

DRŽAVNA UPRAVA ZA ZAŠTITU I SPAŠAVANJE

1221

Na temelju članka 11. stavka 3. Zakona o kritičnim infrastrukturama (»Narodne novine«, broj 56/13), ravnatelj Državne uprave za zaštitu i spašavanje donosi

PRAVILNIK

O METODOLOGIJI ZA IZRADU ANALIZE RIZIKA POSLOVANJA KRITIČNIH INFRASTRUKTURA

I. OPĆE ODREDBE

Članak 1.

(1) Ovim Pravilnikom utvrđuju se smjernice, kriteriji i mjerila za identifikaciju kritičnih infrastrukture i analizu rizika poslovanja kritičnih infrastrukture te nositelji i obveze nositelja izrade analize rizika poslovanja kritičnih infrastrukture koja je sastavni dio procesa procjene rizika.

(2) Smjernice i kriteriji za analizu rizika iz stavka 1. ovog članka sukladni su ISO 31000:2009 standardu za upravljanje rizicima.

Članak 2.

Pojedini izrazi u smislu ovog Pravilnika imaju sljedeće značenje:

1. *Analiza kritičnosti* je postupak identifikacije sustava, mreža i objekata od nacionalne važnosti čiji prekid djelovanja ili prekid isporuke roba ili usluga može imati ozbiljne posljedice na nacionalnu sigurnost, zdravlje i živote ljudi, imovinu i okoliš, sigurnost i ekonomsku stabilnost i neprekidno funkcioniranje vlasti.

2. *Analiza rizika* je proces za razumijevanje prirode rizika i određivanje njegove razine što osigurava temelj za njegovo vrednovanje i odluku o obradi rizika, uključujući detaljnu razradu i gradaciju prijetnji, ranjivosti, vjerojatnosti i posljedica i utvrđivanje kriterija za dobivanje razine rizika.

3. *Događaj* je pojava ili promjena određene skupine okolnosti. Događaj može biti jedna ili više pojava i može imati nekoliko uzroka, a može sadržavati i nešto što se ne događa. Događaj se ponekad može označiti kao »incident« ili »nesreća«. Događaj bez posljedica se može označiti kao »bliski promašaj, incident ili događaj koji je mogao biti koban.

4. *Elementi rizika* su materijalna i nematerijalna imovina u okviru kritične infrastrukture koja može biti oštećena ili uništena, što može imati posljedica na funkciju kritične infrastrukture.

5. *Identifikacija rizika* je proces pronalaženja, prepoznavanja i opisivanja rizika.

6. *Kaskadni događaj – kvar* je poremećaj infrastrukture koji je uzrokovan drugim događajem u istoj ili drugoj infrastrukturi.

7. *Kriterij prihvatljivosti rizika* je opis uvjeta prema kojem se odlučuje o prihvatljivosti rizika.

