

Prednosti i nedostaci metoda za kvalitativnu analizu rizika

INFIGO-MD-2006-06-01

05-06-2006

Hrvoje Šegudović
Hrvoje.Segudovic@infigo.hr



Ovaj dokument originalno je objavljen kao referat u sklopu savjetovanja Sigurnost informacijskih sustava (ISS) na Mipro 2006 skupu.

Dokument je namijenjen javnoj objavi, a vlasništvo je Infigo IS. Svatko ga smije koristiti, pozivati se na njega ili ga citirati, ali isključivo u izvornom obliku i uz obvezno navođenje izvora.

Korištenje dokumenata na bilo koji drugi način od gore navedenog, bez dozvole Infigo IS predstavlja povredu vlasništva i kao takvo podložno je zakonskoj odgovornosti koja je regulirana zakonima Republike Hrvatske ili drugom primjenjivom regulativom.

Infigo IS d.o.o.
Horvatovac 20
10000 Zagreb

tel. +385 1 4662 700
fax. +385 1 4662 701
info@infigo.hr
www.infigo.hr



SADRŽAJ

1. SAŽETAK	4
2. UVOD	5
3. PROCJENA RIZIKA	6
4. KVANTITATIVNI PRISTUP	7
5. KVALITATIVNI PRISTUP	8
6. METODE	9
6.1. METODA 1: MATRICA PREDEFINIRANIH VRIJEDNOSTI	9
6.2. METODA 2 – RANGIRANJE PRIJETNJI PREMA PROCJENI RIZIKA	10
6.3. METODA 3 – PROCJENA VJEROJATNOSTI OSTVARENJA I MOGUĆIH POSLJEDICA	12
6.4. METODA 4 – ODVAJANJE PRIHVATLJIVIH I NEPRIHVATLJIVIH RIZIKA	13
7. EVALUACIJA METODA ZA KVALITATIVNU PROCJENU RIZIKA	14
8. MODIFICIRANA METODA ZA KVALITATIVNU PROCJENU RIZIKA	15
8.1. PRETPOSTAVKE	15
8.2. PROCJENA RIZIKA	15
9. ZAKLJUČAK	17
10. LITERATURA	18

1. SAŽETAK

Upravljanje informacijskom sigurnošću sve se više prepoznaje kao poslovna potreba. Također, upravljanje informacijskom sigurnošću u poslovanju, sve češće, direktno ili indirektno nameću i razni regulatorni propisi.

Upravljanje rizikom je proces kroz koji se potvrđuje poslovna opravdanost odabira sigurnosnih rješenja i kontrola koje će osigurati dovoljnu razinu sigurnosti. Također, proces upravljanja rizikom omogućava razvoj strategije i postavljanje ciljeva u području informacijske sigurnosti.

Najvažniji dio tog procesa, ali i najpodložniji pogreškama jest prvi korak koji predstavlja procjenu rizika. Literatura uglavnom razlikuje kvalitativnu i kvantitativnu procjenu rizika. Kod kvalitativne procjene rizik se procjenjuje iskustveno, odnosno opisno, za razliku od kvantitativne procjene kod koje se rizik opisuje numerički (financijski).

Unatoč teoretskoj osnovi (kvantitativni pristup) koja omogućava preciznu procjenu rizika, praksa pokazuje da takav pristup, kod kojeg se vrijednost informacijskih resursa uglavnom opisuje njihovom knjigovodstvenom vrijednošću nije adekvatan. Zbog toga se kod procjene rizika u informacijskim sustavima preferira kvalitativni, odnosno kombinacija kvalitativnog i kvantitativnog pristupa.

Obzirom da se kvalitativna procjena rizika izrazito oslanja na subjektivnu procjenu, podložna je pogreškama. U radu su analizirane neke od metoda za kvalitativnu (kvantitativno-kvalitativnu) procjenu rizika, s posebnim naglaskom na to kako različiti elementi mogu utjecati na pouzdanost rezultata procjene rizika.

2. UVOD

Upravljanje rizikom je proces kroz koji se potvrđuje poslovna opravdanost odabira sigurnosnih rješenja i kontrola koje će osigurati dovoljnu razinu sigurnosti. Također, proces upravljanja rizikom omogućava razvoj strategije i ciljeva u području informacijske sigurnosti.

Najvažniji, najosjetljiviji i vremenski najzahtjevniji dio procesa upravljanja rizikom je postupak procjene, odnosno analize rizika [5]. U osnovi, postoje dvije vrste pristupa procjeni rizika: kvantitativni i kvalitativni. Literatura, međunarodni standardi ([6], [7]) koji definiraju sustave za upravljanje informacijskom sigurnošću, pa i praksa preferiraju kvalitativni pristup.

U radu je ukratko opisan kvantitativni pristup procjeni rizika, te njegovi nedostaci u primjeni na informacijsku sigurnost, a detaljnije su evaluirane i četiri metode za kvalitativnu procjenu rizika koje opisuju [1] i [2]. Evaluacija se sastojala od opisa metoda, te procjene njihovih prednosti i nedostataka.

Obzirom na nedostatke pojedinih metoda koji utječu na pouzdanost rezultata procjene rizika i daljnju upotrebljivost u postupku upravljanja rizikom, u radu je predložena modificirana metoda kojom se nastoji povećati pouzdanost rezultata procjene rizika, a istovremeno, prioritizacijom, omogućiti i dodatna fleksibilnost prilikom procesa tretiranja rizika, odnosno upravljanja rizikom.

