BEZPEČNOSTNÝ MANAŽMENT

BEZPEČNOSŤ A MANAŽÉRSTVO RIZIKA

2. časť
MANAŽÉRSTVO RIZIKA

prof. Ing. Ľubomír Belan, CSc.

Vydala Žilinská univerzita v Žiline
2015
OBSAH

1 ÚVOD ............................................................................................................................... 5
2 BEZPEČNOSTNÉ PROSTREDIE .................................................................................... 7
  2.1 PROSTREDIE ORGANIZÁCIE .................................................................................. 8
  2.2 CHARakterISTIKA Bezpečnostného Prostredia ........................................................... 13
     2.2.1 Faktory bezpečnostného prostredia .................................................................. 14
     2.2.2 Definícia bezpečnostného prostredia ................................................................. 15
     2.2.3 Vonkajšie bezpečnostné prostredie ................................................................. 16
     2.2.4 Vnútorné bezpečnostné prostredie ................................................................. 18
  2.3 LITERATÚRA ........................................................................................................ 19
3 RIZIKO .......................................................................................................................... 20
  3.1 CHARakterISTIKA RIZIKA ...................................................................................... 23
     3.1.1 Definícia rizika ................................................................................................. 23
     3.1.2 Vztah rizika a neistoty ..................................................................................... 24
     3.1.3 Zdroj rizika ...................................................................................................... 26
     3.1.4 Udalosť .............................................................................................................. 27
     3.1.5 Následok a pravdepodobnosť ........................................................................... 29
  3.2 ÚROVNE RIZIKA ...................................................................................................... 30
  3.3 KATEGORIZÁCIA RIZÍK .......................................................................................... 34
  3.4 LITERATÚRA ........................................................................................................ 37
4 PODNIKATEĽSKÉ RIZIKÁ ........................................................................................... 38
  4.1 CHARakterISTIKA PODNIKATEĽSKÝCH RIZIKÁ ..................................................... 39
  4.2 LITERATÚRA ........................................................................................................ 43
5 BEZPEČNOSTNÉ RIZIKÁ ............................................................................................. 44
  5.1 NEBEZPEČENSTVO ............................................................................................... 45
  5.2 RIZIKÁ ÚMYSELNÉHO NAPADNUTIA ................................................................. 51
  5.3 NÁHODNÉ BEZPEČNOSTNÉ RIZIKÁ ................................................................. 55
     5.3.1 Riziká bezpečnosti zdravia pri práci ............................................................... 55
     5.3.2 Personálne riziká ............................................................................................ 59
     5.3.3 Environmentálne riziká ................................................................................... 59
     5.3.4 Riziká požiaru ................................................................................................. 61
     5.3.5 Riziká technických (technologických) havárií a katastrof .............................. 62
     5.3.6 Prirodné riziká .............................................................................................. 62
     5.3.7 Riziká bezpečnosti priestorov ....................................................................... 63
  5.4 LITERATÚRA ........................................................................................................ 65
6 MANAŽÉRSTVO RIZIKA ............................................................................................ 66
  6.1 USPORIADANIE MANAŽÉRSTVA RIZIKA ........................................................... 69
  6.2 ZÁSADY MANAŽÉRSTVA RIZIKA .......................................................................... 70
  6.3 LITERATÚRA ........................................................................................................ 70
7 ŠTRUKTÚRA MANAŽÉRSTVA RIZIKA ................................................................. 71
  7.1 NÁVRAH ŠTRUKTÚRY MANAŽÉRSTVA RIZIKA .................................................... 73
  7.2 LITERATÚRA ........................................................................................................ 77
8 PROCES MANAŽÉRSTVA RIZIKA .............................................................................. 78
  8.1 KOMUNIKÁCIA A PORADENSTVO ....................................................................... 79
  8.2 VÝTVÁRANIE SÚVISLOSTÍ ..................................................................................... 81
  8.3 DEFINOVANIE KRITÉRIÍ RIZIKA ........................................................................... 85
  8.4 POSUDZOVANIE RIZIKA ....................................................................................... 89
  8.5 IDENTIFIKÁCIA RIZIKA ........................................................................................ 91
     8.5.1 Metódy (techniky) identifikácie rizika ............................................................ 92
     8.5.2 Zoznam rizík .................................................................................................. 93
  8.6 ANALÝZA RIZIKA .................................................................................................... 96
     8.6.1 Metódy analýzy rizika .................................................................................... 97
     8.6.2 Analýza možnosti výskytu a odhad pravdepodobnosti .................................. 100
8.6.3 Analýza následků ................................................................. 101
8.7 HODNOTENÍ RIZIKA .............................................................. 104
8.8 LITERATÚRA ............................................................................. 107
9 ZAOBCHÁDZANÍ S RIZIKOM ..................................................... 108
  9.1 CHARAKTERISTIKA SPÔSOBOV ZAOBCHÁDZANIA S RIZIKOM ... 109
  9.2 VÝBER SPÔSOBOV ZAOBCHÁDZANIA S RIZIKOM ................. 114
  9.3 ĎALŠIE SÚČASTI PROCESU MANAŽÉRSTVA RIZIKA ................. 121
  9.4 LITERATÚRA ............................................................................. 125
10 ZÁVER ......................................................................................... 126

ZOZNAM OBRÁŽKOV

Obr. 1 Vzťah rizika k možným stratám a ziskom .................................................. 23
Obr. 2 Pojem rizika ......................................................................................... 24
Obr. 3 Typické parametre rizika ........................................................................ 29
Obr. 4 Pásma (oblasti) úrovne rizika podľa zásady ALARP ................................. 30
Obr. 5 Vonkajšie a vnútorné riziká organizácie .................................................. 38
Obr. 6 Vztahy medzi zásadami, štruktúrou a procesom manažérsťva rizika ........... 69
Obr. 7 Štruktúra manažérsťva rizika ................................................................. 71
Obr. 8 Proces manažérsťva rizika ...................................................................... 78
Obr. 9 Komunikácia a poradenstvo vo všetkých fázach manažérsťva rizika ........... 80
Obr. 10 Spôsoby zníženia úrovne rizika ............................................................. 110

ZOZNAM TABULIEK

Tab. 1 Spojitosť rizíko – nieistota ........................................................................ 25
Tab. 2 Zdroje rizika, udalosti a následky rizika .................................................. 28
Tab. 3 Úrovne rizika ......................................................................................... 32
Tab. 4 Riziká organizácie .................................................................................. 38
Tab. 5 Nebezpečenstvá a riziká v odvetviach a profesiách .................................. 58
Tab. 6 Prehľad významných aktív v objektoch organizácie (možný vzor) .......... 83
Tab. 7 Stupnica následkov (krok 1) .................................................................... 86
Tab. 8 Stupnica pravdepodobnosti (krok 1) ......................................................... 86
Tab. 9 Matica rizika (krok 2) ............................................................................ 87
Tab. 10 Kritériá rizika (krok 3) .......................................................................... 87
Tab. 11 Pravdepodobnosť výskytu ohrozenia alebo príležitosti ....................... 88
Tab. 12 Možný obsah Zoznamu rizík ................................................................ 95
Tab. 13 Možný vzor Zoznamu rizík .................................................................. 95
Tab. 14 Príklad analýzy rizika .......................................................................... 97
Tab. 15 Príklad určenia veľkosti rizík ............................................................... 99
Tab. 16 Obsah posudzovania rizík ................................................................... 107
Tab. 17 Možné opatrenia na zníženie pravdepodobnosti a následkov rizíka ....... 110
Tab. 18 Príklad na zaobchádzanie s rizíkom .................................................... 112
Tab. 19 Príklad výberu, spôsobu/ spôsobov zaobchádzania s rizíkom ............. 117
Tab. 20 Náklady a prínosy spôsobov zaobchádzania s rizíkom ....................... 117
Tab. 21 Charakteristika nákladov a prínosov .................................................... 118
Tab. 22 Použiteľnosť nástrojov pre posudzovanie rizík .................................... 137
POUŽITÉ SKRATKY

• ADR (Accord Européen au transport international des Marchandises par route) – Európska dohoda o medzinárodnej cestnej preprave nebezpečných vecí.
• ALARP (As Low As Reasonable Practicable) – Zásada znížovania úrovne rizika na tak nízke, ako je to možné.
• BCA (Benefit Cost Analysis) – Analýza prínosov a nákladov.
• BIA (Business Impact Analysis) – Analýza dopadov na podnikateľské činnosti – identifikuje skúma účinky prírodných alebo človekom spôsobených katastrof na kritické podnikové funkcie.
• BPEST analýza – Obchodná, politická, sociálna, technická analýza.
• BOZP – Bezpečnosť a ochrana zdravia pri práci.
• BZ – Chinulklidil benzilát, otrávna látka s psychotomimetickým účinkom, zlúčenina podobná atropínu, vyvoláva rôzne poruchy vyššej nervovej činnosti.
• CBA (Cost Benefit Analysis) – Analýza prínosov a nákladov.
• CEA (Cost-Effectiveness Analysis) – Analýza nákladovej efektívnosti.
• CS – Chlorbenzalmalondinitril, slzotvorová látka.
• ETA (Event Tree Analysis) – Analýza stromu udalostí.
• EÚ – Európska únia.
• FMEA (Failure Models and Effect Analysis) – Analýza príčin a následkov.
• FTA (Fault Tree Analysis) – Analýza stromom porúch.
• HAZOP (Hazard and Operability Studies) – Štúdia nebezpečenstva a prevádzkyschopnosti.
• HRA (Human Reliability Analysis) – Analýza spoľahlivosti ľudského činiteľa.
• IEC (International Electrotechnical Commission) – Medzinárodna elektrotechnická komisia na určovanie medzinárodných noriem a posudzovanie zhody, pre všetky elektrické, elektronické a súvisiace technológie.
• IKT – Informačné a komunikačné technológie.
• ISO (International Organization for Standardization) – Medzinárodná organizácia pre normalizáciu.
• ISO 31000:2009 (Risk management, Principles and guidelines) – Manažérstvo rizika, Zásady a návod.
• MCDA (Multiple-criteria decision analysis) – Analýza multidokritériálneho rozhodovania.
• NATO (North Atlantic Treaty Organization) – Organizácia Severoatlantickej zmluvy.
• NBÚ – Národný bezpečnostný úrad.
• NR SR – Národná rada Slovenskej republiky.
• PEST analýza – Analýza politicko-právneho, ekonomického, sociálno-kultúrneho a technologickeho prostredia.
• PESTLE analýza – Analytická technika určená na strategickú analýzu okolitého prostredia organizácie (politické, ekonomické, sociálne, technologicke, legislatívne, ekologické faktory).
• STEEP analýza – Analýza širšieho prostredia, zamieraná na sociálne, technické, ekonomické, ekologické a politické faktory, charakterizuje prostredie, ktoré determinuje spôsob metódy riadenia podnikateľských subjektov.
• STN – Slovenská technická norma.
• SWOT analýza – Analýza vnútorných silných a slabých stránok, príležitostí a hrozieb.
• VX látka – Nervovoparalytická, extrémne toxická látka.
1 ÚVOD

Každý referenčný objekt je umiestnený v určitom prostredí, ktoré z hľadiska bezpečnosti predstavuje vonkajšie bezpečnostné prostredie. Prostredie vo vnútri objektu z hľadiska bezpečnosti tvorí vnútorné bezpečnostné prostredie. V jednom i druhom bezpečnostnom prostredí je množstvo faktorov, ktoré na jednej strane môžu napomáhať tvorbe zisku, na druhej strane však môžu predstavovať nebezpečné udalosti, ktoré mohu podradná povyšovať dosiahnutie stanovených cieľov.

Organizácie rôznych typov a veľkostí sa stretávajú s rozličnými vonkajšími a vnútornými faktormi a vplyvmi, ktoré vytvárajú neistotu, či a kedy dosiahnu svoje ciele. Účinok, ktorý táto neistota má na zámer (ciele) organizácie, predstavuje riziko.

Manažérstvo rizika je jedným z najdôležitejších problémov, ktorým dnes organizácie čelia. Je dôležitou súčasťou každeho strategického riadenia organizácie. Je to proces, prostredníctvom ktorého sa organizácie venujú rizikám spojeným s činnosťami organizácie, s cieľom dosiahnuť trvalý prospech z každej jednotlivej a súhrnne zo všetkých činností organizačie. Umenie manažérstva rizika tkvie v identifikácii rizík špecifických pre danú organizáciu a ich zvládaní. Manažérstvo rizika by malo byť nepretržitým a stále sa zdokonaľujúcim procesom začleneným do stratégie organizácie a do jej presadzovania.


Slovo „riziko“ bolo často chápané iba negatívnym spôsobom, čo vôbec neumožňuje riešiť riziká podnikateľské, ktoré môžu okrem straty priniesť aj zisk, ktorý nie je vôbec závislý od ohrozenia ani zraniteľnosti. Práve pre rôzne chápanie rizika najmä v negatívnom zmysle bolo z dlhodobého hľadiska potrebné zaviesť určitú normu, ktorá by riešila aj pozitívnu aj negatívnu vlastnosť rizika.


Cieľom druhej časti učebnice Bezpečnostný manažment – Manažérstvo rizika je poznámať základné údaje o rizikách a ich zdrojoch, podnikateľských rizikách, bezpečnostných rizikách a manažérstve rizika. Štruktúra učebnice je zameraná na zodpovedanie nasledujúcich otázok:
• Pred KÝM a ČÍM chrániť referenčný objekt? – pred vonkajšími a vnútornými rizikami.
• AKO možno zvýšiť bezpečnosť referenčného objektu? – uplatňovaním manažérstva rizika.

Na základe uvedených otázok sa v jednotlivých kapitolách riešia problémy:
• bezpečnostné prostredie – prostredie referenčných objektov, vonkajšie a vnútorné bezpečnostné prostredie organizácie.
• **riziko** – charakteristika rizika, kategórie rizík, podnikateľské (špekulatívne) riziká, bezpečnostné riziká, nebezpečenstvo, riziká násilného napadnutia, náhodné riziká.

• **štruktúra manažérstva rizika** podľa STN ISO 31000 Manažérstvo rizika, zásady a návod – základné pojmy, návrh, zavedenie, monitorovanie a preskúmavanie, trvalé zdokonaľovanie manažérstva rizika.

• **proces manažérstva rizika** podľa STN ISO 31000 Manažérstvo rizika, zásady a návod – komunikácia, vytváranie súvislostí (bezpečnostná analýza vonkajšieho a vnútorného prostredia), určenie kritérií rizika, posudzovanie rizika (identifikácia, analýza, hodnotenie), zaobchádzanie s rizikom.

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 a na komerčné potreby, pretože v ucelenej podobe poskytuje informácie potrebné na manažérstvo všetkých druhov rizík.
2  

BEZPEČNOSTNÉ PROSTREDIE

Prostredie predstavuje v danom priestore súhrn podmienok, v ktorých niečo existuje, v ktorých sa niečo koná, situáciu, okolnosti, v ktorých niekoľko žije, niečo sa deje. Prostredie je podmienkou existencie každého referenčného objektu.

Prostredie môže byť:

a) vonkajšie prostredie, okolie, geografická oblasť okolo niečoho, v blízkosti niečoho,

b) vnútorné prostredie, vo vnútri niečoho.

Vonkajším (externým) prostredím referenčného objektu je to, čo ho obklopuje a môže ovplyvňovať, teda jeho okolie. Tento pojem označuje vonkajšie inštitúcie a sily, ktoré potenciálne ovplyvňujú jeho činnosti. Každý objekt či organizácia funguje, t. j. realizuje svoje poslanie, víziu a ciele v určitom prostredí, z ktorého čerpá zdroje fungovania života, z tohto vonkajšieho prostredia sú ovplyvňované množstvom rôznych prvkov, ktorým sa musí prispôsobiť.

Vnútorné (interné) prostredie referenčného objektu tvoria jeho vnútorné podmienky, v ktorých dochádza k transformácii zdrojov a v ktorých manažéri vykonávajú svoju riaditeľskú činnosť. Každý referenčný objekt je určitým prostredím pre fungovanie jeho jednotlivých prvkov. Vo vnútornom prostredí existujú a fungujú jednotlivé články, aj relatívne stabilné, formálne i neformálne väzby medzi nimi.

Zahŕňa každodenné pôsobenie komponentov (faktorov), ktoré sú súčasťou objektu alebo organizácie a ktoré ovplyvňujú manažérsku činnosť. Komponenty (faktory) interného prostredia sú dôležitými potenciálmi úspešného rozvoja, každý má svoje špecifiká, vývoj a navzájom sa ovplyvňujú. Na ich vývoj má stále význam vplyv i pôsobenie vonkajších faktorov.

Dynamika rôznych prvkov prostredia (označujeme ich za činitele, či faktory prostredia) vplyva na dlhodobé zámery, na podnikateľské procesy, bezpečnosť prevádzky, ako aj na bezpečnosť referenčného objektu. Hovoríme o dimenziách vplyvu prostredia, ktoré môžu mať rôzne prejavy (Mika, 2006):

1. faktory okolia sú v neustále, menia sa, ich vplyv na organizáciu sa nie je známa
2. okolie môže byť turbulentne, t. j. nestabilné, rozptylene, so vzájomnou prevádzkou
3. vzájomné vzťahy a spolupráca zvyšujú podmienky úspešného fungovania
4. členy tejto spoločnosti môžu navzájom sa podarovať
5. aj vnútorné prostredie podlieha zmenám – jeden vďaka vnútorným procesom (zlyhanie manažmentu, nedokonalost vnutorných procesov, poruchy a pod.), jednak pod vplyvom vonkajších faktorov (zmeny na trhu, zmeny v dostupnosti zdrojov, odchod kvalifikovanej pracovnej sily, dôsledky iných ekonomických, sociálnych či politických zmien a pod.),
6. v prostredí sú aj zdroje možných ohrození bezpečnosti – prirodzené katastrofy, kriminalita, sabotaže, teroristické činy, dôsledky vojny alebo havárie spôsobené technickou chybou, nedokonalostí materiálu alebo zlyhaním človeka.
2.1 PROSTREDIE ORGANIZÁCIE

Prostredie je podmienkou existencie každého objektu či organizácie, tvoria ho všetky vonkajšie a vnútorné faktory a podmienky, ktoré môžu organizáciu ovplyvňovať. Prostredie možno chápať vo viacerých rovinách.

Organizácia či objekt existujúci v neistom, stále sa meniacom prostredí, musí mať schopnosť prispôsobiť sa, alebo zmeniť sa v záujme dosiahnutia určitých cieľov. Prostredie môžno chápať vo viacerých rovinách.

Organizácia existujúca v neistom, stále sa meniacom prostredí musí mať schopnosť prispôsobiť sa, alebo zmeniť sa v záujme dosiahnutia určitých cieľov. Prostredie môžno chápať vo viacerých rovinách.

Prostredie objektu a organizácie možno deliť na (Míka, 2006):
1. Vonkajšie (externé) prostredie:
   a) globálne prostredie
   b) širšie vonkajšie prostredie – makroprostredie,
   c) bezprostredné (interakčné, odvetvové) vonkajšie prostredie – mezzoprostredie.
2. Vnútorné (interné) prostredie – mikroprostredie.

Globálne vonkajšie prostredie

V posledných rokoch stále intenzívnejšie prenikajú do prostredia objektov a organizácií faktory globálneho prostredia, so všetkými svojimi vplyvmi na jednotlivé faktory bezprostredného a širšieho externého prostredia. Globalizácia je jedným z hlavných faktorov, ktoré ovplyvňujú organizácie a manažment. Manažéri malých i veľkých organizácií sa stretávajú so stále väčším počtom globálnych konkurentov a spotrebiťských trhov.

Medzi najvýraznejšie prejavy a znaky globálneho prostredia, ktoré má vplyv na podnikanie, patria:
- internationalizácia (zahraničné príležitosti, konkurencia, rast spotrebiťských trhov, závislosť od zahraničných zdrojov), informatizácia, intelektualizácia, akcelerácia, humanizácia, ekologizácia, zvyšovanie nárokov na akosť produkcie, tlač na flexibilnosť organizácie a ďalšie.

Širšie vonkajšie prostredie – makroprostredie

Širšie vonkajšie prostredie je dané mnohými ďalšími faktorami, ktoré bezprostredne alebo odvetvové prenikajú do prostredia objektov a organizácií. Medzi najvýraznejšie prejavy a znaky globálneho prostredia, ktoré má vplyv na podnikanie, patria:
- internationalizácia (zahraničné príležitosti, konkurencia, rast spotrebiťských trhov, závislosť od zahraničných zdrojov), informatizácia, intelektualizácia, akcelerácia, humanizácia, ekologizácia, zvyšovanie nárokov na akosť produkcie, tlač na flexibilnosť organizácie a ďalšie.

Medzi najvýraznejšie prejavy a znaky globálneho prostredia, ktoré má vplyv na podnikanie, patria:
- internationalizácia (zahraničné príležitosti, konkurencia, rast spotrebiťských trhov, závislosť od zahraničných zdrojov), informatizácia, intelektualizácia, akcelerácia, humanizácia, ekologizácia, zvyšovanie nárokov na akosť produkcie, tlač na flexibilnosť organizácie a ďalšie.

Medzi najvýraznejšie prejavy a znaky globálneho prostredia, ktoré má vplyv na podnikanie, patria:
- internationalizácia (zahraničné príležitosti, konkurencia, rast spotrebiťských trhov, závislosť od zahraničných zdrojov), informatizácia, intelektualizácia, akcelerácia, humanizácia, ekologizácia, zvyšovanie nárokov na akosť produkcie, tlač na flexibilnosť organizácie a ďalšie.

Medzi najvýraznejšie prejavy a znaky globálneho prostredia, ktoré má vplyv na podnikanie, patria:
- internationalizácia (zahraničné príležitosti, konkurencia, rast spotrebiťských trhov, závislosť od zahraničných zdrojov), informatizácia, intelektualizácia, akcelerácia, humanizácia, ekologizácia, zvyšovanie nárokov na akosť produkcie, tlač na flexibilnosť organizácie a ďalšie.
Bezprostredné (interakčné) vonkajšie prostredie – mezzoprostredie

Bezprostredné vonkajšie prostredie sa skladá z takých faktorov, ktoré sú v bezprostrednom kontakte s organizáciou a ktoré majú priamy a bezprostredný vplyv na rozhodovanie manažérov a dosiahnutie cieľov organizácie. Niekedy sa uvádza aj ako podnikateľské prostredie alebo odvetvové prostredie.

Pôsobí priamo na všetky procesy v organizácii – správanie organizácie, jej zámery, stratégiu, dlhodobé i krátkodobé ciele, ovplyvňuje jej možnosti i príležitosti, pričom je treba akceptovať jeho premenlivosť, dynamickosť a v mnohých prípadoch aj nepredvidateľnosť. Ak organizácia podcení tieto faktory, dostane sa s nimi do konfliktu. Ak organizácia a interakčné prostredie nemajú rozporné záujmy, vzniknú pre organizáciu priaznivé podmienky na realizáciu vytýčených cieľov a záujmov.

Pre každú organizáciu je špecifické vonkajšie prostredie unikátne a mení sa v závislosti od podmienok. Pre podnik ho budú tvoriť: majitelia, dodávatelia, odberatelia, zákazníci, marketingoví sprostredkovatelia, distribútori, veritelia, spolupracujúce organizácie, konkurenčné organizácie, banky, daňové úrady, odborne zväzy, personálne agentúry, ľudské zdroje, verejnosť a pod.]

1. Dodávatelia – dodávajú organizácii potrebné zdroje (kapitál, energiu, stroje, zariadenia, služby, materiály) a ľudské zdroje, spoločnosti sa stále viac zameriavajú na výhradné zdroje (jeden dodávateľ). Problemy v dodávkach môžu ovplyvniť kontinuitu produkcie a následne ponuku na trhu, preto je potrebné sledovať ceny vstupov, pretože zvýšenie nákladov nákupu môže zapričiniť zvýšenie cien výrobkov, a tým ohroziť objem predaja firmy.

2. Odberatelia a zákazníci – zákazník prijíma výstupy organizácie, ktorá musí uspokojíť jeho potreby, zákazníci predstavujú pre organizáciu riziko, ich požiadavky a prijímanie musí organizácia uspokojovať, sledujú podmienné hodnoty vo vzťahu k cenám produktov, prístupnosti výrobkov a služieb vrátane servisu a v mnohých odvetviach je pre nich dôležité i meno a tradícia značky. Podnik môže rozdelenie trhov svojich zákazníkov do piatich skupín:
   a) trhy spotrebitel’ov – jednotlivci a domácnosti, ktorí nakupujú tovar a služby pre osobnú spotrebu,
   b) trhy výrobné sféry – organizácie, ktoré nakupujú produkty pre vlastný výrobný proces alebo na ďalšie spracovateľské účely,
   c) trhy sprostredkovateľov – organizácie, ktoré nakupujú produkty s cieľom ich opätovného predaja so ziskom,
   d) vládne trhy – vládne inštitúcie a orgány, ktoré nakupujú produkty na poskytovanie verejných služieb, alebo zabezpečujú prevod týchto produktov pre tých, ktorí ich potrebujú,
   e) medzinárodné trhy – zahraniční kupujúci, ku ktorým patria tak spotrebitelia a výrobcovia, ako aj sprostredkovatelia a vlády.

3. Marketingoví sprostredkovatelia – firmy, ktoré pomáhajú podniku pri predaji a distribúcii výrobkov cieľovým zákazníkom, pri výskume trhu a aktivitách promotion, pri finančných transakciách a poistení, patria sem: sprostredkovatelia, agentúry marketingových služieb a finančných sprostredkovatelia.

4. Distribútori – distribúcia ako jeden z hlavných marketingových nástrojov; súbor operácií, ktorými sa produkt z oblasti výroby odovzdáva k dispozícii spotrebitel’ovi, v správnom množstve, kvalite, cene, mieste a čase; uplatnenie tovaru na trhu.

5. Veritelia – veriteľ alebo kredítor je fyzická osoba alebo právnická osoba, voči ktoréj vykazuje dôlžnik peňažný záväzok, resp. ktorá mu poskytuje úver. V obchode je veriteľ najmä dodávateľ tovaru alebo služieb, pokým nie sú zaplatené. V čase od odoslania tovaru do je-
ho zaplatenia má platobná povinnosť odberateľov voči veriteľom (dodávateľom) charakter záväzkov a nárok veriteľov voči dôlníkom (odberateľom) charakter pohľadávok, ktoré sa takto vykazujú aj v súvahách.

6. Konkurencia – potreba prispôsobiť sa stratégií konkurentov, čiže uspokojiť želania zákazníkov lepšie, ako to robí konkurencia. Sú to rôzne firmy a organizácie, s ktorými organizácia súperi o zákazníkov a zdroje a voči ktorým organizácia potrebuje dosiahnuť konkurenčné výhody. Konzistentná konkurencia produktujú rovnaké alebo podobné produkty a služby, nekonzistentná sú odlišné a pritom sú konkurujúce organizácie, voči obom potrebuje organizácia dosahovať konkurenčné výhody. Konkurenti z hľadiska cien, nových produktov a ponúkaných služieb sú silou vonkajšieho prostredia, ktorých manažéri musia nielen sledovať a hodnotiť, ale byť i pripravení na ňu reagovať.


8. Personálna agentúra, ľudské zdroje.

9. Verejnosť – ľubovoľná skupina, ktorá prejavuje skutočný alebo potenciálny záujem o produkt alebo o firmu, možno ju rozdeliť do skupín:

   a) finančná verejnosť – ovplyvňuje možnosti získavania finančných zdrojov – banky, investičné spoločnosti a akcionári,
   b) mediálna verejnosť – noviny, časopisy, rozhlasové a televízne stanice, informujú o aktivitych firmy a môžu významne ovplyvniť verejnícť mienu o firme,
   c) verejnosť skladajúca sa z občianskych aktivít, akcii – skupiny angažujúce sa v spotrebiteľských službách, v spolochoch ochrany životného prostredia atď.,
   d) mestná verejnosť – obyvateľstvo bývajúce v územnej blízkosti, ako aj obecné úrady vytvárajú miestnú verejnosť,
   e) všeobecná verejnosť – imidž, predstava verejnosti o podniku, ovplyvňuje preferencie na nákup jeho výrobkov, marketingová komunikácia formou sponzoringu či ďalších akcií z oblasti public-relation napomáha formovaniu pozitívneho postoja verejnosti k podniku.

10. Odborové zväzy.


Vnútorné (interné) prostredie – mikroprostredie


Vnútorné prostredie organizácie tvoria faktory (Mika, 2006):

a) organizačná štruktúra:
   • systém riadenia (jednotlivé stupne manažmentu) a zamestnanci,
   • všetky organizačné útvary organizácie – manažment, finančné oddelenie, nákup, výroba a vývoj, marketing, oddelenie ľudských zdrojov, oddelenie evidencie atď. a vzťahy medzi nimi.

b) zdroje organizácie (hmotné a nehmotné aktiva organizácie):
   • ľudské – charakterizované počtom a štruktúrou (vekovou, profesijnou, kvalifikačnou a pod.) pracovníkov a ich produktitvou,
• **kapacitné** – vymedzené počtom a štruktúrou strojov a zariadení, stupňom fyzického i morálneho opotrebenia, výkonnosťou, časovým využitím a dosahovanou účinnosťou,
• **materiálové** – závislé od dostupnosti zdrojov, skladovacích priestorov, rýchlosti obratu zásob, efektivnosti využitia a dosahovanej účinnosti,
• **finančné** – z pohľadu štruktúry ziskania i štruktúry ich použitia, rýchlosti obratu a dosahovanej účinnosti,
• **informačné** – z hľadiska množstva a štruktúry disponibilných údajov, spôsobu spracovania, spoľahlivosti a hodnotnosti, rýchlosti ich prenosu, dostupnosti a účinnosti.

c) **hlavné činnosti organizácie** – výroba, služby, obstarávanie, skladovanie, financovanie, odbyt, doprava, marketing a iné dôležité činnosti, ktoré sú pre organizáciu nosné a ktoré prínosujú podnikateľským subjektom najvyššiu pridanú hodnotu.

d) **vedľajšie činnosti organizácie** – personalistika (riadenie ľudských zdrojov), investovanie, výskum a vývoj, všeobecná administratíva, správa majetku, logistika, riadenie prevádzky, údržba a servis objektov a technologických zariadení, verejné obstarávanie, energetické zabezpečenie, informatika a telekomunikácie, revízie a odborné prehliadky, havarijná služba, bezpečnosť (bezpečnosť a ochrana zdravia pri práci, ochrana životného prostredia, informačná bezpečnosť, bezpečnosť prevádzky a iné činnosti.

e) **infraštruktúra organizácie** – budovy, výrobné haly, dielne, sklady, garáže, iné priestory.

f) **zainteresované strany (stakeholderi)** – dodávatelia, odboratelia, akcionári, outsourcované služby, návštevníci atď.


g) **odhory** – inštitucionalizované združenia zamestnancov s cieľom presadzovať ich pracovné, hospodárske, sociálne, politické a iné záujmy.

h) **kultúra organizácie** (podniková kultúra) – jadro vnútorného prostredia, predstavuje systém spoločných hodnôt, názorov a presvedčení členov organizácie, ktoré sú v organizácii všeobecne uznávané a podľa ktorých sa správajú bežní pracovníci i manažéri. Spoločne uznávané hodnoty (shared value), symboly kultúry (vysoké a nízke), štruktúra vzťahov (formálne, neformálne), hlavná kultúra a subkultúry a pod., majú podstatný vplyv na úspech či neúspech rôznych podnikateľských zámerov, stratégií a zmien v organizácii.

**Kultúra organizácie**

Silné kultúry sú také, v ktorých sú kľúčové hodnoty hluboško zakorenene a všeobecne rešpektované, majú väčšiu záväznosť. Čím viac zamestnanci akceptujú kľúčové hodnoty organizácie, tým je kultúra silnejšia. Pôvodným zdrojom kultúry organizácie sú obvykle významné udalosti, symboly kultúry, jazyk, rituály a pod. Medzi najvýznamnejšie spôsoby prenosu kultúry organizácie na zamestnancov patria:

• **historické udalosti** (o zakladateľoch, o významných osobách a reakciách na chyby a pod.),
• **rituály** (opakované postupy pre aktivity, ktoré vyjadrujú a posilňujú hodnoty, ktoré platia v organizácii, jej najdôležitejšie ciele a ocenujú tie, ktoré sú pre organizáciu najdôležitejšie),
• **symboly** (usporiadanie zariadenia, oblečenie zamestnancov, používané automobily, lietadlá organizácie, nábytok, zdravotnícka starostlivosť, rekreačné zariadenia),
• **jazyk** (mnoho organizácií a oddelenia používajú svoj špecifický jazyk – skratky, slang atď.).
Komplexný obraz o kultúre organizácie poskytuje hodnotenie týchto siedmich dimenzí:

• orientácia na inovácie a prijímanie rizika – miera, v ktorej sú zamestnanci podnecovaní k inováciám a prijímaniu rizík,
• pozornosť venovaná detailom – miera, v ktorej by zamestnanci mali robiť detailné analýzy a venovať pozornosť podrobnostiam,
• orientácia na výsledky – miera, v ktorej sa manažéri zameriavajú viac na výsledky, než na postupy,
• orientácia na ľudí – miera ohľadu manažérov na zamestnancov pri rozhodovaní,
• orientácia na tímu – miera, v ktorej je práca viac organizovaná podľa tímov než podľa jednotlivcov,
• agresivita – miera, v ktorej sú zamestnanci viac než spolupracujúci agresívni a súťaživí,
• stabilita – miera, v ktorej sa rozhodnutia a činnosti robia pod zorným uhлом udržania súčasného stavu.
2.2 CHARAKTERISTIKA BEZPEČNOSTNÉHO PROSTREDIA

Bezpečnosť je jednou zo základných podmienok existencie a rozvoja akejkoľvek entity, preto je aj hlavnou zložkou problematiky prostredia referenčného objektu. Zaistenie bezpečnosti jednotlivca, skupiny, štátu, spoločnosti, organizácie, objektu je z tohto dôvodu dôležitou činnosťou každého subjektu.

Laml (2014) uvádza, že bezpečnosť existuje v rámci bezpečnostného prostredia, ktoré má dva rozmery:

a) **ontologický** – je daný samotnou existenciou prvkov, faktorov a vzťahov, ktoré vytvárajú bezpečnostného prostredie,

b) **epistemologický** – je vyjadrený poznateľnosťou prvkov, faktorov a vzťahov a ich samotným poznávaním, umožňuje pochopenie bezpečnostného prostredia v súvislostiach:

- v ktorých objektívne jestvujúcich vzťahoch, vplyvoch, javoch, udalostiach, procesoch a trendoch sa subjekt pohybuje, ktorými je formovaný a ovplyvňovaný, teda akési bezpečnostné prostredie „pre seba“;
- ktoré vzťahy, vplyvy, javy, udalosti, procesy a trendy vníma, respektíve je schopný vnímať ich, ako ovplyvňujúce a formujúce bezpečnostné prostredie;
- ako ich vníma, aký je záujem ich vnímať a aká je miera subjektívneho „vkladu“ do výsledného obrazu, ktorým je bezpečnostné prostredie „pre nás“.


V rámci tohto prístupu bezpečnostné prostredie ponímate štvordimenzionálne:

a) **geografická dimenzia:**
- má svoje vyjadrenie v geografickom členení bezpečnostného prostredia,
- geografické členenie bezpečnostného prostredia je najrozšírenejšie a vychádza z prírodzeneho geografického prístupu, napr. bezprostredné, blízke a vzdialené alebo vnútorné, regionálne, euroatlantické a globálne bezpečnostné prostredie.

b) **humanitná dimenzia:**
- je dimenzia tvorená existenciou človeka a jeho aktivitou,
- má sektorové členenie, ktoré je výrazom individuálnych špecifik jej prvkov,
- je obdobou holistického prístupu Kodanskej školy, kde namiesto klasického „úzkeho“ prístupu k bezpečnostným štúdiám založeným na vojensko-politickom pohľade ponúkajú „široký“ prístup k bezpečnosti v rámci komplexu piatich sektorov – vojenský, politický, ekonomický, environmentálny a sociálny.

c) **priestorová dimenzia:**
- vymedzuje priestorové limity pôsobenia jednotlivých prvkov bezpečnostného prostredia najmä vo vzťahu k hrozbám a priestorom možného konfliktu,
- v našom ponúkaní ide o pozemný, vodný, vzdušný a kozmický priestor, mikrosvet a kybernetický priestor,
- priestorová dimenzia umožňuje vyjadriť schopnosti jednotlivých bezpečnostných aktérov pôsobiť v danom priestore, využívať ho na realizácii svojich záujmov.

d) **časová dimenzia:**
• je prirodzeným vyjadrením dynamiky všetkých prebiehajúcich procesov v rámci bezpečnostného prostredia a čas je jedným z jeho rozhodujúcich prvkov,
• konkrétnym prejavom jeho významu je napríklad časové obdobie medzi inicializáciou negatívnej udalosti a jej prejavom, jej pôvodca môže časovú dimenziu využívať vo svoj prospech,
• druhým aspekt časovej dimenzie je časový horizont hodnotenia bezpečnostného prostredia, najčastejšie používané časové horizonty – krátkodobý, strednodobý a dlhodobý nemajú jednoznačne ponímaniu dĺžku svojich trvania,
• v rámci NATO bývajú používané termíny krátkodobý 0 – 2 roky, strednodobý 2 – 5 rokov a dlhodobý 5 – 10 rokov.

Bezpečnostné prostredie je potrebné vnímať ako komplexný systém, v jeho štrukturovanej a diferencovanej totalite jednotlivých prvkov a nimi tvorených dimenzií. Znamená to, že všetky prvky majú určitý význam a je potrebné zohľadňovať ich individuálny význam a osobitosti.

2.2.1 Faktory bezpečnostného prostredia

Bezpečnostné prostredie je súbor vnútorných a vonkajších faktorov referenčného objektu ovplyvňujúcich jeho bezpečnostnú politíku. Je ním možné rozumieť priestor nachádzajúci sa vo vnútri i mimo nieho, v ktorom sa realizujú a stretávajú jeho záujmy so záujmami iných aktérov a kde sa odohrávajú procesy, ktoré majú významný vplyv na úroveň bezpečnosti. Bezpečnostné prostredie SR tvoria nasledujúce faktory:

Geografický faktor bezpečnostného prostredia SR

Vzhľadom na rozlohu patrí Slovensko k menším krajínám Európy (49 036 km²). Patrí ku krajínám, ktoré nemajú priamý prístup k moriam, v porovnaní s Európou SR možno charakterizovať ako krajinu s vyššou nadmorskou výškou a značne zvlneným povrchom. SR je závislá od surovinových zdrojov (predovšetkým ropa, zemný plyn, farebné kovy, obmedzené zásoby železnej rudy, nízke zásoby čierneho uhlia). Na posudzovanie bezpečnosti majú vplyv niektoré vodné diela (Gabčíkovo, Oravská priehrada, Liptovská Mara, Domaša, Šírava).

Ekologický faktor bezpečnostného prostredia SR

V SR sa registruje nežiaducí stav z hládiska zhoršovania životného prostredia, čo je dôsledkom predovšetkým:
• rozsiahleho priebežného znečisťovania zložiek prírody,
• dlhodobej nešetrnej exploatácie prírodných zdrojov,
• nešetrných zásahov do ekosystémov krajiny.

Sociálny faktor bezpečnostného prostredia SR

a) Štruktúra obyvateľstva SR:
• kvantitávitvne faktory – počet obyvateľov, pôrodnosť, úmrtnosť, veková štruktúra a pod., vo vekovej štruktúre obyvateľstva pokračuje proces starnutia.
• kvalitatívne faktory – národnosť štruktúra, religiózná štruktúra,

b) Sociálna diferenciácia obyvateľstva SR – hlavnými kritériami rozlišení jednotlivcov v systéme sociálnej stratifikácie (rozvrstvenia) sú:
• pozícia človeka na trhu práce – zamestnávateľa, zamestnanci, samozamestnávateľa, lúdia mimo trhu práce.
• pozícia človeka v zamestnaní – sociálny status, moc, plat, prestíž, istota zamestnania.
• sociálna pozícia človeka – zohľadňuje majetok človeka a jeho rodiny, trhové, pracovné a iné postavenie členov rodiny, rozsah a kvalitá sociálnych sietí, v ktorých fungujú,
vzdelenie, kultúrna úroveň, spôsob života, súčasný systém sociálnej stratifikácie spoločnosti je tvorený triedami, resp. sociálnymi vrstvami.

c) Regionálna diferenciácia obyvateľstva – najhoršia situácia je vo východných a južných okresoch, kde je priemerná miera nezamestnanosti dlhodobo vysoká, najnižšia nezamestnanosť je v západnej časti SR. Problémom Slovenska je aj chudoba.

2.2.2 Definícia bezpečnostného prostredia


Predovšetkým z vojensko-politického hľadiska charakteristiky bezpečnostného prostredia je potrebné zvýrazniť jeho tri prvky:

• geografická charakteristika, ktorá je okrem polohy spojená aj s ďalšími najmä sociálno-ekonomickými a politickými charakteristikami a zvykne sa spájať aj s geopolitikou, geostratégiou a pod.,
• bezpečnostný aktéri – subjekty, ktoré sa v ňom nachádzajú a pôsobia a majú rôzne zámer, záujmy, vzťahy, vykonávajú rôzne činnosti,
• existencia a pôsobenie hrozieb – ďalšie podmienky a činiteľy (faktory), ktoré rozličným spôsobom priamo i nepriamo ovplyvňujú stav bezpečnosti.

Bezpečnostné prostredie sa spravidla vymedzuje ako „určitá úroveň bezpečnostnej situácie na uvedenom teritóriu, ktorá je výsledkom uskutočňovania bezpečnostnej politiky štátov a ich koalícií na tomto teritóriu“.

Z hľadiska geografického a geopolitického rozsahu je definované bezpečnostné prostredie:

• globálne (celosvetové),
• európske (euroatlantické),
• regionálne (stredoeurópske),
• vnútroštátne.


Vo vnútornom i vonkajšom prostredí referenčného objektu sa vyskytuje množstvo rizikových prvkov, ktoré na jednej strane môžu vytvárať príležitosť na zvýšenie zisku, ale na druhej strane predstavujú nebezpečenstvá zamerané na jeho aktíva, výsledkom ktorých sú vždy negatívne udalosti, ktoré spôsobujú škody. Pre definovanie bezpečnostného prostredia je potom rozhodujúce:

• definovanie aktív, resp. chráneného záujmu (KOHO alebo ČO chrániť),
• systematické hodnotenie bezpečnostného prostredia a z neho vyplývajúcich bezpečnostných rizík, tzn. identifikovanie KÝM a ČÍM môže byť narušená bezpečnosť.

Riziká referenčného objektu je možné vnímať z dvoch hľadísk:

a) ako riziká spojené s existenciou vonkajšieho prostredia, ako sú:
ekonomické vplyvy, napr. strata zákazníkov, zosilňujúci vplyv konkurencie, nepredvídateľný rast cien energie, možnosť získu a pod.,
• ohrozenie bezpečnosti, napr. prirodznými katastrofami, terorizmom, vojnami a pod.,
• riziko vyplývajúce z nedostatočnej pripravenosti, napr. chybajúce alebo málo účinné opatrenia na zníženie zraniteľnosti, nedostatočné opatrenia na vylúčenie či obmedzenie vplyvu nepriaznivých udalostí, a pod.

b) ako riziko spojené s vlastnou činnosťou, ako následok:
• nebezpečnej (rizikovej) činnosti, napr. dopravné nehody a katastrofy, technologické havárie, únik nebezpečných látok, poškodzovanie životného prostredia a pod.,
• chybných rozhodnutí,
• následok nečinnosti v situácii, keď bolo treba konať.

Štruktúra bezpečnostného prostredia bude vždy závislá od charakteru a štruktúry referenčného objektu. Čím väčšia a zložitejšia bude štruktúra referenčného objektu, tým aj geografické hranice i štruktúra prostredia budú rozsiahlejšie, napr. bezpečnostné prostredie samostatného objektu bude mať iný charakter a dosah, ako bezpečnostné prostredie organizácie (podniku, obce, mesta a pod.) alebo ako bezpečnostné prostredie okresu, kraja, štátu (Hofreiter, 2013).

Vo výkladovom slovníku terminológie bezpečnostného manažmentu sa bezpečnostné prostredie rozdeľuje na:
a) Vonkajšie (externé) bezpečnostné prostredie – zahŕňajúce okolie referenčného objektu, konkrétnu lokalitu, mesto a jeho štvrte, obec a pod.
b) Vnútorné (interné) bezpečnostné prostredie – vymedzené sociálnymi a fyzikálnymi činiteľmi vzťahujúcimi sa k referenčnému objektu, ktorý má byť chránený.

2.2.3 Vonkajšie bezpečnostné prostredie
Vonkajšie bezpečnostné prostredie možno považovať za priestor, nachádzajúci sa zvonka hraníc referenčných objektov, v ktorom sa vyskytujú činitele, odohrávajú sa procesy, ktoré majú rozhodujúci vplyv na úroveň bezpečnosti daného referenčného objektu. Do vonkajšieho bezpečnostného prostredia možno zahrnúť (Hofreiter, 2013):
1. Vzdialené vonkajšie bezpečnostné prostredie.
2. Blížšie (interakčné) vonkajšie bezpečnostné prostredie.

Vzdialené vonkajšie bezpečnostné prostredie
Vzdialené vonkajšie bezpečnostné prostredie, niekedy aj vonkajšie bezpečnostné makro prostredie, predstavuje bližšie neohraničený priestor, v ktorom existujú alebo sa môžu vyskytovať činitele s významným vplyvom na plnenie funkcií a existenciu referenčného objektu.

Z hľadiska štátu ho tvoria: svetové teritórium, európsky kontinent, stredná Európa, okolité štáty a charakterizujú ho najmä faktory globalizácie, ktoré môžu ohrozit' bezpečnosť objektov a chránených priestorov, najmä:
• nekontrolovaná migrácia,
• šírenie organizovaného zločinu a drog,
• šírenie jadrových zbranej,
• narastanie nacionalizmu a extrémizmu, náboženské a rasové nepokoje,
• zvyšujúca sa agresivita medzinárodného terorizmu,
• hrubé porušovanie medzinárodných bezpečnostných noriem.
Z hlášiska vnútroštátneho referenčného objektu má vzdialené vonkajšie bezpečnostné prostredie nepriamy vplyv na bezpečnosť, ovplyvňuje klimu, v ktorej referenčný objekt pôsobí a môže sa za určitých okolností zmeniť na priamy vplyv, naprí.:  
- ekonomické podmienky, politicko-právne podmienky, sociálno-kultúrne podmienky, geografické a demografické podmienky, technologické podmienky a pod.,  
- okruh pôsobnosti orgánov štátu a ním riadených bezpečnostných organizácií a služieb, za účelom zaistenia bezpečnosti občanov, bezpečnosti zariadení a pod.

**Bližšie (interakčné) vonkajšie bezpečnostné prostredie**

Bližšie (interakčné) vonkajšie bezpečnostné prostredie, niekedy aj vonkajšie bezpečnostné mikroprostredie, predstavuje bezprostredné prostredie, v ktorom existuje bezprostredná interakcia medzi referenčným objektom a okolím, tzn. že sa vzájomne ovplyvňujú alebo sa môžu ovplyvňovať.

Podľa Hofreitera pod pojmom lokálne prostredie rozumie súbor materiálnych, sociálnych, ekonomických, duchovných a politických činiteľov, ktoré ovplyvňujú existenciu podmienok bytia, utvárania a činnosti referenčných objektov – jedincov a sociálnych skupín v geograficky relatívne malom prostredí.


**Bližšie vonkajšie bezpečnostné prostredie** má nasledujúce charakteristiky:

1. **Urbanistická charakteristika:**
   - urbanistické hodnotenie – veľkosť a osídlenie sídla, v ktorom je objekt dislokovaný, obec, mesto, sídlisko, hustota osídlenia, typ okolitej zástavby a pod.,
   - charakteristika okolia objektu, ktoré môžu mať vplyv na systém ochrany objektu (okolitý terén, členitosť a morfológia územia, prístupové komunikácie, prírodné prekážky) a pod.,
   - dopravná vybavenosť.

2. **Sociálno-ekonomická charakteristika:**
   - štruktúra obyvateľstva,
   - sociálna diferenciácia obyvateľstva,
   - regionálna diferenciácia obyvateľstva: nezamestnanosť chudoba, hmotná núdza.

3. **Kriminalistická bezpečnostná charakteristika:**
   - kvantitatívne a kvalitatívne ukazovatele kriminality v posudzovanom prostredí a jeho okoli (fénomenológia a etiológia kriminality),
   - stav na úseku ochrany majetku a objektov, predovšetkým prírodné a hydrologické podmienky v danom prostredí, početnosť, rozsah a závažnosť živelných pohróm, ktoré by mohli ohroziť alebo ohrozili objekt, klíma a pod.

