P R E D L O G

ZAKON
O INFORMACIONOJ BEZBEDNOSTI

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 pokrajna 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.

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, Uprave za zajedničke poslove republičkih organa i Nacionalnog CERT-a.

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.

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.

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.

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.

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

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.

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 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.

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.

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

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.

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

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.

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.

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.

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.

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.

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.

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.

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.

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

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

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.

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.

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.

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.

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.

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

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.

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.

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

Član 15.

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.

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.

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.

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.

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.

Poseban CERT je pravno lice ili organizaciona jedinica u okviru pravnog lica, koje je upisano u evidenciju posebnih CERT-ova koju vodi Nacionalni CERT.

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

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.

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.

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.

Poslove CERT-a republičkih organa obavlja Uprava za zajedničke poslove republičkih organa.

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.

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

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.

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 implementacija 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.

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 izadatih 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.

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

Kompromitujuće elektromagnetno zračenje

Član 22.

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

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

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.

Proveru zaštićenosti od KEMZ vrši ministarstvo nadležno za poslove odbrane.

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

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.

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

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.

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.

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.

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.

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

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

Odobrenje za kriptografski proizvod može imati rok važenja.

Ministarstvo nadležno za poslove odbrane rešava po zahtevu za izdavanje odobrenja za kriptografski proizvod u roku od 60 dana od dana podnošenja urednog zahteva, koji se može produžiti u slučaju posebne složenosti provere najviše za još 90 dana.

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

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

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.

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.

Ministarstvo nadležno za poslove odbrane prethodno izdato odobrenje za kriptografski proizvod može povući ili promeniti uslove iz st. 3. i 4. ovog člana iz razloga novih saznanja vezanih za tehnička rešenja primenjena u proizvodu, a koja utiču na ocenu stepena zaštite koji pruža proizvod.

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.

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

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.

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.

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.

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

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.

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.

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

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 na koje je ovlašćen inspektor u postupku vršenja inspekcijskog nadzora utvrđenih zakonom:

1) naloži otklanjanjanje 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.

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.

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.

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.).

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 12 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”.

O B R A Z L O Ž E Nj E

I. USTAVNI OSNOV ZA DONOŠENjE ZAKONA

Ustavni osnov za donošenje ovog zakona sadržan je u članu 97. tač. 4, 16. i 17. Ustava Republike Srbije, kojima je, između ostalog, propisano da Republika Srbija uređuje i obezbeđuje bezbednost Republike Srbije, organizaciju, nadležnost i rad republičkih organa, i da obezbeđuje druge odnose od interesa za Republiku Srbiju.

II. RAZLOZI ZA DONOŠENjE ZAKONA

Strategijom razvoja informacionog društva u Republici Srbiji do 2020. godine („Službeni glasnik RS”, broj 51/10), (u daljem tekstu: Strategija razvoja ID) je kao jedna od šest oblasti prioriteta određena informaciona bezbednost. U Strategiji razvoja ID je istaknuto da je odgovarajući stepen informacione bezbednosti u svim oblicima primene informaciono-komunikacionih tehnologija jedan od preduslova stvaranja održivog informacionog društva. Kao prvi prioritet u oblasti informacione bezbednosti je određeno unapređenje pravnog i institucionalnog okvira za informacionu bezbednost.

Postojeći zakonski okvir u ovoj oblasti je Zakon o tajnosti podataka („Službeni glasnik RS”, broj 104/09), Zakon o zaštiti podataka o ličnosti („Službeni glasnik RS”, br. 97/08 i 104/09 - drugi zakon, 68/12 – US i 107/12), Zakon o elektronskom potpisu („Službeni glasnik RS”, broj 135/04), Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala („Službeni glasnik RS”, br. 61/05 i 104/09), Zakon o Vojnobezbednosnoj agenciji i Vojnoobaveštajnoj agenciji („Službeni glasnik RS”, br. 88/09 55/12 – US i 17/13) i Krivični zakonik („Službeni glasnik RS”, br. 85/05, 88/05, 107/05, 72/09, 111/09, 121/12, 104/13 i 108/14). U širem kontekstu, pravni okvir čine i Zakon o elektronskim komunikacijama („Službeni glasnik RS”, br. 44/10 60/13 – US i 62/14) i Zakon o odbrani („Službeni glasnik RS”, br. 116/07, 88/09,104/09 116/07, 88/09 - dr. zakon, 104/09 – dr. zakon i 10/15). Usvajanjem Zakona o informacionoj bezbednosti i odgovarajućih podzakonskih akata uspostavio bi se celovit pravni okvir u ovoj oblasti.

Donošenje Zakona o informacionoj bezbednosti predstavlja jedan od koraka ka harmonizaciji pravnog okvira Republike Srbije sa Evropskom unijom u oblasti informacionog društva. U okviru pregovaračkog postupka za pridruživanje Republike Srbije Evropskoj uniji, materija informacione bezbednosti razmatra se u okviru Pregovaračke grupe 10 – Informaciono društvo i mediji. Nacionalnim programom za usvajanje pravnih tekovina Evropske unije (NPAA) od 2014-2018. godine predviđeno je da će Vlada utvrditi Predlog zakona o informacionoj bezbednosti.

Evropska unija donela je 2013. godine Strategiju bezbednosti IKT sistema Evropske unije, koja utvrđuje osnovne smernice u ovoj oblasti kojima EU i države članice treba da se rukovode. Radi postizanja otpornosti na incidente u IKT sistemima, neophodno je učešće brojnih društvenih činilaca, kako u javnom, tako i u privatnom sektoru, s obzirom da pojedinačni napori često nisu dovoljni da bi se uspostavio adekvatan nivo bezbednosti i zaštite IKT sistema. Putem očuvanja bezbednosti IKT sistema štite se osnovna ljudska prava, lični podaci i privatnost koji su garantovani međunarodnim i nacionalnim pravnim aktima. Strategijom je određeno da je u oblasti informacione bezbednosti potrebno usvojiti odgovarajuće pravne akte (zakone i podzakonska akta), odrediti organ koji će u okviru države članice biti nadležan za informacionu bezbednost i uspostaviti nacionalne timove za prevenciju i reagovanje na incidente u IKT sistema – Nacionalni CERT (eng. Computer Emergency Response Team). U cilju efikasnije prevencije i zaštite, od velike je važnosti da nadležna tela država članica razmenjuju podatke o opasnostima i incidentima u IKT sistemima, kao i da se održavaju posebne vežbe – simulacije

sajber incidenata. Takođe, istaknuto je da je, s obzirom da javne institucije, privatni sektor i građani uglavnom nisu dovoljno svesni rizika i opasnosti u sajber prostoru, potrebno širiti informacije o pretnjama i time pravovremeno preduzeti mere zaštite. Načela istaknuta u ovoj strategiji odražavaju se u Predlogu direktive o mrežnoj i informacionoj bezbednosti Evropske unije (NIS Directive), koja predviđa regulisanje navedenih aspekata u državama članicama, i čije se usvajanje očekuje u narednom periodu. Osim u nekim slučajevima, usaglašavanje sa Evropskom unijom ostavlja dovoljno širok prostor da Republika Srbija pronađe ono rešenje koje odgovara njenim prilikama, potrebama i finansijskim mogućnostima.

U smislu Predloga zakona o informacionoj bezbednosti (u daljem tekstu: Predlog zakona) informaciona bezbednost predstavlja skup mera koje omogućavaju da IKT sistem zaštiti tajnost, integritet, raspoloživost, autentičnost i neporecivost podataka kojima se rukuje putem tog sistema, da bi taj sistem funkcionisao kako je predviđeno, kada je predviđeno i pod kontrolom ovlašćenih lica. Pri tome se pod informaciono-komunikacionim sistemom (u daljem tekstu: IKT sistem) podrazumeva elektronska komunikaciona mreža u smislu zakona koji uređuje elektronske komunikacije; uređaji ili grupa međusobno povezanih uređaja, takav da se u okviru tog uređaja, odnosno u okviru barem jednog iz te grupe uređaja, vrši automatska obrada podataka korišćenjem računarskog programa, potom podaci koji se pohranjuju, obrađuju, pretražuju ili prenose pomoću sredstava, a u svrhu njihovog rada, upotrebe, zaštite ili održavanja, kao i organizaciona struktura putem koje se upravlja IKT sistemom.

S obzirom na bezbedonosne rizike u IKT sistemima, neophodno je da se Zakonom o informacionoj bezbednosti urede mere zaštite od bezbednosnih rizika u IKT sistemima, propišu odgovornosti i obaveze pravnih lica prilikom upravljanja i korišćenja IKT sistema i odrede nadležni organi za sprovođenje mera zaštite, odnosno nadležni organ državne uprave za bezbednost IKT sistema u Republici Srbiji, nadležni organ za odobravanje kriptografskih proizvoda, distribuciju kriptomaterijala i zaštitu od kompromitujućeg elektromagnetnog zračenja (u daljem tekstu: KEMZ), obrazuje Nacionalni centar za prevenciju bezbednosnih rizika u IKT sistemima (Nacionalni CERT), obezbedi koordinacija između činilaca zaštite i praćenje pravilne primene propisanih mera zaštite kao i inspekcijski nadzor u oblasti informacione bezbednosti.

