FBIM Transactions
DOI 10.12709/fbim.07.07.02.06

MODEL UPRAVLJANJA BEZBEDNOSNIM RIZIKOM

SECURITY RISK MANAGEMENT MODEL

Nemanja Jovanov
Poslovni i pravni fakultet, Univerzitet „Union – Nikola Tesla”, Beograd, Srbija

Nikola Glođović
Kriminalističko policijska akademija-Beograd, Beograd, Srbija

Goran Jovanov
Kriminalističko policijska akademija-Beograd, Beograd, Srbija

JEL Kategorija rada: **D81, G32**

Apstrakt

Danas u svetu ima više razvijenih modela za upravljanje bezbednosnim rizikom, a u ovom radu će biti predstavljen model sa osam faza. Faza „Identifikacija poslovnog sistema treba da identifikuje sve objekte poslovnog sistema, aktivnosti koje se u njemu realizuju i zaposlene radnike, jer oni potencijalno mogu biti ugroženi nekom opasnošću. Znači, neophodno je izvršiti procenu zašto i kako bi potencijalni nepredviđeni događaj uticao na poslovni sistem i sve njegove resurse, a takođe treba da se utvrdi da li potencijalni nepredviđeni događaj koji bi mogao prouzrokovati određenu opasnost predstavlja događaj koji bi ostvario štetu koju poslovni sistem ne sme sebi da dozvoli, ili je za njega konkretni potencijalni događaj zanemarljiv. U fazi „Procena opasnosti“ vrši se predviđanje potencijalnih specifičnih opasnosti i situacija u kojima bi one mogle da se dese. U ovoj fazi se znači ne realizuje procena bezbednosnog rizika, ali se dolazi do potrebnih informacija i smernica koje će se koristiti za procenu. „Procena ranjivosti“ je faza modela upravljanja bezbednosnim rizikom u kojoj se trebaju prepoznati snaga i slabosti poslovnog sistema po pitanju bezbednosnih mera koje štite isti od uticaja iz okruženja. U narednoj fazi se realizuje procena bezbednosnog rizika. Vrši se kombinovanje svih raspoloživih relevantnih (direktnih i indirektnih) informacija po pitanju bezbednosti, kako bi se uspeo identifikovati potencijalni uticaj i verovatnoća pojave potencijalne opasnosti po poslovni sistem, tj. dobili trenutni nivo bezbednosnog rizika. U fazi „Bezbednosne mere i strategije“ realizuje se razvoj i stvaranje istih, kako bi se njihovom primenom ostvarilo smanjenje verovatnoće pojave bezbednosnog rizika i njegovog štetnog (opasnog) uticaja. U fazi „Donošenje odluke“ neophodno je da se donesu odluke po pitanju prioriteta, logističke podrške, vremenskih rokova, finansija, itd. Ova faza se realizuje u tri koraka, i to: (1) procedure za

Adresa autora:
Nemanja Jovanov
nemanjjajovanov@gmail.com

smanjenje bezbednosnog rizika na prihvatljiv nivo, (2) utvrđivanje prioriteta, i (3) odobravanje finansija i potrebnih resursa. Posle ove faze realizuje se po ovom modelu priprema i implementacija razvijenih bezbednosnih mera. Na kraju se vrši ocena svega što je urađeno, realizuju se potencijalno potrebne korekcije i vrše se pripreme za buduću modernizaciju bezbednosnih mera i strategija.