3. PROCJENA RIZIKA

Općenito, rizik kao pojam predstavlja kombinaciju vjerojatnosti nekog događaja i utjecaja, odnosno (negativne) posljedice tog događaja u slučaju realizacije prijetnji koje iskorištavaju neku od ranjivosti.

Kad se govori o informacijskoj sigurnosti, rizik (R) za pojedini resurs procjenjuje se procjenom njegove vrijednosti (eng. *asset value* – AV), ranjivosti tog resursa (eng. *vulnerability* – V), prijetnji koje mogu iskoristiti te ranjivosti (eng. *threat* – T), vjerojatnosti ostvarenja prijetnji (eng. *probability* – P) i posljedicama (eng. *impact* – I) koje se mogu dogoditi ukoliko se određena prijetnja ostvari. Dakle, matematički, rizik predstavlja funkciju navedenih varijabli (1).

$$R = f(AV, V, T, P, I) \quad (1)$$

Također, da bi se rezultati procjene rizika mogli smatrati valjanim, sam proces mora zadovoljiti sljedeće kriterije:

- jednoznačnost,
- objektivnost,
- pouzdanost i
- repetabilnost.

4. KVANTITATIVNI PRISTUP

Kvantitativni pristup procjeni rizika temelji se na korištenju egzaktnih numeričkih vrijednosti. U tom slučaju, parametrima za izračun rizika nastoje se odrediti točne vrijednosti. Vrijednost resursa prikazuje se u novčanim jedinicama. Ranjivosti, prijetnje i posljedice u slučaju realizacije se u ovom slučaju promatraju kao tzv. faktor izloženosti (EF) koji se izražava u postotku gubitka vrijednosti resursa u slučaju ostvarenja pojedine prijetnje [3]. Vjerojatnost, koja također ovisi o ranjivostima i prijetnjama, se obično promatra u zadanom vremenskom periodu, pa se u skladu s tim i provodi i kvantifikacija rizika za taj vremenski period (2).

$$R = AV * EF_{I,V,T} * P_{V,T} \quad (2)$$

Npr. za resurs koji ima vrijednost od 1000\$, faktor izloženosti od 20% i vjerojatnost od 0,05 u godini dana rizik se može lako izračunati (3).

$$R = 1000\$ * 0,2 * 0,05 / god = 10\$ / god \quad (3)$$

Iako se kvantitativnim pristupom dobivaju egzaktni, tj. apsolutni vrijednosti rizika, kod procjene rizika u informacijskoj sigurnosti ovaj pristup nije adekvatan iz više razloga.

Kao prvo, novčana vrijednost resursa obično se određuje na temelju knjigovodstvene vrijednosti, što uopće ne mora predstavljati pravu vrijednost resursa za pojedini poslovni proces. Npr. kritična baza podataka može se nalaziti na starom poslužitelju koji više ni nema knjigovodstvenu vrijednost, dok potpuno novi poslužitelj može služiti za poslovno malo važne sustave. U poslovnom smislu, vrijednost prvog poslužitelja mnogo je veća nego drugog, bez obzira na njihovu knjigovodstvenu vrijednost.

Drugi problem kod ovog pristupa kod informacijske sigurnosti je točno određivanje faktora izloženosti, koje je u većini slučajeva praktički nemoguće odrediti, ponekad čak ni približno.

Konačno, vjerojatnost ostvarenja je isto prilično teško procijeniti. Čak i u slučajevima gdje se mogu pronaći statistički podaci, njihovo korištenje može uzrokovati unošenje dodatne pogreške u procjenu rizika. Npr. postoje uglavnom prilično točne statistike o broju pronađenih propusta u operacijskim sustavima u zadnjih nekoliko godina. Iz tih statistika lako je moguće iščitati da operacijski sustav OS1 ima kontinuirano manji broj propusta od operacijskog sustava OS2. Kvantitativni pristup bi u tom slučaju nedvojbeno favorizirao operacijski sustav OS1, što ne mora odgovarati realnoj situaciji.

Na osnovu gore spomenutih činjenica, može se zaključiti da kvantitativni pristup procjeni rizika u sustavima za upravljanje informacijskom sigurnošću nije prikladan jer egzaktni numeričke vrijednosti dobivene kao rezultat procjene rizika nisu pouzdane zbog nepouzdanosti svih parametara koji se koriste za izračun.

Zbog toga, ovaj rad ne ulazi dalje u samu interpretaciju tako dobivenih rezultata, niti na druge potencijalne prednosti i nedostatke ovog pristupa [4].

5. KVALITATIVNI PRISTUP

Za razliku od kvantitativnog pristupa, kvalitativni pristup procjeni rizika ne koristi apsolutne vrijednosti parametara, nego kvalitativno evaluira njihov utjecaj na rizik. Kod kvalitativnog pristupa veliku važnost ima iskustvo, stručnost i nadasve sposobnost osoba koje provode procjenu rizika. Procjena se provodi kvalitativno, no zbog lakše interpretacije rezultata, kod kvalitativne procjene rizika parametri se, isto kao i procijenjeni rizik, kvantificiraju. Za razliku od kvantitativnog pristupa, u ovom slučaju, tako dobivene numeričke vrijednosti nisu apsolutne, već relativne.

