ZAKON
O INFORMACIONOJ BEZBEDNOSTI

("Službeni glasnik RS", br. 6/16 , 94/17 i 77/19)

Prečišćen tekst zaključno sa izmenama iz "Službenog glasnika RS", broj 77/19 koje su u primeni od 08.11.2019. (izmene u čl.: 2 , 3a , 5 , 6 , 6a , 6b , 7 , 11 , 11a , 11b , 12 , 13 , 13a , 14 , 15 , 15a , 16 , 17 , 18 , 19 , 19a , 30 , 31).

I. OSNOVNE ODREDBE

Predmet uređivanja

Član 1.

Ovim zakonom se uređuju mere zaštite od bezbednosnih rizika u informaciono-komunikacionim sistemima, odgovornosti pravnih lica prilikom upravljanja i korišćenja informaciono-komunikacionih sistema i određuju se nadležni organi za sprovođenje mera zaštite, koordinaciju između činilaca zaštite i praćenje pravilne primene propisanih mera zaštite.

Značenje pojedinih termina

Član 2.

Pojedini termini u smislu ovog zakona imaju sledeće značenje:

1) informaciono-komunikacioni sistem (IKT sistem) je tehnološko-organizaciona celina koja obuhvata:

(1) elektronske komunikacione mreže u smislu zakona koji uređuje elektronske komunikacije;

(2) uređaje ili grupe međusobno povezanih uređaja, takvih da se u okviru uređaja, odnosno u okviru barem jednog iz grupe uređaja, vrši automatska obrada podataka korišćenjem računarskog programa;

(3) podatke koji se **vode, čuvaju**, obrađuju, pretražuju ili prenose pomoću sredstava iz podtač. (1) i (2) ove tačke, a u svrhu njihovog rada, upotrebe, zaštite ili održavanja;

(4) organizacionu strukturu putem koje se upravlja IKT sistemom;

(5) sve tipove sistemskog i aplikativnog softvera i softverske razvojne alate;

2) operator IKT sistema je pravno lice, **organ vlasti ili organizaciona jedinica organa vlasti** koji koristi IKT sistem u okviru obavljanja svoje delatnosti, odnosno poslova iz svoje nadležnosti;

3) informaciona bezbednost predstavlja skup mera koje omogućavaju da podaci kojima se rukuje putem IKT sistema budu zaštićeni od neovlašćenog pristupa, kao i da se zaštiti integritet, raspoloživost, autentičnost i neporecivost tih podataka, da bi taj sistem funkcionisao kako je predviđeno, kada je predviđeno i pod kontrolom ovlašćenih lica;

4) tajnost je svojstvo koje znači da podatak nije dostupan neovlašćenim licima;

5) integritet znači očuvanost izvornog sadržaja i kompletnosti podatka;

6) raspoloživost je svojstvo koje znači da je podatak dostupan i upotrebljiv na zahtev ovlašćenih lica onda kada im je potreban;

7) autentičnost je svojstvo koje znači da je moguće proveriti i potvrditi da je podatak stvorio ili poslao onaj za koga je deklarisano da je tu radnju izvršio;

8) neporecivost predstavlja sposobnost dokazivanja da se dogodila određena radnja ili da je nastupio određeni događaj, tako da ga naknadno nije moguće poreći;

9) rizik znači mogućnost narušavanja informacione bezbednosti, odnosno mogućnost narušavanja tajnosti, integriteta, raspoloživosti, autentičnosti ili neporecivosti podataka ili narušavanja ispravnog funkcionisanja IKT sistema;

10) upravljanje rizikom je sistematičan skup mera koji uključuje planiranje, organizovanje i usmeravanje aktivnosti kako bi se obezbedilo da rizici ostanu u propisanim i prihvatljivim okvirima;

11) **incident je svaki događaj koji ima stvaran negativan uticaj na bezbednost mrežnih i informacionih sistema;**

11a) jedinstveni sistem za prijem obaveštenja o incidentima je informacioni sistem u koji se unose podaci o incidentima u IKT sistemima od posebnog značaja koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti;

12) mere zaštite IKT sistema su tehničke i organizacione mere za upravljanje bezbednosnim rizicima IKT sistema;

13) tajni podatak je podatak koji je, u skladu sa propisima o tajnosti podataka, određen i označen određenim stepenom tajnosti;

14) IKT sistem za rad sa tajnim podacima je IKT sistem koji je u skladu sa zakonom određen za rad sa tajnim podacima;

15) **organ vlasti je državni organ, organ autonomne pokrajine, organ jedinice lokalne samouprave, organizacija i drugo pravno ili fizičko lice kome je povereno vršenje javnih ovlašćenja;**

16) služba bezbednosti je služba bezbednosti u smislu zakona kojim se uređuju osnove bezbednosno-obaveštajnog sistema Republike Srbije;

17) samostalni operatori IKT sistema su ministarstvo nadležno za poslove odbrane, ministarstvo nadležno za unutrašnje poslove, ministarstvo nadležno za spoljne poslove i službe bezbednosti;

18) kompromitujuće elektromagnetno zračenje (KEMZ) predstavlja nenamerne elektromagnetne emisije prilikom prenosa, obrade ili čuvanja podataka, čijim prijemom i analizom se može otkriti sadržaj tih podataka;

19) kriptobezbednost je komponenta informacione bezbednosti koja obuhvata kriptozaštitu, upravljanje kriptomaterijalima i razvoj metoda kriptozaštite;

20) kriptozaštita je primena metoda, mera i postupaka radi transformisanja podataka u oblik koji ih za određeno vreme ili trajno čini nedostupnim neovlašćenim licima;

21) kriptografski proizvod je softver ili uređaj putem koga se vrši kriptozaštita;

22) kriptomaterijali su kriptografski proizvodi, podaci, tehnička dokumentacija kriptografskih proizvoda, kao i odgovarajući kriptografski ključevi;

23) bezbednosna zona je prostor ili prostorija u kojoj se, u skladu sa propisima o tajnosti podataka, obrađuju i čuvaju tajni podaci;

24) **informaciona dobra obuhvataju podatke u datotekama i bazama podataka, programski kôd, konfiguraciju hardverskih komponenata, tehničku i korisničku dokumentaciju, zapise o korišćenju hardverskih komponenti, podataka iz datoteka i baza podataka i sprovođenju procedura ako se isti vode, unutrašnje opšte akte, procedure i slično;**

25) usluga informacionog društva je usluga u smislu zakona kojim se uređuje elektronska trgovina;

26) pružalac usluge informacionog društva je pravno lice koje je pružalac usluge u smislu zakona kojim se uređuje elektronska trgovina.

Načela

Član 3.

