ZAKON O INFORMACIONOJ BEZBEDNOSTI

("Sl. glasnik RS", br. 91/2025)

I OSNOVNE ODREDBE

Predmet uređivanja

Član 1

Ovim zakonom se uređuju mere zaštite od bezbednosnih rizika u informaciono-komunikacionim sistemima, odgovornosti subjekata prilikom upravljanja i korišćenja informaciono-komunikacionih sistema, postupci i mere za postizanje visokog opšteg nivoa informacione bezbednosti i određuju se nadležni organi za sprovođenje mera zaštite, koordinaciju između činilaca zaštite, praćenje pravilne primene propisanih mera zaštite, kao i nadležnosti subjekata za nadzor nad sprovođenjem ovog zakona.

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 i usluge* u smislu zakona koji uređuje elektronske komunikacije;

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

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

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

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

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

3) *informaciona bezbednost* predstavlja sposobnost informaciono- komunikacionih sistema i mreža da se odupru i/ili ublaže, uz određeni stepen pouzdanosti, svaki događaj koji bi mogao da ugrozi raspoloživost, integritet, autentičnost, neporecivost i poverljivost podataka koji se čuvaju, prenose ili obrađuju, kao i usluga koje se pružaju ili su dostupne putem tog IKT sistema;

4) *integritet* je svojstvo koje osigurava da podaci ili informacije nisu promenjeni ili uništeni na neovlašćeni način od kada su kreirani, preneti ili uskladišteni;

5) *raspoloživost* je svojstvo kojim se osigurava dostupnost i upotrebljivost IKT sistema na zahtev ovlašćenog subjekta ili procesa onda kada im je potreban;

6) *autentičnost* je svojstvo kojim se osigurava mogućnost da se proveri i potvrdi da je informaciju stvorio ili poslao onaj za koga se tvrdi da je tu radnju izvršio;

7) *poverljivost* je svojstvo kojim se osigurava da su informacije i funkcije IKT sistema dostupne samo ovlašćenim licima;

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* predstavlja mogućnost gubitka ili poremećaja izazvanog incidentom i izražava se kao kombinacija veličine takvog gubitka ili poremećaja i verovatnoće nastanka incidenta;

10) *ranjivost* predstavlja slabost ili nedostatak u IKT proizvodima ili uslugama koji se mogu iskoristiti za realizaciju jedne ili više pretnji;

11) *upravljanje rizikom* je skup sistematičnih aktivnosti identifikacije, procene i uspostavljanje sistema kontrole rizika koji omogućava planiranje, organizovanje i usmeravanje mera zaštite kako bi se obezbedilo da rizici ostanu u propisanim i prihvatljivim okvirima;

12) *izbegnuti incident* predstavlja identifikovani događaj u IKT sistemu koji je mogao dovesti do značajnog ugrožavanja raspoloživosti, autentičnosti, integriteta, neporecivosti ili poverljivosti podataka, usluga ili sistema, ali je pravovremenom intervencijom ili zaštitnim merama sprečeno ostvarivanje štetnih posledica;

13) *pretnja* predstavlja svaku okolnost, događaj ili radnju koja može da ugrozi, poremeti ili na drugi način štetno utiče na IKT sistem, korisnike sistema i druga lica sa jasnom verovatnoćom nastajanja štete u slučaju da izostane reakcija;

14) *ozbiljna pretnja* predstavlja pretnju po informacionu bezbednost za koju se, s obzirom na njena tehnička svojstva, može pretpostaviti da ima potencijal da izazove značajne negativne posledice po IKT sistem, njegovog operatora ili korisnike usluga tog operatora uzrokujući značajnu materijalnu ili nematerijalnu štetu;

15) *incident* je svaki događaj koji ugrožava raspoloživost, integritet, autentičnost, neporecivost ili poverljivost podataka koji se čuvaju, prenose ili obrađuju ili usluge koje se pružaju, odnosno koje su dostupne putem IKT sistema;

16) *zlonamerni softver* je softver namerno kreiran sa ciljem da ošteti, poremeti, onemogući ili neovlašćeno pristupi informaciono-komunikacionim sistemima i obuhvata različite tipove štetnih programa, uključujući viruse, trojance, crve, ransomver i špijunski softver;

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

18) *upravljanje incidentom* podrazumeva preduzimanje svih radnji i postupaka čiji je cilj sprečavanje, otkrivanje, analiza i prekid incidenta, kao i preduzimanje drugih mera radi odgovora na incident i otklanjanja njegovih posledica;

19) *kriza informacione bezbednosti* je događaj ili stanje koje ugrožava, ometa rad ili onemogućuje rad IKT sistema od posebnog značaja i pri tom izaziva rizike, pretnje ili posledice po stanovništvo, materijalna dobra ili životnu sredinu izuzetno velikog obima i intenziteta koje nije moguće sprečiti ili otkloniti redovnim delovanjem nadležnih organa i službi, a odgovor na takav događaj ili stanje zahteva učešće više nadležnih organa, kao i primenu odgovarajućih mera*;*

20) *mere zaštite IKT sistema* su tehničke, organizacione, administrativne i fizičke mere za upravljanje bezbednosnim rizicima IKT sistema;

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

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

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

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

25) *samostalni operatori IKT sistema* su ministarstvo nadležno za poslove odbrane, ministarstvo nadležno za unutrašnje poslove, ministarstvo nadležno za spoljne poslove, službe bezbednosti i Narodna banka Srbije;

26) Centar za prevenciju bezbednosnih rizika u IKT sistemima (u daljem tekstu: CERT*)* je funkcionalna celina u okviru organa ili pravnog lica koja obuhvata skup poslova koji se odnose na prevenciju i zaštitu od incidenata;

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

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

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

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

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

32) *bezbednosna zona* je prostor ili prostorija u kojoj se, u skladu sa propisima o tajnosti podataka, obrađuju i čuvaju tajni podaci, kao i prostor ili prostorija koja je od ključnog značaja za očuvanje informacione bezbednosti IKT sistema;

33) *informaciona dobra* obuhvataju informacije koje se obrađuju u skladu sa funkcijom i namenom IKT sistema; elektronske zapise o konfiguraciji uređaja i elektronske komunikacione mreže; elektronske zapise o interakcijama u IKT sistemima, pristupu i upotrebi IKT sistema (tzv. log zapise); programski kôd; tehničku i korisničku dokumentaciju; elektronske zapise o interakcijama u elektronskoj komunikacionoj mreži (tzv. mrežni saobraćaj); informacije kojima se regulišu namena i korišćenje IKT sistema, procesi, mere zaštite i sl.;

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

35) *pružalac usluge informacionog društva* je pravno lice koje je pružalac usluge u smislu zakona kojim se uređuje elektronska trgovina;

36) *mreža za isporuku sadržaja (Content Delivery Network - CDN)* označava mrežu geografski raspoređenih servera koja je osmišljena da obezbedi visoku dostupnost, pristupačnost i brzu isporuku digitalnog sadržaja i usluga korisnicima interneta, u ime pružalaca sadržaja i usluga;

37) *tačka za razmenu internet saobraćaja (engl. internet exchange point)* je mrežna struktura koja pruža mogućnost povezivanja dve ili više nezavisnih mreža (autonomnih sistema) prvenstveno u svrhu olakšavanja razmene internet saobraćaja, i koja omogućuje međupovezivanje autonomnih sistema, u kom slučaju nije potrebno da internet saobraćaj između autonomnih sistema prođe kroz treći autonomni sistem, te koja takav saobraćaj ne menja i ne utiče na njega na drugi način;

38) *sistem naziva domena (DNS)* je distribuirani, hijerarhijski organizovan sistem koji povezuje nazive domena sa odgovarajućim IP adresama koje se koriste za usmeravanje i povezivanje korisničkih uređaja sa uslugama i resursima na internetu;

39) *pružalac usluge DNS-a* je subjekat koji pruža usluge razrešavanja DNS upita korisnicima interneta ili pruža uslugu autoritativnih servera imena za nazive domena koje koriste treća lica, sa izuzetkom korenskih (engl. root) servera imena;

40) *usluga od poverenja* je usluga u smislu zakona kojim se uređuje elektronski dokument, elektronska identifikacija i usluge od poverenja u elektronskom poslovanju;

41) *pružalac usluge od poverenja* je pružalac u smislu zakona kojim se uređuje elektronski dokument, elektronska identifikacija i usluge od poverenja u elektronskom poslovanju;

42) *kvalifikovana usluga od poverenja* je usluga u smislu zakona kojim se uređuje elektronski dokument, elektronska identifikacija i usluge od poverenja u elektronskom poslovanju;

43) *pružalac kvalifikovane usluge od poverenja* je pružalac u smislu zakona kojim se uređuje elektronski dokument, elektronska identifikacija i usluge od poverenja u elektronskom poslovanju;

