**TÉZY NA SEMESTRÁLNE SKÚŠKY**

Bezpečnostný manažment a riadenie rizík

AR 2020/2021

1. Definujte **sektor** **bezpečnosti** organizácie a uveďte jeho podsektory, oblasti, zložky a ich prvky.

•rieši ochranu všetkých aktív organizácie,

•zasahuje do všetkých hlavných a podporných činností v organizácií, v ktorých tak vznikajú jednotlivé podsektory bezpečnosti.

Rozsah bezpečnostných činností sa odvíja najmä od veľkosti a zložitosti organizácie, preto oblasti budú rôzne, na ktoré sa zameriavajú.

**Sektor bezpečnosti:**

-súhrn jednotlivých komponentov bezpečnostnej štruktúry organizácie, fungovanie ktorých má byť založené na jej celkovej bezpečnostnej politike.

-špeciálne vytvorené subjekty bezpečnosti,

•hlavným cieľom je dosiahnutie, zaistenie a upevňovanie trvalej celkovej bezpečnosti osôb, majetku a životného prostredia v organizácii

**Podsektory:**

(komplexná bezpečnosť organizácie = súčet úrovní bezpečnosti jednotlivých podsektorov) a.Bezpečnosť osôb a majetku.

b.Bezpečnosť životného prostredia (environmentálna bezpečnosť).

c.Bezpečnosť podnikania (podnikateľská bezpečnosť).

**OBLASTI:**

**1. Bezpečnosť osôb a majetku** je najširším podsektorom sektoru bezpečnosti organizácie. Medzi kľúčové oblasti tohto podsektora:

**1.Fyzická bezpečnosť:**

-osôb - ochrana osôb pred úmyselným fyzickým a nefyzickým napadnutím

-objektov - – ochrana objektov a majetku v nich (iného než sú utajované skutočnosti) pred úmyselným fyzickým napadnutím

-kritickej infraštruktúry - ochrana špecifických objektov kritickej infraštruktúry

**2.Požiarna bezpečnosť**:

a.ochrana pred požiarmi,b.protipožiarna bezpečnosť stavieb

**3.Bezpečnosť práce:**

a.bezpečnosť a ochrana zdravia pri práci,

b.bezpečnosť technických zariadení,

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

**4. Bezpečnosť prevádzky:**

(činností na tvorbu produktov alebo poskytovanie služieb):

-bezpečnosť technických zariadení

- bezpečnosť plynulosti podnikania

- prevencia závažných priemyselných havárií

- jadrová bezpečnosť

**5. Informačná bezpečnosť** - utajované skutočnosti

- Ochrana utajovaných skutočností

- Bezpečnosť informačných systémov

- Bezpečnosť dôležitých informácií

**6. Počítačová bezpečnosť (Bezpečnosť IKT)**

a.fyzická bezpečnosť (bezpečnosť informačného systému a jeho častí),

b.počítačová bezpečnosť (bezpečnosť technického a programového vybavenia), c.komunikačná bezpečnosť,

d.bezpečnosť dát (informačná bezpečnosť alebo technická bezpečnosť informačného systému),

e.režimová bezpečnosť, personálna bezpečnosť

**7.Bezpečnosť a ochrana vnútorného poriadku.**

a.ochrana vnútorného poriadku v zmysle organizačných dokumentov a režimových opatrení, b.manažérstvo bezpečnostných incidentov.

**8.Ďalšie možné oblasti bezpečnosti organizácie.**

V organizácii sa nachádzajú aj oblasti bezpečnosti v podsektore bezpečnosti osôb a majetku, ktoré sa vyskytujú len v určitých špeciálnych organizáciách a objektoch, napr.:

1. Bezpečnosť kritickej infraštruktúry - bezpečnosť objektov v sektoroch kritickej infraštruktúry,

2. Jadrová bezpečnosť

3. Schopnosť zabrániť nedovolenému úniku rádioaktívnych látok alebo ionizujúceho žiarenia

1. Uveďte postupný **vývoj manažmentu**, vysvetlite definíciu **bezpečnostného manažmentu** a **manažérstva bezpečnosti** a popíšte **štyri významy** bezpečnostného manažmentu.

**Vývoj manažmentu:**

Slovo „manage“ pochádza z talianskeho maneggiare zo starolatinského ľudového „manidiare.

Anglicky „management“ od „to manage“ – riadiť, zvládať, byť vo vedúcej funkcii, ...

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

Etapy vývoja manažmentu –

1. Vytvorenie teórie vedeckého riadenia o riadení výroby a organizácií, fungujúcich v podmienkach trhového hospodárstva. (vedecké, administratívne a byrokratické riadenie)

2. Manažment v ekonomických organizáciách, najmä ako podnikový manažment do 2. svetovej vojny: –základy riadenia ľudí v organizácii, prístup zdôrazňujúci medziľudské vzťahy, skúmanie vplyvu pracovných podmienok na pracovníka atď.

3. Moderná teória manažmentu – základy riadenia činností a produkcie a. rozhodovací prístup, b. . matematický (kvantitatívny) prístup, c. systémový prístup, d. empirický prístup (manažment vo všetkých druhoch organizácií, manažment ako umenie a ako súbor poznatkov na riadenie podnikovej činnosti). , e. integrované prístupy

**Bezpečnostný manažment:**

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

V mnohých dokumentoch i inštitúciách sa na vyjadrenie riadiacej činnosti v oblasti bezpečnosti bežne používa pojem „bezpečnostný manažment“.

Pri charakterizovaní bezpečnostného manažmentu sa musí vychádzať zo všeobecnej teórie manažmentu, potom je možné vytvoriť základnú definíciu*: BEZPEČNOSTNÝ MANAŽMENT je špecifický druh manažmentu, zameraný na manažérstvo bezpečnosti referenčných objektov.*

Špecifickosť bezpečnostného manažmentu - nie je zameraný na výrobný transformačný proces, vytvárajúci produkty, ani na proces poskytujúci služby, či iba na riešenie krízových situácií, ale je výlučne zameraný na riadenie špecifickej podpornej činnosti dôležitej pre nerušené dosiahnutie stanovených cieľov.

Zaoberá sa teda riešením problematiky bezpečnosti vo všetkých podsektoroch bezpečnostného sektoru organizácie.

**Manažérstvo bezpečnosti:**

***Manažérstvo bezpečnosti – koordinovaná činnosť manažérov, zameraná na riadenie organizácie s ohľadom na bezpečnosť organizácie***

Je oblasť riadenia, ktorá rieši bezpečnosť aktív (zdrojov) a všetkých činností v organizácii, teda ako bezpečnosť fyzickú, tak bezpečnosť elektronického sveta.

Manažérstvo bezpečnosti sa z veľkej časti týka zabezpečenia autorizovaného prístupu osôb k aktívam organizácie (najmä k financiám, informáciám, hnuteľnému i nehnuteľnému majetku).

**4 významy Bezpečnostného manažmentu:**

1. manažment ako **osobitná skupiny ľudí, manažérov**, ktorí sú primárne zodpovední za to, aby sa manažérstvo bezpečnosti v organizácii správne vykonávalo a splnili ciele bezpečnosti.

2. manažment ako **praktická činnosť, či špecifický druh práce** predstavuje množinu aktivít, ktoré **manažéri vykonávajú alebo musia vykonávať na dosiahnutie cieľov bezpečnosti organizácie,**

3. manažment **ako teória či vedná disciplína o manažérstve bezpečnosti** je naakumulovaný a logicky usporiadaný súbor poznatkov o princípoch, metódach a o postupoch riadenia, ktorým sa možno učiť, vyučovať ich a treba ich aplikovať v procese manažmentu,

4. **umenie manažérov riadiť** bezpečnosť.

1. Charakterizujte bezpečnostný manažment z**informačného, rozhodovacieho a funkčného hľadiska.**

**Informačná charakteristika:**

Celý proces manažérstva bezpečnosti organizácie sa môže v určitom zmysle skúmať ako proces získavania, zhromažďovania, triedenia, spracovávania, vyhodnocovania, uschovávania a prenášania informácií o bezpečnosti smerom hore, ale aj dole. Na tomto základe vzniká a existuje informačný systém organizácie.

Manažéri, bez ohľadu na typ organizácie alebo jej úroveň, zastávajú a vykonávajú okrem interpersonálnych rolí a rozhodovacích rolí aj informačné roly: pozorovateľ, šíriteľ informácií, hovorca.

**Rozhodovací prístup:**

Rozhodovací proces je hlavným článkom riadiaceho procesu, jednou z najdôležitejších aktivít, ktoré vykonávajú manažéri.

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

V každej organizácii sa uskutočňuje veľký počet rozhodovacích procesov v rôznych oblastiach činnosti. Rozhodovacie procesy sa navzájom prekrývajú, časovo na seba nadväzujú a vytvárajú hierarchicky usporiadanú štruktúru.

Do tohto systému rozhodovacích procesov patrí aj rozhodovanie pri riešení otázok bezpečnosti v organizácii.

**Z hľadiska rozhodovania:**

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

Rozhodovací proces sa uplatňuje vo všetkých etapách procesu manažérstva bezpečnosti organizácie.

K základným prvkom rozhodovacieho procesu v manažérstve bezpečnosti patria:

• cieľ rozhodovania, • subjekt rozhodovania, • objekt rozhodovania, • možné alternatívy (možnosti) – najmä na riešenie spôsobov zaobchádzania s rizikom, • kritériá rozhodovania.

**Z funkčného hľadiska:**

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

Manažérska funkcia (funkcia riadenia) je: relatívne oddelená, pomerne samostatná.

Manažérske funkcie majú univerzálny charakter vyskytujú sa v každej organizácii, sú veľmi integrované a platia pre akékoľvek procesy riadenia.

Hlavné manažérske funkcie:

1. **plánovanie -** určuje výsledky, aké chce organizácia dosiahnuť.
2. **organizovanie -** špecifikuje, ako chce organizácia dosiahnuť naplánované výsledky.
3. **personálne zaistenie**- – výber a rozmiestňovanie bezpečnostných pracovníkov.
4. **vedenie ľudí -** vykonávané manažérom ich spája dovedna.
5. **kontrola -** určuje, či tieto výsledky dosiahli.
6. Uveďte a popíšte **manažérstvo bezpečnosti** v súčasných organizáciách a vysvetlite možné zloženie **integrovaného systému manažérstva bezpečnosti** so zameraním na centrálny útvar bezpečnosti.

**Manažérstvo bezpečnosti:** koordinovaná aktivita organizácie zameraná na dosiahnutie cieľov bezpečnosti. Manažérstvo bezpečnosti organizácie je sústavný, opakujúci sa súbor navzájom previazaných aktivít, ktorých cieľom je:

• zaistiť bezpečnosť všetkých činností na dosahovanie cieľov,

• modifikovať schopnosti bezpečnostných rizík spôsobiť poškodenie zdravia, straty životov,atď.

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

**Integrovaný systém manažérstva bezpečnosti:**

Systém je množina prvkov a väzieb medzi nimi, pričom obe množiny určujú vlastnosti celku (systému).

Základné znaky každého systému sú: cieľ, funkcia, štruktúra: množina prvkov ich hierarchia a usporiadanie interné vzťahy medzi nimi, a interakcia s prvkami okolia.

