ČINITELE PRE HODNOTENIE BEZPEČNOSTI ORGANIZÁCIE

The factors for security assessment of the organization

prof. Ing. Ladislav HOFREITER, CSc., Katedra bezpečnostného manažmentu, Fakulta bezpečnostného inžinierstva ŽU v Žiline

Ladislav.Hofreiter@fbi.uniza.sk

Ing. Martin HALAJ, Katedra bezpečnostného manažmentu, Fakulta bezpečnostného inžinierstva ŽU v Žiline

Martin.Halaj@fbi.uniza.sk

Abstrakt

Bezpečnosť je základnou podmienkou existencie, pretrvania a rozvoja každej organizácie. Dosiahnutá úroveň bezpečnosti vytvára podmienky pre plnenie požadovaných funkcií organizácie. Na ohodnotenie reálnej bezpečnosti organizácie potrebujeme poznať tie činitele, ktoré zásadným spôsobom ovplyvňujú úroveň jej bezpečnosti.

V tomto článku identifikujeme a popisujeme rozhodujúce činitele bezpečnosti organizácie, ukazujeme ich vzájomné vzťahy a prezentujeme postup, ako s využitím týchto činiteľov a ich vzťahov možno komplexne ohodnotiť bezpečnosť organizácie.

Abstract

Security is an essential condition for the existence, persistence and development of each organization. The achieved level of security creates conditions for fulfilling the required functions of the organization. For real security assessment of the organization, we need to know the factors that fundamentally influence the level of its security.

In this article we identify and describe the crucial security factors of the organization. We show their mutual relationships of those factors and we present procedure, how using these factors and their relations enables comprehensive assessment of the security of the organization.

Úvod

Pretrvanie, rozvoj, zachovanie funkčnosti a spôsobilostí akejkoľvek organizácie je spojené predovšetkým s problémom jej bezpečnosti.

Zaistením a udržiavaním určitej úrovne bezpečnosti získavajú organizácie schopnosť ochrániť svoje hlavné aktíva, ako aj hlavné a podporné činnosti. Tým zvyšujú nielen svoju konkurencie schopnosť, ale aj minimalizujú straty, spojené s vznikom bezpečnostných incidentov.

V doterajších prácach sme sa zameriavali predovšetkým na riešenie ochrany objektov a chránených záujmov z hľadiska tvorby predpokladov a východísk projektovania systémov ochrany. Dominantným sektorom skúmania a posudzovania

bezpečnosti bol sektor ochrany majetku, fyzickej a objektovej bezpečnosti z hľadiska pôsobenia bezpečnostných rizík antropogénnej povahy.

V tejto štúdii sa chceme zamerať na komplexnejšie posudzovanie a hodnotenie bezpečnosti organizácií, či už výrobného alebo nevýrobného charakteru. Objektom nášho skúmania je organizácia a problém jej bezpečnosti, predmetom skúmania je identifikovanie a deskripcia činiteľov, ktoré priamo alebo nepriamo ovplyvňujú bezpečnosť organizácie.

Metodický postup riešenie cieľov štúdie je zvolený tak, aby boli objasnené a popísané teoretické východiská pre hodnotenie bezpečnosti organizácií, boli identifikované a popísané rozhodujúce činitele pre hodnotenie bezpečnosti organizácie a následne vytvorený model hodnotenia bezpečnosti organizácie.

1. Teoretické východiská pre hodnotenie bezpečnosti organizácie

Teoretický prístup k posudzovaniu bezpečnosti organizácie znamená objasniť, čo to organizácia je, ako je charakterizovaná bezpečnosť organizácie, aké činitele vplývajú na bezpečnosť. Objasnenie pojmov organizácia a bezpečnosť sú preto základným a východiskovým výskumným problémom. Je nevyhnutnou podmienkou toho, aby sme dosiahli pochopenie obsahu a významu činností, spojených s posudzovaním a hodnotením bezpečnosti organizácií.