Osim subjektivnosti, koja je inherentni problem kvalitativnog pristupa procjeni rizika, te samim time i direktan uzrok nepouzdanosti, dodatni faktor koji može utjecati na pouzdanost rezultata kvalitativne procjene jest metoda kvantifikacije subjektivno procijenjenih parametara, kvantificiranje rizika, te ponovna reinterpetacija tako dobivenih numeričkih vrijednosti.

Obzirom da se kvalitativne veličine parametara procjenjuju subjektivno, da bi se postigla repetabilnost, vrlo je bitno da se sam način procjene može jednoznačno interpretirati i provoditi s istim ili sličnim rezultatima od strane više kompetentnih osoba.

6. METODE

Postoji priličan broj pristupa kvalitativnoj procjeni rizika. Ovaj rad evaluira četiri metode za kvalitativnu procjenu rizika koje opisuje literatura [1] [2].

Svaka od metoda koristi neke od parametara navedenih u formuli (1). Metode se razlikuju prema parametrima koje koriste, te prema načinu njihove kvantifikacije.

6.1. METODA 1: MATRICA PREDEFINIRANIH VRIJEDNOSTI

Ova metoda za procjenu rizika koristi tri parametra: vrijednost resursa, prijetnje i ranjivosti. Svaki od tih parametara promatra se u odnosu na moguće posljedice, dok se prijetnje promatraju u odnosu na odgovarajuće ranjivosti (4). Svi parametri se kvantificiraju proizvoljno.

$$R = f(AV_I, V_{I,P}, T_{I,V,P}) \quad (4)$$

Varijacija ove metode eksplicitno navedena u [1] i [2], za određivanje vrijednosti resursa koristi numeričke vrijednosti u rasponu od 0 (mala) do 4 (vrlo velika), dok se za kvantifikaciju ranjivosti i prijetnji koristi raspon od 0 (niska razina) do 2 (visoka razina). Razina rizika se određuje sumom vrijednosti parametara (5).

$$R = AV + V + T \quad (5)$$

Tablica 1 prikazuje matricu predefiniраниh vrijednosti.

	Prijetnja	0			1			2		
	Ranjivost	0	1	2	0	1	2	0	1	2
Vrijednost resursa	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Tablica 1: Matrica predefiniраниh vrijednosti

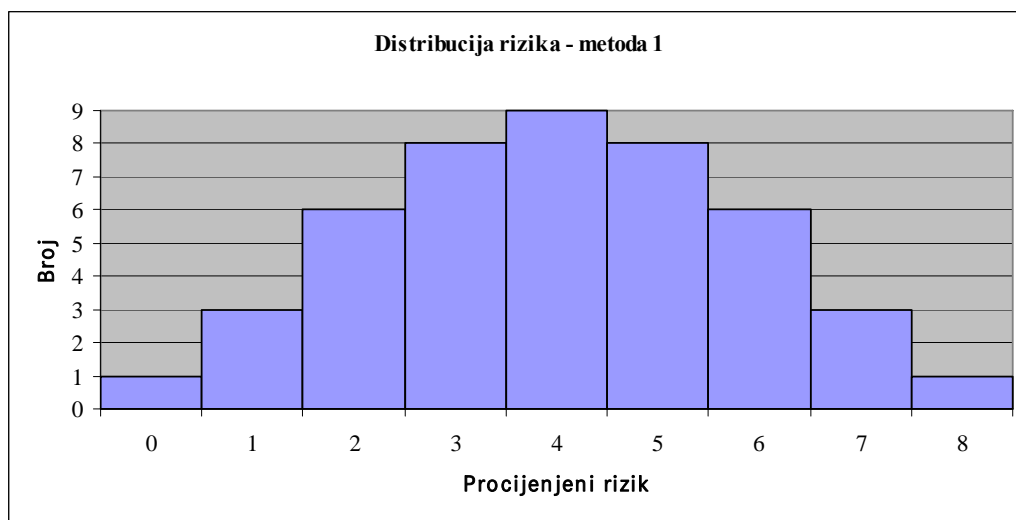
Na temelju (5) i raspona vrijednosti koji navode [1] i [2], mogu se izračunati minimalne i maksimalne vrijednosti procijenjenog rizika (6).

$$\begin{aligned} R_{MIN} &= AV_{MIN} + V_{MIN} + T_{MIN} = 0 \\ R_{MAX} &= AV_{MAX} + V_{MAX} + T_{MAX} = 8 \end{aligned} \quad (6)$$

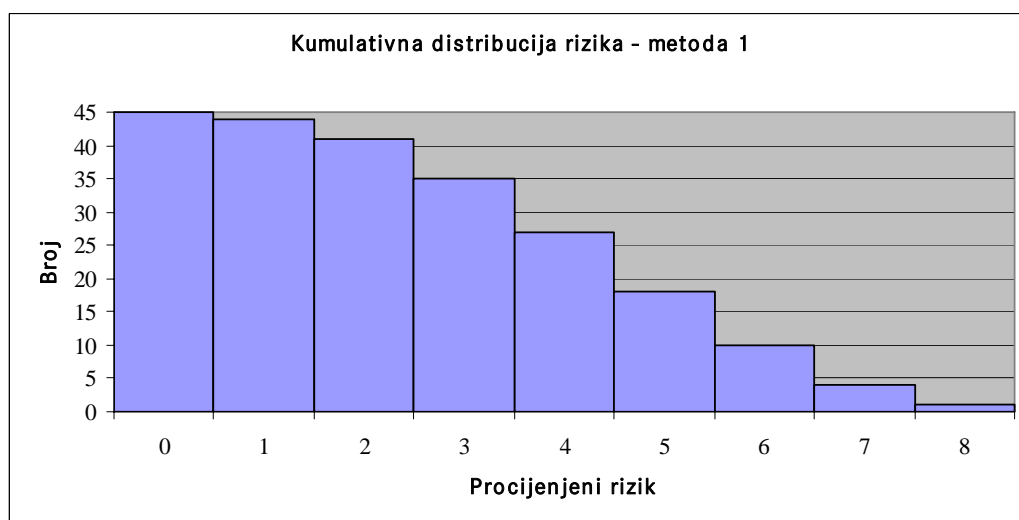
Procijenjeni rizik može poprimiti sve cjelobrojne vrijednosti između R_{MIN} i R_{MAX} , uključujući i njih.