***Ključne reči**: Identifikacija, bezbednosni rizik,bezbednosne mere, strategija*

Abstract

Worldwide there are many developed models for managing security risks. Within this thesis, the developed model with eight phases will be represented. The phase "Business System Identification" should identify all objects of a business system, the activities realized within it, and employees, because these potentially can be jeopardized by some threat. Therefore, it is necessary to make an estimation why and how a potential unpredictable event could influence a business system and all of its resources, as well as it should be determined whether potential unpredictable event, which could cause certain threat, represents the event which would cause damage which business system must not allow, or a specific potential event is irrelevant for it. In the phase "Threat Estimation" potential specific threats and situations in which these may occur are predicted. In this phase, the security risk estimation is not made, but the necessary information and instructions that will be used for the estimate are gathered. "Vulnerability Estimation" is the phase of a security risk management model in which the strength and weakness of a business system should be recognized, related to security measures which protect the system from the surrounding influences. In the next phase, the security risk estimate is realized. All available, relevant (direct and indirect) security-related information are combined, in order to identify potential influence and the probability of the occurrence of a potential threat on the business system, i.e. to get the current level of security risk. In the phase "Security Measures and Strategies" their development and creation are realized, in order to accomplish the reduction of probable occurrence of security risk and its harmful (dangerous) influence by their application. In the phase „Decision Making" it is necessary to bring the decisions related to priorities, logistics support, timelines, financials, etc. This phase is realized in three steps, as follows: (1) Procedures for reducing the security risk to an acceptable level, (2) Priorities setting, and (3) Approving of financials and necessary resources. After this phase, the preparation and implementation of developed security measures are realized by this model. In the end, the evaluation of everything done is made, potentially, necessary corrections are realized, as well as the preparation for future modernization of security measures and strategies is made.

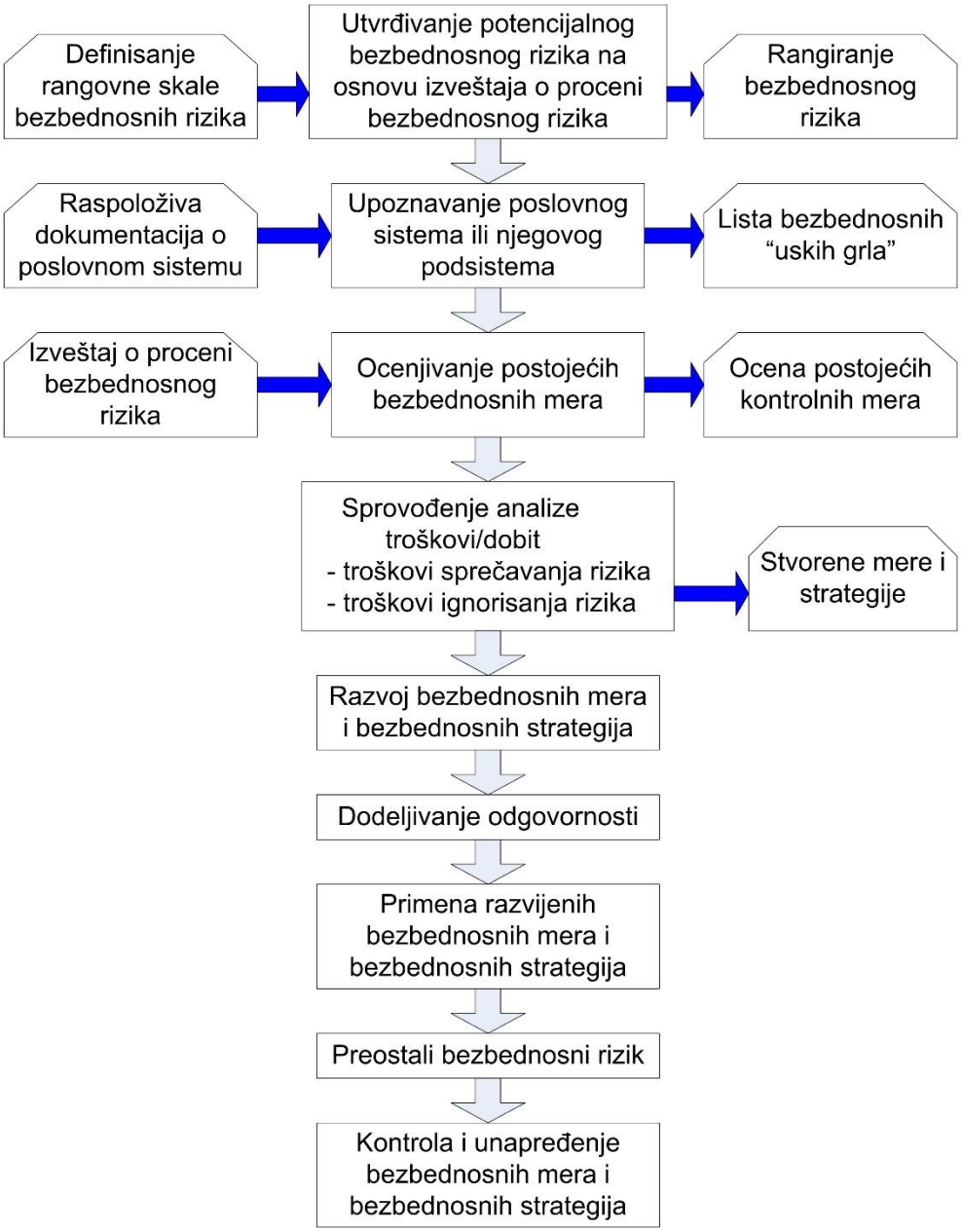
***Keywords:** identification, security risk, security measures, strategy*