Prilikom planiranja i primene mera zaštite IKT sistema treba se rukovoditi načelima:

1) načelo upravljanja rizikom - izbor i nivo primene mera se zasniva na proceni rizika, potrebi za prevencijom rizika i otklanjanja posledica rizika koji se ostvario, uključujući sve vrste vanrednih okolnosti;

2) načelo sveobuhvatne zaštite - mere se primenjuju na svim organizacionim, fizičkim i tehničko-tehnološkim nivoima, kao i tokom celokupnog životnog ciklusa IKT sistema;

3) načelo stručnosti i dobre prakse - mere se primenjuju u skladu sa stručnim i naučnim saznanjima i iskustvima u oblasti informacione bezbednosti;

4) načelo svesti i osposobljenosti - sva lica koja svojim postupcima efektivno ili potencijalno utiču na informacionu bezbednost treba da budu svesna rizika i poseduju odgovarajuća znanja i veštine.

Obrada podataka o ličnosti

Član 3a

U slučaju obrade podataka o ličnosti prilikom vršenja nadležnosti i ispunjenja obaveza iz ovog zakona postupa se u skladu sa propisima koji uređuju zaštitu podataka o ličnosti.

Nadležni organ

Član 4.

Organ državne uprave nadležan za bezbednost IKT sistema je ministarstvo nadležno za poslove informacione bezbednosti (u daljem tekstu: Nadležni organ).

Telo za koordinaciju poslova informacione bezbednosti

Član 5.

(1) U cilju ostvarivanja saradnje i usklađenog obavljanja poslova u funkciji unapređenja informacione bezbednosti, kao i iniciranja i praćenja preventivnih i drugih aktivnosti u oblasti informacione bezbednosti Vlada osniva Telo za koordinaciju poslova informacione bezbednosti (u daljem tekstu: Telo za koordinaciju), kao koordinaciono telo Vlade, u čiji sastav ulaze predstavnici ministarstava nadležnih za poslove informacione bezbednosti, odbrane, unutrašnjih poslova, spoljnih poslova, pravde, predstavnici službi bezbednosti, Kancelarije Saveta za nacionalnu bezbednost i zaštitu tajnih podataka, Generalnog sekretarijata Vlade, **Narodne banke Srbije**, **Centra za bezbednost IKT sistema u organima vlasti i Nacionalnog centra za prevenciju bezbednosnih rizika u IKT sistemima**.

(2) U funkciji unapređenja pojedinih oblasti informacione bezbednosti formiraju se stručne radne grupe Tela za koordinaciju u koje se uključuju i predstavnici drugih **organa vlasti**, privrede, akademske zajednice i nevladinog sektora.

(3) Odlukom kojom osniva Telo za koordinaciju Vlada određuje i njegov sastav, zadatke, rok u kome ono podnosi izveštaje Vladi i druga pitanja koja su vezana za njegov rad.

II. BEZBEDNOST IKT SISTEMA OD POSEBNOG ZNAČAJA

IKT sistemi od posebnog značaja

Član 6.

(1) IKT sistemi od posebnog značaja su sistemi koji se koriste:

1) u obavljanju poslova u organima vlasti;

2) za obradu posebnih vrsta podataka o ličnosti, u smislu zakona koji uređuje zaštitu podataka o ličnosti;

3) u obavljanju delatnosti od opšteg interesa i drugim delatnostima i to u sledećim oblastima:

(1) energetika:

- proizvodnja, prenos i distribucija električne energije;

- proizvodnja i prerada uglja;

- istraživanje, proizvodnja, prerada, transport i distribucija nafte i promet nafte i naftnih derivata;

- istraživanje, proizvodnja, prerada, transport i distribucija prirodnog i tečnog gasa;

(2) saobraćaj:

- železnički, poštanski, vodni i vazdušni saobraćaj;

(3) zdravstvo:

- zdravstvena zaštita;

(4) bankarstvo i finansijska tržišta:

- poslovi finansijskih institucija;

- poslovi vođenja registra podataka o obavezama fizičkih i pravnih lica prema finansijskim institucijama;

- poslovi upravljanja, odnosno obavljanja delatnosti u vezi sa funkcionisanjem regulisanog tržišta;

(5) digitalna infrastruktura:

- razmena internet saobraćaja;

- upravljanje registrom nacionalnog internet domena i sistemom za imenovanje na mreži (DNS sistemi);

(6) dobra od opšteg interesa:

- korišćenje, upravljanje, zaštita i unapređivanje dobara od opšteg interesa (vode, putevi, mineralne sirovine, šume, plovne reke, jezera, obale, banje, divljač, zaštićena područja);

(7) usluge informacionog društva:

- usluge informacionog društva u smislu člana 2. tačka 25) ovog zakona;

(8) ostale oblasti:

- elektronske komunikacije;
- izdavanje službenog glasila Republike Srbije;
- upravljanje nuklearnim objektima;
- proizvodnja, promet i prevoz naoružanja i vojne opreme;
- upravljanje otpadom;
- komunalne delatnosti;
- proizvodnja i snabdevanje hemikalijama;

4) u pravnim licima i ustanovama koje osniva Republika Srbija, autonomna pokrajina ili jedinica lokalne samouprave za obavljanje delatnosti iz tačke 3) ovog stava.

(2) Vlada, na predlog ministarstva nadležnog za poslove informacione bezbednosti, utvrđuje listu delatnosti iz stava 1. tačka 3) ovog člana.

Obaveze operatora IKT sistema od posebnog značaja

Član 6a

Operator IKT sistema od posebnog značaja u skladu sa ovim zakonom u obavezi je da:

1) upiše IKT sistem od posebnog značaja kojim upravlja u evidenciju operatora IKT sistema od posebnog značaja;

2) preduzme mere zaštite IKT sistema od posebnog značaja;

3) donese akt o bezbednosti IKT sistema;

4) vrši proveru usklađenosti primenjenih mera zaštite IKT sistema sa aktom o bezbednosti IKT sistema i to najmanje jednom godišnje;

5) uredi odnos sa trećim licima na način koji obezbeđuje preduzimanje mera zaštite tog IKT sistema u skladu sa zakonom, ukoliko poverava aktivnosti u vezi sa IKT sistemom od posebnog značaja trećim licima;

6) dostavlja obaveštenja o incidentima koji značajno ugrožavaju informacionu bezbednost IKT sistema;

7) dostavi tačne statističke podatke o incidentima u IKT sistemu.

Evidencija operatora IKT sistema od posebnog značaja

Član 6b

(1) Nadležni organ uspostavlja i vodi evidenciju IKT sistema od posebnog značaja (u daljem tekstu: Evidencija) koja sadrži:

1) naziv i sedište operatora IKT sistema od posebnog značaja;

2) ime i prezime, službena adresa za prijem elektronske pošte i službeni kontakt telefon administratora IKT sistema od posebnog značaja;

3) ime i prezime, službena adresa za prijem elektronske pošte i službeni kontakt telefon odgovornog lica IKT sistema od posebnog značaja;

4) podatak o vrsti IKT sistema od posebnog značaja, u skladu sa članom 6. ovog zakona.