Sl. 1. i Sl. 2. prikazuju distribuciju, odnosno kumulativnu distribuciju ovako definirane funkcije za procjenu rizika.

Može se uočiti da funkcija za procjenu rizika teži usrednjavanju vrijednosti (Slika 1), dok je graf kumulativne distribucije rizika konkavan (Slika 2).



Slika 1: Distribucija funkcije za procjenu rizika – metoda 1



Slika 2: Kumulativna distribucija funkcije za procjenu rizika – metoda 1

Korištenje matrice predefiniраниh vrijednosti omogućava proizvoljno rangiranje rizika prema njihovoj vrijednosti prilikom kasnijeg procesa tretiranja rizika, odnosno upravljanja rizikom, no zbog funkcije distribucije ne prioritizira veće rizike.

Nedostatak ove metode jest što procjena rizika eksplicitno uopće ne koristi moguće posljedice i vjerojatnosti ostvarenja. Posljedice se implicitno koriste za procjenu veličina svih parametara, a vrijednosti prijetnji i ranjivosti trebale bi na neki način odgovarati vjerojatnosti realizacije pojedinih događaja.

Također, u praksi je vrlo teško nezavisno promatrati prijetnje i ranjivosti, pa je stoga posebno određivanje vrijednosti za jedan i drugi parametar prilično dvojbeno.

6.2. METODA 2 – RANGIRANJE PRIJETNJI PREMA PROCJENI RIZIKA

Ova metoda za procjenu rizika formalno koristi samo dva parametra: utjecaj na resurs (vrijednost resursa) i vjerojatnost ostvarenja prijetnje. Implicitno se podrazumijeva da je utjecaj na resurs ekvivalentan vrijednosti resursa, dok se prijetnje promatraju u odnosu na odgovarajuće ranjivosti. Na taj način procijenjeni rizik postaje funkcija više parametara (7).

$$R = f(I_{AV,T}, P_{V,T}) \quad (7)$$

Varijacija ove metode eksplicitno opisana u [1] i [2] koristi identični raspon vrijednosti za utjecaj (vrijednost resursa) i vjerojatnost ostvarenja prijetnje. Moguće vrijednosti su u rasponu od 1 (mala) do 5 (vrlo velika). Razinu rizika određuje produkt tih dvaju parametra (8).

$$R = I * P \quad (8)$$

Tablica 2 prikazuje matricu za procjenu rizika dobivenu na taj način, zajedno s rangiranim prijetnjama.

	Utjecaj (vrijednost)	Vjerojatnost ostvarenja	Rizik	Rangiranje prijetnji
Prijetnja A	5	2	10	2
Prijetnja B	2	4	8	3
Prijetnja C	3	5	15	1
Prijetnja D	1	3	3	5
Prijetnja E	4	1	4	4
Prijetnja F	2	4	8	3

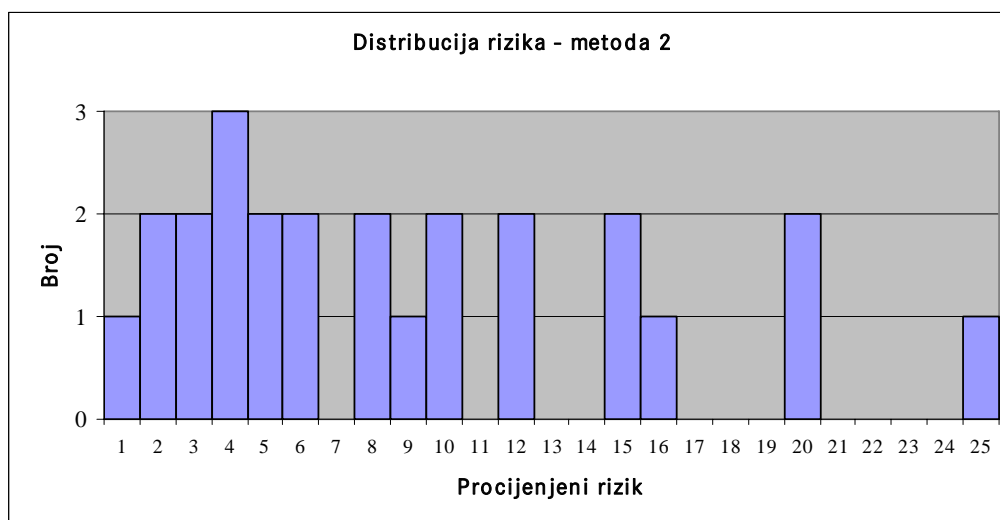
Tablica 2: Rangiranje prijetnji prema procjeni rizika

Na temelju (8) i raspona vrijednosti koji navode [1] i [2], mogu se izračunati minimalne i maksimalne vrijednosti procijenjenog rizika (9).

