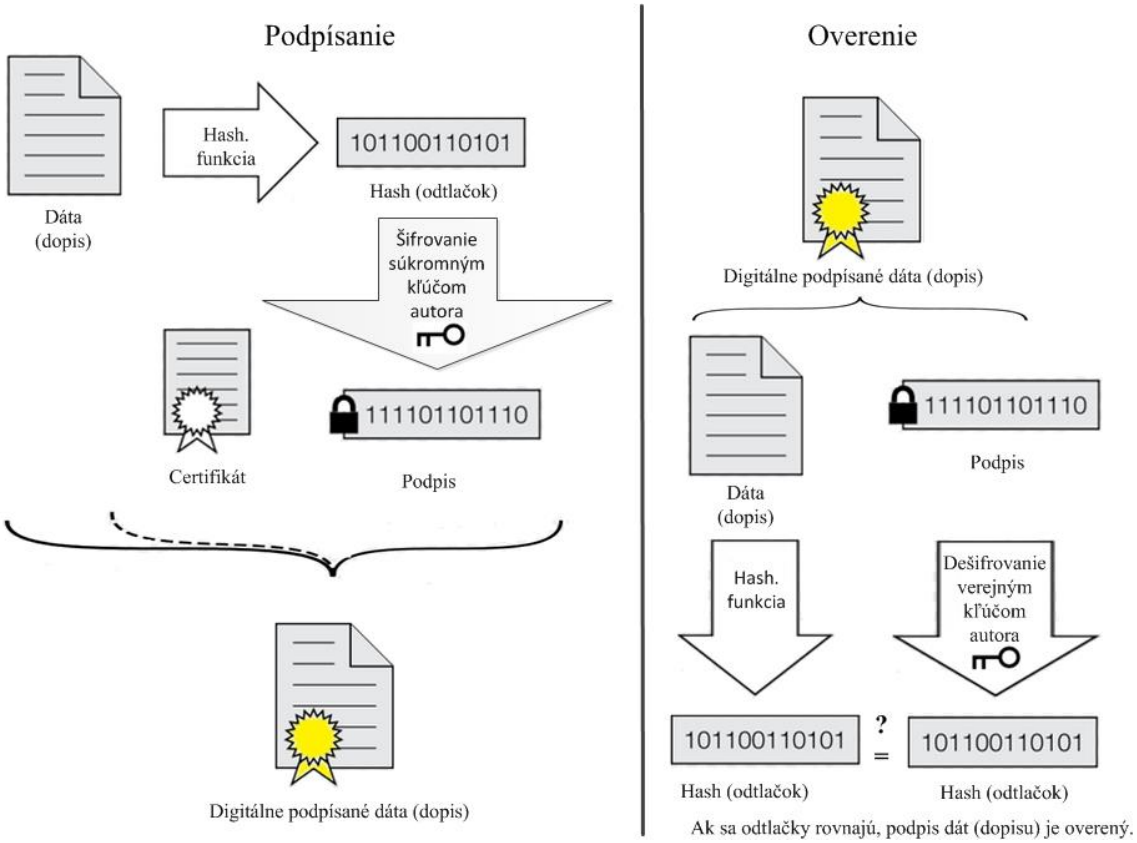
Pri podávaní žiadosti o vydanie elektronického podpisu možno certifikačnú autoritu požiadať i o vydanie časovej pečiatky. V súčasnosti sa dá elektronický podpis využiť pri komunikácii so všetkými inštitúciami s elektronickou podateľňou a nasledujúcimi inštitúciami:

- Finančným riaditeľstvom,
- Obchodným registrom,
- Živnostenským registrom,
- Katastrom nehnuteľností,
- Štatistickým úradom.

Podrobnosti v súvislosti s praktickou aplikáciou EP riešia právne normy:

- Zákon č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
- Vyhláška NBÚ č. 131/2009 Z. z. o formáte, obsahu a správe certifikátov a kvalifikovaných certifikátov a formáte, periodicite a spôsobe vydávania zoznamu zrušených kvalifikovaných certifikátov (o certifikátoch a kvalifikovaných certifikátoch).
- Vyhláška Národného bezpečnostného úradu č. 132/2009 Z. z. o podmienkach na poskytovanie akreditovaných certifikačných služieb a o požiadavkách na audit, rozsah auditu a kvalifikáciu audítorov.
- Vyhláška Národného bezpečnostného úradu č. 133/2009 Z. z. o obsahu a rozsahu prevádzkovej dokumentácie vedenej certifikačnou autoritou a o bezpečnostných pravidlách a pravidlách na výkon certifikačných činností.

- Vyhláška NBÚ č. 136/2009 Z. z. o spôsobe a postupe používania elektronického podpisu v obchodnom styku a administratívnom styku.



Obr. 24 Podpísanie a overenie elektronického podpisu

Trestnoprávna zodpovednosť za porušenie bezpečnosti informačných systémov

Najviac definícií pojmov a právnych vzťahov vo všeobecnej rovine možno nájsť v občianskom práve, ale nie je v ňom zvláštna časť, ktorá by vymedzovala konkrétne aktivity na internete. Občiansky zákonník obsahuje pojmy ako: *spôsobilosť k právnym úkonom, ochrana dobrej viery, ochrana práv tretích osôb,* alebo tiež *zásadu, že „všetko čo je dovolené, nie je zakázané“, základné práva a povinnosti, charakteristiku občiansko-právnych vzťahov.*

Trestné právo, pod ktoré spadá Trestný zákon a Trestný poriadok a samostatne stojaci autorský zákon rieši najmä právne vzťahy súvisiace s počítačovými programami, licenčné zmluvy týkajúce sa softvéru, definíciu osoby s právami k rozmnoženine počítačového programu a pod. Počítačová kriminalita je v Trestnom zákone uvedená napr. v ustanovení § 247 Poškodenie a zneužitie záznamu na nosiči informácií.

11.5 LITERATÚRA

ČABÁK, P. [2013]: *Právna úprava spamu (nevyžiadanej pošty).* In: Právo v kultúre, konferencia Národného centra práva duševného vlastníctva 28.-29.11.2013. Košice.

DVOŘÁK, Z. et al. [2007]: *Informatizácia, informačné systémy a bezpečnostný manažment.* Žilina: EDIS – vydavateľstvo ŽU, ISBN 978-80-8070-783-5.

JAKÁBOVÁ M. – URDZIKOVÁ, J. [2013]: *Štandardizácia systému manažérstva informačnej bezpečnosti.* In: Zborník príspevkov zo seminára Informačné a komunikačné technológie v riadení a vzdelávaní. FEM, SPU v Nitre.

KNAPP, K. – KUNZ, O. [2001]: *Mezinárodní právo autorské,* , Praha Academia.

LOVEČEK, T. [2007]: *Bezpečnosť informačných systémov*. Žilina: FŠI ŽU 2007. ISBN: 80-8070-767-5.

MRAČKO, M. [2009]: *Elektronický podpis, certifikácia a ochrana osobných údajov (príručka)*, Vydavateľ Epos, ISBN 978-80-8057-806-0 (brož.).

MRAČKO,M. [2001]: *Predpisy o autorských a odborných právach,* ISBN 80-8057-255-0 (brož.) , 304 s.

ONDREÁŠOVÁ, V. [2006]: *Ochrana informácií v podniku*. In: Veda a krízové situácie. 2006 ISBN 80-8070-601-8.

12 OCHRANA UTAJOVANÝCH SKUTOČNOSTÍ

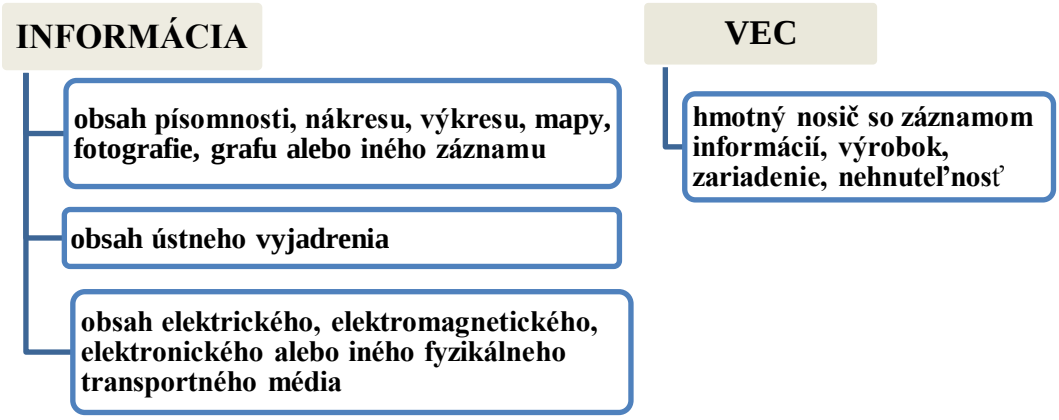
Ochranu utajovaných skutočností (OUS) rieši:

- Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- Nariadenie vlády č. 216/2004 Z. z. ktorým sa ustanovujú oblasti utajovaných skutočností.

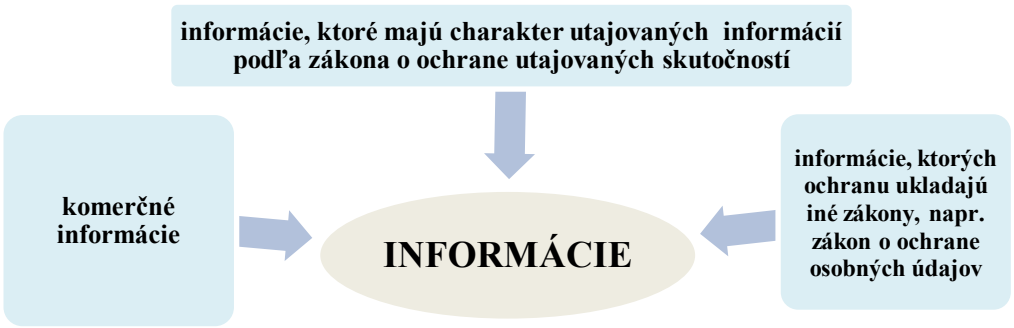
Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností upravuje:

- podmienky na ochranu utajovaných skutočností (OUS) a povinnosti právnických osôb a fyzických osôb pri tejto ochrane,
- pôsobnosť NBÚ a ďalších štátnych orgánov vo vzťahu k utajovaným skutočnostiam,
- pôsobnosť NBÚ pri zabezpečovaní podkladov pre rozhodovanie Súdnej rady SR o splnení predpokladov sudcovskej spôsobilosti,
- zodpovednosť za porušenie povinností ustanovených v zákone.

