Manažérstvo bezpečnosti podniku

Imrich Dufinec[1]

Security Management of Business or Company

ABSTRAKT

Základná orientácia vrcholového manažmentu podniku týkajúca sa komplexnej bezpečnosti podniku musí byť určovaná jeho bezpečnostnou politikou. Na báze manažérstva rizík má reagovať na vzniknuté nežiaduce javy definovanej bezpečnosti a predchádzať im až po prijateľnú mieru rizík. Takáto realizácia bezpečnostnej politiky sa má uskutočňovať metódami a nástrojmi ochrany podopretými právnym a legislatívnym rámcom, zakotveným v bezpečnostnej dokumentácii. Vonkajšia a vnútorná ochrana bezpečnosti sa týka fyzickej ochrany osôb a majetku, ochrany všetkých hmotných i nehmotných aktív podniku, ochrany jeho infraštruktúry a environmentu, ako aj o osobných a administratívnych údajov, ktoré má podnik v správe. Obraz komplexnej bezpečnosti podniku má uzatvárať aj bezpečnosť produktov, ktoré podnik produkuje.

Reálna bezpečnosť podniku a stupeň jej komplexnosti však závisia od bezpečnostnej politiky a najmä finančných možností podniku.

ABSTRACT

Basic orientation of TOP Management of business or company dealing with a complex security must be determined by its security policy. On the risks management base it is necessary to respond to autochthonous and unfavourable phenomena of the defined security and to prevent them pending an acceptable exposure. Such realization of security policy should be realized by means of using the tools of protection supported by the legal and legislative frame embodied in the security documentation. The external and internal protection of security is referred a physical protection of persons and property and protection and all tangible and intangible business property and protection of its infrastructure and environment as well as personal and administrative data which a business holds in its management. The complex security projection of business has to enclose also products security, which are produced by a business. However, the real security of a business and its complexity degree depend to a security policy and especially the finance capabilities of a business or company.

Kľúčové slová: Bezpečnosť podniku, bezpečnostný manažér, ochrana aktív, integrovaný manažérsky systém, ohrozenie a riziká podniku.

Key words: *Business security, security manager, protection of assets, integrated management system, threats and risks facing a business or company.*

1. ÚVOD

Technické prvky zabezpečovania ochrany osôb a majetku podniku súvisia so schopnosťou ich výberu a aplikácie za predpokladu znalosti technických nástrojov aplikovaných prostriedkov. Technika však nestačí. Podnik potrebuje pre svoju bezpečnosť organizáciu, systém podporujúci rozhodovanie manažérov z hľadiska investícií, znalostí princípov funkcie technických bezpečnostných prvkov, ale i zákonov, noriem a pravidiel pre ich bezpečné a zákonné nasadzovanie v podniku. Sem patria aj prvky informačnej bezpečnosti a bezpečnosti informačných technológií. Osobitný miestom sú samotné riadiace procesy.

Bezpečný podnik, bez ohľadu na jeho veľkosť, zameranie a štruktúru predpokladá jeho riadenie manažérmi, ktorí sú vyprofilovaní so všetkými atribútmi tejto profesie, avšak s akcentom na schopnosť aplikovať teóriu rizík a techniku ich eliminácie na akceptovateľnú

[1] Prof. Ing. Imrich Dufinec, CSc., pedagóg ekonomických a manažérskych predmetov v študijnom odbore 8.3.1 – Ochrana osôb a majetku, garant predmetu Bezpečnosť podniku. Ústav ekonomickej a logistickej bezpečnosti Vysokej školy bezpečnostného manažérstva v Košiciach, Košťova 1, 040 01 Košice, Slovensko, e-mail: imrich.dufinec@vsbm.sk

mieru vo všetkých analýzou potvrdených systémových, procesných, osobných i vecných stránok podniku.