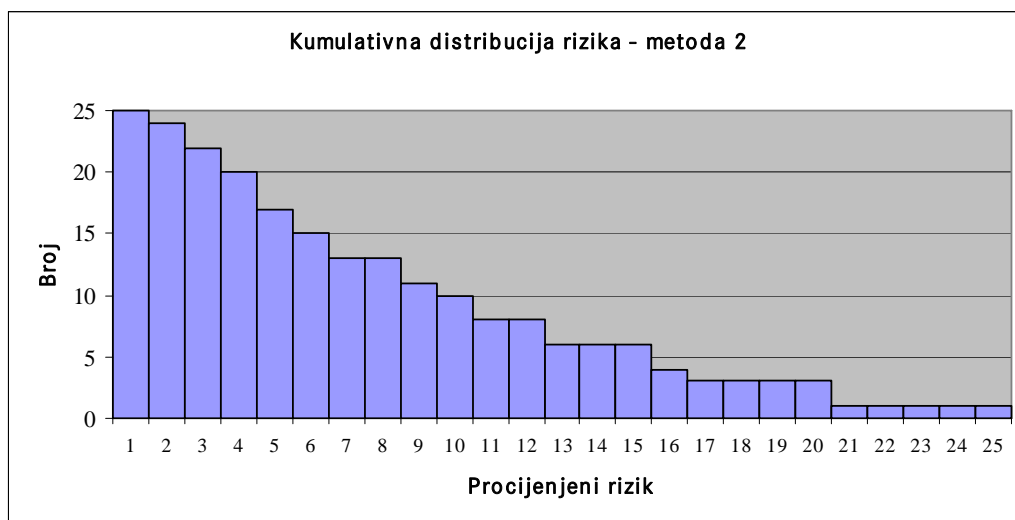
$$\begin{aligned} R_{MIN} &= I_{MIN} + P_{MIN} = 1 \\ R_{MAX} &= I_{MAX} + P_{MAX} = 25 \end{aligned} \quad (9)$$

Procijenjeni rizik može poprimiti cjelobrojne vrijednosti između R_{MIN} i R_{MAX} , uključujući i njih, te isključujući proste brojeve izvan raspona vrijednosti i njihove višekratnike.

Slika 3 i Slika 4 prikazuju distribuciju, odnosno kumulativnu distribuciju ovako definirane funkcije za procjenu rizika.



Slika 3: Distribucija funkcije za procjenu rizika - metoda 2



Slika 4: Kumulativna distribucija funkcije za procjenu rizika – metoda 2

Može se uočiti da funkcija za procjenu rizika teži grupiranju nižih vrijednosti i isticanju viših (Sl. 3.), dok je graf kumulativne distribucije rizika konveksan (Sl. 4.).

Rangiranje prijetnji procjenom rizika omogućava njihovu prioritizaciju u kasnijem postupku tretiranja, odnosno upravljanja rizikom.

Nedostatak ove metode je što se rizik eksplicitno procjenjuje korištenjem samo dva parametra koji su implicitno funkcije više varijabli. Također, ova metoda izjednačava vrijednost resursa i mogućnost utjecaja na resurs, što u nekim slučajevima nije točno.

6.3. METODA 3 – PROCJENA VJEROJATNOSTI OSTVARENJA I MOGUĆIH POSLJEDICA

Postupak procjene rizika kod ove metode nešto je složeniji nego kod prethodne dvije, a provodi se u dva koraka. Prvo se definira vrijednost resursa koja se bazira na potencijalnim posljedicama u slučaju ostvarenja neke prijetnje. Nakon toga se, na temelju ranjivosti i prijetnji, određuje vjerojatnost ostvarenja (10).

$$P = f(V, T) \quad (10)$$

Konačno, rizik se procjenjuje kao kombinacija vrijednosti resursa i vjerojatnosti ostvarenja (11).

$$R = f(P_{V,T}, AV_{I,T}) \quad (11)$$

Varijacija ove metode, eksplicitno opisana u [1] i [2], za određivanje vrijednosti resursa koristi raspon od 0 (mala) do 4 (vrlo velika). Za određivanje ozbiljnosti ranjivosti i prijetnji koristi se raspon od 0 (mala) do 2 (velika). Vjerojatnost ostvarenja (frekvencija) računa se kao suma procijenjenih veličina ranjivosti i prijetnji (12).

$$P = V + T \quad (12)$$

Ukupni rizik računa se kao suma vrijednosti resursa i vjerojatnosti ostvarenja (13).

$$R = AV + P = AV + V + T \quad (13)$$

Tablica 3 prikazuje matricu za određivanje vjerojatnosti ostvarenja.

Uz određenu vjerojatnost ostvarenja i poznatu vrijednost resursa, rizik se procjenjuje kroz definiranu matricu (Tablica 4).

Minimalne i maksimalne vrijednosti procijenjenog rizika mogu se izračunati isto kao i u (6), te ponovno mogu poprimiti sve cjelobrojne vrijednosti između R_{MIN} i R_{MAX} uključujući i njih.

Funkcije distribucije, odnosno kumulativne distribucije također su identične kao i kod metode 1 (Sl. 1. i Sl. 2.).