Predlogom zakona se predviđa da je ministarstvo nadležno za poslove informacione bezbednosti (u daljem tekstu: Nadležni organ) organ državne uprave nadležan za bezbednost IKT sistema. Zakonom o ministarstvima („Službeni glasnik RS”, br. 44/14, 14/15 i 54/15) predviđeno je da Ministarstvo trgovine, turizma i telekomunikacija obavlja poslove državne uprave u oblasti informacionog društva koji se odnose na informacionu bezbednost.

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 ovaj Predlog zakona predviđa da Vlada obrazuje Telo za koordinaciju poslova informacione bezbednosti (u daljem tekstu: Telo za koordinaciju), kao koordinaciono telo Vlade. Predloženo je da ovo telo sačinjavaju predstavnici ministarstva nadležnih za poslove informacionog društva, odbrane, unutrašnjih poslova, spoljnih poslova, pravde, predstavnici službi bezbednosti, Kancelarije Saveta za nacionalnu bezbednost i zaštitu tajnih podataka, Generalnog sekretarijata Vlade, Uprave za zajedničke poslove republičkih organa i Nacionalnog CERT-a.

Predlog zakona uređuje IKT sisteme od posebnog značaja i predviđa obaveze i odgovornost operatora IKT sistema od posebnog značaja za bezbednost IKT sistema i preduzimanje mera zaštite IKT sistema i u slučaju kada su određene aktivnosti u vezi sa tim IKT sistemom poverene trećim licima, kao i obaveza obaveštavanja nadležnih organa o incidentima u IKT sistemima koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti. IKT sistemi od posebnog

značaja su oni IKT sistemi u kojima je neophodno uspostaviti adekvatan nivo informacione bezbednosti, imajući u vidu njihove poslove i delatnosti, kao i rizik nastanka štete po državu i građane u slučaju incidenata u ovim sistemima. Predlogom zakona predviđeno je da Vlada, na predlog ministarstva nadležnog za poslove informacione bezbednosti, bliže uređuje listu poslova i delatnosti kod kojih će postojati obaveza primene adekvatnih mera u skladu sa zakonom.

Predlogom zakona se uređuje da 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, a poslove Nacionalnog CERT-a opredeljuje u nadležnost Regulatorne agencije za elektronske komunikacije i poštanske usluge.

Predlog zakona predviđa da poslove CERT-a republičkih organa obavlja Uprava za zajedničke poslove republičkih organa, kao Centar za bezbednost IKT sistema u republičkim organima (u daljem tekstu: CERT republičkih organa), i to poslove koji se odnose na zaštitu od incidenata u IKT sistemima republičkih organa, izuzev IKT sistema samostalnih operatora.

Prema definiciji iz člana 2. tačka 17) Predloga zakona, samostalni operatori IKT sistema su ministarstvo nadležno za poslove odbrane, ministarstvo nadležno za unutrašnje poslove, ministarstvo nadležno za spoljne poslove i službe bezbednosti.

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

Predlog zakona sadrži posebnu glavu o kriptobezbednosti i zaštiti od kompromitujućeg elektronskog zračenja (KEMZ). Predlogom zakona je predviđeno da je ministarstvo nadležno za poslove odbrane 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. Predlogom zakona se uređuju poslovi i zadaci ministarstva, obaveza primene metoda kriptozaštite, izdavanje odobrenja za kriptografski period i registri u kriptozaštiti.

Radi efikasne primene ovog zakona, potrebno je obezbediti inspekcijski nadzor nad radom IKT sistema od posebnog značaja i drugih IKT sistema stoga je predviđeno u Predlogu zakona da poslove inspekcije za informacionu bezbednost obavlja ministarstvo nadležno za poslove informacione bezbednosti preko inspektora za informacionu bezbednost.

III. OBJAŠNjENjE OSNOVNIH PRAVNIH INSTITUTA I POJEDINAČNIH REŠENjA

U članu 1. Predloga zakona se navodi predmet uređivanja zakona.

Članom 2. se definišu termini koji se koriste u Predlogu zakona.

Član 3. sadrži načela Predloga zakona.

Članom 4. se utvrđuje organ državne uprave nadležan za bezbednost IKT sistema.

U članu 5. propisuje se da Vlada obrazuje Telo za koordinaciju poslova informacione bezbednosti), kao koordinaciono telo Vlade 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.

U članu 6. su utvrđeni IKT sistemi od posebnog značaja, a stavom 2. istog člana propisano je da Vlada, na predlog ministarstva nadležnog za poslove informacione bezbednosti, bliže uređuje listu poslova i delatnosti iz stava 1. ovog člana.

U članu 7. utvrđuju se dužnost operatora IKT sistema od posebnog značaja da preduzimaju odgovarajuće mere zaštite IKT sistema, kojima 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. Ovim članom definišu se i mere zaštite IKT sistema i utvrđuje da bliže uslove za mere uređuje Vlada na predlog Nadležnog organa, uvažavajući međunarodne standarde i standarde koji se primenjuju u odgovarajućim oblastima rada.

U članu 8. se uređuje obaveza operatora IKT sistema od posebnog značaja da donese akt o bezbednosti IKT sistema, kojim se određuju mere zaštite IKT sistema, a naročito principi, način i procedure postizanja i održavanja adekvatnog nivoa bezbednosti ovog sistema, kao i ovlašćenja i odgovornosti u vezi sa ovom bezbednošću i resursima tog sistema, kao i da bliže uslove za sadržaj akta o bezbednosti IKT sistema, način provere IKT sistema i sadržaj izveštaja o proveri IKT sistema od posebnog značaja koji uređuje Vlada na predlog Nadležnog organa.

Član 9. reguliše poveravanje aktivnosti u vezi sa IKT sistemom od posebnog značaja trećim licima, u kom slučaju se propisuje obaveza operatoru da uredi odnos sa tim licima na način koji obezbeđuje preduzimanje mera zaštite tog IKT sistema u skladu sa zakonom.

Članom 10. propisan je izuzetak od odredaba člana 9, ukoliko su aktivnosti u vezi sa IKT sistemom poverene propisom, da se tim propisom mogu drugačije urediti obaveze i odgovornosti operatora IKT sistema od posebnog značaja u vezi poverenih aktivnosti.

Članom 11. propisana je obaveza operatora IKT sistema od posebnog značaja da obaveštavaju Nadležni organ o incidentima u IKT sistemima koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti.

Članom 12. se propisuje dužnost Nadležnog organa da uspostavi i održava međunarodnu bilateralnu i multilateralnu saradnju na polju bezbednosti IKT sistema, a pogotovo da pruži rana upozorenja o rizicima i incidentima, a ako je incident u vezi sa izvršenjem krivičnog dela, po dobijanju obaveštenja od Nadležnog organa, ministarstvo nadležno za unutrašnje poslove da u zvaničnoj proceduri prosledi prijavu nadležnom telu u skladu sa potvrđenim međunarodnim sporazumima.

Članom 13. predviđeno je da će samostalni operatori IKT sistema odrediti posebna lica, odnosno organizacione jedinice za internu kontrolu sopstvenih IKT sistema. A da će lica za internu kontrolu samostalnih operatora IKT sistema izveštaj o izvršenoj internoj kontroli podnositi rukovodiocu samostalnog operatora IKT sistema.

Članom 14. se uređuje Nacionalni centar za prevenciju bezbednosnih rizika u IKT sistemima (u daljem tekstu: Nacionalni CERT) koji obavlja poslove koordinacije prevencije i zaštite od bezbednosnih rizika u IKT sistemima u Republici Srbiji na nacionalnom nivou i utvrđuje nadležnost Regulatorne agencije za elektronske komunikacije i poštanske usluge za poslove Nacionalnog CERT-a.

Članom 15. propisuju se poslovi Nacionalnog CERT-a da 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.

Članom 16. propisuje se nadzor nad radom Nacionalnog CERT-a koji vrši Nadležni organ.

Članom 17. propisuje se osnivanje posebnog centra 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.

Članom 18. propisuje se nadležnost Centra za bezbednost IKT sistema u republičkim organima (u daljem tekstu: CERT republičkih organa) koji obavlja poslove koji se odnose na zaštitu od incidenata u IKT sistemima republičkih organa, izuzev IKT sistema samostalnih operatora, u okviru Uprave za zajedničke poslove republičkih organa.

Član 19. propisuje obavezu samostalnih operatora IKT sistema da formiraju sopstvene centre za bezbednost IKT sistema radi upravljanja incidentima u svojim sistemima i definišu se poslovi iz delokruga rada centra.

Članom 20. propisano je da poslove informacione bezbednosti koji se odnose na kriptobezbednost i KEMZ obavlja ministarstvo nadležno za poslove odbrane.

Članom 21. propisani su poslovi ministarstva nadležnog za poslove odbrane u oblasti kriptobezbednosti i KEMZ.

Članom 22. uređuje se zaštita od kompromitujućeg elektromagnetnog zračenja.

Članom 23. uređuje se obaveza primene metode kriptozaštite.

Članom 24. propisano je da 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 (u daljem tekstu: odobrenje za kriptografski proizvod) i da Vlada, na predlog ministarstva nadležnog za poslove odbrane, bliže uređuje uslove koje moraju da ispunjavaju kriptografski proizvodi iz stava 1. ovog člana.

