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 infrastruktura i analizu rizika poslovanja kritičnih infrastruktura te nositelji i obveze nositelja izrade analize rizika poslovanja kritičnih infrastruktura 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. *Međuovisnost kritičnih infrastruktura* je dvosmjerna ovisnost između dviju ili više kritičnih infrastruktura, pri čemu stanje jedne utječe ili je u korelaciji sa stanjem drugih kritičnih infrastruktura i obratno.

10. *Operativne karakteristike* su karakteristike koje ima kritična infrastruktura kada normalno radi.

11. *Ovisnost kritičnih infrastruktura* je povezanost ili veza između dvije ili više kritičnih infrastruktura 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 štetnog događaja, bilo da je događaj definiran, mjeren 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 infrastrukturom.

26. *Vrednovanje (evaluacija) rizika* je postupak usporedbe rezultata analize rizika s kriterijima prihvatljivosti rizika.

Članak 3.

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

– provode postupak za identifikaciju kritičnih infrastruktura

– vode bazu podataka kritičnih infrastruktura

– utvrđuju sektorska mjerila za analizu rizika kritičnih infrastruktura

– izrađuju sektorsku analizu rizika poslovanja kritičnih infrastruktura.

Članak 4.

Vlasnici/upravitelji kritičnih infrastruktura izrađuju procjenu rizika poslovanja kritičnih infrastruktura 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)

– utvrđivanje podataka o štetnim događajima – utvrđuje se koji se usporedivi štetni događaji mogu razmotriti za dobivanje detaljnijih podataka (povijesni podaci)

– utvrđivanje vjerojatnosti štetnog događaja – utvrđuje se koja se vjerojatnost nastanka štetnog događaja može očekivati ili identificirati.

(9) Scenarij se razvija na temelju popisa prijetnji i relevantnih podataka karakterističnih za sektor kritičnih infrastruktura. Scenariji moraju predstavljati realne događaje koji mogu rezultirati prekidom ili narušavanjem rada kritičnih infrastruktura i/ili prekidom roba i usluga.

(10) U scenarije se obvezno uključuju elementi ovisnosti i međuovisnosti kritičnih infrastruktura koji mogu povećati učinke i posljedice štetnih događaja, što izravno utječe na sektorski plan osiguranja rada kritičnih infrastruktura i sigurnosni plan zaštite kritičnih infrastruktura.

(11) Broj scenarija koji se razvijaju ovisan je o identificiranim prijetnjama i karakteristikama sektora odnosno kritičnih infrastruktura, a izrađuju se za svaki pojedini relevantni događaj posebno.

(12) Scenariji se obvezno testiraju, aktualiziraju i nadopunjuju najmanje jednom godišnje, a po potrebi i češće.

2. Identifikacija rizika

Članak 8.

(1) Rizik je određen prijetnjama čija je pojavnost moguća i vezana za iskorištenje ranjivosti kritičnih infrastruktura te mogu imati negativan utjecaj na ciljeve kritične infrastrukture.

(2) Objedinjavanje relevantnih podataka o prijetnjama i ranjivosti rezultira identifikacijom rizika po elementima rizika, sustavima/pod-sustavima i procesima/pod-procesima.

(3) Elementi rizika obuhvaćaju, osobito:

– ljude – osoblje i druge osobe u kontekstu održavanja funkcionalnosti infrastrukture i/ili pojedinih dijelova infrastrukture

– zemljište – vanjski prostor koji uključuje područja od važnosti za rad i operativnost infrastrukture, putove, skladišta, parkirne površine, zelene površine i slično

– građevine ispod i iznad zemlje (proizvodne hale, skladišta, administrativne građevine, garaže i slično)

– postrojenja i opremu – uključivo izvore napajanja strujom, plinom, vodom, grijanje, informacijsku i komunikacijsku tehnologiju, transport

– specijalizirana postrojenja i opremu

– podatke i datoteke koji uključuju sve podatke potrebne za održavanje procesa i sustava koji se čuvaju u pisanom i/ili elektroničkom obliku.

3. Analiza rizika

Članak 9.