Utajovanou skutočnosťou je ***informácia*** alebo ***vec,*** určená pôvodcom utajovanej skutočnosti, ktorú vzhľadom na záujem SR treba chrániť pred vyzradením, zneužitím, poškodením, neoprávneným rozmnožením, zničením, stratou alebo odcudzením (ďalej len neoprávnená manipulácia) a ktorá môže vznikať len v oblastiach, ktoré ustanoví vláda SR svojím nariadením.



Obr. 25 Utajovaná skutočnosť



Obr. 26 Druhy informácií

Utajované skutočnosti sa podľa stupňa utajenia členia na:

a) **PRÍSNE TAJNÉ** – utajovaná skutočnosť, pri ktorej by následkom neoprávnenej manipulácie s ňou mohlo byť vážne ohrozené zachovanie ústavnosti, zvrchovanosti a územnej celistvosti štátu, alebo by mohli vzniknúť nenahraditeľné a vážne škody v oblasti obrany, bezpečnosti, ekonomických záujmov, zahraničnej politiky alebo medzinárodných vzťahov, a tým mohla vzniknúť ***mimoriadne vážna ujma*** na záujmoch SR.
b) **TAJNÉ** – utajovaná skutočnosť, pri ktorej by následkom neoprávnenej manipulácie s ňou mohlo byť ohrozené zahraničnopolitické postavenie, obrana, bezpečnosť a záujmy štátu v medzinárodnej a ekonomickej oblasti, a tým by mohla vzniknúť ***vážna ujma*** na záujmoch SR.
c) **DÔVERNÉ** – označuje sa utajovaná skutočnosť vtedy, ak by následkom neoprávnenej manipulácie s ňou mohlo dôjsť k poškodeniu štátnych záujmov, verejných záujmov alebo právom chránených záujmov štátneho orgánu, a tým k ***jednoduchej ujme*** na záujmoch SR.
d) **VYHRADENÉ** – označuje sa utajovaná skutočnosť vtedy, ak by neoprávnená manipulácia s ňou mohla zapríčiniť poškodenie právom chránených záujmov právnickej osoby alebo fyzickej osoby, ktoré by mohlo byť ***nevýhodné pre záujmy*** SR.

Medzi základné **bezpečnostné požiadavky na ochranu informácie** pred náhodným alebo úmyselným nesprávnym použitím ľuďmi vo vnútri alebo mimo organizácie alebo objektu patria:

a) **Dôvernosť** *(Confidentiality)* – zabezpečenie toho, že informácie sú poskytnuté a prístupné len oprávneným osobám,
b) **Integrita** *(Integrity)* – zabezpečenie správnosti a úplnosti informácií z hľadiska obsahu a formy,
c) **Dostupnosť** *(Availability)* – informácia je k dispozícii oprávneným osobám vždy, keď ju potrebujú – správne informácie, správnym ľuďom, v správny čas,
d) **Autentickosť** *(Authenticity)* – zabezpečenie integrity a zároveň pôvodu dokumentu,
e) **Sledovateľnosť** *(Accountability)* – možnosť zistiť, ktorý subjekt vykonal bezpečnostne relevantné činnosti, napr. vložil, zmenil, zmazal alebo čítal určitú informáciu,
f) **Ochrana súkromnosti** *(Privacy)* – zabezpečuje chráneným spôsobom prístup ku kompletnej informácií len užšiemu okruhu oprávnených používateľov.

Medzi **kľúčové prvky bezpečnosti informácií** patrí:

- poskytovanie údajov výhradne oprávneným subjektom,
- zabránenie neoprávneným zmenám alebo korupcii dôverných údajov,
- preverenie oprávnených osôb na prístup k dôležitým informáciám a systémom,
- zabezpečenie, aby tieto údaje boli odovzdané, prevzaté alebo spoločne podieľané len určenou stranou,
- zaistenie bezpečnosti vlastníkom informácií.

Ochrana utajovaných skutočností predstavuje vytváranie podmienok pre:

- administratívnu bezpečnosť,
- personálnu bezpečnosť,
- priemyselnú bezpečnosť,
- bezpečnosť technických prostriedkov,
- šifrovú ochranu informácií,
- fyzickú bezpečnosť a objektovú bezpečnosť.

12.1 ADMINISTRATÍVNA BEZPEČNOSŤ

Administratívnu bezpečnosť rieši:

a) Zákon NR SR č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
b) Vyhláška NBÚ č. 453/2007 Z. z. o administratívnej bezpečnosti, ktorá upravuje:
   - administratívnu bezpečnosť registratúrnych záznamov obsahujúcich ***utajované písomnosti,***
   - opatrenia administratívnej bezpečnosti pre ochranu utajovaných skutočností na ***hmotných nosičoch utajovaných písomností***.

Manipulácia s utajovanou skutočnosťou je tvorba, príjem, evidencia, preprava, prenášanie, ukladanie, rozmnožovanie, vyraďovanie, uschovávanie a akékoľvek iné nakladanie s utajovanou písomnosťou, ktorá sa zaznamenáva v *administratívnej pomôcke*. Ochranu utajovanej písomnosti počas manipulácie s ňou zabezpečuje oprávnená osoba.

Administratívnou pomôckou je najmä:

- Protokol utajovaných písomností príslušného stupňa utajenia.
- Doručovací zošit.
- Zápisník oprávnenej osoby.
- Výpožičková kniha.
- Poznámkový zošit na vyhotovovanie výpisov a na prácu s utajovanými skutočnosťami pre označený stupeň utajenia.
- Evidencia utajovaných interných predpisov.
- Evidencia utajovaných písomností.
- Centrálny register utajovaných skutočností.
- Evidencia neoprávnených manipulácií.
- Evidencia osvedčení kuriéra na prepravu utajovaných písomností.
- Evidencia bezpečnostných spisov.

Každá utajovaná písomnosť sa označuje stupňom utajenia už pri jej vytváraní.

Na prvej strane utajovanej písomnosti sa uvádza:

- číslo utajovanej písomnosti,
- stupeň utajenia,
- číslo výtlačku,
- počet listov podľa stupňov utajenia, ak utajovaná písomnosť obsahuje rôzne stupne utajenia,
- počet príloh pevne nespojených s utajovanou písomnosťou, lomený počtom listov jej príloh, rozdelený podľa stupňov utajenia,
- počet príloh utajovanej písomnosti nelistinného charakteru.

12.2 PERSONÁLNA BEZPEČNOSŤ

Personálna bezpečnosť *(Personnel Security)* je systém opatrení súvisiacich s výberom, určením a kontrolou osôb, ktoré sa môžu v určenom rozsahu oboznamovať s utajovanými skutočnosťami. Predstavuje elimináciu hrozieb spôsobených ľudským faktorom.

Podrobnosti o postupe pri určovaní osoby oboznamovať sa s utajovanými skutočnosťami, o zániku určenia a o skúške bezpečnostného zamestnanca rieši Vyhláška NBÚ č. 331/2004 Z. z. personálnej bezpečnosti a o skúške bezpečnostného zamestnanca. Je to:

- súhrn pravidiel s metodikou zverovania zodpovednosti a postupov výberu a kontroly dôveryhodnosti a lojálnosti pracovníkov,
- systém opatrení súvisiacich s výberom, určením a kontrolou osôb, ktoré sa môžu v určenom rozsahu oboznamovať s utajovanými skutočnosťami,
- definuje postupy pre požadované stupne kontroly dôvernosti zamestnancov a udeľovanie oprávnení k rozsahu oboznámenia sa s citlivými informáciami,
- zahŕňa tiež získanie odbornej spôsobilosti systémom nástupných a priebežných školení.

Personálna bezpečnostná politika má **ciele:**

- chrániť citlivé informácie,
- stanoviť kľúčové body týkajúce sa správy a riadenia informačnej bezpečnosti,
- bezpečne riadiť *„životný cyklus“* zamestnania (nástup do zamestnania, v zamestnaní, skončenie pracovného pomeru atď.).

Na základe analýzy kombinácií osvedčených postupov, skutočných udalostí a regulačných požiadaviek možno uviesť niekoľko kľúčových oblastí, ktoré by mali byť zahrnuté v personálnej bezpečnostnej politike, aby čo najlepšie chránili organizáciu (životný cyklus):

Obr. 27 Postupnosť uplatňovania personálnej bezpečnosti

1. **Overovanie** *(Screening)* – proces overovania osobných dokladov budúceho zamestnanca a jeho vhodnosti pre prácu. Najčastejšie je to vo forme kontroly osobných spisov, hodnotenia dobrej povesti alebo emocionálne skúšky stability, alebo podľa hodnotenia posudkov predchádzajúcich zamestnávateľov. Hlavnou myšlienkou je ubezpečenie, že ***v minulosti trestané osoby nie sú prijaté alebo umiestnené na dôverné pozície*** v rámci organizácie.
2. **Dohody** *(Contracts)* – tento krok je rovnako dôležitý, pokiaľ ide o riadenie a schopnosť podniknúť opatrenia proti zamestnancom, ktorí porušujú bezpečnostnú politiku. Dohody zahŕňajú ***pracovné zmluvy, dohody o nepodporovaní konkurencie, dohody o mlčanlivosti a dohody o ochrane duševného vlastníctva.*** Zmluvy sú navrhnuté tak, aby chránili duševné vlastníctvo pred odcudzením alebo stratou.
3. **Potvrdenie znalosti bezpečnostnej politiky** – každý zamestnanec alebo dodávateľ s prístupom k informáciám musia poznať politiky bezpečnosti informácií, s ktorými prichádza-

jú do styku, aby sa neskôr nevyhovárali, že neboli s nimi zoznámení. Bez ***písomného potvrdenia*** sa len málo organizácií dokáže brániť proti tvrdeniam zamestnancov, že nepoznali zásady bezpečnosti.

4. **Bezpečnostné vzdelávanie** – jeden z najčastejšie ignorovaných aspektov personálnej bezpečnosti je osveta a vzdelávanie. Zamestnanci musia byť ***vyškolení o základných zásadách bezpečnosti informácií,*** aby mohli rozpoznať spoločné hrozby, ako napríklad útoky typu phishing. Štúdie preukázali, že ľudská chyba je príčina väčšiny narušenia dát. Okrem základného vzdelávania by zamestnanci mali zvládnuť aj politiku bezpečnosti informácií organizácie.
5. **Monitorovanie** – napriek tomu, že zamestnanci sú preverení ako dôverní pre organizáciu, musí sa ich správanie na určitej úrovni stále monitorovať. Typ a úroveň kontroly závisí od mnohých faktorov, vrátane citlivosti informácií. Organizácie by minimálne mali sledovať všetky aktivity používateľa súvisiace so zabezpečením systémov. Pritom je najlepšie informovať zamestnancov o tom, že sú sledovaní.
6. **Postupy pri ukončení zamestnania** – poslednou podstatnou zložkou personálnej bezpečnosti sú správne postupy pri ukončení zamestnania a ich presadzovanie. Ihneď, ako zamestnanec ukončí pracovnú zmluvu alebo uviedol, že sa chystá odísť, musí sa uskutočniť obvyklý postup. Výstupný proces zvyčajne zahŕňa ***návrat majetku organizácie***, ako sú notebooky alebo prístupové preukazy. Dodržanie postupov ukončenia je potrebné najmä v informačnej bezpečnosti. V mnohých prípadoch bývalí zamestnanci boli schopní ponechať si prístup k sieti svojho zamestnávateľa – buď svoje vlastné prihlasovacie ID alebo spoločne používané ID a kradnúť dáta alebo šíriť škodlivý softvér.