Članom 25. uređuje se izdavanje odobrenja za kriptografski proizvod.

Članom 26. propisano je da opšte odobrenje za korišćenje kriptografskih proizvoda imaju samostalni operatori IKT sistema.

Članom 27. propisano je da samostalni operatori IKT sistema koji imaju opšte odobrenje za korišćenje kriptografskih proizvoda ustrojavaju i vode registre kriptografskih proizvoda, kriptomaterijala, pravila i propisa i kadra kriptozaštite, a Registar stranih kriptomaterijala vodi Kancelarija Saveta za nacionalnu bezbednost i zaštitu tajnih podataka, u skladu sa ratifikovanim međunarodnim sporazumima, kao i da Vlada, na predlog ministarstva nadležnog za poslove odbrane, bliže uređuje vođenje registara iz ovog člana.

U članu 28. propisani su poslovi inspekcije za informacionu bezbednost koja vrši nadzor nad primenom ovog zakona i radom operatora od posebnog značaja, osim samostalnih operatora IKT sistema i sistema za rad sa tajnim podacima.

U članu 29. propisana su ovlašćenja inspektora za informacionu bezbednost.

U čl. 30. i 31. propisane su kaznene odredbe, predviđene su novčane kazne za odgovorna lica koja prekrše odredbe zakona.

U članu 32. propisani su rokovi za donošenje podzakonskih akata.

U članu 33. je definisan rok za donošenje akta o bezbednosti IKT sistema od posebnog značaja.

Član 34. Predloga zakona je završna odredba o stupanju zakona na snagu.

IV SREDSTVA POTREBNA ZA SPROVOĐENjE ZAKONA

Za sprovođenje ovog zakona nije potrebno obezbediti sredstva u budžetu Republike Srbije za 2015. godinu.

Sredstva za realizaciju zakona u narednim godinama realizovaće se u skladu sa bilansnim mogućnostima budžeta Republike Srbije i predviđenim limitima.

Za sprovođenje ovog zakona potrebno je obezbediti sredstva u budžetu Republike Srbije za 2016. godinu, 2017. godinu i 2018. godinu, u iznosu od 722.005.000 dinara, odnosno 57.500.000, dinara u 2016. godini, 326.048.000 dinara u 2017. godini i 338.457.000 dinara u 2018. godini na razdelima Ministarstva trgovine, turizma i telekomunikacija, Ministarstva odbrane i Uprave za zajedničke poslove republičkih organa.

Predlogom zakona o informacionoj bezbednosti predviđeno je da je nadležni organ državne uprave za bezbednost IKT sistema ministarstvo nadležno za poslove informacione bezbednosti, odnosno Ministarstvo trgovine, turizma i telekomunikacija i da bi na osnovu predloženih zakonskih rešenja to Ministarstvo vršilo sledeće poslove:

- pripremalo podzakonske akte Vlade na osnovu zakona;

- pripremalo i donosilo podzakonske akte iz svoje nadležnosti;
- vršilo inspekcijski nadzor nad operatorima IKT sistema od posebnog značaja (IKT sistema organa javne vlasti, IKT sistema u kojima se obrađuju podaci koji se, u skladu sa zakonom koji uređuje zaštitu podataka o ličnosti, smatraju naročito osetljivim podacima o ličnosti i IKT sistema koji se koriste u obavljanju delatnosti od opšteg interesa);
- primalo obaveštenja o incidentima u IKT sistemima koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti i nalagalo njegovo objavljivanje, ako je incident od interesa za javnost;
- uspostavljanje i održavanje međunarodne bilateralne i multilateralne saradnje na polju bezbednosti IKT sistema, a pogotovo pružanje ranih upozorenja o rizicima i incidentima;
- nadzor nad radom Nacionalnog centra za prevenciju bezbednosnih rizika u IKT sistemima (Nacionalni CERT).

Usled toga, kako bi se navedeni poslovi mogli izvršavati u skladu sa zakonom, neophodno je povećati kapacitete Ministarstva trgovine, turizma i telekomunikacija. Procenjeno je da bi u Ministarstvu u periodu od 2016. do 2018 godini ukupno trebalo 99.340.000 dinara za realizaciju zakona, odnosno 25.500.000 dinara u 2016. godini, 38.420.000 dinara u 2017. godini i 38.420.000 dinara u 2018. godini.

Naime, potrebno je da se obrazuje unutrašnja organizaciona jedinica za informacionu bezbednost i u njoj zaposli 11 državnih službenika u 2017. godini usled čega bi ukupni godišnji rashodi za zaposlene iznosili 13.420.000 dinara u 2017. godini i 13.420.000 dinara u 2018.godini, a godišnji rashodi za korišćenje usluga i roba (službena putovanja, obuke, usluge po ugovoru itd) 2.500.000 dinara u 2016. godini i 5.000.000 dinara u 2017. godini i 5.000.000 dinara u 2018. godini. U okviru sredstava za rad nove organizacione jedinice, pored osnovnog kancelarijskog opremanja računarskom opremom, biće potrebna oprema za sprovođenje mera zaštite tajnih podataka, kao i uspostavljanje informacionog sistema za prijem i obradu obaveštenja o incidentima i inspekcijski nadzor uz primenu odgovarajućih mera zaštite IKT sistema, za šta se procenjuje da je u 2016. godini potrebno 20.000.000 dinara, u 2017. godini 20.000.000 dinara i u 2018. godini 20.000.000 dinara.

Finansijska sredstva potrebna Ministarstvu odbrane za sprovođenje zakona bi iznosila 428.665.000 dinara, odnosno 194.628.000 dinara u 2017. godini i 234.037.000 dinara u 2018. godini.

Rešenja sadržana u Predlogu zakona o informacionoj bezbednosti koja se tiču Ministarstava odbrane odnose se na dobijanje nacionalne nadležnosti za odgovarajuće poslove iz oblasti informacione bezbednosti – „odobravanje kriptografskih proizvoda“, „distribucija kriptomaterijala“ i „zaštitu od kompromitujućeg elektromagnetskog zračenja“ koje bi izvršavala namenska ustanova u okviru ovog ministarstva.

Trenutno, navedena ustanova ne raspolaže dovoljnim resursima (ljudskim, materijalnim i stručnim) za nacionalni nivo, tako da ne obezbeđuje u potpunosti izvršavanje svih poslova i zadataka koji su predloženi u Predlogu zakona o informacionoj bezbednosti.

Da bi navedena ustanova mogla uspešno da izvršava poslove i zadatke iz nadležnosti Ministarstva odbrane koje predviđa Predlog zakona o informacionoj bezbednosti, potrebno je preduzeti mere za dostizanje nedostajućih sposobnosti, a koje se tiču obezbeđenja dodatnih ljudskih resursa, opremanja odgovarajućom opremom za merenje kompromitujućeg elektromagnetnog zračenja (KEMZ) i specijalističkog osposobljavanja personala. Bez navedenog, Ministarstvo odbrane ne bi bilo u mogućnosti da uspešno realizuje nadležnosti predviđene Predlogom zakona.

U skladu sa navedenim, za potrebe realizacije zakona potrebna su Ministarstvu odbrane sredstva za rashode zaposlenih u iznosu od 38.798.000 u

2017. godini i 75.637.000 u 2018. godini. Radi dodatnog opremanja, pre svega za nabavku opreme za detekciju i zaštitu od KEMZ, koja se može nabaviti samo iz inostranstva i pod određenim uslovima neophodna novčana sredstva iznose 142.847.000 dinara u 2017. godini i 140.000.000 dinara 2018. godini, dok je za korišćenje usluga i roba potrebno 12.983.000 dinara u 2017. godini i 18.400.000 dinara u 2018. godini.

Finansijska sredstva potrebna Upravi za zajedničke poslove, u naredne tri godine za realizaciju zakona, iznose ukupno 194.000.000 dinara, odnosno 35.000.000 dinara u 2016. godini, 93.000.000 dinara u 2017. godini i 66.000.000 u 2018. godini.

Naime, potrebno je da se obrazuje unutrašnja organizaciona jedinica za informacionu bezbednost i u njoj zaposli 12 državnih službenika usled čega bi ukupni godišnji rashodi za zaposlene iznosili u 2017. godini i 23.000.000 dinara i u 2018. godini 23.000.000 dinara, dok bi godišnji rashodi za korišćenje usluga i roba iznosili 8.000.00 dinara u 2016. godini, 20.000.000 dinara u 2017. godini i 18.000.000 u 2018. godini. U okviru sredstava za rad Upravi je potrebno u 2016. godini 27.000.000 dinara, u 2017. godini 50.000.000 dinara, a u 2018. godini 25.000.000 dinara.