(1) Analizom rizika utvrđuju se učinci i posljedice prekida rada ili značajnog narušavanja rada kritičnih infrastruktura koji mogu nastati kao posljedica prirodne prijetnje, tehničko-tehnološke prijetnje, prijetnje koja je nastala ljudskom djelatnošću (antropogena prijetnja) ili višestruke prijetnje.

(2) Analiza rizika uključuje:

– prikupljanje i analizu referentnih podataka te izradu baze podataka

– izradu scenarija mogućih događaja i rizika (najgori slučaj, najvjerojatniji slučaj)

– identifikaciju i utvrđivanje karakteristika kritičnih infrastruktura

– identifikaciju mogućih opasnosti i procjenu izloženosti

– identifikaciju elemenata rizika

– analizu kritičnosti

– analizu ranjivosti i otpornosti kritičnih infrastruktura na pojedine opasnosti

– utvrđivanje učinaka i posljedica neželjenih događaja na kritične infrastrukture ili dijelove kritičnih infrastruktura te na proizvode i usluge

– odabir i implementaciju metoda za izračun rizika

– uspoređivanje i evaluaciju rizika

– utvrđivanje prihvatljivosti rizika

– analizu ovisnosti i međuovisnosti kritičnih infrastruktura.

(3) U postupku analize rizika obvezno se uzimaju u obzir i izrađuju:

1. međusektorska mjerila

2. identifikacija rizika

3 .kriteriji za procjenu kritičnosti

4. analiza prijetnje i razvoj scenarija

5. analiza ranjivosti

6. metode za izračun rizika

7. analiza jednostrukog i višestrukog rizika

8. vrednovanje rizika.

4. Analiza ranjivosti

Članak 10.

(1) Ranjivost kritičnih infrastruktura, njezinih dijelova ili elemenata rizika od presudne je važnosti za određivanje u kojoj je mjeri sektor, infrastruktura ili njezin dio pogođen i kakve su nastale štete. Što je ranjivost veća, veći su učinci i posljedice štetnog događaja na proizvode i usluge.

(2) Mjerila i kriteriji za identifikaciju ranjivosti su:

– ovisnost infrastrukture o elementima rizika – ako proces ili sustav ovisi o elementima rizika kako bi ispunio svoje zadaće, potencijalni manjak i/ili zamjena tih elemenata čini proces ili sustav ranjivim; u analizi rizika pomoću ovog kriterija utvrđuje se važnost elemenata rizika na sustave i procese

– ovisnost elemenata rizika o drugim infrastrukturama – ako element rizika ovisi o drugoj infrastrukturi kako bi ispunio svoje zadaće i funkciju, potencijalni nedostatak i/ili zamjena te infrastrukture čini element ranjivim

– otpornost – fizička otpornost elemenata rizika (građevina, opreme, postrojenja) je važan čimbenik za utvrđivanje hoće li u slučaju nesreće elementi biti oštećeni i imaju učinke na relevantne sustave i procese, mreže i objekte

– stvarna razina zaštite – elementi su ranjivi ako nisu u dovoljnoj mjeri zaštićeni od prijetnji

– zalihe i zamjene – ako štetan događaj pogodi elemente rizika, nastali problem je lakše riješiti ako postoje rezervni/zamjenski elementi koji će izvršavati iste zadaće/funkcije

– obnova – sposobnost i mogućnost obnove u kontekstu ranjivosti odnosi se na potrebna financijska sredstva i kadrove te uloženo vrijeme obnove

– prilagodljivost – sustavi i procesi su ranjivi ako se ne mogu jednostavno prilagoditi

– sposobnost amortiziranja – sposobnost sustava i procesa da podnesu učinke štetnog događaja do određenog stupnja i da ne budu određeno vrijeme pogođeni negativnim djelovanjem

– transparentnost – mora biti jasno vidljivo i razumljivo kako se elementi rizika spajaju i kako funkcioniraju, da bi se u slučaju štetnog događaja brzo popravili ili zamijenili

– ovisnost o posebnim uvjetima okoliša – infrastruktura radi pod okolnim uvjetima koji prevladavaju na lokaciji i ako ovisi o tim specifičnim okolnim uvjetima ranjiva je u odnosu na potencijalne promjene tih uvjeta.

5. Međusektorska mjerila

Članak 11.