Prijetnja	0			1			2		
Ranjivost	0	1	2	0	1	2	0	1	2
Vjerojatnost ostvarenja	0	1	2	1	2	3	2	3	4

Tablica 3: Određivanje vjerojatnosti ostvarenja

Vrijednost resursa	0	1	2	3	4
Vjerojatnost ostvarenja					
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

Tablica 4: Matrica za procjenu rizika

Procjenom vjerojatnosti ostvarenja i moguće štete omogućava se rangiranje rizika prema procijenjenoj vrijednosti, slično kao i kod korištenja matrice predefiniраниh vrijednosti.

Formalno gledajući, formule za procjenu rizika koje se koriste kod metode 1 (matrica predefiniраниh vrijednosti) (5) i kod ove metode (13) su potpuno identične, no suštinska razlika kod njih je da se kod metode 1 prilikom procjena ranjivosti i prijetnji implicitno odražava vjerojatnost ostvarenja, odnosno frekvencija, dok se kod procjene vjerojatnosti ostvarenja i mogućih posljedica radi obrnuti postupak, odnosno na temelju procjene ranjivosti i prijetnji, određuje se pripadajuća vjerojatnost ostvarenja.

Kod ove metode također je problematična nezavisna procjena razine prijetnje i ranjivosti.

6.4. METODA 4 – ODVAJANJE PRIHVATLJIVIH I NEPRIHVATLJIVIH RIZIKA

Kod ove metode rizik se procjenjuje binarnim vrijednostima; kao prihvatljiv (0) ili neprihvatljiv (1).

Način procjene rizika može biti identičan način kao i u prethodnoj metodi, jedino je matrica procijenjenih vrijednosti rizika binarna (Tablica 5), isto kao i raspon vrijednosti koje može poprimiti procijenjeni rizik (14).

Vrijednost resursa	0	1	2	3	4
Vjerojatnost ostvarenja					
0	0	0	0	0	1
1	0	0	0	1	1
2	0	0	1	1	1
3	0	1	1	1	1
4	1	1	1	1	1

Tablica 5: Matrica za odvajanje prihvatljivih i neprihvatljivih rizika

$$\begin{aligned} R_{MIN} &= 0 \\ R_{MAX} &= 1 \end{aligned} \quad (14)$$

Metoda odvajanja prihvatljivih i neprihvatljivih rizika predstavlja ustvari varijaciju metode 3 (procjena vjerojatnosti ostvarenja i mogućih posljedica) ili metode 1 (matrica predefiniраниh vrijednosti), te kao takva nasljeđuje prednosti i nedostatke tih metoda.

7. EVALUACIJA METODA ZA KVALITATIVNU PROCJENU RIZIKA

Nepostojanje egzaktnih (financijskih) vrijednosti u procjeni rizika može ali i ne mora biti nedostatak pri kvalitativnoj procjeni rizika, pošto potrebna financijska analiza može biti provedena i kroz kasniji postupak tretiranja, odnosno upravljanja rizikom.

Zbog toga se najvećim nedostatkom kvalitativne procjene rizika smatra subjektivnost prilikom procjene vrijednosti parametara kojima se procjenjuje rizik.

Uz pretpostavku da manji broj parametara koji se moraju subjektivno odrediti proporcionalno umanjuje nepouzdanost rezultata, metoda 2 (rangiranje prijetnji prema procjeni rizika), koja rizik procjenjuje na temelju svega dvije eksplicitne vrijednosti mogla bi se smatrati najpouzdanijom.

Međutim, ukoliko se uzme u obzir da su parametri za procjenu rizika međusobno povezani, odnosno da se u opisanim metodama promatraju kao implicitne funkcije drugih parametara, može se utvrditi da puno veću nesigurnost u rezultat procjene rizika unose upravo te implicitne funkcije, pogotovo kada ovise o više parametara. Također, subjektivnost pri korištenju implicitnih funkcija s više parametara može utjecati na repetabilnost postupka procjene rizika, ukoliko taj postupak nezavisno provodi više osoba u različitim vremenskim intervalima.

Kod metode 2 oba parametra su implicitno funkcije više parametara, što ima velik utjecaj na pouzdanost rezultata. Dobra strana ove metode je što se rizik procjenjuje kao produkt parametara, što kao rezultat daje pogodnu distribuciju vrijednosti, te na taj način omogućava preciznije određivanje granice prihvatljivih i neprihvatljivih rizika, odnosno njihovu jasniju prioritizaciju u procesu tretiranja rizika

Metoda 4 predstavlja varijaciju metoda 1 ili 3, te se kao takva neće dalje posebno razmatrati.

Metode 1 i 3 formalno daju iste rezultate procjene rizika. Činjenica da se vjerojatnost ostvarenja kod metode 3 procjenjuje na temelju ranjivosti i prijetnji, može se smatrati prednošću u odnosu na metodu 1, kod koje je to implicitno uključeno u samu procjenu razina ranjivosti i prijetnji.

Kod obje metode razina ranjivosti i razina prijetnji promatraju se nezavisno, što je već prije istaknuto kao problem, pošto je pouzdana nezavisna procjena tih vrijednosti iskustveno vrlo teška.

Konačno, smanjeni raspon veličina procijenjenog rizika zbog korištenja sume parametara u odnosu na produkt može biti ograničavajući faktor u kasnijem procesu upravljanja rizikom.