Shodno navedenom ukupni iznos sredstava za realizaciju ovog zakona bi u nadležnim institucijama u naredne dve godine iznosio:

Sredstva	Godina	MTTT	MO	UZZRO	UKUPNO	
Rashodi za zaposlene	2016	0	0	0	0	187.275.000
	2017	13.420.000	38.798.000	23.000.000	75.218.000	
	2018	13.420.000	75.637.000	23.000.000	112.057.000	
Korišćenje usluga i roba	2016	2.500.000	0	8.000.000	10.500.000	89.883.000
	2017	5.000.000	12.983.000	20.000.000	37.983.000	
	2018	5.000.000	18.400.000	18.000.000	41.400.000	
Osnovna sredstva	2016	20.000.000	0	27.000.000	47.000.000	444.847.000
	2017	20.000.000	142.847.000	50.000.000	212.847.000	
	2018	20.000.000	140.000.000	25.000.000	185.000.000	
UKUPNO		**99.340.000**	**428.665.000**	**194.000.000**	**722.005.000**	

Godina	MTTT	MO	UZZRO	UKUPNO
2016	22.500.000	0	35.000.000	57.500.000
2017	38.420.000	194.628.000	93.000.000	326.048.000
2018	38.420.000	234.037.000	66.000.000	338.457.000
UKUPNO	**99.340.000**	**428.665.000**	**194.000.000**	**722.005.000**

Finansijska sredstva potrebna za uspostavljanje kapaciteta za obavljanje poslova Nacionalnog CERT-a u okviru RATEL-a procenjuju se da su slična sredstvima koja su potrebna Ministarstvu trgovine, turizma i telekomunikacija za poslove nadležnog organa za informacionu bezbednost.

Ukazujemo da je donošenje predmetnog zakona predviđeno Nacionalnim programom za usvajanje pravnih tekovina Evropske unije (NPAA), kao i da su prilikom izrade ovog zakona uvažena strateška rešenja EU u ovoj oblasti i pravne tendencije. Strategijom u ovoj oblasti, Evropska unija je deklarisala odlučnost da se

oblast informacione bezbednosti uredi i da se njen nivo značajno podigne, u čemu moraju da učestvuju nadležni državni organi, koji treba da imaju adekvatne ljudske i tehničke kapacitete.

ANALIZA EFEKATA ZAKONA

1. Problemi koje akt treba da reši

Predmetni zakon predstavlja okvir za uređenje bezbednosti informaciono-komunikacionih sistema u Republici Srbiji. 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.

Upotreba informaciono-komunikacionih tehnologija (IKT) od strane države, privrede i građana je u porastu, i sve više poslova i aktivnosti se zasniva na njihovom korišćenju. Prema podacima Republičkog zavoda za statistiku, objavljenim u okviru dokumenta „Upotreba informaciono-komunikacionih tehnologija u Republici Srbiji, 2015", utvrđeno je da 100% preduzeća na teritoriji Republike Srbije koristi računar u svom poslovanju, da 99,1% preduzeća ima internet priključak, a 98,0% ima širokopojasnu (broadband) internet konekciju. Prema istom izvoru, 94,5% preduzeća koristi elektronske servise javne uprave. Sa druge strane, 64,4% domaćinstava poseduje računar, 63,8% domaćinstava poseduje internet priključak, a 56% domaćinstava u Srbiji ima širokopojasnu (broadband) internet konekciju. Takođe, preko 1.500.000 lica koristi elektronske servise javne uprave, a preko 1.220.000 lica kupovalo je ili poručivalo robu/usluge putem interneta u poslednjih godinu dana.

Razvoj novih tehnologija donosi nesumnjive koristi za društvo, jer se njime omogućava značajno smanjenje troškova, poslovni procesi se automatizuju, olakšavaju i ubrzavaju, brojne informacije postaju dostupne, a mogućnosti komunikacije se znatno proširuju. Brzina razvoja tehnologija je velika, i u kratkim vremenskim intervalima tehnologije napreduju i sadrže nove i naprednije funkcionalnosti. Paralelno sa razvojem novih tehnologija, na globalnom nivou rastu i pretnje njihovoj bezbednosti. Prema navodima iz Strategije informacione bezbednosti Evropske unije (*Cybersecurity Strategy of the European Union*), visokotehnološki kriminal je vrsta kriminala koja je u najvećem porastu, a milion ljudi svakodnevno bude žrtva napada. Prema podacima Ministarstva unutrašnjih poslova, u 2013. godini otkriveno je 855 krivičnih dela u oblasti visokotehnološkog kriminala, a u 2014. godinu otkriveno je 780 krivičnih dela. Preovlađujući oblik ovog kriminala čine falsifikovanje i zloupotreba platnih kartica. Izveštaji institucija koji vrše poslove informacione bezbednosti u IKT sistemima republičkih organa, odnosno naučnoistraživačkoj i obrazovnoj zajednici, govore da su napadi u Republici Srbiji u porastu, pri čemu se ističe da su napadi na mrežu republičkih organa svakodnevni. Narušavanje informacione bezbednosti može da izazove veliku štetu po bezbednost Republike Srbije, imovinu (javnu i privatnu), lične podatke građana i drugo. Povezanost računara i sistema putem Interneta utiče da oni budu ranjiviji i ugroženiji, kao i na mogućnost napada sa bilo koje lokacije u svetu. Prevencija, i zaštita IKT sistema, kao i međusobna saradnja u ovom polju u Republici Srbiji postoje u određenom broju državnih i privatnih subjekata, ali se često vrše na osnovu pojedinačnih inicijativa. Neophodno je da se koordinacija poboljša, i to ne samo na nacionalnom nivou, već i međudržavnom, imajući u vidu da mnogi incidenti u IKT sistemima imaju prekogranični karakter. Osim u pojedinim oblastima gde postoje posebni propisi (u oblasti zaštite tajnih podataka, elektronskih komunikacija, u poslovima finansijskih institucija), nije regulisana obaveza za utvrđivanje mera koje su

neophodne da se preduzmu u cilju zaštite IKT sistema. Organi javne vlasti, lica koja obrađuju naročito osetljive podatke o ličnosti i pravna lica koja obavljaju delatnosti od opšteg interesa moraju da povećaju svoju otpornost na ugrožavanje informacione bezbednosti, jer su poslovi koji vrše od velikog značaja, a njihovo neometano funkcionisanje sve više zavisi od novih tehnologija. U pojedinim delatnostima od opšteg interesa, upotreba IKT sistema je neophodna za vršenje tih delatnosti, te bi ugrožavanje sistema moglo da izazove velike smetnje u obavljanju vitalnih funkcija i prouzrokuje značajnu štetu po državu i njene građane. Pored toga, potrebno je povećati nivo informisanosti o incidentima, na nacionalnom i globalnom nivou, jer se tako širenje incidenata može zaustaviti, ili smanjiti. Takođe, smatra se da je, putem edukacije, potrebno povećati društvenu svest, odnosno svest građana, o opasnostima koje mogu da naruše informacionu bezbednost.

2. Ciljevi koji se aktom postižu

Aktom se informaciona bezbednost reguliše na sistemski način, uz nameru da se odrede nadležni organi u ovoj oblasti i postigne da organi javne vlasti, subjekti koji obrađuju naročito osetljive podatke o ličnosti i subjekti koji obavljaju delatnosti od opšteg interesa (operatori IKT sistema od posebnog značaja) preduzmu adekvatne tehničke i organizacione mere zaštite svojih IKT sistema. Utvrđuje se nadležni organ za informacionu bezbednost u RS, koji će pripremati podzakonske akte na osnovu ovog zakona, vršiti međunarodnu bilateralnu i multilateralnu saradnju na polju bezbednosti IKT sistema i vršiti nadzor nad primenom ovog zakona. Zakonom je predviđeno da ovi subjekti moraju da imaju akt o bezbednosti IKT sistema, kojim se određuju mere zaštite IKT sistema, a naročito principi, način i procedure postizanja i održavanja adekvatnog nivoa bezbednosti ovog sistema, kao i ovlašćenja i odgovornosti u vezi sa ovom bezbednošću i resursima tog sistema. Time se postiže da se poveća bezbednost IKT sistema i unapredi pripremljenost za reagovanje na incidente u onim subjektima koji vrše poslove čija priroda i sadržaj zahtevaju odgovarajući nivo zaštite IKT sistema. Strategijom informacione bezbednosti Evropske unije istaknuto je da je, u cilju unapređenja otpornosti na napade u IKT sistemima, neophodno da javni sektor razvije svoje kapacitete.

S obzirom na globalnu umreženost računara, većina incidenata u IKT sistemima ima međunarodni karakter, a napadi se mogu vršiti sa teritorija različitih država (kao, na primer, putem botnet mreža, gde napadnuti i zaraženi računar postaje računar sa koga se dalje šire napadi) i pričinjavati štetu koja nije ograničena samo na jednu zemlju. U slučajevima ovakvih napada, kvalitetna komunikacija između država doprinosi da se incidenti zaustave i umanje, a počinioci otkriju i onesposobe. Predmetni zakon predviđa da je nadležni organ za informacionu bezbednost u RS dužan da održava međunarodnu bilateralnu i multilateralnu saradnju, a pogotovo da pruži rana upozorenja o rizicima i incidentima koji ispunjavaju najmanje jedan od sledećih uslova: 1) brzo rastu ili imaju tendenciju da postaju visoki rizici, 2) prevazilaze ili mogu da prevaziđu nacionalne kapacitete, 3) mogu da imaju negativan uticaj na više od jedne države.