12.3 PRIEMYSELNÁ BEZPEČNOSŤ

Základným predpisom pre priemyselnú bezpečnosť je Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností. Ďalším všeobecne záväzným predpisom, ktorý upravuje podrobnosti o priemyselnej bezpečnosti, je Vyhláška NBÚ č. 301/2013 Z. z. o priemyselnej bezpečnosti a o bezpečnostnom projekte podnikateľa.

Ak je odôvodnený predpoklad, že **štátny orgán požiada podnikateľa** o vytvorenie utajovanej skutočnosti, alebo ak bude potrebné postúpiť utajovanú skutočnosť zo štátneho orgánu podnikateľovi, je podnikateľ povinný požiadať úrad o vydanie **potvrdenia o priemyselnej bezpečnosti.**

Potvrdenie o priemyselnej bezpečnosti podnikateľa možno vydať iba podnikateľovi, ktorý je:

a. spôsobilý zabezpečiť ochranu utajovaných skutočností – má vytvorené podmienky na zabezpečenie ochrany utajovaných skutočností podľa zákona,
b. ekonomicky stabilný,
c. bezpečnostne spoľahlivý – podnikateľ, u ktorého nebolo zistené bezpečnostné riziko.

Za **bezpečnostné riziko** sa považuje:

a) konanie proti záujmom SR v oblasti obrany štátu, bezpečnosti štátu, medzinárodných stykov, hospodárskych záujmov štátu, chodu štátneho orgánu alebo proti záujmom, ktoré sa zaviazala SR chrániť,
b) zahraničný, obchodný alebo majetkový vzťah, ktorý by mohol spôsobiť ujmu zahraničnopolitickým alebo bezpečnostným záujmom SR,
c) existencia obchodných, majetkových alebo finančných vzťahov s osobami z prostredia organizovaného zločinu,
d) korupčné správanie podnikateľa,
e) personálna nestabilita vo vedúcich funkciách alebo orgánoch podnikateľa alebo
f) zrušenie platnosti osvedčenia vedúceho podnikateľa.

Utajovanú skutočnosť možno **postúpiť zo štátneho orgánu na podnikateľa**, ktorému bolo vydané potvrdenie o priemyselnej bezpečnosti, iba na základe zmluvy.

Zmluva musí obsahovať špecifikáciu postupovaných utajovaných skutočností, stupeň utajenia, obdobie, počas ktorého budú postupované utajované skutočnosti, zoznam osôb, rozsah ich oprávnenia na oboznamovanie sa s utajovanými skutočnosťami, rozsah činností s utajovanou skutočnosťou, rozsah kontrolných opatrení, povinnosť oznámenia o zrušení podnikateľa alebo o zmenách ovplyvňujúcich ochranu utajovaných skutočností, postupovanie utajovaných skutočností na iného podnikateľa, ako i povinnosti podnikateľa pri zániku platnosti potvrdenia o priemyselnej bezpečnosti.

Bezpečnostnou previerkou podnikateľa úrad zisťuje, či spĺňa podmienky priemyselnej bezpečnosti. Zamestnanec podnikateľa, ktorý sa bude oboznamovať s utajovanými skutočnosťami, musí byť oprávnenou osobou pre príslušný stupeň utajenia.

Bezpečnostný projekt podnikateľa je projekt systému ochrany utajovaných skutočností u podnikateľa. Bezpečnostný projekt podnikateľa obsahuje najmä definovanie bezpečnostnej politiky a spôsob jej realizácie v oblasti personálnej bezpečnosti, administratívnej bezpečnosti, objektovej a fyzickej bezpečnosti, šifrovej ochrany informácií a bezpečnosti technických prostriedkov. Jeho súčasťou je tiež zoznam osôb, ktoré sa budú s utajovanými skutočnosťami zoznamovať.

12.4 BEZPEČNOSŤ TECHNICKÝCH PROSTRIEDKOV

Zásady bezpečnosti technických prostriedkov rieši Vyhláška NBÚ č. 339/2004 Z. z. o bezpečnosti technických prostriedkov. Táto vyhláška ustanovuje podrobnosti o:

- bezpečnosti technických prostriedkov,
- schvaľovaní technických prostriedkov do prevádzky,
- použití technických prostriedkov,
- požiadavkách kladených na technické prostriedky, na ktorých sa vytvárajú, spracúvajú, prenášajú, ukladajú a archivujú utajované skutočnosti,
- postupe pri certifikácii technických prostriedkov,
- spracúvaní bezpečnostného projektu na technické prostriedky,
- vydávaní a používaní bezpečnostných štandardov (súbor noriem, ktoré určujú minimálne kritériá pre požadovanú úroveň ochrany technických prostriedkov).

Bezpečnosť technických prostriedkov predstavuje systém opatrení na zabezpečenie ochrany utajovaných skutočností, ktoré sa tvoria, spracúvajú, prenášajú, ukladajú alebo archivujú na technických prostriedkoch.

Technickým prostriedkom je zariadenie alebo systém určený na vytváranie, spracúvanie, prenos, ukladanie a ochranu utajovaných skutočností – ***nosiče utajovaných skutočností***.

Charakter nosiča informácií majú:

- **prenosné technické prostriedky** (notebook, tablet, vreckový počítač),
- **mobilné technické prostriedky,**
- **technické prostriedky umiestnené mimo chráneného priestoru** majú charakter ***nosiča informácií.***

Technický prostriedok sa umiestňuje tak, aby sa zamedzilo nepovolaným osobám oboznamovať sa s utajovanými skutočnosťami. Technické prostriedky sa umiestňujú v ***chránených priestoroch***, v ktorých je zabezpečená ich ochrana pred neoprávneným prístupom nepovolaných osôb, pred poškodením, nežiaducim elektromagnetickým vyžarovaním alebo manipuláciou v súlade s bezpečnostným projektom. Spôsob ochrany technických prostriedkov musí zodpovedať požiadavkám na bezpečnosť technických prostriedkov spracúvajúcich utajované skutočnosti príslušného stupňa utajenia.

Všetky nosiče utajovaných skutočností sa evidujú ako administratívne pomôcky, ak je to možné vzhľadom na charakter nosiča a účel použitia. Na prácu s utajovanými skutočnosťami v štátnom orgáne alebo u podnikateľa možno používať iba technické prostriedky schválené do prevádzky vedúcim. Nepoužiteľné nosiče utajovaných skutočností sa ničia fyzicky alebo špeciálnymi softvérovými a hardvérovými prostriedkami komisionálnym spôsobom, aby žiadnym spôsobom nebolo možné informácie z nosiča spätne získať.

Informačným systémom sa rozumie jeden alebo viac počítačov, ich programové vybavenie, periférne zariadenia, procesy alebo prostriedky, ktoré tvoria celok schopný vykonávať zber, tvorbu, spracovanie, ukladanie, zobrazenie a prenos utajovaných skutočností.

Prevádzkovateľ informačného systému zodpovedná za bezpečnosť jeho prevádzky v súlade s bezpečnostným projektom a smernicami. Na jeho prevádzku určuje oddelene:

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

12.5 ŠIFROVÁ OCHRANA INFORMÁCIÍ

Šifrovú ochranu informácií rieši Vyhláška NBÚ č. 340/2004 Z. z. ktorou sa ustanovujú podrobnosti o šifrovej ochrane, ktorá upravuje podrobnosti o:

- certifikácii a schvaľovaní systémov a prostriedkov šifrovej ochrany informácií do prevádzky, ich použití, nasadení, preprave, evidencii a používaní šifrových materiálov,
- vedení evidencie zamestnancov na úseku šifrovej ochrany informácií a overovaní ich odbornej spôsobilosti,
- zriaďovaní rezortného šifrového orgánu alebo jemu na roveň postaveného šifrového orgánu.

Informácie, ktoré sú utajovanými skutočnosťami, musia byť pri prenose technickými prostriedkami chránené prostriedkami šifrovej ochrany informácií.

Šifrovou ochranou informácií je systém na zabezpečenie ochrany utajovaných skutočností kryptografickými metódami a prostriedkami šifrovej ochrany informácií. Prostriedkom šifrovej ochrany informácií je zariadenie určené na šifrovú ochranu informácií a šifrové materiály.

Systém šifrovej ochrany informácií predstavuje súbor prostriedkov šifrovej ochrany informácií spolu s celou infraštruktúrou na generovanie, distribúciu a likvidáciu šifrových materiálov po skončení ich platnosti.

Certifikáciou prostriedkov šifrovej ochrany sa overuje a osvedčuje spôsobilosť prostriedku chrániť utajované skutočnosti v súlade s bezpečnostným štandardom pre systémy a prostriedky šifrovej ochrany informácií a s bezpečnostným štandardom na ochranu pred nežiaducim elektromagnetickým vyžarovaním.

Rezortný šifrový orgán certifikuje prostriedky na ochranu utajovaných skutočností stupňa utajenia Dôverné a Vyhradené vo svojej pôsobnosti. Certifikuje aj prostriedky na ochranu utajovaných skutočností stupňa utajenia Dôverné a Vyhradené, o ktorých certifikáciu bol požiadaný právnickou osobou, ktorá spĺňa podmienky priemyselnej bezpečnosti podľa osobitného predpisu, ak predpokladá možnosť ich používania.

Pred inštaláciou prostriedku v podmienkach certifikačného pracoviska dodá žiadateľ protokol o vykonaných prevádzkových skúškach prostriedku, vydané certifikáty iných autorizovaných osôb, zoznam noriem, ktorým prostriedok vyhovel, a potrebný počet kusov prostriedku podľa určenia certifikačného pracoviska úradu alebo rezortného šifrového orgánu.

Podľa zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností NBÚ SR plní úlohu ústredného šifrového orgánu v SR. Medzi hlavné úlohy, ktoré NBÚ plní na úseku šifrovej ochrany informácií (ŠOI) patrí:

- vykonávanie certifikácie prostriedkov ŠOI a uznávanie zahraničných certifikátov prostriedkov ŠOI,
- vykonávanie kontroly bezpečnosti ŠOI,
- vydávanie bezpečnostných štandardov pre oblasť ŠOI,
- odborná príprava zamestnancov na úseku ŠOI,
- koordinácia výskumu a vývoja prostriedkov ŠOI,
- metodické riadenie a koordinácia na úseku ŠOI,
- zabezpečovanie vládneho a zahraničného spojenia.