8. MODIFICIRANA METODA ZA KVALITATIVNU PROCJENU RIZIKA

Iz prethodnih razmatranja može se zaključiti da svaka od opisanih metoda ima određene nedostatke koji mogu uzrokovati nepouzdanost rezultata procjene rizika, a u nekim slučajevima raspon veličina procijenjenog rizika može biti ograničavajući faktor u kasnijem procesu upravljanja rizikom.

Zbog toga se predlaže korištenje modificirane metode za kvalitativnu procjenu rizika koja je detaljnije opisana u nastavku.

8.1. PRETPOSTAVKE

Modificirana metoda za kvalitativnu procjenu rizika temelji se na sljedećim pretpostavkama:

- svaki resurs ima svoju vrijednost,
- ranjivost pojedinog resursa postoji ili ne,
- ukoliko ranjivost sustava postoji, postoji barem jedna prijetnja koja je može iskoristiti (prijetnja i ranjivosti su međusobno zavisne),
- prijetnja ima vjerojatnost ostvarenja koja ovisi o okolnostima,
- prijetnja ima moguće posljedice čija veličina ovisi i o okolnostima.

8.2. PROCJENA RIZIKA

Na temelju prethodne pretpostavke procjena rizika može se prikazati kao (15).

$$R = f(AV, P_T, I_T), T = f(V) \quad (15)$$

Može se uočiti da su svi parametri funkcija najviše jedne varijable, što osigurava jednoznačnost i jednostavnost interpretacije.

Da bi procjenu rizika bilo moguće napraviti osjetljivijom na razlike u veličinama pojedinih parametara i na taj način omogućiti više fleksibilnosti u postupku upravljanja rizikom, umjesto operacije zbrajanja koju koriste metode 1 i 3, modificirana metoda koristi operaciju množenja (16).

$$R = AV * P_T * I_T \quad (16)$$

Raspon vrijednosti koje svaki od parametara može poprimiti je proizvoljan, a u primjeru se zbog usporedbe s metodom 1 koristi skala od 5 vrijednosti za vrijednost resursa, te skale od 3 vrijednosti za vjerojatnost ostvarenja prijetnje i moguće posljedice. U odnosu na metodu 1, rasponi počinju s veličinom 1 (zbog uklanjanja mogućih nul vrijednosti).

Tablica 6 prikazuje modificiranu matricu za procjenu rizika.

Prijetnja	Vjerojatnost	1			2			3		
	Posljedica	1	2	3	1	2	3	1	2	3
Vrijednost resursa	1	1	2	3	2	4	6	3	6	9
	2	2	4	6	4	8	12	6	12	18
	3	3	6	9	6	12	18	9	18	27
	4	4	8	12	8	16	24	12	24	36
	5	5	10	15	10	20	30	15	30	45

Tablica 6: Modificirana matrica za procjenu rizika

Ovako definirana matrica usporediva je s matricom prikazanom u Tablici 1.

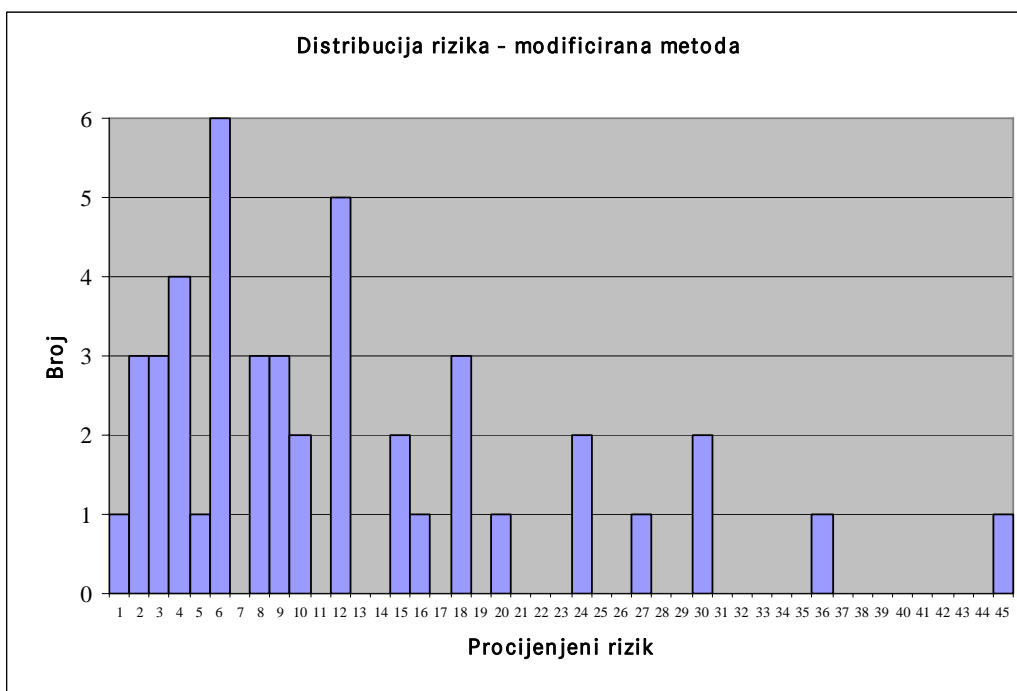
Na temelju (16) i predloženog raspona vrijednosti mogu se izračunati minimalne i maksimalne vrijednosti procijenjenog rizika (17).