2. BEZPEČNÝ PODNIK A BEZPEČNOSŤ PODNIKU

Bezpečnosť reálneho podniku začína a končí pri bráne do podniku a zahŕňa v sebe tak bezpečnosť zamestnanca ako aj zákazníka, či tretej zainteresovanej strany a všetkých ich aktív, ktoré so sebou prinášajú. Prakticky to znamená, že bezpečný podnik vykonáva trvalú množinu bezpečnostných opatrení na ochranu v podniku pôsobiacich osôb a všetkých hmotných i nehmotných aktív súvisiacich s jeho podnikaním. Nutné bezpečnostné opatrenia vykonáva v súlade s prijatou bezpečnostnou politikou a celkovou stratégiou podnikania v systéme prostredníctvom svojich procesov.
Medzi základné zložky bezpečnosti podniku možno zovšeobecnene zaradiť desať týchto parciálnych zložiek:

- Fyzická ochrana osôb a majetku nachádzajúcich sa v podniku
- Ekonomická bezpečnosť aktív podniku
- Environmentálna bezpečnosť, vrátane požiarnej ochrany a prevencie havárií
- Bezpečnosť a ochrana zdravia pri práci v podniku
- Bezpečnosť a ochrana osobných údajov osôb pohybujúcich sa v podniku
- Bezpečnosť informačných systémov
- Bezpečnosť a ochrana vnútorného poriadku podniku
- Bezpečnosť a ochrana utajovaných skutočností nad rámec osobných údajov
- Bezpečnosť infraštruktúry, menovite kritickej, podľa charakteru podniku
- Bezpečnosť produkcie ako aspekt jej kvality

Základné parciálne zložky bezpečnosti podniku predstavujú jednotlivé aspekty komplexnej bezpečnosti podniku zabezpečovanej procesmi. Pri zachovaní ich úrovne na patričnej hladine rizík a ohrození možno hovoriť o bezpečnom podniku.
Úroveň komplexnej bezpečnosti samozrejme závisí od miery integrácie parciálnych zložiek bezpečnosti. Otázky integrácie sú pritom otázkami predmetu podnikania, politiky podnikania a osobností manažérov, schopných s istou dávkou znalostí riadiť problematiku uvedených podsystémov integrovaným spôsobom. Maximálna integrácia predpokladá maximalizáciu informačnej technológie (IT), ako prostriedku komplexného manažérskeho rozhodovacieho procesu, s akcentom nie na separátnu návratnosť investície do bezpečnosti ale celkovú návratnosť trvalo udržateľného rozvoja podniku. Takáto integrácia je dnes možno pre mnohé podniky iba víziou ale aj možnou blízkou realitou pre tých, ktorí správne pochopili integrovaný manažérsky systém založený na procesnom prístupe riadenia s aspektmi komplexne pojatej bezpečnosti. Je možné ju budovať postupne, akceptujúc základne princípy podsystémov a ich integrácie. Nikdy ju však nemožno kopírovať. Je založená na špecifikách každého podniku. Manažéra komplexne poňatej bezpečnosti možno nazvať CSO (Chief Security Officer), ktorý by mal byť podriadený vrcholovému manažérovi CEO (Chief Executive Officer).
Bezpečnostný manažér takejto pozície je zodpovedný za všetky aspekty bezpečnosti podniku, vrátane bezpečnosti produkcie, pokiaľ spadá do kritickej architektúry bezpečnosti. Pre svoje manažérske rozhodovanie využíva podnikovú informačnú technológiu (IT), pretože procesy, ktoré v podniku prebiehajú sú podporované a výsledky zaznamenávané informačnou technológiou. Preto od jej úrovne závisí aj celková, komplexná bezpečnosť podniku. Diery v informačnej technológii znižujú úroveň bezpečnosti podniku v každom jej aspekte. Manažéra IT v ktorejkoľvek forme realizácie procesov možno označiť ako CIO (Chief

Information Officer), ktorý je zároveň aj vlastníkom týchto procesov a ich informačného systému.
Parciálne zložky bezpečnosti podniku i ich integrálna podoba môžu mať niekoľko foriem, závislých od organizačných predpokladov, finančných možnosti a iných predpokladov, zhrnutých do bezpečnostnej politiky podniku. Ukážme si niektoré modely [2].