4. **Ekologické charakteristiky:**
   - znečisťovanie zložiek prírody, nešetrná exploatácia prírodných zdrojov, nešetrné zásahy do ekosystémov krajiny, ohrozené vodné toky a lesy, nepriaznivé zaobchádzanie s odpadom atď.

5. **Zdroje ohrozenia:** stabilné i mobilné zdroje priemyselných havárií, priehrady, vodné nádrže, vodné toky, sopky, sklady nebezpečných látok atď. v danom prostredí, ktoré by mohli ohroziť objekt a chránený priestor,
2.2.4 Vnútorné bezpečnostné prostredie

Vnútorné bezpečnostné prostredie možno považovať za priestor, ktorý sa nachádza vo vnútri hraníc referenčných objektov, v ktorom sa vyskytujú činitele, odohrávajú sa procesy, ktoré majú alebo môžu mať rozhodujúci vplyv na úroveň bezpečnosti daného referenčného objektu. Tvorí ho množina samostatných prvkov v hraniciach referenčného objektu v danom priestore (aktívne) a súhrn vnútorných sociálnych, ekonomických, technických a technologických, ekologických a iných činiteľov. Vnútorné prostredie jednotlivých referenčných objektov sa odlišuje najmä pre ich rozdielne zameranie.

Vnútorné bezpečnostné prostredie organizácie tvoria vnútorné podmienky organizácie, v ktorých dochádza k transformácií zdrojov a v ktorých manažéri vykonávajú svoju činnosť. Môže sa členiť podľa rôznych kritérií či úrovni:

- úrovne (hierarchie) manažmentu – vrcholový (top) manažment, stredný (middle) manažment, manažéri prvej linie, supervízori (firstline),
- funkčnej (horizontálnej) štruktúry – vývoj, výroba, personalistika, ekonomika, marketing, financie atď.,
- organizačnej štruktúry – jednotlivé organizačné články,
- fyzického prostredia – budovy, dielne, iné priestory,
- typov prostredia v organizácii – riadiaci systém, výkonný systém, informačný systém, podporné systémy a pod.,
- zamestnávateľských vzťahov – formálne, neformálne a pod.

Niektorí autori vnútorné bezpečnostné prostriedie organizácie delia na vnútorné bezpečnostné prostredie na makroúrovni a mikroúrovni.

Do vnútorného bezpečnostného prostredia referenčného objektu možno zaradiť:

- vnútorná charakteristika – charakter terénu vo vnútri, vnútorné komunikácie, fyzikálna charakteristika a ochranné opatrenia,
- l'udia – manažéri, zamestnanci a ich duševné vlastníctvo, návštevy,
- štruktúra – úroveň manažmentu, personálneho manažmentu a bezpečnostného manažmentu,
- proces riadenia,
- sociálna úroveň – úroveň vedenia l'údi, úroveň starostlivosti o bezpečnosť a zdravie zamestnancov, medziľudské vzťahy, migrácia pracovníkov, pracovná disciplína a pod.,
- vnútorné právne normy pre bezpečnosť,
- bezpečnostná kultúra,
- hlavné činnosti, najmä výroba, služby, skladovanie, doprava, výrobky (produkty),
- technika a technológie,
- vedľajšie činnosti, najmä personalistika, výskum a vývoj, všeobecná administratíva, údržba a servis objektov a technologických zariadení, havarijná služba,
- hnutelný a nehnuteľný majetok,
- vnútorné finančné hmotné zdroje,
- podporné technické zariadenia – zdroje energií, klimatizačné a vykurovacie zariadenia, osvetlenie, zariadenia na dodávku vody a energií, distribučná sieť, dopravné prostriedky, kanalizácia atď.,
- informácie, informačné systémy, informačné a komunikačné technológie,
- patenty, licencie, know-how,
- životné prostriedie.
Bezpečnostná kultúra je jadrom vnútorného bezpečnostného prostredia. Je to spôsob, akým je bezpečnosť vnímaná a uplatňovaná na pracovisku a často odráža „postoje, názory, predstavy a hodnoty, ktoré zamestnanci zaujímanú vo vztahu k bezpečnosti“ (Cox a Cox, 1991). Predstavuje súbor trvalých hodnôt a postojov týkajúcich sa bezpečnostných otázok, spoločných pre všetkých členov na každej úrovni organizácie. Týka sa rozsahu, v ktorom každý jednotlivec a každá skupina organizácie:

- si uvedomuje riziká a neznáme nebezpečenstvá, spôsobené svojou vlastnou činnosťou,
- sa neustále správa tak, aby sa zachovala a zvyšovala bezpečnosť,
- je ochotná a schopná prispôsobiť sa otázkam bezpečnosti,
- je ochotná komunikovať o bezpečnostných problémoch,
- trvalo vyhodnocuje správanie súvisiace s bezpečnosťou.

Dobrá bezpečnostná kultúra musí byť podporovaná najmenej štyrmi faktormi:

- záväzok hlavného manažmentu na riadenie bezpečnosti,
- schopnosť zaobchádzania s rizikami a starostlivosť o ich dopady na ľudí,
- reálne a flexibilné normy a pravidlá o rizikách,
- neustále využitie v praxi prostredníctvom monitorovania, analýzy a systémov spätnej väzby (Pidgeon a O'Leary, 2000).

2.3 LITERATÚRA


3 RIZIKO

Rizikó má vplyv na každý aspekt ľudského života. Žijeme s ním každý deň a učíme sa riadiť jeho vplyv na naše životy. Váčšinou sa to dať neštruktúrovanou činnosťou, založenou na zdravom rozume, príslušných vedomostiach, skúsenostiach a inšincte.

Rizikó je zahrnuté vo všetkých rozhodnutiach, ktoré robíme: to, aké u robíme rozho

nutia ovplyvní, ako úspešné dosiahneme svoje ciele. Rozhodovanie je postupne neoddeliteľnou súčasťou každodennej existencie a nikdy nie je významnejšie v organizácii, ako v časoch zmien a v reakcii na vonkajšie vývojové trendy. To je dôvod, prečo manažérstvo rizika je tak úzko spojené s manažérsťom zmien a rozhodovaním.

O pôvode slova rizikó možno uvažovať ako o arabskom slove risq alebo ako o latinskom slove riscum (Kedar, 1970).
• risq – arabské slovo – všetko, čo ti bolo dané (Bohom) a z čoho môžeš mať zisk – má význam náhodného a priaznivého výsledku,
• riscum – latinské slovo – vzťahuje sa k pochybnosti, akú predstavuje korálový útes pre námorníkov a používal sa pre náhodnú, ale aj nepriaznivú udalosť,
• grécka odvodenina arabského slova risq v 12. storočí má buď pozitívny alebo negatívny význam.


Sociológ Niklas Luhmann považuje pojem risk za neologizmus, ktorý sa objavil s prechodom od tradičnej k modernej spoločnosti. V stredoveku bol často používaným termín ricicum, predovšetkým v námornom obchode a jeho následných právnych problémoch, ako sú straty a poškodenie. V miestnych nárečiach 16. storočia sa používali slová rischio a riezgo. Tieto významy boli zavedené do kontinentálnej Európy prostredníctvom interakcie s Blízkym východom a severnou Afričou arabskými obchodníkmi.

V angličtine sa termín risk appeared objavuje až v 17. storoči, a „zdá sa, že bol prezatý z kontinentálnej Európy“. Zavedenie pojmu risk nahradiло starší názor, myšlienku „dobrej a zlej prosperity“. Luhmann sa snažil vysvetliť tento prechod: „možno, že to bolo jednoducho strata vie-

rohdnosti v starý pojem Fortuna, ako alegorický postavy náboženského obsahu a Prudentia (vzniešenosť), na základe vznikajúcej obchodnej spoločnosti. Inými slovami, rizikó je šanca na niečo, čo môže dopadnúť lepšie pre vás, alebo by mohlo viest’ k negatívňom výsledkom“ (Luhmann, 1996).

V priebehu vývoja a bežného používania sa význam slova zmenil zo slova popisujúce-
ho akýkoľvek nezamýšľaný alebo neočakávaný výsledok, dobrý alebo zlý, rozhodnutie alebo postup, na slovo, ktoré sa vzťahuje k nechceným výsledkom a k možnostiam ich výskytu. (Wharton, 1992).

Ľudstvo sa aktivne snažilo rizikó riadiť po celú dobu svojej existencie. V posledných storočiach pochopilo, že skúsenosti z riešenia rizík sa dajú využiť aj v budúcnosti, preto sa problematika rizika začala skúmať intenzívnejšie. Až do nedávneho obdobia sa v celom rade vedeckých štúdií, v odbornej literatúre i v právnych normách, ako aj v rôznych slovníkoch termín rizikó označoval rôznymi, často protichodnými definíciami.
V týchto definíciách sa vyskytovali najmä niektoré nedostatky:

- riziko sa definívalo ako „mierea pravdepodobnosti a závažnosti nepriaznivých následkov“, čo znamená, že riziko sa chápalo len z negatívneho hl’adiska, ako možnosť určitej ujmy, škody,
- riziko sa posudzovalo prevažne na základe vzťahu ohrozenia a zraniteľnosti, príčom následky rizika sa nie vždy brali do úvahy,
- pozitívne možnosti, ktoré niektoré riziká prinášajú, sa do úvahy nebrali vôbec, definície sa vyhýbali akémukolvek významu priaznivého výsledku, príčom však v podnikaní je možné rozumným riskovaním získať vyšší zisk,
- Príkladom môžu byť aj niektoré právne normy, v ktorých sa riziko rieši týmto spôsobom:
  - Vyhláška NBÚ č. 336/2004 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti – „riziko možného ohrozenia utajovaných skutočností v chránenom priestore určuje vedúci po z hodnotení... rizika ohrozenia utajovaných skutočností z hľadiska polohy, umiestnenia a zabezpečenia ochrany objektu a chráneného priestoru, činnosti cudzích spravodajských služieb, záškodníkov, teroristických a zločineckých skupín, technických porúch, rizik vyplývajúcich z činností zamestnancov (napríklad nedostatok vedomostí, zábudlivosť, náhoda)... a možností cudzích spravodajských služieb, za riziko sa považuje okolité objekty, ktorých havária by mohla ohroziť alebo narušiť bezpečnosť chráneného objektu“.
- V informačnej bezpečnosti je riziko chápané ako možnosť, že daná hrozba využije zraniteľnosť aktíva alebo skupiny aktív a tým organizáciu spôsobí škodu.

Práve pre rôzne chápanie rizika, najmä v negatívnom zmysle a určovanie jeho úrovne rozdielami spôsobmi, bolo z dlhodobého hl’adiska potrebné zaviesť určitú normu, aby sa zabezpečil súlad:

- terminológie, ktorá sa vzťahuje na používané pojmy,
- procesov, prostredníctvom ktorých sa manažérstvo rizika môže vykonávať,
- organizačnej štruktúry pre manažérstvo rizika,
- cieľov a náplne manažérstva rizika.


Podľa tejto normy sa už riziko chápalo aj v niektorých právnych normách, napr.: 

- Zákon č. 124/2006 Z. z. o bezpečnosti a ochrane zdravia pri práci a o zmene a doplnení niektorých zákonov – riziko je pravdepodobnosť vzniku poškodenia zdravia zamestnanca pri práci a stupeň možných následkov na zdraví.
- Zákon č. 261/2002 Z. z. o prevencii závažných priemyselných havárií – rizikom závažnej priemyselnej havárie je pravdepodobnosť vzniku závažnej priemyselnej havárie a rozsah (závažnosť) jej možných následkov, ktoré môžu naťať počas určiteho obdobia alebo za určitých okolností,
Od roku 2009 je návodom pre manažérsťo rizika skupina noriem ISO 31000. V súčasnosti do tejto skupiny noriem patria:


Okrem týchto noriem manažérsťo rizika riešia:


Tieto normy sa pre posudzovanie rizika využívajú alebo budú využívať aj vo všetkých normách pre systémy manažérsťa upravených podľa prílohy SL (predtým ISO Guide 83), napr. systém manažérsťa kvality, systém manažérsťa informačnej bezpečnosti, systém manažérsťa kontinuity činnosti, environmentálny manažérsťo systém, systém manažérsťa BOZP a v ďalších systémoch manažérsťa.
3.1 CHARAKTERISTIKA RIZIKA

3.1.1 Definícia rizika


RIZIKO – ÚČINOK NEISTOTY ZÁMEROV
risk – effect of uncertainty on objectives

Riziko sa často charakterizuje odkazom na potenciálne udalosti a následky alebo na ich kombináciu a obvykle sa vyjadruje ako kombinácia následkov udalostí (vrátane zmien v okolnostiach) a pravdepodobnosti výskytu tejto udalosti.

Zmena definície rizika presúva dôraz z „udalosti“ (niečo sa stane), na „účinok“, a najmä na účinok, na zámery. Pre názornosť, riziko nie je možnosť podieľať sa na krachu na burze, ale možnosť, že krach naruší alebo ovplyvni vás alebo vaše ciele alebo ciele organizácie, napríklad obmedzi kapitál na rozvoj.

Nová definícia jednoznačne umiestňuje riziko do súvislosti so zámermi, ktoré chce organizácia dosiahnuť. Riziko vznika preto, že tieto zámery budú sledované vzhľadom na neistoty. Organizácia môže stanoviť svoje ciele, ale na ich dosiahnutie musí často zápasť s vnútornými a vonkajšími faktormi, ktoré nemusí ovplyvňovať a ktoré vytvárajú neistotu a tým aj riziko. Tieto faktory môžu pomôcť alebo urýchliť dosiahnutie zámerov, môžu tiež zabrániť alebo oneskoriť dosiahnutie.

Riziko bolo v minulosti chápané iba v negatívnom ponímaní, že organizácie by sa mali pokúsiť vyhnúť sa mu alebo previesť ho na iných. Teraz sa musí uznať, že riziko je jednoduchým životným faktom a nemožno sa mu vyhnúť ani ho popriť. Ak pochopíme riziká a čo ich spôsobuje a ovplyvňuje, môžeme ich niektorým zo spôsobov zaobchádzať s rizikom zmeniť tak, že s väčšou pravdepodobnosťou dosiahneme svoje zámery a môžeme ich dokonca dosiahnuť rýchlejšie, efektívnejšie a s lepšími výsledkami.

Na základe uvedeného je preto pojem riziko nutné chápať nielen ako hrozbu (možné straty), ale tiež ako priležitosť (možné zisky). Straty alebo zisky môžu byť vytvorené na každej úrovni organizácie.

Obr. 1 Vztah rizika k možným stratám a ziskom (zdroj Merna, Al-Thani, 2007)

ÚČINOK znamená výsledok istého pôsobenia, je to pozitívna alebo negatívna odchýlka od očakávania, ktorá môže pozitívne alebo negatívne ovplyvňovať zámery (ciele). Táto definícia ukazuje, že všetci pôsobíme v neistom svete. Kedykoľvek sa pokúsime dosiah-

**NEISTOTA** (alebo nedostatok istoty) predstavuje stav, aj keď čiastočného nedostatku informácií, ktoré sa týkajú čielení alebo vedomostí o udalosti, jej následkoch alebo možnostiach. Tento stav vedie k neprimeranému či neúplnému poznámu alebo porozumeniu udalosti, jej následkov alebo pravdepodobnosti. Z toho dôvodu je potrebné redukovať neistotu, ako je to možné.

**ZÁMER** znamená uvážené rozhodnutie dosiahnuť niečo, úmysel, plán, cieľ. Zámery môžu mať rozličné aspekty (finančné, zdravotné, bezpečnostné, environmentálne) a môžu sa uplatňovať na rozličných úrovniach (strategická úroveň, v rámci celej organizácie, v rámci projektu, produktu alebo procesu). Predstavujú ciele, ktoré chce organizácia dosiahnuť, je to stav, ktorý chce dosiahnuť v budúcnosti.

### 3.1.2 Vzťah rizika a neistoty

Všetky činnosti ovplyvňuje neistota. O neistote možno uvažovať aj vo vzťahu k pravdepodobnosti, za predpokladu, že máme o neistote dostatočné informácie.

Pravdepodobnosť je založená na výskyte udalostí a teda musí mať vplyv na výsledok takejto udalosti.

Následok danej udalosti môže byť určený na základe príčiny a popisu udalosti. Príklad príčiny, popisu a dopadu – „prechádzanie cesty bez rozhľadnutia“ má váčšinou za následok „zranenie“.

Keď môžeme určiť pravdepodobnosť, príčinu a následok nejakého udalosti, môžeme vypočítať rozdelenie pravdepodobnosti. Z tohto rozdelenia pravdepodobnosti možno vzťahom na rozsah možností určiť výskyt daného rizika a možno tiež redukovať neistotu spojenú s touto udalosťou. Predpoveď je obvykle založená na údajoch alebo minulých skúsenostiach a tak poskytuje základ pre potenciálne riziko.

Je potrebné poukázať na to, že chápame (vymedzenie) samotných pojmov rizika a neistoty nie je v literatúre jednotné. Sú autori, ktorí tieto pojmy považujú za synonymá, a sú autori, ktorí ich vymedzujú ako dve samostatné kategórie. V anglickej terminológii existujú dva termíny: risk (riziko), uncertainty (neistota).

Obvykle je vzťah medzi neistotou a rizikom charakterizovaný takto:

1. neistota (ako širší pojem): je to neurčitosť, náhodnosť podmienok či výsledkov nejakých javov či procesov,
2. riziko (ako užší pojem): je to taký druh neistoty, kedy je možné – pomocou obvyklých štatistických metód – kvantifikovať pravdepodobnosti vzniku odchýlných alternatív.

Takéto odlišenie pojmov neistoty a rizika pochádza od amerického ekónoma Franka Knighta, ktorý v diele zdôrazňuje, že *riziko je hlavným zdrojom podnikových ziskov* (*Knight, 1921*).

Neistotu je potrebné brať v istom zmysle radikálne odlišne od známeho pojmou riziko, od ktorého nebola nikdy riadne oddelená. Pojem „riziko“, ktorý možno voľne použiť v každodennej reči a ekonomickej diskuzii, naozaj obsahuje dve veci, ktoré funkčne, aspoň vo svojich príčinných vzťahoch k fenoménu ekonomické organizácie, sú kategoricky odlišné.

Základným faktom je, že „riziko“ znamená v niektorých prípadoch množstvo vnímavých meraní, zatiaľ čo v iných prípadoch to je niečo odlišné od tohto charakteru, a tam sú dôležitosiahle a zásadné rozdiely v základoch tohto javu, v závislosti od toho, ktorý z nich je naopak prítomný a pôsobí. Zodpovedajúcim spôsobom treba obmedziť termín „neistoty“ na prípady, ktoré sú nekvantifikovateľné. Podľa toho je *neistota nemerateľná*, nie je možné ju vypočítať, zatiaľ čo *riziko je merateľné* (*Knight, 1921*).


**Tab. 1 Spojitosť rizíko – neistota (zdroj Rafferty, 1994)**

<table>
<thead>
<tr>
<th>RIZIKO</th>
<th>NEISTOTA</th>
</tr>
</thead>
<tbody>
<tr>
<td>merateľné</td>
<td>nemerateľná</td>
</tr>
<tr>
<td>štatistické ohodnotenie</td>
<td>subjektívna pravdepodobnosť</td>
</tr>
<tr>
<td>pevné informácie (Hard Data)</td>
<td>kvalifikovaný názor</td>
</tr>
</tbody>
</table>

Neistota teda existuje tam, kde existuje v priebehu činnosti viac než jeden možný výsledok, ale pravdepodobnosť každého výsledku nie je známa. Rozhodnutie je podmienené rizikom, keď existuje celý rad možných výsledkov, a keď môžu byť pripojené k výsledku známe pravdepodobnosti (*Bussey, 1978, Merrett a Sykes, 1983*).
Neistota sa používa na popis situácie, kedy nie je možné pripojiť pravdepodobnosť k náhodnosti výskytu udalostí, spôsobuje rozpor medzi dobrým rozhodnutím a dobrým výsledkom. Rozlišujúcim faktorom medzi rizikom a neistotou je, že riziko sa bere ako merateľná vlastnosť a má miesto v kalkulácii pravdepodobnosti, zatiaľ čo neistota takúto vlastnosť nemá (Finkel, 1990).

3.1.3 Zdroj rizika

Vnútorné vlastnosti niečoho, majúce za následok náchylnosť (sklon) stať sa zdrojom rizika, ktorý môže viesť k niekedy združené, nie je možné pripojiť pravdepodobnosť k náhodnosti výskytu udalostí, spôsobuje rozpor medzi dobrým rozhodnutím a dobrým výsledkom. Rozlišujúcim faktorom medzi rizikom a neistotou je, že riziko sa bere ako merateľná vlastnosť a má miesto v kalkulácii pravdepodobnosti, zatiaľ čo neistota takúto vlastnosť nemá (Finkel, 1990).

3.1.3 Zdroj rizika

Vnútorné vlastnosti niečoho, majúce za následok náchylnosť (sklon) stať sa zdrojom rizika, ktorý môže viesť k nejakej udalosti s následkom, predstavuje zraniteľnosť (ISO Guide 73:2009).

Zdroj rizika (risk source) je prvok, ktorý sám osebe alebo v kombinácii má vnútorný potenciál vyvolat’ rizíko. Zdroj rizika predstavuje určitá časť celku (zložka, súčiastka, element), ktorá môžu potenciálne spôsobiť určité udalosti (udalostí).

Zdroj rizika môže obsahovat’ potenciál na spôsobenie:
- udalosti s pozitívnym následkom,
- udalosti s negatívnym následkom,
- aj udalosti s pozitívnym následkom, aj udalosti s negatívnym následkom súčasne.

Zdroj rizika je tam, kde rizíko vzniká, tam, odkiaľ rizíko prichádza, existuje v určitej entite (niečo jestvujúce, akýkoľvek fenomén, vec, bytosť, útvar, objekt, subjekt, ucelená jednotka). Zdroj rizika môže byť hmotný alebo nehmotný. Mnoho zdrojov rizíka sa v priebehu činnosti organizácie vyskytuje v rôznych časoch. Zdrojom rizíka môže byť akýkoľvek prvok (faktor), ktorý môže ovplyvniť výkon, bezpečnosť, majetok a životného prostredia organizácie. K riziku dochádza, keď účinok tohto prvku (faktora) je jednak neistý a jednak významný vo svojom následku.

Rizíka, ktorým je vystavená organizácia a jej činnosti, môžu vyplývať z vonkajších alebo vnútorných faktorov referenčného objektu (prostredia). Existuje mnoho zdrojov rizík, ktoré musí organizácia vziať do úvahy, než predtým vykoná akékoľvek rozhodnutie. Potenciálne zdroje rizík okrem iného zahŕňajú napríklad:
- obchodné vzťahy a záväzky,
- právne očakávania a záväzky,
- ekonomické zmeny a pomery,
- technologické inovácie a zmeny,
- politické zmeny a trendy,
- prírodné javy a sily,
- ľudské chyby a návyky,
- nedostatky a extrémy v riadení.

Rizíka môžu byť špecifické pre jednotlivé úrovne riadenia (strategická, prevádzková). Rizíko by malo byť v závislosti od jeho úrovne modifikované (riadené).

Je preto dôležité, aby organizácia poznala zdroje rizík a udalostí, ktoré môžu spôsobiť. Musí poznáť možné následky týchto udalostí na jednotlivé objekty a priestory (aktíva), pravidelné vykonávať ich identifikáciu, analýzu a hodnotenie a prijímať príslušné opatrenia na zaobchádzanie s rizikami, ktorých úroveň je vyššia než prijateľná úroveň rizíka.
3.1.4 Udalost'

Udalost' predstavuje výskyt alebo zmenu konkrétej množiny (súboru) okolností. Osoby, majetok, životné prostredie a všetky druhy činnosti v organizácii sú ovplyvňované udalost'ami, ktoré môžu pozitívne alebo negatívne ovplyvniť dosahovanie jej cieľov.
Udalosť znamená:
1. účinok, výsledok, alebo výstup niečoho, čo sa vyskytlo, prihodilo, stalo skôr, napr. nehoda bola dôsledkom bezohľadnej jazdy,
2. činnosť alebo príležitosť, ktorá nasleduje ako účinok, výsledok, alebo výstup,
3. výsledok alebo zakončenie po niečom,
4. niečo čo sa stane (stalo) v určitom čase a priestore.

Udalosť sa môže:
• vyskytnúť raz alebo viackrát a môže mať niekoľko príčin,
• mať viacnásobné následky a môže ovplyvniť viacero cieľov.
• niekedy skladat’ z niečoho čo nenastane, aj keď sa to predpokladalo,
• vzťahovať na incident alebo nehodu,
• niekedy znamenat’ len príhodu alebo nešt’astnú udalosť.

V minulosti niektoré normy popisovali riziko ako „naliehavú udalosť“. V súčasnosti sa zvažuje, že riziko môže nastať aj pre pomaly sa meniace a okolnosti a nielen z dôvodu náhlej udalosti. Zmena klímy je príkladom meniacej sa situácie, ktorá predstavuje veľké riziko pre organizácie, a dokonca aj pre planétu, napriek tomu, že nie je charakterizovaná ako jedna udalosť.

Udalosť majú vždy príčiny a obvykle aj následky. Následok udalosti môže byť pozitívny alebo negatívny.

Udalosti s negatívnymi následkami predstavujú incidenty (incident), nehody (accident), prerusenie činnosti, mimoriadne udalosti, krízové situácie, krízové stavy a pod. Špecifickou udalosťou s negatívnymi následkami je úmyselné ohrozenie osoby, majetku, alebo životného prostredia. Tieto udalosti majú zdroj v určitom druhu nebezpečenstva a sú schopné spôsobiť škody, ujmy, čím môžu negatívne ovplyvniť plnenie stanovených cieľov.


<table>
<thead>
<tr>
<th>ZDROJ RIZIKA</th>
<th>UDALOSŤ</th>
<th>NÁSLEDOK UDALOSTI</th>
</tr>
</thead>
<tbody>
<tr>
<td>pozitívny potenciál</td>
<td>s pozitivnym následkom – príležitosť</td>
<td>zíšok</td>
</tr>
<tr>
<td>negatívny potenciál – nebezpečenstvo</td>
<td>s negatívnym následkom – incident, nehoda, prerusenie činnosti, mimoriadne udalosti, krízové situácie alebo krízové stavy</td>
<td>škoda, ujma</td>
</tr>
</tbody>
</table>

O udalosti bez následkov sa môže hovoriť aj ako o takmer strate, príhode, šťastnej náhode alebo o dôvernom upozornení (skoronehode).
3.1.5 Následok a pravdepodobnosť

Merna a Al-Thani podrobne popisujú riziká vo firme a uvádzajú typické parametre rizika na obr. 3.

Dôležité a podstatné je charakterizovanie a meranie rizika vzhľadom na následky a pravdepodobnosť týchto následkov, nie iba abstraktnej pravdepodobnosti udalostí, ktoré by mohli byť odvodené od zámerov organizácie. Následky a ich pravdepodobnosť sa často najvzájomným kombinujú, aby sa definovaľa úroveň rizika.

Niektoré normy stále uvádzajú, že úroveň rizika možno odhadnúť, s zreteľom na pravdepodobnosť udalosti a následky, ktoré z nich vyplývajú, toto však je všeobecné nepoužiteľné a najčastejšie vytvára neriešné odhady úrovne rizika, niekedy nazvané „zdanielvé riziko“, pretože spôsňať možno odhadovanie pravdepodobnosti sa často zveličuje.

NÁSLEDOK (consequence) je to, čo príčinne nasleduje po niečom, je to výsledok udalosti a následky, ktorým sa odvodené od zámerov organizácie. Následky a ich pravdepodobnosť sa často najvzájomným kombinujú, aby sa definovala úroveň rizika.

Jeden z jednoduchých spôsobov na popis potenciálnych následkov je povedať, čo by sa mohlo stať a čo by k tomu mohlo viest'. Následky, ktorými populujeme riziko môžu zahrať stratu, ublíženie alebo negatívne účinky na ciele. Následok môže byť trvalý alebo premenlivý, môže sa vyjadriť kvalitatívne alebo kvantitatívne. Počiatočné následky sa môžu zvyšovať prostredníctvom lavínových efektov.

Jeden z jednoduchých spôsobov na popis potenciálnych následkov je povedať, čo by sa mohlo stať a čo by k tomu mohlo viest'. Následky, ktorými populujeme riziko môžu zahrať stratu, ublíženie alebo negatívne účinky na ciele. Následok môže byť trvalý alebo premenlivý, môže sa vyjadriť kvalitatívne alebo kvantitatívne. Počiatočné následky sa môžu zvyšovať prostredníctvom lavínových efektov.

PRAVDEPODODB OST (likelihood) znamená predpoklad (šanca), že sa niečo stane. Pravdepodobnosť môže byť definovaná, určená alebo meraná objektívne alebo subjektívne a môže byť vyjadrená kvalitatívne alebo kvantitatívne a popisovaná: a) kvalitatívne s využitím všeobecných výrazov (slovne napr. malá, stredná, veľká) alebo b) kvantitatívne s využitím matematiky, ako:

- pravdepodobnosť (probability), veľkosť šance pre výskyt udalosti, vyjadrená číslom (od 0 do 1), kde 0 je nemožnosť a 1 je absolútna istota.
- početnosť (frequency), počet udalostí alebo následkov za určitú časovú jednotku.
3.2 ÚROVNE RIZIKA

Úroveň rizika alebo kombinácie rizík predstavuje jeho (ich) veľkosť, ktorá sa vyjadruje ako kombinácia:
• následkov (consequences) udalosti (zisk alebo ujma),
• pravdepodobnosti (likelihood), že nejaká udalosť nastane.

Klasickými úrovňami rizika boli prijateľná a neprijateľná úroveň rizika, v súčasnosti sa však podľa STN 31010:2011 pre vnímanie úrovne rizika využívajú nasledujúce tri kategórie:
1. riziká sú také veľké, že nie sú prijateľné,
2. riziká sú také malé, že sú prijateľné,
3. riziká sú medzi predchádzajúcimi dvomi kategóriami a potom musí nasledovať posúdenie kompromisu medzi nákladmi na zaobchádzanie s rizikom a prínosom (benefitom).

Úroveň rizika sa obvykle zaradzuje do troch pásiem (oblastí) podľa obr. 4.

Obr. 4 Pásma (oblasti) úrovne rizika podľa zásady ALARP

Horné pásmo – neprijateľná / neakceptovateľná úroveň rizíka (unacceptable) – veľká úroveň rizika, považovaná za neprijateľnú, bez ohľadu na to, či môže znamenať akýkoľvek prínos a zaobchádzanie s rizikom je nevyhnutné bez ohľadu na jeho náklady, zachováva sa len v mimoriadnych situáciách.

Stredné pásmo – prípustná / znesiteľná úroveň rizika (tolerable) – prípustné sú len pri využití všetkých dostupných opatrení na zniženie rizika, pričom ide o úroveň zvažovania
efektívnosti, kde sa berú do úvahy náklady i prínosy a priležitosti sú zvažované s prihliadnutím na potenciálne následky. Podľa zásady ALARP je tu posuvná stupnica pre:
• prípustná nežiaducá rizika, ktoré sú prípustné len v prípade, ak sa ich zníženie nedá uskutočniť alebo ak náklady na jeho zníženie sú výrazne númerné k získaným prínosom, preto sa očakáva, že sa riziko zníži, pokiaľ náklady na zníženie nebudú vysoko prevyšovať získané prírody.
• prípustné znesiteľné rizika, ktoré sú prípustné po znížení nákladov na ich zníženie, ak prípustne prevšťali náklady, preto je pre ich znížovanie vhodné aplikovať prísnu analýzu nákladov a prírody.

Dolné pásmo – všeobecne prijateľná / akceptovateľná úroveň rizika (broadly acceptable) – úroveň rizika je považovaná za zanedbateľnú alebo tak malú, že nie sú potrebné žiadne opatrenia na zaobchádzanie s rizikom, riziká je potrebné monitorovať, aby sa zaistilo, že ostanú nízke.

Všeobecne prijateľné riziko

Je to miera rizika, ktorá je možné podstúpiť (prispúsiť). Predstavuje spoločensky prijateľnú úroveň rizika, pri ktoré pravdepodobnosť výskytu nežiaduceho efektu je taká malá, následky pôsobenia sú také mierne, zisk zo situácie (skutočný alebo len vnímá) je taký veľký, že osoby, skupiny alebo celá spoločnosť je ochotná toto riziko podstúpiť.

To znamená, že táto úroveň rizika sú s hľadiska ochrany ľudskeho združia, ani z hľadiska ochrany ostatných živých systémov nevyžaduje regulačné opatrenia na jeho zníženie. Pretože žiadna ľudska aktivita nie je absolútne bezpečná, je nutné stanoviť miernu úroveň rizika, ktorú je možné akceptovať.

Pásmo akceptovateľných rizík siaha od nulového až po dolnú hranicu prípustného rizika. Hodnota rizika v tomto pásmo je na úrovni, ktorá je spoločensťou, právnymi normami a vnútornými podmienkami procesov tolerovaná, obsahuje riziká, ktoré umožňujú subjektom existovať a plniť stanovené ciele s vedomím existencie rizika. Naprieť tomu je možné zvažiť, či je potrebné zaviesť ďalšie opatrenia na modifikáciu tohto rizika.

Pripustné riziko

Úroveň rizika, ktorú jednotlivec alebo spoločnosť sú ochotní podstúpiť pre zaistenie istých výhod. Podmienkami definície prípustného rizika sú:
• má zabezpečiť určité prínosy,
• rozsah rizika nie je možné považovať za zanedbateľný alebo ako niečo, čo môžeme ignoroovať, ale skôr ako niečo, čo potrebujeme sledovať a znížovať tak, ako je to možné (ALARP).

Prípustné riziko je znamená prijateľné rizisko, úroveň týchto rizík je medzi prijateľnými a neprijateľnými rizikami. Omôr výkonu sa rizikú alebo odstránenia jeho zdroja sa na modifikáciu týchto rizík využívajú najmä spôsoby znížovania úrovne rizika. Platí pre ne pravidlo, že pre ich znížovanie sa musí posúdiť vzťah medzi nákladmi na jeho znížovanie a prínosmi, ktoré sa na jeho znižovanim dostiahnu.

Na tomtom základe sa na znížovanie úrovne rizika budú využívať najmä spôsoby zaobchádzania s rizikom:
• zmena pravdepodobnosti rizika,
• zmena následkov rizika,
• podielanie sa na riziku s ďalšou stranou alebo stranami,
• plánované zachovanie rizika na základe kvalifikovaného rozhodnutia – keď už ďalšie znižovanie úrovne rizika je vzhľadom na vynaložené náklady neúnosné.
Tieto riziká je podľa metodického postupu nutné znižovať až na úroveň, kedy nákłady na jeho zníženie sa stávajú neúmernými v porovnaní s mierou zníženia rizika. K znižovaniu rizika možno pristúpiť z hľadiska zásady ALARP, t. j. zásada znižovania rizika na tak nízke, ako je to možné.

Táto zásada znamená, že náklady na ďalšie zniženie rizika sa stávajú neúmernými v porovnaní s mierou zníženia rizika. K znižovaniu rizika možno pristúpiť z hľadiska zásady ALARP, t. j. zásada znižovania rizika na tak nízke, ako je to možné.

Manažérsstvo rizika podľa zásady ALARP alebo trojuholníka ALARP (As Low As Reasonable Practicable – tak nízke, ako je to možné) je termín často používaný na riziká, ktoré predstavujú ohrozenie ľudského života a zdravia alebo škodu v životnom prostredí a ukazuje, že riziku a modifikácii rizika je potrebné venovať primeranú pozornosť.

Zásada ALARP zahŕňa zväženie a porovnanie úrovne rizika s ťažkosťami, časom a finančnými nákladmi, potrebnými na jeho riadenie. Znamená zistenie, že náklady na ďalšie zníženie rizika z pohľadu časovej náročnosti, zložitosti a vynaloženého úsilia sú neúmerné k prínosu získanému realizáciou ochranných opatrení (výsledku zníženia rizika). Opisuje, do akej miery možno viditeľne očakávať, že riziko na pracovisku bude riadené.

Tento postup nie je normatívny a pretože vyžaduje, aby zamestnávatelia uplatňovali svoje názory, niekedy však môže byť pre nich náročný. Je na zamestnávateľov, aby zaistili, že ním vybraný návrh na modifikáciu rizika zaistí jeho zníženie na úroveň „tak nízke, ako je to pre neho uskutočnitelné.“

**Neprijateľné riziko**

Pásmo neprijateľných rizík leží medzi hornou hranicou prípustného rizika a hranicou maximálnej úrovne rizika. Pri prekročení hranice maximálnej úrovne rizika sa systém môže vychýliť z rovnovážneho stavu.

Neprijateľné úroveň rizika vyžaduje bezodkladné prijatie niektorého opatrenia zo spôsobov zaobchádzania s rizikom.

V prvom rade je vhodné zvážiť prijatie opatrení na vyvarovanie sa riziku alebo odstránenie jeho zdroja. V prípade, že sa obe opatrenia nedajú z rôznych dôvodov uskutočniť, je potrebné prijať opatrenia na zniženie rizika podľa zásady ALARP a jeho prípadný prenos na aľšiu stranu alebo strany. Vo výnimčných prípadoch je možné využiť plánované zachovanie rizika na základe kvalifikovaného rozhodnutia.


Zásada ALARP sa môže uplatňovať na všetky riziká, teda i riziká neprijateľné!

**Tab. 3 Úroveň rizika**

<table>
<thead>
<tr>
<th>R I Z I K O</th>
<th>Prijateľné riziko</th>
<th>Prípustné riziko</th>
<th>Neprijateľné riziko</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zostatkové riziko</td>
<td>zostávajúce riziko po zavedení ochranných opatrení</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

32
Minimálna úroveň rizika – tento pojem sa v praxi často vyskytuje, na jeho úroveň sa snažíme dostat’ v procese znižovania úrovne rizika. Minimálna úroveň rizika teda predstavuje riziko, ktoré:

• je možné považovať za minimálné možnú úroveň rizika (prakticky však o ňom môžeme hovoriť ako o nemožnom),
• je nutné priebežne monitorovať’, aby sme mohli včas zaznamenať prípadné zmeny v miere rizika, ale aj v jeho charakteristike.

Toto riziko má niekedy aj charakter zvyškového rizika, ktoré už d’alej nemôžeme znižovať bez zmien v stanovených vnútorných a vonkajších podmienkach, napr. stanovená výrobná cena, prípadne stanovená kvalita surovín, miera bezpečnosti zariadenia.

Zvyškové riziko (reziduálné riziko) je riziko, ktoré ostane po zaobchádzaní s rizikom. Môže obsahovať neidentifikované riziko alebo môže byť tiež známe ako zachované riziko. Ide o riziko, ktoré zostalo po implementácii vybraných opatrení zaobchádzania s rizikom. Je to riziko, ktoré ostalo po jeho znižení, odstránení zdroja rizika, zmene následkov alebo pravdepodobnosti, prenose rizika či zachovani rizika.

Je to miera rizika, ktorú nie je možné úplne modifikovať pri vytvorení príslušného opatrenia, uvádza sa v informácii pre užívateľa tovaru, vrátene možných následkov príslušného negatívneho javu. Zmyslom zaobchádzania s rizikom je, aby bolo zostatkové riziko nulové (t. j. aby sa odstránilo pôvodné riziko), respektíve aby bola úroveň zostatkového rizika čo najnižšia.

Nulové riziko – predstavuje len teoretické východisko pri skúmaní rizika. Riziko je možné úplne modifikovať len odstránením zdroja rizika alebo vyvarovaním sa riziku na základe rozhodnutia nezačínať činnosť alebo nepokračovať v činnosti, ktorá vytvára riziko.
3.3 KATEGORIZÁCIA RIZÍK

Kategorizácia rizík znamená zoskupenie príbuzných rizík podľa rôznych charakterístík. Kategorizácia rizík môže byť viacdimenziálna, na zachytenie všetkých požadovaných pohľadov na riziká a ich hodnotenie, prípadne splnenie potrebných štandardov. Riziká je možné zoskupovať najmä podľa:

a) vzťahu k organizácii (možnosti výskytu) – vonkajšie (externé); vnútorné (interné),
b) výsledku pôsobenia rizíka:
   • podnikateľské (špekulatívne) – týkajú sa podnikateľských činností, sú spojené s nádejom výsledku v rozpočte na výsledky a súčasne s hrozobou negatívnejšej výsledky ako sa plánovalo, vyplyvajú z podstaty podnikania, vplyv neistoty pri stanovovaní stratégie a pri jej naplnení, výsledkom môže byť buď strata alebo zisk,
   • čisté (bezpečnostné) – vyplývajú z určitého nebezpečenstva, spojené s hrozobou negatívneho vplyvu (škoda na hmotných a nehmotných aktívach podniku, na životnom prostredí, poškodenie zdravia zamestnancov, zákazníkov a ostatných osôb v blízkosti podniku), výsledkom je vždy len ujma,
   • oblasti ich vzniku:
     • v ekonomickej oblasti: podnikateľské (najčastejšie); nové investície (každá investícia môže vieť k zisku, ale aj k strate),
     • vo firemnej oblasti: technické, projektové, výrobné, ekonomické, trhové,
     • v politickej oblasti: makroekonomické zásahy vlád,
     • v právnej oblasti: obrovským zdrojom rizika je nezákonná činnosť,
   • oblasti (formy) ich dopadu na chod organizácie:
     • kritické: spôsobí takú výšku škôd, že vedie k zániku podniku,
     • dôležité: podnik je schopný zvládnuť nepriaznivé okolnosti pomocou vlastných zdrojov alebo aktiv, nevzniká vážnejší finančný tlak,
     • bežné: podnik je schopný zvládnuť nepriaznivé okolnosti pomocou vlastných zdrojov alebo aktiv, nevzniká vážnejší finančný tlak,
   • predvídateľnosti rizika – predvídateľné alebo nepredvídateľné,
   • rozsahu pôsobenia:
     • systematické – tento typ rizika platí pre všetky podnikateľské subjekty, zdrojom sú celkové zmény podnikateľského prostredia, ich následky sa dotýkajú všetkých podnikateľských jednotiek, ale miera vplyvu môže byť rôznia,
     • nesystematické – tento typ rizika platí len pre určitý odbor podnikania, zdrojom sú zmény špecifického prostredia a zmeny v systéme s dopadom na konkrétne podniky,
   • miery ovplyvňiteľnosti rizika:
     • neovplyvniteľné – nie je možné ovplyvniť pravdepodobnosť vplyvu neistoty na ciele podniku (pravdepodobnosť vzniku rizika), podnik môže do určitej miery ovplyvniť veľkosť vplyvu (odchýlky), neovplyvniteľné sú systematické a časť nesystematických rizík,
     • ovplyvniteľné – možno ovplyvniť pravdepodobnosť vzniku vplyvu neistoty na ciele aj veľkosť vplyvu,
   • poradia pôsobenia (vzniku a odstrániteľnosti) – primárne, sekundárne (vzniká pri modifikácii primárnych rizík),
   • veľkosť rizika – malé, stredné, veľké,
   • miery akceptovateľnosti (prijateľnosti, únosnosti) – nevyhnutné (nutné), prijateľné (akceptovateľné, únosné), neprijateľné (neakceptovateľné, neúnosné), zvyškové (rezidualné),
   • pravdepodobnosti vzniku a pôsobenia – nepravdepodobné, málo pravdepodobné, pravdepodobné, veľmi pravdepodobné, takmer isté.
l) početnosti objektov pôsobenia rizika – individuálne a skupinové.

m) merateľnosti rizika – merateľné a nemerateľné.

n) možnosti poistenia rizika – poistiteľné a nepoistiteľné.

F. Škvraňa a P. Zatlkaj (1994) klasifikujú bezpečnostné riziká podľa:

- **teritoriálneho rozsahu**: celosvetové (globálne), kontinentálne (subkontinentálne), regionálne (subregionálne),
- **sektora (zdroja)**: vojenské, politické, ekonomické, sociálne, ekologické, kultúrne (etnické, rasové, náboženské),
- **subjektov, ktoré sú ich nositeľmi**: určité štáty (skupiny štátov, aliancie, bloky a pod.), politické a iné subjekty neštátneho charakteru (teroristické organizácie a pod.),
- **charakteru ich pôsobenia**: bezprostredné, sprostredkované, aktuálne, skryté, potenciálne a pod.,
- **času trvania**: krátkodobé, strednodobé, dlhodobé (dočasné a stále).

Eichler (2004) klasifikuje riziká na:

- vojenské, politické, ekonomické, ekologické, sociálne a kultúrne. Najnaliehavejším a najvážnejším ohrozením súčasnosti je podľa neho prepojené pôsobenie terorizmu a šírenia ZHN, je to zámerné, priame, naliehavé ohrozenie politického a vojenského charakteru.

Šimák (2006) uvádza veľmi podrobnú klasifikáciu rizík z rôznych hládkov. Zo všeobecného pohľadu a v závislosti od pôvodu riziká rozdeľuje do dvoch základných skupín:

a) **riziká antropogénne** – súvisia s činnosťou človeka v procese vytvárania si optimálnych podmienok pre život:
- **sociogénne riziká** – spojené so sociálnymi javmi, správaním sa človeka ako jedinca, ktorý je osobnosťou a neopakovateľnou individualitou,
- **technogénne riziká** – predstavujú zásadné zásahy do výrobných procesov a rôznych služieb,
- **agrogénne riziká** – v systéme poľnohospodárskej a potravinárskej produkcie,
- **kombinované riziká** – nebezpečnejšie než čisté antropogénne riziká.

b) **riziká nezávislé od činnosti človeka**:
- **přírodné riziká** – zdrojom je samotná priroda, jej rôznorodosť a zložitosť:
  - tektonické – pohyby a poruchy v zemskej kôre, najmä na styku litosférických dosiek, zemetrásenia, sopečná činnosť,
  - telurické – geoaktívne zóny, topologické – zosuvy pôdy ako proces svahovej modelácie,
  - meteorologické – fyzikálne javy a procesy v ovzduší, súvisia s vývojom počasia a jeho negatívnymi vplyvmi na výrobu a služby,
- **kozmogénne riziká** – sú minimálne, ale patria do celkovej štruktúry rizík, zrážka Zeme s inou planétou, prípadne s iným vesmírnym telesom.

Merna, A. a Smith uvádzajú, že riziká pre podnikanie a bezpečnosť organizácie možno identifikovať najmä v nasledujúcich oblastiach (Merna, A. a Smith, 1996):

- **Politika** – vládna politika, verejná mienka, zmena ideológie, právne normy, nepokoje (vojna, terorizmus, pouličné nepokoje...), zmény kompetentných orgánov.
- **Ekonomika** – politika finančnej správy, dane, nákladová inflácia, úrokové miery, kurzy mien.
- **Trh** – dopyt a výhľad, konkurencia, zastarávanie, uspokojenie zákazníka, móda.
- **Financie** – bankrot, marže, poistenie, podiel na riziku.
- **Právne predpisy** – zásady spojené so zmenu v právnych normách na štátnej úrovni i v smerniciach EÚ.
- **Príroda** – počasie, zemetrasenie, záplavy, požiar alebo explózia, archeologický výskum, nepredvidateľné pôdne podmienky.
- **Životné prostredie** – kontaminovaná pôda, zodpovednosť za jej znečistenie, verejná mienka, zákaz o ochrane životného prostredia, environmentálne predpisy.
- **Bezpečnosť** – nebezpečné látky, kolízie, kolaps, požiar, explózie.
- **Zločinnosť** – nedostatok bezpečnosti, vandalizmus, krádeže, podvody, korupcia.