Objasnenie ontologických aspektov súvisiacich s hodnotením bezpečnosti organizácie umožňuje použitie kvalitatívnej, explanatívnej metódy. Komplexné posúdenie problému bezpečnosti organizácie vyžaduje, aby sme skúmali tieto výskumné problémy:

- Čo je to organizácia, aký je význam a obsah tohto pojmu?
- Čo to je bezpečnosť, aké sú rozhodujúce činitele bezpečnosti?
- Ako hodnotiť bezpečnosť organizácie ?

1.1 Organizácia, pojem a obsah

V literatúre je možné nájsť veľa prístupov k vymedzeniu pojmu organizácia. H.J. Leawit charakterizoval organizáciu ako systém zložený zo štyroch podsystémov: ľudí, úloh, technológií a štruktúry (March, 1965, s.160).

G. Morgan tiež uplatňoval systémový prístup k organizácii a charakterizoval päť podsystémov: stratégiu, technológie, štruktúru, ľudsko-kultúrny a riadenie (Morgan, 1997, s.51).

L.J. Krzyžanowski (Krzyżanowski,1995, s.37) ako základ pre definovanie organizácie považoval zdroje, pričom podľa neho tvoria organizáciu zdroje tvorivé (ľudia), prírodné a umelé (technika a technológie).

Organizácia podľa Sedláka (Sedlák, 2001. S. 197) je pojem na označenie inštitúcie, organizovaného celku, určitého objektu. V tomto vecnom význame je organizácia celok, v ktorom ľudia vykonávajú spoločnú činnosť zameranú na dosiahnutie vytýčených cieľov.

Míka (Míka, 2013, s. 97-98) charakterizuje organizáciu aj ako reálny, relatívne uzavretý objekt, ako systém sociálnych prvkov, vzťahov a cieľov

v inštitucionalizovanej materializovanej podobe, ako riadenú sociálnu sústavu vytvorenú za účelom plnenia stanovených cieľov.

Pomerne najkomplexnejšiu definíciu organizácie podal L.F. Korzeniowski (Korzeniowski, 2010, s. 313), v ktorej uvádza, že organizácia je v prostredí vyčlenená skupina spolupracujúcich ľudí, usilujúcich o synergický efekt a dosiahnutie prijatého cieľa. Hlavné atribúty ním definovanej organizácie sú spoločný cieľ, riadenie, organizačná kultúra, organizačná štruktúra a súčinnosť všetkých prvkov a členov organizácie pri dosahovaní cieľa.

V našom príspevku budeme za organizáciu považovať *materiálne objekty a technológie výrobného alebo nevýrobného charakteru (inštitúcie), určené na produkciu tovarov, poskytovanie služieb a uspokojovanie potrieb obyvateľov*.

Takúto organizáciu môžeme považovať za otvorený, komplexný, sociálno-technický, cieľovo orientovaný systém, ktorý je v neustálej interakcii so svojím okolím.

1.2 Bezpečnosť a bezpečnosť organizácie

Rozhodujúci teoretický problém pri riešení bezpečnosti organizácie spočíva v objasnení pojmu bezpečnosť.

Hľadanie odpovede na otázku čo je bezpečnosť je jedným zo základných znakov filozofického prístupu k bezpečnosti. Avšak definovať pojem bezpečnosť je nemalý problém a to aj preto, že skoro každý odbor ľudskej činnosti si vytvoril svoj vlastný prístup a svoju vlastnú definíciu.

Pre bezpečnosť, podobne ako pre veľa iných kategórií, neexistuje jediná, určujúca a nespochybniteľná definícia. Bezpečnosť sama o sebe je zložitý, vnútorne štruktúrovaný, multifaktorový a hierarchizovaný fenomén, ktorého obsah, štruktúra i funkcie presahujú hranice nielen jedného vedného odboru (napr. vojenská veda, policajná veda), ale dokonca i celých vedných oblastí (spoločenských, prírodných, technických, a i.) (Hofreiter, 2004).