3. MOŽNÉ FORMY BEZPEČNOSTI PODNIKU

3.1 Model ignorovanej bezpečnosti

Ide o prípad podniku, ktorý je orientovaný na svoje základné funkcie smerom k jadru podnikania. Za IT je zodpovedný príslušný majiteľ procesu, neformálne označovaný ako CIO, avšak s absentujúcou funkciou bezpečností. O bezpečnosť sa nikto nezaujíma. Hmotné aktíva firmy a osoby sú chránené prirodzenou cestou pudom sebazáchovy. Rovnako ako hmotné aktíva, ani informácie nie sú chránené. Snahy o aplikáciu bezpečnostných nástrojov sú buď obmedzované alebo totálne ignorované. Prvé zmeny nastanú, keď dôjde k incidentu.

3.2 Model minimálnej technologickej bezpečnosti

Tento model bezpečnosti počíta iba s IT hlavného procesu tvoriaceho pridanú hodnotu podniku. Aplikácia bezpečnostnej politiky, ak vôbec existuje, prebieha skôr podvedome a spravidla v jednej, nanajvýš v dvoch formách bezpečnostných podsystémov. Môže ísť napr. o implementáciu systému bezpečnosti a ochrany zdravia pri práci, alebo môže ísť o situáciu obchodnej spoločnosti, s minimálnou bezpečnosťou uchovávaných informácií, alebo o jednoduchú ochranu akéhokoľvek majetku firmy, v kombinácii s činnosťou informátora, a pod. Pre takýto model bezpečnosti podnik ani nepredpokladá osobitnú pozíciu bezpečnostného manažéra a bezpečnosť je zabezpečovaná technologickým procesom. Riadením IT nie je poverená žiadna funkcia na plný pracovný úväzok. Takýto podnik je vystavený riziku bezpečnostných incidentov, nielen zo strany systému alebo aj pracovníkov.

3.3 Model formálnej bezpečnosti

Model formálnej bezpečnosti vzniká na základoch modelu minimálnej technologickej bezpečnosti alebo dokonca je s ním stotožnený s tým rozdielom, že funkcia bezpečnosti sa akceptuje uvedomelo a inštitucionálne. Znamená to, že v podniku je menovaná osoba, CSO, zodpovedná za otázky bezpečnosti ale stále ešte v pozícii kumulovanej funkcie, často i funkcie CIO. Ďalší rozvoj bezpečnosti podniku je v tomto prípade založený predovšetkým na osobnosti povereného CSO a na jeho schopnosti presadzovať plnenie nových úloh bezpečnosti prostredníctvom IT. Najväčším nedostatkom tohto modelu je konflikt záujmov CSO, pretože kumuláciou funkcie rozvoja bezpečnosti a gestora bezpečnosti sú porušené princípy kontrolného mechanizmu.

3.4 Model odtrhnutej bezpečnosti

Tento model predpokladá formálne i vecné postavenie CSO, ktorého zodpovednosť za garanciu bezpečnosti inštitucionálne potvrdzuje funkčná pozícia, ktorá je vyššia než akýkoľvek útvar s informačnou technológiou bezpečnosti, resp. CIO. Týmto sa vylučuje stret záujmov, tvorí sa bezpečnostná politika, ciele a kontrolujú sa výsledky. Odtrhnutím CSO od

[2]Modely sú založené na princípe informačnej technológie, ktorá poskytuje informácie pre zabezpečovanie procesov s aspektmi bezpečnosti podľa očakávaných výsledkov.