Merna, T. a Al-Thani (2007) uvádzajú nasledujúce typické riziká vo firme:
- **riziká projektu,**
- **globálne riziká** – politické, právne, obchodné, environmentálne (nekontrolované),
- **elementárne riziká** – stavebné alebo výrobné, prevádzkové, finančné, riziká výnosu (kontrolované),
- **holistické riziko** – spojené s nehmotným majetkom (tržné podiely, reputácia, hodnota, technológie, duševný majetok ako sú údaje, patenty a autorské práva, zmeny v strategii alebo v metódach, predstavy akcionárov, bezpečnosť spoločnosti, kvalita výrobku),
- **stále riziko** – vzťahuje sa iba na potenciálne straty,
- **dynamické riziko** – týka sa maximalizácie príležitostí, znamená, že dôjde k potenciálnemu prírastku, rovnako tak k potenciálnej strate,
- **neodmysliteľné riziko,**
- **náhodné riziko** – keď na organizáciu pôsobí nejaká udalosť priamo v oblasti mimo dosah jej priameho riadenia, ale od ktorej je závislá, napr. zlá dodávatelia,
- **zákaznícke riziko** – závislosť od klienta,
- **fiškálne/regulačné riziko** – potenciálne zmeny v prostredí,
- **riziko spojené s nákupom,**
- **riziko spojené s poškodením povesti / riziko škôd** – skôr je to následok iného rizika,
- **organizačné riziko** – zlá štruktúra môže viesť k slabej kontrole a komunikácii,
- **riziko interpretácie** – používanie profesijných jazykov,
- **riziko IT** – informačné technológie,
- **riziko zo strany OPEC** – výkyvy v cenách ropy,
- **procesné riziko** – proces riadenia projektu,
- **heuristika** – riziká spojené s ľudským faktorom,
- **riziko pri vyraďovaní zariadenia z prevádzky,**
- **inštitucionálne riziko** – sumarizovanie rizík spôsobených organizačnou štruktúrou a správaním.
3.4 LITERATÚRA


EICHLER, J. [2004]: Jak vyhodnocovat bezpečnostní hrozby a rizika dnešního světa. In: Ob- 

FINKEL, A. M. [1990]: Confronting Uncertainty in Risk Management: A Guide for decision- 

Edition), Edward N. Zalta (ed.).

HUBBARD, D. W. [2009]: Zlyhanie manažmentu rizík: Prečo je to rozbíté a ako to vyriešiť. 
John Wiley&Sons.


Italiano Di Studi Sull Alto Medioevo, Spoleto.

KIGHT, F. H. [1921]: Riziko, neistota a zisk. Boston, MA: Hart, Schaffner & Marx, Houg- 

LUHMANN, N. [1996]: Modern Society Shocked by its Risks. University of Hong Kong, 
Department of Sociology Occasional Papers 17, Hong Kong.


MERNÁ, T. – SMITH, N. J. [1996]: Projects Procured by Privately Financed Concession 
Contracts. Časť 1,2. Asia Law. Practice, Hong Kong. 1996.


STN 01 0380 Manažéřstvo rizika, Zásady a návod.

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

ŠKVRNDA, F. – ZATLKAJ, P. [1994]: Národná bezpečnosť SR a európske bezpečnostné 

WHARTON, F. [1992]: Risk: Analysis, assessment, and management. John Wiley and Sons, 
Chichester.
4 PODNIKATEĽSKÉ RIZIKÁ

Riziká, ktorým je vystavený referenčný objekt (objekt, organizácia) a jeho činnosti, možno charakterizovať najmä podľa prostredia ich vzniku (vonkajších alebo vnútorných faktorov), podľa výsledku pôsobenia rizika a zámeru do kategórií (tab. 4):

- podľa charakteru prostredia – vonkajšie (externé) a vnútorné (interné) riziká,
- podľa následkov rizika – špekulatívne (podnikateľské) a čisté (bezpečnostné) riziká,
- podľa zámeru – riziká spôsobené úmyselnou alebo neúmyselnou činnosťou (nedbalošťou).

Tab. 4 Riziká organizácie

<table>
<thead>
<tr>
<th>Vonkajšie (externé) a vnútorné (interné) riziká</th>
<th>Bezpečnostné riziká (čisté)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zdroj</td>
<td>Negatívny potenciál</td>
</tr>
<tr>
<td>Positívny i negatívny potenciál</td>
<td>NEBEZPEČENSTVO</td>
</tr>
<tr>
<td>Udalosť</td>
<td>s negatívym následkom</td>
</tr>
<tr>
<td>s pozitívnym násladkom</td>
<td>s negatívym následkom</td>
</tr>
<tr>
<td>Následok</td>
<td>ZISK</td>
</tr>
<tr>
<td>STRATA</td>
<td>ŠKODA</td>
</tr>
</tbody>
</table>

Vonkajšie (externé) riziká spôsobujú faktory vonkajšieho prostredia, tieto druhy rizík subjekt nemôže priamo ovplyvňovať, preto sa musí na ich prejavy preventívne pripraviť.

Vnútorné (interné) riziká sa prejavujú vo vnútri organizácie, tieto druhy rizík môže subjekt ovplyvňovať a riadiť.

Veľké množstvo rovnakých rizík sa však prejavuje ako vo vonkajšom, tak i vo vnútornom prostredí, ako ukazuje príklad najpodstatnejších rizík z rôznych oblastí, ktorých príčiny ležia zvonku i zvnutra organizácie (Standard Inštitútu riadenia rizík).

Obr. 5 Vonkajšie a vnútorné riziká organizácie

4.1 CHARakteristika podnikateľských rizík

Podnikateľské (špekulatívne) riziká sa týkajú podnikateľských činností, sú spojené s nádejou na pozitívnejšie výsledky a súčasne s hrozobou negatívnejších výsledkov než sa plánovalo. Výplývajú z podstaty podnikania, ako vplyv neistoty pri stanovovaní stratégie a pri jej naplnění.

Podnikateľské riziko môže mať pre podnikanie pozitívny i negatívny následok. Risiko pozitívne stimuláčne pôsobí na podnikateľský subjekt. Spája sa s nádejou na úspech, s úspešným uplatnením na trhu, s dosiahnutím vysokého zisku, s budúcnosťou podniku a jeho ďalším rozvojom. Negatívny vplyv podnikateľského rizika vyplýva z obáv zo straty, prípadne až zániku podniku. Riziko v podnikaní sa môže chápať ako nebezpečenstvo, že skutočné hospodárske výsledky sa budú odchýľovať od plánovaných.

Podnikateľské riziko je možné odstraňovať, alebo znižovať jeho prejavy rôznymi formami napr.: • rozložením do niekoľkých podnikateľských aktivít nepriaznivých dôsledkov, • pružným a pohotovým reagovaním na zmeny v dopyte, • rozložením rizika na viaceré podnikateľské subjekty, často na dodávateľa alebo zákazníka, • presunutím rizika na poistovňu, ktorá podľa poistnej zmluvy finančne pokrýva ďalšie riziká, alebo celkovú stratu.

V podnikoch patria medzi typické rizikové činnosti:
• Strategické plánovanie – identifikácia vonkajších hrozieb a príležitostí v hospodárskej súťaži, spolu so strategickými iniciatívami na ich riešenie.
• Marketing – pochopenie cieľového zákazníka, aby sa zabezpečili súlad výrobok / služba a požiadavky zákazníka.
• Zhoda a etika – sledovanie dodržiavania pravidel správania a zameranie na vyšetrovanie podvodov.
• Účtovníctvo / Finančná zhoda – identifikácia rizik finančného výkazníctva.
• Právne oddelenie – riadenie súdnych sporov a analýza nových právnych trendov, ktoré môžu mať vplyv na organizáciu.
• Poistenie – zabezpečenie správneho poistenia pre organizáciu.
• Finančná správa – zaistenie dostatočnej hotovosti pri splnení obchodných potrieb a riadenie rizík v súvislosti s tvorobou cien alebo devízami.
• Zaistenie kvality prevádzky – overovanie, či produkcia je v rámci toleranci.
• Riadenie prevádzky – zabezpečenie každodenného činnosti a rozlišenie súvisiacich rizíkov.
• Úver – zaistenie, že každý úver poskytnutý zákazníkom, zodpovedá ich platobnej schopnosti.
• Zákaznícky servis – zaistenie rýchleho riešenia st'ažností zákazníkov a hlásenia príčin na rozhodovanie o prevádzke.
• Vnútorný audit – vyhodnotenie účinnosti každého z vyššie uvedených rizík činnosti a odporúčanie na zlepšenie.

c) Štandard Inštitútu riadenia rizík uvádza ako hlavné riziká strategické, finančné a prevádzkové, okrem toho aj riziká správy vedomostí a riziká zhody s právnymi požiadavkami.

Z uvedeného vyplýva, že v každej oblasti činnosti organizácie je množstvo rizík, ktoré môžu mať pozitívne alebo negatívne následky. V ďalšom budú uvedené niektoré závažné špekulatívne riziká, ktoré majú najväčší vplyv na podnikanie, ale aj na bezpečnosť, napr. strategické, finančné, prevádzkové, poistné, právnej zhody.

### Strategické riziká

Strategické riziká sa týkajú dlhodobých strategických cieľov organizácie. Sú tie interné alebo externé neistoty, ktoré majú vplyv na stratégie organizácií a/alebo implementáciu ich stratégii. Na jednej strane sú zdrojom príležitostí, ale aj možným zdrojom strát, ktoré by mohli vzniknúť následkom neúspešného podnikateľského plánu, zlého podnikateľského rozhodnutia, nesprávneho rozdeľovania zdrojov alebo zo zlyhania správnej reakcie na zmeny v podnikateľskom prostredí. Medzi strategické riziká patria najmä:

**a) Vonkajšie strategické riziká:**
- konkurencia, zmeny v dopyte, zmeny v odvetví, zastarávanie, požiadavky zákazníkov,
- riziká spojené s výkonnou mocou, politické riziká, politika vlády, verejná mienka, zmena ideológie, zmeny kompetentných orgánov, právne a verejnoprávne zmeny, sociálne trendy, nepokoje,
- nadnárodné spolužitie, účasť v politicko-hospodárskych zoskupeniach a celková svetová politická klima,
- zmeny v životnom prostredí.

**b) Vnútorné strategické riziká:**
- politika, ciele a stratégie organizácie, nesprávne alebo zle implementované stratégie, nedostatočné riadenie,
- plánovanie – požiadavky na povolenie, zabezpečenie zdrojov, sociálno-ekonomické dopady,
- organizovanie – veľký počet organizačných úrovni, nejasne stanovené práva a povinnosti, kompetence a vzájomný spôsob spolupráce, prílišná centralizácia,
- výskum a vývoj, fúzie a akvizície, dostupnosť kapitálových prostriedkov, nedostatok ľudských zdrojov, duševný kapitál,
- právna zhoda,
- povest’ organizácie (reputačné rizikó).

### Finančné riziká

**Finančné riziko** je zastrešujúci termín pre rôzne typy rizík spojených s financovaním, vrátane finančných transakcií, ktoré zahŕňajú firemné úvery v riziku nezaplatenia. Riziko je termín často používaný s významom rizika negatívneho vývoja, čo znamená neistotu návratnosti a potenciál pre finančnú stratu (Horcher, 2005). Medzi finančné riziká patria najmä:

- politika finančnej správy, dane, nákladová inflácia,
- zahraničné investičné riziká (výmenné kurzy),
- úrokové sadzby, úverové riziká (dostupnosť), akciové riziká, rizikó likvidity, komoditné riziká,
- pät’ kategórií investičných rizík – trhové riziká, riziko spojené s poklesom popularity aktíva, riziko vnútornej hodnoty, zvyškové riziko, riziko prisudzovania nestability,
- bankrot,
- poistenie,
- Cash Flow.
Prevádzkové riziká

Prevádzkové riziká (niekedy tiež výrobné riziká) v manažérstve rizík je pojem, ktorý označuje druh podnikateľského rizika. Ide o širokú oblasť, ktorú sa zameriava na riziká vyplývajúce z ľudí, systémov a procesov, prostredníctvom ktorých spoločnosť pôsobí. Prevádzkové riziko so sebou prináša možnosť vzniku krízy organizácie narušením procesu kontinuity prevádzkových činností.

Zdroje prevádzkových rizík podľa publikácie Krízový manažment vo verejnej správe (Šimák, 2006) môžu byť:
- vnútorné – ekonomické, technické a technologické, sociálne, manažérske,
- vonkajšie – politické, právne, sociálne, prírodne, surovinové, ekonomické, finančné.

Medzi konkrétne prevádzkové riziká patria napríklad:

a) Vonkajšie riziká:
   - vonkajšie prostredie, živelné pohromy, počasie, zemetrasenie,
   - požiar alebo explózie,
   - nedostatok pitnej a úžitkovej vody,
   - zmluvy, dodávatelia,
   - archeologický prieskum,
   - predpisy, kultúra,
   - dodávateľskej reťaze.

b) Vnútorné riziká:
   - organizovanie a vedenie prevádzkových procesov: neúplné uverejňovanie, prípadné utajovanie záverov z problémov vo vedení spoločnosti, nedostatočné a nekonkrétne rozdelenie zodpovedností, nedostatočné delegovanie právomoci, nevhodná reštrukturalizácia, snaha zložiť odlišné prevádzky a pracovné postupy, ktoré nie sú schopné kooperovať, strata dôvery vo vedení, v koncepcií a výrobnom program;
   - plánovanie: neúplné a nedôsledné plánovanie, plánovanie len na niektorých stupňoch vertikálnej štruktúry, nepodrobné schvaľovacie procedúry plánovacích dokumentov, nepremyslené aplikovanie nových technológií, nedostatočne doriešené vzťahy s tretími stranami a závislosť od nich,
   - kontrolná činnosť: nedostatočné monitorovanie výrobných i manažérskych činností, slabé prevádzkovo-kontrolné mechanizmy, nedostatočná práca s výsledkami kontrolnej činnosti,
   - ľudský faktor – strata kľúčových zamestnancov, nevhodné správanie sa zamestnancov, nedostatočná vzdelenosť úrovní, nekompetentnosť, chyby a omyly zamestnancov, ignorancia, únava a vyčerpanie, komunikačná schopnosť, kultúra, práca v noci a za zniženej viditeľnosti,
   - technika a technológia – prevádzková nespoľahlivosť, nebezpečenstvo priemyselných a iných havárií, kolízie, kolaps, výpadky elektrickej energie, poruchy, fyzické poškodenie majetku alebo výrobkov, narušenie infraštruktúry,
   - informačné a komunikačné technológie,
   - nenutelnosti, produkty a služby,
   - bezpečnostná kultúra organizácie,
   - dalšie riziká: krádeže, podvody, právne riziká, zdravotnícke alebo environmentálne riziká, spojené s rizikom zákazníkov.

Široko používanú definíciu prevádzkového rizika uvádza výbor druhej Bazilejskej zmluvy (Basel II): *prevádzkové riziko je riziko straty, vyplývajúce z neprimeraných činností alebo zlyhania vnútorných procesov, ľudí a systémov alebo následkom vonkajších udalostí.*
Typické kategórie prevádzkového rizika podľa Bazilejskej zmluvy:

1. vnútorný podvod – sprenevera finančných aktiv, daňové úniky, úmyselné poškodenie pozícií na trhu, úplatkárstvo (korupcia),
2. externý podvod – krádež informácií, poškodenie hackermi, krádež v prospech tretej strany a falošovanie,
3. postupy pri zamestnávaní a bezpečnosť na pracovisku – diskriminácia, mzda zamestnancov, bezpečnosť a ochrana zdravia zamestnancov,
4. klienti, produkty, a obchodné praktiky – manipulácia trhu, protimonopolné, neoprávnený obchod, chyby výrobku, narušené dovery,
5. škody na hmotnom majetku – prirodzene katastrofy, terorizmus, vandalizmus,
6. prerušenie prevádzky a zlyhanie systémov – prerušenie funkcie, poruchy softvéru, zlyhanie hardvéru,
7. vykonávanie transakcií, dodávky a riadenie procesu – chyby vstupných dát, účtovné chyby, poruchy softvéru, zludnutie alebo neachválené poruchy systémov.


Riadenie prevádzkového rizika sa liši od ostatných druhov rizík, pretože sa nepoužíva na generovanie zisku (napr. úverové riziko sa využíva na požičiavanie inštitúciám vytvárať zisk, trhové riziko sa využíva na obchodných procesoch) a manažéri fondov a poistovcov rizika sa využíva v poisťovniach). Všetci však riadi prevádzkové riziko, aby sa straty pohybovali v rámci ich rizikovej tolerancie – veľkostí rizika, ktorú sú pripravení prijať pri dosahovaní svojich cieľov.

V praxi to znamená, že organizácia toleruje, že ich ľudia, procesy a systémy sú nedokonalé, a že straty budú vytvárať z chýb a neefektívnych činností. Veľkost straty sú ochotní akceptovať, pretože náklady na nápravu chyby alebo zlepšenie systémov sú neprimerané vzhľadom na príjomy, ktoré dosiahnu, čo určuje ich toleranciu na prevádzkové riziko.

Ak napríek prijatým opatreniam dôjde k havárii, je nutné sa intenzívne venovať odstráneniu jej následkov, aby sa minimalizovali vplyvy súvisiace s prerušením výroby.

Poistné riziko


Riziko súladu s právnymi požiadavkami

Toto riziko zahŕňa oblasti, akými sú bezpečnosť a ochrana zdravia pri práci, otázky životného prostredia, obchodné procesy, ochranu zákazníka, ochranu informácií, postupy pri najímaní pracovníkov, nové regulátne požiadavky, ktoré sú upravované právnymi normami.
4.2 LITERATÚRA

ŠIMÁK, L. [2006]: Manažment rizika. Žilina: EDIS – vydavateľstvo ŽU.
5 BEZPEČNOSTNÉ RIZIKÁ

Fyzická bezpečnosť objektu či organizácie sa odvíja od bezpečnostných rizík (rizik bezpečnosti). Keby žiadne bezpečnostné riziká neboli, nemusela by sa bezpečnosť vôbec riešiť. Ideálnym cieľom bezpečnostnej politiky by mala byť snaha o modifikáciu všetkých bezpečnostných rizík. To však v praxi nie je možné, pretože modifikovať všetky riziká by stálo nekonečné množstvo opatrení a organizácia má vždy iba obmedzený limit prostriedkov, ktoré môže do svojej bezpečnosti vložiť.

Táto veľkosť prostriedkov záleží na rozhodnutí vrcholového manažmentu a je v každej organizácii iná. S nimi je možné modifikovať najzávažnejšie bezpečnostné riziká, avšak nikdy sa nepodarí pokryť všetky. Ak má organizácia nulové výdavky na bezpečnosť, nemodifikuje žiadne riziká, teda aj tie najvážšie bezpečnostné riziká pretrvávajú.

Efektívna je len taká bezpečnosť, kde sa na bezpečnosť nevydáva viac, ani menej prostriedkov, než je suma hodnôt nerušených rizík.

Bezpečnostné riziká (čisté riziká) tvoria špecifickú kategóriu rizík, ktoré majú svoj zdroj v určitej nebezpečnosti.

Nabespečenstvo predstavuje zdroj možného poškodenia, môže byť zdrojom rizika. Nabespečenstvo, ako zdroj rizika, je vlastnosť alebo schopnosť objektu (systému, stroja, materiálu, výrobnej technológie a pracovnej činnosti, prípadne ich komponentov) spôsobovať nebezpečné udalosti, ktoré môžu narušiť bezpečnosť, ohroziť stabilitu a fungovanie príslušného systému, prípadne aj jeho okolia.

Pravdepodobnosť výskytu a možný následok úmyselnej alebo náhodnej nebezpečnej udalosti predstavuje konkrétne rizíko, že dojde k ujme na zdraví zamienanca, zákazníkov a ostatných osôb, hmotných a nehmotných aktivách organizácie, životnom prostredí alebo ohroziť činnosti a ciele organizácie.

Bezpečnostné riziká vo všetkých prípadoch vyjadrujú len miernu ohrozenia, nikdy nepredstavujú príležitosť. Bezpečnostné riziko je preto kombináciou pravdepodobnosti výskytu určitej nebezpečnej udalosti a jej potenciálnych následkov (škody).

Rozdelenie bezpečnostných rizík

V závislosti od druhu nebezpečenstva ako zdroja, a spôsobov jeho prejavu možno bezpečnostné riziká deliť na:

a) Riziká úmyselného napadnutia (riziká úmyselného ohrozenia bezpečnosti) – Security risks,
b) Náhodné Bezpečnostné riziká (riziká náhodného ohrozenia bezpečnosti) – Hazard risks.
5.1 NEBEZPEČENSTVO

Nebezpečenstvo *(hazard)* predstavuje subjektívny pojem, ktorý sa vzťahuje na náhodné možnosti, pri ktorých hmota, priestor, informácie, energie alebo spoločne môžu mať vplyv na komplexný systém, čo môže mať určité následky na systém alebo sa môže partnermi v podnikaní (na úrovni myšlenia, cítenia alebo inštinktu) v určitej fáze vývoja vnímať negatívne *(Zaplatiniskyj, 2013)*.

Sperber charakterizuje **nebezpečenstvo** ako akýkoľvek *mechanický, biologický, chemický, ekologický, fyzikálny alebo sociálny faktor*, ktorý môže potenciálne spôsobiť zranenie alebo smrť osôb alebo iných organizmov, škody na majetku alebo životnom prostredí *(Sperber, 2001)*.

Všeobecne možno hovoriť o nasledujúcich možnostiach vzniku nebezpečenstva:

1. **prítomnosť akumulovanej energie**, ktorá pri uvoľnení môže spôsobiť škodu, táto uložená energia sa môže objaviť v mnohých podobách: *chemickej, mechanickej, tepelnej, rádioaktivnej, elektrickej atď.*,  
2. **prítomnosť nebezpečných látok**,  
3. podmienky pre vznik nebezpečných situácií, napr.: *obmedzené alebo ohraničené priestory východov, priestory so zníženým obsahom kyslíka, nevhodne umiestnené stanoviska, opakujúce sa pohyby, nízko visiaci alebo vyčnievajúce predmety a pod.*  

**Nebezpečné látky**

Nebezpečné látky sú podľa Zákona o civilnej ochrane obyvateľstva *prijímané alebo syntetické látky, ktoré svojimi chemickými, fyzikálnymi, toxikologickými alebo biologickými vlastnosťami samostatne alebo v kombinácii môžu spôsobiť ohrozenie života, zdravia alebo majetku.*

Európska dohoda o medzinárodnej cesťnej preprave nebezpečných vecí – ADR *(Accord Européen au transport international des Marchandises par route)* definuje **nebezpečné veci** ako *látka a predmety*, ktorých preprava je podľa ADR zakázaná, alebo sa povoľuje len za podmienok uvedených v ADR.

**Nebezpečné veci (látka a predmety)** podľa ADR:  
1. Výbušné látky a predmety.  
2. Plyn.  
3. Horľavé kvapalné látky.  
4.1. Horľavé pevné látky, samovoľne reagujúce látky a pevné znecitlivene výbušniny.  
4.2. Samozápalné látky (látky náchylné na samovoľné horenie).  
4.3. Látky, ktoré pri styku s vodou vyvíjajú horľavé plyny.  
5.1. Oxidujúce látky.  
5.2. Organické peroxidy.  
6.2. Infekčné látky.  
7. Rádioaktívny materiál.  
8. Žieravé látky.  
9. Rôzne nebezpečné látky a predmety.

Vzhľadom na svoju povahu nebezpečenstvo zahŕňa niečo, čo by potenciálne mohlo byť škodlivé pre život človeka, zdravie, majetok alebo životné prostredie. Medzi nebezpečenstvá, ktoré znamenajú pre organizáciu vždy pravdepodobnosť straty možno zaradiť najmä
nebezpečenstvá: biologické, chemické, fyzikálne, mechanické, ergonomické, technologické, sociálne (societálne), psychologické, ekologické, prírodné.

**Biologické nebezpečenstvo**

Nariadenie vlády SR č. 83/2013 Z. z. o ochrane zdravia zamestnancov pred rizikami súvisiacimi s expozíciou biologickým faktorom pri práci ustanovuje požiadavky na ochranu zdravia a bezpečnosti zamestnancov pred rizikami z expozície biologickým faktorom pri práci a na predchádzanie týmto rizikám pri všetkých činnostiach, pri ktorých zamestnanci sú alebo môžu byť pri práci exponovaní biologickým faktorom.

**Na účely tohto nariadenia:**

**a) Biologické fakty**

- mikroorganizmy vrátane geneticky modifikovaných mikroorganizmov,
- bunkové kultúry a ľudské endoparazity, ktoré môžu vyvolať nákazu, alergiu alebo toxický účinok u ľudí,
- prióny, ktoré môžu spôsobiť u ľudí prenosné ochorenie.

**b) Mikroorganizmy** sú mikrobiologické bunkové alebo nebunkové jedince, ktoré sú schopné procesu zdvojenia alebo prenosu genetického materiálu, bunkové kultúry sú populácie buňiek získané kultiváciou mnohobunkových organizmov v laboratórnych podmienkach.

**c) Ostré zdravotnícke predmety** vrátane injekčných ihiel sú pracovné prostriedky používané na vykonávanie špecifických zdravotníckych činností, ktorými sa dá ponechať, pichnúť, spôsobiť poranenie alebo nákazu.

V prílohe č. 1 k Nariadeniu vlády č. 83/2013 Z. z. je uvedený vzorový zoznam prác s biologickými faktormi:

1. Práca v potravinárskom priemysle.
2. Práca v poľnohospodárstve.
3. Pracovné činnosti, pri ktorých dochádza k styku so zvieratami a výrobkami živočíšneho pôvodu.
4. Práca v zdravotníctve vrátane izolačných jednotiek a patológii.
5. Práca v klinických, veterinárnych a diagnostických laboratóriách vrátane diagnostických mikrobiologických laboratórií.
6. Práca v zariadeniach sociálnych služieb, zariadeniach sociálneoprávnej ochrany detí a sociálnej kurately a iné špecifické činnosti v sociálnej oblasti napríklad sociálna práca v otvorenom prostredí so závislými osobami.
7. Práca v závodech na likvidáciu odpadov.
8. Práca v čistiarňach odpadových vôd.

**Chemické nebezpečenstvo**

Prehľad látok, ktoré predstavujú chemické nebezpečenstvá je uvedený v

- Nariadení Európskeho parlamentu a Rady (ES) č. 1907/2006 o registrácii, hodnotení, autorizácii a obmedzovaní chemických látok (REACH),
- Nariadení Európskeho parlamentu a Rady (ES) č. 1272/2008 o klasifikácii, označovaní a balení látok a zmesí,
- Zákone č. 67/2010 Z. z. o podmienkach uvedenia chemických látok a chemických zmesí na trh a o zmene a doplnení niektorých zákonov (chemický zákon).
Podľa Zákona č. 163/2001 Z. z. o chemických látkach a chemických prípravkoch **nebezpečné chemické látky a nebezpečné chemické prípravky** pre život a zdravie ľudí a pre životné prostredie sú:

a) Výbušné látky a prípravky.
b) Oxidujúce látky a prípravky.
c) Mimoriadne horľavé látky a prípravky.
d) Veľmi horľavé látky a prípravky.
e) Horľavé látky a prípravky.
f) Veľmi jedovaté látky a prípravky.
g) Jedovaté látky a prípravky.
h) Škodlivé látky a prípravky.
i) Žieravé látky a prípravky.
j) Dráždivé látky a prípravky.
k) Senzibilizujúce látky a prípravky.
l) Karcinogénne látky a prípravky.
m) Mutagené látky a prípravky.
n) Látky a prípravky poškodzujúce reprodukciu.
o) Látky a prípravky nebezpečné pre životné prostredie.

Z hľadiska objektu pôsobenia sú nebezpečné chemické látky a nebezpečné chemické prípravky rozdelené na dve skupiny:

- Nebezpečné chemické látky a nebezpečné chemické prípravky **pre ľudí** sú látky a prípravky uvedené v písmenách **f až n**, ktoré môžu spôsobiť smrť, krátkodobé, dlhodobé alebo opakúvané poškodenie zdravia, ak sú vdychované, požívané alebo absorbované počúvaním.
- Nebezpečné chemické látky a nebezpečné chemické prípravky **pre životné prostredie** sú látky a prípravky uvedené v písmene **o**, ktoré ak sa dostanú do životného prostredia, môžu predstavovať okamžité alebo neskoršie nebezpečenstvo pre jednu alebo viac zložiek životného prostredia.

Chemické látky, ktoré boli vytyčované pre použitie ako chemické zbrane, sa zaradzujú do spoločnej skupiny pod názvom **otravné látky**. Sú to chemické zlúčeniny alebo zmesi, ktoré po zasiahnutí organizmu spôsobujú jeho poškodenie alebo usmrtenie a stážujú používanie zamezeného materiálu a techníky.

Z hľadiska toxicity sa otravné látky delia do týchto skupín:

1. Nervovoparalytické, najúčinnejšie z nich sú sarin, soman, látka VX a IVA.
2. Pľuzgierotvorné, ktorých hlavným predstaviteľom je yperit.
3. Dusivé, ako sú chlór, chlórpikrín, fosgén a difosgén, v súčasnosti sem patri aj čpavok.
4. Psychoaktívne, tzv. halucinogény, z ktorých bola vytyčovaná látka s krycím názvom BZ.
5. Všeobecne jedovaté, z nich sú všeobecne známe oxid uhlíka (CO), kyanovodík a sírouhlík.
6. Dráždivé, ktoré podľa miesta ich hlavného účinku delíme na:
   a) lakrimáty, ktoré dráždia hlavne oči,
   b) sternity, hlavným miestom ich pôsobenia sú horné cesty dýchacie,
   c) predstaviteľom dráždivých látok je látka s krycím názvom CS, ktorá rovnako dráždi oči i dýchacie cesty.
**Fyzikálne nebezpečenstvo**

Fyzikálne nebezpečenstvo je definované ako „faktor v prostredí, ktorý môže poškodiť telo, bez toho, že by sa ho nevyhnutne dotýkal. Typickými faktormi fyzikálneho nebezpečenstva sú vibrácie a hluk“.

Fyzikálne nebezpečenstvo je najbežnejšie a je prítomné vo väčšine pracovisk v tej či onej podobe. Zahrňá nebezpečné podmienky, ktoré môžu spôsobiť zranenie, chorobu a smrť, v niektorých prípadoch intenzívny stres. Nebezpečenstvá spôsobené ľudskou činnosťou môžu nevhodným zasahovaním do prírody spôsobiť aj problémy spojené s povodňami, kolísaním klímy a frekvenciou búrok ako prírodných prvkov.

Fyzikálne nebezpečenstvá môžu byť prirodzené alebo spôsobené ľudskou činnosťou. Zahrňujú elektrinu, žiarenie, tlak, hluk, vibrácie, výšky, zemetrasenie, záplavy, tornáda a mnoho ďalších faktorov.

**Ergonomické nebezpečenstvo**


Ergonomické nebezpečenstvo zahŕňa problémy ako: opakujúci sa pohyb, ručná obsluha, pracovisko/ druh a cieľ práce, nepohodlné pracovné miesto (sedieť alebo stáť), zlé polohy tela, nevhodné usporiadanie a prevádzka zariadení, zlé umiestnenie počítačových systémov, hluk, osvetlenie, tepelná pohoda a pod.

**Psychologické nebezpečenstvo**

Práca je všeobecne prospešná pre duševné zdravie a osobnú pohodu. Poskytuje ľuďom struktúru, účel a zmysel života, príležitosť pre rozvíjanie a využitie svojich schopností, tvori sociálne vzťahy a zvyšuje ich pocit vlastnej hodnoty. Existujú však okolnosti, v ktorých môžu práca mať nepriaznivé dôsledky na duševné zdravie, napríklad vymývanie mozgu, šikanovanie, vysmievanie atď. Môže vzniknúť z organizačných alebo osobných faktorov, pričom hlavným faktormi sú zlá organizácia práce a pracovných príležitostí, zlá komunikácia a medziľudské vzťahy, šikanovanie, pracovné násilie a únava.

Následkom býva stres, násilie a ďalšie napätie spojené s pracou alebo životným prostredím alebo môžu nastať v prípade rozvodu, smrti, zmeny pracovného miesta a pod. Závisí to aj od biologických činiteľov (vrodene vlohy) a sociálnych činiteľov (výchova, učenie). Nebezpečenstvo pre duševné zdravie v dôsledku práce je potrebné vnímať rovnakým spôsobom ako pri ostatných zdravotných a bezpečnostných rizikách a záväzok na prevenciu stresu pri práci by mal byť zahrnutý do politiky bezpečnosti a ochrany zdravia organizácie.

**Mechanické nebezpečenstvo**

Mechanické nebezpečenstvo (Mechanical Hazard) je akékoľvek nebezpečenstvo, týkajúce sa činností strojov, použitia nástrojov a náradia a činností. Mechanické nebezpečenstvo predstavujú motorové vozidlá, lietadlá, a airbagy, stlačené plyny alebo kvapaliny. Stroje môžu byť pohárané elektrický alebo ľudskou silou. Nástroje a náradie môžu predstavovať nebezpečenstvo na troch miestach:
a) bod prevádzky – bod, v ktorom sa činnosť vykonáva, napr. hrot vrtačky, šmírľový papier na ručnej brúske, vibrujúcí koniec na masážnom stroječku,
b) bod prenosu energie – miesto, kde sa aplikovaná energia premieňa na prácu, napr. remenica a remen na priehradu, ostré alebo vyčnievajúce body alebo kovové časti na remenici a ostré nástroje či zbrane.
c) priestor pohyblivých častí – zahŕňa všetky činnosti medzi bodom prevádzky a bodom prenosu energie, napr. kolesá alebo kladky na prístroji, ostré alebo vyčnievajúce body alebo kovové časti na remenici a ostré nástroje či zbrane.

Technologické nebezpečenstvo

Nebezpečenstvo pochádzajúce z technologických alebo priemyselných podmienok, vrátane porúch, nebezpečných postupov, zlyhania infraštruktúry alebo špecifickéj ľudskej činnosti, ktoré môžu spôsobiť straty na životoch, zranenia, choroby alebo iné zdravotné poškodenie. Príklady technologických nebezpečenstiev zahŕňajú priemyselné znečistenie, jadrové žiarenie, toxické odpady, zrušenie konštrukcie, narušenie priehrady, havárie v doprave, stavebnictve a výrobe, továrenské výbuchy, požiare a únik chemikálií.

Technologické nebezpečenstvá môžu tiež vzniknúť ako priamy dôsledok udalostí týkajúcich sa prírodných katastrof, ako to bolo v prípade výbuchu dvoch jadrových reaktorov vo Fukušime v Japonsku po cunami, ktorá sprevádzala zemetrasenie.

Sociálne nebezpečenstvo

K sociálnym nebezpečenstvám patria:
• nestabilita zamestnanosti, znížuje sa dostupnosť stabilného zamestnania, obmedzená schopnosť reagovať na zmeny na pracovnom trhu,
• nárast dlhodobej nezamestnanosti vytvára podmienky pre sociálne deviantné správanie, domáce násilie, alkoholizmus, drogovú a inú závislosť, kriminalitu, vandalizmus,
• zmeny vo vzdelanosti a postavení žien prinášajú ich zrovnoprávnenie na pracovnom trhu, na druhej strane dochádza k zle zvládnejnej zmeny v zabezpečení sociálnej starostlivosti v rodinách a k jej finančnému podhodnoteniu,
• nárast potreby sociálnej starostlivosti o starých, chorých, hendikepovaných, rozpor medzi štátnymi a súkromnými poskytovateľmi sociálnych služieb,
• pokles životnej úrovne a kvality života u určitých skupín obyvateľstva, alebo výskyt sociálnych skupín obyvateľstva.

Prírodné nebezpečenstvá

Prírodné nebezpečenstvá sú prirodzene sa vyskytujúce fyzikálne javy, ktoré spôsobujú buď rýchly, alebo pomalý nástup udalosti, medzi ktoré možno zaradiť:
• geofyzikálne – zemetasenia, zosuwy pôdy, cunami a sopečná činnosť,
• hydrologické – laviny a záplavy,
• klimatologické – extrémne teploty, sucho a požiare,
• meteorologické – cyklóny a búrka/zdvúvanie vln,
• biologické – nákažlivé choroby a epidémie spôsobené hmyzom / zvieratami.

Treba rozlišovať aj medzi rýchlostou napadnutia prirodzým nebezpečenstvom, technologickým nebezpečenstvom a sociálnym nebezpečenstvom a následkami poškodenia životného prostredia, ako je rozšírenie púšti a sucha, ktoré sú popísané náhlym výskytom a relatívne krátkou dobu trvania (McGuire a iní, 2002).

Nebezpečenstvo na pracovisku

Na identifikáciu nebezpečenstiev a ohrozenia na pracovisku možno použiť univerzálny kontrolný zoznam nebezpečenstiev, ktorý vypracovala Európska agentúra pre bezpečnosť a ochranu zdravia pri práci. Na jednotlivých pracoviskách je však potrebné individuálne vyhádzať z reality prostredia a taktiež z pracovných činností toho ktorého pracoviska.

V univerzálnom zozname nebezpečenstiev (ohrozenia) sú zaradené:
• nerovné a šmykľavé povrchy, ktoré môžu spôsobiť pošmyknutie, zakopnutie, pád a pod., objekty a časti s nebezpečným povrchom (ostré, drsné a pod.); horúce a chladné povrchy, materiály atď.; horúce a studené klimatické prostredie,
• pohyblivé dopravné prostriedky a stroje, pohyblivé časti strojov,
• pracoviská vo výške a miesta výstupu s možnosťou pádu z výšky, práca v nepriaznivej polohe, zdvihanie a manipulácia s bremenami,
• ručné nástroje,
• elektrické inštalácie a zariadenia,
• možnosť vzniku požiaru, možnosť vzniku výbuchu,
• vysoký tlak, hluk,
• vibrácie rúk, vibrácie celého tela,
• osvetlenie,
• UV žiarenie, infražiarenie, laserové žiarenie, mikrovlnné žiarenie, elektromagnetické polia,
• chemické látky vrátane prachu v ovzduší,
• biologické nebezpečenstvo (virusy, parazity, plesne, baktérie),
• stres, násilie, obťažovanie (mobbing) a iné nebezpečenstvo (ohrozenie).
5.2 RIZIKÁ ÚMYSELNÉHO NAPADNUTIA

Riziká úmyselného napadnutia môžu spôsobiť *ujmu úmyselným konaním*. Znamenajú pravdepodobnosť, že dôjde k ohrozeniu chráneného záujmu (hodnoty) kriminálnym činom iných ľudí a veľkosť možných následkov takejto udalosti (napr. pravdepodobnosť a následky vlámania).

Podrobnejšia definícia podľa Talbota a Jakemana je: „riziko úmyselného napadnutia je *udalosť*, ktorá by mohla viešť k ohrozeniu aktív organízačie, t. j. neoprávnené použitie, strata, poškodenie, prezradenie alebo upravenie aktív organízačie pre získ, osobný záujem alebo politické záujmy jednotlivcov, skupín alebo iných entít, ktoré predstavujú ohrozenie aktív a zahrňajú riziko zranenia ľudí. Ohrozenie aktív môže negatívne ovplyvniť organizáciu, jej prevádzkové jednotky a klientov. Z toho dôvodu je posúdenie bezpečnostných rizík dôležitou súčasťou riadenia rizík“ (Talbot, Jakeman, 2009).

Udalosť – v bezpečnostnom význame zahŕňa tie činnosti, ktoré vykonávajú aktérov zámerne, na účely, ktoré negatívne ovplyvňujú organizáciu a dosahovanie jej cieľov. Úloha aktérov a zámeru udalosti umožňuje oddelenie týchto rizík od iných oblastí rizík, a to najmä od rizík životného prostredia, prevádzkových rizík a finančných rizík.

*Zdrojom úmyselného napadnutia* je teda cieľavedome konajúca fyzická osoba, pričom motiv takéhoto konania môže byť:

- politický, alebo politicko-vojenský, vyplývajúci z politických, vojenských alebo ekonomických záujmov štátov (napr. spravodajské služby),
- ideologický, viažuci sa na určitý politický a/alebo ideologický systém (napr. politický terorizmus, extremismus, náboženský fundamentalizmus, ekologický radikalizmus a pod.),
- ekonomický, založený na snahe o bezprávny zisk (kriminálni jedinci a zločinecké skupiny), alebo poškodenie konkurencie (odporcovia, konkurenti, komerčné spravodajské služby),
- osobný, vyvolaný napr. pocitom nenávisti, krivdy, vydieraním vlastnej osoby alebo ohradzovaním rodinného príslušníka, povahovými črtami osoby a pod.

Medzi *riziká úmyselného napadnutia* možno zaradiť:

1. Sociálnopolitické riziká:
   - vzbury, pouličné nepokoje a teroristické incidenty (Alexander, 2000),
   - rabovanie – nekontrolované branie cudzích vecí a tovaru počas katastrofickej udalosti, či občianskych nepokoje vrátane vojny, kedy štátna zložky dozorujú, ale či ich možnosť riešiť situáciu nie je dostatočná vážne situácie, kedy štátna zložka môže dozorovať, ale mať riešiť situáciu.


3. Riziká úmyselného násilia proti osobám:
   - *fyzické násilie* – úmyselné použitie sily proti innej osobe, bez zákonného oprávnenia, čo môže mat’ za následok fyzické zranenie alebo osobnú ujmou, napr.: útok na zamestnanca, násilie voči skupine, nebezpečné vyhrážanie – vyhrážanie sa smrťou, ťažkou ujmou na zdravi alebo inou ťažkou ujmou takým spôsobom, že to môže vzbudit’ dôvodnú obavu u poškodeného alebo jeho blízkej osobe,
b) sexuálne násilie – forma diskriminácie na základe pohlavia, ktoré má svoje osobité prejavy, príčiny a vyžaduje si preto špecifické spôsoby eliminácie a prevencie. Ide o verbálne, neverbálne alebo fyzické správanie sexuálnej povahy, ktorého úmyslom alebo následkom je alebo môže byť narušenie dôstojnosti osoby a ktoré vytvára zastrašujúce, ponižujúce, nevylievané a / alebo urážlivé prostredie, c) nefyzické násilie – správanie, ktoré priamo naruša slobodnú vôleťu a sebaúctu iného človeka. Nezanecháva síce žiadne viditeľné poranenia, napriek tomu môže byť najhoršou formou násilia, často sa spája s fyzickým násilím. Znamená použitie nevýhodných slov alebo správanie, ktoré spôsobuje strach alebo môže byť zásah do slobody alebo ľudskej dôstojnosti, d) psychické násilie: • psychické násilie, psychický teror, vyhrážky, vulgárna a dotieravá konverzácia; nežiadu ce alebo hanlivé poznámky; ohováranie, • šikanovanie – opakované správanie, ktorého cieľom je vysmievať sa, ublížovať niekomu, ponižovať ho, agresor zneužíva svoju moc nad obeťou, • kyberšikanovanie (elektronické šikanovanie, kyberbullying, kybervictimizing) – forma šikanovania, pri ktorej sa používajú nové technológie, ako je počítač, internet, mobilný telefón. Prebieha vo virtuálnom priestore s využitím rôznych služieb a nástro
jov ako sú e-mail, IM (instant messenger – napr. Skype, ICQ), chat, diskusné fóra, sociálne siete, stránky na zverejňovanie fotografií a videí, blogy, SMS správy, telefonáty,

- kybernetické prenasledovanie (online prenasledovanie, kyberstalking) – neustále sledovanie niekoho vo virtuálnom prostredí, často spojené s obťažovaním, vyháňaním a zavražďovaním.

- happy slapping – násilné alebo sexuálne útoky na obete (často aj náhodne vybrané), ktoré sú natačané na mobilný telefón, útočníci videá ďalej rozposielajú alebo zverejňujú na internete.

- mobbing, čiže psychický teror – trvalé, systematické a intenzívne útoky, intrigy a šikanovanie väčšieho počtu pracovníkov alebo nadriadeného voči jednotlivcovi alebo menšej skupine.

Druhy mobbingu:
- bossing – mobing zhora,
- stalking – spôsob prenasledovania prostredníctvom telefonického teroru, vyháňanie sa násilím, verejné slovne napádanie, vyvolávanie pocitu strachu a znepokojenia,
- chairing – tvrdý, neférový a nekorektný boj ochádzakov o kreslo,
- staffing – správanie podriadených voči nadriadenému, ktoré ma za cieľ jeho zosadenie,
- verbaliz – sexuálne obťažovanie – verbálne, neverbálne alebo fyzické, ktorého úmyslem alebo následkom je a môže byť narušenie dôstojnosti osoby, a ktoré vytvára zastrašujúce, ponižujúce, nepríateľské alebo urážlivé prostredie,
- defaming – zosmiešňovanie, ohováranie, znevažovanie, útok na povesť jednotlivca, skupiny alebo organizácie na verejnosti,
- hightechmobing – právne, počítačových súborov alebo posielanie anonymných výhľadných e-mailov alebo vírusov.

4. Riziko úmyselného spôsobenia majetkovej újmy – úmyselné narušenie bezpečnosti majetku a infraštruktúry organizácie, čo môže spôsobiť majetkové škody, napr.:

- a) krádež – prisvojovanie si cudziej veci či hodnoty zmocnením sa tejto veci či hodnoty:
  - krádež vlámaním – vniknutie do uzatvoreného priestoru šľouchou, nedovoleným prekročením uzamknutia alebo prekročením inej zabezpečovacej prekážky s použitím sily,
  - prostá krádež – zlodej odcudzuje veci, pričom neprekoná Žiadne ochranné zabezpečenie, napr. vojde cez odomknuté dvere do miestnosti, kde sú veci bez dozoru alebo ukradne bicykel bez zámku opretý pred obchodom,
  - krádež zamestnancami (insider),

- b) lúpež (lúpež so zbraňou) – použitie násilných nebo hrozba bezprostredného násilia v úmysle zmocniť sa cudziej veci bez alebo s použitím zbrane,

- c) vandalizmus – úmyselné poškodenie alebo úmyselné zničenie veci, zlomyselné konačne, napr. páchateľ porozbíja okná na budove alebo poleje kyselinou motorové vozidlo atď.,

- d) sabotáž – obvykle utajené a často násilné, úmyselné a plánované narušenie funkčnosti či výkonnosti (dôležitého) zariadenia prostredníctvom jeho poškodenia alebo zničenia,

- e) podvod – obohatenie uvedením niekoho do omýlu alebo využitím omýlu niekoho a spôsobenie škody na cudzom majetku,
f) sprenevera – prisvojenie cudzej veci, ktorá bola zverená zamestnancovi, a spôsobenie škody na cudzom majetku,
g) špionáž – ohrozenie utajovanej skutočnosti,
h) úmyselné porušenie tajomstva – listového, bankového, tajomstva informácie, tajomstvo neverejného prenosu počítačových dát,
i) ďalšie spôsoby poškodzovania cudzej veci:
   • záskodnictvo, podpaľačstvo,
   • zničenie, poškodenie cudzej veci a spôsobenie škody na cudzom majetku,
   • fyzické poškodenie informačných a komunikačných technológií,
   • poškodenie technických zariadení – kanalizácia, vodovod, plynovod, vykurovanie,
   • úmyselný výbuch plynu,
   • použitie výbušniny,
   • poškodenie alebo ohrozenie prevádzky,
k. neoprávnené používanie cudzej vecí, či motorového vozidla.

4. Riziká úmyselného narušenia všeobecnjej bezpečnosti:
   a) útok na verejného činiteľa v organizácii v štádiu prípravy alebo pokusu,
   b) všeobecné ohrozenie.

5. Riziká úmyselného poškodenia životného prostredia – nezákonné nakladanie
   s odpadkami, vypúšťanie znečisťujúcich látok, znečisťovanie vôd a ovzdušia.

Vnútorné riziká spôsobené úmyselným konaním predstavujú najmä vlastní zamestnanci (oprávené osoby, ľudia, ktorí majú prístup k chráneným záujmom – insider), servisní zamestnanci, obslužný personál a pracovníci fyzickej ochrany (strážnej služby), ktorí môžu sami spáchat krádež, byť nápomocní vonkajšiemu páchateľovi pri preniknutí do chráneného priestoru alebo úmyselne vyvoláť haváriu v objekte (chránenom priestore), či spôsobiť inú udalosť s negatívnymi následkami.
5.3 NÁHODNÉ BEZPEČNOSTNÉ RIZIKÁ

Náhodné bezpečnostné riziká predstavujú akékoľvek biologické, chemické, mechanické, environmentálne, ergonomické, fyzikálne, psychologické alebo sociálne faktory, ktoré, ak nebudú riadené, môžu pravdepodobne spôsobiť nebezpečenstvo pre:

1. ľudí a iné organizmy – smrť, úraz, choroba a stres,
2. majetok – poškodenie majetku a ekonomická strata,
3. životné prostredie – úbytok rastlín a živočíchov, znečistenie a straty vybavenosti.

Podľa Štandardu Inštitútu riadenia rizík medzi náhodné riziká patria najmä riziká:

• súvisiace s bezpečnosťou zdravia pri práci (BOZP) – occupational health and safety – related risks,
• personálnej bezpečnosti – personnel security risks,
• bezpečnosti životného prostredia – environmental risks,
• požiaru a iných havárií – fire and other disasters,
• prírodných javov (živelných pohrům) – natural events,
• bezpečnosti priestorov – premises security risks.