(1) U postupku analize rizika poslovanja kritičnih infrastruktura koriste se međusektorska mjerila, definirana u odnosu na posljedice negativnog događaja:

1. posljedice po ljudske živote i ljudsko zdravlje – procjenjuje se broj smrtno stradalih osoba, ozlijeđenih osoba, oboljelih

osoba, osoba sa trajnim tjelesnim invaliditetom, broj premještenih i/ili raseljenih osoba

2. posljedice u gospodarstvu, okolišu i financijama – procjenjuju se i iskazuju kvantitativno kao troškovi prekida gospodarskih aktivnosti, vrijednosti isplaćenih premija osiguranja, troškovi liječenja i medicinskih postupaka, troškovi neposrednih i/ili dugoročnih hitnih mjera, troškovi obnove i/ili izgradnje građevina, prometne i druge infrastrukture, javnog prijevoza, poštanskog i bankarskog prometa i usluga, troškovi ekološke obnove i drugi ekološki troškovi koji uključuju i nenadoknadive (trajne) ekološke štete, troškovi obnove kulturne baštine koji uključuju štete nastale uništenjem nenadoknadive kulturne baštine, druge specifične izravne i neizravne štete i troškove

3. socio-političke posljedice i utjecaj na javnost – procjena uključuje kategorije kao što su gubitak povjerenja javnosti, javni red i mir te sigurnost građana, socio-psihološki utjecaj, narušavanje svakodnevnog života koje uključuje osnovne i/ili javne usluge te političke posljedice.

(2) Pored mjerila iz stavka 1. ovog članka, u pojedinim sektorima u postupku analize rizika poslovanja kritičnih infrastruktura koriste se posebna sektorska mjerila i elementi rizika koja utvrđuju nadležna tijela državne uprave u suradnji s nadležnim regulatornim agencijama.

6. Metode za izračun rizika

Članak 12.

(1) Metode za izračun rizika mogu biti:

– kvalitativne – koje daju grube procjene rizika u obliku teksta, bez izrade i mogućnosti numeričke usporedivosti (Prilog 1.)

– polu – kvantitativne – koje koriste klasifikaciju sustava za procjenu vrijednosti pojedinačnih faktora rizika tako da se oni mogu uspoređivati u numeričkom obliku

– kvantitativne – kojima se matematički izračunavaju faktori rizika.

(2) Odabir metode za izračun rizika ovisan je o specifičnostima sektora i svojstvima kritičnih infrastruktura.

7. Analiza jednostrukog i višestrukog rizika

Članak 13.

(1) Analizom jednostrukog rizika utvrđuje se mogućnost i posljedice određenog štetnog događaja/prijetnje koji se pojavljuje

u nekom zemljopisnom području u određenom vremenskom razdoblju odvojeno od drugih štetnih događaja. Nakon utvrđivanja svih značajnih pojedinačnih rizika može se provesti ukupna evaluacija rizika.

(2) Analizom višestrukih rizika utvrđuje se ukupni učinak svih rizika na objekte, mreže i sustave, uzimajući u obzir međusobno djelovanje mogućih opasnosti i osjetljivosti.

(3) U analizi višestrukih rizika, kada jedan štetni događaj uzrokuje jedan ili više naknadnih štetnih događaja, uzimaju se u obzir naknadni učinci štetnih događaja (sekundarni učinak, domino učinak, kaskadno djelovanje).

8. Vrednovanje rizika

Članak 14.

(1) Vrednovanje rizika je proces usporedbe rezultata analize rizika s kriterijima rizika da bi se utvrdilo da li je rizik prihvatljiv, odnosno da li je prihvatljiva njegova veličina.

(2) U slučaju da je rizik veći od predviđenog, vlasnik/upravitelj kritične infrastrukture utvrđuje mjere za smanjenje rizika.

(3) Vrednovanje rizika treba pokazati može li biti postignuta unaprijed definirana i planirana razina zaštite kritičnih infrastruktura i/ili njezinih dijelova u odnosu na utvrđene rizike.

IV. OVISNOST I MEĐUOVISNOST KRITIČNIH INFRASTRUKTURA

Članak 15.

