M. Bešker, A. Bešker, N. Markulin Grgić*

TRODIMENZIONALNI MODEL PROCESNOG UPRAVLJANJA SIGURNOŠĆU INFORMACIJA

UDK 330.33:316.776
PRIMLJENO: 31.3.2021.
PRIHVAĆENO: 8.2.2022.

SAŽETAK: U radu se daje prikaz pristupa upravljanju sigurnosti informacija utemeljenog na rizicima te multivarijatnoj analizi s više aspekata uz definirane kriterije i težište na preventivno i proaktivno upravljanje rizicima. Sigurnost informacija sustava upravljanja izravno ovisi o upravljanju rizicima poslovanja. Iz tih razloga norma ISO 9000:2015 rizik definira kao učinak nesigurnosti, tj. odstupanje od očekivanog – u pozitivnom ili negativnim smislu, što znači stupanj ostvarenja ciljeva poslovanja. Norma ISO 9001:2015 prvenstveno zahtijeva da se preventivno upravlja rizicima poslovanja pa i informacija ne uvjetujući metode i modele upravljanja. S druge strane norma ISO 31000 (Sustavi upravljanje rizicima) zagovara pored preventivnog i proaktivno upravljanje rizicima poslovanja. Taj zahtjev je veoma opravdan jer omogućava da se pravovremeno reagira na pojave bilo kakvih ugrožavanja informacija. Preduvjeti učinkovite primjene pristupa upravljanju utemeljenom na rizicima je dodatna osposobljenost menadžmenta i raspolaganje alatima (softver) za multivarijatnu analizu rizika.

Ključne riječi: *upravljanje sigurnošću informacija, upravljanje utemeljeno na rizicima, upravljanje rizicima poslovanja, preventivno upravljanje rizicima, proaktivno upravljanje rizicima*

UVOD

Rizične životne situacije pratitelj su razvoja ljudskih zajednica. Rizik je stanje nesigurnosti koje je čovjeka pratilo kroz povijest i s njome se svakodnevno susretao. Pračovjek je bio lovac i na taj način osiguravao je hranu da bi prehranio zajednicu. Pri tome se suočavao s raznim ugrožavanjima. Živio je u špiljama jer je imao osjećaj da mu one pružaju dovoljnu zaštitu – dobro stanje sigurnosti.

Sa stupnjem razvoja ljudskih zajednica razvijali su se određeni organizirani oblici zaštite koji su umanjivali rizike, a povećavali su ukupnu sigurnost. Pored rizika koje su izazivale prirodne pojave javljaju se i društveni rizici kao napadi od strane organiziranih skupina i neprijateljskih zajednica. Da bi se umanjio rizik od takvih napada, gradile su se zaštitne utvrde, uspostavljala su se promatranja kretanja neprijatelja i razvijala se izrada oružja i oruđa za obranu.

Spominje se[1] da su oko 32. stoljeća pr. Kr. u dolini Eufrata i Tigrisa živjeli ljudi koji su se zvali Asipu. Davali su savjete kako se treba suprotstaviti rizicima. Njihovi savjeti su se odnosili na ženidbe, trgovinu, izgradnju objekata i sl. U izradi procjene rizika koristili su prikupljanje podataka o problemu, razvijali scenarij razvoja događaja i procjenjivali posljedice tih događaja. Zapisivali su moguće posljedice događaja i prema naklono-

*Prof. dr. sc. Marko Bešker, (marko.besker@oskar.hr), EOQ menadžer rizika, Anita Bešker, prof., EOQ menadžer rizika, (anita.besker@oskar.hr), Oskar, Centar za razvoj i kvalitetu d.o.o., Zagreb, Hrvatska, Nataša Markulin Grgić, dipl. ing., EOQ menadžer kvalitete, (natasa.markulin-grgic@ina.hr), INA d.d. Zagreb, Hrvatska.

[1]Covello, V. T. and Mumpower, J.: Risk Analysis and Risk Management an Historical Perspective, 1984..

sti bogova govorili o pozitivnom ili negativnom ishodu budućih događanja. Na kraju su izrađivane preporuke klijentu što treba činiti da bi se rizici umanjili.