(2) Pored podataka iz stava 1. ovog člana, evidencija može da sadrži i druge dopunske podatke o IKT sistemu od posebnog značaja koje propisuje Nadležni organ.

(3) Operator IKT sistema od posebnog značaja dužan je da IKT sistem od posebnog značaja kojim upravlja upiše u evidenciju iz stava 1. ovog člana.

(4) Operator IKT sistema od posebnog značaja dužan je da nadležnom organu dostavi podatke iz stava 1. ovog člana najkasnije 90 dana od dana usvajanja propisa iz stava 2. ovog člana, odnosno 90 dana od dana uspostavljanja IKT sistema od posebnog značaja.

(5) Nadležni organ stavlja na raspolaganje Nacionalnom centru za prevenciju bezbednosnih rizika u IKT sistemima (u daljem tekstu: Nacionalni CERT) ažurnu evidenciju iz stava 1. ovog člana.

Mere zaštite IKT sistema od posebnog značaja

Član 7.

(1) Operator IKT sistema od posebnog značaja odgovara za bezbednost IKT sistema i preduzimanje mera zaštite IKT sistema.

(2) Merama zaštite IKT sistema se obezbeđuje prevencija od nastanka incidenata, odnosno prevencija i **smanjenje** štete od incidenata koji ugrožavaju vršenje nadležnosti i obavljanje delatnosti, a posebno u okviru pružanja usluga drugim licima.

(3) Mere zaštite IKT sistema se odnose na:

1) uspostavljanje organizacione strukture, sa utvrđenim poslovima i odgovornostima zaposlenih, kojom se ostvaruje upravljanje informacionom bezbednošću u okviru operatora IKT sistema;

2) postizanje bezbednosti rada na daljinu i upotrebe mobilnih uređaja;

3) obezbeđivanje da lica koja koriste IKT sistem odnosno upravljaju IKT sistemom budu osposobljena za posao koji rade i razumeju svoju odgovornost;

4) zaštitu od rizika koji nastaju pri promenama poslova ili prestanka radnog angažovanja lica zaposlenih kod operatora IKT sistema;

5) identifikovanje informacionih dobara i određivanje odgovornosti za njihovu zaštitu;

6) klasifikovanje podataka tako da nivo njihove zaštite odgovara značaju podataka u skladu sa načelom upravljanja rizikom iz člana 3. ovog zakona;

7) zaštitu nosača podataka;

8) ograničenje pristupa podacima i sredstvima za obradu podataka;

9) odobravanje ovlašćenog pristupa i sprečavanje neovlašćenog pristupa IKT sistemu i uslugama koje IKT sistem pruža;

10) utvrđivanje odgovornosti korisnika za zaštitu sopstvenih sredstava za autentikaciju;

11) predviđanje odgovarajuće upotrebe kriptozaštite radi zaštite tajnosti, autentičnosti **i** integriteta podataka;

12) fizičku zaštitu objekata, prostora, prostorija odnosno zona u kojima se nalaze sredstva i dokumenti IKT sistema i obrađuju podaci u IKT sistemu;

13) zaštitu od gubitka, oštećenja, krađe ili drugog oblika ugrožavanja bezbednosti sredstava koja čine IKT sistem;

14) obezbeđivanje ispravnog i bezbednog funkcionisanja sredstava za obradu podataka;

15) zaštitu podataka i sredstva za obradu podataka od zlonamernog softvera;

16) zaštitu od gubitka podataka;

17) čuvanje podataka o događajima koji mogu biti od značaja za bezbednost IKT sistema;

18) obezbeđivanje integriteta softvera i operativnih sistema;

19) zaštitu od zloupotrebe tehničkih bezbednosnih slabosti IKT sistema;

20) obezbeđivanje da aktivnosti na reviziji IKT sistema imaju što manji uticaj na funkcionisanje sistema;

21) zaštitu podataka u komunikacionim mrežama uključujući uređaje i vodove;

22) bezbednost podataka koji se prenose unutar operatora IKT sistema, kao i između operatora IKT sistema i lica van operatora IKT sistema;

23) **ispunjenje zahteva za informacionu bezbednost** u okviru upravljanja svim fazama životnog ciklusa IKT sistema odnosno delova sistema;

24) zaštitu podataka koji se koriste za potrebe testiranja IKT sistema odnosno delova sistema;

25) zaštitu sredstava operatora IKT sistema koja su dostupna pružaocima usluga;

26) održavanje ugovorenog nivoa informacione bezbednosti i pruženih usluga u skladu sa uslovima koji su ugovoreni sa pružaocem usluga;

27) prevenciju i reagovanje na bezbednosne incidente, što podrazumeva adekvatnu razmenu informacija o bezbednosnim slabostima IKT sistema, incidentima i pretnjama;

28) mere koje obezbeđuju kontinuitet obavljanja posla u vanrednim okolnostima.

(4) Vlada, na predlog Nadležnog organa, bliže uređuje mere zaštite IKT sistema uvažavajući načela iz člana 3. ovog zakona, nacionalne i međunarodne standarde i standarde koji se primenjuju u odgovarajućim oblastima rada.

Akt o bezbednosti IKT sistema od posebnog značaja

Član 8.

(1) Operator IKT sistema od posebnog značaja dužan je da donese akt o bezbednosti IKT sistema.

(2) Aktom iz stava 1. ovog člana određuju se mere zaštite, a naročito principi, način i procedure postizanja i održavanja adekvatnog nivoa bezbednosti sistema, kao i ovlašćenja i odgovornosti u vezi sa bezbednošću i resursima IKT sistema od posebnog značaja.

(3) Akt iz stava 1. ovog člana mora da bude usklađen s promenama u okruženju i u samom IKT sistemu.

(4) Operator IKT sistema od posebnog značaja je dužan da samostalno ili uz angažovanje spoljnih eksperata vrši proveru usklađenosti primenjenih mera IKT sistema sa aktom iz stava 1. ovog člana i to najmanje jednom godišnje i da o tome sačini izveštaj.

(5) Bliži sadržaj akta iz stava 1. ovog člana, način provere IKT sistema od posebnog značaja i sadržaj izveštaja o proveri uređuje Vlada na predlog Nadležnog organa.

Poveravanje aktivnosti u vezi sa IKT sistemom od posebnog značaja trećim licima

Član 9.

(1) Operator IKT sistema od posebnog značaja može poveriti aktivnosti u vezi sa IKT sistemom trećim licima, u kom slučaju je obavezan da uredi odnos sa tim licima na način koji obezbeđuje preduzimanje mera zaštite tog IKT sistema u skladu sa zakonom.

(2) Aktivnostima iz stava 1. ovog člana (u daljem tekstu: poverene aktivnosti) smatraju se sve aktivnosti koje uključuju obradu, čuvanje, odnosno mogućnost pristupa podacima kojima raspolaže operator IKT sistema od

posebnog značaja, a odnose se na njegovo poslovanje, kao i aktivnosti razvoja, odnosno održavanja softverskih i hardverskih komponenti od kojih neposredno zavisi njegovo ispravno postupanje prilikom vršenja poslova iz nadležnosti, odnosno pružanja usluga.