5.3.1 Riziká bezpečnosti zdravia pri práci

Na základe nových právnych noriem EÚ sa mení prístup k riešeniu bezpečnosti a ochrany zdravia pri práci. Jednou zo základných zásad tohto prístupu je zásada, že pre dosiahnutie dobrej úrovne bezpečnosti a ochrany zdravia pri práci nestáči dodržiavať iba bezpečnostné predpisy, ale je nutné zaviesť aktívnu prevenciu do organizácie práce a pracovných podmienok. Je nutné aj nad rámec predpisov posudzovať, čo môže ohroziť ľudí pri práci, je nutné posudzovať riziká.


Riziko pri práci je vyjadrením pravdepodobnosti a závažnosti zranenia alebo ochorenia pôsobením nebezpečenstva.

Hlavným cieľom posudzovania rizík pri práci je ochrana zdravia a bezpečnosti zamestnancov. Posudzovanie rizik môžu minimalizovať možné poškodenie zamestnancov, alebo životného prostredia zavineného pracovnou činnosťou. Posudzovanie rizíka pomáha taktiež pri udržaní konkurenceschopnosti a podávaní efektívnych výkonov v spoločnosti.

Podľa platných právnych predpisov majú všetci zamestnanci právo aktívne sa podieľať na pravidelnom posudzovaní rizík pri práci. Jednou z príčin nedostatočného uplatňovania posudzovania rizík v praxi je aj zbytočný rešpekt k samotnej procedúre. Mnohí vidia v posudzovaní rizík zložitú vedu a neodvážia sa sami logicke, „prostým sedliackým rozumom“ posúdiť, čo môže ľuďom ublížiť.

Posudzovanie rizík môže zvládniť každi zamestnanec na svojom úseku aj sám, už aj z toho dôvodu, že svoje pracovisko dobre pozná a prežije na ňom minimálne jednu tretinu dňa. Posudzovanie rizík je aj akousi filozofiou, prístupom, ktorý je potrebné zaviesť v spoločnosti, aby všetci zamestnanci boli zainteresovaní na odhaľovaní toho, čo môže spôsobiť nežiaducu udalosť.
Riziká bezpečnosti zdravia pri práci a riziká životného prostredia sú samostatné oblasti, ale často sú prepojené. Jedna z najsilnejších väzieb medzi nimi je, že jediná riziková udalosť môže mať následky vo všetkých oblastiach, aj keď v priebehu rôznych časových rám-cov. Napríklad môže nastať nekontrolovaný únik radiácie alebo toxických chemických látok s bezprostredným krátkodobým dopadom na bezpečnosť, dlhšie trvajúce zdravotné následky a ešte oveľa dlhodobejší vplyv na životné prostredie.

Udalosti, ako Černobyľ, napríklad spôsobili okamžité úmrtia a v dlhodobejšom horizonte úmrťa v dôsledku rakoviny, a zanechali aj hlboký dopad na životné prostredie, čo vedie k vročeným chýbám, vplyvu na životné prostredie. Analýza rizík pre životné prostredie je odbor, ktorý sa snaží pochopiť akcie a činnosti, ktoré prinášajú riziko pre ľudské zdravie alebo životné prostredie (Gurjar, Mohan, 2002).

Riziká BOZP predstavujú nasledujúce skupiny rizík:
• fyzikálne riziká,
• mechanické riziká,
• ergonomické riziká,
• biologické riziká,
• chemické riziká.

Fyzikálne riziká
• Poloha pracoviska vo vzťahu k povrchu zeme, napríklad vo výške, v hĺbke, pod zemou, alebo pod vodou, napríklad v jeho blízkosti.
• Práca s mobilným zariadením, ako sú vysokozdvižné vozíky.
• Nevhodné pristroje podľa a komunikácií spôsobujúci pády osôb, napríklad ich pohyblivosť, šikmota, šmykľavosť, nerovnosť.
• Tlak, úder, rez, seknutie, pichnutie, bodnutie, odretie, navinutie pri pohyblivých strojoch, mechanizmoch a ich častiach, na materiáloch, polotovaroch a výrobkoch, s ktorými sa manipuluje, na ostrých hranách, rohoch, drsných povrchoch.
• Oheň, horúce, alebo chladné látky (plynné, kvapalné, tuhé) a predmety, ich povrchová teplo.

Mechanické riziká
• Prístroje alebo nástroje, ktoré rotujú – môžu zachytiť šaty, vlasy a šperky obsluhy, napr. špirálový vrták, rotor odstredívky, prístroje na ukážku odstredivej sily, hriadeľ elektrického motora, pletacie stroje, kolesá a iné zariadenia.
• Ručné odstredivky.
• Nože, kladivá, skrutkovače, nastaviteľné kľúče, kliešte, pilníky.
• Elektrické ručné náradie.

**Ergonomické riziká**

• Zlé osvetlenie.
• Nesprávne upravené pracovné stanice a stoličky.
• Časté zdvihánie a manipulácia s ťažkým nákladom.
• Zlé držanie tela, práca v nepriaznivej polohnej.
• Nešikovné pohyby, najmä ak sú opakované.
• Dlhodobé opakovanie rovnakých pohybov.
• Nutnosť použitia príliš veľkej sily.
• Nedostatočne chránene drôty pod stolmi a stolíkmi atď.
• Vibrácie rúk a celého tela.

**Biologické riziká**

Ako „biologické činitele“ sa označujú hlavne tri skupiny mikroorganizmov:

• **baktérie**,  
• **huby** (kvasINKY, Plesne atď.),  
• **vírusy**.

Podľa európskej smernice 2000/54/ES o ochrone pracovníkov pred rizikami súvisiacimi s vystavením biologickým faktorom pri práci patria medzi biologické činitele aj: **geneticky modifikované mikroorganizmy, bunkové kultúry a ľudské endoparazity**.

Medzi látky a situácie, ktoré môžu znamenať biologické riziko patria:

• rastliny, napr. epifýzie (nákazy poľných kultúr),  
• živočíchy, napr. zvieratá, bodnutie hmyzom, živočišný a vtáčí trus, epizoózia (nákazy zvierať).  
• patogénne mikroorganizmy, napríklad baktérie, vírusy, huby, plesne, krv alebo iné telesné tekutiny, nesprávne alebo nedostatočne pripravené uložené potraviny, nákazlivé choroby ako chrípka H1N1 a sezónna chrípka a pod.

Biologické faktory sa na základe miery rizika nákazy u ľudí klasifikujú na:

a) biologické faktory 1. skupiny, pri ktorých nie je pravdepodobné, že by mohli spôsobiť ochorenie ľudí,  
b) biologické faktory 2. skupiny, ktoré môžu spôsobiť ochorenie ľudí a mohli by predstavovať nebezpečenstvo pre zamestnancov, ale nie je pravdepodobné, že sa ochorenie rozšíri v populácii, pričom obvykle je k dispozícii účinná profilaxia alebo liečba,  
c) biologické faktory 3. skupiny, ktoré môžu spôsobiť závažné ochorenie ľudí a vážne nebezpečenstvo pre zamestnancov; môžu predstavovať riziko rozšírenia v populácii, pričom obvykle je k dispozícii účinná profilaxia alebo liečba,  
d) biologické faktory 4. skupiny, ktoré spôsobujú závažné ochorenie ľudí a sú vážnym nebezpečenstvom pre zamestnancov; môžu predstavovať vysoké riziko rozšírenia v populácii, pričom obvykle nie je k dispozícii účinná profilaxia alebo liečba.
Tab. 5 Nebezpečenstvá a riziká v odvetviach a profesiách (zdroj 2000/54/ES)

<table>
<thead>
<tr>
<th>Odvetvie / Profesia</th>
<th>Nebezpečenstvo / Riziká</th>
</tr>
</thead>
<tbody>
<tr>
<td>Potravinársky priemysel (syr, jogurt, saláma), potravinárské príspady, pekárne</td>
<td>Plesne, kvasinky, baktérie a roztoče spôsobujúce alergie. Organický prach zo zrna, mliečny prach, múka kontaminovaná biologickými činitelia. Toxíny (botulotoxíny, aflatoxíny).</td>
</tr>
<tr>
<td>Poľnohospodárstvo (lesníctvo, záhradníctvo, výroba potravín a krmív pre zvieratá)</td>
<td>Bakterie, huby, roztoče a vírusy prenášané zvieratami, parazitmi a kliešťami. Respiračné problémy spôsobené mikroorganizmami a roztočami z organismického prachu zo zrna, mliečného prachu, múky, korenia. Špecifické alergické plúcne choroby poľnohospodárov a chovateľov vtákov.</td>
</tr>
<tr>
<td>Zdravotníctvo</td>
<td>Niektoré vírusové a bakteriálne infekcie (HIV, žltka, tuberkulóza), Poranenia spôsobené injekčnou ihlou.</td>
</tr>
<tr>
<td>Laboratória</td>
<td>Infekcie a alergie pri manipulácii s mikroorganizmami a bunečnými kultúrami, napr. lúdským tkáníom. Náhodné rozliatie a poranenia spôsobené injekčnou ihlou.</td>
</tr>
<tr>
<td>Kovopriemysel a drevo-priemysel</td>
<td>Kožné problémy spôsobené baktériami a bronchitickou astmou z plesní či kvasiniek v kvapalinách cirkulujúcich pri priemyselnom drvení, mletí, rozmelnení a rezných kvapálnacích pri spracovaní kovov a kameňa.</td>
</tr>
<tr>
<td>Priestory s klimatizačnými zariadeniami či vysokou vlhkosťou</td>
<td>Alergie a respiračné porUCHY z plesní či kvasiniek, Nemoc spôsobená baktériami Legionela.</td>
</tr>
<tr>
<td>Archívy, múzea, knižnice</td>
<td>Plesne, kvasinky a bakterie spôsobujúce alergie a respiračné poruchy.</td>
</tr>
<tr>
<td>Stavebníctvo, stavebné hmoty, prírodný materiál</td>
<td>Plesne a kvasinky spolupôsobiaťe a ochranátorčích zariadení.</td>
</tr>
</tbody>
</table>

Chemické riziká

Riziká spomenuté s chemickými látkami sú závislé od dávky alebo množstva chemickej látky, patria sem: plyny, pary, aerosóly, prachy, pevné, kvapalné látky a ich účinky:
• toxické,
• žieravé, napr. kyselina sírová v autobatérií a výskumných laboratóriách (môže spôsobiť vážne poleptanie kože),
• dráždivé,
• senzibilizujúce – môžu spôsobiť alergickú senzibilizáciu v koncentráciách nižších, než sú bežne stanovené limitné hodnoty pri práci (alergické respiračné symptómy),
• karcinogéne, napr. arzén, benzén, kadmium, kryštalický SiO₂,
• mutagéne, príbuzne karcinogénnym,
• teratogéne,
• látky a prípravky poškodzujúce reprodukciu,
• výbušné látky a prípravky,
• oxidujúce látky a prípravky,
• horľavé látky, ako je benzín, rozpúšťadlá a výbušné chemikálie,
• látky a prípravky nebezpečné pre životné prostredie,
• výrobky s komerčným využitím, ako sú poľnohospodárske a priemyselné chemikálie, ako aj produkty vyvinuté pre domáce použitie – pesticídy, ktoré sa bežne používajú na ovládanie či nežiaducieho hmyzu a rastlín, DDT, organochlórový pesticíd dieldrín,
• ďalšie chemikálie používané v priemyselných a laboratórnych zariadeniach (môžu spôsobiť dýchacie, tráviace problémy alebo zasiahnuť nervový systém, ak sú vdychované, požité alebo absorbované kožou),
• iné chemické látky, ako je alkohol a nikotín,
• nové chemické látky na vyplnenie nových potrieb alebo nahradenie staršej, menej účinnej látky.

Okrem uvedených rizík sú ďalšie riziká BOZP na pracovisku uvedené v Prílohe A.

5.3.2 Personálne riziká

V malých a stredných organizáciách sú personálne riziká veľmi významné, pretože tieto organizácie sú závislé od odborných znalostí a pracovných schopností kľúčových zamestnancov. Termín „personálne riziká“ sa vzťahuje na riziká pre činnosti organizácie, ktoré sa týkajú, alebo sú spôsobené jej personálom. V najhoršom prípade by mohli tieto riziká zmeniť pre organizáciu stratu kľúčových zamestnancov, alebo spôsobiť vedomé konanie zamestnanca proti jej záujmom.

Personálne riziká zahŕňajú:

• únavu a vyčerpanie.
• nehody a choroby,
• zastaranú odbornú kvalifikáciu,
• osobné spory a spory súvisiace so zamestnaním,
• neúmyselné ľudské chyby
• úniky informácií alebo krádeže.

Personálne riziká môžu vytvárať najmä:

1. Riziká BOZP – fyzikálne faktory (napr. hluk, osvetlenie, teplota, atď.), nebezpečenstvo úrazu, fyzická námaha, chemické/biologické faktory, pracovný stres, vzájomná činnosť ľudí a iné faktory.
2. Podmienky pre pracovnú schopnosť a pohodu – uspokojenie z práce, zdravie a telesná zdatnosť, starostlivosť o zdravie a pohodu a iné faktory.
3. Pracovné riziká – nábor a pracovné zaradenie, udržanie kľúčových zamestnancov, pracovné zmluvy, pracovná doba a dovolenka, ukončenie pracovného pomeru a iné.
4. Odbornosť – profesionálne zručnosti, dostatočné odborné zručnosti, vedomosti a zručnosti, ktoré podporujú prácu, napr. počítačová gramotnosť atď., univerzálnosť zručností zamestnancov, znalosti a pokračujúce vzdelávanie, využitie špecialistov, využitie dočasnej pracovnej sily a iné.
5. Osobitné riziká podnikania – vlastné živobytie, odovzdávanie činností ďalším generáciám, rodinné vázby, spory medzi vlastníkmi, nezamestnanosť a pokrytie penzie a iné.
7. Cestovanie a doprava – pracovné riziko na ceste do práce, vnútropodniková doprava, zahraničné cesty a iné.
8. Spôsobenie škôd – úmyselne poškodenie alebo zničenie, únik a alebo krádež informácií, nebezpečné praktiky a riskovanie, neúmyselné škody a iné.

5.3.3 Environmentálne riziká

Environmentálne riziká (riziká životného prostredia) sú skutočné alebo potenciálne nepriaznivé účinky odpadových vôd, emisií, odpadu, vyčerpávania zdrojov atď. na živé organizmy a životné prostredie, ktoré vznikajú z aktivít organizácie. Environmentálne riziká môžu vážne negatívne ovplyvniť finančné zdroje podniku a jeho schopnosť dosiahnuť vytýčené ciele.
Existujúce a stále vznikajúce nové trendy v oblasti environmentálnych rizík a zodpovednosti, môžu mať vplyv na finančné výsledky organizácie, jej reputáciu a značku, cash-flow a kapitálovú hodnotu.

Medzi environmentálne riziká sa zaradujú riziká:

• Znečistenie vonkajšieho ovzdušia – v dôsledku neefektívneho spaľovania palív v doprave, energetike, priemysle i v domácnostiach sa produkujú komplexné zmesi škodlivín, zložených z dvoch primárných emisií, ako sadze a olovo a produktov atmosférickej transformácie, ako sú častice ozónu a sulfátu.

• Znečistenia vnútorného ovzdušia – varenie a kúrenie palivami z biomasy (poľnohospodárskych zvyškov, hnoja, slamy, drevia) alebo uhliom produkuje vysokú úroveň dymu, ktorý obsahuje množstvo znečisťujúcich látok zdraviu škodlivých.

• Znečistenie vody – kvalita pitnej vody po celom svete je ohrozovaná biologickými pôvodcami chorôb a chemikálijami, kontaminovaná voda spôsobuje množstvo chorôb, ktoré sú často život ohrozujúce.

• Chemické nebezpečenstvo – použitie chemikálií sa dramaticky zväčšilo v dôsledku ekonomického rozvoja v rôznych odvetviach, vrátane priemyslu, poľnohospodárstva a dopravy. Ide najmä o chemický priemysel (ťažké kovy, pesticídy a perzistentné organické imisie).

• Chemikálie narušujúce endokrinný systém – sú väčšinou umelé, nachádzajú sa v rôznych materiáloch, ako sú pesticídy, kovy, prídavné látky alebo kontaminanty v potravinách a výrobkoch pre osobnú starostlivosť.

• Elektronický odpad – zdravotné riziko spotrebované s E-odpadom môžu vyplývať z priameho kontaktu so škodlivými látkami, ako je olovo, kadmium, chrom, polychlórované bifenyl, od výchovania jedovatých výparov, aj z hromadenia chemických látok v pôde, vode a potravinách.

• Globálne environmentálne zmeny – riziká pre ľudské zdravie vo veľkej miere, zahŕňajú zmenu klímy, úbytok stratosférického ozónu, stratu biodiverzity, zmeny v hydrologických systémoch a dodávke sladkej vody, degradáciu pôdy a napätia v systémoch určených na produkciu potravín.

• Žiarenie – prírodená vlastnosť životného prostredia – prírodne rádioaktívne zdroje v pôde, vode a vzduchu nás vystavujú ionizujúcemu žiareniu, rovnako ako aj umelé zdroje, vyplývajúce zťažby a využívania prírodne aktívnych materiálov pri výrobe energie, v nukleárnej medicine, spotrebneho tovaru a použití v armáde a priemysle.

• Nové nebezpečenstvá – rastúca industrializácia, explozívny rast mestskej populácie, nedostatočný boj proti znečisteniu, globálna zmena klímy, ubúdanie ozónovej vrstvy, elektromagnetické žiarenie, narušajúce množstvo odpadu, neudržateľná spotreba prirodných zdrojov, nebezpečné používanie a zamorenie chemickými látkami, nedostatok fyzické aktivity, zlá výživa, šírenie pandémie HIV/AIDS a používania nebezpečných látok, to všetko prispieva k vplyvu na životné prostredie a zdravie.

Šimák (2006) medzi environmentálne riziká radí: emisia nebezpečných látok do ovzdušia, znečišťovanie vodných tokov, znečišťovanie spodných vod, produkcia komunálneho a priemyselného odpadu, kontaminácia pôdy, únik toxických a nebezpečných látok, neúmerné využívanie energetických zdrojov (energetická náročnosť výroby), využívanie vzácnych a nereprodukovaťlbných materiálov, poškodzovanie prírody výstavbou hospodárskej, energetickej a dopravné infraštruktúry, poškodzovanie prírody výstavbou ľudskej obydlia a rekreačných zariadení, neúmerné odlesňovanie, nevhodne budované vodohospodárske diela, neprimeraná ťažba surovín, negatívne dôsledky globálneho otepľovania.
Munn (1973) v prehľade látok a vonkajších škodlivých vplyvov, ktoré sú schopné priamo alebo nepriamo pôsobiť na ľudí a biosféru, uvádza: vzduchom šírené oxidy síry a sulfáty, súčasti rozptylených látok (prach, sadze...), kyslíčník uhličitý a nič neodvodené plyny, ktoré pôsobia na chladiace vlastnosti atmosféry, kvalita ovzdušia, vzduchom šírené kyslíčníky a dusičniny, fotochemické oxidanty a reaktívne uhlovodíky, toxické kovy (ortuť, olovo a kadmium), organické zlúčeniny (DDT a jeho metabolity), azbest, ropné uhlovodíky, jedovaté látky biologického pôvodu (z rias, plešní a bakterií), nitráty, dusité a nitrozamíny, čpavok, vybrané ukazovatele akosti vody (dostatok biologického kyslíku), rozptyľadlá, coli baktérie, vybrané rádioaktívne nuklidy, vzduchom šírené alergény, eutrofikátory – látky na podporu výživy a rastu (nitráty a fosfáty), rozpustné soli alkalických kovov a kovov alkalických zemín, iné látky, ktoré majú významný vplyv na problémy lokálne životného prostredia (arzén, bór, fosfor, selén a fluorid), hluk a odpad.

5.3.4 Riziká požiaru

Požiar je nekontrolovateľný oheň, pri ktorom dochádza k usmrteniu osôb alebo zvierať, ku škodám na materiálnych hodnotách alebo životnom prostredí, alebo k bezprostrednému ohrozeniu osôb, zvierat, materiálnych hodnôt alebo životného prostredia. Vzniká zvyčajne buď v dôsledku technickej chyby, prirodzenej nesťastia alebo úmysleného zapálenia (podpaľačstvo).

Vzhľadom na skupenstvo horiacich látok sa požiare delia do tried:

a) **požiare pevných látok**, najmä organického pôvodu, ich horenie je spravidla sprevádzané žeravými uhlíkmi či iskrením – papier, drevo, textil, hasiace prístroje vodné, penové a práškové,

b) **požiare kvapalin alebo látok prechádzajúcich do kvapalného skupenstva** – benzín, nafta, farby, decht, tuky, parafín, hasiace prístroje penové a práškové,

c) **požiare plynov** – acetylén, vodík, metán, propán, používať hasiace prístroje práškové a snehové,

d) **požiar ľahkých kovov** (horčík, zliatiny hliníka) alebo **alkalických kovov** (lítium, sodík, draslík a ďalšie), vzhľadom na vysokú teplotu požiaru vyžaduje použitie špeciálnych hasiacich alebo špeciálne upravených práškov,

e) **požiare jedlých olejov a tukov** (rastlinné alebo živočíšne oleje a tuky).

Medzi všeobecné riziká vzniku požiaru možno zaradiť:

- podpaľačstvo,
- varenie na otvorenom ohni bez dozoru (pečeť na panvici, pečenie na ražni, na miernom ohni),
- fajčiarecké potreby a fajčenie (cigarety, cigary, fajky, zápalky, zapaľovače atď.),
- otvorený oheň (sviečky/kadidlo),
- elektrické nebezpečenstvo (elektroinštalácie v zlom stave, spotrebiče a zariadenia, ktoré sú preťažené, majú za následok prepálenie drôtov alebo spojovacích článkov),
- batérie,
- elektronické a elektrické príslušenstvo,
- bytové zariadenie, ktoré vytvára teplo a využíva horľavé materiály, ohrievadlá,
- vonkajšie kuchynské zariadenie – gril,
- varené spotrebiče – sporáky, rúry,
- vykurowacie zariadenia – krby, kachle na drevo, pece, bojlerky, prenosné ohrievače,
- domáce spotrebiče – sušičky bielizne, kulmy, feny, chladičnéky, mrazničky,
- komíny, ktoré sústreďujú kremoz, krbové komíny nesprávne alebo nepravidelne čistené,
- použitie halogénových žiaroviek,
• horľavé kvapaliny a aerosóly, horľavé rozpúšťadlá (a handry nasiaknuté rozpúšťadlom) umiestnené v uzavretých nádobách na odpadky,
• akumulácia horľavých materiálov, nesprávna manipulácia a skladovanie horľavých/ zápalných kvapalin, s nedostatočnou ochranou, horľaviny v blízkosti zariadení, ktoré generujú teplo, plameň alebo iskry,
• zvýšené zahrievanie pri práci (rezanie, zväzovanie).

5.3.5 Rizíká technických (technologických) havárií a katastrof

Podľa Zákona o civilnej ochrane obyvateľstva sa havária rozumie ako 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. Má za následok zničenie alebo poškodenie nejakého stroja, dôležitého prístroja, budovy, technologického celku, ľudského zdravia alebo života, k rozsiahlym ekologickým alebo hospodárskym škodám a pod. Zvláštnym prípadom havárie je požiar (nie viac prirodzený požiar).

Medzi technologické riziká možno zaradiť najmä:
• úniky nebezpečných látok zo stacionárnych a mobilných zdrojov, únik rangoaktivného odpadu alebo iného nebezpečného odpadu pri jeho likvidácii, únik ropných látok,
• veľké požiare v hospodárskych objektoch, požiare skladov na ropné produkty a v drevo- spracúvacom priemysle,
• výbuchy v chemických prevádzkach a pri skladovaní obilín,
• havárie jadrových zariadení, v leteckej, železničnej, lodnej, cestnej doprave,
• narušenie vodohospodárskej diel, produktovodov, informačných sietí, funkčnosti bankovej sústavy,
• narušenie dodávok elektrickej energie, plynu, tepelnej energie, pitnej vody,
• narušenie nedodaním liekov a zdravotníckeho materiálu,
• nebezpečné úseky komunikácií.

Medzi riziká mechanického ohrozenia možno zaradiť najmä: straty stability, rozpadnutie sa počas prevádzky, riziká spôsobené padajúcimi alebo odletujúcimi predmetmi, riziká spôsobené povrchmi, hranami alebo rohmi, riziká súvisiace s kombinovanými strojovými zariadeniami, riziká súvisiace so zariadeniami, riziká súvisiace s variaciou podmienok prevádzky, riziká súvisiace s pohyblovými časťami, riziko nekontrolovaných pohybov.

Medzi riziká spôsobené inými nebezpečenstvami možno zaradiť najmä: statická elektrická energia, prívod inej ako elektrickej energie, chyby inštalačie, extrémne teploty, požiar, blesk, výbuch, hluk.

Technologické alebo človekom vytvorené riziká (zložité havárie, hladomor, migrácia, priemyselné a dopravné havárie) sú udalosti, ktoré sú spôsobené ľuďmi a vyskytujú sa v ľudských sídlach alebo ich blízkosti. To môže zahŕňať zhoršovanie životného prostredia, znečistenie a havárie. V tejto oblasti existuje množstvo výziev, ako je zmena klimy, neplánovaná urbanizácia, zaostalosť, chudoba, rovnomerná urbanizácia, zaostalosť, chudoba, rovnomerná urbanizácia.

5.3.6 Prírodné riziká

Prírodné riziká predstavujú v prírode sa vyskytujúce udalosti, ktoré môžu mať negatívny vplyv na ľudí a životné prostredie. Následkom pôsobenia prírodných rizík môže nastať živelná pohroma, havária alebo katastrofa.
Podľa Zákona o civilnej ochrane obyvateľstva sa rozumie:

• **živelná pohroma** – 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,

• **katastrofa** – mimoriadna udalosť, pri ktorej dôjde k narastaniu ničivých faktorov a ich následnej kumulácii v dôsledku živelnej pohromy a havárie - môže byť definovaná ako riziko bezpečnosti, ktoré má potenciál spôsobiť značné škody osobné, spoločenské, majetkové a škody na životnom prostredí.

Medzi prírodné riziká patria najmä:

• povodne a záplavy,

• lavíny – snehové, kamenné, zosuv pôdy a skál,

• seizmická činnosť, zemetrasenie, sopečná erupcia,

• poveternostné udalosti – snehová búrka (blizzard), búrka, búrka s víchricou, veterná smršť, tornádo, orkán, tropická búrka, krupobitie, tornádo, vráskové búrky, obrázka s mimozemským telesom.

Šimák (2006) charakterizuje prírodné riziká ako:

• energetickej prejav pre prírodu (pôsobenie samotnej prírody na prírodné i životné prostredie),

• dôsledky zásahov človeka do prírody (pôsobenie človeka na prírodu),

• spoločné pôsobenie človeka a prírodných síl.

Medzi prírodné riziká zaraďuje: záplavy, sucho, víchrice a orkány, búrky a krupobitie, sneženie, mráz a námraza, snehové lavíny, zosuvy pôdy, sopečnú činnosť, zemetrasenia, lesné požiare, pôsobenie meteoritov a drobných kozmických telies.

5.3.7 **Riziká bezpečnosti priestorov**

Pod pojmom priestory možno chápať:

• **priestory organizácií**, napr. podniku, závodu, školy, univerzity, nemocnice, železničnej stanice, nákupné centrum a pod.,

• **areál** – vymedzená časť územia, napr. pozemky so stavbami, areál výstaviska, areál rekreačného zariadenia, areál oblasť u istú činnosť, rezervácia (chránená oblasť), rezervácia (chránená oblasť) a pod.,

• **prevádzkareň** – miesto, dielňa na výrobnú alebo inú hospodársku činnosť,

• **samostatné objekty**, napr. dom s pozemkom,

• **vnútorné priestory budov**, napr. miestnosti, schodiská, terasy, balkóny, výtahy a pod.

V praxi bezpečnostného manažmentu sa uvedené priestory obvykle nazývajú objekty a chránené priestory.

Posúdenie bezpečnostného rizika v priestoroch má zahŕňať nasledujúce aspekty: terén, stavebná konštrukcia, ploty, brány, dvere a okná, osvetlenie a napájanie, informačná a výpočtové technika, plachtopavé a sledovacie zariadenia, manipuláciu s hotovosťou, parkovisko, bezpečnost zamestnancov a to.
Medzi vonkajšie riziká bezpečnosti priestorov možno zaradiť najmä:

- úmyselné napadnutie osôb, napr. teroristický incident, nebezpečné vyhriávanie, vydieranie, podrozivá poštová zásilka, otrava vody alebo potravin, kyberšikanovanie, kybernetické prenasledovanie a pod.,
- úmyselné spôsobenie majetkovej újmy, napr. pouličné nepokoje, rabovanie, krádež, lúpež, vandalizmus, sabotáž, zničenie alebo poškodenie cudzej veci, podvod, špionáž, podpaľačstvo, poškodenie inžinierskych sietí a pod.,
- úmyselné poškodenie životného prostredia, napr. otrava alebo znečistenie pitnej vody a pod.,
- náhodné prirodzene riziká, napr. prirodzene požiar, snehové lavíny, zosuv pôdy a kameňov, zemetrasenie, sopečná činnosť, bôrka, blesk, bôrka s vichricou, veterná smršť, tornádo, orkán, cunami, krupobitie, tropická búrka, extrémna horečka a sucha, extrémna zima (chlad), snehová bôrka (blizzard), extrémne sneženie, zamořenie vody a kontaminácia potravin a pod.,
- náhodné technologické riziká, napr. narušenie dodávok elektrickej energie, plynu, tepelnej energie, pitnej vody a pod.,

Medzi vnútorné riziká bezpečnosti priestorov možno zaradiť najmä:

- činnosť vlastných zamestnancov, napr. krádež, pomoc vonkajšiemu páchateľovi pri preniknutí do chráneného priestoru, úmyselné vyvolanie havárie, sprenervera, úmyselné porušenie tajomstva, zneužitie osobných údajov, záškodnictvo, podpaľačstvo, zničenie, poškodenie cudzej veci a spôsobenie škody na cudzom majetku (poškodenie IKT, inžinierskych sietí, úmyselný výbuch plynu, ohrozenie prevádzky a pod.),
- fyzikálne, mechanické, ergonomické, biologické a chemické riziká vo vnútornom prostredí, ktoré majú vplyv najmä na bezpečnosť práce,
- personálne riziko pre utajované skutočnosti,
- environmentálne riziká, napr. znečistenie vonkajšieho a vnútorného prostredia, vody, E-odpad, žiarenie a pod.,
- riziká vnútorného požiaru, napr. skrat na elektroinštalácii, zanesené komíny, chybné elektrické spotrebiče a pod.,
- technologické riziká, napr. výbuchy, únik nebezpečných látok, únik rádioaktívneho odpuďu alebo iného nebezpečného odpadu pri jeho likvidácii, únik ropných látok a pod.,
- riziká mechanického ohrozenia, napr. straty stability, rozpadnutie sa zariadenia počas prevádzky, riziká spôsobené padajúcimi alebo odletujúcimi predmetmi, riziká spôsobené povrchmi, hranami alebo rohmi, riziká súvisiace s kombinovanými stresovými zariadeniami, riziká súvisiace s variáciou podmienok prevádzky, riziká súvisiace s pohyblivými časťami, riziko nekontrolovaných pohybov a pod.,
- riziká spôsobené inými nebezpečenstvami, napr. statická elektrická energia, prívod inej ako elektrickej energie, chyby inštalácie, extrémne teploty, slabé osvetlenie a pod.,
- stavebné a konštrukčné riziká.
5.4 LITERATÚRA


Biologické materiály. In: Fakta č.41. Európska agentúra pre bezpečnosť a ochranu zdravia pri práci. ISSN 1681-2123.


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


Organizácie všetkých typov a veľkostí čelia rade rizík, ktoré môžu ovplyvniť dosiahnutie ich zámerov (cieľov). Riziká sa vyskytujú vo všetkých činnostiach organizácie, v rozsahu od strategických iniciatív až po jednotlivé operácie, procesy a projekty a môžu ovplyňovať:

- spoločenské, environmentálne, technologické, bezpečnostné a zabezpečujúce výsledky,
- komerčné, finančné a ekonomické opatrenia,
- sociálne, kultúrne a politické následky a dopady na dobré meno spoločnosti.

Manažérstvo rizika je preto jedným z najdôležitejších problémov, ktorým dnes organizácie čelia. Organizácie, ktoré úplne nepochopi riziká svojej činnosti, budú pravdepodobne upadať. Manažérstvo rizika je dôležitou súčasťou každého strategického riadenia organizácie. Je to proces, prostredníctvom ktorého sa organizácie venujú rizikám spojeným ich s cieľom dosiahnuť trvalý prospech z každej jednotlivéj a súhrnne zo všetkých činností organizácie.


Proces manažérstva rizika napomáha pri rozhodovaní tak, že bere ohľad na neistotu a možnosti budúcich udalostí (plánovaných alebo neplánovaných) a ich následkov pre zvolené ciele. Manažérstvo rizika organizácie sa má zaviesť na základe ubezpečenia, že proces manažérstva rizika sa realizuje na základe plánu manažérstva rizika ako súčasť jej praktik a procesov na:

- všetkých príslušných úrovniach,
- a na všetkých funkčných miestach v organizácii.

Organizácie riešia riziko tak, že ho identifikujú, analyzujú a následne posúdia, či ho treba modifikovať tým, že sa s ním budú zaobchádzať (zaobchádzanie s rizikom), aby vyhovovalo určeným kritériám.

Počas tohto procesu organizácie:

- stanovujú štruktúry pre identifikáciu, analýzu, hodnotenie a zaobchádzanie s rizikom, ktoré súvisia s akoukoľvek činnosťou, procesom, funkciou alebo produktom,
- komunikujú a konzultujú so zúčastnenými účastníkmi po celú dobu procesu,
- monitorujú a preskúmavajú rizíko a opatrenia na jeho modifikáciu, s cieľom dosiahnuť, že sa nebude vyžadovať ďalšie zaobchádzanie,
- využívajú systém podávania hlášení a zaznamenávajú výsledky vhodným spôsobom.

Manažérstvo rizika je rýchlo sa rozvíjajúci odbor a existuje veľa rôznych pohľadov a prístupov, ako a prečo riziká riadiť. Práve preto bolo z dlhodobého hľadiska potrebné zavedie určitú normu, ktorá by zjednotila terminológiu, ciele, štruktúru a proces manažérstva rizika.


Účelom normy je poskytnúť zásady a usmernenia pre manažérstvo rizika ako všeobecné uznaný vzor pre odborníkov a firmy, ktoré uskutočňujú procesy manažérstva rizika a nahradiť nespočetné množstvo existujúcich štandardov, metodík a modelov, ktoré sa lišili medzi jednotlivými odvetviami a regiónmi.

Je mnoho spôsobov postupov vedúcich k dosiahnutiu cieľov manažérstva rizika, ale nie je možné všetky popísať v jednom normalizačnom dokumente. Preto tiež zámerom týchto dokumentov nebolo vytvoriť predpisovú normu, ktorá by požadovala plnenie jednotlivých konkrétnych krokov, ani zaviesť postup certifikácie.

Zámerom normy je, aby sa využila pri harmonizovaní procesov manažérstva rizika v jestvujúciach a budúcich normách. Poskytuje všeobecný prístup, zameraný na podporu odborníkov a organizácií, ktoré uskutočňujú procesy manažérstva rizika a nahradiť nespočetné množstvo existujúcich štandardov, metodík a modelov, ktoré sa lišili medzi jednotlivými odvetviami a regiónmi.

 Norma odporúča, aby organizácie vypracovali, zaviedli a nepretržite zlepšovali svoju štruktúru, ktoréj účelom je interogovať proces manažérstva rizika do celkového riadenia organizácie, jej stratégie a plánovania, politiky, hodnôt, kultúry, manažérstva a procesov podávania správ.

Manažérstvo rizika možno kedykoľvek aplikovať na celú organizáciu, jej rozličné oblasti a úrovne, ako aj na osobitné funkcie, projekty a činnosti. Hoci postupy manažérstva rizika sa vyvíjali po istý čas a pre mnohé oblasti s cieľom splniť rozličné požiadavky, prijatie zhodných procesov v rámci celkovej architektúry môže pomôcť ubezpečiť, že sa riziko riadi efektíve, účinne a súvisle v celej organizácii.

Všeobecný prístup opísaný v tejto norme ponúka zásady a návod na manažérstvo akejkoľvek formy rizika systematickým, transparentným a dôveryhodným spôsobom a v akomkoľvek rozsahu a súvislosti.

Súčasné manažérske návody a procesy mnohých organizácií zahŕňajú zložky manažérstva rizika v určitých oblastiach podľa niektorých stávajúcich zákonov a vyhlášok a mnohé organizácie podľa nich už pre konkrétné druhy rizika prijali oficiálny proces manažérstva rizika. V takých prípadoch, aj ked' ešte nie sú zásady tejto normy zavedené do uvedených zákonov a vyhlášok, sa organizácia môže rozhodnúť zrealizovať kritické prekúmanie svojej súčasnej praxe a svojich procesov z pohľadu tejto normy.

Norma môže využiť akákoľvek verejná, súkromná alebo spoločenská organizácia, asociácia, skupina alebo jednotlivec. Preto tato norma nie je špecifická pre nejaký druh alebo pre nejaké odvetvie, pre určité používania normy označujú všeobecným terminom organizácia.

Normu môžu použiť počas existencie akejkoľvek verejnej či súkromnej organizácie, v združeniach a u jednotlivcov na široký rozsah činností vrátane stratégie a rozhodnutí, prevádzky, procesov, funkcí, projektov, produktov, služieb a majetku. Je možné ju aplikovať na akýkoľvek druh rizika a akéhokoľvek charakteru bez ohľadu na to, či má pozitívne alebo negatívne následky.

Hoci norma poskytuje všeobecný návod, jej cieľom nie je propagovať jednotnosť manažérstva rizika v organizáciách – pri jej zavedení sa musia brať do úvahy rozdielne potreby konkrétnych organizácií, jej špecifické ciele, súvislosti, štruktúra, prevádzka, procesy, funkcie, projekty, produkty, služby či majetok a osobitne používané postupy.
Zavedenie a udržiavanie normy manažérstva rizika organizácií umožňuje:

- zvýšiť pravdepodobnosť dosiahnutia cieľov,
- podporovať proaktivý manažment (predsiahnutie udalostí, nie z krízy do krízy),
- uvedomíť si potrebu identifikácie a zaoberania sa rizikom v celej organizácii,
- zlepšiť identifikáciu priležitostí a ohrození,
- byť v súlade s príslušnými právnymi normami,
- zlepšovať povinné a dobrovoľné podávanie správ,
- zlepšiť dozor,
- zlepšiť dôveru a istotu akcionárov,
- vytvoríť spoľahlivú základňu na prijímanie rozhodnutí a plánovanie,
- efektívne umiestňovať a využívať zdroje na zaobchádzanie s rizikom,
- efektivnosť a účinnosť prevádzky,
- zlepšovať zdravotnú a bezpečnostnú výkonnosť, ako aj ochranu prostredia,
- zlepšovať prevenciu strát a manažérstvo udalostí,
- minimalizovať straty,
- zlepšovať vedomosti o organizácii,
- zlepšovať organizačnú pružnosť.

Organizácia, ktorá uskutočňuje manažérstvo rizika chráni svoje aktíva i aktíva všetkých zainteresovaných strán, zároveň zvyšuje ich hodnotu, najmä tým, že:

- poskytuje organizácii štruktúru, ktorá umožní vykonávať všetky budúce činnosti konzistentným a transparentným spôsobom,
- zlepšuje rozhodovací proces, plánovanie a určovanie priorít pomocou obsiahleho štruktúrovaného posúdenia jednotlivých činností organizácie a posúdenia miery neistoty priležitosti/ hrozieb,
- prispieva k účinnejšiemu využívaniu / prideľovaniu finančných prostriedkov zdrojov organizácie,
- znižuje neistotu v oblastiach, ktoré nie sú pre organizáciu zásadné,
- chráni a zhodnocuje aktíva a dobré meno organizácie,
- rozvíja a podporuje znalosti zamestnancov a vedomostnú základňu organizácie,
- zvyšuje efektivitu činností organizácie.

V tejto norme sa používanú pojmy:

- manažérstvo rizika (risk management), ktoré sa týka architektúry efektívneho manažérska rizika (zásad, štruktúry a procesov),
- riadenie rizika (managing risk), ktoré sa týka využitia tejto architektúry pri konkrétном riziku – opatrenie (opatrenia), ktoré modifikuje (modifikujú) riziko.

Norma ISO 31000 sama o sebe nie je certifikovateľná, ale certifikačné orgány môžu posúdiť stav riadenia rizík v každej organizácii v kombinácii s inou normou, ako sú napríklad:

- STN EN ISO 14001 Systémy environmentálneho manažérstva. Požiadavky s pokynmi na použitie.
6.1 USPORIADANIE MANAŽÆRSTVA RIZIKA

Manažérsťo rizika predstavuje usporiadaný a koordinovaný súbor činností a metód, na usmerňovanie a riadenie organizácie vo vzťahu k rizikám, ktoré môžu ovplyvniť jej schopnosť dosiahnuť stanovené ciele.


Táto architektúra, uvedená na obr. 6 zahŕňa:
- zásady manažérsťa rizika,
- štruktúru manažérsťa rizika (framework),
- proces manažérsťa rizika.

Obr. 6 Vzťahy medzi zásadami, štruktúrou a procesom manažérsťa rizika (STN ISO 31000)
6.2 ZÁSADY MANAŽÉRSTVA RIZIKA

Aby manažérstvo rizika bolo efektívne, organizácia má podľa uvedenej normy na všetkých úrovniach rešpektovať nasledujúce zásady:

a) Vytvárať a ochraňovať hodnotu – manažérstvo rizika prispieva k preukázanému dosahovaniu zámerov a zlepšovaniu výkonnosti, napríklad pri ochrane osôb a ich bezpečnosti, pri záruckách, dodržiavaní zákonov a predpisov, verejnom schvaľovaní, ochrane prostredia, v kvalite produktov, v manažérstve projektovania, v prevádzkovej účinnosti a v reputácii.

b) Byť integrálnou súčasťou všetkých procesov v organizácii – manažérstvo rizika je časťou zodpovednosti manažmentu a integrálnou súčasťou všetkých procesov organizácie, vrátane strategického plánovania a všetkých procesov projektovania a manažérstva zmien.

c) Byť súčasťou prijímania rozhodnutí – pomáha tvorcovi rozhodnutí urobiť informovaný výber, uprednostniť činnosti a rozlišiť alternatívny priebeh činností.

d) Byť systematické, štruktúrované a včasné – to prispieva k účinnosti a ku konzistentným, porovnateľným a spoľahlivým výsledkom.

e) Zakladat’ sa na najlepších dostupných informácíach – vstupy do procesu manažérstva rizika vychádzajú z informačných zdrojov, ako sú historické údaje, skúsenosti, spätne vázby od zainteresovaných účastníkov, pozorovanie, predpovede a expertné posúdenie. Tvorcovia rozhodnutí sa však majú navzájom informovať a majú zohľadňovať akékoľvek obmedzenia údajov, či v rámci použitého modelu alebo možnosti odlišných názorov rozlišných expertov.

f) Prispôsobovať sa na mieru – zosúladiť sa s vnútornými a vonkajšími súvislostami v rámci organizácie a s profilom rizika.

g) Zohľadňovať ľudské a kultúrne faktory – uznávať spôsobilosť, vnímanie a zámery externých a interných ľudí, ktoré môžu uľahčiť alebo obmedziť dosiahnutie zámerov organizácie.

h) Byť transparentné a zhrňujúce – vhodné a včasné zapojenie zainteresovaných účastníkov a majú navzájom informovať a majú zohľadňovať dosiahnutie zámerov organizácie.

i) Byť dynamické, opakujúce sa a citlivé na zmeny – nepretržitý cyclus vnímania zmien a reakcia na ne. Keď narastú externé a interné udalosti, menia sa súvislosti a vedomosti, nastupuje monitorovanie a preskúmavanie rizík, objavujú sa nové riziká, niektoré sa zmienia a iné sa stratia.

j) Uľahčovať trvalé zlepšovanie organizácie – organizácia má vypracovať a zaviest stratégiu zlepšovania zrelišky manažéra rizika spoločne so všetkými ďalšími aspektmi organizácie, ďalšie rady na zlepšovanie riadenia rizika sú uvedené v prílohe D.

6.3 LITERATÚRA


STN EN 31010:2011 Manažérstvo rizika, Techniky posudzovania rizika.
Štruktúra manažérstva rizika predstavuje podľa STN ISO 31000:2011 množinu zložiek, ktoré vytvárajú základy a organizačné usporiadanie pre navrhovanie, zavedenie monitorovania, preskúmavanie a trvalé zlepšovanie manažérstva rizika v celej organizácii.

Základy manažérstva rizika zahŕňajú:
• politiku manažérstva rizika,
• ciele,
• mandát a záväzok.

Organizačné usporiadanie zahŕňa:
• plány,
• vzťahy a zodpovednosti,
• zdroje, procesy a činnosti, ktoré sa využívajú v manažérstve rizík organizácie.

Hlavné zložky štruktúry manažérstva rizika sú (obr. 7):
a) Mandát a záväzok.
b) Návrh štruktúry manažérstva rizika.
c) Zavedenie manažérstva rizika.
d) Monitorovanie a preskúmavanie štruktúry.
e) Nepretržité zlepšovanie štruktúry.

Štruktúra manažérstva rizika:
• je súčasťou celkovej strategickej a prevádzkovej politiky a postupov organizácie.
• predstavuje usporiadanú, nepretržitú, cyklickú postupnosť činností manažmentu a vyčlenených odborníkov, ktorí uskutočňujú plánovanie, organizovanie, dosiahnutie a upevňovanie manažérstva rizika v organizácii.
• predstavuje riadiacu štruktúru, ktorá je dôležitou súčasťou architektúry manažérstva rizika a poskytuje východiská a opatrenia, ktoré umožňujú tento rámec implementovať na všetkých úrovniach organizácie.

Štruktúra manažérstva rizika je množina zložiek, ktoré:
• pomáhajú organizácii integrovať manažérstvo rizika do celkového systému riadenia, je súčasťou celkovej strategie a prevádzkovej politiky a postupov organizácie
• pomáhajú efektívne riadiť riziká prostredníctvom aplikácie procesu manažérstva rizika na rozličných úrovniach a v rámci rôznych prostredí organizácie
• zabezpečujú, že informácie o riziku získané z procesu manažérstva rizika sa primerane oznamujú a využívajú ako základ prijímania rozhodnutí a pridelovania zodpovednosti na všetkých príslušných organizačných úrovniach organizácie.

Štruktúra nemá slúžiť ako recept na systém manažérstva, skôr má organizáciu pomôcť integrovať manažérstvo rizika do celkového systému manažérstva, z toho dôvodu organizácie majú prispôsobiť jednotlivé zložky štruktúry svojim konkrétnym potrebám,
7.1 NÁVRH ŠTRUKTÚRY MANAŽÉRSTVA RIZIKA

Návrh štruktúry manažérstva rizika obsahuje:

a) Chápanie organizácie a jej súvislostí.
b) Vytvorenie politiky manažérstva rizika.
c) Zodpovednosť za manažérstvo rizika.
d) Integrácia do procesov organizácie.
e) Zdroje pre manažérstvo rizika.
f) Vytvorenie mechanizmov internej komunikácie a oznamovania.
g) Vytvorenie mechanizmov externej komunikácie a oznamovania.

Predmetom návrhu štruktúry manažérstva rizika je spôsob, akým sú jednotlivé úlohy v súvislosti s manažérstvom rizík v praxi realizované. Správne vytvorený návrh štruktúry podporuje efektívnu implementáciu manažérstva rizika v organizácii. Návrh štruktúry teda obsahuje konkrétné opatrenia a postupy aplikovateľné v špecifických podmienkach danej organizácie a zabezpečuje tak použiteľnosť štruktúry pre riadenie rizík v konkrétnej organizácii.

Pre správny návrh štruktúry manažérstva rizika je preto nevyhnutné celkové pochopenie súvislostí fungovania organizácie a vyhodnotenie jej vnútorného a vonkajšieho prostredia, ktoré môže významne ovplyvňovať návrh štruktúry.

Chápanie organizácie a jej súvislostí

Základom pre pochopenie organizácie a jej súvislostí je zistenie aktuálneho stavu v organizácii, kladov a nedostatkov. Kým sa začne proces manažérstva rizika, je nevyhnutné pochopiť:

• organizáciu a jej schopnosti,
• ciele, zámery a stratégie, ktoré praktizuje, aby ich dosiahla.

Vytváranie súvislostí znamená:

• definovanie interných a externých faktorov, ktoré treba zohľadniť v manažérstve rizika a pri určovaní rozsahu a kritérií rizika.
• určenie a definovanie základných faktorov prostredia, v rámci ktorých sa riziká musia riadiť,
• poskytnutie návodu na rozhodovanie v podrobnejších štúdiách manažérstva rizika.