Zabilježeno je da su se u starom Babilonu (od 24. stoljeća pr. Kr.) izrađivale procjene rizika. To je uvjetovano stalnom opasnošću od pljačke u transportu roba. Zbog organiziranih pljački u transportu roba trgovci su od transportera za izgubljenu robu tražili jamčevine (svojevrsno osiguranje). Jamčevine za pojedine robe određivale su se na temelju vrijednosti robe i razine procijenjenih rizika. Ljudi koji su procjenjivali rizike i predviđali buduća događanja zvali su se proroci.

Prorok Izaija kaže „Kako su proroci nerijetko naviještali buduće događaje, danas se pod tim pojmom često pogrešno smatra osoba koje pretkazuje budućnost".

Iz navedenih povijesnih primjera može se zaključiti da su trenutačni izvori ugrožavanja utjecali na razvoj načina smanjivanja i sprečavanje rizika sve u cilju stvaranja sigurnijih uvjeta života.

U posljednjih 70 godina upravljanju rizicima pristupa se sustavno koristeći dokazane strategije, modele i metode analize i procjene rizika. Počeci sustavnog upravljanja rizicima veže se, od 1950. godine, za uspostavljanje funkcija upravljanja rizicima u poduzećima SAD-a. Organizacije su shvatile da je osiguranje kao dotadašnja strategija prenošenja rizika nedovoljna i manjkava te da treba više pozornosti zaštiti osigurane imovine i ljudi. Poduzeća su se počela baviti kvalitetom zaštite vrijednosti i rizicima zdravlja i sigurnosti te pitanjima odgovornosti za rizike proizvoda i usluga. Sve se više kombinira strategija prenošenja rizika sa strategijom smanjivanja rizika. U Europi tijekom 1970-ih koncept ukupnog troška rizika poslovanja postaje važan pa se pristupa sličnom modelu kao i u SAD-u. Posljedično "Orange Book from HM Treasury" definira upravljanje rizikom kao interakciju „Svih procesa koji su uključeni u identificiranje, analizu i procjenu rizika, dodjeljujući vlasništvo nad rizicima, poduzimanje mjera za njihovo ublažavanje ili smanjivanje, te nadzor i pregled napredaka."

Povijesno gledano, pojam upravljanja rizicima korišten je i primjenjivan samo na rizike opasnosti. Znanstvena disciplina „Upravljanje rizicima" je sada razvijena na način koji omogućava da se upravljanjem rizikom daje doprinos poboljšanju upravljanja rizikom opasnosti i rizikom prilika.

METODE KORIŠTENE U IZRADI MODELA I NAČINA ANALIZE I PROCJENE RIZIKA

Rad je nastao kao rezultat višegodišnjeg promatranja i analize praktičnih rješenja upravljanja sigurnošću kao elementa kvalitete poslovanja u organizacijama u kojima su autori dulje razdoblje sudjelovali kao savjetnici, predavači ili kao zaposlenici. Bilježeni rezultati iz prakse upravljanja sigurnošću uspoređivani su s teorijskim rješenjima i rješenjima danim kao zahtjevi ili smjernice ISO normi. Rađena je usporedba prakse upravljanja sigurnošću poslovanja i teorijskih te normativnih rješenja. Rezultati analiza i usporedbi upućivali su na potrebu izrade modela drugačijeg pristupa upravljanja rizicima i sigurnošću. Naime, skoro u svim analiziranim organizacijama, bilo ih je preko 150, osim banaka i osiguravajućih društava, posao upravljanja rizicima i sigurnošću poslovanja ne obavlja se profesionalno nego usputno bez definiranih vlasnika rizika, i to s vrlo malim znanjima iz ovoga područja. U područjima gdje je zakonska obveza procjena rizika, a time i upravljanje rizicima, u većini njih taj posao su obavile specijalizirane tvrtke koje se time bave, ali bez sudjelovanja menadžmenta organizacije u bilo kojem koraku procesa upravljanja rizicima. Implementacija takvih rješenja svodila se na puku formalnost. Organizacije su ostajale podjednako rizične kao da i nisu obavile te aktivnosti. Autori su niz godina tražili rješenja za pojedina pitanja koja se obrađuju u radu. U izradi modela multivarijatne analize rizika za sve uključene faktore provedena je funkcionalna analiza i simulacija njihova utjecaja na ukupni rizik. Pokazalo se da su svi analizirani faktori osim faktora otpornosti direktno proporcionalni s rizikom. Također se iz tih analiza dalo zaključiti da je pri izradi kriterija za ocjenu intenziteta faktora rizika pogodna skala 1 – 5, osim za faktor otpornosti gdje treba koristiti skalu u rasponu 1 – 3. Svi ti metodološki postupci omogućili su da se izrade konačna rješenja modela i metoda analize i procjene rizika poslovanja. Međutim, i dalje ostaje problem stavova menadžmenta organizacija o suvremenom pristupu upravljanju temeljenom na rizicima.