**Štruktúrou riadiaceho systému** vo všeobecnosti sa rozumie skladba jeho prvkov a väzieb a vzájomné pôsobenie medzi nimi.

Podľa zvoleného hľadiska členenia prvkov je možné definovať rozličné štruktúry riadiaceho systému, napríklad personálnu, technickú, útvarovú a pod.

Centralizácia znamená sústreďovanie rozhodovacej právomoci vo vrcholovom stupni riadenia organizácie. Tvorí ho ucelená štruktúra, od vrcholového manažmentu až po výkonný manažment a všetkých zamestnancov.

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

Štátne a súkromné organizácie a inštitúcie majú v súčasnosti vo svojej organizačnej štruktúre začlenené niektoré útvary, zaoberajúce sa určitou oblasťou bezpečnosti, napr. útvary: • krízového riadenia, • bezpečnosti práce a ochrany zdravia, • manažérstva rizika, • manažérstva incidentov, atď.

Tieto bezpečnostné útvary, najmä vo väčších organizáciách: • môžu byť stabilnými prvkami organizačnej štruktúry, • môžu sa vytvárať z vyškolených vlastných zamestnancov, napr. bezpečnostní technici a iní bezpečnostní pracovníci, alebo sa využijú externé organizácie na základe zmluvy.

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

1. Útvar bezpečnosti vo vedení organizácie:

• bezpečnosť a ochrana zdravia pri práci,

• fyzická bezpečnosť a objektová bezpečnosť,

• požiarna ochrana, • ochrana životného prostredia, • havarijná bezpečnosť, • vyšetrovanie incidentov a podvodov.

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

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

d. Úsek informatiky – ochrana IKT, informačná bezpečnosť,

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

Útvar bezpečnosti, podriadený bezpečnostnému manažérovi, by mal mať zverené zložky bezpečnostného sektoru, ktoré prechádzajú celou organizáciou a vyžadujú jednotné vedenie.

1. V PDCA cykle **manažérstva bezpečnosti** uveďte a vysvetlite obsahetapy **Súvislosti organizácie** so zameraním na pochopenie vonkajších a vnútorných súvislostí.

Organizácia potrebuje:

• určiť svoje závažné vnútorné a vonkajšie súvislosti (prostredie), ktoré môžu mať vplyv na to, čo chce dosiahnuť, rovnako aj všetky zúčastnené strany a ich požiadavky.

• zdokumentovať rozsah a rozhranie systému manažérstva – čo je vo vnútri a čo je mimo nich, toto je potrebné na určenie cieľov organizácie.

• vytvoriť a prevádzkovať svoj systém manažérstva.

Určenie súvislostí zahŕňa identifikáciu:

• zámerov organizácie a plánovaných výsledkov,

• vnútorných a vonkajších záležitostí a problémov,

• významných partnerov v podnikaní a ich požiadaviek,

• rozsahu systému manažérstva.

Toto poskytne súhrnný významný vnútorný pohľad na organizáciu. Nemalo by ísť iba o prostý zoznam, ale o úplný zoznam, ktorý poskytne súhrnný významný vnútorný pohľad na organizáciu, ktorý by bol jasný a zrozumiteľný.

Postup pri riešení vonkajších a vnútorných súvislostí organizácie sa má vykonať v súlade s STN ISO 31000:2011 Manažérstvo rizika (prednáška 02).

Vytváranie súvislostí znamená:

• definovanie interných a externých faktorov, ktoré treba zohľadniť v manažérstve bezpečnosti,

• určenie a definovanie základných faktorov prostredia, v rámci ktorých sa bezpečnosť musí riadiť,

• poskytnutie návodu na rozhodovanie v podrobnejších štúdiách manažérstva bezpečnosti.

a)Interné súvislosti predstavujú vnútorné prostredie, v ktorom organizácia chce dosiahnuť svoje zámery, ich pochopenie umožní identifikovať silné a slabé miesta organizácie, jej príležitosti a obavy.

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

Pochopenie súčasného stavu organizácie a jej vnútorných a externých súvislostí má byť zamerané aj na stav jej bezpečnosti.

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

• prieskum medzi zamestnancami – zameriava sa na parametre, ktoré určujú stav bezpečnostnej kultúry.

• analýza politiky bezpečnosti – poskytuje informácie o oficiálnych hodnotách organizácie a požadovaných štandardoch.

• pohovory s manažérmi, zodpovednými za bezpečnosť a pod.

Aktuálny stav bezpečnosti v organizácii je možné zistiť vykonaním predbežnej analýzy stavu bezpečnosti, ktorá neskúma problematiku bezpečnosti v rovnakom rozsahu, ako bezpečnostná analýza vonkajšieho a vnútorného prostredia.

Zameriava sa obvykle len na podstatné záležitosti bezpečnosti a na jej vykonanie stačí skrátený čas.

1. V PDCA cykle **manažérstva bezpečnosti** uveďte a vysvetlite obsah etapy **Vedenie** so zameraním na bezpečnostnú politiku a roly, zodpovednosti a právomoci v organizácii *(personálna zodpovednosť za bezpečnosť, bezpečnostní funkcionári).*

VEDENIE 5.1 Vedenie a záväzok 5.2 Politika bezpečnosti 5.3 Roly, zodpovednosti a právomoci v organizácii.

**Vedenie a záväzok:**

Osoby vo vrcholovom manažmente musia demonštrovať svoju vodcovskú rolu vzhľadom na SMB.

Vrcholový manažment musí mať zodpovednosť a byť zapojený do SMB. Je potrebné začleniť požiadavky SMB do hlavných procesov organizácie, prideliť mu zdroje. Vrcholový manažment je tiež zodpovedný za dôležitosť komunikácie SMB a zvýšenie uvedomenia si potrebnosti tohto systému a zapojenia zamestnancov do riešenia bezpečnosti.

Manažérstvo bezpečnosti – trvalá a neprerušovaná aktivita, ktorá si vyžaduje jasný a trvalý záväzok, **záväzok-** povinnosť, vyplývajúcu zo záväzného sľubu, zmluvy a pod., **mandát-** Aby bol záväzok trvalý, musí byť iniciovaný mandátom zo strany vedenia organizácie, **t.j. mandát** znamená splnomocnenie (poverenie, oprávnenie) funkcionára mať zodpovednosť za riadenie určitej oblasti bezpečnosti v organizácii.

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

• integrácie požiadaviek SMB do podnikateľských procesov organizácie, • dostupnosti zdrojov potrebných pre SMB, • že SMB dosiahne svoje zamýšľané výstupy, atď.

1. ustanovením rolí, zodpovedností a právomocí,
2. komunikovaním o význame manažérstva bezpečnosti a potreby SMB
3. propagovaním trvalého zlepšovania,
4. podporovaním ďalších manažérskych rolí, ...

**Politika bezpečnosti:**

Prijatie záväzku v politike bezpečnosti obsahuje:

a. vyhlásenie manažmentu o podpore politiky bezpečnosti organizácie,

b. stanovenie úloh manažmentu organizácie pri zaisťovaní bezpečnosti a integrity,

c. zabezpečenie zhody bezpečnostných noriem organizácie

d. vytvorenie základného a východiskového dokumentu, ktorým organizácia deklaruje svoj záujem na implementáciu bezpečnosti do všetkých sfér činnosti organizácie – Politika bezpečnosti

e. vytvorenie systémových politík bezpečnosti.

Prijatie zodpovednosti a záväzku vrcholovým manažmentom za dodržiavanie a zavedenie všetkých bezpečnostných noriem v bezpečnostnej politike veľkej i malej organizácie je významným krokom, ktorý vylepší ich hodnotu a povesť, atď. Manažment sa týmto zaväzuje, že bude podporovať zavádzanie SMB. Bezpečnosť je v politike bezpečnosti deklarovaná ako najvyššia priorita organizácie.

**Roly, zodpovednosti a právomoci v organizácii:**

Vrcholový manažment má prideliť zodpovednosti a právomoci pre :

• zaistenie, že SMB zodpovedá požiadavkám týchto medzinárodných noriem,

• podávanie správ o výkonnosti SMB vrcholovému manažmentu.

Obsahom tohto kroku je najmä:

1. určenie zodpovedného vedúceho pracovníka alebo pracovníkov- mať konečnú zodpovednosť za zavedenie a udržiavanie SMB,
2. vytvorenie riadiaceho orgánu bezpečnosti (výbor alebo rada bezpečnosti) za účelom vyhodnocovania výkonnosti bezpečnosti,
3. určenie zodpovednosti všetkých členov manažmentu,
4. zdokumentovanie zodpovednosti a právomoci za bezpečnosť a zoznámenie celej organizácie (musí obsahovať stanovenie úrovní manažmentu s právomocou prijímať rozhodnutia vzťahujúce sa na prijateľnosť bezpečnostného rizika),
5. menovanie kľúčových bezpečnostných pracovníkov, najmä:

• bezpečnostného manažéra ako zodpovednú samostatnú a hlavnú osobu,

• manažéra rizík a tím manažérstva rizika

1. vymedzenie pomeru zodpovednosti za bezpečnosť medzi manažmentom organizácie a vonkajšími spoločnosťami
2. menovaním jednej alebo viac osôb zodpovedných za SMB s primeranou právomocou a kompetenciami pre prijatie zodpovednosti za zavedenie a udržiavanie SMB, (obvykle sa vytvára tím pre implementáciu SMB)
3. V PDCA cykle **manažérstva bezpečnosti** uveďte a vysvetlite obsah etapy **Plánovanie** so zameraním na stanovenie cieľov bezpečnosti a plánovanie ich dosiahnutia v jednotlivých oblastiach bezpečnosti.

**Plánovanie:**

Táto kapitola vyzdvihuje manažérstvo rizika na prvé miesto.

Fázy plánovania musia ukázať, aké, koho, ako a kedy riziká musia byť riešené. Tento proaktívny prístup nahrádza preventívne kroky a neskôr znižuje potrebu nápravných opatrení.

Osobitný dôraz sa kladie na ciele, ktoré by mali byť merateľné, monitorované, oznamované, zladené s politikou systému manažérstva a v prípade potreby aktualizované. Ciele musia byť stanovené pre dôležité funkcie a úrovne.

**Ciele bezpečnosti a plánovanie ich dosiahnutia:**

Organizácia má stanoviť ciele bezpečnosti pre príslušné funkcie a úrovne.

Ciele bezpečnosti majú:

• zhodovať sa s politikou bezpečnosti,

• byť merateľné (ak je to možné,

• brať do úvahy príslušné požiadavky,

• byť monitorované,

• byť zverejnené,

• byť aktualizované podľa potreby,

Organizácia má udržiavať o cieľoch zdokumentované informácie.

Pri plánovaní dosiahnutia cieľov bezpečnosti má organizácia určiť:

• čo sa má urobiť,

• aké zdroje sa požadujú,

• kto bude zodpovedný,

• dokedy to bude dokončené,

• ako sa budú hodnotiť dosiahnuté výsledky.

Dôležitým predpokladom pre aktívnu implementáciu SMB je plánovanie bezpečnosti. V jeho priebehu sa **formulujú ciele, určujú stratégie,** a spracovávajú plány.