(3) Pod trećim licem iz stava 1. ovog člana smatra se i privredni subjekat koji je imovinskim i upravljačkim odnosima (lica sa učešćem, članice grupe društava kojoj taj privredni subjekt pripada i dr.) povezan sa operatorom IKT sistema od posebnog značaja.

(4) Poveravanje aktivnosti vrši se na osnovu ugovora zaključenog između operatora IKT sistema od posebnog značaja i lica kome se te aktivnosti poveravaju ili posebnim propisom.

Član 10.

Izuzetno od odredaba člana 9. ovog zakona, ukoliko su aktivnosti u vezi sa IKT sistemom poverene propisom, tim propisom se mogu drugačije urediti obaveze i odgovornosti operatora IKT sistema od posebnog značaja u vezi poverenih aktivnosti.

Obaveštavanje o incidentima

Član 11.

(1) Operatori IKT sistema od posebnog značaja obaveštavanje o incidentima u IKT sistemima koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti vrše preko veb stranice Nadležnog organa ili Nacionalnog CERT-a u jedinstveni sistem za prijem obaveštenja o incidentima kojeg održava Nadležni organ.

(2) Ukoliko organi iz stava 1. ovog člana budu obavešteni o incidentu na drugi način, podatke o incidentu unose u sistem iz stava 1. ovog člana.

(3) Izuzetno od stava 1. ovog člana, obaveštenje o incidentima se upućuje:

1) Narodnoj banci Srbije, u slučaju incidenata u IKT sistemima iz člana 6. stav 1. tačka 3) podtačka (4) alineje prva i druga ovog zakona;

2) regulatornom telu za elektronske komunikacije u slučaju incidenata u IKT sistemima iz člana 6. stav 1. tačka 3) podtačka 8) alineja prva ovog zakona.

(4) Narodna banka Srbije i regulatorno telo za elektronske komunikacije obaveštenja iz stava 3. ovog člana dostavljaju u jedinstveni sistem za prijem obaveštenja o incidentima na način iz stava 1. ovog člana.

(5) Nakon prijave incidenta, ukoliko je incident i dalje u toku, operatori IKT sistema od posebnog značaja dostavljaju obaveštenja o bitnim događajima u vezi sa incidentom i aktivnostima koje preduzimaju do prestanka incidenta organu kome su u skladu sa ovim zakonom prijavili incident.

(6) Operatori IKT sistema od posebnog značaja dostavljaju završni izveštaj o incidentu organu koga su u skladu sa ovim zakonom obaveštavali o incidentu u roku od 15 dana od dana prestanka incidenta, a koji obavezno sadrži vrstu i opis incidenta, vreme i trajanje incidenta, posledice koje je incident izazvao, preduzete aktivnosti radi otklanjanja posledica incidenta i, po potrebi, druge relevantne informacije.

(7) U slučaju incidenata u IKT sistemima za rad sa tajnim podacima operatori tih IKT sistema postupaju u skladu sa propisima kojima se uređuje oblast zaštite tajnih podataka.

(8) Odredbe st. 1. i 7. ovog člana ne odnose se na samostalne operatore IKT sistema.

(9) Vlada, na predlog Nadležnog organa, uređuje postupak obaveštavanja o incidentima, listu, vrste i značaj incidenata prema nivou opasnosti, postupanje i razmenu informacija o incidentima između organa iz člana 5. ovog zakona.

(10) Ako je incident od interesa za javnost, Nadležni organ, odnosno organ iz stava 3. ovog člana kome se upućuju obaveštenja o incidentima, može objaviti informaciju o incidentu, nakon savetovanja sa operatorom IKT sistema od posebnog značaja u kome se incident dogodio.

(11) Ako je incident vezan za izvršenje krivičnih dela koja se gone po službenoj dužnosti, organ kome je upućeno obaveštenje o incidentu, obaveštava nadležno javno tužilaštvo, odnosno ministarstvo nadležno za unutrašnje poslove.

(12) Ako je incident povezan sa značajnim narušavanjem informacione bezbednosti, koje ima ili može imati za posledicu ugrožavanje odbrane Republike Srbije, organ kome je upućeno obaveštenje o incidentu obaveštava Vojnobezbednosnu agenciju.

(13) Ako je incident povezan sa značajnim narušavanjem informacione bezbednosti, koje ima ili može imati za posledicu ugrožavanje nacionalne bezbednosti, organ kome je upućeno obaveštenje o incidentu obaveštava Bezbednosno-informativnu agenciju.

(14) U slučaju nastupanja okolnosti ugrožavanja, ometanja rada ili uništenja IKT sistema od posebnog značaja rukovođenje i koordinaciju sprovođenja mera i zadataka u navedenim okolnostima preduzima Republički štab za vanredne situacije, u skladu sa zakonom.

Incidenti u IKT sistemima od posebnog značaja koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti

Član 11a

(1) Operator IKT sistema od posebnog značaja dužan je da prijavi sledeće incidente koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti:

1) incidente koji dovode do prekida kontinuiteta vršenja poslova i pružanja usluga, odnosno znatnih teškoća u vršenju poslova i pružanju usluga;

2) incidente koji utiču na veliki broj korisnika usluga, ili traju duži vremenski period;

3) incidente koji dovode do prekida kontinuiteta, odnosno teškoća u vršenju poslova i pružanja usluga, koji utiču na obavljanje poslova i vršenje usluga drugih operatora IKT sistema od posebnog značaja ili utiču na javnu bezbednost;

4) incidente koji dovode do prekida kontinuiteta, odnosno teškoće u vršenju poslova i pružanju usluga i imaju uticaj na veći deo teritorije Republike Srbije;

5) incidente koji dovode do neovlašćenog pristupa zaštićenim podacima čije otkrivanje može ugroziti prava i interese onih na koje se podaci odnose;

6) incidente koji su nastali kao posledica incidenta u IKT sistemu iz člana 6. stav 1. tačka 3) podtačka (7) ovog zakona, kada IKT sistem od posebnog značaja u svom poslovanju koristi informacione usluge IKT sistema iz člana 6. stav 1. tačka 3) podtačka (7) ovog zakona.

(2) Operator IKT sistema od posebnog značaja dužan je da prijavi i incidente koji su doveli do značajnog povećanja rizika od nastupanja posledica iz stava 1. ovog člana.

Dostavljanje statističkih podataka o incidentima

Član 11b

(1) Operator IKT sistema od posebnog značaja dužan je da, pored obaveštavanja o incidentima iz člana 11. ovog zakona, dostavi Nacionalnom CERT-u statističke podatke o svim incidentima u IKT sistemu u prethodnoj godini najkasnije do 28. februara tekuće godine.