44*) usluge računarstva u klaudu (engl. "cloud computing service")* su digitalne usluge koje omogućavaju upravljanje na zahtev i široki daljinski pristup nadogradivom i elastičnom skupu deljivih računarskih resursa, uključujući i situacije kada su takvi resursi raspoređeni na nekoliko lokacija;

45) *usluga centra za upravljanje i čuvanje podataka* je usluga koja se pruža korišćenjem struktura ili grupa struktura namenjenih za centralizovano smeštanje, međupovezivanje i funkcionisanje računarske i mrežne opreme radi čuvanja, obrade i prenosa podataka, uključujući sve objekte i infrastrukturu za distribuciju električne energije i kontrolu uticaja na životnu sredinu;

46) *naučnoistraživačka organizacija* je organizacija u smislu zakona kojim se uređuju nauka i istraživanje;

47) *javna elektronska komunikaciona mreža* je elektronska komunikaciona mreža u smislu zakona kojim se uređuju elektronske komunikacije;

48) *elektronska komunikaciona usluga* je usluga u smislu zakona kojim se uređuju elektronske komunikacije;

49) *pružalac upravljanih usluga* je subjekt koji pruža usluge u vezi sa postavljanjem, upravljanjem, radom i održavanjem IKT proizvoda, mreža, infrastrukture, aplikacija ili druge mreže i informacionog sistema putem pružanja pomoći ili aktivnog upravljanja koje se sprovodi u prostorijama korisnika usluge ili na daljinu;

50) *pružalac upravljanih bezbednosnih usluga* je pružalac upravljanih usluga koji sprovodi ili pruža pomoć u sprovođenju aktivnosti u vezi sa upravljanjem rizikom u oblasti bezbednosti;

51) *registar naziva domena najvišeg nivoa (engl. TLD name registry)* označava subjekta kojem je dodeljen određeni domen najvišeg nivoa i koji je odgovoran za upravljanje domenom najvišeg nivoa, uključujući registraciju domena pod domenom najvišeg nivoa i tehničko funkcionisanje domena najvišeg nivoa, što obuhvata rad njegovih serverskih imena, održavanje baza podataka i distribuciju zona domena najvišeg nivoa preko serverskih imena, bez obzira na to da li se te aktivnosti obavljaju od strane samog subjekta ili su poverene trećim licima, osim u situacijama kada nazive domena najvišeg nivoa registar koristi isključivo za sopstvene potrebe;

52) *pružalac usluge registracije naziva domena* je registrator naziva domena ili drugi subjekt koji deluje u ime registratora ili za račun registratora;

53) *IKT proizvod* je element ili grupa elemenata u okviru informaciono-komunikacionog sistema;

54) *IKT usluga* je usluga koja se u potpunosti ili u većoj meri sastoji iz prenosa, čuvanja, preuzimanja ili obrade podataka korišćenjem IKT sistema;

55) *IKT proces* je skup aktivnosti koji se obavlja u cilju izrade, razvoja, korišćenja i održavanja IKT proizvoda ili IKT usluge;

56) *TLP (Traffic Light Protocol)* predstavlja standard za deljenje informacija u oblasti informacione bezbednosti, koji je uspostavljen u cilju obezbeđivanja efektivne saradnje i deljenja informacija od izvora informacije do jednog ili više primalaca. Protokol pruža jednostavnu i intuitivnu šemu od četiri oznake za upućivanje na to sa kim se potencijalno osetljive informacije mogu podeliti;

57) *podatak o ličnosti* je svaki podatak koji se odnosi na fizičko lice čiji je identitet određen ili odrediv, neposredno ili posredno, posebno na osnovu oznake identiteta, kao što je ime i identifikacioni broj, podataka o lokaciji, identifikatora u elektronskim komunikacionim mrežama ili jednog, odnosno više obeležja njegovog fizičkog, fiziološkog, genetskog, mentalnog, ekonomskog, kulturnog i društvenog identiteta;

58) *administrator* je lice koje je ovlašćeno i odgovorno za održavanje, upravljanje i obezbeđivanje funkcionalnosti i bezbednosti IKT sistema od posebnog značaja, u skladu sa odredbama ovog zakona i drugim važećim propisima.

59) *tehnička specifikacija* je dokument kojim se utvrđuju tehnički zahtevi koje treba da ispuni proizvod, proces ili usluga, u skladu sa zakonom kojim se uređuje standardizacija.

Termini koji se koriste u ovom zakonu i propisima koji se donose na osnovu njega, a koji imaju rodno značenje, izraženi u gramatičkom muškom rodu, podrazumevaju prirodni ženski i muški pol lica na koja se odnose.

Načela informacione bezbednosti

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;

5) načelo kontinuiranog poboljšanja - mere zaštite i upravljanja informacionom bezbednošću treba redovno procenjivati i unapređivati kako bi se osigurala njihova efikasnost i prilagodljivost novim pretnjama i tehnološkim promenama;

6) načelo ravnopravnosti i nediskriminacije - mere zaštite IKT sistema moraju se sprovoditi na način koji osigurava jednak tretman svih korisnika, bez diskriminacije po bilo kom osnovu, u skladu sa zakonom.

Obrada podataka o ličnosti

Član 4

Na obradu podataka o ličnosti koja je neophodna za vršenje nadležnosti i ispunjenje obaveza iz ovog zakona primenjuju se odredbe ovog zakona, odredbe posebnih zakona kojima se uređuju određene oblasti, kao i odredbe zakona kojim se uređuje zaštita podataka o ličnosti.

II BEZBEDNOST IKT SISTEMA OD POSEBNOG ZNAČAJA

IKT sistemi od posebnog značaja

Član 5

IKT sistemi od posebnog značaja su IKT sistemi koji su od ključnog značaja za održavanje kritičnih društvenih i ekonomskih aktivnosti čiji bi prekid ili poremećaj u pružanju usluga imao ili

mogao da ima značajan uticaj na javnu bezbednost, javno zdravlje, funkcionisanje drugih sektora ili bi stvorio odnosno mogao da stvori značajan sistemski rizik.

IKT sistemi od posebnog značaja su:

1) prioritetni IKT sistemi;

2) važni IKT sistemi.

Operatori prioritetnih IKT sistema su:

1) pravna lica i fizička lica u svojstvu registrovanog subjekta, koja obavljaju poslove i delatnosti u sledećim oblastima:

(1) Energetika i rudarstvo

- proizvodnja električne energije, izuzev proizvodnje koju obavljaju krajnji kupci u smislu zakona kojim se uređuje korišćenje obnovljivih izvora energije i zakona kojim se uređuje energetika;

- kombinovana proizvodnja električne i toplotne energije;

- snabdevanje električnom energijom;

- prenos električne energije i upravljanje prenosnim sistemom;

- distribucija električne energije i upravljanje distributivnim sistemom, kao i distribucija električne energije i upravljanje zatvorenim distributivnim sistemom;

- skladištenje električne energije, izuzev skladištenja koje obavljaju krajnji kupci u smislu zakona kojim se uređuje korišćenje obnovljivih izvora energije i zakona kojim se uređuje energetika;

- upravljanje organizovanim tržištem električne energije;

- proizvodnja, distribucija i snabdevanje toplotnom energijom;

- transport nafte naftovodima, transport derivata nafte produktovodima i transport nafte i derivata nafte drugim oblicima transporta;

- istraživanje i proizvodnja nafte i prirodnog gasa;

- proizvodnja derivata nafte;

- skladištenje nafte i derivata nafte;

- transport i upravljanje transportnim sistemom za prirodni gas;

- skladištenje i upravljanje skladištem prirodnog gasa;

- distribucija i upravljanje distributivnim sistemom za prirodni gas;

- snabdevanje i javno snabdevanje prirodnim gasom;

- proizvodnja i prerada uglja;

- proizvodnja i prerada bakra, zlata, olova, cinka, litijuma i bora;

- proizvodnja, skladištenje i prenos vodonika;

(2) Saobraćaj

- obavljanje javnog avio-prevoza uz važeću operativnu dozvolu;

- upravljanje aerodromom;

- usluge kontrole letenja;

- upravljanje javnom železničkom infrastrukturom;

- poslovi železničkih preduzeća;

- obavljanje prevoza putnika i tereta unutrašnjim vodama;

- upravljanje lukama;

- servis za upravljanje brodskim saobraćajem (VTS);

- rečni informacioni servisi (RIS);

- upravljanje putnom infrastrukturom;

- upravljanje inteligentnim transportnim sistemima (ITS);

(3) Bankarstvo i finansijska tržišta

- poslovi finansijskih institucija i institucija tržišta kapitala, koje su pod nadzorom Narodne banke Srbije odnosno Komisije za hartije od vrednosti;