Stanovenie cieľov bezpečnosti organizácie je záležitosťou vrcholového manažmentu každej organizácie. Podkladmi pre stanovenie cieľov bezpečnosti sú:

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

**Plánovanie bezpečnosti:**

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

a. stanovujú konkrétne ciele bezpečnosti, spôsoby a kritériá ich vyhodnocovania (indikátory bezpečnosti) a spôsoby kontroly ich dosahovania,

b. určujú bezpečnostné normy,

c. plánuje implementácia SMB – Plán implementácie SMB,

d. plánujú postupy na dosiahnutie cieľov bezpečnosti v podsektoroch bezpečnostného sektoru, najmä:

• BOZP – Plán bezpečnosti a ochrany zdravia pri práci na stavenisku.

• Ochrana objektov - Plán zaobchádzania s rizikami – Bezpečnostný plán ochrany objektu (OUS), Bezpečnostný plán (kritická infraštruktúra), pre iné objekty Bezpečnostný plán ochrany objektu alebo Projekt ochrany objektu,

• Informačná bezpečnosť

• Ochrana osobných údajov – Bezpečnostný projekt (smernica) informačného systému na ochranu osobných údajov,

e. koordinuje plánovanie reakcie na núdzové situácie:

f. plánuje postupy na riešenie incidentov – Plán manažérstva incidentov.

g. stanovuje program environmentálneho manažérstva – Akčný plán (programy) environmentálneho manažérstva

1. V PDCA cykle **manažérstva bezpečnosti** uveďte a vysvetlite obsah etapy **Podpora** so zameraním na zásadykomunikácie a vytvárania, aktualizovania a riadenia zdokumentovaných in formácií.

**PODPORA** 7.1 Zdroje 7.2 Kompetencie 7.3 Uvedomenie si 7.4 Komunikácia 7.5 Zdokumentované informácie

Zameranie organizácie na podporu, potrebnú pre dosiahnutie svojich zámerov a cieľov.

**Zdroje** - organizácia musí určiť a poskytnúť zdroje potrebné pre vytvorenie, zavedenie, udržiavanie a trvalé zlepšovanie SMB.

**Komunikácia:**

Organizácia musí určiť spôsob vnútornej a vonkajšej komunikácie, ktorá sa vzťahuje na SMB a obsahuje: o čom, kedy, s kým, a ako komunikovať.

Organizácia musí ustanoviť, zaviesť a udržiavať postupy:

• vnútornej komunikácie,

• vonkajšej komunikácie

• na prijímanie, dokumentovanie a reagovanie na komunikáciu zainteresovaných účastníkov, • na prevzatie a integrovanie národného alebo regionálneho systému informovania o hrozbách

• na zaistenie dostupnosti prostriedkov komunikácie počas rušivého incidentu,

• na uľahčenie štruktúrovanej komunikácie s príslušnými orgánmi

• na prevádzku a testovanie komunikačných prostriedkov určených na použitie pri narušení normálnych komunikácií

**Zdokumentované informácie:**

V rámci SMB organizácie musia obsahovať: zdokumentované info požadované v tejto norme, a zdokumentované info, ktoré organizácia určí ako nevyhnutné pre efektívnosť SMB.

**Rozsah zdokumentovaných informácií sa môže líšiť,** v závislosti na:

• veľkosti organizácie a druhu jej činností, • zložitosti procesov a ich vzájomnej väzby.

Vytváranie a aktualizovanie –

musí organizácia zaistiť vhodné:

• označenie a popis, • formát, • preskúmanie a schválenie, • oprávnenie osôb.

Rozsah zdokumentovaných bezpečnostných informácií Pri stanovení rozsahu bezpečnostnej dokumentácie musí organizácia vychádzať z platných zákonov a ďalších noriem v ktorých je stanovená. Predstavujú okrem uvedených plánovacích dokumentov ďalšiu dokumentáciu SMB, manažérstva rizika a jednotlivé bezpečnostné smernice, metodiky,...

V tejto etape sa určujú spracovatelia a termíny na spracovanie potrebných dokumentov.

**Riadenie zdokumentovaných informácií:**

Zdokumentované info požadované v SMB a medzin bezp normách musia byť spravované pre zaistenie:

• ich dostupnosti a vhodnosti pre požitie tam, kde je to potrebné,

• primeranej ochrany (napr. proti strate dôvernosti,...)

Na uloženie dokumentácie sa musí vytvoriť samostatné pracovisko.

Pre riadenie zdokumentovanej informácie, má vykonať činnosti:

• distribúcia, prístup, získavanie a používanie; • uloženie a ochrana, vrátane zachovania čitateľnosti; • kontrola zmien, • zadržiavanie a voľné použitie.

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

Príkladmi niektorých bezpečnostných dokumentov, môžu byť:

Plánovacie: Krízový plán ochrany objektu, Krízové plány, a pod.

Technické: Technická dokumentácia objektu.

Prevádzkové : • Prevádzkový poriadok objektu • Protipožiarne smernice, a pod.

Výkazové:

• Denný záznam o priebehu služby, • Záznamy o odovzdaní a prevzatí služby zmeny, • Záznam o bezpečnostných incidentoch a mimoriadnych udalostiach, • Záznam o vykonaných zásahoch

Informačné: Kniha hlásení o incidentoch

Pomocné

1. V PDCA cykle **manažérstva bezpečnosti** uveďte a vysvetlite obsah etapy **Prevádzka** so zameraním na zásady personálneho zaistenia bezpečnosti, outsourcing pri riešení bezpečnosti a manažérstvo zmien.

Oblasť prevádzky zahŕňa oblasti:

1. operatívne plánovanie a riadenie
2. organizovanie bezpečnosti
3. personálne zaistenie bezpečnosti
4. prevádzka SMB
5. opatrenia na riešenie rizík a príležitostí, monitorovanie a preskúmavanie rizík
6. manažérstvo zmien
7. outsourcing

**Personálne zaistenie bezpečnosti:**

• analýza potrieb ľudských zdrojov,

• vytvorenie štruktúry pracovných miest bezpečnostných pracovníkov,

• popis pracovných miest bezpečnostných pracovníkov,

• nábor uchádzačov na potrebné (voľné) pracovné pozície,

• výber a rozmiestňovanie vhodných pracovníkov,

• adaptácia bezpečnostných pracovníkov v novom prostredí,

• motivácia a vytváranie systému kariér bezpečnostných pracovníkov,

• hodnotenie bezpečnostných pracovníkov podľa výsledkov práce a správania,

• vnútroorganizačné bezpečnostné vzdelávanie a výcvik,

• dosiahnutie a zvyšovanie odbornej spôsobilosti bezpečnostných pracovníkov,

• komunikáciu bezpečnostných pracovníkov so zamestnancami o problematike bezpečnosti

Následne prebieha prijímanie záujemcov na funkcie bezpečnostných pracovníkov a jedná sa o etapu personalistiky v ktorej ide o výber na základe kvalifikačných požiadaviek a iných stanovených kritérií. Táto etapa obsahuje výber záujemcov, personálne previerky a poučenie.

Taktiež zahŕňa školenie a výcvik personálu a dosiahnutie spôsobilostí kde sa vykonáva:

• tvorba programov výcviku a školení,

• úvodné, pokračujúce a osobitné školenia bezpečnostných pracovníkov,

• školenia a výcvik všetkých zamestnancov,

• dosiahnutie odbornej pripravenosti bezpečnostných pracovníkov,

• kontroly odbornej spôsobilosti a ďalšie.

Posledným krokom je dosiahnutie pripravenosti na núdzový stav a reakciu:

a. vymenovanie koordinátora pre núdzové plánovanie,

b. zavedenie a precvičovanie havarijných plánov, ak je to vhodné, aj v spolupráci s tretími stranami,

c. vytvorenie záchrannej služby, havarijného tímu, tímu obnovy,

d. pravidelné preskúšavanie prostriedkov výstrahy a varovania.

**Outsourcing: inak zaisťovanie externe-** prijať opatrenia v prípade, že externá organizácia vykonáva časť funkcie alebo procesu organizácie.

Organizácia a) musí posúdiť súvisiace riziká b) musí zabezpečiť, aby externe zaisťované procesy a činnosti boli riadené, c) musí určiť a zdokumentovať, ako sa budú tieto činnosti riadiť a ako budú začlenené do SMB organizácie,

Organizácia musí

• procesy a činnosti, ktoré sa budú zaisťovať externe, • zodpovednosti a právomoci vo vnútri organizácie.

**Manažérstvo zmien:** je riadiaci proces v organizácii, ktorý sa zaoberá vnímaním, komunikáciou, metodikou, organizáciou a vyhodnocovaním prechodu organizácií, skupín v organizácii i jednotlivcov v organizácii zo súčasného stavu do požadovaného budúceho stavu.

Riziká súvisiace s akoukoľvek plánovanou zmenou, musia byť posúdené pred zavedením danej zmeny.

Organizácia musí:

1. riadiť plánované zmeny a preskúmavať nezamýšľané následky zmien,
2. prijímať opatrenia pre zmierňovanie všetkých nepriaznivých výsledkov

V prípade manažérstva zmien v etape prevádzkovania SMB sa jedná o:

• vytvorenie a udržiavanie metodického postupu na identifikovanie a manažérstvo zmien, , ktoré by mohli ovplyvniť dosiahnutie stanovených bezpečnostných cieľov,

• zabezpečenie, aby požadované výkony v oblasti bezpečnosti umožnili zníženie alebo modifikáciu bezpečnostných rizík,

• umožnenie, aby sa zaviedli metódy na zisťovanie zmien systémov alebo činností, ktoré môžu naznačovať, že sa niektorý prvok blíži k bodu, kedy už nebude možné dodržať prijateľné úrovne bezpečnosti.

1. V PDCA cykle **manažérstva bezpečnosti** uveďte a vysvetlite obsah etapy **Hodnotenie výkonnosti** so zameraním na monitorovanie a meranie výkonnosti, zásady interného auditu a preskúmanie manažmentom.

**Hodnotenie výkonnosti:**

**Monitorovanie a meranie výkonnosti:** musí sa vykonávať ako rutinná záležitosť najmä s cieľom zlepšenia tam, kde je potrebné, a poskytnúť istotu manažérom zaistením bezpečnosti činností v ich oblastiach.

**Monitorovanie obsahuje:**

1. stanovenie charakteru, rozsahu a časového plánu, skúšky výkonnosti SMB,
2. vytvorenie a udržiavanie prostriedkov na overenie výkonnosti SMB,
3. preukázanie účinnosti opatrení na zaobchádzanie s bezpečnostnými rizikami,
4. analýza výsledkov merania – hodnotenie SMB,
5. stretnutia s riadiacim orgánom pre bezpečnosť
6. zabezpečenie, aby manažment a zamestnanci dodržiavali politiky, postupy, roly a zodpovednosti.

Organizácia musí v priebehu monitorovania a merania výkonnosti hodnotiť úroveň bezpečnosti a účinnosť SMB.

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

Organizácia vyhodnotí výkonnosť bezpečnosti a efektívnosť SMB.