(2) Nacionalni CERT objedinjene statističke podatke iz stava 1. ovog člana dostavlja Nadležnom organu i objavljuje ih na veb stranici Nacionalnog CERT-a.

(3) Vrstu, formu i način dostavljanja statističkih podataka iz stava 1. ovog člana utvrđuje Nacionalni CERT.

Međunarodna saradnja i rana upozorenja o rizicima i incidentima

Član 12.

(1) Nadležni organ ostvaruje međunarodnu saradnju u oblasti bezbednosti IKT sistema, a naročito pruža upozorenja o rizicima i incidentima koji ispunjavaju najmanje jedan od sledećih uslova:

1) brzo rastu ili imaju tendenciju da postanu visokorizični;

2) prevazilaze ili mogu da prevaziđu nacionalne kapacitete;

3) mogu da imaju negativan uticaj na više od jedne države.

(2) Ukoliko je incident u vezi sa izvršenjem krivičnog dela, po dobijanju obaveštenja od Nadležnog organa, ministarstvo nadležno za unutrašnje poslove će u zvaničnoj proceduri proslediti prijavu u skladu sa potvrđenim međunarodnim ugovorima.

Samostalni operatori IKT sistema

Član 13.

(1) Samostalni operatori IKT sistema odrediće posebna lica, odnosno organizacione jedinice za internu kontrolu sopstvenih IKT sistema.

(2) Lica za internu kontrolu samostalnih operatora IKT sistema izveštaj o izvršenoj internoj kontroli podnose rukovodiocu samostalnog operatora IKT sistema.

Shodna primena odredaba o samostalnim operatorima IKT sistema

Član 13a

(1) Na Narodnu banku Srbije kao operatora IKT sistema shodno se primenjuju odredbe čl. 13 , 15 , 15a , 19 , 22 , 26 , 27. i 28. ovog zakona koje se odnose na samostalne operatore IKT sistema.

(2) Na Narodnu banku Srbije kao operatora IKT sistema shodno se primenjuju i odredbe čl. 11. i 11a ovog zakona koje se odnose na operatore IKT sistema od posebnog značaja.

III. PREVENCIJA I ZAŠTITA OD BEZBEDNOSNIH RIZIKA U IKT SISTEMIMA U REPUBLICI SRBIJI

Nacionalni CERT

Član 14.

(1) Nacionalni CERT obavlja poslove koordinacije prevencije i zaštite od bezbednosnih rizika u IKT sistemima u Republici Srbiji na nacionalnom nivou.

(2) Za poslove Nacionalnog CERT-a nadležna je Regulatorna agencija za elektronske komunikacije i poštanske usluge.

Delokrug Nacionalnog CERT-a

Član 15.

(1) Nacionalni CERT prikuplja i razmenjuje informacije o rizicima za bezbednost IKT sistema, kao i događajima koji ugrožavaju bezbednost IKT sistema i u vezi toga obaveštava, pruža podršku, upozorava i savetuje lica koja upravljaju IKT sistemima u Republici Srbiji, kao i javnost, a posebno:

1) prati stanje o incidentima na nacionalnom nivou;

2) pruža rana upozorenja, uzbune i najave i informiše relevantna lica o rizicima i incidentima;

3) reaguje po prijavljenim ili na drugi način otkrivenim incidentima u IKT sistemima od posebnog značaja, kao i po prijavama fizičkih i pravnih lica, tako što pruža savete i preporuke na osnovu raspoloživih informacija o incidentima i preduzima druge potrebne mere iz svoje nadležnosti na osnovu dobijenih saznanja;

4) kontinuirano izrađuje analize rizika i incidenata;

5) podiže svest kod građana, privrednih subjekata i organa vlasti o značaju informacione bezbednosti, o rizicima i merama zaštite, uključujući sprovođenje kampanja u cilju podizanja te svesti;

6) vodi evidenciju Posebnih CERT-ova;

7) izveštava Nadležni organ na kvartalnom nivou o preduzetim aktivnostima.

(2) Nacionalni CERT je ovlašćen da vrši obradu podataka o licu koje se obrati Nacionalnom CERT-u u skladu sa zakonom koji uređuje zaštitu podataka o ličnosti i drugim propisima.

(3) Obrada podataka o licu iz stava 1. tačka 3) ovog člana obuhvata ime, prezime i broj telefona i/ili adresu elektronske pošte i vrši se u svrhu evidentiranja podnetih prijava, informisanja podnosioca prijave o statusu predmeta i, u slučaju potrebe, upućivanja prijave nadležnim organima radi daljeg postupanja, u skladu sa zakonom.

(4) Nacionalni CERT obezbeđuje neprekidnu dostupnost svojih usluga putem različitih sredstava komunikacije.

(5) Prostorije i informacioni sistemi Nacionalnog CERT-a moraju da se nalaze na bezbednim lokacijama.

(6) U cilju obezbeđivanja kontinuiteta rada, Nacionalni CERT treba da:

1) bude opremljen sa odgovarajućim sistemima za obavljanje poslova iz svog delokruga;

2) ima dovoljno zaposlenih kako bi se osigurala dostupnost u svako doba;

3) obezbedi infrastrukturu čiji je kontinuitet osiguran, odnosno da obezbedi redundantne sisteme i rezervni radni prostor.

(7) Nacionalni CERT neposredno sarađuje sa Nadležnim organom, Posebnim CERT-ovima u Republici Srbiji, sličnim organizacijama u drugim zemljama, sa javnim i privrednim subjektima, CERT-ovima samostalnih operatora IKT sistema, kao i sa CERT-om organa vlasti.

(8) Nacionalni CERT promoviše usvajanje i korišćenje propisanih i standardizovanih procedura za:

1) upravljanje i saniranje rizika i incidenata;

2) klasifikaciju informacija o rizicima i incidentima, odnosno klasifikaciju prema nivou incidenata i rizika.

Saradnja CERT-ova u Republici Srbiji

Član 15a

(1) Nacionalni CERT, CERT organa vlasti i CERT-ovi samostalnih operatora IKT sistema održavaju kontinuiranu saradnju.

(2) CERT-ovi iz stava 1. ovog člana održavaju međusobne sastanke u organizaciji Nacionalnog CERT-a najmanje tri puta godišnje, kao i po potrebi u slučaju incidenata koji značajno ugrožavaju informacionu bezbednost u Republici Srbiji.

(3) Sastancima CERT-ova iz stava 1. ovog člana prisustvuju i predstavnici Nadležnog organa.

(4) Sastancima CERT-ova iz stava 1. ovog člana mogu, po pozivu, da prisustvuju i predstavnici posebnih CERT-ova, kao i druga lica.

Nadzor nad radom Nacionalnog CERT-a

Član 16.