12.6 FYZICKÁ BEZPEČNOSŤ A OBJEKTOVÁ BEZPEČNOSŤ

Podľa Zákona č. 215/2004 Z. z. 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.**

12.6.1 Objekty a chránené priestory

Objektom je budova alebo iný stavebne alebo inak ohraničený priestor, v ktorom sa nachádzajú chránené priestory.

Chráneným priestorom je stavebne alebo inak ohraničený priestor vo vnútri objektu, ***ktorý je určený na ukladanie a manipuláciu s utajovanými skutočnosťami,*** zodpovedajúci príslušnému stupňu utajenia. Na účely ochrany utajovaných skutočností sa chránený priestor určuje ako ***chránený priestor kategórie:***

- Prísne tajné alebo skratkou „PT“,
- Tajné alebo skratkou „T“,
- Dôverné alebo skratkou „D“,
- Vyhradené alebo skratkou „V“.

Podľa prístupu k utajovaným skutočnostiam sa chránený priestor kategórie Dôverné, Tajné a Prísne tajné určuje ako chránený priestor triedy I alebo chránený priestor triedy II (Vyhláška NBÚ č. 336/2004 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti).

Chránený priestor triedy I – priestor určený na ukladanie alebo manipuláciu s utajovanými skutočnosťami stupňa utajenia Dôverné alebo vyššieho takým spôsobom, že vstup do tohto priestoru znamená oboznámenie sa s utajovanou skutočnosťou. Takýto chránený priestor má:

a) určenú hranicu, na ktorej sa kontroluje každý vstup a výstup a každý vjazd a výjazd,
b) systém kontroly vstupu, ktorý umožní vstup len oprávneným osobám s oprávnením na vstup vydaným vedúcim,
c) špecifikáciu utajovaných skutočností podľa zoznamu utajovaných skutočností, ktoré sa zvyčajne nachádzajú v tomto chránenom priestore.

Chránený priestor triedy II – priestor určený na ukladanie alebo manipuláciu s utajovanými skutočnosťami stupňa utajenia Dôverné alebo vyššieho tak, že utajované skutočnosti sú chránené voči neoprávnenej manipulácii určenými opatreniami a vstup do tohto priestoru neznamená oboznámenie sa s utajovanou skutočnosťou. Takýto chránený priestor má:

a) určenú hranicu, na ktorej sa kontroluje každý vstup a výstup a každý vjazd a výjazd,
b) systém kontroly vstupu, ktorý umožní vstup bez sprievodu len oprávneným osobám; všetky ostatné osoby musia byť sprevádzané a zároveň musia byť prijaté opatrenia zabraňujúce neoprávnenej manipulácii,
c) špecifikáciu utajovaných skutočností podľa zoznamu utajovaných skutočností, ktoré sa zvyčajne nachádzajú v tomto chránenom priestore.

Nepovolanou osobou je fyzická osoba, ktorá nie je oprávnená oboznamovať sa s utajovanými skutočnosťami, alebo ktorá nie je oprávnená oboznamovať sa s utajovanými skutočnosťami nad rozsah, ktorý jej je určený.

Oprávnenou osobou je právnická osoba alebo fyzická osoba, ktorá je určená na oboznamovanie sa s utajovanými skutočnosťami, alebo ktorej oprávnenie na oboznamovanie sa s utajovanými skutočnosťami vzniklo zo zákona.

Bezpečnostný štandard fyzickej bezpečnosti a objektovej bezpečnosti ustanovuje pravidlá a podmienky na ***minimálnu požadovanú úroveň ochrany objektov a chránených priestorov*** určených na ukladanie a manipuláciu s utajovanými skutočnosťami.

Štruktúra bezpečnostného štandardu umožňuje vytvárať variabilný systém bezpečnostných opatrení podľa miestnych podmienok (dislokácie a štruktúry objektu, vyhodnotenia rizík možného ohrozenia utajovaných skutočností a podobne) v súlade so všeobecne záväznými právnymi predpismi.

Cieľom bezpečnostného štandardu je vytvorenie funkčného, efektívneho a z hľadiska finančnej náročnosti optimálneho ***systému ochrany utajovaných skutočností***. Na ohodnotenie úrovne fyzickej bezpečnosti a objektovej bezpečnosti sa používa **bodovací systém**, ktorý umožňuje voliť v závislosti od konkrétnych podmienok takú kombináciu bezpečnostných opatrení, ktorá najlepšie vyhovuje daným podmienkam.

Pre objekty a chránené priestory sú ustanovené najmenšie bodové hodnoty, ktoré treba dosiahnuť. Používa sa matematická metóda prideľujúca jednotlivým bezpečnostným opatreniam ustanovené bodové ohodnotenia, ktorých súčet sa príslušným spôsobom vyhodnocuje.

12.6.2 Ochrana objektu a chráneného priestoru

Ochrana objektov a chránených priestorov (systém ochrany objektov a chránených priestorov) sa zabezpečuje:

- **mechanickými zábrannými prostriedkami,**
- **technickými zabezpečovacími prostriedkami (poplachové systémy),**
- **fyzickou ochranou,**
- **režimovými opatreniami,**
- **a ich vzájomnou kombináciou** v súlade s bezpečnostným štandardom fyzickej bezpečnosti a objektovej bezpečnosti.

Spôsob, podmienky a rozsah navrhovaných opatrení na ochranu objektov a chránených priestorov ***určí vedúci na základe vyhodnotenia rizík.***

Ochrana objektov a chránených priestorov sa zabezpečuje podľa ***bezpečnostnej dokumentácie fyzickej bezpečnosti a objektovej bezpečnosti, ktorú schvaľuje vedúci.***

Podľa vyhlášky NBÚ č. 336/2004 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti:

1. **Mechanickými zábrannými prostriedkami** sú:
   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. **Technickými zabezpečovacími prostriedkami** sú:
   a) systémy na kontrolu vstupov do objektov a systémy určené 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.

Ochrana objektu v rámci OUS sa zabezpečuje najmä ***mechanickými zábrannými prostriedkami*** uvedenými v písmenách **b** až **g** a ***technickými zabezpečovacími prostriedkami*** uvedenými v písmenách **a** až **c**.

Ak je hranica objektu totožná s hranicou chráneného priestoru, použijú sa na jej ochranu ***certifikované*** mechanické zábranné prostriedky a certifikované technické zabezpečovacie prostriedky príslušnej kategórie. Prostriedky nižšej kategórie sa použijú v prípade, ak sú splnené požiadavky bezpečnostného štandardu (pravidlá a podmienky na minimálnu požadovanú úroveň ochrany objektov a chránených priestorov určených na ukladanie a manipuláciu s utajovanými skutočnosťami).

Ochrana chráneného priestoru určeného na ukladanie ***utajovaných skutočností*** sa zabezpečuje ***všetkými mechanickými zábrannými prostriedkami a všetkými technickými zabezpečovacími prostriedkami***. Ochrana chráneného priestoru určeného na ukladanie utajovaných skutočností stupňa utajenia Prísne tajné a utajovaných skutočností postúpených SR cudzou mocou stupňa utajenia Prísne tajné sa zabezpečuje aj ***elektrickou požiarnou signalizáciou.***

Na ich zavedenie je treba vytvoriť časový harmonogram, plán finančného zabezpečenia a zabezpečiť potrebné zdroje. Fyzická ochrana sa obvykle rieši outsourcingovým spôsobom – prenajímaním príslušníkov SBS, ale aj vlastnými zamestnancami (vlastná ochrana). Veľmi dôležitá je príprava (školenie) týchto zamestnancov a dodržiavanie zásad komunikácie o bezpečnosti.

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.

12.6.3 Bezpečnostná dokumentácia pre fyzickú bezpečnosť a objektovú bezpečnosť

Podľa Vyhlášky NBÚ č. 336/2004 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti bezpečnostnú dokumentáciu fyzickej bezpečnosti a objektovej bezpečnosti objektov a chránených priestorov predstavujú:

1. **Bezpečnostná dokumentácia pre kategórie Tajné a Prísne tajné:**
   a) vyhodnotenie rizík podľa § 5 ods. 1 a 2,
   b) bezpečnostný plán ochrany objektu,
   c) technická dokumentácia objektu,
   d) prevádzkový poriadok objektu,
   e) pravidlá na výkon fyzickej ochrany objektu,
   f) krízový plán ochrany objektu,
   g) kniha kontrol,
   h) kniha návštev chráneného priestoru.
2. **Bezpečnostná dokumentácia pre kategórie Vyhradené a Dôverné:**
   a) vyhodnotenie rizík podľa § 5 ods. 1 a 2,

b) adresa a opis objektu a chráneného priestoru, určenie hranice objektu a chráneného priestoru vrátane opisu jej umiestnenia, vstupov, hrúbky stien, rozmerov okien, výšky okien nad úrovňou terénu a podobne,
c) určenie kategórie a triedy chránených priestorov, ktoré sa v objekte nachádzajú, spolu s opisom činností, ktoré sa v nich budú vykonávať,
d) pre každý chránený priestor spracovaná tabuľka bodového ohodnotenia bezpečnostných opatrení podľa bezpečnostného štandardu,
e) zoznam a špecifikácia mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov, pravidlá a pokyny na používanie mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov, návody na ich obsluhu a údržbu, plány kontroly, údržby a overovania funkčnosti, záznamy z vykonaných kontrol; kontrola funkčnosti sa vykonáva najmenej raz ročne,
f) kópie certifikátov mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov,
g) záznamy o overení funkčnosti mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov používaných užívateľmi po uplynutí doby platnosti certifikátu typu,
h) režimové opatrenia podľa § 10 ods. 1 a spôsob kontroly dodržiavania týchto opatrení.

Vyhodnotenie rizík podľa § 5 ods. 1 a 2 obsahuje:

Riziká *možného ohrozenia* utajovaných skutočností v chránenom priestore určí vedúci po zhodnotení:
a) stupňa utajenia utajovaných skutočností,
b) množstva utajovaných skutočností,
c) požiadavky na obmedzenie počtu oprávnených osôb, ktoré sa majú oboznamovať s utajovanými skutočnosťami,
d) potreby oboznamovať sa s utajovanou skutočnosťou v rámci výkonu svojich povinností alebo úloh vlastnými zamestnancami a zamestnancami zabezpečujúcimi fyzickú ochranu, ktorí vzhľadom na svoje oprávnenia a vstupy do chránených priestorov by mohli byť nápomocní vonkajším narušiteľom alebo byť narušiteľmi (napríklad úmyselné poškodzovanie, únik utajovaných informácií, krádež, pasívne alebo aktívne odpočúvanie),
e) *rizika ohrozenia* utajovaných skutočností najmä z hľadiska polohy, umiestnenia a zabezpečenia ochrany objektu a chráneného priestoru, činnosti cudzích spravodajských služieb, záškodníkov, teroristických a zločineckých skupín, technických porúch, rizík vyplývajúcich z činnosti zamestnancov (napríklad nedostatok vedomostí, zábudlivosť, náhoda) a mimoriadnych situácií) za riziko sa považujú aj okolité objekty, ktorých havária by mohla ochromiť, resp. narušiť bezpečnosť chráneného objektu,
f) *rizika ohrozenia* utajovaných skutočností v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu.