Pored toga, ovim zakonom se u okviru RATEL-a uspostavlja Nacionalni centar za prevenciju i zaštitu od bezbednosnih rizika u IKT sistemima u Republici Srbiji (Nacionalni CERT), koji prati stanje o incidentima o nacionalnom nivou, obaveštava relevantna lica o rizicima i incidentima, reaguje po prijavljenim incidentima, izrađuje analize rizika i incidenata i podiže svest društva o značaju informacione bezbednosti. Jedna od važnih funkcija Nacionalnog CERT-a je i saradnja sa istim institucijama iz drugih zemalja. Imajući u vidu da incidenti u IKT sistemima najčešće imaju prekogranični karakter, odnosno da se dešavaju na teritoriji više zemalja, međusobna saradnja CERT-ova je od izuzetnog značaja,

kako bi se međusobnom razmenom informacija uspešno odgovorilo na incidente. Republika Srbija je jedna od malobrojnih evropskih država koja nema Nacionalni CERT, što znatno otežava prikupljanje informacija o incidentima i reagovanje na njih. Formiranje ove institucije predviđeno je Strategijom razvoja informacionog društva u Republici Srbiji.

Zakonom se reguliše i oblast kriptozaštite i zaštite od kompromitujućeg elektromagnetnog zračenja (KEMZ). Mere kriptozaštite primenjuju se radi zaštite integriteta, autentičnosti i neporecivosti podataka. Kriptografski proizvodi koji se koriste za zaštitu prenosa i čuvanja podataka koji su određeni kao tajni, moraju da budu verifikovani i odobreni za korišćenje, imajući u vidu svojstva podataka koji se prenose i čuvaju, te se zakonom reguliše izdavanje odobrenja za kriptografski proizvod.

3. Razmatrane mogućnosti da se problem reši i bez donošenja akta

Imajući u vidu sadržinu Zakona, koji određuje nadležnosti organa, obaveze u pogledu zaštite IKT sistema, nadzor nad primenom zakona i druge odredbe, bilo je neophodno da se ova oblast uredi zakonom. Strategijom razvoja informacionog društva u Republici Srbiji do 2020. godine („Službeni glasnik RS” broj 51/10) u poglavlju III. Oblasti i prioriteti strategije predviđeni su prioriteti u šest oblasti informacionog društva. U okviru oblasti informacione bezbednosti predviđena su četiri prioriteta: Unapređenje pravnog i institucionalnog okvira za informacionu bezbednost, zaštita kritične infrastrukture, borba protiv visokotehnološkog kriminala, naučno-istraživački i razvojni rad u oblasti informacione bezbednosti. Konkretni ciljevi predviđeni prioritetom 6.1. Unapređenje pravnog i institucionalnog okvira za informacionu bezbednost podrazumevaju da je potrebno doneti propise iz informacione bezbednosti, kojima će se dodatno urediti standardi informacione bezbednosti, područja informacione bezbednosti, kao i nadležnosti i zadaci pojedinih institucija u ovoj oblasti.

4. Zašto je donošenje akta najbolji način za rešavanje problema

Zakonom se obavezuju operatori IKT sistema od posebnog značaja da preduzmu mere zaštite u svojim IKT sistemima, što je veoma važno kako bi se obezbedilo da ti sistemi budu preventivno zaštićeni i spremni za reakciju u slučaju incidenata. Utvrđuje se nadležni organ za informacionu bezbednost u RS, koji će pripremati podzakonske akte na osnovu ovog zakona, vršiti međunarodnu bilateralnu i multilateralnu saradnju na polju bezbednosti IKT sistema i vršiti nadzor nad primenom ovog zakona. Uspostavljanjem Nacionalnog CERT-a doprineće se unapređenju reakcije na incidente, podizanju stepena obaveštenosti i svesti o incidentima u IKT sistemima i vršiti edukacija. Takođe, Zakonom se utvrđuje nadležnost organa u oblasti kriptobezbednosti i zaštite od KEMZ-a.

5. Na koga će i kako će najverovatnije uticati rešenja u zakonu

Budući da informaciona bezbednost znači zaštitu sistema, podataka i infrastrukture u cilju očuvanja poverljivosti, integriteta i raspoloživosti informacija, primena zakona će imati uticaj na sve građane, organe javne vlasti i privredne subjekte koji koriste informaciono-komunikacione tehnologije. Naime, zakonskim rešenjima postiže se poverenje korisnika u bezbedno funkcionisanje IKT sistema, poverenje građana u zaštićenost podataka o ličnosti u IKT sistemima, širenje svesti o neophodnosti sprovođenja mera informacione bezbednosti, zaštita podataka, zaštita IKT sistema, bezbednost elektronskih transakcija, efikasni mehanizmi zaštite i ostvarivanje prava u procesima elektronskog poslovanja i elektronske razmene podataka.

Zakon određuje IKT sisteme od posebnog značaja u Republici Srbiji. To su IKT sistemi koji se koriste u obavljanju poslova u organima javne vlasti, IKT sistemi za obradu podataka koji se, u skladu sa zakonom koji uređuje zaštitu podataka o ličnosti, smatraju naročito osetljivim podacima o ličnosti i IKT sistema u obavljanju delatnosti od opšteg interesa. Rešenja u zakonu će uticati na ova pravna lica, odnosno organe (operatore IKT sistema od posebnog značaja) tako što će oni biti dužni da preduzmu adekvatne tehničke i organizacione mere zaštite svojih IKT sistema i da donesu akt o bezbednosti IKT sistema, kojim se navedene mere zaštite određuju. 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, čime se obezbeđuje adekvatna zaštita subjekata regulacije u domenu informacione bezbednosti. Operatori IKT sistema od posebnog značaja moći će da povere aktivnosti u vezi sa svojim IKT sistemom trećim licima, pri čemu će morati da urede odnos sa tim licima tako da se obezbedi preduzimanje mera zaštite IKT sistema u skladu sa zakonom. Operatori IKT sistema od posebnog značaja biće dužni da obaveštavaju Nadležni organ (ministarstvo nadležno za poslove informacionog društva) o incidentima u IKT sistemima koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti.

U glavi zakona koja se odnosi na kriptobezbednost i zaštitu od kompromitujućeg elektromagnetnog zračenja (KEMZ) određeno je da se, ukoliko je u okviru IKT sistema predviđeno rukovanje podacima koji su određeni kao tajni, u skladu sa zakonom, u IKT sistemu, radi sprečavanja narušavanja informacione bezbednosti, primenjuju mere zaštite od KEMZ-a. Takođe, mere kriptozaštite primenjuju se kada se tajni podaci prenose sredstvima elektronske komunikacije izvan bezbednosne zone koja je utvrđena za čuvanje i postupanje sa odgovarajućim podacima.

6. *Kakve troškove će primena zakona stvoriti građanima i privredi (naročito malim i srednjim preduzećima)*

Primena Zakona neće stvoriti troškove građanima. Privrednim subjektima koji su operatori IKT sistema od posebnog značaja se nameću određene obaveze ovim zakonom. Za privredne subjekte koji su uspostavili sistem upravljanja informacionom bezbednošću u skladu sa međunarodnim standardima i dobrom praksom u ovoj oblasti, ne očekuje se da primena zakona izazove značajne troškove.

Privredni subjekti koji predstavljaju operatore IKT sistema od posebnog značaja, a koji do sada nisu uspostavili odgovarajući sistem upravljanja informacionom bezbednošću imaće određene troškove za ispunjenje zakonskih obaveza koji se ogledaju u eventualnom dodatnom tehnološkom opremanju, obuci zaposlenih, angažovanju novih stručnjaka i slično. Precizni iznosi dodatnih troškova za navedene subjekte variraju u velikom rasponu, budući da isti zavise od više faktora koji mogu da budu veoma različiti u različitim privrednim subjektima. Naime, koliko će finansijskih sredstava za primenu zakona izdvojiti ovi privredni subjekti zavisi od njihove veličine, odnosno broja zaposlenih, tehnološke opremljenosti (posedovanje računarske opreme, informacionog sistema), obučenosti zaposlenih za korišćenje informacionih tehnologija u domenu informacione bezbednosti, i drugih faktora od kojih funkcionisanje informacione bezbednosti zavisi u jednom privrednom subjektu. Shodno navedenom, nije moguće dati ni tačne, ni okvirne iznose po privrednom subjektu.

U obrazloženju Predloga zakona, odeljku IV Finansijska sredstva, prikazani su troškovi za realizaciju zakona u naredne dve godine, koji će se finansirati iz Budžeta Republike Srbije.

7. Da li su pozitivne posledice donošenja zakona takve da opravdavaju troškove koje će on stvoriti

Nesporno je da će donošenje Zakona o informacionoj bezbednosti dovesti do pozitivnih posledica, uređenja, razvoja i unapređenja informacione bezbednosti u Republici Srbiji, i da su troškovi koje će primena zakona stvoriti u potpunosti opravdani.

Zakonom se uspostavlja institucionalni okvir u Republici Srbiji, kojim se obezbeđuje očuvanje bezbednosti IKT sistema, tako što se određuju nadležne institucije i definiše delokrug njihovog rada u oblasti informacione bezbednosti (nadležni organ za IB, Nacionalni CERT, CERT republičkih organa, ministarstvo nadležno za poslove odbrane).

Uloga nadležnih institucija koja se definiše ovim zakonom sastoji se u prevenciji, zaštiti, očuvanju i nesmetanom funkcionisanju IKT sistema na teritoriji Republike Srbije.