informačnej technológie však vzniká často problém zaostávania CSO od prudko sa rozvíjajúcej IT. Pokiaľ bezpečnostný manažér necitlivo komunikuje s pracovníkmi IT, títo ho postupne odizolujú a potom mnohé z toho, čo CSO vypracuje, ako napr. bezpečnostné smernice, predpisy i ciele sa postupne stávajú odtrhnutými od reality technológie. Niekedy stačí, ak CIO spochybní požiadavky CSO, prameniace z nedostatku technologických znalostí CSO, alebo nedostatku informácií, ktoré mu zámerne neposkytnú a je problém. Konflikty medzi pracovníkmi IT a CSO sa postupne riešia rozširovaním útvaru CSO o špecialistov príslušných bezpečnostným podsystémov. Týka sa to tak BOZP, ako aj fyzickej ochrany, environmentálneho manažérstva, ekonomiky, kvality, či výpočtových stredísk, atď. Ďalšie zmierňovanie konfliktov môže nastať formálnou akceptáciou inštitucionálneho postavenia CSO, menovaného vedením podniku a prípadne i samostatným miestom v rozpočtových kapitolách podniku. Najsilnejší vplyv na pozíciu bezpečnosti podniku však i pri formálnosti ostáva na pleciach osobnosti CSO.

3.5 Model utopenej bezpečnosti

Model utopenej bezpečnosti predpokladá tiché skrytie CSO pod krídla CIO v prípadoch prirodzeného vývoja modelu minimálnej technologickej bezpečnosti, kedy napr. osobnosť IT po skúsenostiach, ktoré nadobudol pri koordinácii bezpečnosti priamo v IT a zvládnutí manažérskych úloh prevezme prirodzene pozíciu CSO a pritom zostane CIO. V podsystéme manažérstva kvality tak postupným vývojom z technického kontrolóra kvality sa stane manažér kvality i zmocnenec kvality v jednej osobe, alebo vo výpočtovom stredisku sa zo zamestnanca IT postupne stane CIO a CSO v jednej osobe, čo i pri istom konflikte záujmov je tento model pre ďalší rozvoj bezpečnosti výhodnejší ako model odtrhnutej bezpečnosti.

3.6 Model agilnej bezpečnosti

Agilná bezpečnosť podniku, typická pre stredne veľké podniky, sa zabezpečuje cestou IT samotných procesov, aj prostredníctvom vplyvu ďalších manažérov, zodpovedných za menovité parciálne zložky bezpečnosti, napr. za fyzickú, personálnu, ekologickú, informačnú bezpečnosť a pod. V podniku je vytvorená bezpečnostná rada (Security Board), tvorená z príslušných manažérov bezpečností jednotlivých aspektov komplexnej bezpečnosti podniku a bezpečností IT, na čele ktorej stojí bezpečnostný manažér (CSO), podriadený priamo generálnemu riaditeľovi podniku (CEO). Členmi bezpečnostnej rady, kolektívneho orgánu bezpečnosti, môžu byť menovaní aj ďalší experti podniku alebo externí členovia významných a relevantných inštitúcií. Má funkciu legislatívnu (tvorba predpisov a dokumentácií), kontrolnú (zisťovanie stavu implementovaných opatrení) a riadiacu (v prípade havarijných stavov a mimoriadnych bezpečnostných incidentoch).
Model agilnej bezpečnosti predstavuje svojim spôsobom model integrácie jednotlivých bezpečnostných podsystémov, pričom bezpečnostná rada dbá na to, aby jednotlivé procesy prebiehali v duchu systému manažérstva kvality (ISO 9001:2008), s akcentom na ďalšie aspekty bezpečného podniku, akými sú napr. aspekty environmentálneho manažérstva (ISO 14001:2004), manažérstva BOZP bezpečnostné riziká BOZP (OHSAS 18001:2007), bezpečnosti informačných systémov (ISO 27001:2005), prípadne špecifických požiadaviek bezpečnosti, napr. vo výrobe dielov pre automobilový priemysel technické špecifikácie a požiadavky (ISO/TS 16949:2002), metrologické požiadavky (ISO 10012:2003), či kalibračné požiadavky (ISO/IEC 17025:2005) a ďalšie. Všetky citované medzinárodné štandardy sú generickými normami, vychádzajúcimi z normy manažérstva kvality ISO 9000:2000.