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

V najvšeobecnejšej rovine je bezpečnosť definovaná ako absencia, neprítomnosť nebezpečenstva. Takéto vyjadrenie býva označované ako bezpečnosť v úzkom ponímaní. V praktickom živote je však takéto ponímanie bezpečnosti veľmi obtiažne, pretože neexistuje, alebo je len veľmi ťažko dosiahnuteľný život s úplnou absenciou nebezpečenstva.

Bezpečnosť býva definovaná ako stav, v ktorom nikomu alebo ničomu nehrozí nebezpečenstvo. Z toho vyplýva, že bezpečnosť je predmetná a nemôže existovať bez objektu ohrozenia, vždy sa vzťahuje k niečomu alebo niekomu.

Realistickejšie už vyznieva definovanie bezpečnosti v širšom ponímaní, ktoré vychádza z praktickej koexistencie (spolupráce) indivíduí a sociálnych objektov v určitom prostredí, pričom táto koexistencia je ovplyvňovaná existenciou činiteľov, vplyvov a javov s negatívnym deštruktívnym potenciálom. Proces, v ktorom ide o odvrátenie, oslabenie alebo elimináciu hrozieb vyplývajúcich z bezpečnostného prostredia nám poskytuje predstavu o bezpečnosti v najširšom ponímaní.

Pod pojmom **bezpečnosť organizácie** sa rozumie *sústavné a efektívne využívanie všetkých zdrojov, zabezpečujúcich stabilné fungovanie organizácie v súčasnosti a stály rozvoj v budúcnosti.* To však predpokladá aktívny prístup, najmä v smere:

- nepretržitého odhaľovania proximatívnych (bezprostredných) príčin ohrozenia svojej bezpečnosti, tzn. identifikovania, AKO môže byť ohrozená jeho bezpečnosť,
- nepretržitého odhaľovania ultimatívnych (konečných) príčin ohrozenia svojej bezpečnosti, tzn. zisťovania, PREČO môže byť ohrozená jeho bezpečnosť,
- včasného vytvorenia efektívneho bezpečnostného systému na ochranu svojich aktív.

Gašpierik (Gašpierik, et. al., 2011) uvádza, že bezpečnosť organizácie možno charakterizovať ako aktívne využívanie systému bezpečnosti, ktorého úlohou je zaistiť bezpečné prostredie, v ktorom organizácia môže napĺňať svoje funkcie a plniť vytýčené ciele. Na túto činnosť je potrebné, aby organizácia:

- charakterizovala svoje bezpečnostné prostredie,
- identifikovala možných narušiteľov bezpečnosti,
- určila svoje významné aktíva,
- dohliadala na nepretržitý proces identifikácie rizík a príčin vzniku nebezpečenstva,
- vytvorila včas adekvátnu bezpečnostnú stratégiu,
- zaviedla komplexný plán ochrany a zaistenia bezpečnosti,
- dohliadala na zavedenie a vypracúvanie bezpečnostnej dokumentácie.

Organizácia bude považovaná za bezpečnú, ak:

- nie je zdrojom ohrozenia, neohrozuje seba ani svoje okolie (iné systémy, javy, procesy a objekty),
- je v takom stave, ktorý umožňuje jej stály a progresívny vývoj, resp. plnenie od nej požadovaných funkcií,
- má dostatočný potenciál na elimináciu alebo minimalizáciu vonkajších alebo vnútorných ohrození najrôznejšej povahy,
- je schopná okamžitej reakcie na zmenu svojho stavu i stavu prostredia,
- dokáže reagovať na zmenu rovnováhy medzi ohrozeniami a vlastným ochranným potenciálom (systémom bezpečnosti, resp. systémom ochrany).