Troškovi koji nastaju donošenjem zakona su neophodni za jačanje uloge državnih institucija u ovoj oblasti i primenu zakona u potpunom obimu, kako bi se njihovi poslovi obavljali na način koji će omogućiti održavanje adekvatnog nivoa informacione bezbednosti u Republici Srbiji.

Takođe, zakonska rešenja koja se tiču IKT sistema od posebnog značaja predviđaju obaveze ovih sistema da preduzmu mere zaštite IKT sistema, kojim 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, odnosno donesu Akt o bezbednosti IKT sistema kojim se određuju 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.

Primena zakona kojim se operatorima IKT sistemima od posebnog značaja propisuju navedene obaveze su od posebne važnosti, budući da se ovi IKT sistemi koriste u obavljanju poslova u organima javne vlasti, za obradu naročito osetljivih podataka o ličnosti i u obavljanju delatnosti od opšteg interesa.

Zakonska rešenja koja utvrđuju ulogu nadležnih institucija u domenu informacione bezbednosti, kao i uvođenje obaveza operatorima IKT sistema od posebnog značaja, stvara koristi koje se ogledaju u očuvanju bezbednosti IKT sistema, nacionalne bezbednosti, zaštiti osnovnih ljudskih prava, ličnih podataka i privatnosti koji su garantovani međunarodnim i nacionalnim pravnim aktima.

Troškovi koji će se stvoriti primenom ovog zakona su nužni i neophodni, imajući u vidu da narušavanje informacione bezbednosti može da izazove veliku štetu po nacionalnu bezbednost, funkcionisanje organa javne vlasti i privrednih subjekata, lične podatke, imovinu i druga dobra, kao i porast visokotehnološkog kriminala, neophodno je preduzeti preventivne mere u cilju zaštite od incidenata, i, u slučaju incidenta, reagovati na brz i efikasan način. Da bi se to postiglo, važno je obezbediti da IKT sistem zaštiti tajnost, integritet, raspoloživost, autentičnost i neporecivost podataka kojima se rukuje putem tog sistema, da bi taj sistem

funkcionisao kako je predviđeno, kada je predviđeno i pod kontrolom ovlašćenih lica. S obzirom na značaj informacione bezbednosti, troškovi koji će nastati radi primena mere zaštite su nužni i opravdani, jer je nesporno da IKT sistemi moraju da budu zaštićeni i da troškovi koji nastanu predstavljaju ulaganje koje treba da donese opštu korist. Eventualne štete koje bi se desile narušavanjem informacione bezbednosti u mnogim slučajevima bi mogle da daleko premaše visinu ulaganja u bezbednost IKT sistema.

8. Da li se zakonom podržava stvaranje novih privrednih subjekata na tržištu i tržišna konkurencija

Kao što je navedeno, Zakonom je planirano da se urede mere zaštite od bezbednosnih rizika u IKT sistemima u Republici Srbiji. Očekuje se da će se zbog toga javiti potreba za nabavljanjem proizvoda, odnosno usluga koje će, pored ostalih funkcija, služiti i za zaštitu ovih sistema. Usled toga, procenjuje se da će primena ovog zakona uticati na razvoj tržišta IKT proizvoda i usluga u oblasti informacione bezbednosti, što će dovesti i do prisustva većeg broja učesnika na tržištu odnosno veće tržišne konkurencije u toj oblasti.

9. Da li su sve zainteresovane strane imale priliku da se izjasne o zakonu

Ministarstvo trgovine, turizma i telekomunikacija sprovelo je javnu raspravu o Nacrtu zakona o informacionoj bezbednosti u periodu od 3. do 23. jula 2015. godine, na osnovu zaključka Odbora za privredu i finansije Vlade 05 Broj: 011-7073/2015-1 od 2. jula 2015. godine. Nacrt zakona je objavljen na sajtu Ministarstva trgovine, turizma i telekomunikacija www.mtt.gov.rs i portalu eUprava www.euprava.gov.rs. U okviru javne rasprave, održan je okrugli sto u Privrednoj komori Srbije 10. jula 2015. godine, koji je bio veoma uspešan i posećen. U javnoj raspravi učestvovali su predstavnici državnih organa, privrednog sektora, akademske zajednice, nevladinih organizacija i eminentni stručnjaci u ovoj oblasti. Ministarstvo je, tokom javne rasprave, putem Kancelarije za evropske integracije uputilo Nacrt zakona Evropskoj komisiji, radi pribavljanja ekspertize.

Tokom javne rasprave upućeni su sledeći komentari i sugestije na tekst Nacrta zakona:

- Predstavnik „Društva za informatiku Srbije" istakao je da je potrebno utvrditi u zakonu odgovornosti rukovaoca (operatora) IKT sistema kao i da se Telu za koordinaciju poslova informacione bezbednosti daju jača, izvršena ovlašćenja. U vezi sa navedenom primedbom, konstatovano je da su Nacrtom zakona utvrđene obaveze operatora IKT sistema od posebnog značaja i njihova odgovornost, posebno u slučaju postupanja suprotno zakonu.
  U vezi primedbe da se Telu za koordinaciju poslova daju jača ovlašćenja, konstatovano je da to Telo nije nova institucija, već skup predstavnika organa koji su relevantni u toj oblasti čija će neposredna saradnja i komunikacija obezbediti da se poslovi informacione bezbednosti vrše efikasno.
- Tomislav Unkašević je izneo sugestiju da nije jasna uloga Tela za koordinaciju poslova informacione bezbednosti i predložio da se klasifikacija IKT sistema od posebnog značaja vrši na osnovu obima tog IKT sistema. U vezi primedbe na ulogu Tela za koordinaciju poslova informacione bezbednosti razjašnjena je uloga koju isto ima i značaj učešća saradnje i komunikacije u funkcionisanju istog. Primedba se klasifikacija IKT sistema od posebnog značaja vrši na osnovu obima tog IKT sistema nije usvojena, zakon

precizirao koji su to sistemi koji spadaju u IKT sistema od posebnog značaja, pri tome ne ulazeći u pitanje obima tog IKT sistema.

Takođe, imenovani je istakao da Nacionalni CERT treba da ima operativniju ulogu, i da CERT republičkih organa treba da bude na hijerarhijski višem nivou u odnosu na predloženo rešenje iz Nacrta zakona. Stav predstavnika radne grupe, bio je da se uloga koja je Nacionalnom i republičkom CERT-u dodeljena Nacrtom zakona adekvatna i da je to model koji odgovara potrebama regulisanja informacione bezbednosti u RS.

Postavljeno je i pitanje gde je i kako definisano ko propisuje kriterijume koje kripotografski proizvod treba da ispuni kako bi se rešavalo o njihovom odobravanju, nakon čega je ukazano od strane predstavnika Ministarstva odbrane, da definisanje procedure i kriterijuma za evaluaciju kriptografskih bezbednosnih rešenja vrši Ministarstvo odbrane.

- Predstavnik „Share fondacije“ predložio je da se u Telo za koordinaciju poslova informacione bezbednosti uključe i druga tela iz privrednog sektora i akademske zajednice, NVO i drugih, što je prihvaćeno, te je zakonskim rešenjem predložena da predstavnici ovog sektora mogu da budu u sastavu stručnih radnih grupa Tela za koordinaciju.

  Od strane istog predstavnika predloženo je da se dopune i kaznene odredbe što je prihvaćeno i izvršena je dopuna članova koji regulišu kaznene odredbe.

  Predloženo je takođe da se u članu 7. definiše dostavljanje podataka bezbednosnim službama i ministarstvu nadležnom za poslove unutrašnje politike samo po nalogu suda, međutim ovaj član zakona je brisan, imajući u vidu da je predmetna materija već uređena Zakonikom o krivičnom postupku i drugim propisima, tako da primedba nije od uticaja.

  Sugestija, istog predstavnika, da se podaci o incidentima od strane operatora IKT sistema od posebnog značaja ne dostavljaju samo Nadležnom organu, već i Nacionalnom CERT-u, kao i da se osnaži uloga CERT nije prihvaćena budući da je stav radne grupe bio da se CERT-u ne daju veća ovlašćenja i odgovornosti od one koja je predviđena Nacrtom zakona.
- Dat je predlog da se termin „rukovalac IKT sistema“ promeni, što je i prihvaćena, te je termin zamenjen terminom „operator IKT sistema“
- Predstavnik Nacionalnog konventa o Evropskoj uniji smatrao je da je zakon uopšteno napisan, a naročito kod uređenja IKT sistema pod posebnog značaja. Povodom toga izvršene su izmene i dopunjene su odredbe koje se tiču IKT sistema od posebnog značaja, tako što su definisane mere zaštite IKT sistema kojima se obezbeđuje prevencija od nastanka incidenata, odnosno prevencija i minimizacija štete od incidenata koji ugrožavaju vršenje nadležnosti i obavljanje delatnosti. Prilikom definisanja mera uzeti su u obzir međunarodni standardi u oblasti informacione bezbednosti, kako je i sugerisano.
- Isti predstavnik istakao je da su odredbe o Nacionalnom CERT-u adekvatno napisane.
- Predstavnik „Društva za informacionu bezbednost“ napomenuo je da je pitanju kripotozaštite i zaštite od KEMZ-a dato previše prostora u Nacrtu zakona, kao i da bi lica koja obavljaju poslove u IKT sistemima morala biti sertifikovana. U vezi sa tim, ukazujemo da su Nacrtom zakona predviđene mere zaštite koje operatori IKT sistema moraju preduzeti u odnosu na zaposlena lica.
- Predstavnik Registra nacionalnog Internet domena Srbije ponovio je da bi odredbe o dostavljanju podataka bezbednosnim službama i MUP-u morale da se dopune u smislu da se ti podaci mogu dostavljati uz nalog suda, s tim da je

član 7. koje to pitanje reguliše brisan, iz razloga koji su gore navedeni, pa je samim tim primedba bez uticaja.