Na základe uvedeného zhodnotenia vedúci:
a) posúdi stav zabezpečenia objektu a chráneného priestoru a stav bezpečnostných opatrení v súlade s touto vyhláškou; ak prijaté opatrenia nepostačujú, rozhodne o prijatí ďalších opatrení,
b) vyhodnotí zostatkové riziká,
c) *stanoví mieru rizika ohrozenia* utajovaných skutočností ako malú, strednú alebo veľkú.

Bezpečnostný plán ochrany objektu obsahuje:

a) umiestnenie a opis objektu, a to najmä opis hranice objektu, počtu vstupov, opis okolia objektu budov, prípadne počet budov alebo podlaží, ak sa objekt skladá z viacerých budov alebo z viacerých podlaží,
b) určenie kategórie a triedy chránených priestorov, ktoré sa v objekte nachádzajú, spolu s opisom činností, ktoré sa v nich budú vykonávať,
c) určenie hranice objektu a chráneného priestoru vrátane opisu jej umiestnenia, vstupov, hrúbky stien, rozmerov okien, výšky okien nad úrovňou terénu a podobne,
d) grafické zobrazenie objektu, hranice objektu, chráneného priestoru a hranice chráneného priestoru,
e) pre každý chránený priestor spracovanú tabuľku bodového ohodnotenia bezpečnostných opatrení podľa bezpečnostného štandardu.

Technická dokumentácia objektu obsahuje:

a) zoznam a špecifikáciu mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov určených na ochranu objektu a chráneného priestoru,
b) pravidlá a pokyny na používanie mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov, návody na ich obsluhu a údržbu, plány kontroly, údržby a overovania funkčnosti, záznamy z vykonaných kontrol mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov; kontrola funkčnosti mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov sa vykonáva najmenej raz ročne, ak táto vyhláška neustanovuje inak,
c) kópie certifikátov mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov,
d) záznamy o overení funkčnosti mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov používaných užívateľmi po uplynutí doby platnosti certifikátu,
e) správy z technických bezpečnostných prehliadok.

Prevádzkový poriadok objektu obsahuje **režimové opatrenia** uvedené v § 10 Režimové opatrenia, ods. 1 písm. a) až i) Vyhlášky NBÚ č. 336/2004 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti a spôsob kontroly ich dodržiavania.

Režimové opatrenia sú opatrenia:

a) určujúce podmienky vstupu osôb a vjazdu dopravných prostriedkov do objektu a chráneného priestoru a podmienky výstupu osôb a výjazdu dopravných prostriedkov z objektu a chráneného priestoru,
b) určujúce podmienky pohybu osôb, dopravných prostriedkov v objekte a v chránenom priestore, a to v pracovnom čase a mimopracovnom čase,
c) určujúce podmienky používania mobilných telefónov, videokamier, fotoaparátov, audiozáznamových zariadení a podobne,
d) určujúce podmienky ochrany priestorov, kde sa utajované skutočnosti spracovávajú, rozmnožujú a ničia,
e) určujúce podmienky a spôsob kontroly objektu a chráneného priestoru po opustení pracoviska zamestnancami, ktoré zabezpečia, že nedôjde k neoprávnenej manipulácii s utajovanými skutočnosťami,
f) na ochranu rokovacích miestností,
g) určujúce podmienky používania, prideľovania, označovania, úschovy a evidencie originálov a kópií bezpečnostných kľúčov a médií do zámkov a uzamykateľných systémov,
h) určujúce podmienky používania, prideľovania, označovania, úschovy a evidencie kódových nastavení a hesiel používaných na prístup do objektov, chránených priestorov a bezpečnostných úschovných objektov,

i) určujúce podmienky manipulácie s mechanickými zábrannými prostriedkami a technickými zabezpečovacími prostriedkami a podmienky ich používania,
j) spôsob kontroly dodržiavania uvedených opatrení.

Krízový plán ochrany objektu obsahuje režimové opatrenia uvedené v § 10 ods. 1 písm. j) a k):

- určujúce postup pri narušení objektu a chráneného priestoru alebo pri pokuse o narušenie objektu a chráneného priestoru,
- určujúce postup v prípade vzniku mimoriadnej situácie, ktorých súčasťou je aj **plán na ochranu, evakuáciu alebo zničenie utajovaných skutočností** spolu s uvedením zodpovedných osôb,
- spôsob kontroly dodržiavania uvedených opatrení.

Kniha návštev chráneného priestoru obsahuje meno, priezvisko, titul a číslo občianskeho preukazu alebo iného platného dokladu na preukazovanie totožnosti.

Bezpečnostná dokumentácia sa spracuje tak, aby bola jasná, stručná, prehľadná a výstižná. Ukladá sa u vedúceho alebo ním poverenej osoby. Vedúci zodpovedá za zhodu dokumentácie so skutočným stavom a za oboznámenie zamestnancov v rozsahu nutnom na výkon ich povinností alebo úloh najmenej raz za rok. Aktualizácia bezpečnostnej dokumentácie sa vykonáva po každej zmene majúcej vplyv na jej obsah. O každej zmene v bezpečnostnej dokumentácii sa vykoná záznam v knihe kontrol a oboznámia sa s ňou zamestnanci v súlade s potrebou oboznámenia sa na výkon svojich povinností alebo úloh.

Aktuálnosť bezpečnostnej dokumentácie sa kontroluje najmenej raz za:
a) dva roky pre chránené priestory kategórie Vyhradené a Dôverné,
b) rok pre chránené priestory kategórie Tajné a Prísne tajné.

12.6.4 Právne normy fyzickej bezpečnosti a objektovej bezpečnosti

Právne predpisy

- Zákon NR SR č. 215/2004 Z. z. o ochrane utajovaných skutočností v znení neskorších predpisov,
- Vyhláška NBÚ č. 336/2004 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti v platnom znení,
- Príloha k vyhláške NBÚ č. 336/2004 Z. z. Bezpečnostný štandard fyzickej bezpečnosti a objektovej bezpečnosti,
- Vyhláška NBÚ č. 337/2004 Z. z., ktorou sa upravujú podrobnosti o certifikácii mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov a o ich používaní v znení neskorších predpisov,
- Zákon č.473/2005 Z. z. o poskytovaní služieb v oblasti súkromnej bezpečnosti a o zmene a doplnení niektorých zákonov (zákon o súkromnej bezpečnosti).

LITERATÚRA

GYMERSKÁ, J. [2003]: *Mechanické prostriedky a systémy technickej ochrany objektov,* APZ, Bratislava, 2003.

LOVEČEK, T. – REITŠPÍS, J. [2011]: *Projektovanie a hodnotenie systémov ochrany objektov- ŽU v Žiline,* Žilina: FŠI ŽU, 2011 ISBN 978-80-554-0457-8.

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. Fakulta špeciálneho inžinierstva, ŽU Žilina.

MACH, V. [2010]: *Mechanické zábranné prostriedky*. Žilina: EDIS – vydavateľstvo ŽU. ISBN 978-80-970410-6-9.

ZÁBOJNÍKOVÁ, I. – VIDRIKOVÁ, D. [2010]: *Ochrana objektu, bezpečnostný projekt vybranej firmy.* Žilina: EDIS – vydavateľstvo ŽU.

13 ENVIRONMENTÁLNA BEZPEČNOSŤ

Bezpečnosť životného prostredia sa zameriava na ochranu pred poškodením životného prostredia, ako je neoprávnené nakladanie s odpadmi, neoprávnenie vypúšťanie znečisťujúcich látok, porušovanie ochrany vôd a ovzdušia, rastlín a živočíchov, stromov a krov, šírenie nákazlivej choroby zvierat a rastlín, pytliactvo a pod.

Vzťah medzi životným prostredím a bezpečnosťou ľudí a prírody bol predmetom mnohých výskumov a predmetom mnohých publikácií v posledných desaťročiach, ale iba v poslednej dobe sa stáva významným predmetom záujmu medzinárodnej politiky v oblasti životného prostredia. Životné prostredie je najdôležitejším nadnárodným problémom a jeho bezpečnosť je dôležitým aspektom mieru, národnej bezpečnosti a ľudských práv.

Environmentálna bezpečnosť je základom bezpečnosti štátu, zahŕňa dynamiku a prepojenie medzi základňou prírodných zdrojov, spoločenskou štruktúrou štátu a je ekonomickým nástrojom pre miestnu a regionálnu stabilitu. Ľudstvo v značnej miere zanedbáva zachovanie ekosystémov podporujúcich tvorbu vody, potravín, liekov a čistého vzduchu pre súčasné a budúce generácie, ktoré budú konfrontované so stále závažnejšími environmentálnymi zmenami.

Vzácnosť životného prostredia je daná zmenami životného prostredia, počtom obyvateľov a jeho nárastom a nerovnomerným rozdelením alebo prístupom k zdrojom. Objavujú sa nebezpečné príznaky, spojené so zmenami životného prostredia:

- vyčerpanie a znečistenie pitnej vody,
- vyčerpávanie rybolovu,
- degradácia a zmenšovanie biodiverzity,
- degradácia a zmenšovanie poľnohospodárskej pôdy a potravinovej a zdravotnej bezpečnosti,
- ochudobnenie ozónovej vrstvy a globálne otepľovanie.

Vo svete sa komplexným zhodnotením definícií environmentálnej bezpečnosti zaoberá The Millennium Project. The Millennium Project prebieha od roku 1996 pod patronátom Americkej rady pre Univerzitu OSN – American Council for The United Nations University, ktorá celý projekt koordinuje v spolupráci so Smithsonian Institution vo Washingtone a The Futures Group International. Prípravné práce projektu začali už v roku 1992. Zatiaľ najkomplexnejšie hodnotenie životného prostredia na Zemi bolo výsledkom projektu Millennium Ecosystem Assessment (*Hodnotenie ekosystémov na prelome tisícročí)*.