8. *Kriterij rizika* je opis uvjeta prema kojima se vrednuje razina rizika, a temelji se na ciljevima kritične infrastrukture te vanjskom i unutarnjem kontekstu. Kriteriji rizika mogu proizlaziti iz propisa, politika ili drugih uvjeta.
9. *Međuvisnost kritičnih infrastrukture* je dvosmjerna ovisnost između dviju ili više kritičnih infrastrukture, pri čemu stanje jedne utječe ili je u korelaciji sa stanjem drugih kritičnih infrastrukture i obratno.
10. *Operativne karakteristike* su karakteristike koje ima kritična infrastruktura kada normalno radi.
11. *Ovisnost kritičnih infrastrukture* je povezanost ili veza između dvije ili više kritičnih infrastrukture pri čemu stanje jedne utječe ili je u korelaciji sa stanjem druge kritične infrastrukture. Ovisnost može biti fizička, informacijska, logička, zemljopisna, itd.
12. *Posljedica* je rezultat događaja koji utječe na ciljeve, a može biti određena ili neodređena i može imati pozitivne ili negativne učinke na ciljeve te može biti izražena kvalitativno ili kvantitativno. Jedan događaj može voditi nizu posljedica, a početna posljedica može eskalirati putem sekundarnih/naknadnih učinaka.
13. *Prijetnja* je mogući uzrok neželjenog događaja koji može izazvati štetu kritičnoj infrastrukturi.
14. *Prijetnja antropogena* je mogući uzrok neželjenog događaja izazvan djelovanjem ili ne djelovanjem ljudi što može izazvati štetu na kritičnoj infrastrukturi.
15. *Prijetnja prirodnih sila* je uzrok neželjenog događaja izazvana djelovanjem prirodnih sila (potresi, poplave, itd.) što može izazvati štetu na kritičnoj infrastrukturi.
16. *Prijetnja tehničko-tehnološka* je uzrok neželjenog događaja izazvan djelovanjem tehničkim i/ili tehnološkim sustavima što može izazvati štetu na kritičnoj infrastrukturi.
17. *Prijetnja biološko-kemijska* je uzrok neželjenog događaja izazvan djelovanjem biološkim i/ili kemijskim sredstvima što može izazvati štetu na kritičnoj infrastrukturi.
18. *Prihvatljivi rizik* je razina rizika koju je društvo svjesno spremno prihvatiti, obzirom na društvenu, političku i gospodarsku analizu koristi i troškova.
19. *Procjena rizika* je cjelokupni proces identifikacije rizika, analize rizika i vrednovanja (evaluacije) rizika.
20. *Razina rizika* je veličina rizika ili kombinacije rizika, izražena indeksom kritičnosti dobivenim umnoškom posljedica i njihove vjerojatnosti.
21. *Ranjivost* je obilježje elemenata rizika koje ga čini podložnima štetnim utjecajima prijetnji.
22. *Rizik* je učinak neizvjesnosti za ciljeve kritične infrastrukture, a koji se karakterizira u odnosu na kombinaciju potencijalnih događaja i posljedica. Pod učinkom se smatra odstupanje od očekivane funkcionalnosti kritične infrastrukture, a neizvjesnost je stanje, čak i djelomičnog, nedostatka informacija o događajima i posljedicama.
23. *Scenarij rizika* je prikaz događaja jednog ili više vrsta rizika koji izazivaju štetne posljedice na kritičnoj infrastrukturi, a koji su odabrani radi detaljne procjene određene vrste rizika.
24. *Vjerojatnost* je mogućnost pojave šetnog događaja, bilo da je događaj definiran, mjeran ili utvrđen objektivno ili subjektivno, kvalitativno ili kvantitativno i opisan uz upotrebu općih termina ili matematički (kao što je mogućnost ili učestalost u danom vremenskom periodu).
25. *Vlasnik/upravitelj infrastrukture* je fizička ili pravna osoba odgovorna i ovlaštena za upravljanje kritičnom infrastrukturuom.
26. *Vrednovanje (evaluacija) rizika* je postupak usporedbe rezultata analize rizika s kriterijima prihvatljivosti rizika.

Središnja tijela državne uprave, u suradnji s nadležnim regulatornim agencijama, u svom djelokrugu radi izrade analize rizika:

- provode postupak za identifikaciju kritičnih infrastrukture
- vode bazu podataka kritičnih infrastrukture
- utvrđuju sektorska mjerila za analizu rizika kritičnih infrastrukture
- izrađuju sektorsku analizu rizika poslovanja kritičnih infrastrukture.

Članak 4.

Vlasnici/upravitelji kritičnih infrastrukture izrađuju procjenu rizika poslovanja kritičnih infrastrukture kojih su vlasnici i/ili kojima upravljaju.

II. POSTUPCI IDENTIFIKACIJE KRITIČNIH INFRASTRUKTURA

Članak 5.

(1) Identifikacija kritičnosti infrastrukture u pravilu se izrađuje za svaki sustav, mrežu i objekt infrastrukture u djelokrugu nadležnosti središnjeg tijela državne uprave.

(2) Kriteriji za procjenu kritičnosti infrastrukture mogu biti:

- život i zdravlje – utvrđuje se utjecaj poremećaja i/ili prekida rada na život i zdravlje ljudi
- vremenski okvir – ako dođe do poremećaja/prekida rada određuje se u kojem će vremenu taj poremećaj/prekid imati posljedice na ukupno poslovanje/pružanje usluga (što je vrijeme kraće, veća je kritičnost)
- opseg – utvrđuje se koliko će ukupnog proizvoda i/ili usluga biti pogođeno u slučaju poremećaja ili potpunog prekida rada
- zakonski, regulatorni i ugovorni značaj
- gospodarska/financijska šteta.

