Z A K O N

O IZMENAMA I DOPUNAMA ZAKONA O INFORMACIONOJ BEZBEDNOSTI

Član 1.

U Zakonu o informacionoj bezbednosti („Službeni glasnik RS”, br. 6/16 i 94/17), u članu 2. stav 1. tačka 1) podtačka (3) reč: „pohranjuje” zamenjuje se rečima: „vode, čuvaju”.

Posle podtačke (4) dodaje se podtačka (5), koja glasi:

„(5) sve tipove sistemskog i aplikativnog softvera i softverske razvojne alate.”.

U tački 2) reči: „organ javne vlasti ili organizaciona jedinica organa javne vlasti” zamenjuju se rečima: „organ vlasti ili organizaciona jedinica organa vlasti”.

Tačka 11) menja se i glasi:

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

Posle tačke 11) dodaje se tačka 11a), koja glasi:

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

Tačka 15) menja se i glasi:

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

Tačka 24) menja se i glasi:

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

Posle tačke 24) dodaju se tač. 25) i 26), koje glase:

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

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

Član 2.

Posle člana 3. dodaje se član 3a, koji glasi:

„Obrada podataka o ličnosti

Član 3a

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

Član 3.

U članu 5. stav 1. posle reči: „Generalnog sekretarijata Vlade” dodaju se reči: „Narodne banke Srbije”, a reči: „CERT-a republičkih organa i Nacionalnog CERT-a” zamenjuju se rečima: „Centra za bezbednost IKT sistema u organima vlasti i Nacionalnog centra za prevenciju bezbednosnih rizika u IKT sistemima.”

U stavu 2. reči: „organa javne vlasti” zamenjuju se rečima: „organa vlasti”.

Član 4.

Član 6. menja se i glasi:

„IKT sistemi od posebnog značaja

Član 6.

IKT sistemi od posebnog značaja su sistemi koji se koriste:

1) u obavljanju poslova u organima vlasti;

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

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

(1) energetika:

- proizvodnja, prenos i distribucija električne energije;
- proizvodnja i prerada uglja;
- istraživanje, proizvodnja, prerada, transport i distribucija nafte i promet nafte i naftnih derivata;
- istraživanje, proizvodnja, prerada, transport i distribucija prirodnog i tečnog gasa.

(2) saobraćaj:

- železnički, poštanski, vodni i vazdušni saobraćaj;

(3) zdravstvo:

- zdravstvena zaštita;

(4) bankarstvo i finansijska tržišta:

- poslovi finansijskih institucija;
- poslovi vođenja registra podataka o obavezama fizičkih i pravnih lica prema finansijskim institucijama;
- poslovi upravljanja, odnosno obavljanja delatnosti u vezi sa funkcionisanjem regulisanog tržišta;

(5) digitalna infrastruktura:

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

(6) dobra od opšteg interesa:

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

(7) usluge informacionog društva:

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

(8) ostale oblasti:

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

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

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

Član 5.

Posle člana 6. dodaju se čl. 6a i 6b, koji glase:

„Obaveze operatora IKT sistema od posebnog značaja

Član 6a

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

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

2) preduzme mere zaštite IKT sistema od posebnog značaja;

3) donese akt o bezbednosti IKT sistema;

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

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

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

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

Evidencija operatora IKT sistema od posebnog značaja

Član 6b

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

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

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

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

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

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

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

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

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

Član 6.

U članu 7. stav 2. reč: „minimizacija” zamenjuje se rečju: „smanjenje”.

U stavu 3. tačka 11) reč: „odnosno” zamenjuje se rečju: „i”.

U tački 23) reči: „pitanja informacione bezbednosti” zamenjuju se rečima: „ispunjenje zahteva za informacionu bezbednost”.

Član 7.

Član 11. menja se i glasi:

„Obaveštavanje o incidentima

Član 11.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Član 8.

Posle člana 11. dodaju se čl. 11a i 11b, koji glase:

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

Član 11a

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

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

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

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

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

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

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

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

Dostavljanje statističkih podataka o incidentima

Član 11b

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

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

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

Član 9.

U članu 12. stav 1. tačka 1) reči: „visoki rizici” zamenjuju se rečju: „visokorizični”.

Član 10.

Iznad člana 13. dodaje se naziv člana, koji glasi: „Samostalni operatori IKT sistema”.

Član 11.

Posle člana 13. dodaje se član 13a, koji glasi:

„Shodna primena odredaba o samostalnim operatorima IKT sistema

Član 13a

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

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

Član 12.

U nazivu člana 14. i u stavu 1. reči: „Nacionalni centar za prevenciju bezbednosnih rizika u IKT sistemima (u daljem tekstu: Nacionalni CERT)” zamenjuju se rečima: „Nacionalni CERT”.

Član 13.

Član 15. menja se i glasi:

„Delokrug Nacionalnog CERT-a

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, pruža podršku, upozorava i savetuje lica koja upravljaju IKT sistemima u Republici Srbiji, kao i javnost, a posebno:

1) prati stanje o incidentima na nacionalnom nivou;

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

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

4) kontinuirano izrađuje analize rizika i incidenata;

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

6) vodi evidenciju Posebnih CERT-ova;

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

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

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

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

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

U cilju obezbeđivanja kontinuiteta rada, Nacionalni CERT treba da:

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

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

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

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

Nacionalni CERT promoviše usvajanje i korišćenje propisanih i standardizovanih procedura za:

1) upravljanje i saniranje rizika i incidenata;

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

Član 14.

Posle člana 15. dodaje se član 15a, koji glasi:

„Saradnja CERT-ova u Republici Srbiji

Član 15a

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

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

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

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

Član 15.

Iznad člana 16. dodaje se naziv člana koji glasi: „Nadzor nad radom Nacionalnog CERT-a”.

Član 16.

U članu 17. stav 2. posle reči: „pravnog lica” dodaju se reči: „sa sedištem na teritoriji Republike Srbije”.

U stavu 4. posle reči: „pošte” dodaje se zapeta i reči: „a u svrhu angažovanja posebnih CERT-ova u slučaju bezbednosnih rizika i incidenata u IKT sistemima.”.

Stav 5. menja se i glasi:

„Nacionalni CERT propisuje sadržaj, način upisa i vođenja evidencije iz stava 3. ovog člana.”

Član 17.

Član 18. menja se i glasi:

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

„Član 18.

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

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

Poslovi CERT-a organa vlasti obuhvataju:

1) zaštitu Jedinstvene informaciono-komunikacione mreže elektronske uprave;

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

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

Član 18.

Iznad člana 19. dodaje se naziv člana koji glasi: „CERT samostalnog operatora IKT sistema”.

U stavu 2. reči: „republičkih organa” zamenjuju se rečima: „organa vlasti”.

Član 19.

Posle člana 19. dodaje se član 19a, koji glasi:

„Zaštita dece pri korišćenju informaciono-komunikacionih tehnologija

Član 19a

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

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

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

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

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

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

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

1) bude opremljen sa odgovarajućim sistemima za prijem prijava;

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

3) obezbedi infrastrukturu čiji je kontinuitet osiguran.

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

Član 20.

Člana 30. menja se i glasi:

„Član 30.

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

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

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

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

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

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

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

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

Član 21.

Član 31. menja se i glasi:

„Član 31.

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

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

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

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

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

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

Član 22.

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

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

Član 23.

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