Novi pristup, koji se odnosi na prihvaćanje nove strategije, modela i metoda, traži nova znanja i alate koji mogu biti jedini pokretač promjena u upravljanju poslovanjem.

RASPRAVA I RJEŠENJA

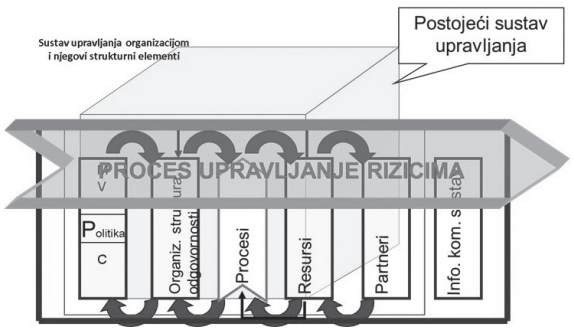
Rizik i sigurnost

U izradi ovoga rada koristi se pristup dan u normi ISO 9000:2015 u kojoj je rizik definiran kao *učinak nesigurnosti*, gdje se podrazumijeva da je učinak odstupanje od očekivanog – u pozitivnom ili negativnim smislu. Prema tome, može se reći da je sigurnost takvo stanje koje ima malu prisutnost rizika u organizaciji. Bez obzira na područje razmatranja problema upravljanje rizicima ključ je držanja rizika pod kontrolom. Norma ISO 9001:2015 utvrđuje zahtjev da organizacija shvati svoj kontekst i utvrdi rizike kao osnovu za planiranje. To podrazumijeva primjenu *pristupa utemeljenog na rizicima* na planiranje i provedbu procesa sustava upravljanja kvalitetom. Isti zahtjevi trebaju se primijeniti na sve sustave upravljanja uključivo i upravljanje sigurnošću informacijskih sustava. Zbog svega spomenutog u bilo koje upravljanje treba ugraditi upravljanje utemeljeno na rizicima *(Risk based thinking)*, što znači odlučivanje i rješavanje problema zasnovano na rizicima.

Ovi pristupi ulaze u suštinu donošenja poslovnih odluka pa se i u opći menadžment trebaju ugraditi ti novi pristupi u upravljanju. To zahtijeva promjene u obrazovnim programima, usavršavanje nastavnika i cjelokupnog aktualnog menadžmenta organizacija.

Integracija upravljanja rizikom u postojeći sustav upravljanja

Potpuno je jasno da upravljanje rizicima bez integracije u postojeći sustav upravljanja nema smisla! Budući da su rizici pratitelji upravljanja poslovanjem, a javljaju se u procesima, projektima, objektima i na infrastrukturi, treba razumjeti kako provesti tu integraciju. Tu su najmanje tri problema. Prvi, razumijevanje modela integracije i primjena u vlastitoj organizaciji. Drugo, educiranost za novi oblik upravljanja. Treće, procesna orijentiranost organizacije sa strogo definiranim odgovornostima.