1.3 Systém bezpečnosti organizácie

Problematika bezpečnosti organizácie je interdisciplinárnou záležitosťou. Preto i pri riešení praktických otázok bezpečnosti organizácie sa vyžaduje systémový prístup. Systém bezpečnosti organizácie musí byť vytvorený tak, aby účelným usporiadaním a použitím disponibilných síl (ľudských zdrojov), technických prostriedkov (EZS, MZP, ap.) a organizačných opatrení zabezpečoval efektívnu ochranu proti identifikovaným bezpečnostným ohrozeniam.

Systém bezpečnosti organizácie by mal zabezpečovať:

- **rozvoj** , ktorý predstavuje jeden z činiteľov ekonomickej bezpečnosti podniku. Ak sa podnik nerozvíja, potom veľmi rýchlo stráca schopnosť prežiť a prispôsobovať sa meniacim sa vnútorným i vonkajším podmienkam.

- **pevnosť, stálosť** – odráža odolnosť a spoľahlivosť štruktúr podniku, vertikálnych, horizontálnych a iných väzieb v štruktúrach podniku a schopnosť odolávať vonkajším i vnútorným negatívnym javom.

Systém bezpečnosti organizácie môže tvoriť:

- systém ochrany hmotného i nehmotného majetku, realizovaný použitím technických zabezpečovacích systémov a/alebo fyzickej ochrany, resp. režimovej ochrany,
- systém ochrany osôb, napr. ochrana zdravia pri práci, ochrany dôležitých osôb *(bodyguarding)* ap.,
- systém ochrany informačných systémov,
- systém ochrany utajovaných skutočností (vrátane ochrany osobných údajov, obchodného tajomstva, citlivých firemných informácií ap.),
- systém technickej (technologickej) bezpečnosti, vrátane prevencie závažných priemyselných havárií,
- systém protipožiarnej ochrany,
- systém ochrany životného prostredia,
- systém ochrany vnútorného poriadku v podniku,
- systém ochrany ďalších bezpečnostných záujmov podniku.

2. Činitele bezpečnosti organizácie

Pri uplatnení všeobecného prístupu k definovaniu bezpečnosti uplatňujeme paradigmu, že každý referenčný objekt, ktorým je aj organizácia, sa mení v každom časovom okamihu buď sám osebe, alebo sa menia jeho vzťahy (väzby) voči okoliu (bezpečnostnému prostrediu). Rovnako tak je v neustálom vývoji aj bezpečnostné prostredie. Práve meniace sa podmienky v okolí objektu najviac ovplyvňujú bezpečnosť objektu. Bezpečnosť je teda závislá na vzájomnom pôsobení nasledujúcich činiteľov:

- ohrození (*threat)*, ktoré sa nachádzajú v otvorenej alebo latentnej podobe v danom prostredí (*environment*)
- objektu s jeho obrannými, ochrannými schopnosťami, ktoré môžeme kvantifikovať pomocou zraniteľnosti (*vulnerability*), odolnosti (*resilience).*

Z hľadiska riešenia bezpečnosti organizácie budeme sa zaoberať dvomi skupinami činiteľov:

- vonkajšie činitele, ku ktorým zaraďujeme vonkajšie bezpečnostné prostredie, bezpečnostné výzvy a bezpečnostné ohrozenia,
- vnútorné činitele, zahrňujúce vnútorné bezpečnostné prostredie, zraniteľnosť a odolnosť organizácie.

Z hľadiska logického postupu skúmania a definovania činiteľov bezpečnosti organizácie prioritu má analýza a hodnotenie bezpečnostného prostredia a to z toho dôvodu, že vytvára rámec pre identifikovanie bezpečnostných výziev i ohrození.