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

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

- poslovi kliringa odnosno saldiranja finansijskih instrumenata, u smislu zakona kojim se uređuje tržište kapitala;

- poslovi pružalaca usluga povezanih s digitalnom imovinom, u smislu zakona kojima se uređuje digitalna imovina;

(4) Zdravstvo

- pružanje zdravstvene zaštite;

- rad nacionalnih referentnih laboratorija;

- istraživanje i razvoj lekova;

- proizvodnja farmaceutskih lekova i preparata namenjenih za zdravstvenu upotrebu;

- proizvodnja lekova i drugih proizvoda namenjenih upotrebi u zdravstvu, uključujući proizvode koji su od vitalnog značaja tokom vanrednog stanja u oblasti javnog zdravlja;

- obrada genetskih, biomedicinskih podataka i drugih podatka od značaja za istraživanje i razvoj u oblasti biotehnologije, bioinformatike, bioekonomije, genetike i medicine;

(5) Voda za piće

- snabdevanje i distribucija vode namenjene za ljudsku potrošnju, izuzev distributera kojima navedeni poslovi nisu pretežni deo njihove delatnosti;

(6) Otpadne vode

- sakupljanje, odvođenje ili prečišćavanje komunalnih otpadnih voda, otpadnih voda naselja i privrede, izuzev privrednih subjekata kojima navedeni poslovi nisu pretežni deo njihove delatnosti;

(7) Digitalna infrastruktura

- pružanje usluga računarstva u klaudu;

- pružanje usluge centra za čuvanje i skladištenje podataka;

(8) Upravljanje IKT uslugama koje se pružaju operatorima prioritetnih IKT sistema

- pružanje upravljanih usluga;

- pružanje upravljanih bezbednosnih usluga;

(9) Ostale oblasti

- upravljanje nuklearnim objektima;

- pružanje usluga od poverenja, uključujući kvalifikovane usluge od povrenja, pružanje usluga sistema domena (DNS), upravljanje registrom domena najvišeg nivoa i pružanje usluga registracije domena sa izuzetkom operatora korenskih servera imena;

- pružanje usluga mreže za isporuku sadržaja;

- obavljanje delatnosti elektronskih komunikacija;

- tačka za razmenu internet saobraćaja;

- izdavanje Službenog glasnika Republike Srbije i vođenje Pravno-informacionog sistema Republike Srbije;

- oblasti u kojoj u Republici Srbiji postoji samo jedan pružalac usluge i koja je neophodna za obavljanje kritičnih društvenih i privrednih delatnosti;

2) organi;

3) subjekti koji su određeni kao operatori kritične infrastrukture u skladu sa propisima kojima se uređuje kritična infrastruktura.

Pored subjekata iz stava 3. ovog člana, kao operatori prioritetnih IKT sistema mogu se odrediti subjekti kod kojih prekid rada IKT sistema ili poremećaj u radu IKT sistema:

1) može imati značajan uticaj na javnu bezbednost, nacionalnu bezbednost ili javno zdravlje;

2) može izazvati značajan sistemski rizik, a posebno u sektorima gde poremećaj može imati prekogranični uticaj.

Subjekte iz stava 4. ovog člana određuje ministarstvo nadležno za poslove informacione bezbednosti, a po pribavljenom mišljenju organa u čijoj je nadležnosti oblast u kojoj subjekt obavlja delatnosti.

Na operatore prioritetnih IKT sistema od posebnog značaja koji obavljaju delatnost u sektoru bankarstva i finansijskih tržišta iz stava 3. tačka 1) podtačka (3) alineje prva, druga i peta ovog člana primenjuju se posebni, sektorski propisi kojima se bliže, odnosno na drukčiji način uređuju pojedina pitanja iz ovog zakona, a kojima se obezbeđuje najmanje isti nivo delotvornosti mera upravljanja bezbednosnim rizicima tih operatora shodno merama iz člana 10. ovog zakona, pri čemu se obezbeđuje i izveštavanje o incidentima koji predstavljaju krizu informacione bezbednosti u skladu sa ovim zakonom.

Narodna banka Srbije, kao nadležni nadzorni organ nad poslovanjem operatora prioritetnih IKT sistema od posebnog značaja koji obavljaju delatnost u sektoru bankarstva i finansijskih tržišta iz stava 3. tačka 1) podtačka (3) alineje prva, druga i peta ovog člana (subjekti nadzora Narodne banke Srbije), u skladu sa ovim zakonom i odredbama posebnih zakona kojima se uređuje poslovanje tih subjekata donosi propise kojima se uređuju pitanja informacione bezbednosti za te subjekte, i to mere zaštite IKT sistema, donošenje akata o proceni rizika i akta o bezbednosti IKT sistema, klasifikacija incidenata, dostavljanje obaveštenja o incidentu, postupanje u vezi sa incidentima, izveštavanje tokom i nakon incidenta, dostavljanje statističkih podataka o incidentu i druga pitanja od značaja za bezbednost informacionog sistema ovih subjekata, kao i nadzora koji vrši nad njima.

Operatori važnih IKT sistema

Član 6

Operatori važnih IKT sistema su:

1) pravna lica i fizička lica u svojstvu registrovanog subjekta, koja obavljaju poslove i delatnosti u sledećim oblastima:

- poštanske usluge u smislu zakona kojim se uređuje oblast poštanskih usluga;

- upravljanje otpadom, u smislu zakona kojim se uređuje upravljanje otpadom, izuzev privrednih subjekata kojima navedeni posao nije pretežni deo njihove delatnosti;

- upravljanje ambalažnim otpadom, u smislu zakona kojim se uređuje upravljanje ambalažnim otpadom;

- proizvodnja i snabdevanje hemikalijama, u skladu sa zakonom kojim se uređuju hemikalije;

- proizvodnja, prerada i distribucija hrane u segmentu veleprodaje i industrijske proizvodnje i prerade;

- proizvodnja računara, elektronskih i optičkih proizvoda;

- proizvodnja električne opreme;

- proizvodnja mašina i uređaja;

- proizvodnja motornih vozila, prikolica i poluprikolica i proizvodnja ostale opreme za prevoz;

- proizvodnja medicinskih uređaja i proizvodnja in vitro dijagnostičkih medicinskih sredstava;

- usluge informacionog društva u smislu zakona o elektronskoj trgovini;

- proizvodnja, promet i prevoz naoružanja i vojne opreme;

- svemirske usluge koje se oslanjaju na zemaljsku infrastrukturu, naročito aktivnosti upravljanja kontrolnim centrima, objektima za praćenje i komunikaciju i pružanje usluga lansiranja;

2) naučnoistraživačke institucije;

3) pravna i fizička lica u svojstvu registrovanog subjekta i organi iz člana 5. ovog zakona, a koji ne spadaju u operatore prioritetnih IKT sistema prema kriterijumima za određivanje operatora.

Pored subjekata iz stava 1. ovog člana, kao operatori važnih IKT sistema mogu se odrediti subjekti kod kojih prekid rada IKT sistema ili poremećaj u radu IKT sistema:

1) može imati značajan uticaj na javnu bezbednost, nacionalnu bezbednost ili javno zdravlje;

2) može izazvati značajan sistemski rizik, a posebno u sektorima gde poremećaj može imati prekogranični uticaj.

Subjekte iz stava 2. ovog člana određuje ministarstvo nadležno za poslove informacione bezbednosti, a po pribavljenom mišljenju organa u čijoj je nadležnosti oblast u kojoj subjekt obavlja delatnosti.

Podzakonski akt kojim se bliže uređuju uslovi, opšti i sektorski kriterijumi uključujući i kriterijume u pogledu veličine privrednih subjekata, za određivanje operatora prioritetnih i važnih IKT sistema donosi Vlada, na predlog ministarstva nadležnog za poslove informacione bezbednosti.

Ministarstva u čijim nadležnostima su oblasti u kojima operatori prioritetnih i važnih IKT sistema obavljaju delatnosti i Narodna banka Srbije, dužni su da u postupku izrade podzakonskog akta iz stava 4. ovog člana, dostave ministarstvu nadležnom za poslove informacione bezbednosti predloge sektorskih kriterijuma radi određivanja operatora IKT sistema od posebnog značaja.