- Predstavnik „Diplo fondacije“ istakao je da je previše obaveza dato ministarstvu nadležnom za informaciono društvo i da je potrebno osnažiti Nacionalni CERT.
  Takođe je sugerisano da Telo za koordinaciju poslova informacione bezbednosti treba da sadrži i članove iz drugih struktura, što je i prihvaćeno i te je zakonskim rešenjem predloženo da predstavnici ovog sektora budu u sastavu stručnih radnih grupa Tela za koordinaciju.
- Predstavnik kompanije „SBB” smatrao je da Nacrt zakona sadrži mnogo podzakonskih akata, što je prihvaćeno i smanjen je broj podzakonskih akata, tako što su umesto donošenja podzakonskog akta određene stavke regulisane u samom Zakonu.

U skladu sa navedenim komentari na tekst Nacrta zakona, izneti tokom javne rasprave, najčešće se odnose na nekoliko pitanja koje Nacrt zakona obuhvata. Istaknuto je da je donošenje ovog zakona veoma značajno i da ga je neophodno što pre doneti, s obzirom na potrebu da se informaciono-komunikacioni (IKT) sistemi u Republici Srbiji zaštite na način koji će omogućiti potreban nivo informacione bezbednosti. Iskazani su predlozi za izmenu i preciziranje definicija pojmova datih u Zakonu.

Više učesnika je upućivalo pitanje o tome na koje će se subjekte ovaj zakon odnositi, da li samo na državne organe, ili i na privredne subjekte. Predstavnici Ministarstva su na okruglom stolu ukazali da su članom 8. Nacrta zakona o informacionoj bezbednosti obuhvaćeni IKT sistemi koje koriste državni organi, ali i subjekti u privatnom sektoru.

Komentarisano je osnivanje Tela za koordinaciju poslova informacione bezbednosti, koje se osniva u skladu sa članom 62. Zakona o državnoj upravi („Službeni glasnik RS” broj 79/05, 101/07, 95/10 i 99/14) u cilju ostvarivanja saradnje i usklađenog obavljanja poslova u funkciji unapređenja informacione bezbednosti, i navedeno je da je potrebno ovom telu dati izvršna ovlašćenja, kao i da bi, pored državnih organa, u njegov rad trebalo uključiti predstavnike privrede, nevladinih organizacija i drugih subjekata, što je prihvaćeno i te je zakonskim rešenjem predloženo da predstavnici ovog sektora budu u sastavu stručnih radnih grupa ovog Tela.

U vezi sa članom 6, kojim se propisuje da su rukovaoci svih IKT sistema odgovorni za preduzimanje odgovarajućih mera informacione bezbednosti, napomenuto je da je odredba suviše uopštena i da nije regulisana odgovornost za njeno kršenje, te je ta odredba zakona brisana.

U pogledu člana 7, kojim se predviđa obaveza dostavljanja podataka od značaja za informacionu bezbednost, koji su službama bezbednosti i ministarstvu nadležnom za unutrašnje poslove potrebni pri obavljanju poslova iz njihove nadležnosti u skladu sa zakonom, sugerisano je da je neophodno izvršiti preciziranje tog člana, odnosno da se konkretno definiše koji se podaci dostavljaju, kao i da se predvidi da podaci mogu da se traže na osnovu odluke suda. Međutim, član 7. je brisan jer je obaveza dostavljanja podataka bezbedonosnim službama i ministarstvu zaduženom za unutrašnje poslove već regulisana Zakonikom o krivičnom postupku i Zakonom o elektronskim komunikacijama.

Takođe, navedeno je da se član 11, kojim se definiše poveravanje IKT sistema trećim licima treba detaljnije urediti, pre svega po pitanja regulisanja odnosa između operatora IKT sistema od javnog značaja i trećih lica u pogledu eventualne odgovornosti za štetu. Ukazujemo da je pitanje naknade štete uređeno opštim propisima koji se shodno primenjuju.

U pogledu odredaba zakona o Nacionalnom centru za prevenciju bezbednosnih rizika u IKT sistemima (Nacionalnom CERT-u), više učesnika je sugerisalo da bi Nacionalni CERT trebao da ima snažnija ovlašćenja, u smislu da mu je potrebno dati operativne nadležnosti. Međutim kako se Nacionalni CERT prvi put osniva ovim zakonom ideja je da njegova uloga bude sa tzv. mekim ovlašćenjima, te će se u praksi potom utvrditi da li je potrebno njegovu ulogu učiniti jačom ili ne.

Učesnici smatraju da je predviđeno malo kaznenih odredbi u Zakonu i da bi trebalo propisati više prekršajnih kazni, što je prihvaćeno i izvršene su izmene kaznenih odredbi u Nacrtu zakona.

Istaknute su primedbe na brojnost podzakonskih akata koji treba da se donesu na osnovu zakona, kao i na, kako se smatra, preduge rokove za donošenje podzakonskih akata, koji iznose 12 meseci od dana na stupanja na snagu ovog zakona. Prihvaćena je sugestija o smanjenju broju podzakonskih akata, te je broj istih smanjen tako što su umesto donošenja podzakonskog akta određene stavke regulisane u samom zakonu, međutim rok od 12 meseci za donošenje podzakonskih akata nije menjan, budući da je usled kompleksnosti materije koja se reguliše podzakonskim aktima procenjeno da je potreban rok od 12 meseci za donošenje istih.

10. Koje će se mere tokom primene zakona preduzeti da bi se ostvarilo ono što se donošenjem zakona namerava

Institucionalne mere potrebno je preduzeti u sledećim organima:

- Nadležni organ (ministarstvo nadležno za poslove informacione bezbednosti, odnosno Ministarstvo trgovine, turizma i telekomunikacija)

  U okviru Nadležnog organa, odnosno Ministarstva trgovine, turizma i telekomunikacija potrebno je da se obrazuje unutrašnja organizaciona jedinica za informacionu bezbednost i u njoj zaposli 11 državnih službenika usled čega bi ukupni godišnji rashodi za zaposlene iznosili 13.420.000 dinara, a godišnji rashodi za korišćenje usluga i roba (službena putovanja, obuke, usluge po ugovoru itd) 5.000.000 dinara. U okviru sredstava za rad nove organizacione jedinice, pored osnovnog kancelarijskog opremanja računarskom opremom, biće potrebna oprema za sprovođenje mera zaštite tajnih podataka, kao i uspostavljanje informacionog sistema za prijem i obradu obaveštenja o incidentima i inspekcijski nadzor uz primenu odgovarajućih mera zaštite IKT sistema, za šta se procenjuje da je u 2016. godini potrebno 40.000.000 dinara, a u 2017. godini 20.000.000 dinara.

  Na predlog ministarstva nadležnog za poslove informacione bezbednosti formira se i Telo za koordinaciju poslova informacione bezbednosti. Navedeno Telo obrazuje Vlada 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, kao koordinaciono telo Vlade. Obrazovanje Tela za koordinaciju informacione bezbednosti ne iziskuje dodatne troškove.

- Ministarstvo nadležno za poslove odbrane (Ministarstvo odbrane)

  Rešenja sadržana u Predlogu zakona o informacionoj bezbednosti koja se tiču Ministarstava odbrane odnose se na dobijanje nacionalne nadležnosti za odgovarajuće poslove iz oblasti informacione bezbednosti – „odobravanje kriptografskih proizvoda“, „distribucija kriptomaterijala“ i „zaštitu od kompromitujućeg elektromagnetskog zračenja“ koje bi izvršavala namenska ustanova u okviru ovog ministarstva.

Da bi navedena ustanova mogla uspešno da izvršava poslove i zadatke iz nadležnosti Ministarstva odbrane koje predviđa Predlog zakona o informacionoj bezbednosti, potrebno je preduzeti mere za dostizanje nedostajućih sposobnosti, a koje se tiču obezbeđenja dodatnih ljudskih resursa, opremanja odgovarajućom opremom za merenje kompromitujućeg elektromagnetnog zračenja (KEMZ) i specijalističkog osposobljavanja personala. Bez navedenog, Ministarstvo odbrane ne bi bilo u mogućnosti da uspešno realizuje nadležnosti predviđene Predlogom zakona.

U skladu sa navedenim, za potrebe realizacije zakona potrebna su Ministarstvu odbrane sredstva za rashode zaposlenih u iznosu od 60.580.000 dinara u 2016. godini i 71.360.000 u 2017. godini. Radi dodatnog opremanja, pre svega za nabavku opreme za detekciju i zaštitu od KEMZ, koja se može nabaviti samo iz inostranstva i pod određenim uslovima neophodna novčana sredstva iznose 142.847.000 dinara u 2016. godini i 140.000.000 dinara 2017. godini, dok je za korišćenje usluga i roba potrebno u naredne dve godine po 18.919.000 dinara.