2.1. Bezpečnostné prostredie organizácie

Bezpečnostné prostredie organizácie tvorí *časť prírodného, sociálneho a technogénneho prostredia,* v ktorom vzniká v danom čase a priestore, v dôsledku interakcií aktérov a vplyvu činiteľov prostredia adekvátna *bezpečnostná situácia*. (Hofreiter, L., Matis, J., 2010)

Štruktúru takto vymedzeného bezpečnostného prostredia tvoria:

- organizácie, ktorých význam a hodnota vyžaduje ich ochranu, pričom tieto môžu mať schopnosť interakcie so svojím prostredím[1],
- ďalšie podmienky a činitele, ktoré priamo či nepriamo ovplyvňujú situáciu[2] v bezpečnostnom prostredí, teda i situáciu organizácií.

Z priestorového hľadiska rozlišujeme vonkajšie a vnútorné bezpečnostné prostredie organizácie.

Vonkajšie bezpečnostné prostredie organizácie môžeme považovať za *priestor, nachádzajúci sa zvonka hraníc organizácie, v ktorom sa vyskytujú činitele, odohrávajú sa procesy, ktoré majú rozhodujúci vplyv na úroveň bezpečnosti danej organizácie.* (Hofreiter, L., 2006) Vonkajšie bezpečnostné prostredie je tvorené súhrnom sociálnych, prírodných a technogénnych determinánt a iných činiteľov, ktoré môžu mať vplyv na bezpečnosť a plnenie funkcií organizácie. Vonkajšie bezpečnostné prostredie organizácie môžeme tiež identifikovať ako:

- ***bližšie,*** v ktorom existuje bezprostredná interakcia medzi organizáciou a okolím, tzn. že sa vzájomne ovplyvňujú alebo sa môžu ovplyvňovať,
- ***vzdialené***, ktoré tvorí bližšie neohraničený priestor, v ktorom existujú, alebo sa môžu vyskytnúť činitele s významným vplyvom na plnenie funkcií a existenciu organizácie.

Vnútorné bezpečnostné prostredie môžeme považovať za *priestor, nachádzajúci sa vo vnútri hraníc organizácie, v ktorom sa vyskytujú činitele, odohrávajú sa procesy, ktoré majú alebo môžu mať rozhodujúci vplyv na úroveň bezpečnosti organizácie.* (Hofreiter, L., 2006) Vnútorné bezpečnostné prostredie organizácie budeme identifikovať a hodnotiť vtedy, ak si to vyžaduje charakter organizácie – teda v prípade rozsiahlejších materiálnych objektov, ktoré samy o sebe predstavujú zložitejšiu, členitú štruktúru.

---

[1] Forma interakcie objektu s prostredím môže byť **aktívna**: objekt vplýva na charakter situácie v prostredí, alebo **pasívna**, charakterizovaná zraniteľnosťou objektu voči vonkajším vplyvom.

[2] Pod pojmom situácia rozumieme časovo usporiadanú **štruktúru vzťahov, interakcií a väzieb** medzi subjektom a objektom, viazanej na určitý priestor, ktorého parametre spolu s charakterom činností naplňujúcich tieto vzťahy určujú špecifiku situácie.

2.2.Bezpečnostné výzvy a ohrozenia

V bezpečnostnej praxi sa často stretávame s pojmami bezpečnostné výzvy a bezpečnostné ohrozenia. Neznamenajú to isté a nemôžu sa zamieňať.

Bezpečnostné výzvy sú také zmeny v bezpečnostnom prostredí organizácie, ktoré môžu mať destabilizujúci účinok na organizáciu a preto vyžadujú adekvátnu reakciu na ne. Bezpečnostné výzvy nemožno automaticky považovať za ohrozenia. Ak organizácia včas a primerane reaguje na aktuálne výzvy, nielenže eliminuje vznik ohrozenia, ale môže i zvýšiť úroveň svojej bezpečnosti.