Slika 1. Sastavnice sustava upravljanja

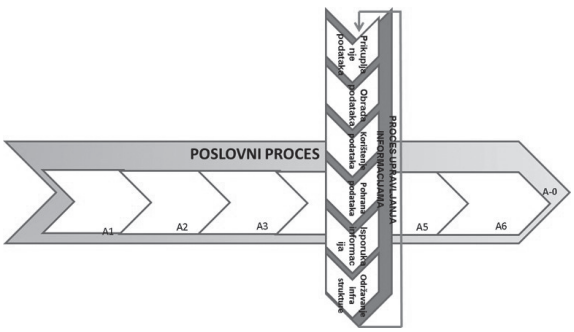
Figure 1. Components of the management system

Na slici 1 jasno je da svaka sastavnica sustava upravljanja zahtijeva upravljanje rizicima u procesima i projektima koji se događaju unutar njih. Preduvjet za operacionalizaciju modela je da su svi procesi (temeljni, upravljački i podrške) kao i projekti opisani s utvrđenim interakcijama, ciljevima i odgovornostima.

Informacijski sustav kao potpora odlučivanju u upravljanju

Informacijski sustav daje podatkovnu sliku poslovnih procesa iz realnog sustava upravljanja. Svrha mu je da kao podsustav poslovnog sustava daje potporu odlučivanju u upravljanju, a u funkciji je: prikupljanja, obrade, korištenja i pohrane podataka te isporuke potrebnih informacija uz brižno održavanje objekata i potrebne mu infrastrukture.

Takav značaj ovog podsustava upućuje na to da se u svim koracima procesa upravljanja informacijama, uključivo i održavanje objekata i potrebne infrastrukture, zahtijeva velika pozornost pri upravljanju rizicima.



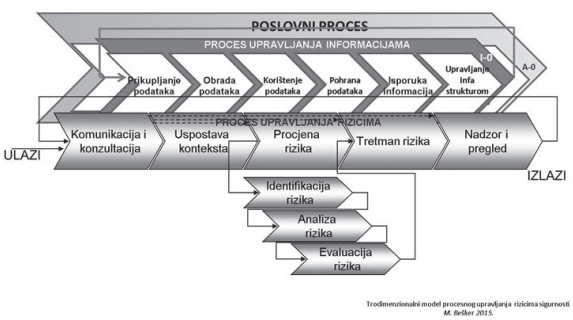
Slika 2. Interakcija poslovnog procesa s procesom upravljanja informacijama

Figure 2. Business process interaction with information management process

Složenost je u tome što u svakom koraku (A1, A2, A3, A4, A5, A6)[2] poslovnog procesa A-0 treba implementirati sve korake (**I**1, **I**2, **I**3, **I**4, **I**5, **I**6) procesa upravljanja informacijama I-0. U praksi je to izvedivo samo onda kada je organizacija u potpunosti procesno orijentirana (definirani su i opisani svi poslovni procesi i utvrđene interakcije među njima).

Trodimenzionalni model procesnog upravljanja sigurnošću informacijskih sustava

Trodimenzionalni model upravljanja sigurnošću potrebno je koristiti u svim situacijama kada procesi podrške (upravljački ili logistički) u poslovnom procesu mogu biti generatori rizika.



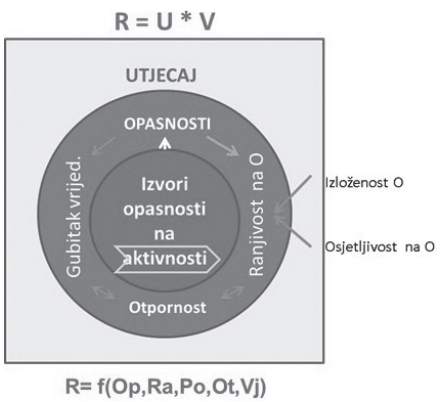
Slika 3. Trodimenzionalni model upravljanja sigurnošću informacija

Figure 3. Three-dimensional information security management model

U čemu je sadržana ta složenost? Želimo li upravljati sigurnošću informacijskog sustava implementiranog u neki poslovni proces, nužno je u svakom koraku (A1, A2, A3, A4, A5, A6) poslovnog procesa A-0 implementirati sve korake (I1, I2, I3, I4, I5, I6): procesa upravljanja informacijama I-0, a potom u svaki korak implementirati proces upravljanja rizicima u procesu U-0. Ovaj model sprečava da se rizici procesa upravljanja informacijama ne prenose u poslovni proces gdje se stvara nova vrijednost.