- Uprava za zajedničke poslove republičkih organa

  Finansijska sredstva potrebna Upravi za zajedničke poslove, u naredne dve godine za realizaciju zakona, odnosno za osnovna sredstva iznose ukupno 132.138.000 dinara, odnosno 82.138.000 dinara u 2016. godini i 50.000.000 dinara u 2017. godini. Budući da ovaj organ raspolaže ljudskim kapacitetima, sredstava za te namene nisu predviđena.

- Regulatorna agencija za elektronske komunikacije
  Finansijska sredstva potrebna za uspostavljanje kapaciteta za obavljanje poslova Nacionalnog CERT-a u okviru RATEL-a procenjuju se da su slična sredstvima koja su potrebna Ministarstvu trgovine, turizma i telekomunikacija za poslove nadležnog organa za informacionu bezbednost i da iznose oko 100 miliona dinara za period od naredne dve godine.

- Neregulatorne mere

  Nakon usvajanja Zakona, ministarstvo nadležno za poslove informacione bezbednosti planira upoznavanje javnosti sa zakonom, kako u okviru svojih redovnih informativnih kampanja, tako i putem namenskih okruglih stolova i drugih vidova informisanja kojima će se građanima Republike Srbije pružiti neophodne informacije o rešenjima koja predviđa zakon. Takođe, Predlogom zakona je predviđeno da je jedna od nadležnosti Nacionalni CERT-a da 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.

Radi izvršavanja Predloga zakona o informacionoj bezbednosti (u daljem tekstu: Predlog zakona), predviđeno je da Vlada donese sledeće akte:

- Odluka o obrazovanju Tela za koordinaciju poslova informacione bezbednosti (na osnovu člana 5. Predloga zakona)
- Uredba o bližem uređenju Liste poslova i delatnosti IKT sistema od posebnog značaja (na osnovu člana 6. Predloga zakona)
- Uredba o bližim uslovima za mere zaštite IKT sistema od posebnog značaja (na osnovu člana 7. Predloga zakona)

- Uredba o bližem sadržaju akta o bezbednosti IKT sistema, načinu interne provere IKT sistema i sadržaju izveštaja o proveri IKT sistema (na osnovu člana 8. Predloga zakona)
- Uredba o usvajanju Liste incidenata i načinu obaveštavanja o incidentima u IKT sistemima koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti (na osnovu člana 11. Predloga zakona)
- Uredba o bližim uslovima za proveru kompromitujućeg elektromagnetnog zračenja (KEMZ) i načina procene rizika od oticanja podataka putem KEMZ (na osnovu člana 22. Predloga zakona)
- Uredba o tehničkim uslovima 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 (na osnovu člana 23. Predloga zakona)
- Uredba o bližim uslovima koje moraju da ispunjavaju kriptografski proizvodi koji se koriste za zaštitu prenosa i čuvanja podataka koji su određeni kao tajni (na osnovu člana 24. Predloga zakona)
- Uredba o sadržaju zahteva za izdavanje odobrenja za kriptografski proizvod, uslovima za izdavanje odobrenja za kriptografski proizvod, načinu izdavanja odobrenja, naknadi za izdavanje odobrenja i sadržaju registra izdatih odobrenja za kriptografski proizvod (na osnovu člana 25. Predloga zakona)
- Uredba o bližim uslovima za vođenje registara kriptografskih proizvoda, kriptomaterijala, pravila i propisa i kadra kriptozaštite koje vode samostalni rukovaoci IKT sistema (na osnovu člana 27. Predloga zakona).

Predlogom zakona predviđeno je da ministarstvo nadležno za poslove informacionog društva donosi sledeće podzakonske akte:

- Pravilnik o bližim uslovima za upis u evidenciju posebnih centara za prevenciju bezbednosnih rizika u IKT sistemima (na osnovu člana 17. Predloga zakona)

Prema članu 32. Predloga zakona, podzakonska akta predviđena ovim zakonom doneće se u roku od 12 meseci od dana stupanja na snagu ovog zakona.

IZJAVA O USKLAĐENOSTI PROPISA SA PROPISIMA EVROPSKE UNIJE

1. Ovlašćeni predlagač propisa: Vlada

Obrađivač: Ministarstvo trgovine, turizma i telekomunikacija

2. Naziv propisa

Predlog zakona o informacionoj bezbednosti
Draft Law on Information Security

3. Usklađenost propisa s odredbama Sporazuma o stabilizaciji i pridruživanju između Evropskih zajednica i njihovih država članica, sa jedne strane, i Republike Srbije sa druge strane („Službeni glasnik RS”, broj 83/08) (u daljem tekstu: Sporazum), odnosno s odredbama Prelaznog sporazuma o trgovini i trgovinskim pitanjima između Evropske zajednice, sa jedne strane, i Republike Srbije, sa druge strane („Službeni glasnik RS”, broj 83/08) (u daljem tekstu: Prelazni sporazum):

a) Odredba Sporazuma i Prelaznog sporazuma koja se odnose na normativnu sadržinu propisa

Naslov VII „Politike saradnje”, član 105. Informaciono društvo - Sporazum o stabilizaciji i pridruživanju između Evropskih zajednica i njihovih država članica, sa jedne strane, i Republike Srbije sa druge strane.

b) Prelazni rok za usklađivanje zakonodavstva prema odredbama Sporazuma i Prelaznog sporazuma

Tri godine.

v) Ocena ispunjenosti obaveze koje proizlaze iz navedene odredbe Sporazuma i Prelaznog sporazuma

Ispunjava u potpunosti.

g) Razlozi za delimično ispunjavanje, odnosno neispunjavanje obaveza koje proizlaze iz navedene odredbe Sporazuma i Prelaznog sporazuma

/

d) Veza sa Nacionalnim programom za usvajanje pravnih tekovina Evropske unije

Nacionalni program za usvajanje pravnih tekovina Evropske unije (2014-2018), Prilog A – Plan usklađivanja zakonodavstva Republike Srbije sa pravnim tekovinama Evropske unije, 3.10. Informaciono društvo i mediji, 3.10.2. Informaciono društvo, Redni broj 28, Šifra plan. propisa: 2014-345. Plan zakonodavnog postupka: 2015/VI

4. Usklađenost propisa sa propisima Evropske unije:
a) Navođenje odredbi primarnih izvora prava Evropske unije i ocene usklađenosti sa njima

Naslov V, Poglavlje I, član 67. i 73. Ugovora o funkcionisanju Evropske unije. Predlog zakona o informacionoj bezbednosti je potpuno usklađen sa navedenim članovima.

b) Navođenje sekundarnih izvora prava Evropske unije i ocene usklađenosti sa njima

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace ***/* JOIN/2013/01 final */*** - POTPUNO USKLAĐENO

v) Navođenje ostalih izvora prava Evropske unije i usklađenost sa njima

/

g) Razlozi za delimičnu usklađenost, odnosno neusklađenost

/

d) Rok u kojem je predviđeno postizanje potpune usklađenosti propisa sa propisima Evropske unije

/

5. Ukoliko ne postoje odgovarajuće nadležnosti Evropske unije u materiji koju reguliše propis, i/ili ne postoje odgovarajući sekundarni izvori prava Evropske unije sa kojima je potrebno obezbediti usklađenost, potrebno je obrazložiti tu činjenicu. U ovom slučaju, nije potrebno popunjavati Tabelu usklađenosti propisa. Tabelu usklađenosti nije potrebno popunjavati i ukoliko se domaćim propisom ne vrši prenos odredbi sekundarnog izvora prava Evropske unije već se isključivo vrši primena ili sprovođenje nekog zahteva koji proizilazi iz odredbe sekundarnog izvora prava (npr. Predlogom odluke o izradi strateške procene uticaja biće sprovedena obaveza iz člana 4. Direktive 2001/42/EZ, ali se ne vrši i prenos te odredbe direktive).
U oblasti koju zakon uređuje nije donet propis (direktiva) Evropske unije, usled čega nije bilo moguće sačinjavanje tabele usklađenosti. Prilikom izrade Predlog zakona o informacionoj bezbednosti, uvažena su rešenja iz Predloga direktive o mrežnoj i informacionoj bezbednosti (*Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, COM(2013) 48 final, 2013/0027 (COD)).* Takođe, poštovana su načela iz Strategije informacione bezbednosti Evropske unije (*JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* ***/* JOIN/2013/01 final */*** *,)*.
S obzirom da je predlog gore navedene direktive još uvek u fazi pripreme i usaglašavanja na nivou EU, i da nije važeći akt, tabela usklađenosti nije izrađena.

6. Da li su prethodno navedeni izvori prava Evropske unije prevedeni na srpski jezik?

/

7. Da li je propis preveden na neki službeni jezik Evropske unije?
/

8. Učešće konsultanata u izradi propisa i njihovo mišljenje o usklađenosti

Tekst Nacrta zakona o informacionoj bezbednosti poslat je Evropskoj komisiji, putem Kancelarije za evropske integracije, radi davanja ekspertize. Imajući u vidu da propis Evropske unije iz ove oblasti još uvek nije donet, predstavnici Evropske komisije obavestili su Kancelariju za evropske integracije da analiza usklađenosti Nacrta zakona o informacionoj bezbednosti pre donošenja direktive nije celishodna.