Pre začatím realizácie návrhu a zavádzaním štruktúry manažérstva rizika je dôležité posúdiť externé i interné súvislosti organizácie, ktoré môžu významne ovplyvniť návrh štruktúry.

Interné súvislosti

Interné súvislosti predstavujú vnútorné prostredie, v ktorom organizácia chce dosiahnuť svoje zámery.

Externé súvislosti

Externé súvislosti predstavujú vzťah organizácie k externému prostrediu, v ktorom organizácia chce dosiahnuť svoje zámery, ich pochopenie umožní najmä určiť externých zaинтересovaných účastníkov, ich ciele, názory a politiku komunikácie s nimi.

Politika manažérstva rizika

Politika znamená vyhlásenie hlavného záväzku, smerovania alebo zámeru organizácie. Politika manažérstva rizika (Risk management policy) vyjadruje celkový zámer a smerovanie organizácie k manažérstvu rizika.
Postoj organizácie k riziku (Risk attitude) ukazuje jej prístup k hodnoteniu a prípadne vykonávaniu, zachovávaniu, akceptovaniu či odvráteniu sa od rizika. Postoj organizácie k riziku a stanovené kritériá rizika ovplyvňujú:

• ako budú riziká vyhodnotené a adresované,
• či sa riziká príjmu, budú prípustné (tolerované), zachovajú, prenesú na ďalšiu stranu, znížia, alebo sa im organizácia vyhne,
• či spôsob zaobchádzania s rizikom bude zavedený alebo odložený.

Politika manažérstva rizika sa má vhodne oznamovať všetkým zamestnancom. Má jasne určiť cieľ organizácie a jej záväzok za manažérstvo rizika a musí zvyčajne obsahovať:

• rozumné zdôvodnenie organizácie riadiť riziko,
• zodpovednosti a právomoci v manažérstve rizika,
• spôsoby, ako riešiť konfliktné záujmy,
• záväzok sprístupniť potrebné zdroje a tak pomôcť pracovníkom zodpovedným za manažérske riziko,
• spôsob, akým sa výkonnosť manažérstva rizika bude meriť a oznamovať,
• zabezpečiť vyhodnotenie, podávanie externých alebo interných správ a zlepšovať politiku a štruktúru manažérstva rizika.

Zodpovednosť za manažérstvo rizika

Zodpovednosť za manažérstvo rizika znamená zodpovednosť, právomoc a primeranú kompetentnosť v manažérstve rizika, zavedenie a udržiavanie procesu manažérstva rizika, primeranosť, efektivnosť a účinnosť akýchkoľvek kontrol.

Tieto postupy možno uľahčiť:

• identifikáciou vlastníkov rizika (osoby alebo zložky so zodpovednosťou a právomocou riadiť riziko),
• identifikáciou osob zodpovedných za vývoj, zavedenie a udržiavanie štruktúry manažérstva rizika,
• identifikáciou d'alších l'udí na všetkých úrovniach organizácie, zodpovedných za proces manažérstva rizika,
• vytvorením procesov merania výkonnosti manažérstva rizika, podávania externých alebo interných správ a zdokonaľujúcich procesov,
• zabezpečiť vyhodnotenie rizika.

Integrácia do procesov organizácie

Implementovanie manažérstva rizika predstavuje krok, ktorého úlohou je zavádzanie navrhnutej štruktúry do praxe a oživenie riadenia rizik v organizácii.

Manažérstvo rizika sa má:

• začleniť do všetkých postupov a procesov organizácie vhodným, efektívnym a účinným spôsobom,
• osobitne zahrnúť do politiky vývoja, podnikania, strategického plánovania a preskúmava- nia, ako aj do procesov manažérskych zmien

Proces manažérstva rizika sa má mať súčasťou organizácií a nesmie sa oddeľovať.

Úspešné implementovanie manažérstva rizika musí garantovať:

• že vlastník rizika (osoba alebo entita so zodpovednosťou a právomocou riadiť riziko) rozumie procesu manažérstva rizika,
že aktivity v súvislosti s manažérstvom rizika sa budú skutočne realizovať, 
a podnikové procesy a rozhodovanie budú reálne uvažovať s rizikami.

Plán manažérstva rizika (Risk Management Plan) popisuje zámer na manažérstvo rizika v organizácii. Plán manažérstva rizika možno aplikovať na konkrétne výrobok, proces či projekt alebo na celú organizáciu či jej časť.

Plán tvorí základ všetkých činností riadenia rizika a ďalších rizikových aktivít, je to dokument, ktorý pripravuje na predvidanie rizík, odhadovanie následkov a definovanie odpovedí na rôzne otázky. Má byť spracovaný pre celú organizáciu, zabezpečuje, že politika manažérstva rizika sa zavedie a že manažérstvo rizika sa stane súčasťou všetkých praktík a procesov organizácie. Plán manažérstva rizika možno integrovať do iných plánov organizácie, napríklad do strategického plánu.

Plán manažérstva rizika špecifikuje prístup, zložky manažérstva rizika a zdroje, ktoré sa majú využiť v manažérstve rizika. Zložky manažérstva rizika obvyčajne obsahujú postupy, skúsenosti, pridelenie zodpovednosti, postupnosť či časovanie činností.

Plán manažérstva rizika obsahuje:
1. Prístup k manažérstvu rizika:
   • implementácia manažérstva rizika do organizácie,
   • stanovenie zodpovednosti manažmentu za riziká,
   • politika manažérstva rizika,
2. Zložky manažérstva rizika:
   • dokumentáciu zisteného rizika – zoznam (register, katalóg) rizík, voľba počiatočnej odozvy,
   • výstupy analýzy rizika – najdôležitejšie riziká, výsledné hodnoty rizík, priorit rizík,
   • zvolené voľby odozvy na riziko – pridelenie rizíka medzi zúčastnené strany, zaistenie, zaopatrenie a zmluvné usporiadanie týkajúce sa rizíka, plán eventualít, poistenia a ďalšie usporiadanie prenosu rizíka,
   • monitoring a controlling – porovnanie skutočných výsledkov rizíka s predpokladanými,
   • udržiavanie systému riadenia rizíka – prostriedky aktualizácie a jeho vylepšovanie,
   • vyhodnotenie – zaznamenávanie informácií o riziku.

Zdroje pre manažérstvo rizika

Na manažérstvo rizika má organizácia vydeliť vhodné zdroje, do úvahy treba brať tieto skúsenosti:
• ľudia, ich zručnosť, skúsenosť a kompetentnosť,
• zdroje potrebné na každý krok procesu manažérstva rizika,
• procesy, metódy a nástroje organizácie, ktoré sa majú využiť v manažérstve rizika,
• zdokumentované procesy a postupy (v minulosti),
• systémy manažérstva poznaní a informácií (knowledge management – vedomostný manažment),
• programy školení.

Vytvorenie mechanizmov internej a externé komunikácie

Organizácia má vytvorit mechanizmy internej komunikácie a oznámovania s cieľom zabezpečiť a podporiť zodpovednosť a vlastníctvo rizika. Tieto mechanizmy majú zabezpečiť, že:
• klúčové zložky štruktúry manažérstva rizika a akékoľvek následné modifikácie sa prime- rane oznámusujú.
• jestvuje primerané podávanie vnútorných správ o štruktúre, jej efektivnosti a výsledkoch,
• na príslušných úrovniach a vo vhodnom čase sú dostupné závažné informácie odvozené z aplikácie manažérshta rizika,
• jestvujú konzultačné procesy s internými zainteresovanými účastníkmi.


Vytvorenie mechanizmov externej komunikácie a oznamovania

Organizácia má vypracovať a zaviesť plán, ako bude komunikovať so zainteresovanými účastníkmi.

Plán komunikácie so zainteresovanými účastníkmi má zahŕňať:
• angažovanie vhodných externých zainteresovaných účastníkov a zabezpečenie efektívnej výmeny informácií,
• externé podávanie správ v súlade so zákonnými, predpisovými a vládnymi požiadavkami,
• poskytovanie spätných väzín a podávanie správ o komunikácii a konzultáciiach,
• využívanie komunikácie na vytváranie dôvery v organizácii,
• komunikáciu so zainteresovanými účastníkmi v prípade krízovej situácie alebo nepredvídané dejnosti.

Mechanizmy externej a internej komunikácie a oznamovania majú podľa potreby obsahovať procesy zjednocovania informácií o rizikách z rozličných zdrojov a môžu vyžadovať zvažovanie citlivosti informácií.

ZAVEDENIE MANAŽÉRSTVA RIZIKA

Zavenie manažérstva rizika je podľa STN ISO 31000:11 proces, ktorý obsahuje:

1. Zavenenie štruktúry manažérstva rizika

Pri zavádzaní organizačnej štruktúry manažérstva rizika organizácia má:
• definovať vhodný harmonogram a vhodnú stratégiu zavádzania štruktúry,
• aplikovať politiku manažérstva rizika a súvisiaci proces na organizačné procesy,
• byť v súlade s požiadavkami zákonov a predpisov,
• zabezpečiť, aby prijímanie rozhodnutí vrátane vývoja a určovania cieľov bolo v súlade s výstupmi procesov manažérstva rizika,
• poskytovať informácie a školiace príležitosti,
• komunikovať a konzultovať so zainteresovanými účastníkmi s cieľom ubezpečiť sa, že jej štruktúra manažérstva rizika je nadálne vhodná.

2. Zavenenie procesu manažérstva rizika.

Manažérstvo rizika sa má zaviesť na základe ubezpečenia, že proces manažérstva rizika sa realizuje na základe plánu manažérstva rizika na všetkých príslušných úrovniach a na všetky funkčné miesta v organizácii ako súčasť jej praktík a procesov.

MONITOROVANIE A PRESKÚMÁVANIE ŠTRUKTÚRY

Monitorovanie (monitoring) znamená sledovanie a nepretržité kontrolovanie, dozor, a kritické pozorovanie. Znamená to určovanie aktuálneho stavu, s cieľom zistiť zmenu požadované alebo očakávané úrovne činnosti.
Preskúmanie (review) znamená činnosť, vykonávanú s cieľom určiť vhodnosť, primeranosť a efektívnosť sledovanej záležitosťi a dosiahnuť určené ciele.

S cieľom uabezpečiť sa, že manažérstvo rizika je efektívne a naďalej podporuje výkonnosť organizácie, organizácia má:

- merat’ výkonnosť manažérstva rizika pomocou ukazovateľov, ktorých vhodnosť sa periodicky preskúmava,
- periodicky merat’ pokrok oproti plánu manažérstva rizika, ako aj prípadné odchylky,
- periodicky preskúmavat’, ši štruktúru, politiku a plán manažérstva rizika sú stále v daných externých a interných súvislostiach vhodné,
- podávať správy o rizikách, pokroku v pláne manažérstva rizika a ako sa dodržiava politika manažérstva rizika,
- preskúmavat’ efektívnosť štruktúry manažérstva rizika.

NEPRETRŽITÉ ZLEPŠOVANIE ŠTRUKTÚRY

Na základe výsledkov monitorovania a z preskúmavania sa majú prijať rozhodnutia, ako možno zlepšiť štruktúru manažérstva rizika, politiku a príslušný plán. Takéto rozhodnutia by mali vyústiť do zlepšovania manažérstva rizika organizácie a jej kultúry manažérstva rizika.

7.2 LITERATÚRA

8 PROCES MANAŽÉRSTVA RIZIKA

Proces manažérstva rizika predstavuje systematickú aplikáciu manažérskej politiky, postupov a skúseností na súbor aktívnych činností, určených na vytváranie súvislostí, komunikáciu a poradenstvo s podnikateľskými partnermi a na identifikáciu, analyzovanie, hodnotenie, zaobchádzanie, monitorovanie a preskúmanie rizika. Proces manažérstva rizika má byť integrálnou súčasťou manažérstva, zabudovaný do kultúry a praktyk a prispôsobený podnikateľským procesom organizácie.

Zavedenie procesu manažérstva rizika zahŕňa (obr. 8):

a) Komunikáciu a poradenstvo.

b) Vytváranie súvislostí – vytváranie externých súvislostí, vytváranie interných súvislostí,

   vytváranie súvislostí procesu manažérstva rizika, definovanie kritérií rizika.

c) Posudzovanie rizika – identifikácia rizika, analýza rizika, hodnotenie rizika.

d) Zaobchádzanie s rizikom – výber jednej alebo viacerých možností zaobchádzania a ich zavedenie, príprava a zavedenie plánov zaobchádzania s rizikom.

![Obr. 8 Proces manažérstva rizika](image-url)
8.1 KOMUNIKÁCIA A PORADENSTVO

Komunikácia a poradenstvo s externými a internými zainteresovanými účastníkmi sa majú realizovať počas všetkých etáp procesu manažérstva rizika (obr. 9).

Zahrnutie zainteresovaných účastníkov do procesu manažérstva rizika prispeje k:
- vypracovaniu plánu komunikácie a poradenstva,
- zodpovednému stanoveniu štruktúry,
- zaistaniu, aby zainteresovaní účastníci boli pochopení a ich záujmy zohľadnené,
- prepojeniu rôznych oblastí odborných znalostí pre identifikáciu a analýzu rizika,
- zaistaniu, že rôzne hládanská budú vhodne zohľadnené pri hodnotení rizika,
- zaistaniu, že rizíká budú primerane identifikované,
- zabezpečeniu schválenia a podpory pre plán zaobchádzania s rizikami.

Efektívna vnútorná a vonkajšia komunikácia je potrebná, aby poverení pracovníci zodpovední za implementáciu manažérstva rizika a zainteresované strany spolu rozumeli, na akom základe sú prijímané rozhodnutia a tiež rozumeli dôvodom, prečo sú vyžadované určité činnosti. Počas celého procesu manažérstva rizika sa vyskytuje množstvo rôznej písomnej a ústnej komunikácie medzi rizikovým manažérom, vlastníkom rizika a zainteresovanými účastníkmi. Komunikovanie a konzultovanie tak predstavuje činnosť, ktorá má zjednodušiť presnú a zrozumiteľnú výmenu informácií, zohľadňujúc dôvernosť a osobnú integritu zainteresovaných strán.

Plány komunikácie a poradenstva sa majú vypracovať v rannom štádiu, aby sa mohli využívať počas všetkých etáp procesu manažérstva rizika. Plány sa majú týkať skutočností súvisiacich so samotným rizikom, jeho pričinami, následkami (ak sú známe), ako aj opatrení prijímaných na zaobchádzanie s rizikom.

Má sa uskutočniť efektívna interná a externá komunikácia a konzultácie s cieľom upevniť proces manažérstva rizika. Má sa uskutočniť efektíva, aby poverení pracovníci zodpovední za zavedenie procesu manažérstva rizika a zainteresované strany spoločne rozumeli, na akom základe sú prijímané rozhodnutia a ich dôvodu, prečo sa vyžadujú konkrétne činnosti.

Konzultácia a komunikácia znamená nepretržité a postupné procesy, ktoré organizácia vykonáva s cieľom poskytnúť informácie, podieľať sa na nich alebo ich získať a zapojiť sa do dialógu so zainteresovanými účastníkmi v problematike manažérstva rizika. Informácie sa môžu týkať existencie, podstaty (charakteru), formy, pravdepodobnosti, významu, hodnotenia, prijateľnosti a procesu zaobchádzania v manažérstve rizika.

Konzultácia je dvojsmerný proces komunikácie o informáciách medzi organizáciou a zainteresovanými účastníkmi pre potreby rozhodovania alebo určenie smerovania. Konzultácia je proces, ktorý ovplyvňuje rozhodovanie skôr prostredníctvom autority než síly a tvorbu vstup pre rozhodovanie, nie tvoru rozhodnutia.

Konzultácia a konzultácie so zainteresovanými účastníkmi sú dôležité, pretože zainteresovaní účastníci posudzujú riziko podľa svojho vnímania. Toto vnímanie sa môže meniť vzhľadom na rozdielnosť hodnôt, potrieb, predpokladov, koncepcií, prístupov a záujmov zainteresovaných účastníkov. Keďže ich názory môžu mať významný vplyv na prijímané rozhodnutia, majú sa pri prijímaní rozhodnutí identifikovať, zaznamenávať a zohľadňovať názory zainteresovaných účastníkov.

Komunikácie a konzultácie majú uľahčovať správnu a pochopiteľnú výmenu informácií vzhľadom na aspekty dôvernosti a ochrany osobností.

Komunikácia sa uskutočňuje prostredníctvom poradenského (konzultačného) tímu.
Prístup poradenského tímu môže:
- pomôcť určiť **primerané súvislosti manažérstva rizika**,  
- zabezpečiť, že sa **pochopia a zvážia záujmy zainteresovaných účastníkov**,  
- pomôcť ubezpečiť, že sa **riziká primerane identifikovali**,  
- pospájať rozlíčné oblasti **expertízy** na analýzu rizík,  
- ubezpečiť, že sa v **definícií kritérií rizika a pri vyhodnocovaní rizík** vhodne zvážili rozličné názory,  
- zabezpečiť vypracovanie a podporu **Plán zaobchádzania s rizikom**,  
- zvýrazniť vhodné **manažérstvo zmény** počas procesu manažérstva rizika,  
- vyvinúť vhodný **Plán externej a internej komunikácie a konzultácií**.

Obr. 9 Komunikácia a poradenstvo vo všetkých fázach manažérstva rizika
8.2 VYTVÁRANIE SÚVISLOSTÍ

Proces manažérstva rizika musí začať tým, že definujeme, čo chceme dosiahnuť, a pochopíme vonkajšie a vnútorné faktory, ktoré môžu ovplyvniť úspech pri dosahovaní cieľov organizácie. Tento krok, nazvaný „vytváranie súvislostí“, nevyhnutne predchádza identifikácii rizika.

Vytváranie súvislostí znamená určenie vonkajších a vnútorných parametrov, ktoré sa musia brať do úvahy pri riadení rizika, a určenie oblastí a kritérií rizík pre stratégie manažérstva rizika. Cieľom vytvárania súvislostí je nastavenie parametrov a hraníc vymedzujúcich jednoznačný postoj organizácie k riziku a aktivitám manažmentu rizík, ktoré má organizácia zohľadniť v manažérstve rizika.

Veľa z týchto parametrov sa podobá parametrom uvedeným v návrhu štruktúry manažérstva rizika. Pri určovaní súvislostí v procese manažérstva rizika sa musia brať do úvahy s väčšimi podrobnosťami a najmä zvážiť, ako súvisia so zámerom konkrétneho procesu manažérstva rizika.

Vytváraním súvislostí organizácia:
- stanoví ciele posudzovania rizík,
- definuje interné a externé parametre v manažérstve rizika,
- určuje rozsah kritérií rizík pre zostávajúci proces.

Dôležitou súčasťou vytvárania súvislostí je identifikovanie zainteresovaných účastníkov a pochopenie ich cieľov a potrieb, aby sme ich mohli zohľadniť a vzťať do úvahy ich cieľov pri stanovovaní kritérií rizík. Analýza zainteresovaných účastníkov je často aj súčasťou kroku „komunikácia a poradenstvo“ a pokračuje v priebehu celého procesu manažérstva rizík.

Vytváranie súvislostí v procese manažérstva rizika zahŕňa:
- vytváranie externých súvislostí,
- vytváranie interných súvislostí,
- vytváranie súvislostí procesu manažérstva rizika,
- definovanie kritérií rizík.

Externé súvislosti


Externé súvislosti môžu zahŕňať:
- sociálne, kultúrne, politické, právne, finančné, technické, ekonomické, prírodné a konkurénčné faktory prostredia na medzinárodnnej, národnej, regionálnej alebo miestnej úrovni,
- klúčové vplyvy a trendy, ktoré ovplyvňujú ciele organizácie,
- vzťahy, vnímanie a hodnoty externých zainteresovaných účastníkov,
- alebo neobmedzujú sa len na tieto skutočnosti.

Interné súvislosti

Interné súvislosti predstavujú interné prostredie, v ktorom organizácia chce dosiahnuť svoje ciele. Proces manažérstva rizika sa má zosúladit s kultúrou, procesmi, štruktúrou a
stratégiou organizácie. Interné súvislosti predstavujú niečo v rámci organizácie, čo môže ovplyvniť spôsob, akým organizácia bude riešiť riziko. Vytvoríť sa majú, pretože:

a) manažérstvo rizika sa realizuje v súvislosti s cieľmi organizácie,
b) ciele a kritériá konkrétneho projektu, procesu alebo konkrétnej činnosti sa majú brať do úvahy z pohľadu celkových cieľov organizácie,
c) niektoré organizácie zlyhávajú pri uvedomovaní si príležitosti dosiahnuť svoje strategické, projektové alebo podnikateľské cieľy, aby tak ovplyvňovali trvalý záväzok organizácie, jej vieronhodnosť, dôveru a hodnotu.

Interné súvislosti môžu zahŕňať:
a) riadenie, organizačnú štruktúru, úlohy a zodpovednosti,
b) zámery (ciele) a strategiu, ktorá sa využíva na ich dosiahnutie,
c) politiky a procesy,
d) spôsobilosť organizácie v zmysle zdrojov a znalostí (napr. kapitál, čas, ľudia, procesy, systémy a technológie),
e) informačné systémy, tok informácií a procesy prijímania rozhodnutí (oficiálne i neoficiálne),
f) vzťahy s internými zainteresovanými účastníkmi, ich vnímanie a hodnoty,
g) vnímanie hodnôt a kultúry organizácie,
h) normy, návody, a modely prijaté organizáciou,
i) formu a rozsah zmluvných vzťahov,
j) ale neobmedzujú sa len na tieto skutočnosti.

Charakteristika externých a interných súvislostí je uvedená v Prílohe B.

Inventarizácia významných aktív

V manažérstve aktív organizácie sa inventarizujú všetky aktíva, vo všetkých priestoroch. Ochrana priestorov a objektov sa však organizuje len v priestoroch, kde sú umiestnené významné aktíva, nie vo všetkých priestoroch, napr. v miestnosti pre upratovačku nie sú tak dôležité aktíva, že by potrebovali ochranu.

Inventarizácia významných aktív sa preto využíva na určenie:

• významných aktív organizácie, ktoré je potrebné chrániť a priestorov, v ktorých sú uložené,
• súčasnej ochrany týchto priestorov (chránených priestorov) bezpečnostnými prostriedkami alebo fyzickou ochranou,
• či je potrebné doplniť alebo nahradit’ súčasné zabezpečenie chránených priestorov,
• kritérií rizika v závislosti od celkovej hodnoty aktiv organizácie (majú byť primerané).

Pri inventarizácii významných aktív je potrebné zahrnúť priestory a objekty celej organizácie, ale aj významné aktíva, umiestnené v jednotlivých priestoroch vo vnútri objektov, ktoré sa nazývajú chránené priestory.

Medzi aktíva, ktoré je potrebné chrániť v priestoroch a objektoch organizácie, možno zaradit’ najmä:

• oplotenie a vstupy,
• dôležité budovy, napr. administratívna budova, budovy s výrobnými priestormi, budovy skladov tovaru, sklady zásob a náhradných dielov, garáže pre osobné a nákladné vozidlá,
• technické zariadenia budov – kanalizácia, vodovod, plynovod, vykurovanie, výtahy,
• informačné a komunikačné technológie a informačné systémy,
• výrobné činnosti alebo činnosti poskytujúce služby,
• životné prostredie,
• prísunové a odsunové komunikácie,
• ďalšie objekty podľa účelu organizácie.

Medzi významné aktíva, umiestnené v jednotlivých chránených priestoroch vo vnútri objektov, patria najmä:
• priestory so zamestnancami,
• priestory s utajovanými skutočnosťami,
• priestory s finančnou hotovosťou, napr. učtáreň, pokladňa,
• priestory s inými významnými hodnotami, napr. pošta, server, počítačové miestnosti, pre-
dajne so zásobami a pod.,
• priestory, v ktorých sa vykonávajú dôležité činnosti, ktoré by pri prerušení spôsobili výz-
namné straty, napr. kancelárie vrcholového manažmentu, výrobné linky a pod.,
• priestory s uloženými nebezpečnými látkami,
• priestory, v ktorých sú umiestnené zariadenia dôležité pre nepretržitý chod organizácie, napr. rozvody energie, vody, plynu, kotolne, kuchyne,
• ďalšie priestory, v ktorých sú umiestnené významné hmotné a nehmotné aktíva, alebo
v ktorých sa vykonávajú dôležité činnosti.

Na spracovanie zoznamu významných aktív (tab. 6) nie je stanovený formát, každá
organizácia však môže využiť svoj inventárny zoznam všetkých aktív spracovaný v písomnej
alebo elektronickej forme. Pre spracovanie prehľadu významných aktív, na ktoré môžu naj-
viac pôsobiť vonkajšie alebo vnútorné riziká je potrebné uviesť najmä:
• objekt,
• umiestnenie aktíva v objekte (chránený priestor),
• počet osôb v danom priestore,
• rozsah hmotného a nehmotného majetku v danom priestore a jeho finančná hodnota,
• spôsob súčasnej ochrany chráneného priestoru.

<table>
<thead>
<tr>
<th>Chránený priestor</th>
<th>Počet osôb</th>
<th>Majetok</th>
<th>Stav ochrany</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Objekt: Administratívna budova</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>101 Recepcia, prízemia</td>
<td>1</td>
<td>Počítač, telefóny... 5.000 €</td>
<td>recepčný, typ dverí, kamera,</td>
</tr>
<tr>
<td>105 Server, prízemia</td>
<td>2</td>
<td>IKT 50.000 €</td>
<td>poplachové zariadenie</td>
</tr>
<tr>
<td>207 Spisovňa, 2. poschodie</td>
<td>2</td>
<td>Utajované dokumenty, zmluvy, V, T, 2 počítače – veľká škoda</td>
<td>poplachové zariadenie</td>
</tr>
<tr>
<td>508 Pokladňa, 5. poschodie</td>
<td>4</td>
<td>4 počítače, trezor s finančnou hotovosťou, kalkulačky... 100.000 €</td>
<td>poplachové zariadenie napojené na PZ</td>
</tr>
<tr>
<td>601 Kancelária riaditeľa, 6. poschodie</td>
<td>2</td>
<td>Nábytok, počítačí... 10.000 €</td>
<td>dvere typu, okná typu poplachové zariadenie...</td>
</tr>
<tr>
<td><strong>Objekt: Garáže</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01 osobné</td>
<td>Škoda SUPERB – 25000 € Volkswagen – 18000 €</td>
<td>plechové dvere, kamera</td>
<td></td>
</tr>
</tbody>
</table>

Na základe posúdenia už zavedeného spôsobu ochrany jednotlivých chránených
priestorov zodpovední funkcionári rozhodnú či je potrebné ochranu doplniť, či zaviesť nový
alebo iný spôsob ochrany. Rozsah chránených priestorov, pre ktoré sa musia identifikovať
riziká sa takto môže znižiť.
Súvislosti procesu manažérstva rizika

Pri vytváraní súvislostí procesu manažérstva rizika sa určia:

- **ciele, stratégia, rozsah a parametre činnosti** organizácie alebo časti organizácie, na ktoré sa aplikuje manažérstvo rizika,
- **zodpovednosti a právomoci,**
- **požadované zdroje,**
- **zdokumentované informácie, ktoré treba uchovávať.**

Súvislosti procesu manažérstva rizika sa budú meniť v závislosti od potrieb organizácie. Môžu zahŕňať:

- definovanie **zámeru a cieľov** manažérstva rizika,
- vymedzenie **zodpovedností** v rámci procesu a za proces manažérstva rizika,
- definovanie **rozsahu, hĺbky a šírky činností manažérstva rizika,** ktoré sa majú vykonáť, vrátane špecifických činností, ktoré majú byť do procesu zahrnuté a tých, ktoré majú byť z procesu vylúčené,
- definovanie **činnosti, procesu, funkcie, projektu, produktu, služby alebo prínosu v zmysle času a lokalizácie,**
- definovanie **vzťahov** medzi konkrétnym projektom, procesom, alebo konkrétnej činnost’ou a ďalším projektmi, procesmi alebo činnost’ami v rámci organizácie,
- určenie **metódik posudzovania rizika,**
- vymedzenie **kritérií rizík,**
- definovanie spôsobu **hodnotenia výkonnosti a efektívnosti** v manažérstve rizika,
- identifikácia a špecifikácia **rozhodnutí a zásahov,** ktoré treba prijať,
- identifikácia, skúmanie **súvislostí a potrebnej štruktúry,** ich rozsahu a cieľov, ako aj **zdrojov** požadovaných na takéto skúmanie.

Pozornosť venovaná obsahu súvislostí procesu manažérstva rizika má ubezpečiť, že prijatý prístup k manažérstvu rizika zodpovedá okolnostiam, organizácií a rizikám ovládaným dosiahnutie cieľov organizácie.
8.3 DEFINOVANIE KRITÉRIÍ RIZIKA

Pred posudzovaním rizík sa definujú kritériá rizika. Kritériá rizika definuje vrcholový manažment organizácie v závislosti na veľkosti svojich aktiví. Organizácia definovaním kritérií rizika určuje, aká miera (závažnosť) rizika je pre ňu ešte prijateľná.

Kritériá rizika predstavujú súbor podkladov, v porovnaní s ktorými sa bude hodnotiť závažnosť rizíka. Sú založené na cieľoch organizácie a vonkajších a vnútorných súvislostiach, môžu byť odvodnené z noriem, zákonov, politíky a iných požiadaviek.

Kritériá rizika:
• majú byť v súlade s politicou manažérstva rizika organizácie,
• musia sa definovať na začiatku procesu manažérstva rizika,
• musia sa neustále preskúmavať a prehodnocovať.

Pri definovaní kritérií rizika uvažované faktory majú zahŕňať:
• podstatu a druhy príčin následkov, ktoré môžu nastať a spôsoby ich merania,
• ako sa bude definovať pravdepodobnosť,
• časový rámec (časové rámce) pravdepodobnosti alebo následku (následkov) – obvykle krátkodobý, strednodobý, dlhodobý rámec alebo sa odhadujú mesiace či roky,
• ako sa určí úroveň rizika,
• názory zainteresovaných účastníkov,
• úroveň, na ktorej bude rizíko prijateľné alebo prípustné,
• úroveň, pri ktorej sa rozhodne o dalsom zaobchádzaní s rizikom,
• úvahu, či treba zohľadňovať kombinácie viacnásobných rizík, a ak áno, ako a ktoré kombinácie treba zvažovať.

Pri stanovení kritérií rizika je vhodné využiť techniku Matice následkov a pravdepodobnosti z STN EN 31010 (tab. 7-10), pričom je potrebné dodržať nasledujúci postup:
1. Určiť rozsah stupňov následkov a pravdepodobnosti a hodnoty možných následkov a pravdepodobnosti pre jednotlivé vybrané stupne (krok 1 – Stupnica následkov, Stupnica pravdepodobnosti):
   a) niektoré organizácie používajú iba tri stupne následkov i pravdepodobnosti, napr. malé, stredné, veľké, ale možno využiť aj viac stupňov, napr. veľmi malé, malé, stredné, veľké, veľmi veľké a pod.,
   b) určiť kategórie aktív, pre ktoré sa budú určovať následky, napr.:
      • majetkové straty, návratnosť investícií – finančný dosah,
      • zdravie a pracovná bezpečnosť – pracovná neschopnosť, invalidita, usmrtenie,
      • prostredie a verejnosť – stupne a doba poškodenia prostredia, postoj verejnosti,
      • prerušenie prevádzky – doba vyradenia z prevádzky,
      • povest’ organizácie – medializácia, dopad na povest’ partnerov a strata podpory partnerov a investícií,
      • ciele organizácie – úroveň vplyvu na ich dosiahnutie,
      • právo a jeho dodržiavanie – náklady na žaloby a súdy, postih manažérov, zamestnancov a celej organizácie,
      • iné kategórie.
   c) Určiť hodnoty možných následkov a pravdepodobnosti pre jednotlivé zvolené kategórie aktív.
2. Spracovať matiču rizika - pomôcka na hodnotenie a zobrazenie rizík, definovaním následku a pravdepodobnosti, (krok 2).
3. Stanovíť **kategórie a intervály kritérií rizika** pre hodnotenie úrovne rizík:
   - niektoré organizácie používajú iba kategórie prijateľné/akceptovateľné riziko a neprijateľné/neakceptovateľné riziko,
   - pre podrobnejšie hodnotenie je výhodné využívať kategórie prijateľné/akceptovateľné riziko, prípustné nežiaduce riziko, prípustné znesiteľné riziko a neprijateľné/neakceptovateľné riziko,
   - pre zvolené kategórie stanovíť podľa matice rizík **intervaly veľkosti** (krok 3).

   **Tab. 7 Stupnica následkov (krok 1)**

<table>
<thead>
<tr>
<th>Hodnota následku</th>
<th>Majetkové straty</th>
<th>Zdravotnícke straty</th>
<th>Prerušenie prevádzky</th>
<th>Povest' organizácie</th>
<th>Ciele organizácie</th>
</tr>
</thead>
<tbody>
<tr>
<td>Veľmi malý</td>
<td>Finančné straty do 5 000 €</td>
<td>Žiadne alebo len ľahké zranenie s prvou pomocou, bez PN</td>
<td>Kritické systémy vyradené do 1 hodiny</td>
<td>Zanedbateľný vplyv</td>
<td>Vyriešené v každodennom riadení</td>
</tr>
<tr>
<td>Malý</td>
<td>Finančné straty do 10 000 €</td>
<td>Menšie zranenia, lekárske ošetrenia, PN niekoľko dní</td>
<td>Kritické systémy vyradené na niekoľko hodín</td>
<td>Nežiaduce, iba miestne mediálné pokrytie</td>
<td>Menší vplyv</td>
</tr>
<tr>
<td>Stredný</td>
<td>Finančné straty do 25 000 €</td>
<td>Zranenia, možná dlhodobá hospitalizácia</td>
<td>Kritické systémy vyradené kratšie ako deň</td>
<td>Nežiaduce, medzinárodné média v hlavnom meste</td>
<td>Významný vplyv</td>
</tr>
<tr>
<td>Veľký</td>
<td>Finančné straty do 50 000 €</td>
<td>Jedno úmrie alebo dlhodobá choroba, alebo viac vážnych zranení</td>
<td>Kritické systémy vyradené na deň</td>
<td>Nežiaduce, rozšírené celoštátne mediálné pokrytie</td>
<td>Hlavný vplyv</td>
</tr>
<tr>
<td>Veľmi veľký</td>
<td>Finančné straty nad 100 000 €</td>
<td>Umrtia alebo trvalé postihnutia, alebo zlý zdravotný stav s následkami</td>
<td>Kritické systémy vyradené dlhšie než 1 deň</td>
<td>Potreba informovať vládu</td>
<td>Katastrofálny vplyv</td>
</tr>
</tbody>
</table>

   **Tab. 8 Stupnica pravdepodobnosti (krok 1)**

<table>
<thead>
<tr>
<th>Pravdepodobnosť</th>
<th>Očakávané alebo skutočné pravdepodobnosti a frekvencie udalostí</th>
</tr>
</thead>
<tbody>
<tr>
<td>Veľmi malá</td>
<td>Môže dôjsť len vo výnimočných prípadoch, bez predchádzajúceho výskytu</td>
</tr>
<tr>
<td>Malá</td>
<td>Mohlo by dôjsť raz za rok; menej ako 25% šanca, že sa vyskytne</td>
</tr>
<tr>
<td>Stredná</td>
<td>Môže dôjsť raz za pol roka; 25 -50% pravdepodobnosť, že sa vyskytne</td>
</tr>
<tr>
<td>Veľká</td>
<td>Nastane pravdepodobné raz za 3 mesiace, 50-75% šanca na vyskytnutie</td>
</tr>
<tr>
<td>Veľmi veľká</td>
<td>Možno očakávať raz za mesiac, viac ako 75% šanca, že sa vyskytne</td>
</tr>
</tbody>
</table>
### Tab. 9 Matica rizika (krok 2)

<table>
<thead>
<tr>
<th>Následky</th>
<th>Pravdepodobnosť</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Veľmi malá</td>
</tr>
<tr>
<td>1 Veľmi malý</td>
<td>1</td>
</tr>
<tr>
<td>2 Malý</td>
<td>2</td>
</tr>
<tr>
<td>3 Stredný</td>
<td>3</td>
</tr>
<tr>
<td>4 Veľký</td>
<td>4</td>
</tr>
<tr>
<td>5 Veľmi veľký</td>
<td>5</td>
</tr>
</tbody>
</table>

### Tab. 10 Kritériá rizika (krok 3)

<table>
<thead>
<tr>
<th>Kategória</th>
<th>Hodnota P/N</th>
<th>Charakter rizika</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neprijateľné neakceptovateľné</td>
<td>17-25</td>
<td>Vyžaduje zastavenie prebiehajúceho procesu a prijatie regulačných opatrení na jeho zniženie. Môže ohroziť prežitie alebo udržanie efektívneho fungovania programu alebo organizácie, či už finančné alebo politicky. <strong>Bezprostredný zásah</strong> musí byť riadený vrcholovým manažmentom s podrobným Plánom zaobchádzania s rizikami, Hlásenie nadriadeným orgánom.</td>
</tr>
<tr>
<td>Pripustné nežiaduce (neželateľné)</td>
<td>12-16</td>
<td>Nežiaduce riziko, pripustné len v prípade, ak jeho zniženie sa nedá uskutočniť alebo je značne neefektívne (náklady na zniženie vysoko prevyšujú prínosy). Môže spôsobiť nejaké škody, narušenia alebo porušenia riadenia. <strong>Správa</strong> – vrcholové vedenie musí venovať pozornosť a zodpovedať za riadenie (modifikovanie) týchto rizík. <strong>Hlásenie nadriadeným orgánom</strong>.</td>
</tr>
<tr>
<td>Pripustné znesiteľné</td>
<td>5-11</td>
<td>Riziko je pripustné po zvažení nákladov na jeho zniženie, ak prínosy prevyšujú náklady na jeho zniženie. Pravdepodobne nespôsobí veľké škody alebo neohrozí účinnosť a efektívnosť činnosti. <strong>Správa</strong> – podľa osobitného monitorovania a reakcie postupov. <strong>Hlásenie nadriadeným orgánom</strong>.</td>
</tr>
<tr>
<td>Prijateľné zanedbaneľná úroveň</td>
<td>1-4</td>
<td>Predstavuje spoločensky prijateľnú úroveň rizika, pri ktorej sa nevyžadujú regulačné opatrenia na jeho zniženie. <strong>Správa</strong> – bežnými postupmi. Monitorovanie a hodnotenie.</td>
</tr>
</tbody>
</table>

87
Uvedené kritériá sú stanovené pre *bezpečnostné riziká*, pri ktorých sa nepredpokladajú pozitívne výsledky. Možné stanovenie pravdepodobností ohrozenia i príležitosti pre špekulatívne (podnikateľské) riziká uvádza tab. 11.

Tab. 11 Pravdepodobnosť výskytu ohrozenia alebo príležitosti (zdroj Inštitút riadenia rizík)

<table>
<thead>
<tr>
<th>Oceňenie</th>
<th>Pravdepodobnosť udalosti ohrozenie</th>
<th>Pravdepodobnosť udalosti príležitosti</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vysoká (pravdepodobná)</td>
<td><strong>Popis</strong></td>
<td>Možnosť opakovaneho výskytu v určitom časovom období (napr. 10 rokov). Vyskytla sa nedávno.</td>
</tr>
<tr>
<td>Stredná (možná)</td>
<td><strong>Popis</strong></td>
<td>Mohla sa vyskytnúť viac než raz v určitom časovom období (napr. 10 rokov). Hrozbu je ťažké kontrolovať pre niektoré vonkajšie vplyvy. Vyskytla sa v minulosti?</td>
</tr>
<tr>
<td>Nízka (nepredpokladaná)</td>
<td><strong>Popis</strong></td>
<td>Doteraz sa nevyskytla. Výskyt je nepravdepodobný.</td>
</tr>
</tbody>
</table>
8.4 POSUDZOVANIE RIZIKA

Posudzovanie rizík patri medzi časť manažérstva rizika, ktorá poskytuje štruktúrovaný proces, pri ktorom sa zisťuje, ako môžu byť ovplyvené ciele organizácie a pomocou ktorej sa analyzujú rizík v zmysle následkov a ich pravdepodobnosti predtým, než sa rozhodne, či je potrebné ďalšie zaobchádzanie s rizikom. Pri posudzovaní rizík treba odpovedať na nasledujúce zásadné otázky:

• čo sa môže stať a prečo (pomocou identifikácie rizík)?
• aké sú následky?
• aká je pravdepodobnosť ich ďalšieho výskytu?
• existujú nejaké faktory, ktoré zmiernia následky rizíka alebo ktoré znižia pravdepodobnosť rizíka?
• je úroveň rizíka únosná, alebo prijateľná a vyžaduje ďalšie zaobchádzanie?

Posudzovanie rizíka je súhrnný proces:

a) identifikácia rizík – proces, ktorý sa používa na nájdenie, preskúmanie a popísanie rizík, ktoré by mohli ovplyvniť dosiahnutie cieľov (zámerov),

b) analýza rizík – proces, ktorý sa používa na pochopenie podstaty, zdrojov a príčín rizík na určenie a ocenenie úrovne rizíka, používa sa aj na skúmanie ich dopadov a následkov a preskum zavedených opatrení na riadenie rizíka,

c) hodnotenie rizík – proces, ktorý sa používa na porovnanie výsledkov analýzy rizík s kritériami rizíka a rozhodnutie či zistená úroveň rizíka je prijateľná, neprijateľná alebo pripustná.


Rizíká môžu byť posúdené na úrovni organizácie alebo jej časťí, pre projekty, jednotlivé činnosti alebo ako jednotlivé rizíká. Posudzovanie rizík umožňuje riadiaci pracovníkom a zainteresovaným účastníkom lepšie chápať rizíká, ktoré by mohli ovplyvniť dosahovanie cieľov, ich príčiny, následky a pravdepodobnosti a efektívnosť opatrení zavedených na riadenie rizíka. To poskytuje základ pre rozhodovanie o nasledujúcich skutočnostiach:

• či má byť činnosť podniknutá,
• ako maximalizovať príležitosti,
• či je potrebné zaobchádzanie s rizíkami,
• o voľbe medzi variantmi s rôznymi rizíkami,
• o stanovení priorít pri voľiteľnej možnosti variantov zaobchádzania s rizíkam,
• o najvhodnejšej voľbe stratégií zaobchádzania s rizíkom, pomocou ktorých sú nepriaznivé rizíká modifikované na prijateľnú úroveň.

Výstup z posudzovania rizík je vstupom do procesov rozhodovania danej organizácie. Spôsob, akým sa proces posudzovania rizík uskutoční, nezáleží iba na súvislostiach procesu manažérstva rizíka, ale tiež na metódach použitých pri vykonávaní posudzovania rizík. Posudzovanie rizík môže vyžadovať multidisciplinárný prístup, pretože rizíká môžu zahŕňať široký rozsah podniknutia.

Medzi základné prínosy posudzovania rizík patria:
• cieľove rizík a potenciálneho dopadu na ciele,
• poskytovanie informácií pracovníkom, ktorí vyháňajú rozhodnutia, 
• prispievanie k cieľovom pomoci pri výbore variantov zaobchádzania s rizikam a slabých článkov v organizácii, 
• porovnanie rizík v alternatívnych systémoch, technológiách a prístupoch,
• oznamovanie rizík a neistôt,
• pomoc pri stanovení priorit pre zaobchádzanie s rizikom,
• možnost' vybrať rôznych foriem zaobchádzania s rizikom,
• príspevok k predchádzaniu incidentom na základe vyšetrovania po incidente,
• plnenie požiadavie, ktoré vyplývajú z predpisov a nariadení,
• poskytovanie informácií, ktoré pomôžu zhodnotiť, či má byť riziko prijaté, keď sa porovná
s vopred určenými kritériami,
• posudzovanie rizík pre vyrovnání sa na konci životnosti.

**Posudzovanie rizík v priebehu etáp životného cyklu**

Pre životný cyklus, od etapy počiatočnej koncepcie a stanovenia požiadaviek, cez rea-
lizáciu až po záverečné ukončenie, ktoré môže zahrňať spôsobenie škôd a vyradenie
z prevádzky, je nutné zvážiť množstvo činností, projektov a produktov. Posudzovanie rizík sa
môže aplikovať vo všetkých etapách životného cyklu, a zvyčajne sa aplikuje veľačrát, s rôz-
nymi úrovňami detailov tak, aby napomáhalo pri rozhodovaniach, ktoré sa musia vykonávať
v každej etape.

Etapy životného cyklu majú rôzne požiadavky a vyžadujú rôzne techniky, napr., keď
je v etape počiatočnej koncepcie a stanovenia požiadaviek identifikovaná príležitost', posúde-
nie rizík sa môže použiť na rozhodnutie, či pokračovať, alebo nie. Ak je k dispozícii niekoľko
možností hodnotenia rizika, môže byť posudzovanie rizík použité na vyhodnotenie alternatív-
ných koncepcii, ktoré pomôžu rozhodovaniu, čo poskytuje najlepšie vyváženie pozitívnych
a negatívnych rizík. Počas etapy návrhu a vývoja prispieva posudzovanie rizík pre:
• zaistenie, že riziká systému sú prijateľné,
• proces spresnenia návrhu,
• štúdie nákladovej efektívnosti,
• identifikáciu rizík, ktoré majú dopad na nasledujúce etapy životného cyklu.
8.5 IDENTIFIKÁCIA RIZIKA

Identifikácia rizika znamená proces hl’adania, spoznávania a popísania rizika.

Identifikácia rizika zahŕňa identifikáciu:

1. zdrojov rizika – prvkov, ktoré samy osebe alebo v kombinácií majú vnútorný potenciál vyvoláť riziko a oblasti ich následkov,
2. udalostí, ktoré zdroje rizika môžu spôsobiť,
3. okolností, ktoré by mohli mať potenciálne následky na dosiahnutie cieľov,
4. príčin rizika – toho, ČO sa môže stať, Kedy a Kde, Prečo a AKO sa to môže stať,
5. potenciálnych následkov,
6. opatrení zavedených na modifikáciu rizika.

Cieľom identifikácie rizík je vytvoriť obsažný zoznam rizík a násl murderous, založený na udalosťiach, ktoré by mohli vytvoriť, podporiť, zabrániť, znehodnotiť, urýchliť, alebo pozdržať dosiahnutie cieľov.

Účelom identifikácie rizík je zistiť, čo by sa mohlo stať alebo aké by mohli nastať situácie, ktoré by mohli ovplyvniť dosiahnutie cieľov systému alebo organizácie. Hned, ako je riziko identifikované, má organizácia vytypovať vhodné opatrenia na jeho modifikáciu, ako sú napr. MZP, TZP, režimové opatrenia, fyzická ochrana a iné. Tieto opatrenia sa uvádzajú v zozname rizík.

Dôležité je identifikovať riziká, ktoré súvisia s nevyužitím príležitostí. Vyčerpávajúca identifikácia musí byť kritická, pretože rizík, ktoré nie sú identifikované v tejto etape sa nezahrnú do ďalšej analýzy. Následne tieto riziká nemôžu byť a ani nebúdú modifikované, alebo inak ovplyvňované.

Identifikácia rizika je rozhodujúcim predpokladom a východiskom na efektívne modifikovanie rizík. Platí zásada, že riziká sa musia identifikovať vo všetkých objektoch a chránených priestoroch, pretože pravdepodobnosť výskytu, ale najmä následok udalostí je v každom priestore, kde sa riziko vyskytuje, odlišná, napr. pravdepodobnosť požiaru v dielni s chemickými látkami je vyššia než v kancelárii a následok krádeže auta z garáže je vyšší než krádež počítača z kancelárie.

Pre každé aktívum v určitom chránenom priestore je potrebné identifikovať všetky možné riziká, ktoré naň môžu pôsobiť, napr. prípadné poškodenie, odskočenie alebo zničenie a tak ďalej. Identifikácia rizika má obsahovať preskúmanie vyvolaných účinkov s osobitnými následkami vrátane kaskádovitých a kumulatívnych účinkov. Údaje o rizikách sa mäť v zozname rizík, ktorý sa obnovuje na základe prípade.

Identifikácia má zahŕňať riziká bez ohľadu na to, či ich zdroj je pod kontrolou organizácie, dokonca aj vtedy, ak zdroj rizika alebo jeho príčina nie sú zrejmé. Identifikácia rizika má obsahovať preskúmanie vyvolaných účinkov s osobitnými následkami vrátane kaskádovitých a kumulatívnych účinkov. Údaje o rizikách sa mäť v zozname rizík, ktorý sa obnovuje na základe prípade.