Multidimezionalna analiza rizika

Prema definiciji rizik je funkcija od utjecaja i vjerojatnosti R = f(U,V). To krije opasnost ako se utjecaj promatra jednodimenzionalno, što u pravilu daje pogreške u procjeni rizika. Utjecaj je vrlo složen jer je U funkcija više varijabli, U = f(Op, Ra, Gv, Ot i Vj). To se može analizirati na sljedećem modelu multivarijatne analize (slika 4).

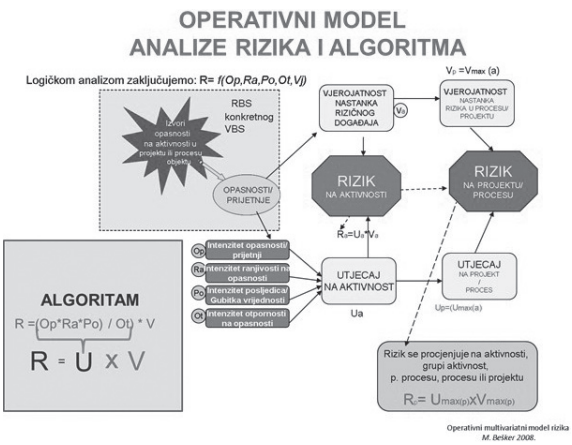


Slika 4. Model multivarijatne analize

Figure 4. Multivariate analysis model

Izvori opasnosti (prijetnji) nalaze se u procesnim aktivnostima na objektima i infrastrukturi. Oni generiraju *opasnosti* (prijetnje) u procesnim aktivnostima, objektima i infrastrukturi. Na te opasnosti javlja se *ranjivost* u procesnim aktivnostima, objektima i infrastrukturi. Opasnosti mogu izazvati manji ili veći *gubitak vrijednosti* u procesnim aktivnostima, objektima i infrastrukturi. Ako funkcionira sustav upravljanja rizicima, svaka procesna aktivnost, objekt i infrastruktura imaju svoju otpornost. Intenzitet faktora rizika procjenjuje se prema utvrđenim kriterijima na skali (1-5). Sinergijski učinak faktora rizika daje *utjecaj*. Nakon toga se množenjem *utjecaja i vjerojatnosti dobiva ukupni rizik* koji se u matrici rizika razvrstava prema zadanim kriterijima prihvatljivosti na odabranoj skali.

[2]Oznake procesa i potprocesa usklađene su prema IDEF0 metodologiji.



Slika 5. Operativni multivarijatni model analize
Figure 5. Operational multivariate analysis model

Aspekti analize rizika procesa, projekta ili infrastrukture

Često se u analizi i procjeni rizika procesa, projekta, objekta i infrastrukture pokušava dobiti univerzalni rizik. To je naprosto nemoguće jer u stvarnom životu postoje različiti rizici koji se vežu s aspektima analize. Primjera radi, u nekom poslovnom procesu sasvim su različiti rizici s aspekta kvalitete, zdravlja i sigurnosti ili elementarnih nepogoda.

Na slici 6 očite su bitne razlike u rizicima prema aspektima, a to je dalje povezano s izradom kriterija za ocjenu razine faktora rizika.