Nadzor nad radom Nacionalnog CERT-a u vršenju poslova poverenih ovim zakonom vrši Nadležni organ, koji periodično, a najmanje jednom godišnje, proverava da li Nacionalni CERT raspolaže odgovarajućim resursima, vrši poslove u skladu sa članom 15. ovog zakona i kontroliše učinak uspostavljenih procesa za upravljanje sigurnosnim incidentima.

Posebni centri za prevenciju bezbednosnih rizika u IKT sistemima

Član 17.

(1) Poseban centar za prevenciju bezbednosnih rizika u IKT sistemima (u daljem tekstu: Poseban CERT) obavlja poslove prevencije i zaštite od bezbednosnih rizika u IKT sistemima u okviru određenog pravnog lica, grupe pravnih lica, oblasti poslovanja i slično.

(2) Poseban CERT je pravno lice ili organizaciona jedinica u okviru pravnog lica **sa sedištem na teritoriji Republike Srbije**, koje je upisano u evidenciju posebnih CERT-ova koju vodi Nacionalni CERT.

(3) Upis u evidenciju posebnih CERT-ova vrši se na osnovu prijave pravnog lica u okviru koga se nalazi poseban CERT.

(4) Evidencija posebnih CERT-ova od podataka o ličnosti sadrži podatke o odgovornim licima, i to: ime, prezime, funkciju i kontakt podatke kao što su adresa, broj telefona i adresa elektronske pošte **, a u svrhu angažovanja posebnih CERT-ova u slučaju bezbednosnih rizika i incidenata u IKT sistemima.**

(5) **Nacionalni CERT propisuje sadržaj, način upisa i vođenja evidencije iz stava 3. ovog člana.**

Centar za bezbednost IKT sistema u organima vlasti (CERT organa vlasti)

Član 18.

(1) CERT organa vlasti obavlja poslove koji se odnose na zaštitu od incidenata u IKT sistemima organa vlasti, izuzev IKT sistema samostalnih operatora.

(2) Poslove CERT-a organa vlasti obavlja organ nadležan za projektovanje, razvoj, izgradnju, održavanje i unapređenje računarske mreže republičkih organa.

(3) Poslovi CERT-a organa vlasti obuhvataju:

1) zaštitu Jedinstvene informaciono-komunikacione mreže elektronske uprave;

2) koordinaciju i saradnju sa operatorima IKT sistema koje povezuje jedinstvena mreža iz tačke 1) ovog stava u prevenciji incidenata, otkrivanju incidenata, prikupljanju informacija o incidentima i otklanjanju posledica incidenata;

3) izdavanje stručnih preporuka za zaštitu IKT sistema organa vlasti, osim IKT sistema za rad sa tajnim podacima.

CERT samostalnog operatora IKT sistema

Član 19.

(1) Samostalni operatori IKT sistema su u obavezi da formiraju sopstvene centre za bezbednost IKT sistema radi upravljanja incidentima u svojim sistemima.

(2) Centri iz stava 1. ovog člana međusobno razmenjuju informacije o incidentima, kao i sa nacionalnim CERT-om i sa CERT-om **organa vlasti**, a po potrebi i sa drugim organizacijama.

(3) Delokrug centra za bezbednost IKT sistema, kao organizacione jedinice samostalnog operatora IKT sistema, pored poslova iz st. 1. i 2. ovog člana, može obuhvatati:

1) izradu internih akata u oblasti informacione bezbednosti;

2) izbor, testiranje i implementaciju tehničkih, fizičkih i organizacionih mera zaštite, opreme i programa;

3) izbor, testiranje i implementaciju mera zaštite od KEMZ;

4) nadzor implementacije i primene bezbednosnih procedura;

5) upravljanje i korišćenje kriptografskih proizvoda;

6) analizu bezbednosti IKT sistema u cilju procene rizika;

7) obuku zaposlenih u oblasti informacione bezbednosti.

Zaštita dece pri korišćenju informaciono-komunikacionih tehnologija

Član 19a

(1) Nadležni organ preduzima preventivne mere za bezbednost i zaštitu dece na internetu, kao aktivnosti od javnog interesa, putem edukacije i informisanja dece, roditelja i nastavnika o prednostima, rizicima i načinima bezbednog korišćenja interneta, kao i putem jedinstvenog mesta za pružanje saveta i prijem prijava u vezi bezbednosti dece na internetu, i upućuje prijave nadležnim organima radi daljeg postupanja.

(2) Operator elektronskih komunikacija koji pruža javno dostupne telefonske usluge dužan je da omogući svim pretplatnicima uslugu besplatnog poziva prema jedinstvenom mestu za pružanje saveta i prijem prijava u vezi bezbednosti dece na internetu.

(3) U slučaju da navodi iz prijave upućuju na postojanje krivičnog dela, na povredu prava, zdravstvenog statusa, dobrobiti i/ili opšteg integriteta deteta, na rizik stvaranja zavisnosti od korišćenja interneta, prijava se prosleđuje nadležnom organu vlasti radi postupanja u skladu sa utvrđenim nadležnostima.

(4) Nadležni organ je ovlašćen da vrši obradu podataka o licu koje se obrati Nadležnom organu u skladu sa zakonom koji uređuje zaštitu podataka o ličnosti i drugim propisima.

(5) Obrada podataka o licu iz stava 4. ovog člana obuhvata ime, prezime i broj telefona i/ili adresu elektronske pošte i vrši se u svrhu evidentiranja podnetih prijava, informisanja podnosioca prijave o statusu predmeta i, u slučaju potrebe, upućivanja prijave nadležnim organima radi daljeg postupanja, u skladu sa zakonom.

(6) Podaci o ličnosti iz stava 5. ovog člana čuvaju se u rokovima predviđenim propisima koji uređuju kancelarijsko poslovanje.

(7) U cilju obezbeđivanja kontinuiteta rada jedinstvenog mesta za pružanje saveta i prijem prijava u vezi bezbednosti dece na internetu, Nadležni organ treba da:

1) bude opremljen sa odgovarajućim sistemima za prijem prijava;

2) ima dovoljno zaposlenih kako bi se osigurala dostupnost u radu;

3) obezbedi infrastrukturu čiji je kontinuitet osiguran.

(8) Vlada bliže uređuje način sprovođenja mera za bezbednost i zaštitu dece na internetu iz st. 1. i 3. ovog člana.

IV. KRIPTOBEZBEDNOST I ZAŠTITA OD KOMPROMITUJUĆEG ELEKTROMAGNETNOG ZRAČENJA

Nadležnost

Član 20.

Ministarstvo nadležno za poslove odbrane je nadležno za poslove informacione bezbednosti koji se odnose na odobravanje kriptografskih proizvoda, distribuciju kriptomaterijala i zaštitu od kompromitujućeg elektromagnetnog zračenja i poslove i zadatke u skladu sa zakonom i propisima donetim na osnovu zakona.

Poslovi i zadaci

Član 21.