Environmentálna bezpečnosť podľa The Millennium Project 2008 je:

1. ***relatívna bezpečnosť verejnosti*** pred environmentálnymi hrozbami zapríčinenými prírodnými alebo ľudskými procesmi, spôsobenými neznalosťou, nehodou, zlým riadením alebo návrhom riadenia a má pôvod vnútri alebo za štátnymi hranicami.
2. stav dynamiky životného prostredia ľudí, ktorý zahŕňa ***obnovenie poškodenia životného prostredia*** spôsobené vojenskými zásahmi, meliorániami nedostatočných zdrojov, environmentálnou degradáciou a biologickými hrozbami, ktoré môžu viesť k sociálnym nepokojom a konfliktom.
3. ***cyklus premeny prírodných zdrojov v produkty, odpad a prírodné zdroje*** spôsobmi, ktoré podporujú sociálnu stabilitu.
4. ***zachovanie fyzického životného prostredia*** spoločnosti pre jej potreby bez znižujúcej sa prirodzenej zásoby.
5. ***nezávislosť od sociálnej nestability***, ktorá vedie k environmentálnej degradácii.

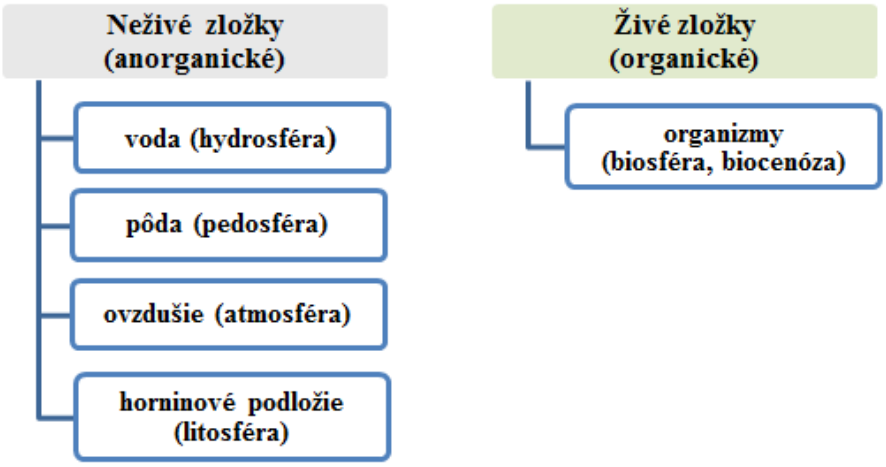
13.1 ŽIVOTNÉ PROSTREDIE

Životné prostredie alebo zriedkavo **environment** je všetko, čo vytvára prirodzené podmienky existencie organizmov vrátane človeka a je predpokladom ich ďalšieho vývoja. Je to súbor všetkých činiteľov, s ktorými prichádza do styku živý subjekt, a ktorými je obklopený, všetko, na čo subjekt priamo i nepriamo pôsobí.

Subjektom môže byť ***organizmus, populácia, človek i celá ľudská spoločnosť***. Väčšinou sa pojem *životné prostredie* chápe ako ***životné prostredie človeka.***

Zložkami životného prostredia sú najmä ***ovzdušie, voda, horniny, pôda, organizmy.*** Vo funkčnom ponímaní je životné prostredie súhrn materiálnych zložiek sveta, prírodných i umelo vytvorených, v ktorých a za pomoci ktorých si človek uspokojuje svoje materiálne a duchovné potreby, čím ich mení, pretvára a súčasne vytvára materiálne podmienky svojho ďalšieho života a života budúcich generácií. Životné prostredie je jednou z určujúcich zložiek kvality života spoločnosti.

Životné prostredie sa delí na zložky podľa obr. 28.



Obr. 28 Zložky životného prostredia

Bezpečnosť životného prostredia alebo **environmentálna bezpečnosť** *(Environmental Security)* predstavuje stav, v ktorom:

- ľudská spoločnosť a ekologický systém na seba pôsobia trvalo udržateľným spôsobom,
- jednotlivci majú dostatočný prístup ku všetkým prírodným zdrojom,
- existujú mechanizmy na zvládanie kríz a konfliktov priamo či nepriamo spojených so životným prostredím.

V tomto stave sú minimalizované riziká a ohrozenia spojené so životným prostredím a spôsobené prírodnými alebo antropologickými silami, alebo procesmi vyvolanými antropologickými silami. Pre oblasť týkajúcu sa environmentálnej bezpečnosti sú prioritné právne nástroje, ktorými sú národné či nadnárodné zákony a predpisy, týkajúce sa ochrany životného prostredia. V podmienkach SR sú to napríklad:

- Zákon č. 17/1992 Zb. o životnom prostredí,
- Zákon č. 525/2003 Z. z. o štátnej správe starostlivosti o životné prostredie,
- Zákon č. 205/2004 Z. z. o zhromažďovaní, uchovávaní a šírení informácií o životnom prostredí,

- Vyhláška MŽP SR č. 448/2010 Z. z. ktorou sa vykonáva zákon č. 205/2004 Z. z. v znení neskorších predpisov,
- Zákon č. 587/2004 Z. z. o Environmentálnom fonde,
- Zákon č. 245/2003 Z. z. o integrovanej prevencii a kontrole znečisťovania životného prostredia,
- Zákon č. 24/2006 Z. z. o posudzovaní vplyvov na životné prostredie.

Ochrana životného prostredia

Ochrana životného prostredia predstavuje podľa Zákona o životnom prostredí ***činnosti, ktorými sa predchádza znečisťovaniu alebo poškodzovaniu životného prostredia alebo sa toto znečisťovanie alebo poškodzovanie obmedzuje a odstraňuje.***

Zahŕňa ochranu jeho jednotlivých zložiek alebo konkrétnych ekosystémov a ich vzájomných väzieb, ale aj ochranu životného prostredia ako celku. Termín sa často nesprávne zamieňa s termínmi ekológia a ochrana prírody.

Ochrana životného prostredia je systematická a vedecky podložená ľudská činnosť, ktorá zahŕňa ochranu okolitého prostredia nutného na uspokojivý život všetkých organizmov na Zemi, vrátane človeka. Znamená starostlivosť o celý rad prírodných zdrojov – rastliny, živočíchy, vzduch, vodu i pôdu, zahŕňa činnosti, ktorými sa predchádza znečisťovaniu alebo ohrozovaniu životného prostredia.

Ochrana životného prostredia sa delí na sektory:

a. všeobecnú ochranu prostredia – ochrana ovzdušia, pôdy, vody a pod.,
b. špeciálnu ochranu prírody – ochrana významných častí prírody, napr. rastlín, živočíchov, chránených území a pod.,
c. ochranu kultúrnych pamiatok – ochrana diel, ktoré majú historickú, kultúrnu a umeleckú hodnotu.

Ochrana vody

Ochranu vodných zdrojov je potrebné chápať ako integrovanú ochranu kvality a kvantity podzemných a povrchových vôd. Oba aspekty ochrany vôd sú premietnuté v tzv. územnej ochrane vôd.

Pri **ochrane kvality vodných zdrojov** je rozhodujúcim faktorom problematika zdrojov znečisťovania vôd, či už s priamym alebo nepriamym dopadom na vodné zdroje.

Pri **ochrane kvantity (množstva) vôd** sú dôležité zvyšovanie akumulačnej schopnosti krajiny a kontrola dodržiavania vypočítaných hodnôt pre odoberané množstvá vôd. Pre tento účel sa stanovujú limity využívania zásob podzemných vôd (ekologické limity), ako aj záväzné minimálne prietoky.

Ochranu vody riešia najmä:
- Zákon č. 364/2004 Z. z. o vodách a o zmene zákona SNR č. 372/1990 Zb. o priestupkoch v znení neskorších predpisov (vodný zákon),
- Nariadenie vlády SR č. 269/2010 Z. z. ktorým sa ustanovujú požiadavky na dosiahnutie dobrého stavu vôd.

Ochrana ovzdušia

Ochranu ovzdušia upravujú najmä normy:
- Zákon č. 137/2010 Z. z. o ovzduší,
- Vyhláška MŽP SR č. 410/2012 Z. z., ktorou sa vykonávajú niektoré ustanovenia zákona o ovzduší,

- Zákon č. 478/2002 Z. z. o ochrane ovzdušia a ktorým sa dopĺňa zákon č. 401/1998 Z. z. o poplatkoch za znečisťovanie ovzdušia v znení neskorších predpisov (Zákon o ovzduší) v znení neskorších predpisov.
- Vyhláška MŽP SR č. 705/2002 Z. z. o kvalite ovzdušia.
- Vyhláška MŽP SR č. 706/2002 Z. z. o zdrojoch znečisťovania, o emisných limitoch, o technických požiadavkách a všeobecných podmienkach prevádzkovania, o zozname znečisťujúcich látok, o kategorizácií zdrojov znečisťovania ovzdušia a o požiadavkách zabezpečenia rozptylu emisií znečisťujúcich látok.

Ochrana pôdy

Ochrana pôdy ako zložky životného prostredia nebola v rezorte životného prostredia osobitne právne ustanovená. Na ochranu pôdy sa uplatňuje najmä Zákon č. 220/2004 Z. z. o ochrane a využívaní poľnohospodárskej pôdy a o zmene zákona č. 245/2003 Z. z. o integrovanej prevencii a kontrole znečisťovania životného prostredia a o zmene a doplnení niektorých zákonov.

Tento zákon ustanovuje:
- ochranu vlastností a funkcií poľnohospodárskej pôdy a zabezpečenie jej trvalo udržateľného obhospodarovania a poľnohospodárskeho využívania,
- ochranu environmentálnych funkcií poľnohospodárskej pôdy, ktoré sú: *produkcia biomasy, filtrácia, neutralizácia a premena látok v prírode, udržiavanie ekologického a genetického potenciálu živých organizmov v prírode,*
- ochranu výmery poľnohospodárskej pôdy pred neoprávnenými zábermi na nepoľnohospodárske použitie, a to hlavne poľnohospodárskej pôdy zaradenej podľa kódu bonitovanej pôdno-ekologickej jednotky do 1. až 4. kvalitatívnej skupiny.

Špeciálna ochrana prírody

Ide o osobitnú ochranu druhov **rastlín, živočíchov, nerastov a skamenelín**, vrátane ich systematických jednotiek nižšieho radu. Ohrozené, zriedkavé, vzácne alebo inak významné druhy rastlín, živočíchov, nerastov a skamenelín môže MŽP vyhlásiť za chránené druhy v týchto kategóriách: ***chránené rastliny, chránené živočíchy, chránené nerasty, chránené skameneliny.***

Za chránené rastliny a živočíchy sa podľa tohto zákona považujú aj druhy chránené medzinárodnými dohovormi, ktorými je SR viazaná. Chránené rastliny a živočíchy sa podľa stupňa ich ohrozenia členia na: ohrozené, veľmi ohrozené, kriticky ohrozené. Špeciálnu ochranu prírody rieši najmä Zákon č. 543/2002 Z. z. o ochrane prírody a krajiny.

Kultúrne pamiatky

Kultúrne pamiatky sú výberovou skupinou hnuteľných a nehnuteľných vecí ako významných dokladov historického vývoja spoločnosti, jej spôsobu života a prostredia od najstarších dôb po súčasnosť. Sú prejavom tvorivej práce človeka v rôznych odboroch ľudskej činnosti, pre ich historické, umelecké, vedecké a iné hodnoty je potrebné chrániť ich ako kultúrne pamiatky a sú zapísané a evidované v Ústrednom zozname kultúrnych pamiatok SR.