Proaktivno upravljanje rizicima

Često se misli da se preventivnim upravljanjem rizicima potpuno rješavaju problemi sigurnosti poslovanja. Tu se ponovo krije opasnost da nismo sveobuhvatno procijenili rizike i da će se pojaviti neki novi rizici. Naime, pojava rizika je jako dinamična. S promjenama u kontekstu organizacije javljaju se novi rizici koje ranije nismo identificirali. Iz tih razloga treba težiti kombiniranom rješenju koje uključuje preventivno, proaktivno i kurativno upravljanje rizicima.

Kako uspostaviti proaktivno upravljanje rizicima?

U svim procesima preko vlasnika procesa (potprocesa) treba uspostaviti sustav informiranja prema menadžeru rizika. Izrađuju se upute i postupci za slučaj nemilog događaja na procesnoj aktivnosti, objektu ili infrastrukturi. Nakon prijema informacije menadžer rizika saziva tim za procjenu rizika te za nove identificirane opasnosti provodi, prema utvrđenoj metodologiji, analizu, procjenu i tretman novih rizika. O rezultatima procjene informira se uprava koja odobrava ili ne odobrava predložene mjere tretmana rizika.

ZAKLJUČAK

Cilj ovoga rada bio je metodološki, koristeći nove modele i metode, prikazati suvremeni pri-

ODREĐIVANJE ASPEKATA ANALIZE RIZIKA
Na primjeru „Proces plasmana poljoprivrednih proizvoda"
U procesu ne postoji univerzalni rizik, rizik se procjenjuje prema aspektima analize.

OPIS ASPEKATA ANALIZE RIZIKA					
ASPEKTI	**KVALITETE**	**OPERATIVNIH RIZIKA**	**TRŽIŠNIH RIZIKA**	**DRUŠTVENIH RIZIKA** (politički, društveni, pravni)	**RIZIK ELEMENTARNIH NEPOGODA**
Opis aspekata	**Rizik** mogućnosti ispunjenja specificiranih zahtjeva za proizvodom ili uslugom ili na drugi način neispunjenje ugovorne obveze.	**Rizici:** lošeg rukovođenja i koordinacije; nedefiniranih odgovornosti; ne kompetentnosti; kršenja propisanog izvođenja radnih operacija; zle namjere; oštećenja imovine; greška u procesu rada; netočnih informacija i lošeg informacijskog sustava.	**Rizici:** promjene uvjeta na tržištu (uvoz –izvoz), kamatne stope, promjene cijene valute; re-financiranje novim zaduživanjem; nemogućnosti naplate; urušavanja tržišta; neizvjesnosti prihoda; nelikvidnost; gubljenje ugleda.	**Rizici:** nestabilnost i neefikasnost države; socijalni nemiri, nezaposlenost; insolventnost klijenta; pravnog sustava; promjene zakona; nepoštivanje zakona; neusklađenost zakona.	**Rizici:** od elementarnih nepogoda koje mogu uništiti imovinu organizacije ili imovinu kupca.

Slika 6. Određivanje aspekta analize rizika
Figure 6. Determining the aspect of risk analysis

stup upravljanju rizicima i sigurnosti u poslovanju s težištem na upravljanju rizicima informacijskih sustava kao posebno važne potpore odlučivanju u upravljanju. Čitatelji će dobiti orijentaciju kako bi se trebao uspostaviti sustav upravljanja rizicima i sigurnosti u organizaciji te koje modele i metode koristiti što bi ih moglo potaknuti na osuvremenjivanje postojećih sustava upravljanja rizicima u organizaciji. Iz konteksta ovoga rada nameću se pitanja organizacije i njezine strukture, novih znanja o procesnom upravljanju i upravljanju rizicima te odgovarajućih alata (softvera) za upravljanje rizicima.

Autori rada će biti počašćeni ako se ovim radom, barem kod jednog dijela čitatelja, iskaže interes za traženjem još novijih rješenja upravljanja rizicima u njihovoj organizaciji.

LITERATURA

Bešker, M.: Zaštita u informatičkoj djelatnosti, *Bezbednost i društvena samozaštita*, 1988., 6, 27-33.