3.7 Model outsorcovanej bezpečnosti

Model outsorcovanej bezpečnosti predstavuje model dodávok takých technológií, v ktorých je otázka ich bezpečnosti inherentne zakomponovaná. Je však zrejmé, že v podniku musí existovať osoba, zodpovedná za koordináciu IT. Technologická bezpečnosť musí mať oporu v bezpečnostnej politike odberateľa a táto politika musí byť premietnutá aj do politiky dodávateľa so všetkými dôsledkami zodpovednosti za dodávaný produkt v zmysle požiadaviek ISO 9001:2008.
Na bezpečnostného manažéra podniku sú kladené veľké nároky, pretože musí zabezpečovať definovanú bezpečnosť dodávateľských služieb a koordinovať ju so všetkými procesmi vo vnútri podniku. Vo svojej pozícii je osamotený ako v prípade modelu odtrhnutej bezpečnosti s výhodou možnosti expertných posudkov podnikových expertov a špecialistov. Prípad outsorcovanej bezpečnosti je aj prípad externých služieb súkromných bezpečnostných služieb (SBS) pre výkon fyzickej ochrany osôb a majetku podniku ako parciálnej zložky komplexnej bezpečnosti podniku.

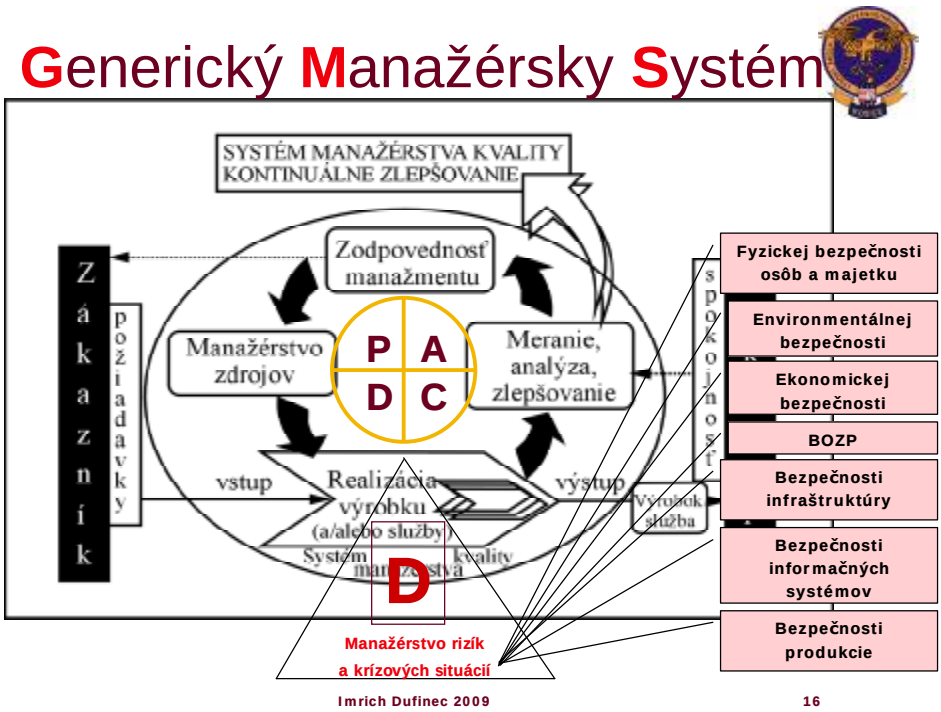
3.8 Model rozsiahlej inštitucionálnej bezpečnosti

Veľké podniky a inštitúcie ako sú banky, silové rezorty a pod. majú organizačnú štruktúru pomerne zložitú a tomu primerane prispôsobenú bezpečnosť, ktorá predstavuje neodmysliteľnú súčasť ich podnikania, či činností. V týchto inštitúciách a podnikoch existujú profesionálne bezpečnostné útvary, profesne špecializované a priebežne udržiavané na požadovanú úroveň spôsobilosti. Tento model môže byť rozvinutý do formy rozvinutej formálnej bezpečnosti, pričom bezpečnostný manažér (CSO) vedie a riadi rozsiahly bezpečnostný útvar technologickej bezpečnosti a ochrany, alebo do formy agilnej bezpečnosti, tvorenej relatívne nezávislými bezpečnostnými útvarmi technologickej bezpečnosti a ochrany, riadenými vrcholovým bezpečnostným manažérom (CSO). Bezpečnosť takéhoto podniku je plne procesne formalizovaná a je budovaná podľa štandardov a odporúčaní, ktoré boli pre ne vybrané ako najvhodnejšie a stávajú sa záväznými. V týchto inštitúciách je na pomerne vysokom stupni zabezpečovaná aj osobná bezpečnosť a bezpečnosť osobných údajov zamestnancov i klientov.