Obaveze operatora IKT sistema od posebnog značaja

Član 7

Operator IKT sistema od posebnog značaja, shodno ovom zakonu, u obavezi je da:

1) podnese prijavu za upis u evidenciju IKT sistema od posebnog značaja;

2) preduzme odgovarajuće tehničke, operativne, organizacione i fizičke mere zaštite IKT sistema od posebnog značaja, upravljanje rizicima i prevenciju i smanjenje štetnih posledica incidenata;

3) izvrši procenu rizika i donese akt o proceni rizika;

4) donese akt o bezbednosti IKT sistema od posebnog značaja;

5) vrši proveru usklađenosti mera zaštite IKT sistema koje se primenjuju sa aktom o bezbednosti IKT sistema i to najmanje jednom godišnje;

6) 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;

7) dostavlja obaveštenja, bez odlaganja, o svakom incidentu koji značajno narušava bezbednost IKT sistema od posebnog značaja;

8) prijavi izbegnute incidente koji predstavljaju ozbiljnu pretnju u skladu sa ovim zakonom;

9) dostavlja statističke podatke o incidentima i izbegnutim incidentima u IKT sistemima.

Obaveze samostalnih operatora

Član 8

Samostalni operator dužan je da:

1) podnese prijavu za upis u evidenciju IKT sistema od posebnog značaja;

2) preduzme odgovarajuće tehničke, operativne, organizacione i fizičke mere zaštite IKT sistema od posebnog značaja, upravljanje rizicima i prevenciju i smanjenje štetnih posledica incidenata;

3) donese akt o bezbednosti IKT sistema;

4) vrši proveru usklađenosti mera zaštite IKT sistema koje se primenjuju sa aktom o bezbednosti IKT sistema u skladu sa sopstvenim pravilima za proveru usklađenosti mera zaštite, a 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 sa trećim licima;

6) formira sopstveni CERT radi upravljanja incidentima u svojim sistemima.

Samostalni operatori mogu da međusobno razmenjuju informacije o incidentima sa Kancelarijom za informacionu bezbednost, a po potrebi i sa drugim organizacijama.

Na samostalne operatore ne primenjuju se odredbe ovog zakona o prijavljivanju incidenata koji značajno ugrožavaju informacionu bezbednost, odredbe o dostavljanju statističkih podataka o incidentima i odredbe o proaktivnom skeniranju mreže operatora IKT sistema od posebnog značaja.

Samostalni operatori, mogu samostalno i u koordinaciji sa Kancelarijom za informacionu bezbednost, radi otkrivanja ranjivosti da vrše proaktivno skeniranje sopstvenih IKT sistema povezanih na Jedinstvenu informaciono-komunikacionu mrežu elektronske uprave.

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.

Evidencija operatora IKT sistema od posebnog značaja

Član 9

Ministarstvo nadležno za poslove informacione bezbednosti (u daljem tekstu: Ministarstvo) uspostavlja i vodi evidenciju prioritetnih i važnih IKT sistema (u daljem tekstu: Evidencija) koja sadrži:

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

2) ime i prezime, službenu adresu za prijem elektronske pošte i službeni kontakt telefon administratora zaduženog za održavanje i upravljanje IKT sistemom od posebnog značaja;

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

4) podatak o vrsti IKT sistema od posebnog značaja, odnosno da li IKT sistem od posebnog značaja potpada pod prioritetan ili važan;

5) podatak o delatnosti operatora IKT sistema od posebnog značaja;

6) adresni opseg internet protokola (engl. "IP address range") koji pripadaju IKT sistemu od posebnog značaja, a koji obuhvata podatke o javnim statičkim IP adresama;

7) veb prezentaciju operatora IKT sistema od posebnog značaja;

8) broj lokacija na kojima se IKT sistem od posebnog značaja nalazi.

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

Samostalni operatori IKT sistema izuzeti su od obaveze dostavljanja podataka iz stava 1. tač. 4), 5), 6) i 8) ovog člana.

Podzakonski akt kojim se bliže uređuje sadržaj i struktura evidencije, kao i način podnošenja zahteva za unos i promenu podataka u Evidenciji donosi Ministarstvo.

Operator IKT sistema od posebnog značaja dužan je da Ministarstvu dostavi podatke iz st. 1. i 2. ovog člana najkasnije 90 dana od dana usvajanja propisa iz stava 4. ovog člana, odnosno 90 dana od dana uspostavljanja IKT sistema od posebnog značaja.

Operator IKT sistema od posebnog značaja dužan je da u slučaju promene podataka iz stava 1. ovog člana o tome obavesti Ministarstvo u roku od 15 dana od dana nastanka promene.

Podaci iz stava 1. tač. 2) i 3) ovog člana obrađuju se u svrhu izvršenja odredbi ovog zakona u pogledu dostavljanja obaveštenja i upozorenja značajnih za bezbednost IKT sistema od posebnog značaja, kao i radi uspostavljanja komunikacije i ostvarivanja saradnje u cilju otklanjanja štetnih posledica incidenata i preventivnog delovanja.

Podaci iz stava 1. tač. 2) i 3) ovog člana obrađuju se u skladu sa zakonom kojim se uređuje zaštita podataka o ličnosti i čuvaju se do trenutka prestanka svrhe obrade ili do izvršene promene podataka u skladu sa stavom 6. ovog člana.

Ministarstvo stavlja na raspolaganje ažurnu Evidenciju Kancelariji za informacionu bezbednost radi izvršenja odredbi ovog zakona u pogledu prikupljanja i razmene informacija o pretnjama, ranjivostima i incidentima i pružanja podrške, upozoravanja i savetovanja lica koja upravljaju IKT sistemima.

Evidencija predstavlja tajni podatak u smislu zakona kojim se uređuje tajnost podataka.

Mere zaštite IKT sistema od posebnog značaja

Član 10

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 smanjenje štete od incidenata koji ugrožavaju vršenje nadležnosti i obavljanje delatnosti, a posebno u okviru pružanja usluga drugim licima.

Mere zaštite primenjuju se u svim IKT sistemima operatora iz stava 1. ovog člana.

Mere zaštite IKT sistema se odnose na:

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

2) prikupljanje podataka o pretnjama po informacionu bezbednost IKT sistema;

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

4) obezbeđivanje da lica koja koriste IKT sistem odnosno upravljaju IKT sistemom budu osposobljena za posao koji rade i razumeju svoju odgovornost, odnosno da obezbedi održavanje osnovnih i po potrebi naprednih informatičkih obuka za sve zaposlene i angažovana lica koja imaju pristup IKT sistemima, obuka za rukovodioce odnosno organe upravljanja operatora IKT sistema od posebnog značaja, kao i specijalizovane stručne obuke za zaposlene odgovorne za upravljanje informacionom bezbednošću, radi obezbeđivanja kontinuirane edukacije;

5) obezbeđivanje dovoljno resursa za adekvatno upravljanje informacionom bezbednošću;

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

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

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

9) zaštitu nosača podataka;

10) ograničenje pristupa podacima i sredstvima za obradu podataka;

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

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

13) predviđanje upotrebe kriptografskih kontrola i drugih tehnika za sakrivanje podataka radi zaštite poverljivosti, autentičnosti i integriteta podataka;

14) primena mera zaštite radi sprečavanja oticanja podataka;

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

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

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

18) primenu odgovarajućih procedura i mera zaštite prilikom korišćenja usluge računarstva u klaudu;

19) praćenje IKT sistema u cilju otkrivanja ranjivosti i pretnji;

20) ograničenje pristupa veb prezentacijama koje mogu potencijalno da naruše bezbednost IKT sistema;

21) zaštitu podataka i sredstava za obradu podataka od zlonamernog softvera;

22) zaštitu od gubitka podataka redovnom izradom rezervnih kopija podataka, softvera i sistema putem odgovarajućih sredstava za razmenu podataka;

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

24) obezbeđivanje integriteta softvera i operativnih sistema;

25) zaštitu od zloupotrebe tehničkih bezbednosnih slabosti IKT sistema;

26) obezbeđivanje zaštite IKT sistema prilikom sprovođenja revizorskog testiranja;

27) zaštitu podataka u komunikacionim mrežama, uključujući uređaje i vodove;

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

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

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

31) procedure za čuvanje i brisanje informacija u IKT sistemima, u skladu sa propisima;

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

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

34) prevenciju i reagovanje na bezbednosne incidente, što podrazumeva adekvatnu razmenu informacija o bezbednosnim slabostima IKT sistema, incidentima i pretnjama, kao i primenu mera sanacije posledica incidenta;

35) mere koje obezbeđuju kontinuitet obavljanja posla u vanrednim okolnostima koje se definišu Planom kontinuiteta obavljanja posla;

36) usvajanje dokumenata kojima se definišu procedure za proveru adekvatnosti mera zaštite;

37) upotrebu multifaktorske autentikacije ili rešenja kontinuirane provere autentičnosti, zaštićene glasovne, video i tekstualne komunikacije, te bezbednih komunikacionih sistema u hitnim slučajevima unutar operatora IKT sistema.