**Interný audit:**

Organizácia riadi vnútorný audit v plánovaných intervaloch kvôli info o tom

či SMB je v súlade s:

1. s požiadavkami organizácie na svoj SMB
2. požiadavkami medzinárodných noriem

či je efektívne zavedený a udržiavaný.

Organizácia musí:

1. plánovať, vytvoriť, zaviesť a udržiavať program (y) auditov
2. definovať kritériá auditu a rozsah každého auditu,
3. vybrať audítorov a vykonávať audity,
4. zabezpečiť, aby výsledky auditov boli hlásené príslušným vedúcim pracovníkom,
5. uchovávať zdokumentované informácie ako dôkazy o programe/och.

Cieľom interného auditu je overovať stav realizácie Politiky bezpečnosti, stav realizácie Plánu implementácie SMB a výkonnosti SMB, zisťovať platnosť prijatej bezpečnostnej koncepcie, hodnotiť výsledky aplikácie opatrení na zaobchádzanie s rizikom, overovať spoľahlivosť prevádzky technických prostriedkov ochrany, a ďalšie.

Interný audit môže obsahovať:

1. prípravu plánov interných auditov,
2. prípravu postupov pre periodický interný audit na zaistenie bezpečnostných nedostatkov
3. recenzie protokolov, zhromaždených metrických hodnôt z vykonávaných previerok a auditov,
4. posúdenie úspechov pri plnení bezpečnostných cieľov,
5. vykonávanie pravidelného preskúšavania záložných prostriedkov, a ďalšie.

**Preskúmanie manažmentom:**

Predstavuje opakovanú činnosť manažmentu na posúdenie vhodnosti, primeranosti a efektívnosti SMB organizácie. Vykonáva v plánovaných intervaloch, aby sa zabezpečila jeho trvalá vhodnosť, primeranosť a efektívnosť. Odporúčaný interval – jeden rok.

Preskúmanie manažmentom musí zahŕňať úvahy o:

a. stave opatrení z predchádzajúcich preskúmaní vedením,

b. zmenách externých a interných súvislostí,

c. spätnej väzbe na výkonnosť bezpečnosti,

d. spätnej väzbe od zainteresovaných účastníkov,

e. výsledkoch posúdenia rizík a stavu plánu zaobchádzania s rizikami,

f. príležitostiach pre trvalé zlepšovanie.

Preskúmanie sa vyhodnocuje formou Správy z preskúmania manažmentom. Tento súbor musí zahŕňať všetky rozhodujúce oblasti, zdroje, vstupy a výstupy zo všetkých častí, ktoré sú súčasťou prevádzkovaného SMB, politiky a cieľov kvality. Výstupy musia zahŕňať rozhodnutia vzťahujúce sa k trvalému zlepšovaniu a potrebám zmeny v SMB.

Pri výstupoch musia byť prijaté adekvátne opatrenia a potrebné zdroje na odstránenie nezhôd, ale hlavne na zlepšovanie účinnosti a efektívnosti všetkých činností a procesov.

1. V PDCA cykle **manažérstva bezpečnosti** uveďte a vysvetlite obsah etapy **Zlepšovanie** so zameraním na pojmynezhoda a nápravné opatrenie a trvalé zlepšovanie.

Zdroje - organizácia musí určiť a poskytnúť zdroje potrebné pre vytvorenie, zavedenie, udržiavanie a trvalé zlepšovanie SMB.

**Zlepšovanie:**

**Nezhoda a nápravné opatrenia:**

Určené na zlepšenie procesov organizácie prijatých na odstránenie príčin nezhôd alebo iných nežiaducich situácií. Zamerané na systematické vyšetrovanie základných príčin nezhôd.

Pri výskyte nezhody organizácia musí:

1. reagovať na nezhodu a podľa potreby:

• prijať opatrenia na riadenie a nápravu nezhody,

• riešiť následky.

1. vyhodnotiť potrebné opatrenia na odstránenie príčin nezhody, aby sa znova neopakovala alebo nevyskytla na inom mieste, a to:

• preskúmať nezhodu,

• určiť príčiny nezhody,

• určiť, či existujú podobné nezhody, alebo by mohli nastať,

c. vykonať všetky potrebné opatrenia;

d. posudzovať účinnosť prijatých nápravných opatrení,

e. vykonávať zmeny v SMB, pokiaľ je to nutné.

Náprava znamená činnosť na odstránenie zistenej nezhody, za účelom odstránenia príčin nezhôd a zabránenia ich opakovaniu, Nápravná činnosť sa využíva ako nástroj na zlepšovanie.

Nápravné opatrenia sa vykonávajú v reakcii na:

• sťažnosti zákazníkov,

• nežiaduce vnútorné nezhody,

• prípady nezhody zistené počas interného auditu

Aby nápravné a preventívne opatrenia boli účinné, je rozhodujúci systematický prieskum hlavných príčin neúspechu. Nápravné opatrenia musia byť primerané dopadom nezhôd, ktoré sa vyskytli.

Organizácia musí uchovávať informácie o:

• povahe nezhôd a prípadných prijatých následných opatreniach,

• výsledky akéhokoľvek nápravného opatrenia

**Trvalé zlepšovanie:**

Organizácia musí trvale zlepšovať vhodnosť, primeranosť a účinnosť SMB. Zlepšovanie znamená využívanie politiky kvality, cieľov kvality, zistení z auditov, analýzy údajov, nápravných a preventívnych činností, a preskúmaní manažmentom akýmkoľvek spôsobom zlepšovať SMB organizácie.

Zlepšovaniu môžu pomôcť nasledovné činnosti:

• vytvorenie a udržiavanie metodického postupu pre určenie príčin neštandardnej výkonnosti SMB,

• určenie dopadov neštandardnej výkonnosti na prevádzku,

• stanovenie nových strategických cieľov pre bezpečnosť,

• optimalizácia SMB.

1. Definujte **aktíva***(normy, definícia, hodnota,**životnosť, životný cyklus, spôsoby zoskupovania, typy podľa ISO 55000)* apopíšte spôsoby ochrany aktív.

Aktívum je položka, vec alebo entita, ,ktorá má potenciálnu alebo skutočnú hodnotu pre organizáciu. Pre organizáciu ekonomické prostriedky, ktoré sú výsledkom minulých udalostí a od ktorých sa očakáva, že v budúcnosti povedú k zvýšeniu ekonomických prínosov, predstavujú príležitosti, pri ktorých dosahuje zisk.

Hodnota aktíva môže byť hmotná, nehmotná, finančná, nefinančná a zahŕňa úvahy o rizikách a zodpovednostiach.

Hodnota aktíva má pre organizáciu viacero významov:

• schopnosť poskytovať úžitok,

• niečo cenné, napr. majetok

• cena (obyčajne v peniazoch)

• význam, dôležitosť, napr. umelecká, vedecká,

ŽIVOTNOSŤ A ŽIVOTNÝ CYKLUS AKTÍVA:

Zainteresovaný účastník (stakeholder) je osoba alebo organizácie, ktorá môže mať vplyv na určité rozhodnutie alebo činnosť.

Životnosť aktíva (asset life) je obdobie od vzniku aktíva do konca jeho životnosti. V rôznych etapách životnosti aktíva môže byť jeho hodnota kladná alebo záporná.

Životný cyklus (life cycle) predstavuje etapy zahrnuté v manažérstve aktíva. Názvy a počet etáp a činnosti v jednotlivých etapách sa obvykle v rôznych pracovných odvetviach líšia a určuje ich organizácia.

ZOSKUPOVANIE AKTÍV:

Organizácia sa môže podľa svojich potrieb rozhodnúť, že bude svoje aktíva riadiť skôr ako skupinu než jednotlivo.

Takéto zoskupenia môžu byť tvorené podľa typov aktív, systémov aktív alebo portfólií aktív. Systém aktív (asset system) – súbor vzájomne pôsobiacich alebo vzájomne súvisiacich aktív –

• zoskupenie aktív označované ako systém aktív,

Portfólio aktív (asset portfolio) – aktíva, ktoré sú v rámci systému manažérstva aktív:

-sa obvykle vytvára a určuje pre manažérske kontrolné účely,

• portfóliá pre fyzický hardvér môže byť vymedzené kategóriou

• portfóliá pre softvér môžu byť vymedzené vydavateľmi softvéru alebo platformou

Systém manažérstva aktív môže zahŕňať viac portfólií aktív:

• v prípade používania viacerých portfólií aktív a viacerých systémov manažérstva aktív by mali byť aktivity v rámci manažérstva aktív koordinované medzi portfóliami a systémami.

1. Definujte **incident** a **bezpečnostný incident,** popíšte ich druhy, uveďte postupnosť a vysvetlite **životný cyklus** reakcie na bezpečnostný incident.

INCIDENT:

Udalosť (incident) je teda ľubovoľná zmena v čase na danom objekte Udalosť je pozorovaná zmena normálneho správania sa systému, životného prostredia, procesu, priebehu práce alebo osoby (zložky).

Existujú tri základné typy udalostí:

1. Normálna udalosť - nemá vplyv na rozhodujúce zložky alebo požiadavky na zmenu riadiacich prvkov
2. Vystupňovanie - narastanie udalosti ovplyvňuje rozhodujúce systémy produkcie alebo vyžaduje, vydanie rozhodnutia, ktoré musí následne zmeniť riadiaci proces
3. Stav núdze (emergency)- udalosť, ktorá môže:

ovplyvniť zdravie alebo bezpečnosť ľudí,

narušiť základné prvky riadenia rozhodujúcich systémov,

významne ovplyvniť výkon súčastí alebo vplývať na súčasti systémov,

byť považovaná za stav núdze vyplývajúci z bezpečnostnej politiky alebo z vyhlásenia koordinátora incidentu.

BEZPEČNOSTNÝ INCIDENT:

proces, ktorý sa pripravuje, vzniká, má svoj priebeh a zaniká a ktorý má za následok zhoršenie bezpečnostnej situácie.

Bezpečnostný incident:

• nejaká neštandardná, alebo nepríjemná bezpečnostná udalosť, ktorá vedie k narušeniu pravidiel bezpečnosti v organizácii,

• vzniká ako následok zlyhania bezpečnostných opatrení, alebo porušenia bezpečnostnej politiky,

• je to udalosť, ktorá môže viesť k strate alebo narušeniu činností organizácie, služby alebo jej určitej funkcie.

Podľa ISO 22301:2012 Spoločenská bezpečnosť:

incident je situácia, ktorá spôsobuje alebo môže spôsobiť:

• prerušenie činností, • škodu, • krízovú situáciu, • alebo krízu.

Termín incident zahŕňa pojmy:

• nehoda (Accident), • incident(Incident), • skoronehoda (Near Miss), • nebezpečná udalosť (DangerousOccurrence).

Následkom niektorej nebezpečnej udalosti môže byť aj:

• porucha, • prerušenie činnosti.

Udalosťami s vyšším stupňom nebezpečenstva sú:

• mimoriadne udalosti, • krízové situácie, • kríza

KLASIFIKÁCIA INCIDENTOV:

Každý incident sa vyznačuje svojimi prvkami, ktoré ho determinujú a špecifikujú, napr. krádež, je špecifikovaná spôsobom spáchania, miestom, osobou ale aj motívom.