1. UVOD

Vrlo je teško obezbediti apsolutnu sigurnost. Ako poslovni sistem nije fizički bezbedan, ništa što je u vezi sa istim ne može se smatrati bezbednim, uključujući zaposlene, tehničke sisteme, procese, dokumentaciju, finansijska sredstva poslovnog sistema, itd. Neki sigurnosni sistemi zahtevaju da pojedini tehnički sistemi (serveri, komunikacioni linkovi, itd.) u poslovnom sistemu budu naročito fizički obezbeđeni.

Standardi bezbednosnih rizika danas zahtevaju da poslovni sistemi obezbede kvalitetne i u skladu sa zakonom bezbednosne politike i procedure za otkrivanje i sprečavanje bezbednosnih rizika. Ukoliko se činjenicama argumentuje da bezbednosna politika poslovnog sistema nije primerena i/ili u skladu sa zakonom, poslovni sistem mora da na relevantan zahtev usvoji nove mere bezbednosne politike, koje će biti prihvaćene kao zadovoljavajuće.

Neki od bezbednosnih rizika su neznatni, a samim tim i zanemarljivi, dok drugi mogu imati štetne posledice koje su nedopustive za poslovni sistem. Procena bezbednosnih rizika pomaže u razvoju strategije bezbednosti i pruža osnovu za uspostavljanje isplativog bezbednosnog programa koji će minimizirati verovatnoću pojave bezbednosnog rizika, odnosno minimizirati efekte bezbednosnog rizika.



Slika.1. Metodologija za umanjenje bezbednosnog rizika

2. PROCENA BEZBEDNOSNOG RIZIKA

Za procenu bezbednosnog rizika možemo reći da je sastavni deo procesa upravljanja bezbednosnim rizicima i da ona predstavlja proces identifikacije opasnosti (koje bi mogle da utiču na zaposlene, procese u poslovnom sistemu ili materijalna sredstva poslovnog sistema), procene bezbednosnih rizika (po pitanju verovatnoće njihovog potencijalnog nastanka i uticaja), kao i utvrđivanje prioriteta tih bezbednosnih rizika i identifikovanje mera i strategija za njihovo sprečavanje, tj. umanjenje. U početnoj fazi procene bezbednosnog rizika, analitičari su nekada primorani da izvrše procenu bezbednosnog rizika (u nekim situacijama čak i da predlože bezbednosne mere i strategije za rešenje konkretnog bezbednosnog rizika) u odsustvu brojnih neophodnih parametara, što je nedopustivo. Metodologija za umanjenje rizika prikazana je šematski na slici 1 (Adamović, Jovanov, Radojević, & Meza, 2008, str. 128). Kako bi se identifikovao kritičan bezbednosni rizik koji zahteva kvalitetno bezbednosno rešenje najčešće se vrši rangiranje.

Rangiranje bezbednosnih rizika se vrši na osnovu relevantnih kriterijuma za poslovni sistem po pitanju mogućnosti poslovnog sistema da preuzme rizik. Kada se identifikuju i analiziraju ponuđena rešenja bezbednosnih rizika, vrši se njihovo ocenjivanje po pitanju efekata verovatnoće pojave i potencijalnih neželjenih događaja po poslovni sistem. Naravno, potencijalni neželjeni događaj nije jedini faktor koji utiče na odluku odabira rešenja između ponuđenih alternativa, jer različita rešenja mogu imati različite prateće posledice na poslovni sistem (npr. cenu proizvoda, nivo zarada zaposlenih, troškove zaštite životne sredine, itd.).