(1) U skladu sa ovim zakonom, ministarstvo nadležno za poslove odbrane:

1) organizuje i realizuje naučnoistraživački rad u oblasti kriptografske bezbednosti i zaštite od KEMZ;

2) razvija, implementira, verifikuje i klasifikuje kriptografske algoritme;

3) istražuje, razvija, verifikuje i klasifikuje sopstvene kriptografske proizvode i rešenja zaštite od KEMZ;

4) verifikuje i klasifikuje domaće i strane kriptografske proizvode i rešenja zaštite od KEMZ;

5) definiše procedure i kriterijume za evaluaciju kriptografskih bezbednosnih rešenja;

6) vrši funkciju nacionalnog organa za odobrenja kriptografskih proizvoda i obezbeđuje da ti proizvodi budu odobreni u skladu sa odgovarajućim propisima;

7) vrši funkciju nacionalnog organa za zaštitu od KEMZ;

8) vrši proveru IKT sistema sa aspekta kriptobezbednosti i zaštite od KEMZ;

9) vrši funkciju nacionalnog organa za distribuciju kriptomaterijala i definiše upravljanje, rukovanje, čuvanje, distribuciju i evidenciju kriptomaterijala u skladu sa propisima;

10) planira i koordinira izradu kriptoparametara (parametara kriptografskog algoritma), distribuciju kriptomaterijala i zaštite od kompromitujućeg elektromagnetnog zračenja u saradnji sa samostalnim operatorima IKT sistema;

11) formira i vodi centralni registar verifikovanog i distribuiranog kriptomaterijala;

12) formira i vodi registar izdatih odobrenja za kriptografske proizvode;

13) izrađuje elektronske sertifikate za kriptografske sisteme zasnovane na infrastrukturi javnih ključeva (Public Key Infrastructure - PKI);

14) predlaže donošenje propisa iz oblasti kriptobezbednosti i zaštite od KEMZ na osnovu ovog zakona;

15) vrši poslove stručnog nadzora u vezi kriptobezbednosti i zaštite od KEMZ;

16) pruža stručnu pomoć nosiocu inspekcijskog nadzora informacione bezbednosti u oblasti kriptobezbednosti i zaštite od KEMZ;

17) pruža usluge uz naknadu pravnim i fizičkim licima, izvan sistema javne vlasti, u oblasti kriptobezbednosti i zaštite od KEMZ prema propisu Vlade na predlog ministra odbrane;

18) sarađuje sa domaćim i međunarodnim organima i organizacijama u okviru nadležnosti uređenih ovim zakonom.

(2) Sredstva ostvarena od naknade za pružanje usluga iz stava 1. tačka 17) ovog člana su prihod budžeta Republike Srbije.

Kompromitujuće elektromagnetno zračenje

Član 22.

(1) Mere zaštite od KEMZ za rukovanje sa tajnim podacima u IKT sistemima primenjuju se u skladu sa propisima kojima se uređuje zaštita tajnih podataka.

(2) Mere zaštite od KEMZ mogu primenjivati na sopstvenu inicijativu i operatori IKT sistema kojima to nije zakonska obaveza.

(3) Za sve tehničke komponente sistema (uređaje, komunikacione kanale i prostore) kod kojih postoji rizik od KEMZ, a što bi moglo dovesti do narušavanja informacione bezbednosti iz stava 1. ovog člana, vrši se provera zaštićenosti od KEMZ i procena rizika od neovlašćenog pristupa tajnim podacima putem KEMZ.

(4) Proveru zaštićenosti od KEMZ vrši ministarstvo nadležno za poslove odbrane.

(5) Samostalni operatori IKT sistema mogu vršiti proveru KEMZ za sopstvene potrebe.

(6) Bliže uslove za proveru KEMZ i način procene rizika od oticanja podataka putem KEMZ uređuje Vlada, na predlog ministarstva nadležnog za poslove odbrane.

Mere kriptozaštite

Član 23.

(1) Mere kriptozaštite za rukovanje sa tajnim podacima u IKT sistemima primenjuju se u skladu sa propisima kojima se uređuje zaštita tajnih podataka.

(2) Mere kriptozaštite se mogu primeniti i prilikom prenosa i čuvanja podataka koji nisu označeni kao tajni u skladu sa zakonom koji uređuje tajnost podataka, kada je na osnovu zakona ili drugog pravnog akta potrebno primeniti tehničke mere ograničenja pristupa podacima i radi zaštite integriteta, autentičnosti i neporecivosti podataka.

(3) Vlada, na predlog ministarstva nadležnog za poslove odbrane uređuje tehničke uslove za kriptografske algoritme, parametre, protokole i informaciona dobra u oblasti kriptozaštite koji se u Republici Srbiji koriste u kriptografskim proizvodima radi zaštite tajnosti, integriteta, autentičnosti, odnosno neporecivosti podataka.

Odobrenje za kriptografski proizvod

Član 24.

(1) Kriptografski proizvodi koji se koriste za zaštitu prenosa i čuvanja podataka koji su određeni kao tajni, u skladu sa zakonom, moraju biti verifikovani i odobreni za korišćenje.

(2) Vlada, na predlog ministarstva nadležnog za poslove odbrane, bliže uređuje uslove koje moraju da ispunjavaju kriptografski proizvodi iz stava 1. ovog člana.

Izdavanje odobrenja za kriptografski proizvod

Član 25.

(1) Odobrenje za kriptografski proizvod izdaje ministarstvo nadležno za poslove odbrane, na zahtev operatora IKT sistema, proizvođača kriptografskog proizvoda ili drugog zainteresovanog lica.

(2) Odobrenje za kriptografski proizvod se može odnositi na pojedinačni primerak kriptografskog proizvoda ili na određeni model kriptografskog proizvoda koji se serijski proizvodi.

(3) Odobrenje za kriptografski proizvod može imati rok važenja.

(4) Ministarstvo nadležno za poslove odbrane rešava po zahtevu za izdavanje odobrenja za kriptografski proizvod u roku od 45 dana od dana podnošenja urednog zahteva, koji se može produžiti u slučaju posebne složenosti provere najviše za još 60 dana.

(5) Protiv rešenja iz stava 4. ovog člana žalba nije dopuštena, ali može da se pokrene upravni spor.

(6) Ministarstvo nadležno za poslove odbrane vodi registar izdatih odobrenja za kriptografski proizvod.

(7) Registar iz stava 6. ovog člana od podataka o ličnosti sadrži podatke o odgovornim licima, i to: ime, prezime, funkcija i kontakt podatke kao što su adresa, broj telefona i adresa elektronske pošte.

(8) Ministarstvo nadležno za poslove odbrane objavljuje javnu listu odobrenih modela kriptografskih proizvoda za sve modele kriptografskih proizvoda za koje je u zahtevu za izdavanje odobrenja naglašeno da model kriptografskog proizvoda treba da bude na javnoj listi i ako je zahtev podneo proizvođač ili lice ovlašćeno od strane proizvođača predmetnog kriptografskog proizvoda.