Špecifikácia o aký druh incidentu ide, ovplyvňuje vznik konkrétneho druhu a zabezpečenie špecifických činností bezpečnostných orgánov.

Medzi najvýznamnejšie určujúce kritériá patrí:

právne posúdenie danej udalosti - škodová udalosť, priestupok,

zavinenie danej udalosti – úmyselné zavinenie, zavinenie z nedbanlivosti,

spôsobenie následku (ujmy) – škoda, ublíženie na zdraví,

KATEGÓRIE INCIDENTOV (MOŽNÉ ÚROVNE):

Uvádzajú sa rôzne kritéria na stanovenie závažnosti incidentov, napr.:

• jednotlivé stupne závažnosti: nízka, stredná, vysoká, kritická,

• podľa množstva postihnutých užívateľov: jeden alebo niekoľko málo užívateľov,

• podľa úrovne, ktorá sa bude incidentom zaoberať: referent, nižší manažment,

• podľa toho, kto musí byť s incidentom zoznámený: jeden alebo niekoľko málo zamestnancov spoločnosti,

• podľa úrovne odbornosti: prvá úroveň podpory,

DRUHY BEZPEČNOSTNÝCH INCIDENTOV:

Medzi incidenty v organizácii možno zaradiť:

1. Incident BOZP,

2. Personálny bezpečnostný incident

3. Bezpečnostný incident fyzickej povahy (majetkový bezpečnostný incident)

4. Poriadkový incident, 5. Environmentálny incident (environmental incident),

6. Informačný bezpečnostný incident (information security incident),

7. Bezpečnostný incident v prevádzke, 8. Incidenty spôsobené prírodnou katastrofou

MANAŽÉRSTVO INCIDENTU:

charakterizujúci činnosti organizácie pri:

• predchádzaní incidentu,

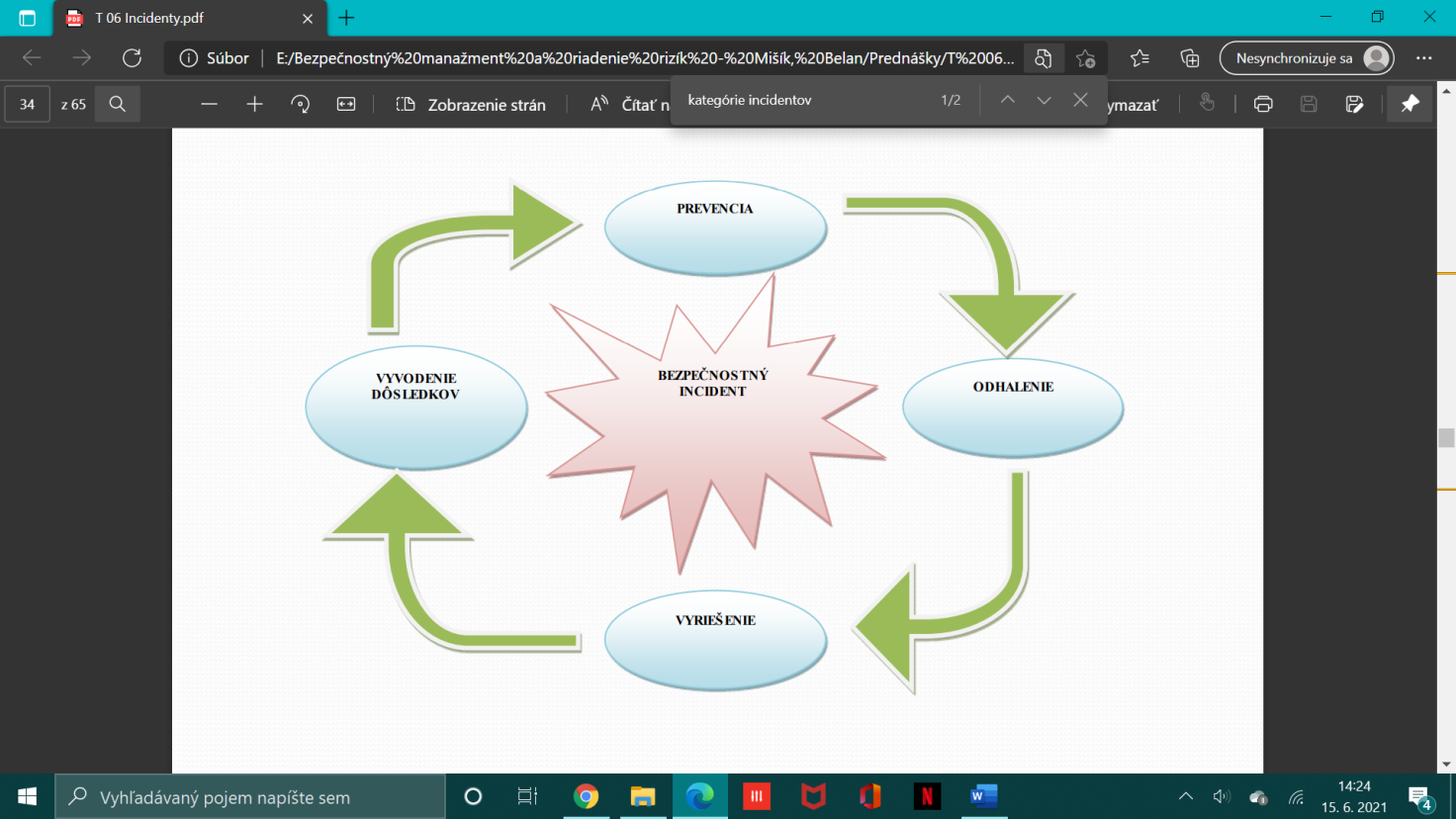
• identifikovaní incidentu,

• analýze a regulovaní nebezpečenstva,

• vyvodení dôsledkov pre budúcu činnosť.

Cieľom manažérstva incidentu je čo najskôr obnoviť činnosť organizácie.

ŽIVOTNÝ CYKLUS BEZPEČNOSTNÉHO INCIDENTU:



1. Prevencia – príprava na incident
2. ODHALENIE INCIDENTU
   1. Zistenie a registrácia incidentu

a. identifikácia incidentu:

• zistenie,

• hlásenie o vzniku nehody určenej osobe v rámci organizácie (prvý stupeň),

• poskytnutie prvej pomoci a lekárskej starostlivosti pre poškodené osoby a zabránenie ďalšiemu zraneniu alebo škode,

b. registrácia – záznam zistenej alebo hlásenej udalosti v systéme,

2.2 Klasifikácia a prvotná podpora

a. kategorizácia - udalosti sú rozdelené do kategórií,

b. stanovenie priority incidentu podľa dôležitosti pre lepšie využitie zdrojov a času podporného personálu,

3. RIEŠENIE INCIDENTU Keď je incident kategorizovaný a zaradený podľa priority, môže sa vyriešiť. Riešenie incidentu zahŕňa 5 stupňov:

3.1 Počiatočná diagnostika - odhalí všetky príznaky incidentu, uskutočňuje sa, keď používateľ popíše problém a dá odpoveď na problémové otázky.

3.2 Eskalácia (stupňovanie) incidentu na druhý stupeň podpory, ak je to potrebné - keď incident vyžaduje širšiu podporu, napr. vyslanie technika, či pomoc od kvalifikované špecialistu.

3.3 Vyšetrovanie a diagnostika - tieto procesy sa vykonávajú v priebehu riešenia problému, kedy je potvrdená počiatočná hypotéza o incidente, ak nie je nájdené žiadne riešenie z minulosti, incident sa preskúma a nájde príčina.

3.4 Vyriešenie a obnova –

a. vypracovanie plánu pre prijatie nápravných opatrení,

b. vykonávanie plánu,

c. obnova poškodeného systému,

d. vyhodnotenie účinnosti nápravných opatrení,

e. správa o vyšetrovaní incidentu.

3.5. Uzavretie incidentu-

a. výpočet vzniknutej škody,

b. uvedenie koncového stavu incidentu do záznamu o incidente.

4 VYVODENIE NÁSLEDKOV

a. starostlivosť o tých, ktorí sú ovplyvnení incidentom,

b. monitorovanie, sledovanie a komunikácia: sledovanie výsledku vyriešenia incidentu,

c. aktualizácia Plánov reakcie na incident a dodatočné zabezpečenie systému,

d. vykonanie zmien pre neustále zlepšovanie,

e. poučenie do budúcnosti.

PREVENCIA - PRÍPRAVA NA INCIDENT

Bezpečnostný manažér, vedúci manažér incidentu (koordinátor incidentov) a tímy na manažérstvo incidentu:

• vypracujú postupy na riešenie incidentov v Pláne manažérstva incidentu

• spracujú Metodiky (smernice) na vyšetrovanie bezpečnostných incidentov,

• uskutočňujú vzdelávanie zamestnancov

Pre úspešné zvládnutie riešenia bezpečnostných incidentov treba:

• mať definované postupy,

• mať vypracované postupy pre riešenie najpravdepodobnejších bezpečnostných incidentov,

-aktualizovať vypracované preventívne programy a pracovné postupy, v prípade objavenia sa nových bezpečnostných rizík,

• v prípade vzniku závažných havárií mať vypracované havarijné plány a mať pripravené zásahové jednotky.

1. Definujte **riziko a bezpečnostné riziko,** uveďte a popíšte zdroje rizika, možné udalosti, úrovne rizika, pravdepodobnosť a následok, uveďte riziká, ktorým je vystavená organizácia a jej činnosti**.**

**Riziko** je pojem, ktorý označuje neistý výsledok s možným nežiaducim stavom. Znamená hrozbu, potenciálny problém.

✓Riziko teda vyjadruje určitú mieru neistoty

✓Riziko predstavuje neurčitosť,

✓Riziko chápeme aj ako pravdepodobnosť akéhokoľvek výsledku,

✓Riziko je kombinácia pravdepodobnosti a škody.

RIZIKO – ÚČINOK NEISTOTY ZÁMEROV

• STN ISO 31000:2019 – Pojem riziko je potrebné chápať nielen ako hrozbu (možné straty), aj ako príležitosti (možné zisky).

**Bezpečnostné riziká:**

• teritoriálneho rozsahu, • sektora (zdroja): vojenské, politické, ..., • subjektov, ktoré sú ich nositeľmi: určité štáty, politické a iné subjekty neštátneho charakteru, • charakteru ich pôsobenia: bezprostredné, sprostredkované, • času trvania: krátkodobé, strednodobé,...