4. KOMPLEXNÁ BEZPEČNOSŤ PODNIKU

V komplexnej bezpečnosti podniku vystupujú jej parciálne zložky ako výsledok kvality riadenia procesov v danom systéme[3], pričom bezpečnostný aspekt tohto riadenia kvality je manažérstvo rizík relevantných procesov podniku[4].
Reálne to môže nastať vtedy, ak vedenie podniku vyhlási takú bezpečnostnú politiku, ktorá inštitucionalizuje a legalizuje do organizačnej štruktúry niektorého z modelov riadenia bezpečnosti manažérsky systém, v najlepšom prípade odvodený od procesného systému manažérstva kvality podľa ISO 9000:2000 ako Generický Manažérsky Systém. Schéma takéhoto systému založeného na základnom systéme manažérstva kvality podľa ISO 9000 a princípoch riadenia rizík a krízových javov podľa ISO 3100 je znázornená na nasledujúcom obrázku č. 1[5].

[3] Procesný prístup manažérstva kvality
[4] Kvalita je kategória technicko-ekonomická a jej riadenie podľa ISO 9001:2008 predpokladá riadenie rizík podľa ISO 31000
[5] DUFINEC Imrich: *Príspevok kvality k celkovej bezpečnosti podniku* [2]



Obr. 1 – Generický manažérsky systém bezpečnosti podniku [2]

Generický systém má fungovať na podklade základnej normy ISO 9001, pričom z generických noriem preberá riešenie tých aspektov, ktoré sú pre parciálnu bezpečnosť relevantné, najmä teda environmentálne aspekty a bezpečnostné riziká. Tie sa manažujú podľa špecifických štandardov, riziká podľa ISO 31000 a ďalších, platných pre jednotlivé oblasti alebo parciálne zložky bezpečnosti, napr. riziká BOZP v stavebníctve, ochrana osôb a majetku cez zákon o SBS, atď. Čo ostáva v GMS bez zmien za každých okolnosti je ISO 9001. Tá pracuje v štyroch klastroch procesov (kap. 5 – Zodpovednosť, 6 – Zdroje, 7 – Realizácia produktu, 8 – Meranie, analýza a zlepšovanie), pričom v procese neustáleho zlepšovania systému v cykle PDCA[6] je ťažisko vykonávania (D – Do) sústredené do realizácie produktu, to je klaster 7 a ak pozrieme na štruktúru klastra realizácie, ten začína podľa ISO 9001 plánovacími krokmi (kap.7.1, 7.2), vrátane vývoja (kap. 7.3), pokračuje ozajstnou realizáciou (kap. 7.4, 7.5) a končí spätnou väzbou cez technické prostriedky merania (kap. 7.6). Takže implementáciu a riešenie všetkých rizík vykonávame v realizácii produktu. Tam aplikujeme aj všetky realizačné nástroje (napr. APQP, FMEA, DOE,...) ale i všetky požiadavky plynúce z legislatívy a požiadaviek tretích strán, čo sa premietne v dokumentovaných postupoch realizácie. Bezpečnostná politika, ako akt plánovania (P) bezpečnosti je v klastri 5 – Zodpovednosť (kap. 5.3 – Politika), kontrola a audit ako akty spätnej väzby a preverovania (C) sú v klastri 8 – Meranie, analýza a zlepšovanie a napokon aktualizácia (A) i (nové) plánovanie systému ako výsledok preverovania je v klastri 8 ako nápravné opatrenia a v klastri 5 ako preventívne opatrenia (zmena politiky, cieľov, napr. aj akceptovateľných rizík, atď.), sú časťami cyklu nového zlepšovania systému. Tieto zlepšenia prejdú cez politiku, ciele a realizačné akty opäť do realizácie produktu ako kvalitatívne vyššia úroveň. Čím dokonalejšia integrácia, čím podrobnejšie inštitucionálne zabezpečenie fungovania GMS, tým je bezpečnosť (podniku) vyššia, vo všetkých jej parciálnych zložkách.