(1) Nositelji izrade sektorske analize rizika poslovanja kritičnih infrastruktura i analize rizika poslovanja kritičnih infrastruktura pri procjenjivanju rizika i potrebnog stupnja zaštite obvezno uzimaju u obzir ovisnost i međuovisnost kritičnih infrastruktura.

(2) Kritične infrastrukture mogu istovremeno biti ovisne o više drugih infrastruktura unutar jednog sektora, kao i o više drugih infrastruktura iz drugih sektora.

(3) Međuovisnost kritičnih infrastruktura izravno i neizravno utječe na njihovo funkcioniranje te se kod izračuna rizika moraju uzeti u obzir i ovisnosti koje utječu na promatranu infrastrukturu, kao i ovisnosti drugih kritičnih infrastruktura o promatranoj kritičnoj infrastrukturi.

Članak 16.

Za utvrđivanje i analizu međuovisnosti kritičnih infrastruktura u obzir se uzimaju sljedeće značajke:

1. karakteristike infrastrukture – organizacijske, operativne, vremenske, prostorne

2. stanje rada – normalno/redovno, poremećeno, popravak i obnova

3. vrste međuovisnosti – fizička, zemljopisna, informatička, logička

4. okruženje/okolina infrastrukture – gospodarsko, poslovno, tehničko, socio-političko, pravno i regulatorno, zdravstveno, sigurnosno, javna politika

5. sprega/povezanost i ponašanje u reakciji – stupanj sprege (labava, čvrsta), vrsta međuovisnosti (linearna, kompleksna), ponašanje u reakciji (nepopustljivo/neelastično, prilagodljivo)

6. vrste kvara – kaskadni, eskalirajući, kvar s istim uzrokom.

Članak 17.

(1) Nositelji izrade sektorske analize rizika poslovanja kritičnih infrastruktura za utvrđivanje i analizu međuovisnosti kritičnih infrastruktura surađuju i razmjenjuju podatke s nositeljima analize rizika kritičnih infrastruktura iz drugih sektora i vlasnicima/upraviteljima kritičnih infrastruktura, u cilju sagledavanja međuovisnosti i s njima povezanih rizika i ranjivosti pojedinih kritičnih infrastruktura.

(2) Središnja tijela državne uprave i regulatorne agencije obvezne su vlasnicima/ upraviteljima kritičnih infrastruktura iz svoga sektora dostavljati podatke od značaja za izradu analize rizika kritičnih infrastruktura kojima upravljaju te pružati stručnu pomoć u definiranju i primjeni međusektorskih i sektorskih mjerila za analizu prijetnji, rizika i ranjivosti identificiranih kritičnih infrastruktura i izradu njihovih sigurnosnih planova.

V. PRIJELAZNE I ZAVRŠNE ODREDBE

Članak 18.

(1) Središnja tijela državne uprave u suradnji s nadležnim regulatornim agencijama i strukovnim udrugama dužna su predložiti Vladi Republike Hrvatske kritične infrastrukture u sektorima iz svoga djelokruga u roku od šest mjeseci od dana stupanja na snagu ovog Pravilnika.

(2) Središnja tijela državne uprave u suradnji s nadležnim regulatornim agencijama dužna su izraditi sektorske analize rizika kritičnih infrastruktura u sektorima iz svojega djelokruga u roku od dvanaest mjeseci od dana stupanja na snagu ovog Pravilnika.

(3) Vlasnici/upravitelji kritičnih infrastruktura dužni su izraditi analizu rizika kritične infrastrukture kojom upravlja u roku od šest mjeseci od dana primitka odluke kojom čelnik nadležnog središnjeg tijela državne uprave određuje nacionalne kritične infrastrukture.

Članak 19.

Danom stupanja na snagu ovoga Pravilnika prestaje važiti Pravilnik o metodologiji za izradu analize rizika poslovanja kritičnih infrastruktura (»Narodne novine«, broj 128/13).

Članak 20.

Ovaj Pravilnik stupa na snagu osmog dana od dana objave u »Narodnim novinama«.

Klasa: 012-02/16-03/01

Urbroj: 543-01-08-01-16-11

Zagreb, 4. svibnja 2016.

Ravnatelj
dr. sc. Jadran Perinić, v. r.

PRILOG 1. – PRILOG 3.