Bešker, M.: Sigurnost i informiranje, *Zbornik radova: Novinarstvo i Europa 92*, 114-118, Alinea Zagreb, Zagreb, 1991.

Bešker, M.: Faktori rizika poslovanja, *Konferencija MAZUK*, Zbornik radova, Ohrid, 2004.

Bešker, M.: Upravljanje rizicima poslovanja. *Zbornik radova*, Europski centar za kvalitetu, Međunarodni simpozij, Moskva – Šibenik, 2005.

Bešker, M. i dr.: *Procjena i obrada rizika uporabom VPR metodologije & "ERM Venture" softverskog alata*, Hera, Mostar, 2015.

Covello, V. T., Mumpower, J.: Risk Analysis and Risk Management an Historical Perspective, *Risk Analysis*, 5, 1984., 2, 103-120.

Ćurak, M., Jakovčević, D.: *Osiguranje i rizici*, RRIF-plus, Bjelovar, 2007.

De Rosa, C. T., Johnson, B. L.: *Environmetal policy and public health*, CRC press, United States, 2017.

Duffey, R. B., Saull, J. W.: *Managing Risk: The Human Element*, John Wiley & Sons, United States, 2008.

HRN ISO 45001:2018, Sustavi upravljanja zaštitom zdravlja i sigurnosti pri radu – Zahtjevi s uputama za uporabu

HRN EN ISO 9001: 2015, Sustavi upravljanja kvalitetom – Zahtjevi

Hubbard, D.: Hurdling Risk, *CIO Magazine*, 1998.

ISO 31000:2018, Upravljanje rizikom – Smjernice

ISO/IEC 31010: 2010, Upravljanje rizicima – Tehnike procjena rizika

ISO/IEC 27005: 2018 - Informaciona tehnologija - Sigurnosne tehnike - Upravljanje rizikom informacijske sigurnosti (3. izdanje)

Nadrljanski, Đ., Nadrljanski, M.: *Menadžment rizika*, Visoka škola za inspekcijski i kadrovski menadžment, Split, 2014.

Nolan, D.: *Handbook of Fire and Explosion Protection Engineering Principles for Oil, Gas, Chemical, and Related Facilities (Fourth Edition)*, Gulf Professional Publishing, e-book, 2019.

Rausand, M.: *Risk Assessment: Theory, Methods, and Applications*, Wiley, United States, 2011.

Risk engineering, dostupno na: https://risk-engineering.org/hazard-analysis/, pristupljeno: 2.1.2021.

Runje, B., Mudronja, V., Horvatić, A.: *Metode procjene rizika*, Fakultet strojarstva i brodogradnje, Zagreb, 2016.

Tafra-Vlahović, M.: *Upravljanje krizom*, Visoka škola za poslovanje i upravljanje „Baltazar Adam Krčelić", Zaprešić, 2011.

Uredba EU 2016/679, Smjernice o procjeni učinka na zaštitu podataka i utvrđivanje mogu li postupci obrade „vjerojatno prouzročiti visok rizik"

THREE-DIMENSIONAL MODEL OF INFORMATION SECURITY PROCESS MANAGEMENT

SUMMARY: The paper presents an approach to risk - based information security management and multivariate analysis with defined criteria and an emphasis on preventive and proactive management of business risks. The security of a management system depends directly on managing the risks of the business. For these reasons, ISO 9000: 2015 defines risk as the effect of uncertainty, ie deviation from what is expected - in a positive or negative sense, which means the degree of achievement of the business objectives. ISO 9001: 2015 primarily requires that the risks of a business be preventively managed but not conditional which management methods and models. ISO 31000 (Risk Management Systems), on the other hand, advocates in addition to preventive and proactive management of business risks and information. This request is very justified because it allows to react in a timely manner to the occurrence of any information threats. The preconditions for effective implementation of a risk-based management approach are additional management skills and the availability of tools (software) for multivariate risk analysis.

Key words: *information security management, risk-based management, business risk management, preventively manage risks, proactively manage risks*

Subject review
Received: 2021-03-31
Accepted: 2022-02-08