$$\begin{aligned} R_{MIN} &= AV_{MIN} * V_{MIN} * T_{MIN} = 1 \\ R_{MAX} &= AV_{MAX} * V_{MAX} * T_{MAX} = 45 \end{aligned} \quad (17)$$

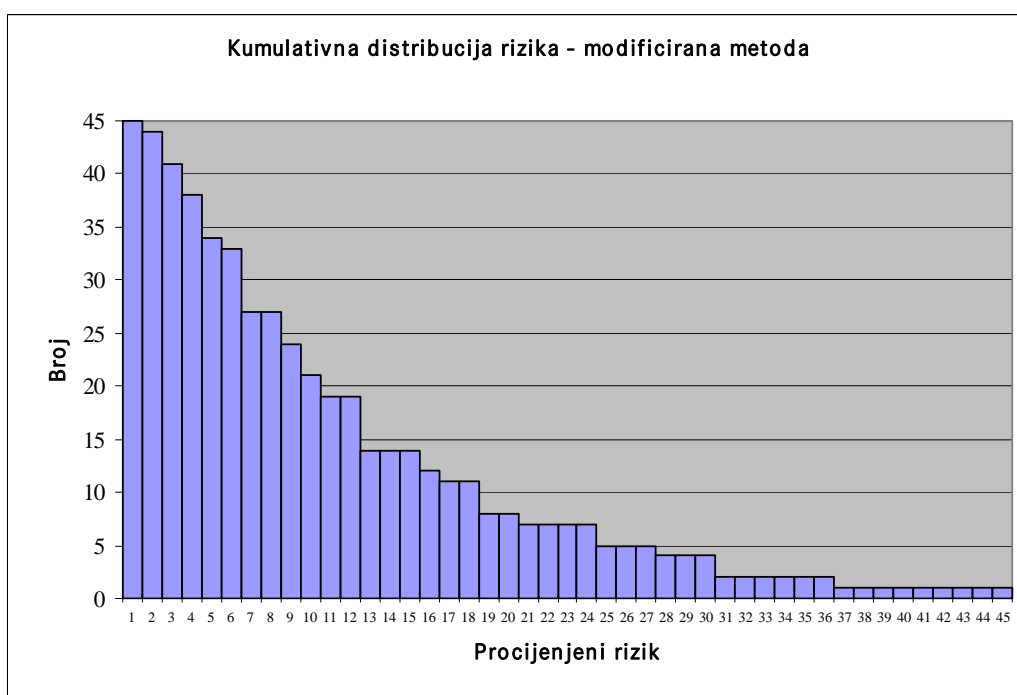
Procijenjeni rizik može poprimiti vrijednosti između R_{MIN} i R_{MAX} , uključujući i njih, isključujući proste brojeve izvan raspona vrijednosti parametara i njihove višekratnike.

Slika 5 i Slika 6 prikazuju distribuciju, odnosno kumulativnu distribuciju ovako definirane funkcije za procjenu rizika.

Kao i kod metode 2, može se uočiti da funkcija za procjenu rizika teži grupiranju nižih vrijednosti i isticanju viših (Slika 5), dok je graf kumulativne distribucije rizika konveksan (Slika 6).



Slika 5: Distribucija funkcije za procjenu rizika – modificirana metoda



Slika 6: Kumulativna distribucija funkcije za procjenu rizika – modificirana metoda

Na taj način, funkcija distribucije, isticanjem većih rizika, omogućava veću fleksibilnost pri upravljanju rizikom u odnosu na metodu 1.

9. ZAKLJUČAK

Kvalitativna procjena rizika je temelj za upravljanje rizikom u sustavima za upravljanje informacijskom sigurnošću.

Međutim, osiguranje jednoznačnosti, pouzdanosti, objektivnosti i repetabilnosti u postupcima kvalitativne procjene često je problematično. Metode koje predlažu postojeći standardi imaju određene nedostatke zbog kojih ne ispunjavaju sve kriterije potrebne za procjenu rizika.

U radu je predložena modifikacija opisanih metoda, kojom se na sustavan i jednoznačan način procjena rizika provodi bez implicitnih parametara i funkcija. Također, raspon vrijednosti procijenjenog rizika omogućava više fleksibilnosti u kasnijem postupku upravljanja rizikom, što može biti prednost, pogotovo kod kompleksnih sustava s velikim brojem resursa, pošto omogućava preciznije rangiranje i efikasnu prioritizaciju kritičnih elemenata.

10. LITERATURA

- [1] ISO/IEC TR 13335-3, *Information technology – Guidelines for the management of IT security*, 1st edition, 1998.
- [2] PD 3002:2002, *Guide to BS 7799 Risk Assessment*, British Standards Institution, 2002.
- [3] Ronald L. Krutz, Russell Dean Vines, *The CISSP Prep Guide—Mastering the Ten Domains of Computer Security*, John Wiley & Sons, Inc., 2001.
- [4] H. Šegudović, *Upravljanje sigurnošću informacijskih sustava*, KOM 2003 p III-31, 2003 (in Croatian).
- [5] CARNet CERT & LSS, *Upravljanje sigurnosnim rizicima*, CARNet CERT, 2003 (in Croatian).
- [6] ISO/IEC 27001, *Information technology – Security techniques – Information security management systems – Requirements*, 1st edition, 2005.
- [7] ISO/IEC 17799, *Information technology – Security techniques – Code of practice for Information security management*, 2nd edition, 2005.