(3) Središnje tijelo državne uprave može koristiti i druge kriterije za procjenu kritičnosti infrastrukture i odlučiti koje će i koliko kriterija istodobno primijeniti te koju će klasifikaciju koristiti unutar utvrđenih kriterija.

Članak 6.

(1) Kritičnost infrastrukture se izražava razinom rizika. Razina rizika određuje rang rizika, odnosno indeks kritičnost.

(2) Posljedice događaja definiraju se, u pravilu, u odnosu na utjecaj štete/kvara/prestanka rada infrastrukture na:

- zdravlje, sigurnost i okoliš
- proizvode i usluge
- vrijeme potrebno za popravak, obnovu ili oporavak.

(3) Vjerojatnost događaja (kvara/prestanka rada) definira se u odnosu na vrstu, karakter i namjenu infrastrukture, a uključuje i sljedeće pokazatelje:

- učestalost događaja u prošlosti
- pouzdanost u razdoblju prije nastanka kvara/prestanka rada
- način uporabe

- način održavanja
- normiranu uporabu
- uvjete pružanja usluga.

(4) Nositelj izrade procjene rizika može uključiti i druge pokazatelje za izračun razine rizika, sukladno karakteristikama i specifičnostima infrastrukture.

(5) Procjena kritičnosti infrastrukture rezultira identifikacijom svih kritičnih objekata, mreža, procesa, pod-procesa, sustava i pod-sustava.

III. POSTUPCI PROCJENE RIZIKA

1. Izrada scenarija i analiza prijetnje

Članak 7.

(1) Scenarij rizika je opis mogućih događaja koji mogu imati neizvjestan utjecaj na postizanje ciljeva kritične infrastrukture.

(2) Dobro razvijen scenarij rizika pretpostavka je za uspješnost identifikacije rizika, analizu i njihovu daljnju obradu.

(3) Scenarij rizika može se razviti koristeći dva različita mehanizma:

- top-down (prema dolje) pristup, pri čemu se polazi od ukupnih ciljeva kritične infrastrukture i provodi analiza onih najrealnijih scenarija rizika koji mogu utjecati na ciljeve
- bottom-up (prema gore) pristup, pri čemu se koristi generički popis scenarija pojedinačnih rizika na temelju čega se definira skup više relevantnih scenarija u okviru jednog prilagođenog scenarija, primijenjen na pojedinačne situacije u kojima se može naći kritična infrastruktura.

(4) Pristupi su komplementarni i mogu se koristiti istovremeno. Scenariji rizika moraju biti relevantni i povezani s realnim rizicima kritične infrastrukture.

(5) Uporaba generičkog popisa scenarija rizika može pomoći da se identificiraju rizici i povećaju mogućnosti da glavni scenarij bude sveobuhvatan i referentan za kritičnu infrastrukturu.

(6) U izradi scenarija u obzir se uzimaju rizici koji mogu imati utjecaj na ciljeve i zahtjeve ostvarenja ciljeva svake kritične infrastrukture.

(7) Generički popis scenarija prilagođava se specifičnoj situaciji svake kritične infrastrukture.

(8) Analiza prijetnje i razvoj scenarija obuhvaćaju sljedeće postupke:

- izradu popisa prijetnji – opisuju se opće karakteristike prijetnje, njihov intenzitet, trajanje i mogući učinci (Prilog 2.)
- procjenu očekivane izloženosti – utvrđuje se koji objekti, sustavi/pod-sustavi i procesi/pod-procesi mogu biti pogođeni
- procjenu očekivanog intenziteta prijetnje
- procjenu očekivanog trajanja prijetnje
- rano upozoravanje – utvrđuje se koje je očekivano vrijeme između upozorenja i štetnog događaja
- utvrđivanje sekundarnih učinaka (psihološki učinci događaja, utjecaj na javnost i medije i slično)