Podzakonski akt kojim se bliže uređuju mere zaštite prioritetnih i važnih IKT sistema uvažavajući načela iz člana 3. ovog zakona, nacionalne i međunarodne standarde, i standarde koji se primenjuju u odgovarajućim oblastima rada i relevantne tehničke specifikacije donosi Vlada, na predlog Ministarstva.

Akt o proceni rizika IKT sistema od posebnog značaja

Član 11

Operator IKT sistema od posebnog značaja dužan je da donese akt o proceni rizika za IKT sisteme (u daljem tekstu: akt o proceni rizika) kojima upravlja.

Aktom o proceni rizika vrši se procena rizika za IKT sistem od posebnog značaja s obzirom na stepen izloženosti riziku, veličinu operatora i izvesnost pojave incidenta i njegove ozbiljnosti, kao i njegov potencijalni društveni i ekonomski uticaj.

Akt o proceni rizika revidira se najmanje jednom godišnje.

Akt o proceni rizika izrađuje se u skladu sa opštom metodologijom za procenu rizika u prioritetnim i važnim IKT sistemima od posebnog značaja koju donosi organ, odnosno organizacija u kojoj se obavljaju poslovi Nacionalnog CERT-a.

Operator IKT sistema od posebnog značaja nije u obavezi da donese akt iz stava 1. ovog člana u slučaju kada ima definisanu procenu rizika u drugim postojećim internim aktima, koja obuhvata zahteve iz opšte metodologije iz stava 4. ovog člana.

Akt o bezbednosti IKT sistema od posebnog značaja

Član 12

Operator IKT sistema od posebnog značaja dužan je da donese akt o bezbednosti IKT sistema (u daljem tekstu: akt o bezbednosti).

Aktom o bezbednosti 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 o bezbednosti IKT sistema od posebnog značaja zasniva se na Aktu o proceni rizika iz člana 11. ovog zakona. Primena mera zaštite IKT sistema mora biti u skladu sa procenjenim rizicima, kako bi se obezbedila adekvatna zaštita sistema i minimizirao uticaj potencijalnih incidenata.

Akt o bezbednosti mora da bude usklađen s promenama u okruženju i u samom IKT sistemu.

Operator IKT sistema od posebnog značaja dužan je da, samostalno ili uz angažovanje spoljnih eksperata, vrši proveru iz prethodnog stava najmanje jednom godišnje i da o tome sačini izveštaj.

Podzakonski akt kojim se bliže uređuje sadržaj akta o bezbednosti, način provere IKT sistema od posebnog značaja i sadržaj izveštaja o proveri, kao i dostavljanje izveštaja nadležnom organu, donosi Vlada na predlog Ministarstva.

Obaveza obaveštavanja o incidentima koji značajno narušavaju informacionu bezbednost

Član 13

Operatori IKT sistema od posebnog značaja dužni su da dostave obaveštenje o incidentu koji može da ima značajan uticaj na narušavanje informacione bezbednosti, bez odlaganja, a najkasnije u roku od 24 sata od kada su saznali za incident.

Incidenti koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti su:

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

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

3) incidenti 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) incidenti koji dovode do prekida kontinuiteta, odnosno teškoća u vršenju poslova i pružanju usluga i imaju uticaj na veći deo teritorije Republike Srbije;

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

6) incidenti koji su nastali kao posledica incidenta u IKT sistemu operatora prioritetnih IKT sistema koji obavljaju delatnosti u oblasti digitalne infrastrukture, iz člana 5. stav 3. tačka 1) podtačka (7) ovog zakona, kada IKT sistem od posebnog značaja u svom poslovanju koristi informacione usluge u oblasti digitalne infrastrukture;

7) incidenti koji izazivaju ili mogu da izazovu znatnu materijalnu ili nematerijalnu štetu operatoru IKT sistema od posebnog značaja i drugim fizičkim i pravnim licima.

Operatori IKT sistema od posebnog značaja dužni su da prijave i izbegnute incidente koji predstavljaju ozbiljnu pretnju i koji bi mogli dovesti do okolnosti sličnih onima opisanim u stavu 2. ovog člana. 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.

Dostavljanje obaveštenja o incidentima

Član 14

Operatori IKT sistema od posebnog značaja dužni su da obaveštenja o incidentima dostave u jedinstveni sistem za prijem obaveštenja o incidentima putem veb prezentacije Ministarstva ili Kancelarije za informacionu bezbednost.

Operatori prioritetnih IKT sistema od posebnog značaja koji obavljaju delatnosti u oblasti bankarstva i finansijskih tržišta iz člana 5. stav 3. tačka 1) podtačka (3) ovog zakona dužni su da obaveštenje o incidentu dostave Narodnoj banci Srbije, a ako su operatori prioritetnih IKT sistema u oblasti finansijskih tržišta koji su pod nadzorom Komisije za hartije od vrednosti, obaveštenje dostavljaju i Komisiji za hartije od vrednosti.

Operatori prioritetnih IKT sistema koji obavljaju delatnosti elektronskih komunikacija iz člana 5. stav 3. tačka 1) podtačka (9) alineja četvrta ovog zakona i operatori važnih IKT sistema od posebnog značaja koji obavljaju delatnost poštanskih usluga iz člana 6. stav 1. tačka 1) alineja prva ovog zakona, dužni su da obaveštenje o incidentu dostave Regulatornom telu za elektronske komunikacije i poštanske usluge.

Narodna banka Srbije, Regulatorno telo za elektronske komunikacije i poštanske usluge i Komisija za hartije od vrednosti dužni su da dobijena obaveštenja iz st. 2. i 3. ovog člana proslede u jedinstveni sistem za prijem obaveštenja o incidentima.

Operatori IKT sistema od posebnog značaja, osim operatora IKT sistema iz st. 2. i 3. ovog člana, dužni su da putem odgovarajućih kanala komunikacije obaveste o incidentu korisnike kojima pružaju usluge, bez odlaganja, u slučaju incidenta koji može da izazove ili izaziva štetan uticaj na pružanje i korišćenje usluga, kao i o merama koje korisnici mogu da preduzmu i upotrebe u cilju umanjenja ili eliminacije štetnih posledica incidenta.

Operatori IKT sistema od posebnog značaja iz st. 2. i 3. ovog člana obaveštavaju korisnike o incidentima u skladu sa posebnim propisima.

Organ kome je u skladu sa ovim zakonom upućeno obaveštenje o incidentu, ukoliko je reč o IKT sistemu od posebnog značaja koji je određen kao kritična infrastruktura u skladu sa zakonom kojim se uređuje kritična infrastruktura, informaciju o tome prosleđuje ministarstvima nadležnim za sektore kritične infrastrukture.

Organi iz st. 1-3. ovog člana, kojima je upućeno obaveštenje o incidentu, dužni su da, u slučaju incidenta koji je nastao u IKT sistemu operatora kritične infrastrukture utvrđenog u skladu sa zakonom kojim se uređuje kritična infrastruktura, dobijenu informaciju bez odlaganja proslede nadležnim ministarstvima za sektore kritične infrastrukture, u skladu sa propisima o zaštiti tajnih podataka.

Sadržaj obaveštenja o incidentu

Član 15

Obaveštenje o incidentu mora da sadrži sledeće podatke:

1) podatke o podnosiocu prijave;

2) vrstu i opis incidenta i procenu da li je incident posledica krivičnog dela;

3) datum i vreme početka incidenta, odnosno saznanja o incidentu i trajanje incidenta;

4) posledice koje je incident izazvao;

5) preduzete aktivnosti radi ublažavanja posledica incidenta;

6) inicijalnu procenu nivoa opasnosti i uticaja incidenta na IKT sistem od posebnog značaja, kao i indikatore kompromitacije;

7) informaciju o eventualnom prekograničnom dejstvu incidenta;

8) podatke o prethodno prijavljenim sličnim incidentima, ako su postojali, uključujući vreme i prirodu tih incidenata, kao i mere koje su tom prilikom preduzete;

9) druge relevantne informacije, po potrebi.

Značaj incidenata prema nivou opasnosti

Član 16

Incidenti u IKT sistemima od posebnog značaja koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti svrstavaju se prema nivou opasnosti, imajući u vidu posledice incidenta, u sledeće nivoe opasnosti:

1) nizak;

2) srednji;

3) visok;

4) veoma visok.

Podzakonski akt kojim se uređuje postupak obaveštavanja o incidentima, obrasci za obaveštavanje, lista incidenata prema vrstama i klasifikacija incidenata prema nivou opasnosti donosi Vlada, na predlog Ministarstva.

Operativni tim za reagovanje na incidente

Član 17

U cilju koordinisane reakcije na incidente visokog i veoma visokog nivoa Kancelarija za informacionu bezbednost obrazuje stalni operativni tim.

Kancelarija za informacionu bezbednost bliže uređuje kriterijume za imenovanje članova, kao i vršenje poslova i zadatke stalnog operativnog tima.

