ZAKON
O INFORMACIONOJ BEZBEDNOSTI

(Sl. glasnik RS br. 6/16 , 94/17)

Prečišćen tekst zaključno sa izmenama iz Sl. gl. RS br. 94/17 koje su u primeni od 27/10/2017
(izmene u čl.: 5 , 18).

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 pohranjuju, 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;

2) operator IKT sistema je pravno lice, organ javne vlasti ili organizaciona jedinica organa javne 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 unutrašnja ili spoljna okolnost ili događaj kojim se ugrožava ili narušava informaciona bezbednost;

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 javne vlasti je državni organ, organ autonomne pokrajine, organ jedinice lokalne samouprave, organizacija kojoj je povereno vršenje javnih ovlašćenja, pravno lice koje osniva Republika Srbija, autonomna pokrajina ili jedinica lokalne samouprave, kao i pravno lice koje se pretežno, odnosno u celini finansira iz budžeta;

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, unutrašnje opšte akte, procedure i slično.

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.

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, **CERT-a republičkih organa** i Nacionalnog CERT-a.

(2) U funkciji unapređenja pojedinih oblasti informacione bezbednosti formiraju se stručne radne grupe Tela za koordinaciju u koje se uključuju i predstavnici drugih organa javne 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 javne vlasti;

2) za obradu podataka koji se, u skladu sa zakonom koji uređuje zaštitu podataka o ličnosti, smatraju naročito osetljivim podacima o ličnosti;

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

(1) proizvodnja, prenos i distribucija električne energije;

(2) proizvodnja i prerada uglja;

(3) istraživanje, proizvodnja, prerada, transport i distribucija nafte i prirodnog i tečnog gasa;

(4) promet nafte i naftnih derivata; železničkog, poštanskog i vazdušnog saobraćaja;

(5) elektronska komunikacija;

(6) izdavanje službenog glasila Republike Srbije;

(7) upravljanje nuklearnim objektima;

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

(9) proizvodnja, promet i prevoz naoružanja i vojne opreme;

(10) upravljanje otpadom;

(11) komunalne delatnosti;

(12) poslovi finansijskih institucija;

(13) zdravstvena zaštita;

(14) usluge informacionog društva namenjene drugim pružaocima usluga informacionog društva u cilju omogućavanja pružanja njihovih usluga.

(2) Vlada, na predlog ministarstva nadležnog za poslove informacione bezbednosti, utvrđuje listu poslova i delatnosti iz stava 1. tačka 3) 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 minimizacija 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 odnosno 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) pitanja informacione bezbednosti 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 Nadležnog organa o incidentima

Član 11.

(1) Operatori IKT sistema od posebnog značaja obavezni su da obaveste Nadležni organ o incidentima u IKT sistemima koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti.

(2) Izuzetno od stava 1. ovog člana, finansijske institucije obaveštenja upućuju Narodnoj banci Srbije, telekomunikacioni operatori regulatornom telu za elektronske komunikacije, a operatori IKT sistema za rad sa tajnim podacima postupaju u skladu sa propisima kojima se uređuje oblast zaštite tajnih podataka.

(3) Odredbe st. 1 i 2. ovog člana ne odnose se na samostalne operatore IKT sistema.

(4) Postupak dostavljanja podataka, listu, vrste i značaj incidenata i postupak obaveštavanja iz stava 1. ovog člana uređuje Vlada.

(5) Ako je incident od interesa za javnost, Nadležni organ, odnosno organ iz stava 2. ovog člana kome se upućuju obaveštenja o incidentima, može naložiti njegovo objavljivanje.

(6) Ako je incident vezan za izvršenje krivičnih dela koja se gone po službenoj dužnosti, Nadležni organ, odnosno organ iz stava 2. ovog člana kome se upućuju obaveštenja o incidentima, obaveštava nadležno javno tužilaštvo, odnosno ministarstvo nadležno za unutrašnje poslove.

(7) Ako je incident povezan sa narušavanjem prava na zaštitu podataka o ličnosti, Nadležni organ, odnosno organ iz stava 2. ovog člana kome se upućuju obaveštenja o incidentima i samostalni operator IKT sistema, o tome obaveštavaju i Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti.

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 visoki rizici;

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.

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.

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

Nacionalni centar za prevenciju bezbednosnih rizika u IKT sistemima (Nacionalni CERT)

Član 14.

(1) Nacionalni centar za prevenciju bezbednosnih rizika u IKT sistemima (u daljem tekstu: 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.

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, 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, tako što pruža savete na osnovu raspoloživih informacija licima koja su pogođena incidentom 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 javne vlasti o značaju informacione bezbednosti, o rizicima i merama zaštite, uključujući sprovođenje kampanja u cilju podizanja te svesti,

6) vodi evidenciju Posebnih CERT-ova.

(2) Evidencija iz stava 1. tačka 6) ovog člana 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.

(3) 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 republičkih organa.

(4) Nacionalni CERT promoviše usvajanje i korišćenje propisanih i standardizovanih pravila za:

1) upravljanje i saniranje rizika i incidenata;

2) klasifikaciju informacija o rizicima i incidentima;

3) klasifikaciju ozbiljnosti incidenata i rizika;

4) definiciju formata i modela podataka za razmenu informacija o rizicima i incidentima i definiciju pravila po kojima će se imenovati značajni sistemi.

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, 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.

(5) Bliže uslove za upis u evidenciju iz stava 3. ovog člana donosi Nadležni organ.

Centar za bezbednost IKT sistema u republičkim organima (CERT republičkih organa)

Član 18.

(1) Centar za bezbednost IKT sistema u republičkim organima (u daljem tekstu: CERT republičkih organa) obavlja poslove koji se odnose na zaštitu od incidenata u IKT sistemima republičkih organa, izuzev IKT sistema samostalnih operatora.

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

(3) Poslovi CERT-a republičkih organa obuhvataju:

1) zaštitu IKT sistema Računarske mreže republičkih organa (u daljem tekstu: RMRO);

2) koordinaciju i saradnju sa operatorima IKT sistema koje povezuje RMRO u prevenciji incidenata, otkrivanju incidenata, prikupljanju informacija o incidentima i otklanjanju posledica incidenata;

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

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 republičkih organa, 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.

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 pravno lice ako:

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

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

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

4) 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 pravnom licu 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 pravno lice ako o incidentima u IKT sistemu ne obavesti Nadležni organ, odnosno organ nadležan za obezbeđenje primene standarda u oblasti zaštite tajnih podataka, Narodnu banku Srbije ili regulatorno telo za elektronske komunikacije (član 11. st. 1. i 2.).

(2) Za prekršaj iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara.

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".