**Zdroj rizika:**

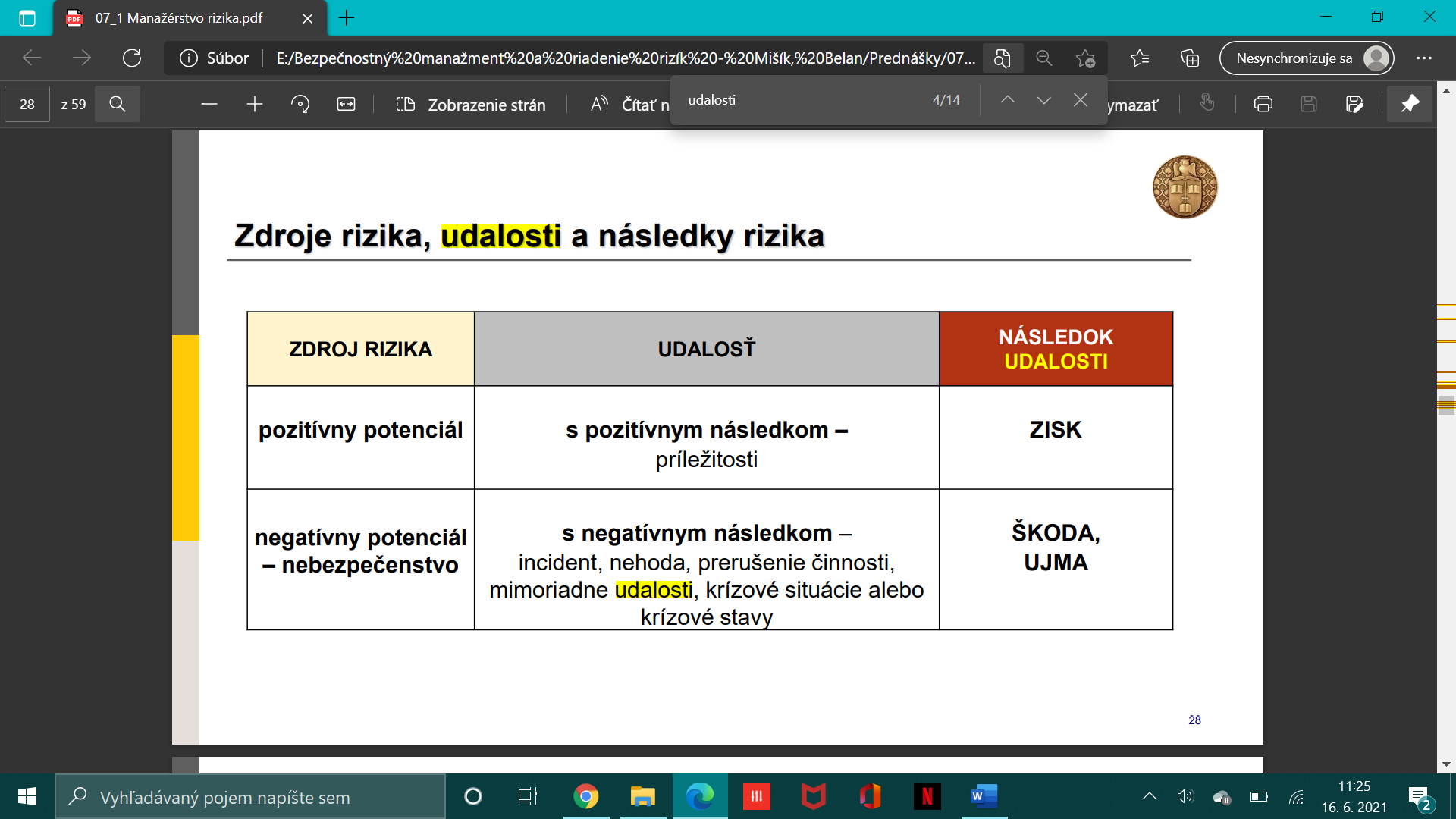
▪ Vnútorné vlastnosti niečoho, majúce za následok náchylnosť stať sa zdrojom rizika, predstavujú zraniteľnosť.

▪ Zdroj rizika, je prvok, ktorý má vnútorný potenciál vyvolať riziko.

▪ Zdroj rizika môže obsahovať potenciál na spôsobenie:

▪ udalosti s pozitívnym následkom, ▪ udalosti s negatívnym následkom, ▪ aj udalosti s pozitívnym následkom, aj udalosti s negatívnym následkom súčasne.

**Udalosti:**

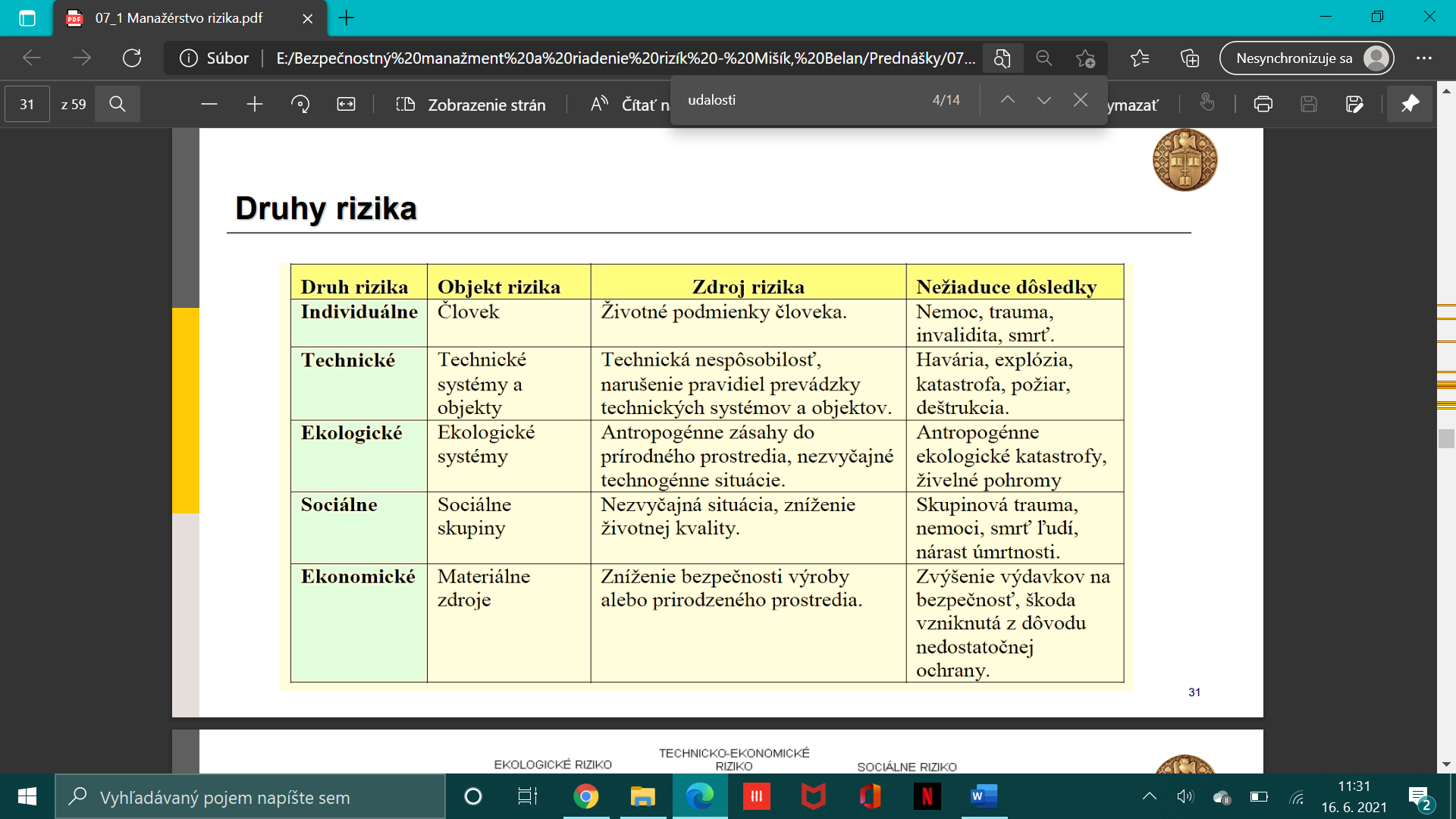


**Úrovne rizika:**

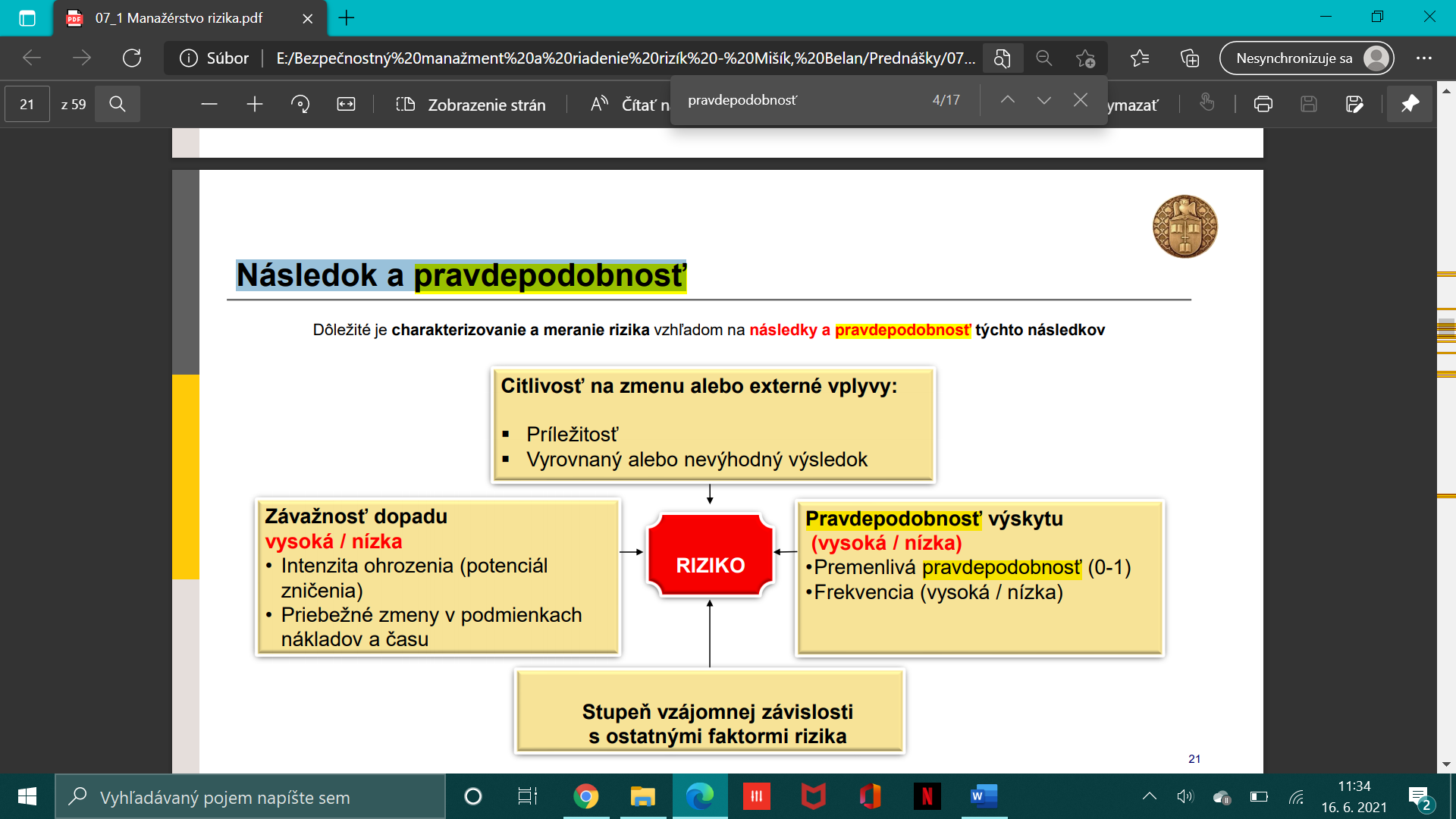
Úroveň rizika sa obvykle zaraďuje do troch pásiem (oblastí):

1. oblasť neprijateľnosti – neprijateľné riziko
2. oblasť prípustnosti – prípustné nežiaduce riziko a prípustné znesiteľné riziko
3. široko prijateľná oblasť – bezvýznamné riziko ktoré treba iba monitorovať





**Následok a pravdepodobnosť:**



**Pravdepodobnosť –** šanca že sa niečo stane.

Pravdepodobnosť môže byť definovaná, určená alebo meraná:

1. kvalitatívne s využitím všeobecných výrazov (slovne napr. malá, stredná, veľká),
2. 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.