Kancelarija za informacionu bezbednost može da, zavisno od prirode i posledica incidenta, zatraži uključivanje drugih organa u rad operativnog tima u okviru njihovih nadležnosti.

Po potrebi, sastancima operativnog tima mogu prisustvovati i predstavnici samostalnih operatora, lica uključena u rad Tela za koordinaciju poslova informacione bezbednosti, kao i predstavnici posebnih CERT-ova.

Lica koja učestvuju u radu stalnog operativnog tima dužna su da se sertifikuju za rad sa tajnim podacima.

Plan za reagovanje u slučaju incidenta visokog nivoa i kriza informacione bezbednosti

Član 18

Vlada donosi Plan za reagovanje u slučaju incidenta visokog nivoa i krize informacione bezbednosti, na predlog Kancelarije za informacionu bezbednost.

Plan iz stava 1. ovog člana obuhvata:

1) ciljeve mera i aktivnosti za reagovanje u slučaju incidenata visokog nivoa i kriza informacione bezbednosti;

2) delovanje nadležnih organa u cilju sprovođenja plana;

3) opis procedura u slučaju incidenata visokog nivoa i kriza informacione bezbednosti;

4) aktivnosti za unapređenje sposobnosti reagovanja na incidente, a pre svega planove odgovarajućih vežbi i obuka;

5) modele saradnje sa privatnim, nevladinim i akademskim sektorom;

6) međusobnu saradnju nadležnih organa.

Prilikom izrade plana iz stava 1. ovog člana uspostavlja se saradnja sa organima i pravnim licima čije su nadležnosti, odnosno poslovi i delatnosti povezani sa planiranim aktivnostima.

Plan iz stava 1. ovog člana se periodično menja i dopunjuje u skladu sa potrebama i novim okolnostima, a u celini se ponovo izrađuje i donosi svake treće godine, a ukoliko su se okolnosti u značajnoj meri promenile i ranije.

Postupanje po prijemu obaveštenja o incidentu

Član 19

Po prijemu obaveštenja o incidentu u IKT sistemu od posebnog značaja, Kancelarija za informacionu bezbednost postupa u skladu sa nadležnostima utvrđenim zakonom, odnosno prikuplja, analizira i razmenjuje informacije o rizicima za bezbednost IKT sistema, kao i incidentu, i u vezi sa tim obaveštava, pruža podršku, upozorava i savetuje operatora IKT sistema od posebnog značaja i vrši druge poslove iz svoje nadležnosti.

Kancelarija za informacionu bezbednost, nakon izvršene analize, utvrđuje nivo opasnosti incidenta.

Kada je neophodno da javnost bude upoznata sa incidentom ili kada je incident takav da je od interesa za javnost, Kancelarija za informacionu bezbednost objavljuje informaciju o incidentu, nakon savetovanja sa operatorom IKT sistema od posebnog značaja u kome se incident dogodio.

Izuzetno od stava 3. ovog člana, Kancelarija za informacionu bezbednost može objaviti informaciju o incidentu koji se dogodio u operatoru prioritetnog IKT sistema od posebnog značaja koji obavlja delatnost u oblasti bankarstva i finansijskih tržišta iz člana 5. stav 3. tačka 1) podtačka (3) ovog zakona, uz prethodno pribavljenu saglasnost Narodne banke Srbije odnosno Komisije za hartije od vrednosti.

Kancelarija za informacionu bezbednost, Narodna banka Srbije, Komisija za hartije od vrednosti i Regulatorno telo za elektronske komunikacije i poštanske usluge dužni su da obaveštenja o incidentima proslede:

1) nadležnom javnom tužilaštvu, odnosno ministarstvu nadležnom za unutrašnje poslove, u slučaju da je incident vezan za izvršenje krivičnih dela koja se gone po službenoj dužnosti,

2) organu nadležnom za bezbednosne i kontraobaveštajne poslove od značaja za odbranu Republike Srbije ili organu nadležnom za poslove nacionalne bezbednosti, u slučaju da je incident povezan sa značajnim narušavanjem informacione bezbednosti koje ima ili može imati za posledicu ugrožavanje odbrane ili nacionalne bezbednosti Republike Srbije.

Prilikom upravljanja incidentom Kancelarija za informacionu bezbednost, Narodna banka Srbije, Komisija za hartije od vrednosti i Regulatorno telo za elektronske komunikacije i poštanske usluge označavaju obaveštenje o incidentu, odnosno informacije o incidentu u skladu sa propisima i TLP (eng. "traffic light protocol") protokolom.

Postupanje u slučaju incidenta nivoa opasnosti "nizak"

Član 20

U slučaju incidenata kojima je u skladu sa klasifikacijom utvrđen nivo opasnosti "nizak" Kancelarija za informacionu bezbednost po potrebi daje preporuke za postupanje operatoru IKT sistema od posebnog značaja.

Postupanje u slučaju incidenta nivoa opasnosti "srednji"

Član 21

U slučaju incidenata kojima je u skladu sa klasifikacijom utvrđen nivo opasnosti "srednji" Kancelarija za informacionu bezbednost daje preporuke za postupanje operatoru IKT sistema od posebnog značaja.

Postupanje u slučaju incidenta nivoa opasnosti "visok"

Član 22

U slučaju incidenata kojima je u skladu sa klasifikacijom utvrđen nivo opasnosti "visok" Kancelarija za informacionu bezbednost je dužna da o tome obavesti Ministarstvo.

Kancelarija za informacionu bezbednost, u saradnji sa operativnim timom, priprema preporuke i mere za rešavanje incidenta.

Ministarstvo nakon prijema obaveštenja iz stava 1. ovog člana saziva sednicu Tela za koordinaciju poslova informacione bezbednosti.

Nakon završetka incidenta Kancelarija za informacionu bezbednost, u saradnji sa operativnim timom, sačinjava završni izveštaj koji dostavlja Ministarstvu u roku od 30 dana nakon završenog incidenta.

Postupanje u slučaju incidenta nivoa opasnosti "veoma visok"

Član 23

U slučaju incidenta kojem je u skladu sa klasifikacijom utvrđen nivo opasnosti "veoma visok" i koji predstavlja krizu informacione bezbednosti, rukovođenje i koordinaciju sprovođenja mera i zadataka preduzima Vlada.

Kancelarija za informacionu bezbednost, u saradnji sa operativnim timom, izrađuje predlog za proglašavanje krize informacione bezbednosti, u skladu sa Planom za reagovanje u slučaju incidenta visokog nivoa i krize informacione bezbednosti, koji sadrži:

1) podatke o incidentu;

2) informacije o preduzetim merama;

3) razloge za proglašenje krize informacione bezbednosti;

4) zaduženje organa za postupanje u skladu sa svojim nadležnostima;

5) mere za rešavanje krize.

Predlog za proglašenje krize informacione bezbednosti upućuje se Ministarstvu, koje po prijemu predloga bez odlaganja saziva sednicu Tela za koordinaciju poslova informacione bezbednosti.

Vlada na predlog Ministarstva donosi odluku o proglašenju krize informacione bezbednosti i zadužuje organe da postupaju prema predloženim merama u skladu sa svojim nadležnostima.

Kancelarija za informacionu bezbednost, u saradnji sa operativnim timom, koordinira rešavanjem krize informacione bezbednosti i najmanje jednom nedeljno izveštava Ministarstvo i Vladu o svim aktivnostima.

Predlog za proglašenje završetka krize informacione bezbednosti upućuje se Ministarstvu.

Odluku o proglašenju završetka krize informacione bezbednosti donosi Vlada na predlog Ministarstva.

Nakon završetka krize informacione bezbednosti Kancelarija za informacionu bezbednost sačinjava završni izveštaj koji dostavlja Ministarstvu i Vladi u roku od 30 dana nakon završetka krize.

Izveštavanje tokom i nakon incidenta

Član 24

Operatori IKT sistema od posebnog značaja dužni su da:

1) dostavljaju izveštaj o incidentu, tokom trajanja incidenta, sa opisom mera koje su preduzete za rešavanje incidenta, u jedinstveni sistem za prijem obaveštenja o incidentima i to:

(1) na svaka tri dana u slučaju incidenta srednjeg nivoa;

(2) na svaka 24 sata u slučaju incidenata visokog i veoma visokog nivoa;

2) dostavljaju obaveštenja i dodatne izveštaje o bitnim događajima u vezi sa incidentom i aktivnostima koje preduzimaju, na zahtev Kancelarije;

3) dostavljaju završni izveštaj o incidentu u roku od 15 dana od dana prestanka incidenta, koji sadrži sledeće podatke:

(1) vrstu i detaljan opis incidenta;

(2) vrstu pretnje i uzrok koji je doveo do incidenta;

(3) vreme i trajanje incidenta;

(4) obim i stepen uticaja incidenta (ostvareni rizik), odnosno posledice koje je incident izazvao;

(5) informaciju o eventualnom prekograničnom dejstvu incidenta;

(6) preduzete aktivnosti radi otklanjanja posledica incidenta i, po potrebi, druge informacije od značaja za evidentiranje incidenta i statističku obradu.