Pod ochranou kultúrnej pamiatky sa rozumie súhrn činností a opatrení vykonávaných na predchádzanie jej ohrozeniu, poškodeniu, zničeniu alebo odcudzeniu, na trvalé udržiavanie dobrého stavu vrátane prostredia kultúrnej pamiatky a na taký spôsob využívania a prezentácie, ktorý zodpovedá jej pamiatkovej hodnote a technickému stavu.

Výkon špecializovanej štátnej správy na ochranu pamiatkového fondu zabezpečuje od roku 2002 Pamiatkový úrad SR (PÚ SR) a krajské PÚ. Medzi základné právne predpisy

usmerňujúce nakladanie s kultúrnymi pamiatkami je Zákon č. 49/2002 Z. z. o ochrane pamiatkového fondu, podľa ktorého sa okrem iného kultúrne pamiatky a národné kultúrne pamiatky zapísané v Ústrednom zozname kultúrnych pamiatok považujú za „národné kultúrne pamiatky“.

Znižovanie environmentálnych rizík

Pre znižovanie environmentálnych rizík by sa organizácia mala zamerať na:

- ochranu ovzdušia, klímy a ozónovej vrstvy,
- odpadové hospodárstvo,
- environmentálne záťaže,
- environmentálne hodnotenie a označovanie produktov,
- environmentálne manažérstvo a audit,
- chemické a fyzikálne faktory,
- ionizované žiarenie a jadrovú bezpečnosť,
- neionizujúce žiarenie a elektromagnetizmus,
- hluk a vibrácie,
- ochranu pred požiarmi a civilnú ochranu,
- protipovodňovú ochranu,
- bezpečnosť a ochranu pri práci, ochranu, podporu a rozvoj verejného zdravia.

Na ochranu životného prostredia sa v organizáciách vytvára **Environmentálny manažérsky systém – EMS.**

13.2 LITERATÚRA

BETUŠ, Ľ. [2014]: *Chráň náš svet, chráň svoj život, pomáhaj ohrozeným*. In: Civilná ochrana 2/2014. ISSN 1335-4094.

ČEREŠŇÁK, D a kol. [2013]: *Environmentálna zodpovednosť v podnikaní,* nakladateľstvo Verlag Dashöfer.

ČERMÁK, O. [2007]: *Životné prostredie. Vysokoškolská učebnica.* Bratislava, STU. ISBN: 978-80-2272-958-1.

JÚDOVÁ, J. – ŠALGOVIČOVÁ, D. – PAVLOVIČOVÁ, D. [2008]: *Environmentálny monitoring.* Žilina: Ústav vysokohorskej biológie Žilinskej univerzity. ISBN: 978-80-8892-317-6.

KOLLÁR, V. – BROKEŠ, P. [2005]: *Environmentálny manažment.* Bratislava: SPRINT, ISBN 80- 8908-537-7.

VIRČÍKOVÁ, E. – PALFY, P. [2007]: *Environmentálne manažérstvo – teória a metodika,* druhé vydanie. Košice. ISBN: 978-80-8928-219-7.

14 INÉ DRUHY BEZPEČNOSTI

14.1 EKONOMICKÁ BEZPEČNOSŤ

Ekonomickú bezpečnosť podniku je možné považovať za základ ekonomickej bezpečnosti štátu. Zdroje, ktoré využíva podnik pri vykonávaní svojej činnosti sú súčasne zdrojmi jeho ekonomickej bezpečnosti. Môžu mať hmotnú alebo nehmotnú formu *(Strelcová, 2012)*, patria k nim:

a) finančné hmotné zdroje,
b) naturálne hmotné zdroje,
c) nehmotné zdroje.

Finančné hmotné zdroje vznikajú vo vnútri podniku alebo ich podnik získava z vonkajšieho prostredia. Pre ekonomickú bezpečnosť je dôležité, aby podnik dokázal zabezpečiť dostatočné množstvo finančných zdrojov tak, aby bol schopný vykonávať podnikateľskú činnosť, uhrádzať svoje záväzky voči obchodným partnerom, bankám, poisťovniam, štátu a v prípade mimoriadnych udalostí dokázal zabezpečiť uvedenie podniku do pôvodného stavu.

Finančné hmotné zdroje tvoria:

a) vnútorné zdroje, ktoré podnik vytvára: zo zisku (samofinancovanie), odpisov, dlhodobých rezerv, prostriedkov uvoľnených zrýchleným obratom kapitálu,
b) vonkajšie zdroje, ktoré podnik získava:
- ***z vlastných zdrojov***, napr. rozšírením základného imania (akcie, podielové listy),
- ***z cudzích zdrojov***, napr. prostredníctvom rôznych druhov krátkodobých a dlhodobých úverov, emisiou obligácií, využitím lízingu, faktoringu, príp. finančných derivátov.

Naturálne hmotné zdroje predstavujú budovy, výrobné a iné zariadenia, dopravné prostriedky, pozemky a zásoby, inými slovami hmotné zložky dlhodobého a krátkodobého majetku, ktoré sú využívané v rámci podnikateľskej činnosti alebo zabezpečujú priestory pre jej vykonávanie. Z hľadiska ekonomickej bezpečnosti je dôležité, aby boli naturálne zdroje rozmiestňované v podniku tak, aby umožňovali dosiahnuť čo najväčšie úspory a aby ich využitie bolo čo najvyššie.

Nehmotné zdroje ekonomickej bezpečnosti podniku tvoria ľudské schopnosti, informácie, využívané technológie, patenty, licencie, know-how, ale aj povesť podniku. Z hľadiska ekonomickej bezpečnosti sa za najdôležitejšie nehmotné zdroje považujú ***ľudské schopnosti a informácie.***

Podnikový manažment musí stanoviť **optimálne množstvo a štruktúru pracovníkov**. Nekvalifikovaná pracovná sila môže totiž spôsobovať prestoje, zvyšovať množstvo reklamácií a zhoršenie povesti podniku. Rovnaký dopad môže mať aj malý počet pracovníkov, ktorí pracujú pod stresom a „chybujú“. Na druhej strane príliš veľký počet pracovníkov znižuje produktivitu práce. ***Riadenie ľudských zdrojov (personálnu prácu)*** je preto možné pokladať za jeden z najdôležitejších faktorov úspešnej existencie podniku a teda jeho ekonomickej bezpečnosti.

Informácie často predstavujú významnejšie aktívum podniku, preto je potrebné zabezpečiť ich ochranu počas celého životného cyklu informácie, tzn. od jej vzniku, cez spracovanie, uloženie, aktualizácie, prenos až po likvidáciu. Informácie môžu byť z oblasti pracovných postupov, obchodných kontraktov, personálnej agendy a pod. a reprezentujú dáta používané pri rozhodovaní. Môžu mať fyzickú (papierovú) alebo elektronickú podobu.

14.2 PREVENCIA ŠKÔD

Na prevenciu škôd a ochranu ekonomických aktív sa uskutočňujú tieto činnosti:

- predchádzanie podvodom *(Fraud Prevention),*
- vyšetrovanie podvodov *(Fraud Investigation),*
- vyšetrovanie krádeží identity*(Identity Theft Investigation),*
- ochrana kreditných kariet a vymáhanie pohľadávok *(Credit Cards and Account Receivable),*
- všeobecný prevod majetku dlžníka na veriteľov *(General Assignment).*

Predchádzanie a vyšetrovanie podvodov

Podvodné konanie zamestnancov a tretích osôb vystavuje každodenne väčšinu podnikov hrozbám finančných strát, poškodeniu reputácie, odchodu najlepších zamestnancov, súdnym sporom a najmä udržateľnosti ich podnikania. Neexistujúce alebo nedostatočné opatrenia a kontrolné mechanizmy môžu ovplyvniť schopnosť spoločnosti úspešne čeliť konkurencii a ohroziť jej postavenie na trhu. Podniky sa pred podvodmi chránia prevenciou, odhaľovaním a vyšetrovaním podvodných udalostí.

Organizácia ACFE *(The Association of Certified Fraud Examiners)* definuje podvod ako *„úžitok jedinca zameraný na osobné obohatenie sa pomocou zámerného zneužitia alebo použitia zdrojov alebo majetku zamestnávajúcej organizácie“.*

Na základe jednoduchých podmienok možno rozdeliť podvod do troch kategórií:

- základná sprenevera,
- korupcia,
- falošné správy.

Najúčinnejším spôsobom, ako čeliť podvodom, je zamedziť ich vzniku. Zavedenie **Programu prevencie podvodom** *(Fraud Prevention)* by preto malo byť nevyhnutnou súčasťou podnikového riadenia. Organizácie sa tradične pozerajú na prevenciu a detekciu podvodov pomocou zavedenia interných kontrol formou ***interného*** alebo ***externého auditu***. Jednou z najúčinnejších metód ako odhaliť podvod v organizácii sú ***operatívne analýzy*** a neustále ***monitorovanie***.

Na vytvorenie účinnej obrannej stratégie zamedzujúcej podvodom treba najprv špecifikovať **riziká** vzniku podvodov v organizácii. Postup pri vyhodnocovaní rizika výskytu podvodov v organizácii možno rozdeliť na:

- identifikáciu a zmapovanie rizík výskytu podvodov,
- vyhodnotenie pravdepodobnosti výskytu a významnosť podvodov,
- posúdenie stávajúcich a návrh nových vnútorných kontrol, účinne odhaľujúcich možné riziká vzniku podvodov,
- zavedenie opatrení na modifikáciu podvodov na čo najmenšiu mieru.

Podľa vyhodnotených rizík a cieľov preventívneho programu sa vytvára súbor kontrolných mechanizmov, smerníc a firemných procesov s cieľom identifikovať a zamedziť podvodom.

Vyšetrovanie krádeží identity

Krádež identity nastáva, keď sa podvodníci snažia získať prístup k informáciám o totožnosti niekoho (meno, priezvisko, dátum narodenia, adresa) na spáchanie zneužitia totožnosti. Podvodné zneužitie totožnosti možno opísať ako použitie ukradnutého dokumentu s cieľom získať tovar alebo služby podvodom.

Podvodníci môžu používať údaje na:

- otvorenie bankového účtu,
- získanie kreditnej karty, pôžičky a dávky štátnej sociálnej podpory,
- objednávanie tovaru na iné meno,
- prevzatie existujúceho účtu,
- uzatvorenie zmluvy na mobilný telefón,
- získanie originálnych dokladov, ako sú pasy a vodičské preukazy.