**Riziká, ktorým je vystavená organizácia a jej činnosti:!!!**

1. Mimoriadne udalosti -
2. Uveďte a popíšte **riziká úmyselného napadnutia** a **náhodné bezpečnostné riziká**.
3. **úmyselné napadnutie – ktoré sa zaraďuje medzi vonkajšie riziká bezpečnosti priestorov, organizácie, f**yzická bezpečnosť osôb môže byť narušená rôznymi personálnymi bezpečnostnými incidentmi, ktoré znamenajú fyzické narušenie osobnej bezpečnosti, napr. napadnutie; lúpež; ublíženie na zdraví; usmrtenie; útok na verejného činiteľa; útok na orgán verejnej moci;
4. **náhodné bezpečnostné riziká -** predstavujú akékoľvek biologické, chemické, mechanické, environmentálne, ergonomické, fyzikálne, psychologické alebo sociálne faktory, môžu spôsobiť nebezpečenstvo pre:
5. ľudí a iné organizmy,
6. majetok,
7. životné prostredie.

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

• súvisiace s bezpečnosťou zdravia pri práci (BOZP),

• personálnej bezpečnosti ,

• bezpečnosti životného prostredia ,

• požiaru a iných havárií ,

• prírodných javov (živelných pohrôm) ,

• bezpečnosti priestorov.

1. Podľa normy STN ISO 31000:2011 uveďte obsah architektúry a štruktúry manažérstva rizika, popíšte zásady **vytvárania súvislostí** s dôrazom na vonkajšie a vnútorné súvislosti (zoznam aktív) a postup pri definovaní kritérií rizika.

Proces manažérstva rizika sa realizuje na základe plánu manažérstva rizika ako súčasť jej praktík a procesov na :

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

Manažérstvo rizika je rýchlo sa rozvíjajúci odbor a existuje veľa rôznych pohľadov a prístupov, ako a prečo riziká riadiť.

**STN ISO 31000:2011** Manažérstvo rizika. Zásady a návod. Účelom normy je poskytnúť zásady a usmernenia pre manažérstvo rizika ako všeobecne uznávaný vzor pre odborníkov a firmy.

Norma odporúča, aby organizácie vypracovali, zaviedli a nepretržite zlepšovali svoju štruktúru, ktorej účelom je integrovať proces manažérstva rizika do celkového riadenia organizácie, jej stratégie a plánovania, politiky, hodnôt,...

Norma nie je špecifická pre nejaký druh alebo pre nejaké odvetvie.

Normu možno použiť na široký rozsah činností vrátane stratégie a rozhodnutí, prevádzky, procesov, funkcií, projektov, produktov, služieb a majetku. Je možné ju aplikovať na akýkoľvek druh rizika a akéhokoľvek charakteru.

Podľa normy STN ISO 31000:2011 sa pojem manažérstvo rizika odkazuje na architektúru efektívneho manažérstva rizika(architecture).

Táto **architektúra**, uvedená na obr. 6 zahŕňa:

• zásady manažérstva rizika, • štruktúru manažérstva rizika (framework), • proces manažérstva rizika.

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

1. vytvárať a ochraňovať hodnotu,
2. byť integrálnou súčasťou všetkých procesov
3. byť súčasťou prijímania rozhodnutí
4. byť systematické, štruktúrované a včasné
5. zakladať sa na najlepších dostupných informáciách
6. prispôsobovať sa na mieru
7. zohľadňovať ľudské a kultúrne faktory
8. byť transparentné a zahrňujúce
9. byť dynamické, opakujúce sa a citlivé na zmeny
10. uľahčovať trvalé zlepšovanie organizácie

**ŠTRUKTÚRA MANAŽÉRSTVA RIZIKA:**

Predstavuje množinu zložiek, ktoré vytvárajú základy a organizačné usporiadanie pre navrhovanie, zavedenie monitorovania, preskúmavanie a trvalé zlepšovanie manažérstva rizika.

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.

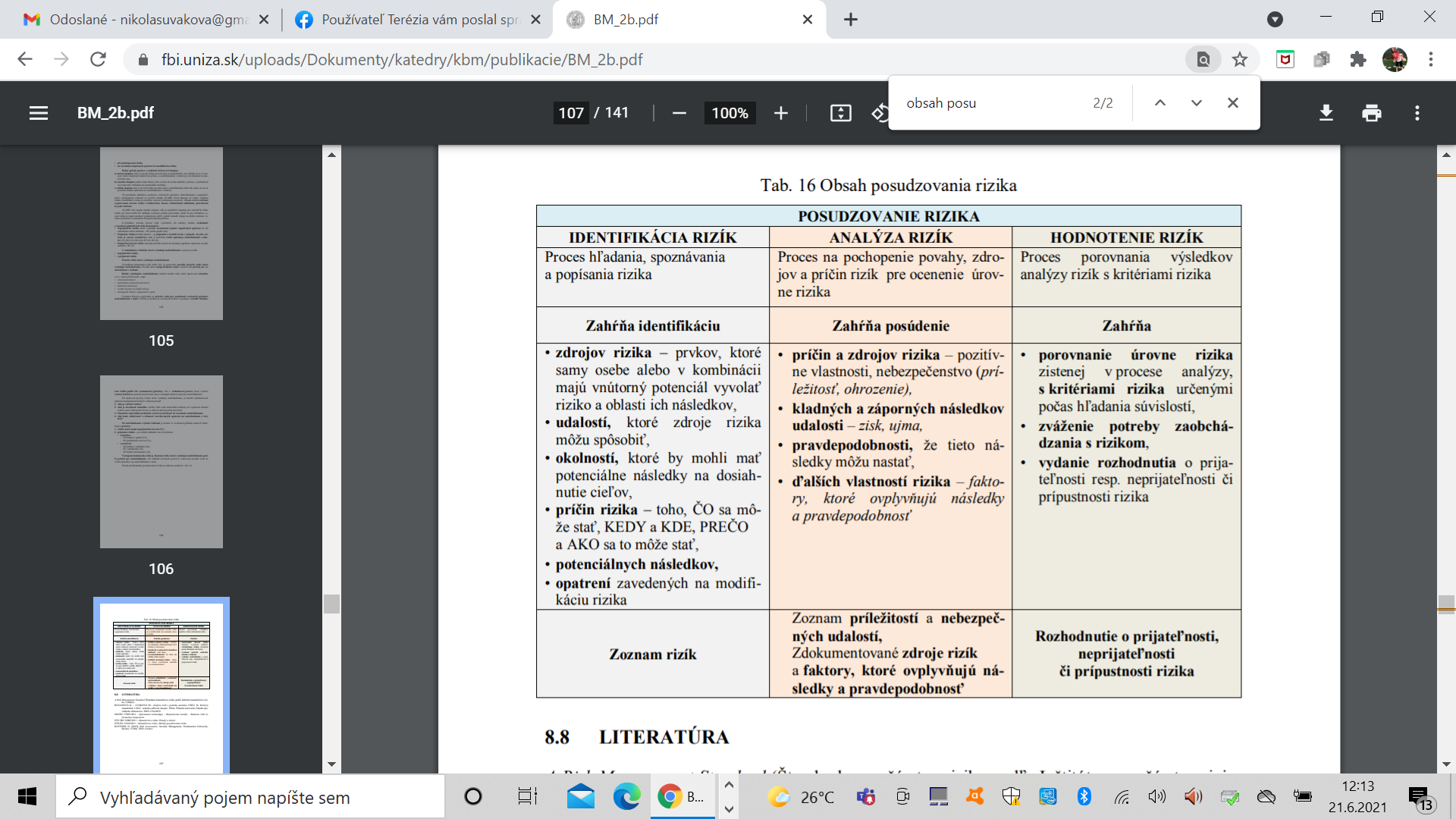
Štruktúra manažérstva rizika:

• 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.

1. Uveďte obsah **posudzovania rizika**,popíšte zásady identifikácie rizika, analýzy rizika, a hodnotenia rizika, uveďte metódy identifikácie rizika, metódy analýzy rizika a popíšte  rozhodnutia o rizikách, ktoré vyžadujú zaobchádzanie.



Identifikácia rizika

Identifikácia rizika znamená proces hľadania, spoznávania a popísania rizika.

Identifikácia rizika zahŕňa identifikáciu:

• zdrojov rizika – prvkov, ktoré samy osebe alebo v kombinácii majú vnútorný potenciál vyvolať riziko a oblasti 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.

Cieľom identifikácie rizík je vytvoriť obsažný zoznam rizík, založený na udalostiach, ktoré by mohli vytvoriť, podporiť, zabrániť, znehodnotiť, urýchliť, alebo pozdržať dosiahnutie zámerov.

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. Hneď, 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 riziká, ktoré nie sú identifikované v tejto etape sa nezahrnú do ďalšej analýzy.

Následne tieto riziká nemôžu byť a ani nebudú 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 udalosti 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. prísne tajný písomný dokument uložený v chránenom priestore môže byť odcudzený, odfotografovaný alebo inak rozmnožený alebo zničený páchateľom (násilné napadnutie), spálený ohňom, prípadne znehodnotený hlodavcami či nadmernou vlhkosťou a pod.

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 .

Do úvahy sa má brať aj široký rozsah následkov, i keď zdroj rizika alebo jeho príčina nie sú zrejmé. 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 viať všetky významné príčiny a následky. Pochopenie a vyhodnotenie príčin rizík sú životne dôležité informácie pre zaobchádzanie s rizikami.

Nedostatky, ktoré sa vyskytnú v systematickom procese identifikácie rizík môžu viesť organizácie k sústredeniu pozornosti len na známe riziká, a preto sa zabudne na tie, ktoré sú zatiaľ neznáme a ktoré potom nemôžu nikdy byť riešené zodpovedajúcim spôsobom.

Metódy (techniky) identifikácie rizika

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

1. Deduktívne metódy (metódy ex post) – metódy založené na dôkaze – sú založené na analýze už predtým vzniknutých udalostí, hľadaní a objasnení ich príčin a súvislostí medzi nimi.

Uvažuje sa poslednej udalosti a vyhľadávajú sa okolnosti, ktoré ju mohli zapríčiniť. Pomocou nich možno zostaviť scenáre vzniku a prejavov rôznych rizík, sú zdrojom inovácie procesov bezpečnostného manažmentu, patria sem napr. kontrolné zoznamy, preskúmanie 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 predvídať 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 tieto 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 zámery organizácie, pomáhajú vyhodnotiť pravdepodobnosť vzniku udalostí a ich následky, 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 scenára, analýza spôsobov a následkov porúch, analýza príčin a následkov, analýza bezporuchovej činnosti človeka, údržba zameraná na bezporuchovosť, matica následkov a pravdepodobnosti.