Takisto treba posúdiť, čo by sa mohlo stať a zvážiť možné príčiny a okolnosti, ktoré naznačujú, aké následky by mohli nastať. Do úvahy sa majú vstúpiť všetky významné príčiny a následky. Pochopenie a vyhodnotenie príčin rizík sú životné dôležité informácie pre zaobchádzanie s rizikami.

Nedostatky, ktoré sa vyskytnú v systematickom procese identifikácie rizík môžu viesť organizácii k sústredeniu pozornosti len na známe riziká, a preto sa zabudne na tie, ktoré sú zatiaľ neznámé a ktoré potom nemôžu nikdy byť riešené zodpovedajúcim spôsobom.
Organizácia má využiť nástroje a techniky na identifikáciu rizika, ktoré zodpovedajú jej cieľom a spôsobilostí, ako aj vyskytujúcim sa rizikám. Tieto nástroje a techniky sú popísané v STN EN 31010 Manažérstvo rizika. Techniky posúdzovania rizík. Do identifikácie rizík sa majú zapájať lúdia s vhodnými vedomostami a skúsenosťami. Pri identifikácii rizík sú dôležité aktuálne a závažné informácie, ak je to možné, majú obsahovať vhodné informácie zo spätnej vázby.

Identifikácia rizika môže zahrať:
- historické údaje,
- teoretické analýzy,
- názory informovaných osôb a expertov,
- potreby zainteresovaných účastníkov.

Riziká predstavujú udalosti, ktoré pri spustení, môžu spôsobiť problémy alebo výhody. Identifikácia rizík musí preto začať od možných zdrojov rizík, napr. zainteresovaní účastníci, zamestnanci, meteorologické vplyvy, hlavné a podporné činnosti, informačné systémy a pod.

Identifikácia zdrojov (source identification) znamená proces nájdenia, zaznamenania a popísania zdrojov rizík. V kontexte bezpečnosti sa identifikácia zdrojov nazýva aj identifikácia nebezpečenstva. Pokiaľ je známy zdroj alebo problém, môžu sa udalosti, ktoré môže vyvoláť zdroj alebo udalosti riešiť, napríklad:
- účastníci zastavia priebeh projektu pri ohrození jeho financovania,
- doverné informácie môžu byť ukradnuté zamestnancami aj v rámci uzavretej siete.

V procese identifikácie rizík objektu a chránených priestorov sa obvykle uskutočňuje:
- fyzická prehliadka objektu a jeho okolia, chránených priestorov,
- štúdium hlavných a podporných činností,
- získavanie informácií od zamestnancov,
- konzultácie so zainteresovanými účastníkmi,
- štúdium tabuliek, diagramov, schém a priebehov udalostí v minulosti,
- preskum predchádzajúcich udalostí v rovnakom alebo podobnom odvetví,
- identifikácia možných zdrojov rizík a oblastí ich následkov,
- vytytovanie možných udalostí, ktoré môžu ovplyvniť zámery organizácie a ich pričin,
- spracovanie zoznamu rizík.

Po identifikácii rizíka by riziká mali byť potvrdené (napr. presnosť informácií na ktorých stojí), mali by sa skontrolovať charakteristiky ich popisu a zvažiť vol'by odozy (reakcie) na riziko – definovanie krokov na vylepšenie priležitosti a reakcie na ohrozenie (zaobchádzanie s rizikom).

8.5.1 Metódy (techniky) identifikácie rizíka

Podľa STN EN 31010 sa na identifikáciu rizík môžu využívať najmä tieto skupiny technik (metód):

1. Deduktívne metódy (metódy ex post) – metódy založené na dôkaze – sú založené na analýze už predtrým vzniknutých udalostí, hľadaní a objasnení ich pričin a súvislostí medzi nimi. Uvažuje sa poslednej udalosti a vyhľadávajú sa okolnosti, ktoré ju mohli zariadiť. Pomocou nich možno zostaviť scénáre vzniku a prejavov rôznych rizík, sú zdrojom inovácie procesov bezpečnostného manažmentu, patria sem napr. kontrolné zoznamy,
prespúmanie historických údajov, analýza stromu porúch (FTA), analýza druhov porúch a ich dôsledkov (FMEA), analýza druhov, dôsledkov a kritickosti porúch (FMECA).

2. Induktívne metódy (metódy ex ante) – umožňujú predviáť možné riziká pre chránené aktíva, pričom sa analyzujú zdroje, ktoré by mohli spôsobiť negatívne udalosti. Využitím týchto metód je možné vyhodnotiť predpokladaný (očakávaný, pravdepodobný) počet udalostí, odhadnúť ich možné následky a prijať vhodné preventívne opatrenia. Induktívne metódy spravidla využívajú:

a) Expertné odhady – systematické tímové prístupy, pri ktorých tím expertov vykonáva systematický proces, s cieľom identifikovať riziká pomocou štruktúrovaného súboru výziev alebo otázok. Podľa STN EN 31010 sa na identifikáciu rizík používajú najmä tie-to expertné techniky: brainstorming, štruktúrované alebo semištruktúrované rozhovory, technika Delphi, kontrolné zoznamy, matica následkov a pravdepodobnosti, štruktúra „čo sa stane, ak?“, okrem nich sa môžu použiť aj: nominálna skupinová technika, analýza úloh, zoznam rizík a pod.

b) Pravdepodobnostné modely – techniky induktívneho uvažovania – analyzujú sa možné budúce očakávané udalosti, ktoré môžu pozitívne alebo negatívne ovplyvniť zá-mery organizácie, pomáhajú vyhodnotiť pravdepodobnosť vzniku udalostí a ich násled-ky, obvykle sa využívajú pravdepodobnostné modely. Podľa STN EN 31010 sa na identifikáciu rizík používajú najmä nasledujúce pravdepodobnostné modely: predbežná analýza nebezpečenstva, štúdia nebezpečenstva a prevádzkyschopnosti HAZOP, analýza nebezpečenstva a kritické kontrolné body HACCP, analýza scenárlov, analýza príčin a následkov a následkov porúch, analýza pričín a následkov, analýza bezporuchovej činnosti člove-ka, údržba zameraná na bezporuchovosť, matica následkov a pravdepodobnosť. Okrem nich sa môžu použiť aj: analýza dopadov na podnikanie, analýza stromu poru-chových stavov, analýza stromu udalostí, analýza vztahu pričina – následok, analýza ochranných vrstiev LOPA, analýza parazitných javov, Markovova analýza, krvinky FN, indexy rizika, analýza nákladov a prínosov, analýza multikriteriálneho rozhodovania MCDA.

Pravdepodobnostné modely pracujú s rizikom ako s rýdzo pravdepodobnosťnou veličinou. Tento prístup je založený na tom, že sa daný jav vyskytuje s určitou pravdep-odo-bnosťou, ktorú je možné určiť na základe určitých štatistických veličín (napr. po-čet výskytov danej skupiny javov, dĺžky sledovaného obdobia a pod.). Pretože sledova-ných faktorov môže byť značné množstvo, proces je často komplikovaný a je možný iba s použitím počítačovej techniky.

Uplatnenie týchto modelov v bezpečnostnej praxi je preto veľmi zložité, pretože často chyba všetky štatistické údaje, na základe ktorých by sa mohli stanoviť parametre pravdepodobnostných vzťahov. Okrem toho niekedy ide aj o javy a udalosti, ktoré sa doposiaľ neobjavili. Korektné využitie týchto modelov je tiež možné len v prípadoch, keď sa podmienky a predpoklady daných javov v čase zásadne nemenia. V sociálnom prostredí sú ale východiskové podmienky vzniku relevantných udalostí veľmi prízna-čné.

8.5.2 Zoznam rizík

Výstupom z procesu identifikácie rizík je slovný popis rizík (Risk Description) v Zozname rizík (List Risks), ktoré organizácia podstupuje (niekedy sa používa aj Register rizík, Katalóg rizík, Checklist Risks). Cieľom popisu rizika je zachytiť identifikované riziko do štruktúrovaného prehľadného formátu, napr. tabuľky.
Na vytvorenie zoznamu rizík nie je stanovená žiadna norma (šablóna), ani nemusí byť zapísaný vo forme tabuľky. Štruktúru popisu je však v organizácii nutné riadne stanoviť, aby sa dosiahlo jednotný proces identifikácie, popisu a určenia. Je v zásade jedno, akou formou sa riziká popíšu, ale jednu stanovenú metodológiu potom treba dodržiavať v celej organizácii.

Riziká spojené s činnosťami a rozhodovaním organizácie môžu byť podľa Štandardu Inštitútu riadenia rizík rozdelené:
- podľa ich druhu, napríklad ako riziká stratégickej, finančné, prevádzkové, bezpečnostné atď.,
- podľa ich prítomnosti v jednotlivých chránených priestoroch.

Bezpečnostné riziká sa môžu usporiadať najmä do týchto kategórií:
- riziká úmyselného napadnutia – krádež, vlámanie, sabotáž, vandalizmus, špionáž, teroristický útok, narušenie vnútorného poriadku, pouličné nepokoje a pod.,
- náhodné bezpečnostné riziká:
  - zdravotné,
  - bezpečnosti práce,
  - personálnej bezpečnosti (vlastní zamestnanci, oprávnené osoby, ľudia, ktorí majú prístup k utajovaným informáciám – insideri, servisní zamestnanci a obslužný personál, pracovníci fyzickej ochrany, strážnej služby),
  - poškodenia mena organizácie (jej imidž, spoľahlivosť a pod.),
  - environmentálne,
  - prevádzkové – požiar, incidenty, prerušenie činnosti, nehoda, technické, technologické, dopravné a energetické havárie; katastrofy,
  - prírodné – živelné pohromy,
  - sociálne.

V zozname rizík je potrebné uviešť najmä:
- Základné informácie o riziku, napr.: číslo rizika, názov rizika, popis rizika, kategória rizika, zodpovednosť za riziko a zainteresované strany; dátum zistenia a posledná aktualizácia.
- Informácie pre analýzu rizík, napr.: pravdepodobnosť výskytu udalosti, následok udalosti, popis následku, časová os.
- Informácie o reakcii (odozve) na vyhodnotenie rizika: opatrenia na modifikáciu rizika; stav odpovede – neplánovaná, plánovaná, ale neprijatá; plán prijatý, ale účinnosť nie je doteraz známa; plán nadobudne plátnosť a účinnosť; stav rizika – otvorené (ešte môže nastať), uzavreté (skončilo alebo bolo ošetrené), vyradené (realizovalo sa); možné postupy pre zlepšenie.
Tab. 12 Možný obsah Zoznamu rizík (zdroj: A Risk Management Standard)

<table>
<thead>
<tr>
<th>Číslo rizika</th>
<th>R1 – Rx</th>
</tr>
</thead>
<tbody>
<tr>
<td>Názov rizika</td>
<td>Napr. Úmyselné napadnutie majetku</td>
</tr>
<tr>
<td>Popis rizika</td>
<td>Kvalitatívny popis udalostí, miesto, rozsah, druh, počet a závislosti, pro-stredie, úmysel, čo sa môže stať v budúcnosti a možný dopad na organi-záciu, napr. vlámanie do priestoru garáže v objekte garáži cez vstupné dvere, možnosť krádeže vozidiel, PHM, narušenie dopravnej kapacity organizácie</td>
</tr>
<tr>
<td>Kategória rizika</td>
<td>Napr. strategické, prevádzkové, finančné, bezpečnostné a iné</td>
</tr>
<tr>
<td>Zodpovednosť za riziko, zainteresované strany</td>
<td>Vlastník rizika – fyzická osoba zodpovedná za zabezpečenie toho, že pracovníci sa zodpovedným spôsobom zoznámili s vykonávanými pro-tiopatreniami Zainteresované strany, ich očakávanie a záujmy</td>
</tr>
<tr>
<td>Dátum hlásenia</td>
<td>Dátum, kedy bolo riziko prvýkrát zaznamenané (DD-MM-RR)</td>
</tr>
<tr>
<td>Pravdepodobnosť</td>
<td>Veľmi malá, malá, stredná, veľká, veľmi veľká</td>
</tr>
<tr>
<td>Následok</td>
<td>Veľmi malý, malý, stredný, veľký, veľmi veľký</td>
</tr>
<tr>
<td>Popis následku</td>
<td>Konkrétne dopady rizika – potenciál a veľkosť možných strát / ziskov, ohrozená hodnota, náklady na riziko, napr. možná krádež dvoch nákladných aut a 100 l nafty, veľká finančná strata, náklady na opravu</td>
</tr>
<tr>
<td>Časová os</td>
<td>Blízky termín, stredný termín, ďaleký termín, podľa definovania časovej osi</td>
</tr>
<tr>
<td>Opatrenia na modifikáciu rizika</td>
<td>Ako je riziko v súčasnosti riadené, spôsob monitorovania a kontroly Miera dôvery (spôlahlivosť) v súčasné spôsob riadenia rizika Určenie možných postupov pre monitorovanie a preskúmanie</td>
</tr>
<tr>
<td>Možné postupy pre zlepšenie</td>
<td>Odporúčania pre dažšie spôsoby zaobchádzania s rizikami</td>
</tr>
</tbody>
</table>

**Na popis rizík je možné využiť aj iné spôsoby.** Vzhľadom na vyhodnocovanie následku a pravdepodobnosti každého rizika je možné využiť pre popis iba klúčové riziká a tie analyzovať vo viacerých detailoch. Pre praktické použitie je výhodné zoznam rizík spracovať tak, aby sa jednotlivé riziká zapisovali pod sebou, ako je uvedené v tab. 13.

**Tab. 13 Možný vzor Zoznamu rizík**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>R01</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>R02</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
8.6 ANALÝZA RIZIKA

Analýza rizika (Risk Analysis) sa týka rozvíjania a chápania rizika. Je to proces, ktorý zahŕňa pochopenie podstaty rizika a určenie jeho úrovne. Poskytuje vstup do hodnotenia rizika a rozhodnutí, či sa rizikami treba zaoberať a akú najvhodnejšiu stratégiu a metódy treba použiť. Môže poskytnúť aj vstup do prijímania rozhodnutí tam, kde treba urobiť výber a možnosti obsahujú rozličné druhy a úrovne rizika. Analýza rizika zahŕňa ocenenie rizika (odhad, výpočet).

Analýza rizika obsahuje úvahy o:

a) pričinách a zdrojoch rizika,
b) kladných a záporných následkoch udalosti – zisk, ujma,
c) pravdepodobnosti, že tieto následky môžu nastať,
d) faktoroch, ktoré ovplyvňujú následky a ich pravdepodobnosť.

Riziko sa analyzuje určením:

- následkov,
- ich pravdepodobnosti,
- ďalších vlastností rizika.

Ďalšie vlastnosti rizika

V priebehu analýzy rizika sa majú identifikovať aj faktory, ktoré ovplyvňujú pravdepodobnosť a následky udalosti. Úroveň rizika bude závisieť na primeranosti, efektívnosti a účinnosti už zavedených opatrení na zniženie úrovne rizika. Otázky, na ktoré je treba zameriť pozornosť sú:

- Aké sú zavedené opatrenia na zníženie úrovne rizika?
- Sú tieto opatrenia schopné primerane modifikovať riziko na přípustnú úroveň?
- Používajú sa tieto opatrenia v praxi zamýšlaným spôsobom a môžu byť na požiadanie preukázane ako efektívne?

Na tieto otázky je možné s istotou odpovedať len vtedy, keď existuje riadna dokumentácia a vhodné procesy preukazovania. Úroveň účinnosti konkrétneho opatrenia na riadenie rizika alebo súboru súvisiacich opatrení na riadenie rizika, môže byť vyjadrená kvalitatívne, semikvantitatívne alebo kvantitatívne. Vo väčšine prípadov nie je zaručená vysoká úroveň presnosti. Môže však byť užitočné výjadriť a zaznamenat miernu efektívnosť riadenia rizika, potom je možné posúdiť, či bolo vynaložené najlepšie úsilie na zlepšenie riadenia rizík, alebo potrebu poskytnutia iného spôsobu zaobchádzania s rizikom.

Medzi faktory, ktoré ovplyvňujú pravdepodobnosť vzniku nebezpečnej udalosti možno zaradiť najmä napr. výstražné a varovné označenia, strážny pes, viditeľné nainštalované technické zabezpečovacie systémy (kamery, detektory a pod.) a iné opatrenia.

Medzi faktory, ktoré ovplyvňujú následky nebezpečnej udalosti možno zaradiť najmä: preventívne opatrenia, opatrenia na zniženie hodnoty aktív v jednom chránenom priestore, uloženie aktív v úschovných objektoch, havarijné plánovanie, priprava záchranných tímov a prostriedkov a pod.

Spôsob, akým sú v analýze rizík vyjadrené následky a pravdepodobnosť ich vzniku a spôsob, akým sú kombinované pre určenie úrovne rizika má odrážať:

- druh rizika,
- dostupné informácie,
účel, na ktorý sa má výstup z posudzovania rizika využiť.

Všetky tieto skutočnosti majú zodpovedať kritériám rizika. Takisto je dôležité zvažiť vzájomné súvislosti rozličných rizík a ich zdrojov.

Dôveryhodnosť určenia úrovne rizika a jeho citlivosť na predbežné podmienky a predpoklady sa má v analýze brať do úvahy a má sa efektívne oznamovať prijímateľom rozhodnutí a podľa potreby aj ďalším zainteresovaným účastníkom. Majú sa uviesť a vyjasniť také faktory, ako:
• rozdielnosť názorov expertov,
• neistota,
• dostupnosť, kvalita, množstvo a pokračujúca závažnosť informácií,
• obmedzenia pri modelovaní.

Tab. 14 Príklad analýzy rizika

<table>
<thead>
<tr>
<th>Číslo rizika</th>
<th>Názov rizika</th>
<th>Zdroj rizika</th>
<th>Pravdepodobnosť výskytu udalosti</th>
<th>Veľkosť rizika</th>
<th>Faktory ovplyvňujúce pravdepodobnosť</th>
<th>Faktory ovplyvňujúce následok</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1</td>
<td>požiar v garáži</td>
<td>podpaľač</td>
<td>stredná</td>
<td>3 veľmi veľký</td>
<td>5</td>
<td>nechránený vstup do areálu v noci, osvetlenie</td>
</tr>
<tr>
<td>R2</td>
<td>elektroinštalácia</td>
<td>malá</td>
<td>2 veľmi veľký</td>
<td>5</td>
<td>10</td>
<td>vykonávanie revízií elektroinštalácie</td>
</tr>
<tr>
<td>R3</td>
<td>kraša v garáži</td>
<td>pripravený vlamač</td>
<td>stredná</td>
<td>3 veľmi veľký</td>
<td>5</td>
<td>kvalita zámku, zabezpečenie okien, osvetlenie</td>
</tr>
</tbody>
</table>

8.6.1 Metódy analýzy rizika

Analýza rizika sa môže realizovať s rozličnou úrovňou podrobnosti a v závislosti od samotného rizika, účelu analýzy, informácií, údajov a dostupných zdrojov.

Analýza môže byť:
• kvalitatívna,
• semikvantitatívna (polokvantitatívna),
• kvantitatívna,
• prípadne podľa okolností ich kombinácia.

Kvantitatívne metódy analýzy rizika

Kvantitatívne metódy využívajú expertné odhady, ktoré využívajú priame, formalizovaným výpočtom spravídia priamo nepodložené vyjadrenie výskytu rizikovej udalosti, stanovenie jeho veľkosti alebo významnosti. Expertné odhady sa využívajú najmä v prípadoch, ak chybajú alebo sú t'ažko vyjadriteľné či selné hodnoty (údaje) pre kvantitatívne ohodnotenie rizika, sú jednoduchšie a rýchlejšie, ale sú viac subjektívnejšie.

Významnosť rizika sa v tomto prípade posudzuje podľa dvoch základných hodnôt, a to podľa:
• veľkosť následku udalosti,
• pravdepodobnosti výskytu udalosti.

Tento postup je pomerne prehľadný a jednoduchý, je v ňom však značný stupeň subjektivity. Takéto ohodnotenie jednotlivých udalostí využíva subjektívnu pravdepodobnosť.
ktorá vyjadruje mieru osobného presvedčenia o výskyte posudzovaného javu (udalosti) v závislosti na definovaných faktoroch.

**Expertný odhad** môže byť založený na:

- **intuitívnom zhodnotení rizika ako celku**, tzn. bez rozboru jeho jednotlivých veličín a predpokladov, alebo
- **dôkladnom zvážení kvalitativnej závažnosti týchto veličín** (parametrov rizika) a odhade rizika ako veličiny z týchto parametrov odvozených.

Podľa STN EN 31010 sa z kvalitativných metód na analýzu rizika používajú najmä expertné techniky: *matica následkov* a *pravdepodobnosť* a štruktúra „*čo sa stane, ak?*“.

**Spôsob vyjadrenia o veľkosťi rizika** môže byť:

- **slovnou deskripciou** (malé, stredné, veľké),
- **abstraktnej číselnej hodnotou** (tzv. ordinálnou poradovou stupnicou 0 – X),
- **percentuálne** (tzv. kardinálne percentuálnou stupnicou 0 – 100 %).

Slovná deskripcia je pre väčšinu užívateľov zrozumiteľnejšia a intuitívne prijateľnejšia. S jej využitím sa dá hodnotiť riziko s využitím úrovní dôležitosti (*slovami*), napr. ako *prijateľné, prípustné alebo neprijateľné* a definovať *následok, pravdepodobnosť a úroveň rizika* napr. *mála, stredná, veľká úroveň*.

Medzi číselnými hodnotami a slovným popisom existuje vzájomná korešpondencia, ktorá však nie je záväznou korešpondenciu, ktorá však nie je záväznou normou a každý užívateľ ju môže interpretovať podľa vlastných preferencií. Pritom sa môže kombinovať následok a pravdepodobnosť a možno hodnotiť výslednú úroveň rizika vo vztahu k kvalitatívnom kritériám. Použité popisné stupnice (*škály*) môžu byť prispôsobené alebo upravené tak, aby vyhovovali okolnostiam, a rôzne riziká môžu byť popísané rôznym spôsobom. V kvalitatívnej analýze má existovať jasné vysvetlenie všetkých termínov a majú byť zaznamenané podklady pre všetky kritériá.

Niektorí autori predpokladajú, že informácie získané z kvalitatívnej analýzy sú skoro vždy hodnotnejšie než z kvantitatívnej analýzy, a potom nie je kvantitatívna analýza vždy nutná. Odporúčajú kvalitatívnu analýzu najmä pre vývoj počiatočného ohodnotenia rizika, neskôr sa môže spoľahlivejšou interpretať aj kvantitatívnu analýzu.

Kvalitatívna analýza sa používa najmä:

- ako úvodný prehľad vedúci k identifikácii rizík, ktoré vyžadujú podrobnšie skúmanie;
- tam, kde tento druh analýzy postačuje na rozhodovanie; alebo
- tam, kde číselné údaje alebo zdroje nie sú dostatočné na vykonanie kvantitatívnej analýzy.

Kvalitatívne prístupy a metódy môžu byť založené na hodnotení, ktoré využíva mnohorové skupiny respondentov, hodnotení špecialistov a expertov, štruktúrovaných interview a dotazníkov.

Kvalitatívne induktívne expertné metódy je výhodné využivať predovšetkým pri riešení úloh analýzy rizík v oblasti fyzickej bezpečnosti a objektovej bezpečnosti, pretože:

- podmienky a predpoklady vzniku rizík sú veľmi premenlivé,
- kvantitatívne vyjadrenie parametrov rizík je vzhľadom na rôznorodosť podmienok a výrazný vplyv ľudského činiteľa velmi obľúbený,
- kvalitatívne metódy nevyžadujú množstvo štatistických údajov, ale využívajú logické výsledky z medzi faktormi ovplyvňujúcimi vznik rizík a
- kvalitatívne metódy poskytujú jasné a zrozumiteľné deskripciu rizík a ich parametrov.
Semikvantitatívne metódy analýzy rizika

Pri semikvantitatívnych metódach sa pre následok a pravdepodobnosti využívajú numerické klasifikačné stupnice a kombinujú sa s cieľom stanoviť úroveň rizika s použitím vzorca. Stupnice môžu byť lineárne alebo logaritmické, alebo môžu vyjadrovať iný vzťah. Použité vzorce sa môžu tiež líšiť.

Semikvantitatívne metódy využívajú najmä kvalitatívne popísanie stupnice, ktoré majú pridelené číselné hodnoty, kombináciou týchto charakteristik sa určí hodnota rizika. Cieľom je vytvoriť stupnice, ktoré sú podrobnejšie, než môže obvykle poskytnúť kvalitatívna analýza. Cieľom nie je navrhnúť realisticke hodnoty pre popis rizík, ako sa o to pokúša kvantitatívna analýza.

Pretože však číselná hodnota priradená každej vlastnosti nemusí vyjadrovať presný pomer k skutočnej veľkosti následkov alebo pravdepodobnosti, tieto hodnoty by sa mali vyskytovať iba vo vzorcach, ktoré rešpektujú obmedzenia zavedených stupníc. Použitím semikvantitatívnej analyzy je treba venovať osobitnú pozornosť, pretože vybrané číslo nemusia správne popísať skutočnosť, čo môže viest k nezrozumelostiam alebo k neobvyklým či nesprávnym výsledkom. Semikvantitatívna analýza nemusí správne rozlišovať rozdiely medzi rizikami, najmä ked následky alebo pravdepodobnosti usporadávajú sú mimoriadne.

Kvantitatívne metódy analýzy rizika

Kvantitatívne metódy využívajú numerické ohodnotenie rizík vyjadrením ich pravdepodobnosti, početnosti, vierochnosti, potenciálu, následkov a pod. Tieto metódy sa dajú použiť v prípadoch, ak je dostatok relevantných údajov, ktoré sa dajú hodnotiť štatisticky. Kvantitatívne metódy na určenie veľkosti rizíka využívajú dve základné hodnoty:
- pravdepodobnosť (početnosť) vzniku udalosti,
- následky, ktoré takúto udalosť sprevádzajú, alebo sú ňou spôsobované.

Kvantitatívne metódy potom využívajú na ohodnotenie veľkosti rizíka využívajú dve základné hodnoty: 

\[ R = P \times N \]

kde je:
- \( R \) veľkosť rizika,
- \( P \) pravdepodobnosť výskytu udalosti,
- \( N \) následok udalosti.

Na základe uvedeného vzťahu je možné určiť veľkosť jednotlivých identifikovaných rizík podľa tab. 15.

<table>
<thead>
<tr>
<th>Názov rizika</th>
<th>Pravdepodobnosť</th>
<th>Následok</th>
<th>Veľkosť rizika</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1 krádež v recepcii na prízemi</td>
<td>veľmi malá</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>R2 poškodenie serveru</td>
<td>stredná</td>
<td>3</td>
<td>12</td>
</tr>
<tr>
<td>R3 požiar v garáži</td>
<td>veľká</td>
<td>4</td>
<td>20</td>
</tr>
<tr>
<td>R4 krádež v garáži</td>
<td>stredná</td>
<td>3</td>
<td>15</td>
</tr>
<tr>
<td>R5 krádež dokumentov zo spisovne</td>
<td>malá</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>R6 krádež v pokladni</td>
<td>malá</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>R7 vandalizmus v kancelárii riaditeľa</td>
<td>stredná</td>
<td>3</td>
<td>9</td>
</tr>
</tbody>
</table>
Pri kvantitatívnych analýzach sú odhadnuté praktické hodnoty následkov a ich pravdepodobnosti a určia sa hodnoty výsledkov a ich pravdepodobností a určia sa hodnoty veľkosti rizika v špecifických jednotkách, stanovených v priebehu spracovania súvislostí. Úplná kvantitatívna analýza nemusí byť vždy možná alebo žiaduca pre nedostatok informácií o systéme alebo analyzovanej činnosti, nedostatok dát, vplyv ľudských faktorov a pod., alebo keď nie je úsilie o kvantitatívnu analýzu zaručené alebo požadované.

Za týchto okolností môže byť stále efektívna semikvantitatívna alebo kvalitatívna klasifikácia rizík, vykonaná skúsenými odborníkmi v prísľušnom odbore. Aj keď sa vykoná úplná kvantitatívna analýza, je možné uznáť len to, že vypočítané úrovne rizika sú tiež len odhady. Má sa dbať na to, že nemajú úroveň presnosti a precíznosti ako presnosť použitých dát a metód.

V niektorých prípadoch jedna číselná hodnota nestačí na určenie následkov v rôznych časoch, miestach alebo situáciách. Analýza by mala zvážiť a popísať aj neurčitosť a pravdepodobnosť následkov a ich pravdepodobnosť.

Podľa STN EN 31010 sa na analýzu rizika používajú najmä nasledovné metódy: štúdia ohrozenia a prevádzkyschopnosti HAZOP (Hazard and Operability Studies), analýza scéna, analýza dopadov na podnikanie, analýza koreňových príčin, analýza spôsobov a následkov porúch, analýza čoraz nešťastí, analýza spôsobov a následkov porúch, analýza nákladov a príjmov, analýza nákladov a príjmov, analýza multikriteriálneho rozhodovania (MCDA).


8.6.2 Analýza možností výskytu a odhad pravdepodobnosti

Proces analýzy rizika začína určením pravdepodobnosti, že riziko bude mať hmotné následky. Určenie pravdepodobnosti výskytu udalostí je zásadný problém v oblasti hodnotenia rizík, pretože štatistické údaje nie sú k dispozícii pre všetky druhy minulých udalostí. Určenie pravdepodobnosti môžu podporovať nasledujúce otázky:

- Vyskytli sa tieto udalosti už v minulosti, alebo je to ojedinelý výskyt?
- Vyskytujú sa takéto udalosti aj v iných zariadení a súčastiach?
- Kofko ľudí je touto udalosťou ohrozených?
- V akom časovom rozsahu sa podozrivé vybavenie alebo problematický postup používa?
- Aké sú tam organizačné, administratívne alebo regulačné následky, ktoré by mohli spôsobiť váčšie ohrozenie verejnosti?

Na odhad pravdepodobnosti sa bežne používajú tri všeobecné prístupy, môžu byť použité jednotlivé alebo spoločne:

a) Použitie príslušných historických údajov:

- cieľom bude identifikovanie udalostí alebo situácií, ktoré nastali v minulosti, čo dáva možnosť približne odvoditi (extrapolovať) pravdepodobnosť ich výskytu v budúcnosti,
• použité údaje sa majú týkať uvažovaného typu systému, vybavenia, organizácie alebo činnosti a tiež prevádzkových noriem príslušnej organizácie,
• v prípade, že v histórii bola veľmi nízka početnosť výskytu, potom akýkoľvek odhad pravdepodobnosti bude veľmi neistý, platí to najmä pre nulové výskytu, kedy nie je možné predpokladať, že sa udalosť, situácia alebo okolnost nevyskytne v budúcnosti.

b) Pravdepodobnosť predpovede pomocou prediktívnej techniky:
• napr. ako sú analýza stromu poruchových stavov a analýza stromu udalostí,
• keď sú historické údaje nedostupné alebo neprimerané, je nutné odvoditi pravdepodobnosť analýzou systému, činnosti, zariadenia alebo organizácie a s nimi zdrojených porúch alebo stavov úspechu,
• číselné údaje pre zariadenie, ľudí, organizácií a systémy vychádzajúce z prevádzkových skúseností alebo zo zdrojov zverejnených dát sú potom zlúčené, s cieľom odhadnúť pravdepodobnosť vrcholovej udalosti,
• pri používaní prediktívnych techník je dôležité zaistiti, aby bola v analýze vytvorená príslušná vôľa pre možnosť porúch so spoločným spôsobom poruchy tým, že sa v rámci systému zarátajú poruchy radu rôznych častí alebo súčastí, ktoré sa vyskytujú súčasne,
• môžu sa využiť simulačné techniky s cieľom vygenerovať pravdepodobnosť porúch zariadenia a konštrukčných porúch, vznikajúcich následkom starnutia a iných degradácíových procesov pomocou výpočtu nižšej pravdepodobnosti.

• môžu sa využiť simulačné techniky s cieľom vygenerovať pravdepodobnosť porúch súčasnej nižšej pravdepodobnosti.

• môžu sa využiť simulačné techniky s cieľom vygenerovať pravdepodobnosť porúch konštrukčných porúch, vznikajúcich následkom starnutia a iných degradácíových procesov pomocou výpočtu nižšej pravdepodobnosti.

8.6.3 Analýza následkov
Pri analýze následkov sa určuje povaha a druh následku, ku ktorému by mohlo dôjsť za predpokladu, že došlo k zvláštnej situácii alebo udalosti. Udalosť môže mať množstvo rôznych obyčajných následkov a môže ovplyvniť množstvo rôznych cieľov a rôzne zúčastnené strany. Po ustanovení súvislostí sa rozhoduje o druhoch následkov, ktoré budú analyzované a o zúčastnených stranách, ktoré budú ovplyvnené. V prípadoch, kedy následky budú pravdepodobne nevýznamné alebo sa očakáva, že pravdepodobnosť bude extrémne nízka, bude možno zaistiť na prijatie rozhodnutia o odhad jedného parametra.

Analýza následkov sa môže pohybovať od jednoduchého popisu výsledkov po detailné kvantitatívne modelovanie alebo analýzu zraniteľnosti.

Udalosti môžu mať:
• nízky následok, ale s vysokou pravdepodobnosťou,
• vysoko závažný následok a nízku pravdepodobnosť,
• nejaký stredný výsledok.

V niektorých prípadoch je vhodné zamerat sa na riziká s potenciálne veľmi rozsiahlymi následkami, pretože o tieto majú často obavy manažéri.

V ďalších prípadoch môže byť dôležité analyzovať riziká s vysoko závažným následkom a riziká s nízkym následkom oddelene. Napríklad, častý (alebo dlhotrvajúci) problém
s nízkym následkom môže mať veľké kumulatívne alebo dlhodobé účinky. Navyše zásahy spojené s liečením pri zaobchádzaní s týmito dvomi odlišnými druhami rizika sú často úplne odlišné, a preto je vhodné analyzovať ich oddelene.

**Analýza následkov môže zahŕňať:**

- zohľadnenie existujúcich opatrení na riadenie rizika s cieľom modifikovať následky spoľočne so všetkými príslušnými činiteľmi, ktoré majú vplyv na následky;
- uvedenie následkov rizika do spojitosti s pôvodnými cieľmi;
- zohľadnenie okamžitých následkov a tých, ktoré môžu vzniknúť po uplynutí určitej doby, ak je to v súlade s rozsahom posudzovania;
- zohľadnenie sekundárnych následkov, ako sú tie, ktoré majú vplyv na pridružené systémy, činnosti, zariadenia alebo organizácie.

Následky sa môžu vyjadriť v termínoch *hmotných alebo nehmotných následkov* (*finančných, technických, zdravotných alebo iných*). V niektorých prípadoch sa pre vyjadrenie následkov a ich pravdepodobnosti v rozličnom čase, v rozličných miestach a situáciách a pre rozličné skupiny vyjadzuje *viac ako jedna numerická hodnota*. Posúdenie závažnosti následkov udalosti (vplyv) je často veľmi ťažké pre dlhodobý nehmotný majetok, ďalšia otázka, ktorú treba riešiť je ocenenie aktív.

**Predbežná analýza rizika**

Riziká je možné triediť za účelom:

- identifikácie najvýznamnejších rizík, alebo
- na vylúčenie menej významných či menších rizík z ďalšej analýzy.

Cieľom je zabezpečiť, že:

- zdroje budú zamerané na najdôležitejšie rizíká,
- nebudú vyradené nízke rizíká, ktoré sa vyskytujú často a majú výrazný kumulatívny účinok.

Triedenie by malo byť založené na kritériách definovaných v súvislostiach. Na základe predbežnej analýzy sa určuje jeden alebo viacerých nasledujúcich postupov:

- rozhodnúť o zaobchádzaní (ošetrení, liečení) rizíka bez ďalšieho posudzovania,
- odložiť nevýznamné rizíká, pre ktoré by okamžité zaobchádzanie nebolo odôvodnené,
- pokračovať s podrobnejším posudzovaním rizík.

**Neistoty a citlivosti**

S analýzou rizík sú často spojené značné neistoty. Chápanie neistôt je potrebné pre efektívnu interpretáciu a oznamovanie výsledkov analýzy rizík. Má dôležitú rolu pri aplikácii neistôt spojených s dátami, metódami a modelmi používanými na identifikáciu a analýzu rizík.

**Analýza neistôt** zahŕňa *určenie odchýly alebo nepresnosti vo výsledkoch*, vyplývajúcej zo spoločných odchýlok parametrov a predpokladov používaných na definovanie výsledkov. Oblast, ktorá úzko súvisí s analýzou neistôt je analýza citlivosti.
Analýza citlivosti zahŕňa určenie rozsahu a významu veľkosti rizika pri zmenách v jednotlivých vstupných parametroch. Používa sa na identifikáciu tých údajov, ktoré musia byť presné, i tých, ktoré sú menej citlivé a preto majú menší vplyv na celkovú presnosť. Úplnosť a presnosť analýzy rizik by mala byť uvedená v najvyššej možnej miere.

Zdroje neistoty by mali byť identifikované vždy, keď je to možné, a je potrebné zame- rať sa ako na dátu, tak na neistoty modelu/metódy. Majú byť určené parametre, na ktoré je analýza citlivá a stupeň citlivosti.

Hlavným výstupom analýzy rizika je:
- zoznam príležitostí, ktoré sa musia sledovať (podnikateľské riziká),
- nebezpečné udalosti (ohrozenia, bezpečnostné riziká), ktoré vyžadujú pozornosť,
- zdokumentované zdroje rizík,
- zdokumentované faktory, ktoré ovplyvňujú následky a pravdepodobnosť.

Profil rizika

V rámci organizácie je vhodné určiť aj zodpovednosť za každé riziko. Výsledok procesu analýzy rizika je preto možné použiť na vytvorenie profilu rizík. Profil predstavuje súbor jednotlivých vlastností, čít rizíka. Profil rizíka je písomný popis súboru rizík, ktoré sa týkajú:
- celej organizácie,
- alebo jej časti, napr. jednotlivých objektov,
- alebo len jej niektorých činností, napr. výrobný proces, pracovný proces a pracovné podmienky, informačný proces, marketingový proces a pod.

Uvedené rozdelenie zodpovedností pomáha zaistíť, že vlastníctvo rizík je jasne stanovené a že boli vyčlenené príslušné zdroje na zaobchádzanie s nimi.
8.7 HODNOTENIE RIZIKA

Účelom hodnotenia rizika (Risk Assessment) je pomôcť pri prijímaní rozhodnutí o:
• rizikách, vyžadujúcich zaobchádzanie a
• priorite pre zavedenie zaobchádzania.

Hodnotenie rizika zahŕňa:
• porovnanie veľkosti rizika zistenej v procese analýzy, s kritériami rizika určenými počas vytvárania súvislostí,
• zváženie potreby zaobchádzania s rizikom,
• vydanie rozhodnutia o rizikách, ktoré vyžadujú zaobchádzanie,
• určenie priorít rizík, ktoré vyžadujú zaobchádzanie.

Rozhodnutie o rizikách, ktoré vyžadujú zaobchádzanie

Tieto rozhodnutia sú založené na výstupoch z analýzy rizika. Riziká sa zoradia podľa ich úrovne do kategórií (prijateľné, prípustné alebo neprijateľné) na určenie, či sa na základe analýzy prínosov a nákladov vyplatí riziko modifikovať. Vyhodnotenie rizík je preto určené na rozhodnutie o závažnosti rizík pre organizáciu, či konkrétne rizíko akceptovať alebo ho modifikovať niektorým zo spôsobov zaobchádzania s rizikom.

Rozhodnutia majú bráť do úvahy širší rámec rizika a musia zohľadniť úvahy o tolerancii rizika pre iných účastníkov, ako je organizácia, ktorá má z rizika osôb. Rozhodnutia sa majú prijať v súlade s požiadavkami zákonov, predpisov a s ďalšími požiadavkami. V niektorých prípadoch vyhodnotenie rizika môže priviesť k rozhodnutiu:
• vykonať ďalšiu analýzu,
• zvoliť najpomôcnejšie opatrenia na jeho kontrolu a nezaobierať sa rizikom nijakým iným spôsobom (takéto rozhodnutie ovplyvňuje prístup organizácie k riziku a k určeným kritériám rizika).

O povahy rozhodnutí, ktoré sa musia vykonať a o kritériách, ktoré boli použité na rozhodovanie sa rozhodlo v priebehu určenia súvislostí, ale v tejto etape, keď je viac poznatkov o konkrétnych rizikách, je potrebné prehodnotiť viac podrobností. Počiatočné predpoklady a výsledky majú byť zdokumentované.

Najjednoduchšia na definovanie rizika je jednotná úroveň, v ktorej rozdeľuje riziká na:
• ktoré vyžadujú zaobchádzanie – patria sem neprijateľné/nekancelovateľné riziká a prípustné riziká, pre ktoré sa posudzujú náklady a prínosy,
• ktoré to nepotrebujú – prijateľné/akceptovateľná úroveň rizika.

Toto delenie poskytuje lákavé jednoduché výsledky, ale neodráža neistoty:
• zahrnuté v odhadovaní rizika,
• definovania hranice medzi rizikami, ktoré potrebujú zaobchádzanie, a tými, ktoré ho nepotrebujú.

K rozhodnutiam môžu viest' nasledujúce aspekty:
• či riziko potrebuje zaobchádzanie,
• priority pre zaobchádzanie,
• či má byť podniknutá nejaká činnosť,
• ktorou z množstva ciest sa vydáť.

Rozhodnutie o tom, či a ako zaobchádzat' s rizikom môže najmä pri prípustných rizikách závisieť od nákladov a prínosov:
• pri podstupovaní rizika,
• na zavádzaní zlepšených opatrení na modifikáciu rizika.

Bežný spôsob spočíva v rozdelení rizík na tri skupiny:

a) horná skupina, kde je úroveň rizika považovaná za neprijateľnú, bez ohľadu na to, či činnosť môže znamenat’ akýkol’vek prínos, a zaobchádzanie s rizikom je nevyhnutné za akúkol’vek cenu,

b) stredná skupina (alebo šedá oblasť), kde sa berú do úvahy náklady i prínosy, a príležitosti sú zvažované vzťažením na potenciálne následky,

c) dolná skupina, kde je úroveň rizika považovaná za zanedbateľnú alebo tak malú, že nie sú potrebné žiadne opatrenia na zaobchádzanie s rizikom.

Na posúdenie nákladov a prínosov vybraných spôsobov zaobchádzania s neprijateľnými i prípustnými rizikami sa využíva zásada ALARP, ktorá ukazuje, že riziku, riadieniu rizika a modifikácii rizika je potrebné venovať primeranú pozornosť. Zásada zahŕňa zváženie a porovnanie úrovne rizika s t’jažkost’ami, časom a finančnými nákladmi, potrebnými na jeho riadenie.

ALARP rieši najmä strednú skupinu, kde je pohyblivá stupnica pre znesiteľné nízke riziká, pre ktoré môžu byť náklady a prínosy priamo porovnané, zatiaľ čo pre nežiaduce vysoké riziká je nutné možnosť poškodenia znížiť, pokiaľ nebudú výdaje na ďalšie zníženie výrazne neúmerné k získanému bezpečnostnému prínosu.

Z výsledkov určenia úrovne rizík v priebehu ich analýzy možno rozhodnúť o zaradení jednotlivých rizík do kategórií:

• Neprijateľné riziká, ktoré vyžadujú nevyhnutné prijatie regulačných opatrení na ich odstránenie alebo zníženie – R3 požiaľ garáží (20).

• Prípustné rizíko(stredné pásmo) – je prípustné a neríadi sa len v prípade, ak jeho zníženie je značne neefektívne, inak je potrebné zvoliť spôsob(y) zaobchádzania s ním – R4 (15), R2 (12), R6 (10), R7 (9), R5 (8).

• Prijateľná úroveň rizika (akceptovateľná), ktorá nevyžaduje regulačné opatrenia na jeho zníženie – R1 (3).

V rozhodnutí o rizikách, ktoré vyžadujú zaobchádzanie sa potom uvedú:

• neprijateľné riziká,
• a prípustné riziká.

Priority rizík, ktoré vyžadujú zaobchádzanie

Výsledkom hodnotenia rizík môže byť aj zostavenie poradia priority rizík, ktoré vyžadujú zaobchádzanie. Poradie dáva rating každému riziku a stanoví tak priority pre zaobchádzanie s rizikami.

Riziká vyžadujúce zaobchádzanie nebude možné vždy začať upravovať okamžite, a to z viacerých dôvodov, napr.: časová náročnosť, materiálno technická náročnosť, finančná náročnosť, vysoké nároky na ľudské zdroje, strategické zámery organizácie a pod.

Uvedené dôvody ovplyvňujú aj priority rizík pre zavádzanie zvolených spôsobov zaobchádzania s nimi. Cieľom je pomocou zvolených kritérií a postupov zoradiť ohodno-
tené riziká podľa ich významnosti (priority). Ide o rozhodovací proces, ktorý využíva zvolené kritéria na určenie priorít rizík, ktoré vyžadujú niektoré spôsoby zaobchádzania.

Pripomenete, že rozhodovací proces, ktorý využíva zvolené kritéria na určenie priorít rizík, ktoré vyžadujú niektoré spôsoby zaobchádzania.

1. Aká je veľkosť rizika?
2. Aká je závažnosť následku – koľko ľudí a aké materiálne hodnoty sú vystavené tomuto riziku a pod. (ohrozenie životov a zdravia má najvyššiu prioritu)?
3. Finančná, materiálno-technická a časová náročnosť na zavedenie zaobchádzania.
4. Aká bude efektívnosť a účinnosť navrhovaných opatrení na zaobchádzanie s rizikom?

Na zaobchádzanie s týmito rizikami je možné vo vznietenom príklade stanoviť nasledujúce priority:

1. Riziká, ktoré majú neprijateľnú úroveň (R3),
2. Prípustné riziká – po zvážení nákladov na ich zníženie:
   • nedávne:
     - R4 krádež v garáži (15),
     - R2 poškodenie serveru (12),
   • znesielene:
     - R6 krádež v pokladni (10),
     - R7 vandalizmus (9),
     - R5 krádež dokumentov (8).

Výsledkom hodnotenia rizík je Zoznam rizík, ktoré vyžadujú zaobchádzanie podľa priorít pre zaobchádzanie. Na základe určených priorít je stanovené poradie rizík na volbu spôsobov (u) zaobchádzania s nimi.

Obsah problematiky posudzovania rizika je súhrne uvedený v tab. 16.
Tab. 16 Obsah posuzovania rizíka

<table>
<thead>
<tr>
<th>IDENTIFIKÁCIA RIZÍK</th>
<th>ANALÝZA RIZÍK</th>
<th>HODNOTENIE RIZÍK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proces hľadania, spoznávania a popísania rizika</td>
<td>Proces na pochopenie povahy, zdrojov a príčín rizík pre ocenenie úrovne rizika</td>
<td>Proces porovnania výsledkov analýzy rizík s kritériami rizika</td>
</tr>
</tbody>
</table>

- **Zahŕňa identifikáciu**
  - zdrojov rizíka – prvkov, ktoré samy osebe alebo v kombinácii majú vnútorný potenciál vyvoláť riziko a oblastí ich následkov,
  - udalostí, ktoré zdroje rizika môžu spôsobiť,
  - okolností, ktoré by mohli mať potenciálne následky na dosiahnutie cieľov,
  - príčin rizika – toho, ČO sa môže stať, KEDY a KDE, PREČO a AKO sa to môže stať,
  - potenciálnych následkov,
  - opatrení zavedených na modifikáciu rizika

- **Zahŕňa posúdenie**
  - príčin a zdrojov rizíka – pozitívne vlastnosti, nebezpečenstvo (pôžičiteľnosť, ohrozenie),
  - kladných a záporných následkov udalostí – zisk, ujma,
  - pravdepodobnosti, že tieto následky môžu nastať,
  - dôsledných vlastností rizika – fakto-ry, ktoré ovplyvňujú následky a pravdepodobnosť

- **Zahŕňa**
  - porovnanie úrovne rizika zistenej v procese analýzy, s kritériami rizika určenými počas hľadania súvislostí,
  - zváženie potreby zaobchádzania s rizikom,
  - vydanie rozhodnutia o prijateľnosti resp. neprijateľnosti či prípustnosti rizika

8.8 LITERATÚRA


STN EN 31010:2011 – Manažérstvo rizika, Metódy posuzovania rizika.

9 ZA OBCHÁDZANIE S RIZIKOM

Zaobchádzanie s rizikom je podľa STN ISO 31000 proces modifikovania rizika. Ak bol proces manažérstva rizík postupný a systematický a boli v ňom identifikované a analýzo-vané riziká, možno pokračovať so zaobchádzaním s rizikami.