Izveštaj o proceni bezbednosnog rizika treba da kreira operativni menadžment jednog poslovnog sistema za potrebe višeg menadžmenta poslovnog sistema i vlasnika. Na osnovu dobijenog izveštaja, višem menadžmentu je u velikoj meri obezbeđen materijal koji mu je neophodan za donošenje ispravne i kvalitetne odluke o bezbednosnoj politici poslovnog sistema, bezbednosnim procedurama, budžetu za potrebe bezbednosti, sistemu upravljanja bezbednošću i određenim potencijalnim promenama u menadžmentu. Izveštaj o proceni bezbednosnog rizika treba da sadrži sledeće elemente: opšti pregled poslovnog sistema, tehničke sisteme poslovnog sistema, računarski hardver, softver, komunikacione linkove, analizu topologije računarske mreže, kritična mesta poslovnog sistema, metode sakupljanja podataka, analizu podataka, preporuke sigurnosnih mera, preporuke za strategije rešenja analiziranog bezbednosnog rizika, itd. (Vujović, 2003, str. 187).

3. MODEL UPRAVLJANJA BEZBEDNOSNIM RIZIKOM

Danas u svetu postoji više modela razvijenih za upravljanje bezbednosnim rizikom, a u ovom radu će se prikazati razvijeni model sa osam faza (slika 2).

Faza „Identifikacija poslovnog sistema“ treba da identifikuje sve objekte poslovnog sistema, aktivnosti koje se u njemu realizuju i zaposlene radnike, jer oni potencijalno mogu biti ugroženi nekom opasnošću. Znači, neophodno je izvršiti procenu zašto i kako bi potencijalni nepredviđeni događaj uticao na poslovni sistem i sve njegove resurse, a takođe treba da se utvrdi da li potencijalni nepredviđeni događaj, koji bi mogao prouzrokovati određenu opasnost, predstavlja događaj koji bi ostvario štetu koju poslovni sistem ne sme sebi da dozvoli, ili je konkretni potencijalni događaj zanemarljiv za sistem.

U fazi „Procena opasnosti“ vrši se predviđanje potencijalnih specifičnih opasnosti i situacija u kojima bi one mogle da se dese. U ovoj fazi se ne realizuje procena bezbednosnog rizika, ali se dolazi do potrebnih informacija i smernica koje će se koristiti za procenu.

„Procena ranjivosti“ je faza modela upravljanja bezbednosnim rizikom u kojoj treba prepoznati snagu i slabosti poslovnog sistema u pogledu bezbednosnih mera koje štite isti od uticaja iz okruženja (Starčević, Ilić, & Paunović-Pfaf, 2010, str.78).