Nakon završenog incidenta Kancelarija za informacionu bezbednost priprema preporuke i savete za zaštitu od potencijalnih rizika, na osnovu sprovedene analize izvršenog incidenta.

Dostavljanje statističkih podataka o incidentima

Član 25

Operator IKT sistema od posebnog značaja dužan je da, pored obaveštavanja o incidentima iz člana 13. ovog zakona, dostavi organu, odnosno organizaciji nadležnoj za poslove Nacionalnog CERT-a statističke podatke o svim incidentima u IKT sistemu, uključujući i izbegnute incidente, u prethodnoj godini najkasnije do 28. februara tekuće godine.

Organ, odnosno organizacija iz stava 1. ovog člana izveštaje o statističkim podacima dostavlja Ministarstvu i objavljuje na svojoj veb prezentaciji.

Vrstu, formu i način dostavljanja statističkih podataka iz stava 1. ovog člana utvrđuje organ, odnosno organizacija iz stava 1. ovog člana.

III ORGANI NADLEŽNI ZA PREVENCIJU I ZAŠTITU OD BEZBEDNOSNIH RIZIKA U IKT SISTEMIMA U REPUBLICI SRBIJI

Nadležni organ

Član 26

Organ državne uprave nadležan za informacionu bezbednost je ministarstvo nadležno za poslove informacione bezbednosti.

U okviru svojih nadležnosti Ministarstvo:

1) priprema i predlaže propise i planska dokumenta iz oblasti informacione bezbednosti u skladu sa ovim zakonom;

2) vodi evidenciju operatora IKT sistema od posebnog značaja;

3) vrši nadzor nad radom Kancelarije za informacionu bezbednost u vršenju poslova za koje je nadležna u skladu sa ovim zakonom;

4) 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;

5) ostvaruje međunarodnu saradnju u okviru svojih nadležnosti.

Telo za koordinaciju poslova informacione bezbednosti

Član 27

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, poslove pravosuđa, predstavnici službi bezbednosti, Kancelarije za informacionu bezbednost, Kancelarije za informacione tehnologije i elektronsku upravu, Kancelarije Saveta za nacionalnu bezbednost i zaštitu tajnih podataka, Generalnog sekretarijata Vlade, Narodne banke Srbije i Regulatornog tela za elektronske komunikacije i poštanske usluge.

U funkciji unapređenja pojedinih oblasti informacione bezbednosti formiraju se stručne radne grupe Tela za koordinaciju u koje se uključuju i predstavnici drugih organa, 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.

Kancelarija za informacionu bezbednost

Član 28

Radi obavljanja poslova prevencije i zaštite od bezbednosnih rizika i incidenata u IKT sistemima u Republici Srbiji osniva se Kancelarija za informacionu bezbednost (u daljem tekstu: Kancelarija), kao posebna organizacija u smislu zakona kojim se uređuje položaj državne uprave.

Kancelarija ima svojstvo pravnog lica.

Radom Kancelarije rukovodi direktor koji mora da bude lice odgovarajuće stručnosti sa najmanje pet godina radnog iskustva u oblasti informacione bezbednosti i koga imenuje Vlada, u skladu sa zakonom kojim se uređuje položaj državnih službenika.

Kancelarija ima zamenika direktora, koji mora biti lice odgovarajuće stručnosti sa najmanje pet godina radnog iskustva u oblasti informacione bezbednosti, koji se postavlja u skladu sa propisima kojim se uređuje položaj državnih službenika i ima ovlašćenja u skladu sa propisima o državnoj upravi.

Nadzor nad radom Kancelarije

Član 29

Nadzor nad radom Kancelarije u vršenju poslova sprovodi Ministarstvo, u skladu sa zakonom kojim se uređuje državna uprava.

Nadležnosti Kancelarije

Član 30

Kancelarija u okviru svoje nadležnosti obavlja sledeće poslove, i to:

1) vrši prevenciju i zaštitu od bezbednosnih rizika na nacionalnom nivou u skladu sa ovim zakonom (poslovi Nacionalnog CERT-a);

2) preduzima preventivne i reaktivne mere u cilju zaštite Jedinstvene informaciono-komunikacione mreže elektronske uprave u skladu sa ovim zakonom (poslovi CERT-a organa vlasti);

3) obavlja saradnju na nacionalnom nivou u oblasti informacione bezbednosti;

4) vrši poslove jedinstvene tačke kontakta;

5) vrši poslove sertifikacije IKT sistema, IKT proizvoda, IKT procesa i IKT usluga, izuzev sistema, proizvoda, procesa i usluga za potrebe odbrane i bezbednosti i IKT sistema za rad sa tajnim podacima;

6) propisuje minimalne mere zaštite IKT sistema organa, uvažavajući načela iz člana 3. ovog zakona, mere zaštite iz člana 10. ovog zakona, nacionalne i međunarodne standarde i standarde koji se primenjuju u odgovarajućim oblastima rada;

7) u saradnji sa nadležnim organima i drugim subjektima iz javnog, akademskog, privrednog i nevladinog sektora učestvuje u razvoju i sprovođenju programa obuka i stručnog usavršavanja lica koja rade na poslovima informacione bezbednosti;

8) obavlja saradnju i razmenu informacija na međunarodnom nivou u oblasti informacione bezbednosti u cilju praćenja i usaglašavanja sa međunarodnim propisima i standardima;

9) vrši stručni nadzor nad radom operatora IKT sistema od posebnog značaja;

10) vodi bazu ranjivosti IKT proizvoda i IKT usluga;

11) izveštava Ministarstvo na kvartalnom nivou o preduzetim aktivnostima;

12) obavlja druge poslove u skladu sa ovim zakonom.

Podzakonski akt kojim se bliže uređuje način vršenja sertifikacije IKT sistema, IKT proizvoda, IKT procesa i IKT usluga iz stava 1. tačka 5) ovog člana donosi Vlada, na predlog Ministarstva.

Poslovi prevencije i zaštite od bezbednosnih rizika na nacionalnom nivou (Nacionalni CERT)

Član 31

U okviru poslova prevencije i zaštite od bezbednosnih rizika i incidenata Kancelarija vrši poslove Nacionalnog CERT-a, i to:

1) prikuplja i razmenjuje informacije o pretnjama, ranjivostima, izbegnutim incidentima i incidentima i pruža podršku, upozorava i savetuje lica koja upravljaju IKT sistemima u Republici Srbiji, kao i javnost;

2) prati stanje o incidentima u Republici Srbiji;

3) pruža rana upozorenja, uzbune i najave i informiše relevantna lica o pretnjama, ranjivostima i incidentima;

4) reaguje bez odlaganja 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;

5) na zahtev operatora IKT sistema od posebnog značaja, pruža pomoć u praćenju stanja bezbednosti IKT sistema u realnom vremenu ili približno realnom vremenu;

6) na zahtev operatora IKT sistema od posebnog značaja, vrši proaktivno skeniranje IKT sistema u cilju utvrđivanja ranjivosti koje mogu da potencijalno znatno naruše bezbednost IKT sistema, pri čemu takvo skeniranje ne sme imati štetan uticaj na poslove i delatnosti operatora;

7) postupa kao koordinator za potrebe koordiniranog otkrivanja ranjivosti, u skladu sa ovim zakonom;

8) učestvuje u razvoju i korišćenju tehnoloških alata za razmenu informacija sa operatorima IKT sistema od posebnog značaja i drugih subjekata sa kojima sarađuje;

9) kontinuirano izrađuje analize rizika i incidenata, na osnovu prikupljenih informacija;

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

11) vodi Evidenciju posebnih CERT-ova;

12) priprema izveštaje na kvartalnom nivou o preduzetim aktivnostima;

13) pruža podršku u prikupljanju i analiziranju forenzičkih podataka i pruža dinamičke analize rizika i incidenata u skladu sa propisima;

14) sarađuje sa CERT-ovima stranih država i na njihov zahtev pruža uzajamnu pomoć u skladu sa svojim kapacitetima i nadležnostima.

Kancelarija podstiče primenu i korišćenje propisanih i standardizovanih procedura za:

1) upravljanje incidentima;

2) klasifikaciju informacija o incidentima, odnosno klasifikaciju prema nivou opasnosti incidenata;

3) upravljanje kriznim situacijama;

4) koordinirano otkrivanje ranjivosti.