Okrem nich sa môžu použiť aj: analýza dopadov na podnikanie, analýza stromu poruchových stavov, analýza stromu udalostí, analýza vzťahu príčina – následok, analýza ochranných vrstiev LOPA, analýza parazitných javov, Markovova analýza, krivky FN, indexy rizika, analýza nákladov a prínosov, analýza multikriteriálneho rozhodovania MCDA.

Pravdepodobnostné modely pracujú s rizikom ako s rýdzo pravdepodobnostnou veličinou. Tento prístup je založený na tom, že sa daný jav vyskytuje s určitou pravdepodobnosťou, ktorú je možné určiť na základe určitých štatistických veličín (napr. počet výskytov danej skupiny javov, dĺžky sledovaného obdobia a pod.). Pretože sledovaných 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 chýbajú 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 premenlivé.

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) príčinách 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 zníženie úrovne rizika.

Otázky, na ktoré je treba zamerať pozornosť sú:

• Aké sú zavedené opatrenia na zníženie úrovne rizika?

• Sú tieto opatrenia schopné primerane modifikovať riziko na prípustnú úroveň?

• Používajú sa tieto opatrenia v praxi zamýšľaným spôsobom a môžu byť na požiadanie preukázané 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 vyjadriť a zaznamenať mieru efektívnosti 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, viditeľne 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 zníženie hodnoty aktív v jednom chránenom priestore, uloženie aktív v úschovných objektoch, havarijné plánovanie, príprava 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 zvážiť 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.

Metódy analýzy rizika

Analýza rizika sa môže realizovať s rozličnou úrovňou podrobností 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.

Kvalitatívne metódy analýzy rizika Kvalitatívne metódy využívajú expertné odhady, ktoré využívajú priame, formalizovaným výpočtom spravidla priamo nepodložené vyjadrenie výskytu rizikovej udalosti, stanovenie jeho veľkosti alebo významnosti.

Expertné odhady sa využívajú najmä v prípadoch, ak chýbajú alebo sú ťažko vyjadriteľné číselné 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:

• veľkosti 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, 98 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 kvalitatívnej závažnosti týchto veličín (parametrov rizika) a odhade rizika ako veličiny z týchto parametrov odvodených. Podľa STN EN 31010 sa z kvalitatívnych metód na analýzu rizika používajú najmä expertné techniky: matica následkov a pravdepodobnosti a štruktúra „čo sa stane, ak?“.

Spôsob vyjadrenia o veľkosti rizika môže byť:

• slovnou deskripciou (malé, stredné, veľké),

• abstraktnou číselnou hodnotou (tzv. ordinálnou poradovou stupnicou 0 – X),

• percentuálne (tzv. kardinálnou 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. malá, stredná, veľká úroveň.

Medzi číselnými hodnotami a slovným popisom existuje vzájomná korešpondencia, 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 vzťahu ku kvalitatívnym 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 spresňovať aj kvantitatívnou analýzou.

Kvalitatívna analýza sa používa najmä:

• ako úvodný prehľad vedúci k identifikácii rizík, ktoré vyžadujú podrobnejšie 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 mnohoodborové skupiny respondentov, hodnotení špecialistov a expertov, štruktúrovaných interview a dotazníkoch.

Kvalitatívne induktívne expertné metódy je výhodné využívať 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 veľmi obťažné,

• kvalitatívne metódy nevyžadujú množstvo štatistických údajov, ale využívajú logické väzby medzi faktormi ovplyvňujúcimi vznik rizika,

• kvalitatívne metódy poskytujú jasnú a zrozumiteľnú deskripciu rizík a ich parametrov.

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 riziko akceptovať alebo ho modifikovať niektorým zo spôsobov zaobchádzania s rizikom.

Rozhodnutia majú brať do úvahy širší rámec rizika a musia zahŕňať úvahy o tolerancii rizika pre iných účastníkov, ako je organizácia, ktorá má z rizika osoh. 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,

• zachovať jestvujúce opatrenia na jeho kontrolu a nezaoberať sa rizikom nijakým iným spôsobom (takéto rozhodnutie ovplyvňuje prístup organizácie k riziku a k určeným kritériám rizika). O povahe 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, ktorá rozdeľuje riziká na riziká:

• ktoré vyžadujú zaobchádzanie – patria sem neprijateľné/neakceptovateľné riziká a prípustné riziká, pre ktoré sa posudzujú náklady a prínosy,

• ktoré to nepotrebujú – prijateľná/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 viesť nasledujúce aspekty:

• či riziko potrebuje zaobchádzanie,

• priority pre zaobchádzanie,

• či má byť podniknutá nejaká činnosť,

• ktorou z množstva ciest sa vydať.

Rozhodnutie o tom, či a ako zaobchádzať 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 znamenať akýkoľvek prínos, a zaobchádzanie s rizikom je nevyhnutné za akúkoľvek cenu,

b) stredná skupina (alebo šedá oblasť), kde sa berú do úvahy náklady i prínosy, a príležitosti sú zvažované vzhľadom 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.

1. Uveďte a popíšte spôsoby **zaobchádzania s rizikom**, vysvetlite proces výberu spôsobov zaobchádzania s rizikom, definujte pojmy riadenie rizika, zvyškové riziko a uveďte obsah plánu zaobchádzania s rizikami

Charakteristika spôsobov zaobchádzania s rizikom

**Vyvarovanie sa riziku**

Vyvarovať sa riziku na základe rozhodnutia nezačínať činnosť alebo nepokračovať v činnosti, ktorá vytvára riziko znamená vyhnutie sa činnostiam, ktoré sú vystavené mimoriadnym 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 pohľadávok a iných nevýhod – nevstupovať do obchodovania síce zabráni riziku straty, ale tak isto zabráni možnosti profitovať.

**Akceptovanie alebo zvýšenie rizika**

Cieľom je využiť príležitosť v podnikaní, čo sa napríklad môže uskutočniť nasledujúcimi opatreniami:

• alokáciou (rozmiestnením) zdrojov zaručujúcou najlepšie finančné vyhliadky,

• diverzifikáciou (rozdelením) špecifických činností na zníženie rizika,

• expanziou 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 neefektívnosti,

• ovplyvnením verejnej mienky prostredníctvom reklamy a iných spôsobov 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 zníženie rizika zahŕňať: zmenu pravdepodobnosti rizika, zmenu následkov rizika, prípadne zmenu oboch

**Podieľanie sa na riziku s ďalšou stranou alebo stranami**

Podieľanie sa na riziku je formou zaobchádzania s rizikom, ktorá zahŕňa dohodnutý spôsob rozdelenia rizika s ostatnými stranami. Toto rozdelenie môžu obmedziť, zakázať alebo nariadiť právne alebo regulačné požiadavky. Podieľanie sa na riziku sa môže uskutočniť prostredníctvom poistenia alebo inej formy zmluvy. Poistenie je spôsob podieľania sa na riziku, v ktorom sú prenášané iba potenciálne finančné následky rizika, nie zodpovednosť za riadenie rizík a riziko sa tým nezníži. Rozsah rozdelenia rizika môže závisieť na spoľahlivosti a prehľadnosti usporiadania podielnictva.

**Prenos rizika je formou podieľania sa na riziku.**

Financovanie rizika je formou zaobchádzania s rizikom, ktorá zahŕňa možné opatrenia pre zaopatrenie fondov 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 ňom podieľať,

• outsourcing spoločných podnikov,

• partnerstvá a pod.

Podieľanie sa na rizika neznižuje riziko, iba jeho časť posunuje na ďalšie zmluvné strany. Spoluúčasť na riziku je vhodná stratégia pre nízke riziká, kde náklady na obnovu oproti riziku by mali byť väčšie. V niektorých prípadoch podieľanie sa na riziku môže podstatne zvýšiť riziko, pretože strana, na ktorú sa prevádza, si nemusí byť vedomá rizika a toho, že sa od nej 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 – vzťah medzi rizikom a prínosom funguje tak, že bez vystavenia sa riziku nemôže organizácia očakávať odmenu.

**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 (ovládacích 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. Zahŕňa taktiky, postupy, skúsenosti, procesy, technológie, techniky, metódy a zariadenia na modifikovanie tohto rizika.

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

Proces výberu zaobchádzania 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 analyzované riziká, možno pokračovať so zaobchádzaním s rizikami.

Zaobchádzanie s rizikom zahŕňa opakujúci sa proces:

• posudzovania zaobchádzania s rizikom,

• rozhodovania, či zvyšková úroveň rizika je prípustná,

• vytváranie nového zaobchádzania s rizikom, ak zvyšková úroveň rizika nie je prípustná,

• posudzovanie efektívnosti realizovaného spôsobu zaobchádzania.

Zaobchádzanie s rizikami môže v organizácii:

• vytvoriť lepšie možnosti pre pôsobenie rizík, z ktorých môže mať prospech,

• obmedziť možnosti pôsobenia rizík, ktoré sú pre ňu nevýhodné.

Zaobchádzanie s rizikom, ktoré sa zaoberá 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.

Zaobchádzanie s rizikami je zamerané na tie riziká, ktoré neboli posúdené ako prijateľné, t. j. ich hodnota je nad hranicou akceptovateľnosti.

Spočíva v návrhu, prijatí a realizácii opatrení, pomocou ktorých sa vybraným spôsobom ovplyvňuje ich hodnota.

Spôsoby zaobchádzania s rizikom sa nemusia nevyhnutne navzájom vylučovať alebo nemusia byť vhodné za každých okolností.

Zaobchádzanie s rizikom môže vytvoriť nové riziká alebo modifikovať existujúce riziká.

Spôsoby zaobchádzania s rizikom môžu zahŕňať tieto možnosti:

1. Vyvarovanie sa riziku (avoiding the risk) na základe rozhodnutia nezačínať 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 thel ikelihood).

5. Zmenu následkov rizika (changing the consequences).

6. Podieľanie 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).

Riadenie rizika

Riadenie rizika predstavuje opatrenie na modifikáciu konkrétneho rizika. Zahŕňa taktiky, postupy, skúsenosti, procesy, technológie, techniky, metódy a zariadenia na modifikovanie tohto rizika.

• riadenie rizika (managing risk), ktoré sa týka využitia tejto architektúry pri konkrétnom riziku – opatrenie (opatrenia), ktoré modifikuje (modifikujú) riziko.

Zvyškové riziko

Zvyškové riziko (reziduálne 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 znížení, odstránení zdroja rizika, zmene následkov alebo pravdepodobnosti, prenose rizika či zachovaní rizika

Zvyškové riziko sa musí:

• zdokumentovať,

• monitorovať,

• preskúmavať,

• a ak treba, musí sa organizácia ním naďalej zaoberať.

Obsah plánu zaobchádzania s rizikom:

Plán zaobchádzania s rizikom má obsahovať:

a) príčiny výberu možností zaobchádzania vrátane očakávaných účinkov, ktoré možno získať,

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) navrhované 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.