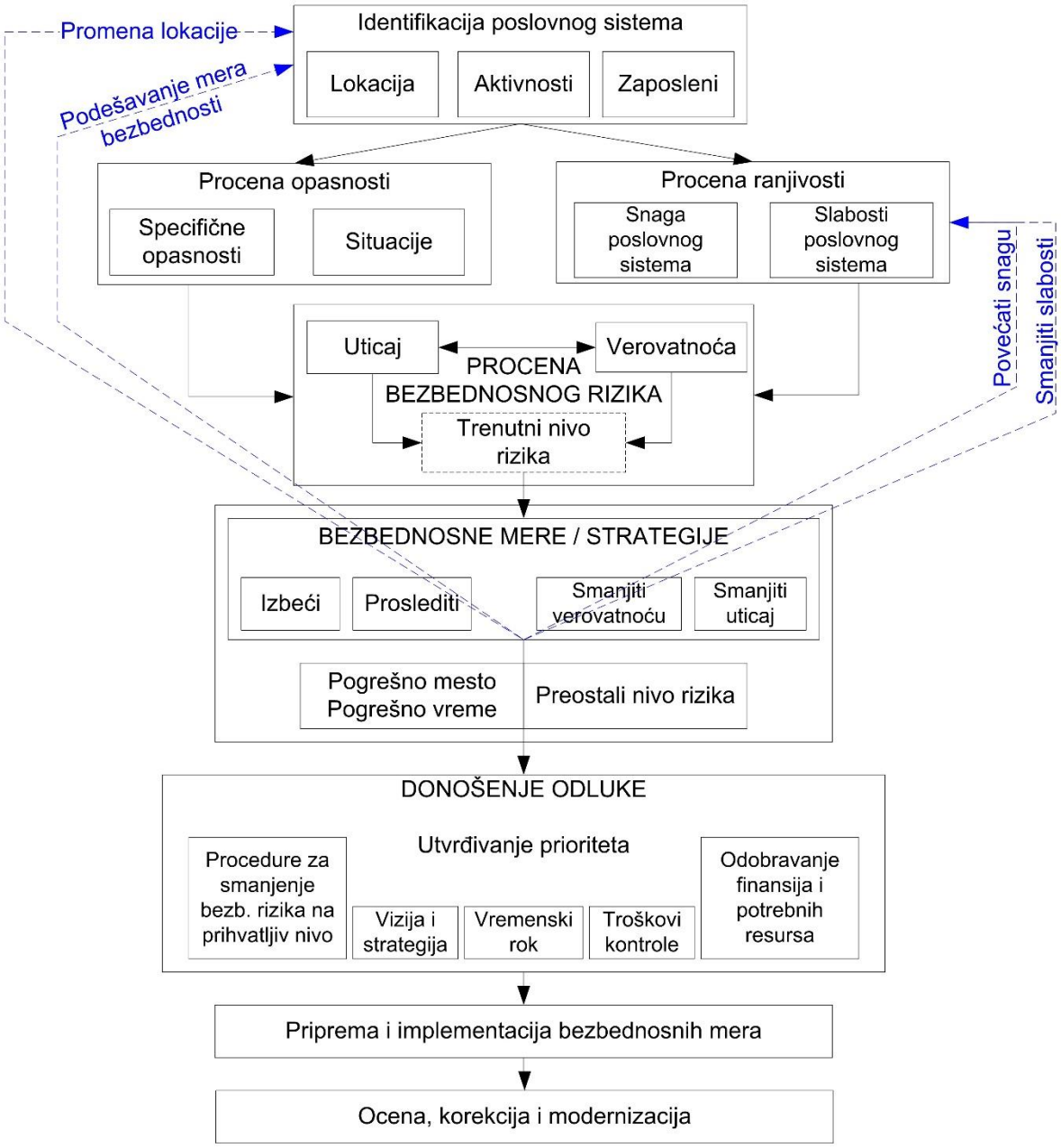
U narednoj fazi se realizuje procena bezbednosnog rizika. Vrši se kombinovanje svih raspoloživih relevantnih (direktnih i indirektnih) informacija po pitanju bezbednosti, kako bi se identifikovali potencijalni uticaj i verovatnoća pojave potencijalne opasnosti po poslovni sistem, tj. dobili trenutni nivo bezbednosnog rizika.

U fazi „Bezbednosne mere i strategije“ realizuje se razvoj i stvaranje istih, kako bi se njihovom primenom ostvarilo smanjenje verovatnoće pojave bezbednosnog rizika i njegovog štetnog (opasnog) uticaja.

U fazi „Donošenje odluke“ neophodno je da se donesu odluke po pitanju prioriteta, logističke podrške, vremenskih rokova, finansija, itd. Ova faza se realizuje u tri koraka, i to:

1. procedure za smanjenje bezbednosnog rizika na prihvatljiv nivo,
2. utvrđivanje prioriteta, i
3. odobravanje finansija i potrebnih resursa.

Posle ove faze realizuju se po ovom modelu priprema i implementacija razvijenih bezbednosnih mera (Adamović, Voskresenski, & Tul, 2007, str. 48).



Slika 2. Model upravljanja bezbednosnim rizikom

Na kraju se vrši ocena svega što je urađeno, realizuju se potencijalno potrebne korekcije i vrše se pripreme za buduću modernizaciju bezbednosnih mera i strategija.

Uzroci nastanka štetnog događaja su slučajni tako da su i štetni događaji slučajne pojave koje možemo modelirati i definisati zakonima verovatnoće.

Mogućnost da se šteta dogodi može se predstaviti na dva načina. Objektivan način je razlomak u kome je brojilac predstavljen brojem jedinica koje su pretrpele, ili za koje se očekuje da će pretrpeti štetu, a imenilac je predstavljen ukupnim brojem jedinica izloženih mogućem dejstvu štetnog događaja.

Objektivna ocena mogućnosti, zasnovana na verovatnoći, odnosi se na dugoročnu relativnu učestalost događaja prema pretpostavkama beskonačnog broja posmatranja i na nepostojanju izmene u datim uslovima.