[6] Plan – Do – Check – Act (Demingov cyklus zlepšovania, ISO 9001:2000)

Takto riadený systém nadobúda charakter bezpečnostného manažérskeho systému[7].
Manažérstvo bezpečnostného systému je založené na manažérstve rizík, t.j. na postupe, čo a ako vykonať aby nedošlo k nežiaducim javom a udalostiam a manažérstve krízových situácií, t.j. na postupe, čo a ako konať, ak došlo k nežiaducemu javu alebo udalosti [4].
Model bezpečnosti podniku ako projekt bezpečnostného manažérskeho systému vychádza z bezpečnostnej politiky, ktorá môže byť ovplyvňovaná vonkajšími a vnútornými vplyvmi, napr. od bezpečnostnej politiky štátu po finančné možnosti a orientáciu vlastníkov podniku[8].

5. ZÁVER

Aktuálnosť problematiky organizovania bezpečnosti podnikov je v dôsledku globálnej finančnej krízy znásobovaná, pričom otvára nové cesty rizík a ohrození nielen podnikov samotných ale celej makroekonomickej sféry. Znalostná ekonomika podporuje rozvoj vzdelávania, vedy a výskumu za účelom efektívneho využívania disponibilných zdrojov orientovaných na trvalo udržateľný rozvoj. Efektívne riadenie podniku vo všetkých aspektoch jeho bezpečnosti podporuje túto výzvu v značnom rozsahu, pretože ekonomický dopad bezpečnostných incidentov nechránených alebo slabo chránených aktív sa priamo alebo nepriamo dotýka práve týchto zdrojov.

LITERATÚRA

[1] DUFINEC, I. – ČALFOVÁ, M. *On a Security of Business in a Reflex of Knowledgeable Economic*. In *Internet, Competitiveness and Organisational Security in Knowledge Society*, Zborník príspevkov medzinárodnej vedeckej konferencie, Universita Tomáše Bati Zlín, 2009. ISBN 978-80-7318-828-3
[2] DUFINEC, Imrich *Príspevok kvality k celkovej bezpečnosti podniku*. In *Zborník príspevkov pedagogického seminára KVALITA PRODUKCIE*, Technická univerzita v Košiciach, Košice – Herľany, 2009. ISBN 978-80-553-0238-6
[3] DUFINEC, Imrich. *Bezpečnosť produktu ako aspekt jeho kvality*. In *Zborník príspevkov 2. medzinárodnej vedeckej konferencie*, VŠBM Košice 2008, s.59-65. ISBN 978-80-89282-28-9
[4] MESÁROŠ, M. – HRÁDOCKÝ, L. – DUFINEC, I. – KRIŽOVSKÝ, S.: *Podnikové manažérstvo*. VŠBM Košice, 2007, str. 115. ISBN 978-80-89282-15-9
[5] RAK, R. - PORADA, V. – LOŠONCZI, P.: *Kvalifikační předpoklady bezpečnostního manažéra a jeho profesní potřeby, začlenění v organizaci*. Zborník z medzinárodného odborného vedeckého seminára, VŠBM Košice, 2007, str. 52-84. ISBN 978-80-89282-19-7

Článok recenzovali:

Prof. Ing. **Hana Pačaiová**, PhD. – Technická univerzita v Košiciach
Strojnícka fakulta, Katedra bezpečnosti a kvality

Prof. Ing. J**ozef Reitšpís**, PhD. – Žilinská univerzita v Žilne
Fakulta špeciálneho inžinierstva

[7] DUFINEC, I. – ČALFOVÁ, M: *Bezpečnosť podniku vo svetle znalostnej ekonomiky* [1]
[8] DUFINEC, I. – ČALFOVÁ, M: *Bezpečnosť podniku vo svetle znalostnej ekonomiky* [1]