Zaobchádzanie s rizikom zahŕňa opakujúci sa proces:
• posudzovania zaobchádzania s rizikom,
• rozhodovania, či zvyšková úroveň rizika je pripustná,
• vytváranie nového zaobchádzania s rizikom, ak zvyšková úroveň rizika nie je pri-pustná,
• posudzovanie efektívnosti realizovaného spôsobu zaobchádzania.

Zaobchádzanie s rizikami môže v organizácii:
• vytvorit' lepšie možnosti pre pôsobenie rizík, z ktorých môže mať prospech,
• obmedziť možnosti pôsobenia rizík, ktoré sú pre ňu nevyhodné.

Zaobchádzanie s rizikom, ktoré sa zaobrá a jeho zápornými následkami (bezpečnostné riziko) sa niekedy označuje ako zmiernenie rizika, eliminácia rizika, prevencia rizika alebo zníženie rizika.

Zaobchádzanie s bezpečnostným rizikom je proces, pri ktorom sa môžu:
• zlepšiť zavedené ochranné opatrenia
• alebo vytvoriť a implementovať nové.


Spôsoby zaobchádzania s rizikom môžu zahŕňať tieto možnosti:
1. Vyvarovanie sa riziku (avoiding the risk) na základe rozhodnutia nezačínat' činnosť alebo nepokračovať v činnosti, ktorá spôsobuje riziko.
2. Akceptovanie alebo zvýšenie rizika s cieľom využiť príležitosť (taking or increasing risk in order to pursue an opportunity)
3. Odstránenie zdroja rizika (removing the risk source).
4. Zmenu pravdepodobnosti rizika (changing the risk likelihood).
5. Zmenu následkov rizika (changing the consequences).
6. Podiel'anie sa na riziku s ďalšou stranou alebo stranami (vrátane zmlúv a financovania rizika) (sharing the risk with another party or parties).
7. Zachovanie rizika na základe kvalifikovaného rozhodnutia (retaining the risk by informed decision).
9.1 CHARAKTERISTIKA SPÔSOBOV ZAOBCHÁDZANIA S RIZIKOM

Vyvarovanie sa riziku

Vyvarovať sa riziku na základe rozhodnutia *nezačínat činnosť alebo nepokračovať v činnosti*, ktorá vytvára riziko znamená vyhnutie sa *činnosťam, ktoré sú vystavené mimo-riadnym rizikám (ohrozenia)*. Vyvarovanie môže byť založené na základe výsledkov hodnotenia rizika a/alebo právnych a regulačných povinností.

Po odstránení pôvodného rizika je *zostatkové riziko nulové*. Táto alternatíva sa *používa izolovane* od zostávajúcich možností zaobchádzania s rizikom. Toto sa môže dosiahnuť napr.:

- ústupom z existujúcich trhov,
- zákazom vysokorizikových aktivít prijatím systému limitov akceptovateľného rizika,
- zastavením špecifických aktivít s neakceptovateľným rizikom zmenou zámerov, cieľov alebo premiestnením zdrojov,
- zamedzením rizikových činností, ktoré nesúvisia s rozvojom určeným v stratégii,
- zabránením projektom s vysokou rizikovosťou.

**Príklad 1** – nezakúpiť majetok alebo neurobiť obchod, pretože to prináša riziko po- hľadávok a iných nevýhod – nevstúpovať do obchodovania sťažnou riziku straty, ale tak isto zabrániť možnosti profitovať.

**Príklad 2** – neletieť preto, lebo existuje riziko, že lietadlo spadne – riešenie iným druhom dopravy však znamená časovú stratu a čas sú peniaze.

Vyvarovanie sa riziku sa teda môže zdať vhodnou odpoveďou na všetky riziká, ale zabrániť rizikám znamená na druhej strane úplne stratiť potenciálny zisk, s ktorým je riziko spojené.

Akceptovanie alebo zvýšenie rizíka

Cieľom je využiť príležitosť v podnikaní, čo sa napríklad môže uskutočniť nasledujú- cimi opatreniami:

- alokáciou (rozmiestnením) zdrojov zaručujúcou najlepšie finančné vyhliadky,
- diverzifikáciou (rozdelením) špecifických činností na zníženie rizika,
- expanzíou na nové trhy a tým zabezpečenie nových zdrojov pri udržateľnej miere rizika,
- zavedením nových produktov a služieb zaručujúcich rýchly rast,
- implementáciou (zavedením) zdokonalených procesov vedúcich k eliminácii príčin neefektnosti,
- ovplyvnením verejnej mienky prostredníctvom reklamy a iných spôsoob mediálnej komunikácie.

**Odstránenie zdroja rizika**

Zdrojom rizika, ktorý môže spôsobiť potenciálne ohrozenie, je určitý druh nebezpečenstva. Medzi možnosti, ako odstrániť zdroj rizika, možno zaradiť najmä:

- odstránenie identifikovaných zdrojov rizika projektovaním,
- implementácia interných preventívnych procesov.

Po odstránení zdroja rizika je *zostatkové riziko nulové.*
Zníženie úrovne rizika

Pretože význam rizika sa vzťahuje na pravdepodobnosť jeho výskytu i na jeho vplyv na organizáciu, ak k nemu dôjde, môže zniženie rizika zahŕňať: zmene pravdepodobnosti rizika, zmene následkov rizika, prípadne zmene oboch (obr. 10).

Pravdepodobnosť

\[
\begin{align*}
\text{Úroveň existujúceho rizika} \\
\text{Hranica neakceptovateľného rizika}
\end{align*}
\]

Následok

Vysvetlivky: 1 zniženie následku, 2 zniženie pravdepodobnosti, 3 zniženie následku i pravdepodobnosti, 4 kvadrant optimálneho zniženia pravdepodobnosti i následku

Obr. 10 Spôsoby zniženia úrovne rizika

Možné opatrenia na zniženie pravdepodobnosti výskytu rizika a zniženie jeho následkov sú uvedené v tab. 17.

Tab. 17 Možné opatrenia na zniženie pravdepodobnosti a následkov rizika

<table>
<thead>
<tr>
<th>Zniženie pravdepodobnosti</th>
<th>Zniženie následkov</th>
</tr>
</thead>
<tbody>
<tr>
<td>• ochranné zariadenia a prostriedky na zniženie pravdepodobnosti vzniku udalosti,</td>
<td>• zniženie vysokej hodnoty aktív v jednom chránenom priestore,</td>
</tr>
<tr>
<td>• využitie doplnkových bezpečnostných prvkov,</td>
<td>• prijatie preventívnych opatrení,</td>
</tr>
<tr>
<td>• výstražné zariadenia a prostriedky,</td>
<td>• ochranné zariadenia a prostriedky na zniženie následkov udalostí,</td>
</tr>
<tr>
<td>• kontroly vstupu,</td>
<td>• prijatie bezpečnostných opatrení,</td>
</tr>
<tr>
<td>• politiky a postupy,</td>
<td>• školenie personálu,</td>
</tr>
<tr>
<td>• fyzická ochrana,</td>
<td>• zmluvné podmienky,</td>
</tr>
<tr>
<td>• organizačné a režimové opatrenia,</td>
<td>• havarijný plán,</td>
</tr>
<tr>
<td>• školenie personálu,</td>
<td>• núdzové postupy,</td>
</tr>
<tr>
<td>• zmluvné podmienky,</td>
<td>• obnova po havárii,</td>
</tr>
<tr>
<td>• starostlivosť a údržba,</td>
<td>• plány kontinuity činností,</td>
</tr>
<tr>
<td>• testovanie, správa investícií,</td>
<td>• externé zálohovanie dát,</td>
</tr>
<tr>
<td>• technické kontroly,</td>
<td>• styk s verejnosťou,</td>
</tr>
<tr>
<td>• programy zaistenia kvality,</td>
<td>• iné opatrenia.</td>
</tr>
<tr>
<td>• audit a programy overovania,</td>
<td></td>
</tr>
<tr>
<td>• monitorovanie,</td>
<td></td>
</tr>
<tr>
<td>• iné opatrenia.</td>
<td></td>
</tr>
</tbody>
</table>
Príklady:

• závažnosť zranení spôsobených padajúcimi predmetmi na stavenisku budovy (následok) sa môže znižiť pomôcťným nosením ochranných príslušenství, zatiaľ čo prijatie bezpečnostných opatrení môže znižiť pravdepodobnosť výskytu padajúcich predmetov,
• kontroly divákov prichádzajúcich na fotbalový štadión detektormi kovov a prehliadkou tašiek znižujú pravdepodobnosť prinesenia zbraní a výbušníctva do tohto priestoru,
• stavanie hrádzí proti povodňam obmedzuje alebo zabraňuje povodňovým škodám – znižujú následok.

Na redukované množstvo strat e je výhodné použiť dizajnový prístup – znižuje pravdepodobnosť i následok, spočíva v spôsobení dizajnu (alebo usporiadaní) tak, aby sa znižilo riziko na zanedbateľnú úroveň (zásadná zmenna zdroja či diel rizika energie, množstva energie, spôsobu uvoľnenia energie, usporiadaním prvkov v rámci systému, princípu či principov prevádzky). Tento spôsob je spomenutý všetkých skupín opatrení najnáročnejšej, ale aj najúčinnnejšej.

Podieľanie sa na riziku s ďalšou stranou alebo stranami


Rozsah rozdelenia rizika môže závisieť na spoľahlivosti a prehľadnosti usporiadaní podielnicťa. Prenos rizika je formou podieľania sa na riziku.

Financovanie rizika je formou podieľania sa na riziku, ktorá zahrňa možné opatrenia pre zaopatrenie fondu na uhradenie alebo modifikovanie finančných následkov.

Na činnosti organizácie sú zainteresovaní početní zainteresovaní účastníci, preto by mal mať každý z nich aj svoj proporcionálny diel rizika, aby dostal svoj výnos. Prenos rizika môže zahŕňať:
• využívanie zmlúv s ďalšou stranou, ktorá preberie nejakú časť rizika alebo sa bude na ném podieľať,
• outsourcing spoločných podnikov,
• partnerstvá a pod.

Príklad: pri projekte na stavbu zariadenia by mala byť určitá časť rizika presená z organizácie klienta – zmluvnú stranu, ktorá za práce ručí – pri dodržaní limitov zmluvná strana očakáva odmenu, ak nie, musí niest svoj podiel na oneskorení.

Podieľanie sa na riziku neznížuje riziko, iba jeho časť posunu na ďalšie zmluvné strany. Spoluúčast na riziku je vhodná stratégia pre nízke rizika, kde náklady na obnovu oproti riziku by mali byť výsledné. V niektorených prípadoch podieľanie sa na riziku môže podstatne zvýšiť riziko, pretože strana, na ktorej sa prevádzka, si nemusí byť vedomá rizika a toho, že sa od niej požaduje, aby riziko zvládla.

Pri rozhodovaní o rozdelení rizika sa musí zvážiť:
• kto môže najlepšie zvládať riziká,
• aké sú náklady alebo prínosy prenosu rizika oproti internému zaobchádzaniu s rizikom.
Pri rozhodovaní o prenose rizika sa musí zvážiť:
• kto môže najlepšie zvládať riziká,
• aké sú náklady alebo prínosy prenosu rizika oproti internému zaobchádzaniu s rizikom.

Zachovanie rizika na základe kvalifikovaného rozhodnutia
Zachovanie rizika znamená prijatie potenciálnej výhody zo zisku, alebo nákladov na škody z určitého rizika. Zachovanie rizika zahŕňa prijatie reziduálneho rizika. Úroveň rizika pre jeho zachovanie môže závisieť od kritérií rizika.

Neúmyselné zachovanie rizika sa vyskytuje ako výsledok zlyhania identifikácie a analýzy rizika. Ak nie je riziko identifikované, alebo ak sú jeho potenciálne následky podcenené, nie je pravdepodobné, že sa mu organizácia vyhne, alebo ho vedome zníži alebo primeraným spôsobom prenesie

Plánované zachovanie rizika zahŕňa úplný alebo čiastočný predpoklad potenciálneho dopadu rizika – vztah medzi rizikom a prínosom funguje tak, že bez vystavenia sa riziku nemôže organizácia očakávať odmenu.

Zachovanie rizika sa uplatňuje najmä v prípadoch, keď:
• na základe súčasných vedeckých a technických poznatkov nie je možné toto riziko odstrániť ani znížiť na prijateľnú úroveň,
• náklady na zníženie rizika vysoko prevyšujú jeho potenciálny následok,
• veľké alebo katastrofické riziká nemôžu byť v niektorých prípadoch modifikované alebo poistené pre vysokú cenu poistenia.

Zachovanie rizika teda zahŕňa akceptovanie strát ak nastanú. Príkladom je vojna, kedy veľké množstvo rizika nie je možné ošetriť, musí sa tolerovať. V každom prípade je však nutné tieto riziká monitorovať a predchádzať im.

Tab. 18 Príklad na zaobchádzanie s rizikom

<table>
<thead>
<tr>
<th>Nebezpečenstvo</th>
<th>Ohrozenie</th>
<th>Riziko</th>
<th>Zaobchádzanie s rizikom</th>
</tr>
</thead>
<tbody>
<tr>
<td>býrka</td>
<td>• zásah bleskom, lokálna povodeň, zmoknutie</td>
<td>• bleskom spôsobený požiar alebo zranenie, usmrtenie osôb, zatopené obydlia a poli, poškodenie odevu a vecí citlivých na vlhkosť, prechladnutie, vyvarovanie sa riziku</td>
<td>• blesku a povodňov sa nedá vyhnúť, zmoknutie – nevyhýbať sa do býrky, odstránenie zdroja rizika, býrku nie je možné odstrániť</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• bleskozvod, vypnutie mobilu, budovanie hrádzie proti povodňam, dáždník, pláštenka, ochrana citlivých vecí</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• zmena následkov rizika</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>prenos rizika</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>zachovanie rizika</td>
</tr>
</tbody>
</table>

Riadenie rizika
V priebehu zaobchádzania s rizikom sa z niekoľkých zvolených variantov zvolí jeden alebo viac spôsobov zaobchádzania s rizikom a v nich aj niekoľko variantov na výber opatrení na modifikáciu rizika (ovládacie prvkov).
Po implementácii vybraného opatrenia(í) sa zaobchádzanie s rizikom stane riadením rizika alebo modifikáciou už zavedených opatrení na zníženie úrovne rizika.

Riadenie rizika predstavuje opatrenie na modifikáciu konkrétneho rizika. Zahrňa taktiky, postupy, skúsenosti, procesy, technológie, techniky, metódy a zariadenia na modifikovanie tohto rizika.
9.2 VÝBER SPÔSOBOV ZAOBCHÁDZANIA S RIZIKOM

Kritickou fázou procesu zaobchádzania s rizikami je **výber najvýhodnejšieho spôsobu (spôsobov) zaobchádzania s rizikom**, ktorý je **rozhodovacím procesom**, vychádzajúcim z analýzy rizika a nadvázuje na výsledky procesu hodnotenia rizík.

Výber najvýhodnejšej možnosti zaobchádzania s rizikom zahŕňa **porovnanie nákladov a úsilia na zavedenie opatrení a dosiahnutého úžitku** vzhľadom na:

- požiadavky zákonov, predpisov,
- sociálnu zodpovednosť,
- ochranu životného prostredia.

Pri výbere spôsobov zaobchádzania s rizikami sa **okrem neprijateľných a prípustných rizík majú byť bráti do úvahy aj riziká prijateľné**, ktoré by mali závažné negatívne následky, napr. zranenie alebo usmrtenie osôb, ale pre riziku pravdepodobnosť výskytu sú zadané ako akceptovateľné (bezvýznamné).

**Vzťah k riziku** znamená prístup organizácie k hodnoteniu a prípadnému sledovaniu, zachovaniu, prijatíu alebo odmietnutiu rizíka. Môže riziko prijať, znášať, hromadiť alebo mať avérziu.

- **Prijateľnosť rizika** znamená veľkosť a druh rizika, ktoré je organizácia ochotná sledovať alebo zachovať.
- **Prevzatie rizika** znamená kvalifikované rozhodnutie prevziať zodpovednosť za jednotlivé riziko. Môže sa to uskutočniť bez zaobchádzania s rizikom alebo v priebehu procesu zaobchádzania s rizikom. Prevzatie rizika je podmienené jeho monitorovaním a preskúmaním.
- **Znášanlivosť rizika** predstavuje pripravenosť organizácie alebo zúčastneného účastníka znášať riziko po jeho ošetrení, za účelom dosiahnutia svojich cieľov. Môže byť ovplyvnená právnymi alebo regulačnými požiadavkami.
- **Hromadenie rizika** znamená kombináciu niekoľkých rizík do jedného rizika a vytváranie ďalšieho komplexného chápania celkového rizika.
- **Averzia voči riziku** – názor organizácie na odvrátenie sa od rizika.

Počet možností zaobchádzania s rizikom možno zvážiť jednotlivo alebo v kombinácii. Organizácia má zvyčajne prospech z realizácie **kombinácií možností zaobchádzania**.

Pri výbere možností zaobchádzania s rizikom má organizácia zvážiť význam a chápanie zainteresovaných účastníkov a najvhodnejšie spôsoby, ako s nimi komunikovať. Keď niektoré možnosti zaobchádzania s rizikom môžu **ovplyvniť riziko na inom mieste** alebo na základe **zainteresovaných účastníkov**, má sa to zohľadniť v rozhodnutí. Aj keď niektoré zaobchádzanie s rizikom môže byť rovnako efektívne, pre niektorých zainteresovaných účastníkov môže byť prijateľnejšie ako pre iných.

Samotné zaobchádzanie s rizikom môže vyvoliť **ďalšie rizíká**. Významným nedostatkom môže byť zlyhanie alebo nefektívnosť opatrení na zaobchádzanie s rizikom, preto integračnou súčasťou Plánu zaobchádzania s rizikom musí byť **monitorovanie, ktoré poskytuje garanciu, že opatrenia boli efektívne**.

Zaobchádzanie s rizikom môže vyvoliť aj **sekundárne riziká**, ktoré treba posúdiť, venovať mu pozornosť, monitorovať a preskúmať – toto riziko sa má zahrniť do rovnakého plánu zaobchádzania ako je originálny plán a nezaoberať sa s ním ako s novým rizikom. Väzba medzi týmito dvomi rizíkami sa má zistiť a udržiavať.
Postup pri zaobchádzaní s rizikom:

1. určiť riziko, ktoré treba riadiť (modifikovať),
2. zvoliť možný spôsob (spôsoby) zaobchádzania s rizikom,
3. vo zvolených spôsoboch zaobchádzania s rizikom zvoliť druhu opatrení na modifikáciu rizika, napr. pre bezpečnostné riziká: MZP, TZP, strážna služba, režimové opatrenie a pod.,
4. v každom zvolenom druhu opatrení na modifikáciu rizika variantne posúdiť spôsoby, sily a prostriedky na modifikáciu rizika, napr. porovnaním nákladov a prínosov a vybrať najvýhodnejšie spôsoby, sily a prostriedky, napr. najvýhodnejšiu kamenu, zámok, dvere, trezor, najlacnejšiu SBS, poistovňu a pod.,
5. vybrať najvýhodnejšie opatrenie(a) na modifikáciu rizika, napr. zavedenie konkrétnej kamery na zniženie pravdepodobnosti, využitie konkrétneho trezoru na zniženie následkov, poistenie v určitej poistovni a pod.,
6. prijať rozhodnutie o realizácii opatrenia (opatrení) na zaobchádzanie s rizikom, resp. o ďalšom monitorovaní rizika v prípade vysokého stupňa neistôt, spojených so súčasným stupňom poznania a tým nemožnosti znížiť riziko v etape tvorby rozhodnutia.

Výber najvýhodnejších spôsobov zaobchádzania s rizikom

Na zodpovedný výber najvýhodnejšieho spôsobu (spôsobov) zaobchádzania s rizikom je potrebné zvoliť niekoľko variantov a posúdiť ich týmto postupom:

a) analýzu nákladov a prínosov variantných riešení na zaobchádzanie s rizikom, vzhľadom na požiadavky zákonom a predpisom:
   • Cost Benefit Analysis (CBA) niekedy nazývaná analýza prínosov a nákladov Benefit Cost Analysis (BCA),
   • Analýza nákladovej efektívnosti – Cost-Effectiveness Analysis, CEA.

b) zhodnotenie spoločenských dopadov a prínosov (napr. vplyvy na prírodné a kultúrne dedičstvo) a politickú analýzu možných politických následkov z prijatého rozhodnutia.

c) analýzu verejnej mienky.

Výber opatrení na modifikáciu rizika

Opatrenia na modifikáciu rizika sú spôsoby, sily a prostriedky, ktorými sa môžu riziká modifikovať. Možno ich považovať zaopatrenia, ktoré umožnia dosiahnuť stanovené ciele. Pri výbere vhodného variantu na modifikáciu rizika objektov a chránených priestorov je potrebné zvažovať, ktoré opatrenia sú pre daný variant najvýhodnejšie, pričom by sa, okrem ceny, mali zvažovať viaceré faktory, najmä:
   • ktoré funkcie umožňuje vykonávať – prevencia, odstrašenie, detekcia, monitorovanie,
   • zložitosť či jednoduchosť používania,
   • účinnosť (dosah, citlivosť a pod.),
   • funkčnosť v rôznych stážených prevádzkových podmienkach,
   • dlhodobá životnosť,
   • záručné podmienky,
   • bezporuchovosť, servis,
   • opraviteľnosť, rýchlosť obnovy,
   • aké povedomie má pre zamestnancov a iné.

Pri preverovaní celkovej bezpečnosti alebo množiny použitých ochranných opatrení by mala byť zabezpečená rovnováha medzi uvedenými faktormi, pokiaľ je to možné. To napomáha celkovej bezpečnosti z pohľadu jej efektívnosti a účinnosti. Výber ochranných opatrení by mal vždy zahŕňať vyváženosť prevádzkových (netechnických) a technických opatrení.
ktoré sa navzájom podporujú a doplňajú. Výsledkom tohto kroku by mal byť výber ochranných opatrení na modifikovanie všetkých rizík, ktoré boli vybrané na zaobchádzanie.

**Postup pri výbere a hodnotení spôsobu/ spôsobov zaobchádzania s rizikom**

Vždy sa *najprv treba snažiť o odstránenie rizika v jeho samom zdroji* (nebezpečenstvo – ohrozenie), *ako prijímať opatrenia na jeho zníženie!*

V priebehu výberu najvýhodnejších spôsobov/ spôsobu zaobchádzania s daným rizikom je možné postupovať takto:

1. **Určiť riziko**, pre ktoré sa budú vyberať spôsob /spôsoby zaobchádzania s rizikom, riziká začať posudzovať podľa priorít pre zaobchádzanie.
2. Posúdiť vhodnosť využitia všetkých *spôsobov zaobchádzania s rizikom*, vylúčiť tie, ktoré nie sú vhodné a nedajú sa uskutočniť*, napr.:*
   - vyvarovanie sa riziku nie je možné, pretože vykonávaná činnosť sa nedá zastaviť ani prerušiť;  
   - nie je možné *odstrániť zdroj rizika*, ktorým je násilný páchateľ a pod.
3. Zvoliť *spôsob(y) zaobchádzania s rizikom, ktoré sa dajú uskutočniť*.
4. Vo zvolenom spôsobe (spôsoboch) *vytvoríť varianty opatrení na modifikáciu rizika*, napr. na:
   a) zmenu pravdepodobnosti rizika – využiť napr. ochranné zariadenia a prostriedky na zníženie pravdepodobnosti vzniku udalosti, doplnkové bezpečnostné prvky, výstražné zariadenia a prostriedky, kontroly vstupu, fyzická ochrana, organizačné a režimové opatrenia a pod.
   b) zmenu následkov rizika – využiť napr. zniženie hodnoty aktiv v jednom chránenom priestore, prijatie preventívnych opatrení, ochranné zariadenia a prostriedky na zníženie následkov udalostí, prijatie bezpečnostných opatrení, školenie personálu, zmluvné podmienky, havarijný plán, plány kontinuity činností, externé zálohovanie dát a pod.  
   c) prenos rizika na ďalšiu stranu – zvoliť zmluvnú stranu alebo poist'ovňu na základe zmluvných podmienok.
5. V každom zo zvolených variantov opatrení na modifikáciu rizika vybrať *najvýhodnejšie spôsoby, síly a prostriedky na modifikáciu rizika* (najmä porovnaním nákladov a prínoch), napr. najvýhodnejšiu kamenu, kamerový systém, zámok, dvere, mreže, trezor, najlacnejšiu SBS, poist'ovňu a pod.,
6. Prijat' *rozhodnutie o zavedení opatrenia/opatrení* v jednotlivých zvolených spôsoboch na zaobchádzanie s rizikom, *resp. o ďalšom monitorovaní rizika* v prípade vysokého stupňa neistot, spojených so súčasným stupňom poznania a tým nemožnosti znížiť riziko v etape tvorby rozhodnutia.
7. **Implementovať rozhodnutie na riadenie rizika.**
Tab. 19 Príklad výberu, spôsobu/spôsobov zaobchádzania s rizikom

<table>
<thead>
<tr>
<th>Riziko: Krádež vlámaním do objektu X</th>
<th>Variancy na prijatie opatrení</th>
<th>Výber najvýhodnejších prostriedkov</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zmena pravdepodobnosti rizika</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Zavedenie kamerového systému</td>
<td>Výber z viacerých typov kamerových systémov</td>
<td></td>
</tr>
<tr>
<td>2. Zavedenie poplachového systému na vstupe do objektu</td>
<td>Výber z viacerých typov poplachových systémov</td>
<td></td>
</tr>
<tr>
<td>3. Zavedenie fyzickej ochrany</td>
<td>Výber vhodnej SBS</td>
<td></td>
</tr>
<tr>
<td>Zmena následkov rizika</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Zniženie hodnoty aktiv v jednom priestore ich rozložením do viacerých priestorov</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Úloženie najcennejších aktiv do trezoru</td>
<td>Výber vhodného trezoru z viacerých typov</td>
<td></td>
</tr>
<tr>
<td>Prenos rizika na ďalšiu stranu</td>
<td>Poistenie objektu proti krádeži</td>
<td>Výber najvýhodnejšieho druhu poistenia</td>
</tr>
<tr>
<td>Vyvarovanie sa riziku</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Odstránenie zdroja rizika</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Vyhodnotenie zvolených variantov spôsobov zaobchádzania s rizikom

Po stanovení variantných riešení pre zaobchádzanie s neprijateľnými a prípustnými rizikami by každá možná alternativa mala byť vyhodnotená na základe stanovených kritérií. Počet možností zaobchádzania s rizikom možno zvážiť jednotlive alebo v kombinácii – organizácia má zvyčajne prospech z realizácie kombinácií možností zaobchádzania, preto je výhodné prijať viac spôsobov zaobchádzania s rizikom a v každom spôsobe zvoliť niekoľko variantov. Pri výbere možností zaobchádzania s rizikom má organizácia zvažiť význam a chápanie zainteresovaných účastníkov a najvhodnejšie spôsoby, ako s nimi komunikovať.

Tab. 20 Náklady a prínosy spôsobov zaobchádzania s rizikom

<table>
<thead>
<tr>
<th>Prínosy</th>
<th>Náklady</th>
</tr>
</thead>
<tbody>
<tr>
<td>• zvýšenie ochrany zdravia a počtu chránených osôb,</td>
<td>a) investičné náklady:</td>
</tr>
<tr>
<td>• zvýšenie ochrany majetku,</td>
<td>• cena technológie, zariadenia, prostriedku,</td>
</tr>
<tr>
<td>• zvýšenie ochrany životného prostredia,</td>
<td>• náklady na bezpečnostné sily,</td>
</tr>
<tr>
<td>• redukcia toxicity, mobility alebo objemu nebezpečnej látky,</td>
<td>• náklady na implementáciu.</td>
</tr>
<tr>
<td>• predlženie účinnosti a trvácnosti ochranných zariadení,</td>
<td>b) prevádzkové náklady:</td>
</tr>
<tr>
<td>• veľkosť ušetrených možných strát, dodržanie súladu s bezpečnostnými normami,</td>
<td>• náklady na údržbu,</td>
</tr>
<tr>
<td>• akceptovanie štátmiorgámi,</td>
<td>• náklady na opravy,</td>
</tr>
<tr>
<td>• akceptovanie verejnosťou</td>
<td>• náklady na poistenie.</td>
</tr>
</tbody>
</table>

Okrem uvedených kritérií na posudzovanie nákladov a prínosov si organizácie môžu zvoliť ďalšie kritériá.
Analýza nákladovej efektívnosti

Pri analýze nákladovej efektívnosti sa predpokladá, že je žiaducí určitý prínos alebo výsledok a že existuje niekoľko alternatívnych spôsobov, ako ho dosiahnuť, ktoré sa porovnávajú. V tejto analýze sa berú do úvahy iba náklady a to, ako najlacnejšie dosiahnuť prínos. Účelom analýzy efektívnosti nákladov je zistiť, ktorý variant zaobchádzania s rizikom môže dosiahnuť stanovené ciele na zvýšenie bezpečnosti s čo najmenším nákladom. Používa sa najmä, keď je ocenenie prínosov v peňažných jednotkách pomocou CBA komplikované.

Analýza nákladov a prínosov

Analýza nákladov a prínosov sa môže použiť tam, kde sú celkové očakávané náklady porovnávané s celkovými očakávanými prínosmi s cieľom zvoliť najlepší alebo najviac ziskový variant. Podľa STN EN 31010 analýza môže byť:

- *kvalitatívna* – nehľadá sa žiadne peňažné hodnoty pre nehmotné náklady a prínosy, skôr sa o nich uvažuje kvalitatívne, než aby bol poskytnutý jediný údaj, v ktorom by boli zahrnuté všetky náklady a prínosy, vzťahy a optimalizácia nákladov a prínosov medzi rôznymi nákladmi a prínosmi,
- *kvantitatívna* – zhromažďuje sa peňažná hodnota všetkých nákladov a všetkých prínosov pre všetky zainteresované strany, ktoré sú zahrnuté do rozsahu platnosti analýzy a nastavuje je sa podľa rôzných časových období, v ktorých náklady a prínosy narastajú. Čistá súčasná hodnota, ktorá sa vytvorí, sa stáva vstupom pre rozhodnutie o riziku, alebo môže zahŕňať *kombináciu kvantitatívnych a kvalitatívnych prvkov.*

Analýza nákladov a prínosov sa môže použiť na prijatie rozhodnutia medzi variantami, ktoré zahŕňajú riziko, napr.:

- ako vstup pre rozhodovanie o tom, či riziko má byť modifikované,
- na rozlišenie medzi spôsobmi zaobchádzania s rizikom a rozhodnutie o najlepšom spôsobe (spôsoboch) zaobchádzania,
- na rozhodnutie medzi rôznymi postupmi zásahu.

Charakteristika nákladov a prínosov je uvedená v tabuľke 21.

**Tab. 21 Charakteristika nákladov a prínosov**

<table>
<thead>
<tr>
<th>Náklady</th>
<th>Prínosy</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Obsah</strong></td>
<td><strong>pozitívne výsledky,</strong></td>
</tr>
<tr>
<td>• spotrebované zdroje,</td>
<td>• negatívne výsledky, ktorým sa zabránilo,</td>
</tr>
<tr>
<td>• negatívne následky udalosti – náklady na odstraňovanie následkov, skutočná škoda, ušlý zisk a pod.</td>
<td>• ušetrené zdroje.</td>
</tr>
<tr>
<td><strong>Druhy</strong></td>
<td><strong>priame náklady – vyplývajú z priamo uskutočneného opatrenia zaobchádzania s rizikom,</strong></td>
</tr>
<tr>
<td>• priame náklady – vynaložené na opatrenia zaobchádzania s rizikom,</td>
<td>• nepriame prínosy – vedľajšie prínosy, náhodné, ale stále ešte môžu prispievať k rozhodnutiu, napr. zlepšenie povesti, spokojnosť personálu a pod.</td>
</tr>
<tr>
<td>• nepriame náklady – dodatočné, vedľajšie a utopené náklady, ako sú strata použiteľnosti, mŕvanie časom manažmentu, odvod kapitálu z ďalších potenciálnych investícií a pod.</td>
<td></td>
</tr>
</tbody>
</table>

Vstupy zahŕňajú informácie o nákladoch a prínosoch pre príslušné zainteresované strany a o neistotách ohľadne tých nákladov a prínosov. Majú sa zohľadniť hmotné a nehmotné náklady a prínosy. Identifikujú sa priame i nepriame prínosy a náklady zvolených
variantov pre všetky príslušne zainteresované strany. Keď sa analýza nákladov a prínosov využíva na rozhodnutie či modifikovať riziko, majú byť do nej zahnuté:

- na jednej strane náklady a prínosy súvisiace s modifikáciou rizika,
- na druhej strane náklady a prínosy súvisiace s podstúpením rizika.

Výstupom z analýzy nákladov a prínosov je informácia o relatívnych nákladoch a prínosoch rôznych variantov, čo sa môže vyjadriť:

- kvantitatívne – ako čistá súčasná hodnota (NVP – Net Present Value), vnútorná miera návratnosti (IRR – Internal Rate of Return) alebo ako pomer súčasnej hodnoty prínosov k súčasnej hodnote nákladov,
- kvalitatívne – obvykle ako tabuľka, v ktorej sú porovnané náklady a prínosy rôznych typov nákladov a prínosov, ktoré upozorňujú na optimalizáciu nákladov a prínosov.

Náklady na zavedenie opatrení je treba spočítať s určitou presnosťou, pretože sú základnou mierkou, podľa ktorej sa posudzuje finančná náročnosť a účinnosť opatrení. Ďalej je potrebné odhadnúť pravdopodobné straty, ak nebudú podniknuté žiadne kroky, a až na základe výsledkov môže vedenie rozhodnúť, či zaviesť alebo nezaviesť navrhované opatrenia na zniženie rizík.

Pritom je nutný súlad so zákonní. Organizácia musí poznávať príslušné zákony a musí zaviesť súbor opatrení, ktoré umožnia dosiahnuť súlad s týmito zákonní. Iba vo výnimkových prípadoch je povolená určitá voľnosť a to v prípadoch, kedy náklady na zniženie rizika sú značne neprimerané samotnému riziku.

Jedným zo spôsobov, ako si zaistiť finančnú ochranu proti následkom rizík je financovanie rizík, tento spôsob zahŕňa poistenie. Pritom sú treba uvedomiť, že niektoré straty alebo čiastočné straty sa nedajú poistiť, napríklad náklady spojené s bezpečnosťou a ochranou zdravia pri práci alebo inými udalosťami, ktoré môžu viest’ k narušeniu pracovnej disciplíny zaostatnancov alebo povesti organizácie.

Plán zaobchádzania s rizikom

Účelom plánu zaobchádzania s rizikom je zdokumentovať’ ako sa vybraté možnosti zaobchádzania budú zavádzať. Plán zaobchádzania s rizikom má jasne definovať poradie priorít, v akom sa jednotlivé spôsoby zaobchádzania budú zavádzať.

Plán zaobchádzania s rizikom má obsahovať:

a) príčiny výberu možnosti zaobchádzania vrátane očakávaných účinkov, ktoré možno ziskat’,
b) určenie pracovníkov zodpovedných za schválenie plánu, ako aj pracovníkov zodpovedných za jeho zavedenie,
c) definovanie poradia priorít, v akom sa jednotlivé metódy zaobchádzania budú zavádzať,
d) navrhané činnosti (opatrenia na riešenie jednotlivých rizík),
e) požiadavky na zdroje, vrátane neočakávaných nákladov,
f) mieru výkonnosti a obmedzenia,
g) požiadavky na monitorovanie, že opatrenia na zaobchádzanie s rizikom boli efektívne a monitorovanie sekundárneho rizika a podávanie správ,
h) harmonogram a časový rozvrh (postupnosť implementácie plánu a termíny realizácie zaobchádzania s jednotlivými rizikami).

Plán zaobchádzania s rizikom (Risk treatment plan) sa má stať súčasťou manažérskych procesov organizácie a musí sa prediskutovať’ s príslušnými zainteresovanými účastníkmi.
Pracovníci, prijímajúci rozhodnutia, a ďalší zainteresovaní účastníci si majú uvedomovať podstatu a rozsah zvyškového rizika po jeho ošetrení. Zvyškové riziko sa musí:
• zdokumentovať,
• monitorovať,
• preskúmavať,
• a ak treba, musí sa organizácia ním naďalej zaoberať.
9.3 ĎALŠIE SÚČASTI PROCESU MANAŽÉRSTVA RIZIK

Monitorovanie a preskúmavanie

Monitorovanie znamená nepretržité kontrolovanie, dozor, kritické pozorovanie či určovanie stavu na to, aby sa zistila zmena požadovanej či očakávanej úrovne. Preskúmavanie predstavuje aktivitu podniknutú na určenie vhodnosti, primeranosti a účinnosti manažérstva rizika pre dosiahnutie stanovených cieľov.

Monitorovanie aj preskúmavanie možno podľa ISO Guide 73:2009 aplikovať na:
• štruktúru manažérstva rizika,
• proces manažérstva rizika,
• riziko,
• riadenie rizika.

Monitorovaná a zdokumentovaná má byť účinnosť opatrení na riadenie rizika, aby bolo možné zabezpečiť posúdenie na účely analýzy rizík. Majú byť stanovené povinnosti pre prijatie zodpovednosti za tvorbu a preskúmanie dokladov a dokumentov.

Jedným z najúčinnejších spôsobov, ako sledovať riziká je sledovanie životného prostredia jednotlivcami, poverenými zaobchádzať s jednotlivými rizikami a pretože ochranné opatrenia, na ktoré sme sa spoliehali mnoho rokov, sa stali nedostatočné alebo nieefektívne. Ak organizačia nesleduje zmeny svojich vnútorných a vonkajších súvislostí a hodnotenia, či jej ovládavé prvky sú ešte účinné, potom zhodnotenie rizík, ktorým čelí a úrovne týchto rizík môžu byť nesprávne.

Tieto faktory majú byť špecificky identifikované pre pokračujúce monitorovanie a preskúmavanie, aby bolo možné zabezpečiť údaje na účely analýzy rizík. Majú byť stanovené povinnosti pre prijatie zodpovednosti za tvorbu a preskúmanie dokladov a dokumentov.

Jedným z najúčinnejších spôsobov, ako sledovať riziká, je sledovanie životného prostredia jednotlivcami, poverenými zaobchádzať s jednotlivými rizikami a pretože ochranné opatrenia, na ktoré sme sa spoliehali mnoho rokov, sa stali nedostatočné alebo nieefektívne. Ak organizačia nesleduje zmeny svojich vnútorných a vonkajších súvislostí a hodnotenia, či jej ovládavé prvky sú ešte účinné, potom zhodnotenie rizík, ktorým čelí a úrovne týchto rizík môžu byť nesprávne.

Tieto faktory majú byť špecificky identifikované pre pokračujúce monitorovanie a preskúmavanie, aby bolo možné zabezpečiť údaje na účely analýzy rizík. Majú byť stanovené povinnosti pre prijatie zodpovednosti za tvorbu a preskúmanie dokladov a dokumentov.

Jedným z najúčinjejších spôsobov, ako sledovať riziká, je sledovanie životného prostredia jednotlivcami, poverenými zaobchádzať s jednotlivými rizikami a pretože ochranné opatrenia, na ktoré sme sa spoliehali mnoho rokov, sa stali nedostatočné alebo nieefektívne. Ak organizačia nesleduje zmeny svojich vnútorných a vonkajších súvislostí a hodnotenia, či jej ovládavé prvky sú ešte účinné, potom zhodnotenie rizík, ktorým čelí a úrovne týchto rizík môžu byť nesprávne.

Tieto faktory majú byť špecificky identifikované pre pokračujúce monitorovanie a preskúmavanie, aby bolo možné zabezpečiť údaje na účely analýzy rizík. Majú byť stanovené povinnosti pre prijatie zodpovednosti za tvorbu a preskúmanie dokladov a dokumentov.

Jedným z najúčinnejších spôsobov, ako sledovať riziká, je sledovanie životného prostredia jednotlivcami, poverenými zaobchádzať s jednotlivými rizikami a pretože ochranné opatrenia, na ktoré sme sa spoliehali mnoho rokov, sa stali nedostatočné alebo nieefektívne. Ak organizačia nesleduje zmeny svojich vnútorných a vonkajších súvislostí a hodnotenia, či jej ovládavé prvky sú ešte účinné, potom zhodnotenie rizík, ktorým čelí a úrovne týchto rizík môžu byť nesprávne.
• záznam procesu manažérstva rizika.

Monitorovanie a preskúmavanie sa vykonáva s cieľom overiť, že:
• predpoklady o rizikách ostávajú platné,
• ostávajú platné predpoklady, na ktorých je založené posudzovanie rizik vrátane vonkajších a vnútorných súvislostí,
• sú dosiahnuté očakávané výsledky,
• výsledky posudzovania rizík sú v zhode so skutočnou skúsenosťou,
• techniky (metódy) posudzovania rizík sa vhodne používali,
• zaobchádzanie s rizíkom je efektívne,

Za monitorovanie a preskúmavanie sa má jasne definovať zodpovednosť. Procesy monitorovania a preskúmavania organizácie majú obsahovať všetky aspekty procesu manažérstva rizík s cieľom:
• zabezpečiť, že kontroly počas navrhovania a prevádzky sú efektívne a účinné,
• získať dôsledné informácie na zlepšenie hodnotenia rizíka,
• analyzovať udalosti a získat' z nich poučenia, zmeny, trendy, úspechy a neúspechy,
• zistiť zmeny v externých a interných súvislostiach vrátane zmien v kritériách rizíka a v samotnom rizíku, ktoré môžu vyžadovať revíziu zaobchádzania s rizíkom a revíziu priorit,
• identifikovať vznikajúce riziká.

Meradlom výkonnosti je pokrok v zavádzaní plánov zaobchádzania s rizíkami. Výsledky možno začleniť do celkového manažérstva výkonnosti organizácie, do merania a podávania externých a interných správ. Výsledky monitorovania a preskúmavania sa majú začleniť do celkového manažérstva rizíka.

S cieľom ubezpečiť sa, že manažérstvo rizíka je efektívne a naďalej podporuje výkonnosť organizácie, organizácia má:
• merat' výkonnosť manažérstva rizíka pomocou ukazovateľov, ktorých vhodnosť sa periodicky preskúmava,
• periodicky merat' pokrok oproti plánu manažérstva rizíka, ako aj prípadné odchýlky,
• periodicky preskúmavať, ší štruktúra, politika a plán manažérstva rizíka sú stále v danych externých a interných súvislostiach vhodné,
• podávať správy o rizikách, pokroku v pláne manažérstva rizíka a ako sa dodržiava politika manažérstva rizíka,
• preskúmať efektívnosť štruktúry manažérstva rizíka.

Proces monitorovania by mal poskytovať záruky, že sú zavedené vhodné opatrenia pre činnosti organizácie a postupy riadenia rizík v organizácii sú zrozumiteľné a dodržiavané.

Výsledky monitorovania a preskúmavania:
• možno začleniť do celkového manažérstva výkonnosti organizácie, do merania a podávania externých a interných správ,
• sa majú zaznamenáť, podľa potreby interne a externe oznamovať a aj využívať ako vstupy do preskúmania štruktúry manažérstva rizíka.

Cyklus hodnotenia rizík sa uskutočňuje vždy:
• pred uvedením nového zariadenia, prípadne pracoviska do používania (východiskové vyhodnotenie rizík),
• ako kontrolu po prežití nebezpečných udalostí,
• po každej zmene, ktorá mohla mať vplyv na bezpečnosť práce,
• po nehode / úrazu,
• keď nastanú závažné organizačné zmeny, napríklad zavedenie druhej zmeny nebo zmena kvalifikácie zamestnancov,
• na základe zistenia orgánov Inšpekcie práce alebo orgánov ochrany verejného zdravia,
• na záväzný pokyn príslušného odborového orgánu alebo návrh zástupcu zamestnancov pre BOZP.

**Hodnotenie rizík by sa malo vykonávať** v pravidelných intervaloch alebo v intervaloch stanovených pre jednotlivé pracoviská zamestnávateľom podľa vykonávaných rizikových prác a ďalších skutočností, ktoré rizikovosť a početnosť prevencie ovplyvňujú.

**Audit manažérstva rizika** predstavuje systematický, nezávislý a zdokumentovaný proces pre získanie dôkazov a objektívne hodnotenie na určenie primeranosti a efektívnosti štruktúry manažérstva rizika alebo jej zvolenej časti.

**Podávanie správy o riziku** (review) predstavuje formy komunikácie využívané na informovanie vnútorných alebo vonkajších zainteresovaných účastníkov, poskytovanie informácií o aktuálnom stave rizika a jeho manažérstve.

**Záznamy o procese manažérstva rizika**
Činnosti manažérstva rizika majú byť sledovateľné, proces posudzovania rizík má byť zdokumentovaný spolu s výsledkami posudzovania.

**Záznamy o procese manažérstva rizika** poskytujú podklad na zlepšovanie metód a nástrojov, ako aj na zlepšovanie celkového procesu. Rozhodnutia týkajúce sa tvorby záznamov majú brať do úvahy:
• potreby organizácie neustále sa učiť,
• úžitok z opakovaného využívania informácií na manažérske účely,
• náklady a úsilie obsiahnuté v tvorbe a udržiavanie záznamov,
• zákonné, predpisové a prevádzkové požiadavky záznamov,
• metódy prístupu, ľahkosti vstupu a uloženia informácií,
• periódu uchovávania,
• citlivosť informácií.

Proces posudzovania rizika má byť zdokumentovaný spolu s výsledkami posudzovania. Rizíká majú byť vyjadrené zrozumiteľné a jednotné, v ktorých je vyjadrená úroveň rizika, rozsah bude závisieť od cieľov a rozsahu posúdenia. Rozsah bude závisieť od cieľov a rozsahu posúdenia. S výnimkou veľmi jednoduchého posúdenia je možné do dokumentácie zahrnúť:
• ciele a rozsah platnosti,
• popis dôležitých častí systému a ich funkcí,
• súhrn vonkajších a vnútorných súvislostí organizácie, a ako tieto súvislosti súvisia s posudzovanou situáciou, systémom alebo okolnostami,
• použité kritériá rizika a ich zdôvodnenie,
• obmedzenia, predpoklady a zdôvodnenie hypotéz,
• metodika posudzovania,
• výsledky identifikácie rizík,
• dáta, predpoklady a ich zdroje a overenie,
• výsledky analýzy rizík a ich hodnotenia,
analýza citlivosti a neistôt,
kritické predpoklady a ďalšie faktory, ktorej je potrebné monitorovať,
rozbor výsledkov,
závery a odporúčania,
odkazy.

Záznamy o procesoch manažérstva rizika poskytujú podklad na zlepšovanie metód a nástrojov, ako aj na zlepšovanie celkového procesu. Ak posudzovanie rizika podporuje pokračujúci proces manažérstva rizika, posudzovanie má byť vykonané a zdokumentované takým spôsobom, že môže byť zachované v priebehu životného cyklu systému, organizácie, zariadenia alebo činnosti. Posudzovanie má byť aktualizované v súlade s potrebami procesu manažérstva, keď sa podstatné informácie stanú dostupnými a zmenia sa súvislosti.

Nepretržité zlepšovanie manažérstva rizika

Na základe výsledkov z monitorovania a z preskúmavania sa majú prijať rozhodnutia, ako možno zlepšiť výkonnosť manažérstvo rizika, politiku a príslušný plán. Takéto rozhodnutia by mali vyústiť do zlepšovania manažérstva rizika organizácie a jej kultúry manažérstva rizika.

Vysoké úroveň výkonnosti v manažérstve rizika predstavuje nasledujúci zoznam vlastností, v ktorom sú uvedené konkrétne ukazovatele výkonnosti pre každú vlastnosť:

- nepretržité zlepšovanie,
- plná zodpovednosť za riziko,
- aplikácia manažérstva rizika v prijímaných rozhodnutiach,
- nepretržitá komunikácia,
- úplné začlenenie manažérstva rizika do riadiacej štruktúry organizácie.

Dôraz sa kladie na nepretržité zlepšovanie manažérstva rizika prostredníctvom určenia cieľov výkonnosti organizácie, merania, preskúmavania a následnej modifikácie procesov, systémov, zdrojov, spôsobilostí a zručností. Možno to vyjadriť vytvorením explicitných cieľov výkonnosti, vzhľadom na ktoré sa meria výkonnosť organizácie a jednotlivých manažérov.

Výkonnosť organizácie sa môže publikovať a oznamovať. Posúdenie výkonnosti manažérstva rizika predstavuje integrálnu časť celkového posúdenia výkonnosti organizácie a meracieho systému pre oddelenia a jednotlivcov. Všetky organizácie sa majú snažiť o vhodnú úroveň výkonnosti svojej štruktúry manažérstva rizika v súlade s kritickosťou rozhodnutí, ktoré treba urobiť. Zvyčajne sa realizuje aspoň ročné preskúmanie výkonnosti nasledované revíziou procesov a určením revidovaných cieľov výkonnosti pre nasledujúce obdobie.