(9) Ministarstvo nadležno za poslove odbrane prethodno izdato odobrenje za kriptografski proizvod može povući ili promeniti uslove iz st. 2. i 3. ovog člana iz razloga novih saznanja vezanih za tehnička rešenja primenjena u proizvodu, a koja utiču na ocenu stepena zaštite koji pruža proizvod.

(10) Vlada, na predlog ministarstva nadležnog za poslove odbrane, bliže uređuje sadržaj zahteva za izdavanje odobrenja za kriptografski proizvod, uslove za izdavanje odobrenja za kriptografski proizvod, način izdavanja odobrenja i sadržaj registra izdatih odobrenja za kriptografski proizvod.

Opšte odobrenje za korišćenje kriptografskih proizvoda

Član 26.

(1) Samostalni operatori IKT sistema imaju opšte odobrenje za korišćenje kriptografskih proizvoda.

(2) Operator IKT sistema iz stava 1. ovog člana samostalno ocenjuje stepen zaštite koji pruža svaki pojedinačni kriptografski proizvod koji koristi, a u skladu sa propisanim uslovima.

Registri u kriptozaštiti

Član 27.

(1) Samostalni operatori IKT sistema koji imaju opšte odobrenje za korišćenje kriptografskih proizvoda ustrojavaju i vode registre kriptografskih proizvoda, kriptomaterijala, pravila i propisa i lica koja obavljaju poslove kriptozaštite.

(2) Registar lica koja obavljaju poslove kriptozaštite od podataka o ličnosti sadrži sledeće podatke o licima koja obavljaju poslove kriptozaštite: prezime, ime oca i ime, datum i mesto rođenja, matični broj, telefon, adresu elektronske pošte, školsku spremu, podatke o završenom stručnom osposobljavanju za poslove kriptozaštite, naziv radnog mesta, datum početka i završetka rada na poslovima kriptozaštite.

(3) Registar kriptomaterijala za rukovanje sa stranim tajnim podacima vodi Kancelarija Saveta za nacionalnu bezbednost i zaštitu tajnih podataka, u skladu sa ratifikovanim međunarodnim sporazumima.

(4) Vlada, na predlog ministarstva nadležnog za poslove odbrane, bliže uređuje vođenje registara iz stava 1. ovog člana.

V. INSPEKCIJA ZA INFORMACIONU BEZBEDNOST

Poslovi inspekcije za informacionu bezbednost

Član 28.

(1) Inspekcija za informacionu bezbednost vrši inspekcijski nadzor nad primenom ovog zakona i radom operatora IKT sistema od posebnog značaja, osim samostalnih operatora IKT sistema i IKT sistema za rad sa tajnim podacima, a u skladu sa zakonom kojim se uređuje inspekcijski nadzor.

(2) Poslove inspekcije za informacionu bezbednost obavlja ministarstvo nadležno za poslove informacione bezbednosti preko inspektora za informacionu bezbednost.

(3) U okviru inspekcijskog nadzora rada operatora IKT sistema, inspektor za informacionu bezbednost utvrđuje da li su ispunjeni uslovi propisani ovim zakonom i propisima donetim na osnovu ovog zakona.

Ovlašćenja inspektora za informacionu bezbednost

Član 29.

Inspektor za informacionu bezbednost je ovlašćen da u postupku sprovođenja nadzora, pored nalaganja mera za koje je ovlašćen inspektor u postupku vršenja inspekcijskog nadzora utvrđenih zakonom:

1) naloži otklanjanje utvrđenih nepravilnosti i za to ostavi rok;

2) zabrani korišćenje postupaka i tehničkih sredstava kojima se ugrožava ili narušava informaciona bezbednost i za to ostavi rok.

VI. KAZNENE ODREDBE

Član 30.

(1) Novčanom kaznom u iznosu od 50.000,00 do 2.000.000,00 dinara kazniće se za prekršaj operator IKT sistema od posebnog značaja ako:

1) ne izvrši upis u evidenciju u roku iz člana 6b stav 4. ovog zakona;

2) ne donese Akt o bezbednosti IKT sistema iz člana 8. stav 1. ovog zakona;

3) ne primeni mere zaštite određene Aktom o bezbednosti IKT sistema iz člana 8. stav 2. ovog zakona;

4) ne izvrši proveru usklađenosti primenjenih mera iz člana 8. stav 4. ovog zakona;

5) ne dostavi statističke podatke iz člana 11b stav 1. ovog zakona;

6) ne postupi po nalogu inspektora za informacionu bezbednost u ostavljenom roku iz člana 29. stav 1. tačka 1. ovog zakona.

(2) Za prekršaj iz stava 1. ovog člana kazniće se i odgovorno lice u operatoru IKT sistema od posebnog značaja novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara.

Član 31.

(1) Novčanom kaznom u iznosu od 50.000,00 do 500.000,00 dinara kazniće se za prekršaj operator IKT sistema od posebnog značaja ako:

1) o incidentima u IKT sistemu ne obavesti organe iz člana 11. st. 1, 3. i 7. ovog zakona;

2) ne dostavlja obaveštenja o bitnim događajima u vezi sa incidentom i aktivnostima iz člana 11. stav 5. ovog zakona;

3) ne dostavi završni izveštaj u roku iz člana 11. stav 6. ovog zakona.

(2) Za prekršaje iz stava 1. ovog člana kazniće se i odgovorno lice u operatoru IKT sistema od posebnog značaja novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara.

(3) Izuzetno od st. 1. i 2. ovog člana, ako finansijska institucija ne obavesti Narodnu banku Srbije o incidentima u IKT sistemu od posebnog značaja, Narodna banka Srbije izriče toj finansijskoj instituciji mere i kazne u skladu sa zakonom kojim se uređuje njeno poslovanje.

VII. PRELAZNE I ZAVRŠNE ODREDBE

Rokovi za donošenje podzakonskih akata

Član 32.

Podzakonska akta predviđena ovim zakonom doneće se u roku od šest meseci od dana stupanja na snagu ovog zakona.

Član 33.

Operatori IKT sistema od posebnog značaja su dužni da donesu akt o bezbednosti IKT sistema od posebnog značaja u roku od 90 dana od dana stupanja na snagu podzakonskog akta iz člana 10. ovog zakona.

Stupanje na snagu

Član 34.

Ovaj zakon stupa na snagu osmog dana od dana objavljivanja u "Službenom glasniku Republike Srbije".

ODREDBE KOJE NISU UŠLE U PREČIŠĆEN TEKST

Zakon o izmenama i dopunama Zakona o informacionoj bezbednosti
("Službeni glasnik RS", broj 77/19)

Član 22.

(1) Podzakonski akti iz čl. 4 , 7. i 19. ovog zakona doneće se u roku od šest meseci od dana stupanja na snagu ovog zakona.

(2) Podzakonski akti iz čl. 5. i 8. ovog zakona doneće se u roku od tri meseca od dana stupanja na snagu ovog zakona.