U poslovnim industrijskim sistemima štetni događaj može biti u oblasti procesa rada

(oslobađanje štetnih materija kao što su to razne hemikalije ili radioaktivnost, prašina, dim, velika buka i vibracije, oslobađanje mikroorganizama, oslobađanje raznih alergenata, emitovanje štetnog nivoa energije iz industrijskih objekata ili opreme u čovekovu okolinu, itd.) Ovo se obično dešava u obliku eksplozije, požara, prosipanja, iscurivanja ili otpada. Ovakvi štetni događaji mogu nastati kao posledica faktora koji su unutrašnji u nekom industrijskom sistemu (tj. ljudski faktor), ili kao posledica spoljašnjih faktora (ekstremni događaji u prirodi). Oslobađanja mogu da budu iznenadna i intenzivna kao što je to eksplozija, ili postepena i opsežna kao što je to ispuštanje materijala u stratosferu koje uništavaju ozonski omotač, ili pak dugotrajno oticanje toksičnih materija koji nisu uništeni ili odloženi na odgovarajući način (na primer, oticanje otpadnih voda iz deponija u unutrašnjost zemlje pri čemu dolazi do zagađivanja podzemnih voda).

Pored štetnih događaja koji se mogu javiti u oblasti procesa rada jednog poslovnog sistema, imamo i štetne događaje koji se mogu dogoditi i kao posledica psihičkih i psihofizičkih napora (npr. stres na radnom mestu, monotonija radnih aktivnosti, psihička naprezanja usled velikog stepena odgovornosti, dugotrajno stajanje, dugotrajno sedenje dugotrajno klečanje, ručno guranje, nošenja ili vučenje velikog tereta, itd.), kao posledica loše organizacije rada (npr. neadekvatna organizacija rada zaposlenih u smenama, učestali rad u noćnoj smeni, čest prekovremeni rad, itd.), kao posledica rada u atmosferi sa visokim ili niskim pritiskom, kao posledica rada u blizini vode ili ispod površine vode, itd. (George, 2005, str.145).

Uzroci nastanka štetnog događaja su slučajni tako da su i štetni događaji slučajne pojave koje možemo modelirati i definisati zakonima verovatnoće. Uzroke štetnih događaja možemo grupisati u dve grupe a to su:

1. potencijalno predvidivi (koji se nalaze u propustima praktične primene, zakonima i tehničkim standardima, propisanim merama preventivne zaštite i sl.), i
2. potencijalno nepredvidivi (pojavne oblike nije moguće predvideti u realnom vremenu).

Pošto su svi faktori koji izazivaju štetni događaj, najčešće slučajnog karaktera, to je i štetni događaj u osnovi slučajna kategorija koja se pokorava zakonima verovatnoće. Drugim rečima, štetni događaji su neminovni i ne mogu se nikada potpuno sprečiti, ali verovatnoća njihovog nastanka može biti manja ili veća. Otuda i veoma dobar stav da su svi štetni događaji normalni, što znači da je mogućnost pojave štetnih događaja ugrađena u samu strukturu složenih sistema, te da se štetni događaji ne mogu potpuno sprečiti boljim konstrukcijama, kvalitetnijim informacijama ili pametnijim, odnosno boljim rukovodiocima, projektantima, inženjerima, radnicima.

Da bi se sagledao uticaj štetnih događaja na privredu neke zemlje potrebno je navesti da samo u štetnim događajima koji su posledica požara naša zemlja nepovratno gubi oko 2% bruto materijalnog proizvoda. Ostali štetni događaji samo povećavaju ovaj, nažalost poražavajući rezultat. Vrste i pojavni oblici štetnih događaja su brojni, raznorodni i često međusobno uzročno-posledični.

4. ZAKLJUČCI

Poslovanje savremenih proizvodno poslovnih sistema se odvija, u složenim, neizvesnim i dinamičnim uslovima koji zahtevaju stalne inovacije i promene. Uvođenje inovacija kroz inovativnost, inventivnost i kreativnost zaposlenih može znatno uticati na oblast menadžmenta rizicima u proizvodno poslovnim sistemima, što svakako zahteva novo znanje i veštine kod zaposlenih.