Vymáhanie pohľadávok

Pri predaji tovaru je možné využívať ***platby v hotovosti*** alebo sa uplatňujú pohľadávky z obchodného styku. Najviditeľnejšie výhodou hotovosti pred pohľadávkami je, že hotovosť je likvidné aktívum, ktoré je možné použiť okamžite. Pre podnikanie s používaním pohľadávok je potrebné čakať, čo môže nejakú dobu trvať. Spoločný termín pre návrat pohľadávky je 30 dní.

Väčšie spoločnosti môžu mať ***úverových manažérov***, ktorí zisťujú, či firma alebo jednotlivec s pohľadávkami sú solventní. Väčšina firiem ponúka platobné karty ako možnosti pre kupujúcich, ktoré fungujú ako veľmi krátkodobé pohľadávky. Platby z kreditných kariet sú obvykle uložené v priebehu niekoľkých dní na bankový účet.

Základným faktom pre vymáhanie pohľadávok je, či sa vôbec pohľadávka dá vymôcť. Dôležitým faktom je to, v akom stave sa nachádza majetok dlžníka. Ak je jasné, že majetok má, vymáhanie môže byť úspešné, v opačnom prípade firma na vymáhanie pohľadávok zhodnotí situáciu ako negatívnu a vymáhanie nebude realizované. Existuje však možnosť monitorovania daných pohľadávok (dlžníkov a ich majetkové pomery). Na tomto základe sa zistí, či a kedy začať vymáhanie peňazí od dlžníka.

Všeobecný prevod majetku dlžníka na veriteľov

Všeobecný prevod majetku dlžníka na veriteľov znamená dobrovoľný prevod celého alebo väčšiny majetku dlžníka inej dôveryhodnej osobe, ktorá bude zhromažďovať všetky peniaze, ktoré dlžník dlhuje, predá majetok dlžníka, a použije peniaze na úhradu dlhov, pričom vráti prípadný prebytok dlžníkovi.

14.3 PROJEKTOVÁ BEZPEČNOSŤ

V každej organizácii neustále prebiehajú zmeny, uskutočňuje sa dynamický rozvoj v oblasti vedy, techniky, informatiky a iných odvetviach, čo predurčuje jej ďalšie smerovanie z hľadiska toho, čo chce v budúcnosti dosahovať. Na dosiahnutie želanej zmeny organizácie využívajú **projektovanie.**

Definícia projektu hovorí, že ide o činnosť, ktorá je jedinečná (unikátna) a obmedzená v čase. Tieto dve kľúčové charakteristiky odlišujú projekt od procesu. Ide o činnosť, ktorá nie je realizovaná opakovane pri dosiahnutí rovnakých výsledkov.

Projekt ovplyvňujú:

- ***čas,***
- ***zdroje (ľudské, materiálne, finančné),***
- ***požadované výstupy.***

Vo všetkých týchto parametroch však existujú aj **riziká,** ktoré zásadne ohrozujú činnosti v jednotlivých fázach projektového riadenia. Riziká projektovania sú špeciálnym druhom rizík, na ktorých často závisí úspech alebo neúspech vytvoreného projektu. Sú to situácie s negatívnym dopadom (škodou) na celkovú či čiastkovú úspešnosť projektu, čiastkové výsledky projektu alebo jeho jednotlivé udalosti. Bezpečnosť projektu znamená riadiť tieto riziká tak, aby sa v jednotlivých fázach projektovania ***nevyskytli neakceptovateľné alebo prípustné riziká.***

Najpodstatnejšie je, aby sa všetky riziká dokázali identifikovať. Ak sa podarí identifikovať všetky riziká spojené s projektom, je možné sa na ne pripraviť a vypracovať **Plán projektových rizík,** podľa ktorého tieto riziká možno odvrátiť alebo ich minimalizovať, prípadne minimalizovať ich následky.

14.3.1 Riziká projektu

Základné projektové riziká možno členiť spôsobmi:

1. Riziká, podľa situácií

- **komunikačné riziká** – ide o nedorozumenie, prílišnú alebo naopak nedostatočnú zainteresovanosť a iniciatívu pri spolupráci,
- **sociálne riziká** – pridelenie pracovníkov s nezodpovedajúcou kvalifikáciou, problémy so spoluprácou v tíme, ochrana proti lovcom mozgov, problémy s motiváciou pracovníkov,
- **technologické riziká** – chyby pri návrhu workflow, strata alebo poškodenie dokumentov a dát,
- **externé riziká** – ide o riziká, ktoré sa nedajú ovplyvniť, zmeny úrokových sadzieb, inflácie, cien na trhu práce pre kľúčových zamestnancov, postoj verejnosti voči IT, právne normy, daňové a politické zmeny,
- **interné riziká** – podnikové stratégie, zmeny likvidity, solventnosti a bonity.

2. Riziká vo vzťahu k projektu

a) Všeobecné projektové riziká:

- voľba nevhodných členov tímu,
- zlá komunikácia medzi členmi projektového tímu,
- nesprávne nastavené zodpovednosti a právomoci členov projektového tímu,
- nezáujem členov tímu na výsledku projektu,

- nedostatočná komunikácia s užívateľmi projektu, sponzorom; dlhé komunikačné reťazce,
- opomenutie informovať verejnosť (public relations),
- nedostatočná podpora zo strany sponzora projektu,
- absencia častejších osobných porád pracovných skupín,
- nerealistické termíny,
- neustále sa meniace požiadavky,
- nedodržanie rozpočtu,
- podcenenie fázy školenia užívateľov,
- veľký počet užívateľov alebo členov projektového tímu,
- náročné a nepremyslené väzby medzi systémami,
- nedostatočná skúsenosť ľudí pri projekte,
- nedostatočný dôraz na strategické ciele projektu,
- neprofesionálne postupy pri vývoji a nedostatky vo vývojovom prostredí,
- nedostatočné alebo neúplné testovanie.

b) Špecifické riziká pre daný projekt – existuje rad ďalších rizík, ktoré sa v predchádzajúcich projektoch nevyskytli a ani nemohli vyskytnúť, vzhľadom na jeho jedinečnosť a neopakovateľnosť v určitej sfére (súkromný sektor, verejný sektor, subjekt zaoberajúci sa výrobou, subjekt ponúkajúci služby) *(Doležal 2009)*.

Najzávažnejšie riziká, ktoré ovplyvňujú projekty, uvádzajú Thompson a Perry:

- neschopnosť držať sa odhadnutých nákladov,
- neschopnosť dosiahnuť požadované dátumy dokončenia,
- neschopnosť dosiahnuť požadovanú kvalitu a požiadavky na prevádzku (*Thompson, Perry,1992)*.

14.4 LITERATÚRA

DUFINEC, I. [2008]: *Bezpečnosť produktu ako aspekt jeho kvality.* In Zborník príspevkov 2.medzinárodnej vedeckej konferencie, Košice: VŠBM 2008, ISBN 978-80-8928-228-9.

DOLEŽAL, J. a kol. [2009]: *Projektový management podle IPMA.* Praha: Grada Publishing, 2009 - 512 s. ISBN 978-80-247-2848-3.

STRELCOVÁ, S. [2012]: *Ekonomické teórie. Úvod do riadenia rizika.* 1. vyd. Žilina: Žilinská univerzita v Žiline, 2012. ISBN 978-80-554-0541-4.

THOMPSON P. A. – PERRY J. G. [1992]: *Engineering construction risks.* London: Thomas Telford.

VŠETEČKA, P. – BELAN, L. [2006]: *Projektový manažment – I.* Liptovský Mikuláš: Akadémia ozbrojených síl. ISBN 978-80-8040-298-3.

15 ZÁVER

Bezpečnosť zohrávala a stále zohráva významnú rolu v spoločnosti i v prírode. Od jej prítomnosti alebo neprítomnosti závisel rozvoj alebo stagnácia, aj v spoločnosti, aj v prírode. Bezpečnosť bola pritom nepretržite v protiklade k nebezpečenstvu a z neho vyplývajúcich nebezpečných udalostí – ohrození.

Teoretické otázky bezpečnosti skúmalo množstvo výskumných pracovníkov, ktorí ju hodnotili najmä z hľadiska sociológie, ekonómie, práva, politológie, ekológie, vojenstva či technológií. Jej definície sa vyskytujú v množstve monografií, slovníkov, vedeckých a odborných článkov, zákonov, technických noriem a pod.

Podľa toho, ako je v definíciách vnímaná podstata a význam bezpečnosti, môžeme **jednotlivé prístupy k bezpečnosti** kategorizovať:

a) ***ako stav vo vzťahu k nebezpečenstvu, ohrozeniu a riziku,***

b) ***ako subjektívny pocit*** *– pri ktorom sa daný* ***objekt necíti byť ohrozený*** *z hľadiska svojich oprávnených záujmov,*

c) ***ako schopnosť objektu (subjektu) vytvárať aktivity na vlastnú ochranu,***

d) ***ako súhrn spoločenských vzťahov, ktoré upravujú právne normy*** na ochranu práv a oprávnených záujmov jednotlivcov, sociálnych skupín, organizácií, štátu a životného prostredia.

V problematike bezpečnosti je veľmi dôležité pochopiť množstvo rozporov, ktoré sú hybnou silou vývoja. Z bezpečnostného hľadiska pritom je hlavným rozporom bezpečnosť – nebezpečnosť. Práve z nebezpečenstva, ako schopnosti objektu spôsobiť negatívne udalosti, môžu prameniť rôzne incidenty, nehody, mimoriadne udalosti alebo krízové situácie a krízy, ktoré je potrebné riešiť čo najskôr.

Bezpečnosť sa až donedávna chápala najmä z hľadiska vojenského, ale najmä v posledných storočiach sa objavili nové, závažné riziká, ktoré podstatným spôsobom vplývajú na bezpečnosť osôb, majetku, životného prostredia, ale aj na bezpečnosť podnikania. Tieto nové riziká sa odvíjajú najmä od technického a technologického rozvoja, vzniku a presadzovania informačnej spoločnosti, rozširovania pracovných príležitostí a zásahov človeka do prírody.

Základné druhy bezpečnosti osôb a majetku sa, okrem BOZP a bezpečnosti objektov, rozširujú do nových oblastí, ako sú napr.:

- informačná bezpečnosť,
- bezpečnosť prevádzky (činností),
- bezpečnosť kritickej infraštruktúry,
- jadrová bezpečnosť,
- iné druhy bezpečnosti.

Prvý diel učebnice je preto okrem všeobecných otázok bezpečnosti zameraný aj na riešenie týchto nových oblastí bezpečnosti. Bezpečnosť je, okrem neprítomnosti alebo znižovania úrovne rizík na prijateľnú úroveň, závislá aj od schopnosti spoločnosti vytvárať podmienky na ochranu pred všetkými rizikami, ktoré ju môžu narušiť. Problematika posudzovania rizík a zaobchádzania s rizikami bude náplňou ďalšej časti učebnice pod názvom:

MANAŽÉRSTVO RIZIKA