Bezpečnostné ohrozenie predstavuje konkrétny, fyzicky existujúci objekt, jav, udalosť či proces, ktorý má schopnosť spôsobiť škodu alebo ujmu. V najširšom význame sa takto označuje všetko, čo je pre organizáciu nebezpečné, čo by mohlo negatívne zmeniť úroveň jeho bezpečnosti. Ohrozením označujeme aj udalosti a javy, ktoré môžu v relatívne krátkom čase nastať alebo už nastali a môžu spôsobiť dramatické zmeny podmienok existencie referenčného objektu (Hofreiter a kol, 2013). Ohrozenia môže byť vyvolané silami prírody alebo ľudskou aktivitou, môžu nastať s určitou pravdepodobnosťou a majú potenciál spôsobiť drastické zmeny v podmienkach existencie organizácie .

2.3. Zraniteľnosť organizácie

Zraniteľnosť vo všeobecnosti znamená vlastnosť ľubovoľného materiálneho objektu, technického prostriedku alebo sociálneho subjektu stratiť schopnosť plniť svoju prirodzenú alebo stanovenú funkciu v dôsledku pôsobenia vonkajších alebo vnútorných ohrození rôznej povahy a intenzity. Vyjadruje výsledok expozície a citlivosti systému na negatívne javy a udalosti antropogénnej, prírodnej či techno-génnej povahy. V najširšom ponímaní je to predispozícia objektu alebo systému na narušenie jeho existencie, stability, rozvoja, integrity a/alebo poškodenie.

Takto ponímaná zraniteľnosť má aspekty:

- vonkajší, prezentovaný pôsobením ohrození prírodnej alebo antropogénnej povahy,
- priestorový, spočívajúci v rizikovosti priestoru umiestnenia (dislokácie) organizácie,
- vnútorný, vyjadrujúcu citlivosť a predispozíciu organizácie na ujmu, poškodenie, apod.

Pri vnímaní zraniteľnosti ako rizika expozície sa analýza zraniteľnosti zameriava na charakteristiky činiteľov, podmienok a dopadov expozície. Analyzuje sa udalosť pôsobiaca na organizáciu, resp. na jej systém ochrany. Pri tomto prístupe nie sú posudzované príčiny a ďalšie faktory, ktoré ovplyvňujú zraniteľnosť organizácie, ale len aspekt časovej a priestorovej koexistencie organizácie a pôsobiaceho ohrozenia.

2.4.Odolnosť organizácie

Pri výskume bezpečnosti sa často stretávame s tým, že sa pojmy zraniteľnosť a odolnosť viac-menej stotožňujú, odolnosť predstavuje synonymum zraniteľnosti. Význam oboch pojmov však nemožno považovať za totožný.

Pokiaľ zraniteľnosť (*vulnerability*) vyjadruje výsledok expozície a citlivosti systému na negatívne javy a udalosti, **odolnosť** (*resilience*) znamená *schopnosť organizácie vyrovnať sa s pôsobením negatívnych javov a udalostí, zachovať si svoju funkčnosť, integritu, pretrvať bez poškodenia, resp. rýchlo odstrániť škody a straty a obnoviť normálne podmienky svojej existencie*.

Odolnosť organizácie v tomto kontexte môžeme vnímať ako jej schopnosť obnoviť svoju funkčnosť a reorganizovať sa po vzniku zmien, vyvolaných poruchami, resp. vonkajšími negatívnymi vplyvmi, udalosťami rôzneho charakteru. Môže byť charakterizovaná:

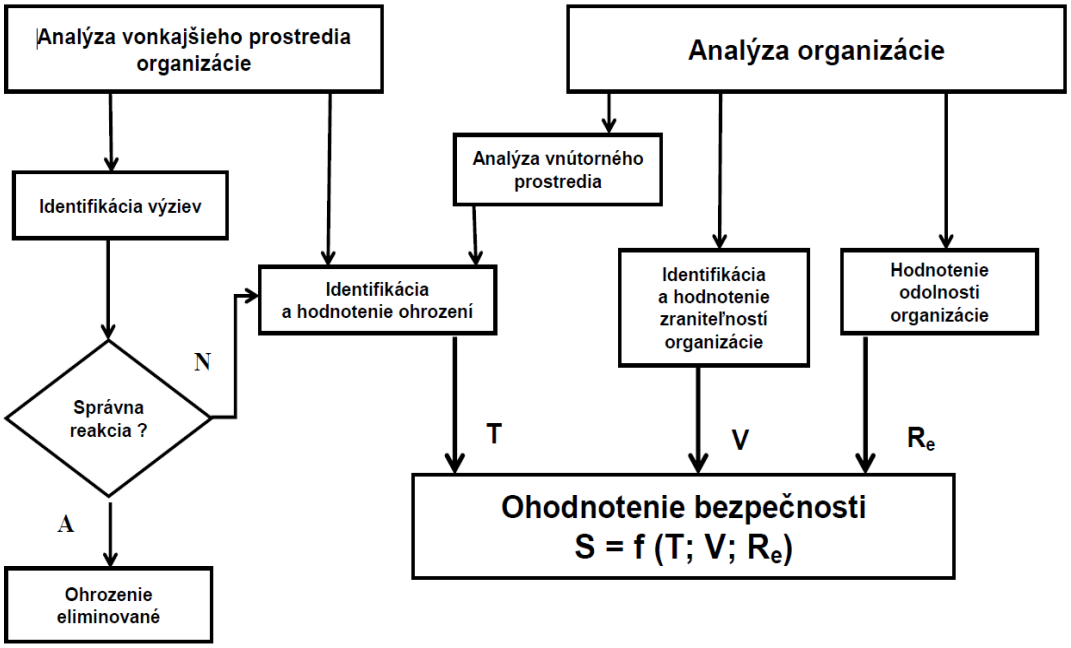
- rezistenciou voči negatívnym vplyvom, udalostiam,
- rýchlosťou návratu do pôvodného stavu, ak došlo k negatívnym javom a udalostiam.

Úroveň odolnosti organizácie bude závisieť na množstve a kvalite ľudských, materiálnych, hmotných a finančných zdrojov a zásob, použiteľných na odstraňovanie následkov negatívnych javov a udalostí, ako aj od akcieschopnosti síl a prostriedkov krízového reagovania.

3. Hodnotenie bezpečnosti organizácie

Hodnota (miera) bezpečnosti organizácie bude vždy výsledkom interakcie vonkajších a vnútorných bezpečnostných ohrození (T) a jej ochranných (obranných) vlastností, schopností a možností, parametrizovaných prostredníctvom činiteľa zraniteľnosti (V) a odolnosti (R_e) .

Na hodnotenie bezpečnosti organizácie odporúčame postup, ktorý je uvedený na obrázku 1. Spočíva v postupnosti identifikovania a hodnotenie činiteľov bezpečnosti organizácie a následné komplexné ohodnotenie bezpečnosti organizácie.



Obrázok 1. Model hodnotenie bezpečnosti organizácie. Vlastné spracovanie

Dosiahnutý alebo očakávaný stupeň bezpečnosti organizácie môžeme ohodnotiť na základe vzťahu identifikovaných činiteľov bezpečnosti: veľkosti a intenzity identifikovaných ohrození, zraniteľnosti a odolnosti. Ohodnotenie spočíva v logickom posúdení vzťahu týchto činiteľov a ich vplyvu na bezpečnosť sektoru, napr.:

- ak veľkosť identifikovaného ohrozenia je ohodnotená ako veľká, ale zraniteľnosť organizácie je ohodnotená ako veľmi malá, odolnosť organizácie je veľká, to ukazuje na dostatočnú bezpečnosť organizácie, pretože dané ohrozenie nemôže, vzhľadom na minimálnu zraniteľnosť a veľký stupeň odolnosti narušiť funkčnosť organizácie alebo spôsobiť jej dramatickú škodu či inú ujmu.