Posebnu pažnju treba posvetiti onim situacijama i scenarijima događaja u privrednim sistemima, a naročito u njihovim proizvodnim pogonima, koji kao posledicu mogu imati povrede na radu radnika, invalidnost, a u nekim slučajevima i katastrofalnu posledicu po zaposlenog, tj. smrt. Ove neželjene situacije, odnosno vanredne i akcidentne situacije mogu ostaviti štetne posledice kako po zaposlene radnike, privredni sistem, tako i po njegovo okruženje (lokalno, a u nekim slučajevima i daleko šire).

U svakom slučaju, prosečan broj povreda na radu u odeljenju održavanja je procentualno veći nego u proizvodnom delu, jer je broj radnika u odeljenju održavanja daleko manji. I zbog same prirode posla, radnici funkcije održavanja su izloženiji akcidentnim situacijama. Opravdano je tvrditi da

je rad na održavanju tehničkih sistema mnogo opasniji nego rad u proizvodnom sektoru.

Evidentna je korelacija između stepena tehnološke razvijenosti i broja akcidenata. Što je viši stepen tehnološkog razvoja, to je veći procentualni udeo aktivnosti održavanja, tj. veći je i broj akcidentnih situacija koje se javljaju tokom sprovođenja ovih aktivnosti.

Proizvodni pogoni sa aktivnostima održavanja baziranim na kriterijumu rizika imaće manju frekventnost akcidentnih situacija, a samim tim i manji broj izgubljenih radnih dana zbog povreda radnika na radu

REFERENCE

Adamović, Ž., Jovanov, G., Radojević, M., & Meza, S. (2008). *Upravljanje rizikom.* Univerzitet u Novom Sadu. Tehnički fakultet „Mihajlo Pupin“, Zrenjanin.

Adamović, Ž., Milošević, Ž., Popović, L., & Adamović, M. (2008). *Modeli održavanja na bazi rizika*. Društvo za energetsku efikasnost Bosne i Hercegovine, Banja Luka.

Adamović, Ž., Voskresenski, V., & Tul, R., (2007). *Održavanje na bazi rizika*. TEHDIS, Beograd

George, E. Rejda. (2005). *Principles of Risk Management and Insurance*. Ninth Edition, Addisom Wesley, Boston.

Starčević, J., Ilić, M., & Paunović-Pfaf, J. (2010) *Priručnik za procenu rizika*, Globe Design, Beograd.

Vujović, R., Jovanović, S., & Todorović, J. (2003). Unapređenje metoda upravljanja rizikom u industrijskim postrojenjima, *Tokovi osiguranja*, (1-2).

Datum prve prijave: 10.09.2018.
Datum prijema korigovanog članka: 11.07.2019.
Datum prihvatanja članka: 11.10.2019.

Kako citirati ovaj rad? / How to cite this article?

*Style – **APA** Sixth Edition:*

Jovanov, N., Glođović, N., & Jovanov, G. (2019, 10 15). Model upravljanja bezbednosnim rizikom. (Z. Čekerevac, Ed.) *FBIM Transactions, 7*(2), 52-58. doi:10.12709/fbim.07.07.02.06

*Style – **Chicago** Sixteenth Edition:*

Jovanov, Nemanja, Nikola Glođović, and Goran Jovanov. 2019. "Model upravljanja bezbednosnim rizikom." Edited by Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (2): 52-58. doi:10.12709/fbim.07.07.02.06.

*Style – **GOST** Name Sort:*

Jovanov Nemanja, Glođović Nikola and Jovanov Goran Model upravljanja bezbednosnim rizikom [Journal] // FBIM Transactions / ed. Čekerevac Zoran. - Beograd : MESTE, 10 15, 2019. - 2 : Vol. 7. - pp. 52-58.

*Style – **Harvard** Anglia:*

Jovanov, N., Glođović, N. & Jovanov, G., 2019. Model upravljanja bezbednosnim rizikom. *FBIM Transactions,* 15 10, 7(2), pp. 52-58.

Style – **ISO 690** Numerical Reference:

Model upravljanja bezbednosnim rizikom. **Jovanov, Nemanja, Glođović, Nikola and Jovanov, Goran.** [ed.] Zoran Čekerevac. 2, Beograd : MESTE, 10 15, 2019, FBIM Transactions, Vol. 7, pp. 52-58.