Kľúčovými výsledkami manažérstva rizika sú:

- organizácia má súčasné, správne a obsažné chápanie svojich rizík,
- kritériá rizika obsahujú riziká organizácie,
- nepretržité zlepšovanie.

Účasť verejnosti

Neoddeliteľnou súčasťou procesu zaobchádzania s rizikami je účasť verejnosti na prijímaní rozhodnutí. Účelom účasti verejnosti je získať nezávislý pohľad na proces, a zároveň mať priestor pre informovanie a ovplyvňovanie verejnosti. Účasť verejnosti prispieva ku:

- skvalitneniu vstupných údajov použitých v procese,
- tvorbe ďalších variantných riešení znižovania rizika,
akceptovateľnosti výsledkov verejnosťou.

Pri rokovaniach s verejnosťou sú využívané rôzne techniky dohadovalosť, s cieľom vyjasnenia záujmov a postojov. Veľmi dôležitou časťou je správne odhadnúť a pozitívne ovplyvniť štruktúru vnímania rizík u jednotlivec, tým ho dovest′ k prijímaniu a realizácii opatrení na minimalizáciu rizíka na prijateľnú úroveň. Prikladom na zapojenie verejnosti môže byť BOZP, kde je organizácia okrem toho povinná:

• zoznámiť zamestnancov, príslušné odborové orgány alebo zástupcov pre oblasť BOZP s výsledkom vyhodnotenia rizík vrátane prijatých bezpečnostných opatrení na zníženie ich pôsobenia na zdravie zamestnancov na pracovisku,

• zaistiť kvalitné školenie zamestnancov a vedúcich zamestnancov o právnych a ostatných predpisoch pre zaistenie BOZP vrátane informácií o rizíkach, ktoré sa týkajú ich práce a pracoviska a zaistiť pravidelné overovanie ich znalostí,

• prerokovať so zamestnancami, prípadne ich zástupcami, aj výsledky kontrol zameraných na účinnosť prijatých bezpečnostných opatrení, pretože sústavné vyžadovanie a kontrolovanie je nutným predpokladom pre zaistenie bezpečných a zdravie neohrožujúcich podmienok práce,

• informovať o rizíkach i osoby, ktoré nie sú priamo zamestnancami, ale pohybujú sa s vedomím zamestnávateľa na jeho pracoviskách.

9.4 LITERATÚRA


10 ZÁVER

Bezpečnosť spoločnosti i prírody ovplyvňovali po mnohých tisíce rokov najmä riziká:
• prirodňé, napr. bleskom spôsobené požiare, povodne, záplavy, extrémne suchá, lavíny, vichrice a iné živelné pohromy,
• spoločenské, najmä vojnové konflikty, hlad spôsobený neúrodu, rôzne epidémie a pandémie, ktoré si vyžiadal oveľa viac strát ako riziká prirodne.

S rozvojom spoločnosti, najmä po priemyselnej revolúcií, sa charakter, počet, intenzita a zameranie rizík postupne menili. Prírodné riziká ostali, ich vplyv a účinnosť sa však najmä škodlivými zásahmi človeka do prírody zvýšili. Podobne tak pretrváva v spoločnosti riziko hladu a vyskytujú sa aj nové, zložitejšie zdravotné epidémie a pandémie. Až príliš veľké spoločenské riziká predstavujú neobmedzené zbrojenie, rozšírenie zbraní hromadného ničenia a širenie spoločenskej neznášanlivosti, najmä rôznych druhot extrémizmu.

V minulých dvoch storočiach sa objavili nové, závažné riziká, ktoré podstatným spôsobom vplyvajú na bezpečnosť ľudí, majetku, životného prostredia, ale aj na bezpečnosť podnikania. Tieto nové riziká sa odvádajú najmä od technického a technologického rozvoja, vzniku a presadzovania informačnej spoločnosti, rozšírenia pracovných príležitostí a zásahov človeka do prírody.

Tieto riziká na jednej strane, najmä pre podnikanie, predstavujú možnosť zisku, na druhej strane riziká, ktoré majú zdroj v určitom nebezpečenstve, môžu mať za následok rôzne škody.

S vývojom nových rizík postupoval aj vývoj spôsobov, ako ich možno využívať vo svoj prospech i ako sa pred nimi chrániť. Až donedávna sa riziká hodnotili najmä z ich negatívneho vplyvu, preto sa tieto teórie museli prehodnotiť. V nových normách o manažérstve rizika sa riziko posúdzuje z oboch strán, napriek tomu, že ešte v mnohých odborných, najmä technologických normách sa ešte hodnotí najmä ich negatívny účinok.

Druhá časť učebnice nerieši podnikateľské riziká, z hľadiska dosahov zisku, je zameraná najmä na riešenie vonkajších a vnútorných rizík, ktoré ovplyvňujú referenčné objekty, so zameraním na bezpečnostné riziká, vyplývajúce z určitého nebezpečenstva.

Popisuje druhy nebezpečenstva a rizík, ktoré z nich môžu vzniknúť. V ďalšej časti rieši štruktúru a proces manažérstva týchto rizík v organizáciách, ktoré prijímajú mandát a záväzok na dodržiavanie bezpečnosti vo všetkých oblastiach ich činností.

Kvalitné vykonaná identifikácia, analýza a hodnotenie bezpečnostných rizík umožní nájsť vhodné spôsoby na zaobchádzanie s prípustnými a neprijateľnými rizikami, ktoré je potrebné určitým spôsobom modifikovať a monitorovať, aby nespôsobili závažné negatívne následky.

Manažérstvo rizika je jedným z prvých krokov pri zavádzaní bezpečnostnej politiky a plánovaní bezpečnosti v organizácii. Tento proces sa bude riešiť v ďalšej časti učebnice pod názvom: MANAŽÉRSTVO BEZPEČNOSTI
RIZIKÁ BOZP NA PRACOVISKÁCH

Pracovníci čelia pri práci radu bezpečnostných rizík, vrátane menších a traumatických fyzických zranení, požiarov a násilia. Ak sú pracovníci poškodené alebo zranené, podniky prídu o peniaze, zvýšia sa poistné a zdravotné náklady a nastanú možné súdy. Pochopenie základných rizikových faktorov a plánovité zavedenie ich riadenia pomôže zvýšiť zníženú produktivitu a znižiť náklady súvisiace so zraneniami.

Administratívne pracoviská
- nevhodné pokrytie podlahy, napríklad diery a prekážky,
- nevhodné rozmyšliené miestnosti, ktoré nielen pozdvojným členom alebo zamestnancov a zodpovedajúce právne normy,
- nepripravené dostatočne osvetlenie,
- okná nevybavené zatemnením pre používanie zobrazovacích jednotiek,
- svetelné odrážadlo na obrazovku, prípadne rôznych zdrojoch,
- rušenie pozornosti a verbálnej komunikácie rôznych hlukom,
- káble a vedenie pochádzajúce na podlahe alebo v priestore prekáža voľnému pohybu,
- necítzenie a neudržiavanie budovy,
- nedostupnosť lekárničky na obrázku prvej pomoci,
- neodoznacené a zatartasené únikove cesty a nitézové východy,
- nestabilné a ergonomické prílohy stoličky, ich neprimeraná výška alebo nemožnosť šňůrko prednej foteliny, chýbajúce opierky ramena alebo opierky chodidiel v prípade potreby,
- výška stolu neumožňuje šňůru pohyblivosť nôh,
- kmitanie obrazov zo zobrazovacích jednotiek, nemožnosť premierniť obrazovacie jednotky podľa potreby, pôsobenie rušivých svetelných reflexov na obrazovku,
- nedodržanie vzdialenosť 50 – 80 cm medzi očami a obrazovkou, nevhodné umiestnenie klávesnice, nedostatok priestoru medzi klávesnicou a myšou,
- povrch klávesnice nie je matný, aby neodrážal svetlo, symboly na klávesnici nie sú jasne rozlišiteľné a pre obsluhu dobre šnitoľné,
- nemožnosť prestávok v prípade dlhodobo práce pred obrazovkou,
- nemožnosť zmeniť typ práce pri dlhodobej práci pred obrazovkou,
- vydávanie rôznorôdých úloh zamestnancom, udržiavanie zamestnancov pod nadmerným pracovným tlakom, ich vystavenie nadmernému psychickému zaťaženiu,
- neabsolvovanie výcviku, konzultácií a neposkytnutie informácií zamestnancom skôr, než boli zaradené na konkrétne pracovné miesto,
- nevenovanie pozornosti informáciám zamestnancov, ak sa sťažujú na problémy so zrakom, nesystematicky sledovanie stavu zraku zamestnancov v zmysle platnej národného poriadku,
- sťažnosti zamestnancov na svalovo-pohybové problémy (krk, chrbát, ramena, nohy) a nevykonanie ergonomického posúdenia ich pracoviska.

Stavebné práce
- nebezpečný prístup zamestnancov na pracovisko, nezabezpečenie vstupov na pracovisko pred vstupom nepovolaných osôb, nepreehľadne usporiadané pracovisko,
- voľnej neprevážne a neosvetlené dopravné cesty,
- nevybavenie vozidiel akustickou výstrahou pri cestovaní,
- zlé osvetlenie pracovisko,
- nesprávne bezpečnostné označenia pracoviska,
nedostatočné zariadenia pre osobné potreby zamestnancov, napr. umývárne, prezlikařské, oddychové miestnosti,
nevybavenie pracoviska prostriedkami prvej pomoci,
nevyškolenie zamestnancov v bezpečnosti manipulácie,
nie sú k dispozícii vhodné zdvihacie zariadenia a pomôcky pre manipuláciu s ťažkými bremenami,
nie sú definované systematizované bezpečnostné pokyny ohľadom elektrických vedení,
nezabezpečenie pravidelnej údržby a kontroly elektrických zariadení na pracovisku,
práca s lešeniami nie je zverená osobám s odbornou spôsobilosťou, lešenia nie sú periodicky kontrolované,
šírka pracovného priestoru na lešení je menšia než minimum (60 cm),
zdvihacie zariadenia a výťahy nie sú správne inštalované a pravidelne kontrolované,
zamestnanci nepoužívajú správne zaistenie pri práci vo výškach súlade s platnými bezpečnostnými normami,
nie sú vykonané opatrenia na zabránenie pádu osôb a predmetov,
nie sú vykonané preventívne opatrenia na zniženie rizika vystavenia zamestnancov pôsobeniu prachu (napr. z drevca, cementu),
nie sú prijaté opatrenia na zniženie škodlivých vplyvov hluku a vibrácií,
stroje a zariadenia nie sú udržiavané v bezpečnom stave,
zvukové výstražné signály na strojoch nie sú funkčné,
pri výkopocho nie sú vykonané bezpečnostné opatrenia na zabránenie zrútenia sa ich stien,
vodiči a obsluha strojov nie sú správne vycvičení na vykonávanie svojej práce,
všetkým zamestnancom nie sú poskytnuté bezpečnostné pokyny o potenciálnych rizikách.

**Elektrická inštalácia a elektrické vybavenie**
- bezpečnostné zariadenia a vypínače nie sú na mieste a nefungujú správne,
- poškodenie izolácie, zásuviek alebo objímok, elektrických rozvodných skříní alebo nie sú chránené pred neoprávnênim vniknutím,
- elektrické rozvodné skříně bez označení podľa IEC,
- možnosť nesprávného použitia elektrického vybavenia,
- možný kontakt s elektrickým zariadením s vlhkými rukami alebo vo vlhkom oblečení,
- možnosť pracovať v nebezpečnej blízkosti elektrických zariadení,
- sú nejaké živé časti v blízkosti pracovných oblastí,
- všetkým zamestnancom nie sú poskytnuté odradovací zariadenia,
- možnosť vzniku elektrostatických nábojov.

**Osvetlenie**
- osvetlenie pracoviska nedostatočné vzhľadom na efektívne a presné plnenie pracovných úloh,
- niektoré pracovné oblasti zatiaľ nie sú dostatočne osvetlené,
- napríklad v zornom poli existujú nadmerné kontrasty, ktoré zhoršujú vizuálne vnímanie a môžu spôsobiť poškodenie zraku,
- zhoršujú sa vytvorené kontrasty pri osvetlení nevysoko nebo nedostatočne,
- v osevnaďať vysevádnej oblasti s komplikovaným terénom, ktoré môžu spôsobiť poškodenie zraku,
- na niektorých miestach vznikajú svetelné odrady,
- v osvetlení pracoviska sú veľké rozdiely, ktoré môžu spôsobiť zrakový stres,
- pri umelom osvetlení nie sú zachované pôvodné farebné odtiene,
- pri existujúcom umelom osvetlení nie sú rešpektované bezpečnostné opatrenia,
- obťažovanie zamestnancov blikajúcimi svetlami,
**Pohybujúce sa časti strojov**
- nechránené pohybujúce sa časti strojov,
- ochranné zariadenia nechránia ruky, ramená a iné časti tela zamestnancov pred kontaktom s nebezpečnými pohybujúcimi sa časťami,
- nie sú pevne uchycené a ľahko odstrániteľné všetky ochranné kryty strojov,
- možnosť padnutia nejakého predmetu na pohybujúcu sa časť stroja,
- nechránené ozubené kolesá, reťazové kolesá, bubny alebo zotrvačníky,
- niektoré remeňové alebo reťazové prevody sú nechránené,
- pre obsluhu je ťažké dosiahnuť na vypínače ZAPNI a VYPNI,
- jeden vypínač slúži viacerým operátorom.

**Podlahy**
- na podlahách sú oblasti s nerovnosťami, poškodeným povrchom, diery a pod.,
- podlahy nie sú udržiavané v čistote, sú niekedy klzké, napr. po umýtí, rozliatí kvapalin, od dážďa alebo sú zaprášené v dôsledku pracovných procesov,
- na podlahu sa vyskytujú prahy alebo iné zmeny úrovne,
- na podlahe sú nátiahnuté káble,
- zamestnanci môžu spadnúť alebo sa šmyknúť v dôsledku nepoškodených priemyselných prevádzok,
- v okolí pracovných priestorov sú ponechané prekážky alebo zavadzajúce objekty,
- nezabezpečenie neodstránených prekážok,
- nesprávne označenie dopravných ciev,
- nezabezpečenie vhodného osvetlenia podlá a dopravných ciev.

**Autoopravovne a garáže**
- ploché povrchy nie sú pravidelne čistené,
- pracovníci nie sú povinní udržiavať čistotu na pracovisku,
- povrchy nie sú odolné voči používaným chemickým látkam ako napr. olej, nafta, petrolej,
- olej nie je uskladňovaný v správnych nádobách,
- schody do montážnej jamy nie sú z protišmykového materiálu, zamestnanci nenosia protišmykovú obuv,
- zamestnancom nie je zdôrazňovaný zákaz vstupu pod zdvihané vozidlo,
- montážna jama, v ktorej sa nepracuje, nie je zakrytá, nie je vhodne označená a nie je dostatočne vetraná,
- zamestnanci pracujú v stisnených priestoroch,
- pracovné náradie nemá svoje stále miesto,
- nie sú vyznačené trasy vstupu vozidiel na servisné stanovišta,
- nie sú prijaté opatrenia na zabránenie úrazom pri fyzických prácou, napr. zváraní, brúsení, natieraní a pod.,
- nie sú stanovené bezpečnostné predpisy pre montážne práce a pre práce so zásobníkmi paliva,
- nie sú prijaté opatrenia na zabránenie pádu predmetov z vozidla, napr. keď je vozidlo zdvihnuté, alebo sa pracuje okolo neho,
- garážové dvere sa nedajú zafixovať proti samovolnému zavretiu,
- osvetlenie montážnej jamy nie je vhovovujúce vzhladom na vykonávaný druh montážnych a servisných prác,
- nie je zabezpečená vhodná teplota na pracovisku v zime aj v lete,
- zamestnanci nie sú oboznámení s bezpečnostnými predpismi a nie sú správne vyškolení na plnenie svojich pracovných úloh.
EXTERNÉ A INTERNÉ SÚVISLOSTI

EXTERNÉ SÚVISLOSTI

Externé súvislosti predstavujú externé prostredie, v ktorom organizácia chce dosiahnuť svoje zámery. Z podnikateľského hľadiska môžu faktory externého prostredia predstavovať priležitosti, na druhej strane však môžu pre podnikanie znamenať nebezpečenstvá, ktoré prinášajú straty. Medzi ne patria najmä faktory:

a) Faktory prostredia na medzinárodnej, národnej, regionálnej alebo miestnej úrovni:
   - Sociálne faktory súvisia so spôsobom života ľudí vrátane životných hodnôt, patria sem najmä: viera, hodnoty, názory a životný štýl ľudí v prostredí, vývoj populácií, kultúrnych, ekologických, demografických, náboženských a etnických podmienok, rast úrovne vzdelávania a vzdelanosti, záujem o celoživotné vzdelávanie a jeho ponuka, štruktúra školstva v regióne, životný štýl v regione, podmienky pre rekreáciu a využitie volného času, dĺžka materskej dovolenky, sekularizácia, masmédiá, skupinové názory ľudí na spoločenské problémy a pod.
   - Demografické faktory predstavujú najmä: štruktúra obyvateľstva, demografická krvíka prírastku, priemerná dĺžka života, hustota obyvateľstva, rodinné faktory, zmeny vo veľkovej štruktúre obyvateľstva, zmeny v počte členov rodiny, geografické rozloženie populácie, zmeny v pracovnom postavení.
   - Kultúrne faktory ovplyvňujú základné hodnoty spoločnosti, postoje, záľuby a správanie, napríklad: pretrvávanie základných hodnôt, zmeny sekundárnych hodnôt, subkultúry (skupiny ľudí s rovnakými hodnotovými systémami).
   - Ekonomické a finančné faktory sú v makroprostredí rozhodujúce, charakterizujú sa vývojom rastu hrubého národného produktu, priame úrokové miery, miera inflácie, úroveň použiteľného príjmu, zmeny v štruktúre výdavkov obyvateľstva, miera nezamestnanosti, menový kurz, fluktuácia akciového trhu, veľkosť štátneho rozpočtu, obchodný deficit, všeobecná dostupnosť úverov.
   - Politické faktory predstavujú najmä: stabilita vlády a jej prístup k podnikaniu, zahraničná orientácia, politika, vznik záujmových skupín na ochranu verejného záujmu, zahranično-obchodné rozhodnutia, sústavy daní, právne predpisy vymedzujúce minimálnu mzdu, cenové regulácie, opatrenia, ktorých cieľom je ochrana ekonomickej stability krajiny, zamestnancov, zákazníkov, verejného záujmu a životného prostredia.
   - Právne faktory predstavujú najmä: právne a etické normy, výkonové predpisy, zákonov v oblasti podnikania, antimonopolné zákony, etické právne predpisy, zákonov v posilnení postavenia kontrolných orgánov, ktoré svojomu činnosťou dohliadajú na dodržiavanie zákonov.
   - Technické a technologické faktory predstavujú najmä: neohraničené možnosti vo vývoji vedy, rozpočet na výskum a vývoj, výskumné ústavy, výskumnovo-vývojové základne, technologické parky, inovačné centrá, počet novovýrobených, ale hlavne novozavedených technológií umožňujúcich veľké inovácie, vynálezy a inovácie prinášajúce nové možnosti pre tvorbu nových výrobkov, zlepšovanie existujúcich výrobkov a pre zmenu výrobných a marketingových postupov, miniaturizácia a zvyšovanie výkonu informačných technológií, automatizácia a robotizácia, použitie e-biznisu, zvyšené regulacné zásahy v záujme ochrany spotrebiteľa.
   - Prírodné (geografické) faktory predstavujú súbor prírodných vplyvov: dážď, voda, vextor, striedanie teplôt, slnečné žiarenie a UV žiarenie, prach, emisie (chemické pôsobe-
nie) a pod. Z geografického hľadiska sem patria prírodné zdroje, ktoré sa využívajú ako vstupy, dnes existujú štyri skupiny trendov: nedostatok prírodných surovín, zvýšené energetické náklady, zvýšenie stupňa znečistenia škodlivinami, štátné zásahy v riadení prírodných zdrojov.

• **Ekologické faktory** predstavujú najmä produkcii ekologicky škodlivých látok: množstvo znečistenia, vznik nových ochorení, znečistenie základných životných potrieb ako vzduch, pôda a voda, odpadové hospodárstvo.

• **Konkurenčné faktory** predstavujú rôzne firmy a organizácie, s ktorými organizácia súperi o zákazníkov a zdroje a voči ktorým organizácia potrebuje dosiahnuť konkurenčné výhody. Konzistentný konkurenti produkujú rovnaké alebo podobné produkty a služby, nekonzistentnú sú odlišné a pritom si konkurujúce organizácie, voči obom potrebuje organizácia dosahovať konkurenčné výhody.

b) **Kľúčové vplyvy a trendy,** ktoré ovplyvňujú ciele organizácie.

c) **Vzťahy,** vnímanie a hodnoty externých zainteresovaných účastníkov a pod.

Z **bezpečnostného hľadiska** faktory externého bezpečnostného prostredia predstavujú nebezpečenstvá, ktoré môžu mať vplyv na bezpečnosť organizácie (objektu). Tieto faktory sa vyhodnocujú v priebehu analýzy vonkajšieho bezpečnostného prostredia. Medzi ne patria najmä tieto faktory:

1. Geografické a urbanistické faktory okolia organizácie, ktoré môžu mať vplyv na bezpečnosť:
   a) urbanistické vymedzenie územia, v ktorom je organizácia dislokovaná – obec, mestos, sídliisko, hustota osídlenia, typ okolitej zástavby, dopravná vybavenosť a pod.,
   b) geografický opis okolia – okolitý terén, členitosť a morfológia územia, prístupové komunikácie, prírodné prekážky a pod.

2. **Sociálno-ekonomické faktory:**
   a) základné demografické ukazovatele v okolí – počet obyvateľov, pôrodnosť, úmrtnosť, veková štruktúra, prírastok obyvateľstva, výskyt bezdomovcov, počet migrantov a pod.,
   b) sociálna diferenciácia obyvateľstva – do vrstiev a skupín, ktoré sa líšia svojim podielom na majetku a službách, prístupom k moci a výskou svojej prestíže, vplyv na bezpečnosť môžu mať napr.:  
      • rôzne druhy nerovnosti (prijmová, v bohatstve, v spotrebe, statusová, na trhu práce, životných podmienok a pod.),
      • nerovnomerný prístup k vzdelávaniu a úroveň vzdelania,
      • faktory sociálnych nepokojov, konfliktov a kríz a pod.
   c) diferencné ukazovatele, ktoré charakterizujú populáciu podľa príslušnosti k skupine, напр. podľa národnosti alebo náboženstva, napr. výskyt antisemitizmu, rasizmu a xenofóbie (strach z cudzincov), potláčanie náboženských menšín, prejavy náboženskeho radikalizmu, náboženskej neznášanlivosti, narušovania náboženskej slobody, etnických a náboženských konfliktov a pod.,

3. **Politické faktory,** napr. nárast subjektov organizovaného zločinu a ich prepájanie s politickou mocou, migrácne procesy, ktoré môžu vyvoláť nárast miestnych a regionálnych náboženských konfliktov a pod.,

4. **Ekologické faktory,** napr. zmeny v životnom prostredí a klimatické zmeny, zmeny podmienok na zabezpečenie potravinami, energiou, vodou a ďalšími zdrojmi, znečistenie zložiek prírody, nešetrná exploatacia prírodných zdrojov, nešetrné zásahy do ekosystemov krajiny, znečistenie vodných tokov a lesov, nesprávne zaobchádzanie s odpadom a pod.
5. Zdroje mimoriadnych udalostí:

a) zdroje živelných pohrôm: prírodné a hydrologické podmienky v danom prostredí, priehrazy, vodné nádrže, vodné toky, sopky, lavínové terény a pod.,

b) zdroje havárií a katastrof: stabilné i mobilné zdroje priemyselných havárií, sklady nebezpečných látkov, elektrárne, ropovody, plynovody, bane, huty, kalové nádrže a pod.,

c) zdroje terorizmu, nástroja presadzovania tých záujmov (politických a náboženských skupín), ktoré sa nebudú dať presadiť legálnou cestou,

d) zdroje závažného ohrozenia združia: pašovanie drog, pandémie, zdroje radiácie, biologické nebezpečenstvá, zdroje prenosného ochorenia, zdroje chemických látkov ohrozujúcich život, zdravie, životné prostredie a majetok, únik mikroorganizmov alebo toxinov z uzavretých priestorov a pod.

5. Kriminalistické bezpečnostné faktory:

a) kvantitatívne a kvalitatívne ukazovatele kriminality v posudzovanom prostredí a jeho okolí:
  • fenomenológia kriminality – javová stránka kriminality, jej stav, štruktúra, dynamika, intenzita, skupiny a typy páchateľov (pohľadie, vek, sociálny, resp. ekonomický status páchateľov a pod., priestorový výskyt kriminality,
  • etiológia kriminality – súhrn príčin a podmienok podieľajúcich sa na vzniku kriminality,

b) stav na úseku bezpečnosti osôb, majetku a životného prostredia:
  • právne normy, zákony a iné predpisy v oblasti bezpečnosti,
  • dislokácia policajno-bezpečnostných orgánov (policajný zbor, kolná správa, polícia), možnosť ich zapojenia do ochrany objektu (hladkovanie, nepravidelné kontroly, pripojenie na pult centralizovanej ochrany a pod.),
  • možnosti využitia zásahových jednotiek pri ochrane organizácie, predovšetkým vzhľadom na čas zásahu,
  • projekty prevencie kriminality,
  • štatistické ukazovatele objasnenosti kriminálnych delítkov, ktoré prezentujú úspešnosť boja s kriminalitou,
  • právne povedomie občanov, postoj občanov voči kriminalite, názory na stav a zaistenie ich bezpečnosti, miera tolerancie občanov voči jednotlivým druhom kriminality, spolupráca s policajno-bezpečnostnými orgánmi, vplyv samosprávy na stav kriminality.

INTERNÉ SÚVISLOSTI

INTERNÉ SÚVISLOSTI predstavujú interné prostredie, v ktorom organizácia chce dosiahnuť svoje ciele. Z podnikateľského hľadiska môžu faktory interného prostredia predstavovať príležitosti, na druhej strane však môžu pre podnikanie znamenať nebezpečenstvá, ktoré prinášajú straty. Medzi ne patria najmä faktory:

1. Priestor a štruktúra organizácie:
   a) vymedzenie územia (priestoru) organizácie – vonkajšie hranice priestoru organizácie, charakter terénu vo vnútri priestoru, jednotlivé objekty v priestore, vstupy a výhody, vnútorné komunikácie, nakladacie a vykladacie priestory a pod.,
   b) organizačná štruktúra (všetky organizačné útvary organizácie – manažment, finančné oddelenie, nákup, výroba a vývoj, marketing, oddelenie ľudských zdrojov, oddelenie evidencie, odbory a pod., a vztahy medzi nimi),
c) objekty a infraštruktúra organizácie – budovy, výrobné haly, dielne, sklady, garáže, priemyselné elektrické stanice (transformovňa), elektrické rozvodné zariadenia a iné priestory,

d) technické zariadenia budov – kanalizácia, vodovod, plynovod, vykurovanie, zdroje energií, klimatizačné zariadenia, osvetlenie, výtah a pod.

2. Manažment organizácie:
   a) systém riadenia (štruktúra a procesy), úlohy a zodpovednosti,
   b) politiky, zámery (ciele), ktoré sa zaviedli, aby sa splnili úlohy a stratégie, ktorá sa vyúžíva na dosiahnutie cieľov,
   c) procesy prijímania rozhodnutí (oficiálne i neoﬁciálne) a tok informácií.

3. Aktíva a spôsobilosti organizácie:
   a) zdroje (ľudské, kapacitné, materiálové, ﬁnančné, informačné),
   b) hmotné aktíva najmä: technické (technologické) zariadenia (systémy), nebezpečné látky, informačné systémy, informačné a komunikačné technológie,
   c) nehmotné aktíva – znalosti, informácie, patenty, licencie, projekty, know-how, kultúra organizácie,
   d) hlavné činnosti a podporné činnosti (výrobné a nevýrobné procesy),
   e) normy, návody, a modely prijaté organizáciou,
   f) forma a rozsah zmluvných vzťahov, vzťahy s internými zainteresovanými účastníkmi, ich vnímanie a hodnoty – dodávatelia, odberatelia, akcionári, outsourcingové služby, návštevníci a pod.

Z bezpečnostného hl’adiska faktory interného bezpečnostného prostredia predstavujú nebezpečenstvá, ktoré môžu mať vplyv na bezpečnosť organizácie (objektu). Tieto faktory sa vyhodnocujú v priebehu analýzy vnútorného bezpečnostného prostredia. Medzi nie patria najmä tieto faktory:

1. Priestor a štruktúra organizácie:
   a) vymedzenie územia (priestoru) organizácie –, vonkajšie hranice priestoru organizácie, charakter terénu vo vnútri priestoru, vstupy a výjazdy, vnútorné komunikácie, nakladacie a výkladacie priestory, (schéma),
   b) jednotlivé objekty v priestore a infraštruktúra – architektonická klasifikácia a členenie zástavby, použité stavebné materiály, stavebné konštrukcie, technické zariadenia budov.

2. Manažment organizácie:
   a) systém riadenia (štruktúra a procesy) a možnosti jeho narušenia – úroveň vedenia ľudí, úroveň starostlivosti o bezpečnosť a zdravie zamestnancov, medziľudské vzťahy, migrácia pracovníkov, pracovná disciplína a pod.,
   b) procesy prijímania a oznamovania rozhodnutí a možností ich narušenia,
   c) informačné systémy, informačné a komunikačné technológie, tok informácií a možnosti ich narušenia.

3. Inventarizácia dôležitých aktív:
   a) hmotné aktíva – zdroje, technické (technologické) zariadenia a systémy, nebezpečné látky, informačné systémy, informačné a komunikačné technológie,
   b) nehmotné aktíva – informácie, patenty, licencie, projekty, know-how, bezpečnostná kultúra organizácie,
   c) hlavné činnosti, najmä výroba, služby, skladovanie, doprava, výrobky (produkty), služby,
   d) podporné činnosti, najmä personalistika, výskum a vývoj, všeobecná administratíva, ûdržba a servis objektov a technologických zariadení, havarijná služba,
e) **zoznam** významných hmotných a nehmotných aktiv v každom chránenom priestore.

4. **Stav na úseku bezpečnosti osôb, majetku a životného prostredia:**
   a) Interné normatívne akty pre bezpečnosť.
   b) Zdroje, ktoré môžu byť využité pre manažérstvo bezpečnosti a ochranu.
   c) **Stav bezpečnosti a ochrany:**
      - osôb,
      - **objektov** – plášťová a obvodová ochrana, priestorová ochrana, kontrola vstupov, predmetová ochrana, režimová ochrana, fyzická ochrana, požiarnia ochrana,
      - **infraštruktúry** – priemyselná elektrická stanica (transformovňa), elektrické rozvadéľné zariadenia a pod.
      - **technického zariadenia budov** – kanalizácia, vodovod, plynovod, vykurovanie, zdroje energií, klimatizačné zariadenia, osvetlenie, výťah a pod.),
      - pred účinkami priemyselných a iných havárií,
      - utajovaných skutočností (OUS), osobných údajov, komerčných informácií a pod.,
      - životného prostredia v organizácii.


TECHNIKY POSUDZOVANIA RIZÍK

Posudzovanie rizík sa môže vykonávať do rôznej hĺbky, s rôznymi podrobnosťami, s využitím jednej alebo viacerých metód, od jednoduchých až po zložité. Formy posudzovania rizík a jeho výsyp majú byť v súlade s kritériami rizík, ktoré boli vytvorené v rámci určenia súvislostí. Príloha znázorňuje vzťah medzi množstvom kategórií techník posudzovania rizík a faktormi prítomnými v danej rizikovej situácii, a poskytuje názorné príklady toho, ako môžu organizácie zvoliť vhodné metódy pre hodnotenie rizík pre každú konkrétну situáciu.

Všeobecne by vhodné techniky mali mať nasledujúce vlastnosti:
• majú byť oprávnené a vhodné, vzťahom k situáciu alebo uvažovanú organizáciu;
• majú poskytnúť výsledky vo forme, ktorá zvyšuje pochopenie charakteru rizíka a spôsobov, ako môže byť riziko riadené;
• ich použitie má byť sledovateľné a overiteľné.

Pre výber techník by sa mali uviest dôvery zváženok na ich význam a vhodnosť. Pri integrovaní výsledkov z rôzných štúdií sa majú použiť porovnateľné techniky a výsledky.

Faktory výberu techník na posudzovanie rizík

Po rozhodnutí vykonať posúdenie rizík a definovať jeho cieľov a rozsahu, by sa mali zvoliť techniky,ktoré sú založené na týchto faktoroch:
• Ciele štúdie – ciele posudzovania rizík majú priamy vplyv na výber použitých techník, napr. v prípade, že sa vykoná porovnávacia štúdia pre rôzne varianty, môže byť prijateľné použiť menej podrobný model následku pre časti systému, ktoré nie sú ovplyvnené ich odlišnosťami;
• Potreby pracovníkov s rozhodovacími právomocami – na dosiahnutie dobrého rozhodnutia je v niektorých prípadoch potrebná vysoká úroveň podrobnosti, v iných prípadoch postačí všeobecnéjšie chápanie;
• Druhy a rozsah posudzovanych rizík;
• Potenciálna závažnosť následkov – rozhodnutie o tom, do akej hĺbky sa má vykonáť posudzovanie rizík, môže odrážať početnuteľné vnímanie následkov (hoci je možné, že bude nutné ich upraviť, keď sa dokončí predbežné posúdenie);
• Stupeň potrebných expertov, ľudskeho a iných zdrojov – jednoduchá, dobre vykonaná metóda, môže poskytnúť lepšie výsledky ako sofistikovanejšia, zle vykonaný postup, pokiaľ splní ciele a rozsah posudzovania, pričom úsilie vynaložené na posudzovania má byť obvykle v súlade s potenciálnou úrovňou posudzovaných rizík;
• Dostupnosť informácii a dát - niektoré metódy vyžadujú viac informácii a dát než iné;
• Potreba zmeny/ aktualizácie posudzovania rizíka – v budúcnosti môže byť potrebné posudzovanie upraviť/ aktualizovať, pričom niektoré techniky sú v tomto smere výhodnejšie než iné;
• Všetky požiadavky vyplývajúce z predpisov a nariadení a zo zmluvy.

Vol otra prístupu k posudzovaniu rizík ovplyvňujú rôzne faktory, ako je dostupnosť zdrojov, povaha a stupne neistoty dostupných údajov a informácii a zložitosť aplikácie. Tieto faktory sú pre jednotlivé techniky podrobnějšie uvedené v tabuľke A 2 STN EN 31010 Manažment rizík – Techniky posudzovania rizík.
a) Dostupnosť zdrojov – medzi zdroje a schopnosti, ktoré môžu ovplyvniť výber postupov posudzovania rizík patria:
• rozsah odborných skúseností a spôsobilosť tímu manažérstva rizika;
• obmedzenia týkajúce sa času a iných zdrojov v rámci organizácie;
• dostupný rozpočet, ak sú potrebné externé zdroje.

b) Povaha a stupeň neistoty – povaha a stupeň neistoty vyžaduje pochopenie kvality, množstva a integrity dostupných informácií o riziku. To zahŕňa rozsah, v akom sú k dispozícii dostatočné informácie o riziku, jeho zdrojoch a príčinách a jeho následkoch ovplyvňujúcih dosiahnutie cieľov. Neistota môže prameniť z nedostatočnej kvality dát alebo nedostatku základných a spoľahlívých údajov. Pre názornosť, metódy zberu dát sa môžu meniť, môže sa meniť spôsob, akým organizácie používajú tieto metódy, alebo organizácia v obc nemusí mať vhodnú účinnú metódu pre zbieranie dát o identifikovanom riziku.

Neistota môže tiež spočívať vo vonkajších alebo vnútorných súvislostiach (prostredí) organizácie. Dostupné údaje nie vždy poskytujú spoľahlivý základ pre predviedanie budúcnosti. Pre jedinečné typy rizík nemusia byť k dispozícii historické dáta, alebo dostupné údaje môžu byť rôznymi zainteresovanými stranami rôzne interpretované. Pri takomto posudzovaní rizík je potrebné pochopiť typ a charakter neistoty a oceniť následky pre spoľahlivosť výsledkov hodnotenia rizíka. Toto má byť vždy oznámené pracovníkom s rozhodovacou právomocou.


d. Aplikácia posudzovania rizík počas etáp životného cyklu softvéru a hardvéru – pre životný cyklus začínajúci od etapy tvorby počiatočnej štruktúry a stanovenia požiadaviek, cez realizáciu až po finálne dokončenie, ktorý môže zahŕňať oficiálna vyradenie z prevádzky a likvidáciu hardvéru, je nutné zvážiť názorno rôzne aktivity, projekty a produkty. Posudzovanie rizík sa môže aplikovať vo všetkých etápach životného cyklu, a zvyčajne sa aplikuje vo všetkých etápach životného cyklu, a zvyčajne sa aplikuje vo všetkých etápach životného cyklu, a zvyčajne sa aplikuje vo všetkých etápach životného cyklu.
<table>
<thead>
<tr>
<th>Nástroje a techniky</th>
<th>Proces posuzovania rizík</th>
<th>Identifikácia rizík</th>
<th>Analýza rizík</th>
<th>Hodnotenie rizík</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Následok</td>
<td>Pravdepodobnosť</td>
<td>Uroveň rizika</td>
<td></td>
</tr>
<tr>
<td>Brainstorming</td>
<td>VDP</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Štruktúrované alebo semištruktúrové rozhovory</td>
<td>VDP</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Delphi</td>
<td>VDP</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Kontrolné zoznamy</td>
<td>VDP</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Predbezná analýza nebezpečenstva</td>
<td>VDP</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Štúdia nebezpečenstva a prevádzkyschopnosti - HAZOP</td>
<td>VDP</td>
<td>VDP</td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td>Analýza nebezpečenstva a kritické kontrolné body - HACCP</td>
<td>VDP</td>
<td>VDP</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Posuzovanie environmentálnych rizík</td>
<td>VDP</td>
<td>VDP</td>
<td>VDP</td>
<td>VDP</td>
</tr>
<tr>
<td>Štruktúra „Čo keby?“ (SWIFT)</td>
<td>VDP</td>
<td>VDP</td>
<td>VDP</td>
<td>VDP</td>
</tr>
<tr>
<td>Analýza scenárov</td>
<td>VDP</td>
<td>VDP</td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td>Analýza vplyvu na podniky</td>
<td>P</td>
<td>VDP</td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td>Analýza pričína</td>
<td>VDP</td>
<td>VDP</td>
<td>VDP</td>
<td>VDP</td>
</tr>
<tr>
<td>Analýza spôsobov a následkov príčína</td>
<td>VDP</td>
<td>VDP</td>
<td>VDP</td>
<td>VDP</td>
</tr>
<tr>
<td>Analýza stromu porúčat</td>
<td>P</td>
<td>N</td>
<td>VDP</td>
<td>P</td>
</tr>
<tr>
<td>Analýza stromu udalostí</td>
<td>P</td>
<td>VDP</td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td>Analýza vzťahu príčina- následok</td>
<td>VDP</td>
<td>VDP</td>
<td>VDP</td>
<td>P</td>
</tr>
<tr>
<td>Analýza príčin a následkov</td>
<td>VDP</td>
<td>VDP</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Analýza ochranných vrstiev LOPA</td>
<td>P</td>
<td>VDP</td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td>Analýza rozhodovacieho stromu</td>
<td>N</td>
<td>VDP</td>
<td>VDP</td>
<td>P</td>
</tr>
<tr>
<td>Analýza štastistiky a Bayesovského siete</td>
<td>VDP</td>
<td>VDP</td>
<td>VDP</td>
<td>P</td>
</tr>
<tr>
<td>Analýza typu motýlik</td>
<td>N</td>
<td>VDP</td>
<td>P</td>
<td>VDP</td>
</tr>
<tr>
<td>Údržba zameraná na spoľahlivosť</td>
<td>VDP</td>
<td>VDP</td>
<td>VDP</td>
<td>VDP</td>
</tr>
<tr>
<td>Analýza parazitných javov</td>
<td>P</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Markovova analýza</td>
<td>P</td>
<td>VDP</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Simulácia Monte Carlo</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Bayesovská štastistika a Bayesovské siete</td>
<td>N</td>
<td>VDP</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Krivky FN</td>
<td>P</td>
<td>VDP</td>
<td>VDP</td>
<td>P</td>
</tr>
<tr>
<td>Indexy rizika</td>
<td>P</td>
<td>VDP</td>
<td>VDP</td>
<td>P</td>
</tr>
<tr>
<td>Matica následkov a prívedpodobností</td>
<td>VDP</td>
<td>VDP</td>
<td>VDP</td>
<td>P</td>
</tr>
<tr>
<td>Analýza nákladov a prínosov</td>
<td>P</td>
<td>VDP</td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td>Analýza multikriteriálneho rozhodovania MCDA</td>
<td>P</td>
<td>VDP</td>
<td>P</td>
<td>VDP</td>
</tr>
</tbody>
</table>

VDP – veľmi dobre použiteľné, P - použiteľné, N - nepoužiteľné
**Typy techník**

Klasifikácia v tabuľke ukazuje, ako sa techniky vzťahujú na každý krok procesu posudzovania rizík:

- identifikácia rizík,
- analýza rizík – analýza následkov,
- analýza rizika – kvalitatívny, semikvantitatívny alebo kvantitatívny odhad pravdepodobnosti,
- analýza rizík – posúdenie účinnosti prípadných existujúcich prvkov riadenia rizika,
- analýza rizík – odhad úrovne rizika,
- hodnotenie rizík.

Pre každý krok v procese posudzovania rizík je použitie metódy popísané ako veľmi dobre použiteľná (VDP), použiteľná (P) alebo nepoužiteľná (N).

**Faktory ovplyvňujúce výber techník posudzovania rizík**

Ďalšími charakteristickými znakmi uvedených metód sú:

- zložitosť problému a metód potrebných na jeho analýzu,
- povaha a miera neistoty posudzovania rizík na základe množstva dostupných informácií, a na tom, čo je potrebné na splnenie cieľov,
- rozsah potrebných zdrojov z hľadiska času a úrovne odborných znalostí, potrebných dát alebo nákladov,
- či metóda môže poskytnúť kvantitatívny výstup.

Príklady typov dostupných techník hodnotenia rizík sú uvedené v prílohe C.
ZDOKONALOVANIE MANAŽÉRSTVA RIZIKA

Všetky organizácie sa majú snažiť o vhodnú úroveň výkonností svojej štruktúry manažérska rizika v súlade s kritickosťou rozhodnutí, ktoré treba urobiť. Klúčovými výsledkami manažérska rizika sú:
• organizácia má súčasné, správne a obsažné chápanie svojich rizík,
• kritériá rizika pokrývajú riziká organizácie.

Vysokú úroveň výkonnosti v manažérstve rizika predstavuje nasledujúci zoznam vlastností, v ktorom sú uvedené konkrétne ukazovatele výkonnosti pre každú vlastnosť:

VLASTNOSTI ZDOKONALENÉHO MANAŽÉRSTVA RIZIKA

1. Nepretržité zlepšovanie

Dôraz sa kladie na nepretržité zlepšovanie manažérska rizika prostredníctvom určenia cieľov výkonnosti organizácie, merania, preskúmavania a následnej modifikácie procesov, systémov, zdrojov, spôsobilostí a zručností. Možno to vyjadriť vytvorením explicitných cieľov výkonnosti, vzhľadom na ktoré sa meria výkonnosť organizácie a jednotlivých manažérov. Výkonnosť organizácie sa môže publikovať a oznámoť. Zvyčajne sa realizuje aspoň ročné preskúmanie výkonnosti nasledované revíziou procesov a určením revízovaných cieľov výkonnosti pre nasledujúce obdobie. Posúdenie výkonnosti manažérsca rizika predstavuje integralnú časť celkového posúdenia výkonnosti organizácie a meracieho systému pre oddeleňia a jednotlivcov.

2. Plná zodpovednosť za riziko

Zdokonalené manažérsvo rizika zahŕňa podrobnú, plne definovanú a plne akceptovanú zodpovednosť za riziko, jeho kontrolo a za vyhavovanie požiadaviek na riziko.

Určení jednotlivci plne akceptujú zodpovednosť, majú vhodné skúsenosti a primerané zdroje na overovanie kontroly, monitorujú rizíká, zlepšujú kontrolu a efektívne komunikujú o rizikách a ich manažérstve s externými a internými zainteresovanými účastníkmi. To môžu potvrdiť všetci členovia organizácie, ktorí sú plne vedomí rizík, kontrol a požiadaviek, za ktoré zodpovedajú. Obyčajne sa to zaznamenáva v opisoch práce či funkčného postavenia, databázach alebo informačných listoch. Definície úloh v manažérstve rizika, definície zodpovednosti a právomoci majú byť súčasťou školiacich programov organizácie.

Organizácia musí:
• zabezpečiť, že zodpovední pracovníci sú dostatočne vybavení na plnenie svojich úloh,
• zabezpečiť právomoc, čas, prípravu, zdroje a skúsenosti dostatočne na predpokladanú zodpovednosť.

3. Aplikácia manažérska rizika vo všetkých prijímaných rozhodnutiach

Všetky rozhodnutia prijímané v organizácii, bez ohľadu na ich závažnosť a význam, obsahujú do určitého stupňa implicitné úvahy o rizikách a o aplikácii manažérska rizika. Možno to dokumentovať záznamami zo stretnutí a rozhodnuti, ktoré dokazujú, že prebehli otvorené diskusie o rizikách.

Okrem toho má byť možné preukázať, že všetky zložky manažérska rizika sú zabudované do klúčových procesov prijímania rozhodnutí v organizácii, napr. do rozhodnutí o umiestnení kapitálu, do hlavných projektov, a do rekonštrukcií a organizačných zmien.
Z týchto dôvodov sa **rozumne vytvorené manažérstvo rizika v organizácii pokladá za nástroj poskytujúci základ efektívneho riadenia.**

4. **Nepretržitá komunikácia**

Zdokonalené manažérstvo rizika obsahuje plynulú **komunikáciu s externými a internými zainteresovanými účastníkmi,** vrátane obsažného a častého podávania správ o výkonnosti manažérstva rizika ako súčasti dobrého riadenia. Komunikácia sa musí pokladať za **dvojstranný proces,** a to taký, že možno urobiť vhodné zdôvodnené rozhodnutia o úrovni rizík a potrebe sa s nimi zaoberať vzhl'adom na správne určené a výstižné kritériá rizika. Obsažné a časté externé a interné správy o významných rizikách a výsledkoch manažérstva rizika výrazne prispievajú k efektívnomu riadeniu organizácie.

5. **Úplné začlenenie do riadiacej štruktúry organizácie**

Manažérstvo rizika sa pokladá za ohnisko manažérskych procesov organizácie, a to tak, že riziká sa berú do úvahy v zmysle účinku neistoty na ciele. Riadiaca štruktúra a proces vychádzajú z manažérstva rizika. Efektívne manažérstvo rizika manažéri pokladajú za podstatné pri dosahovaní cieľov organizácie.

Prejavuje sa to v jazyku manažérov a v dôležitých písomných materiáloch organizácie, kde sa riziká spájajú s termínom **neistota.** Táto vlastnosť sa zvyčajne premieta do vyhlásení politiky organizácie, najmä do tej časti, ktorá súvisí s manažérstvom rizika. Zvyčajne sa táto vlastnosť overuje pohovormi s manažérfmi a preukázaním ich činnosti a vyhlásení.
prof. Ing. Ľubomír Belan, CSc.

BEZPEČNOSTNÝ MANAŽMENT
BEZPEČNOSŤ A MANAŽÉRSTVO RIZIKA
Vydala Žilinská univerzita v Žiline, Univerzitná 8215/1, 010 26 Žilina
v edičnom rade Vysokoškolské učebnice

Vedecký redaktor: prof. Ing. Miloslav Seidl, PhD.

Zodp. red. Ing. Jana Handriková
Tech. red. Mgr. Jana Pauriková

Vyťlačilo EDIS-vydavateľské centrum ŽU,
Univerzitná HB, 010 26 Žilina v roku 2015 ako svoju 4046 publikáciu.
353 strán, 53 obrázkov, 36 tabuliek, AH 31,09 (Bezpečnosť 17, 93 AH,
Manažérstvo rizika 13,16 AH) VH 31,54
1. vydanie, náklad 200 CD
www.edis.uniza.sk