Záver

Bezpečnosť je taký stav bezpečnostnej situácie a procesov tento stav ovplyvňujúcich, ktorý zaisťuje priaznivé podmienky pre existenciu, pretrvanie a rozvoj organizácie.

Efektívnosť hodnotenia bezpečnosti organizácie je v podstatnej miere závislá od toho, ako bude zvládnutý proces identifikácie a hodnotenie činiteľov, ktoré sú zásadne determinujú bezpečnosť organizácie.

Pri analýze a hodnotení bezpečnosti organizácie budeme uplatňovať princíp ***rozhodujúcich činiteľov***. Tento princíp umožňuje abstrahovať nepodstatné, vedľajšie javy a procesy, ktoré nemajú významnejší vplyv na bezpečnosť organizácie.

Pri rešpektovaní uvedeného prístupu môžeme prijať záver, že k narušeniu (zmene úrovne) bezpečnosti organizácie dôjde vtedy, keď:

- nastanú také zmeny v organizácii , ktoré výrazne zvýšia jej zraniteľnosť, znížia jej odolnosť, pričom vývoj v prostredí zostane nezmenený,
- v prostredí (okolí) organizácie dôjde k zmenám, ktorých výsledkom bude pôsobenie ohrození vysokej intenzity, prevyšujúcich stupeň zraniteľnosti a mieru odolnosti organizácie.

Je v možnostiach organizácie, eliminovať tieto negatívne javy. Jednak aktívnym vplyvom na vývoj situácie v jej okolí, ale aj aktívnou vlastnou bezpečnostnou politikou, formovaním zodpovedajúcej úrovne kultúry bezpečnosti (Halaj, 2016), vytváraním priaznivej bezpečnostnej klímy v organizácii.

Zavedením a udržiavaním kultúry bezpečnosti je možné ovplyvňovať nielen materiálny pilier bezpečnosti (systém bezpečnosti a jeho prvky), ale aj ľudský činiteľ, duchovný pilier kultúry bezpečnosti prejavujúci sa v bezpečnostnom povedomí zamestnancov organizácie, ale aj v zodpovednom prístupe vedenia organizácie k otázkam a problémom jej bezpečnosti.

LITERATÚRA

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

HALAJ, M. 2016. *Kultúra bezpečnosti ako aspekt bezpečnosti organizácie.* In: Súčasnosť a perspektívy bezpečnostného výskumu, medzinárodný workshop. EDIS-Vydavateľstvo ŽU v Žiline, 2016.

HOFREITER, L. 2006. *Securitológia*. 1.vyd. Liptovský Mikuláš :AOS, 2006

HOFREITER, L., MATIS, J. 2010. *Komplexná metodika hodnotenia bezpečnostného prostredia*. Priebežná výskumná správa. Liptovský Mikuláš: Akadémia ozbrojených síl gen. M.R. Štefánika, 2010.

HOFREITER, L. a kol. 2013. *Ochrana objektov kritickej dopravnej infraštruktúry*. EDIS – vydavateľstvo ŽU v Žiline 2013. 238 s.,

KORZENIOWSKI, L.F. 2010. *Menedżment . Podstawy zarządzania*. EAS, Krak'ow, 2010.

KRZYŻANOWSKI, L. J.1999. *O podstawach kierowania organicajami*. PWN, Warszawa1999.

MARCH, J.G. 1965. *Handbook of Organization*. Rand Mc Nally, Chicago, 1965.

MÍKA, V.T. *Manažment. Úvod do riadenia organizácie v podmienkach rizika a v krízových situáciách*. EDIS- Vydavateľstvo ŽU v Žiline, 2013.

MORGAN, G. 1997. *Obrazy organizacji*. PWN, Warszawa, 1997.

SEDLÁK, M. 2001. *Manažment*. IURA EDITION, Bratislava, 2001.