Kancelarija je ovlašćena da vrši obradu podataka o licu koje prijavi incident, pri čemu obrada podataka o licu 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.

Kancelarija obezbeđuje neprekidnu dostupnost svojih usluga putem različitih sredstava komunikacije.

U okviru obavljanja poslova Nacionalnog CERT-a potrebno je obezbediti sledeće zahteve:

1) visok nivo dostupnosti komunikacionih kanala izbegavanjem jedinstvenih tačaka prekida i korišćenje više sredstava za dvosmerno kontaktiranje;

2) prostorije Nacionalnog CERT-a i informacioni sistemi za podršku treba da budu smešteni na sigurnim lokacijama;

3) upotrebu odgovarajućeg sistema za upravljanje zahtevima i njihovo usmeravanje, posebno kako bi se olakšala efikasna i efektivna razmena informacija;

4) obezbeđivanje poverljivosti i pouzdanosti svojih aktivnosti;

5) postojanje adekvatnih kadrovskih kapaciteta;

6) opremljenost redundantnim sistemima i rezervnim radnim prostorom kako bi se osigurao kontinuitet usluga.

Podzakonski akt kojim se bliže uređuje postupak proaktivnog skeniranja IKT sistema iz stava 1. tačka 6) ovog člana, zaštitni, tehnički i bezbednosni uslovi i mere koje mora da ispuni subjekat koji neposredno vrši skeniranje, kao i procedura kojom se utvrđuju uslovi u cilju zaštite bezbednosti sistema, mreža i podataka kojima se pristupa i način izveštavanja nadležnog organa, donosi Vlada na predlog Ministarstva.

Preventivne i reaktivne mere u cilju zaštite Jedinstvene informaciono-komunikacione mreže elektronske uprave (CERT organa vlasti)

Član 32

U okviru preduzimanja preventivnih i reaktivnih mera u cilju zaštite Jedinstvene informaciono-komunikacione mreže elektronske uprave (u daljem tekstu: mreža eUprave) Kancelarija obavlja sledeće poslove:

1) vrši zaštitu mreže eUprave;

2) obavlja koordinaciju i saradnju sa operatorima IKT sistema koje povezuje mreža eUprave u prevenciji incidenata;

3) aktivno učestvuje u otkrivanju incidenata, prikupljanju informacija o incidentima i otklanjanju posledica incidenata;

4) vrši proaktivno skeniranje mreže operatora IKT sistema od posebnog značaja koji su korisnici mreže, pri čemu takvo skeniranje ne sme imati štetan uticaj na poslove i delatnosti operatora;

5) u slučaju otkrivene ranjivosti:

(1) obaveštava operatore IKT sistema koji su korisnici mreže eUprave o tome;

(2) nalaže operatorima IKT sistema od posebnog značaja koji su korisnici mreže da preduzmu adekvatne mere zaštite u cilju sprečavanja, smanjenja i otklanjanja posledica incidenta;

6) izdaje stručne preporuke za zaštitu IKT sistema organa, osim IKT sistema za rad sa tajnim podacima;

7) donosi akt kojim se uređuje postupanje operatora IKT sistema od posebnog značaja koji koriste mreže u slučaju incidenta;

8) u saradnji sa nadležnim organima vrši procenu potrebe za stručnim usavršavanjem zaposlenih u operatorima IKT sistema od posebnog značaja koji koriste mrežu;

9) planira i organizuje proceduralne i praktične vežbe u oblasti informacione bezbednosti za zaposlene u operatorima IKT sistema od posebnog značaja koji koriste mrežu;

10) izrađuje predloge za unapređenje bezbednosnih karakteristika mreže eUprave;

11) izrađuje analize rizika i incidenata u okviru mreže eUprave;

12) obavlja druge poslove u skladu sa zakonom u cilju unapređenja informacione bezbednosti mreže eUprave.

Podzakonski akt kojim se bliže uređuje postupak proaktivnog skeniranja IKT sistema iz stava 1. tačka 4) ovog člana, zaštitni, tehnički i bezbednosni uslovi i mere koje mora da ispuni subjekat koji neposredno vrši skeniranje, kao i procedura kojom se utvrđuju uslovi u cilju zaštite

bezbednosti sistema, mreža i podataka kojima se pristupa i način izveštavanja nadležnog organa, donosi Vlada na predlog Ministarstva.

Saradnja na nacionalnom nivou

Član 33

Kancelarija neposredno sarađuje sa Ministarstvom, Regulatornim telom za elektronske komunikacije i poštanske usluge, Posebnim CERT-ovima u Republici Srbiji, sa javnim i privrednim subjektima i CERT-ovima samostalnih operatora IKT sistema.

CERT-ovi mogu, u skladu sa svojim nadležnostima i bezbednosnim protokolima, samostalno uspostavljati saradnju sa relevantnim akterima iz javnog i privatnog sektora, uz obavezu obaveštavanja Kancelarije radi koordinacije i razmene informacija od značaja za nacionalni sistem informacione bezbednosti.

Kancelarija i CERT-ovi samostalnih operatora IKT sistema održavaju međusobne sastanke u organizaciji Kancelarije najmanje tri puta godišnje, kao i po potrebi u slučaju incidenata koji značajno ugrožavaju informacionu bezbednost u Republici Srbiji.

Sastancima iz stava 3. ovog člana prisustvuju i predstavnici Ministarstva, a po pozivu mogu da prisustvuju i predstavnici posebnih CERT-ova, kao i druga lica.

Prilikom saradnje sa subjektima iz stava 1. ovog člana Kancelarija je dužna da obezbedi efektivnu, efikasnu i bezbednu razmenu informacija uz primenu adekvatnih procedura, uključujući "traffic light protocol" (TLP), i poštujući propise o zaštiti podataka o ličnosti.

Međunarodna saradnja i poslovi jedinstvene tačke kontakta

Član 34

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

1) brzo rastu ili imaju tendenciju da postanu visokorizični;

2) prevazilaze ili mogu da prevaziđu nacionalne kapacitete;

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

Prilikom razmene podataka iz stava 1. ovog člana, Kancelarija je dužna da postupa tako da se ne ugrozi poverljivost podataka, kao i da takva razmena podataka ne utiče na potencijalno narušavanje bezbednosti IKT sistema.

Razmena podataka iz stava 1. ovog člana podrazumeva prenos ili obradu podataka koji su neophodni za procenu i reagovanje na bezbednosne rizike i incidente u skladu sa ovim zakonom. U slučaju da se razmena odnosi na podatke o ličnosti, Kancelarija je dužna da obezbedi da takav prenos ili obrada budu usklađeni sa propisima kojima se uređuje zaštita podataka o ličnosti, uključujući i pravila koja se odnose na prenos podataka u druge države ili međunarodne organizacije.

Ukoliko je incident u vezi sa izvršenjem krivičnog dela koje se goni po službenoj dužnosti, Kancelarija će o tome obavestiti nadležno javno tužilaštvo, koje će samostalno ili preko ministarstva nadležnog za unutrašnje poslove u zvaničnoj proceduri proslediti prijavu u skladu sa potvrđenim međunarodnim ugovorima.

Kancelarija obavlja poslove jedinstvene tačke kontakta za informacionu bezbednost u slučaju prekograničnih bezbednosnih pretnji i incidenata i sarađuje sa jedinstvenim tačkama kontakta drugih država.

Posebni centri za prevenciju bezbednosnih rizika u IKT sistemima

Član 35

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 sa sedištem na teritoriji Republike Srbije, koje je upisano u evidenciju posebnih CERT-ova koju vodi organ, odnosno organizacija nadležna za poslove Nacionalnog CERT-a i objavljuje je javno.

Upis u evidenciju posebnih CERT-ova, koju vodi Kancelarija, 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, a u svrhu angažovanja posebnih CERT-ova u slučaju bezbednosnih rizika i incidenata u IKT sistemima.

Organ, odnosno organizacija iz stava 2. ovog člana propisuje sadržaj, način upisa i vođenja evidencije iz stava 3. ovog člana.

Baza ranjivosti

Član 36

Organ, odnosno organizacija nadležna za poslove Nacionalnog CERT-a uspostavlja i održava bazu ranjivosti IKT proizvoda i IKT usluga u Republici Srbiji i omogućava fizičkim i pravnim licima, kao i proizvođačima, dobavljačima i pružaocima usluge u IKT sistemu, da na dobrovoljnoj bazi prijave ranjivosti u IKT proizvodima ili IKT uslugama, a koje se mogu prijaviti anonimno.

Baza ranjivosti IKT proizvoda i IKT usluga sadrži:

1) podatke o ranjivosti;

2) podatke o ranjivostima IKT proizvoda ili IKT usluga.

Vlada, na predlog Ministarstva, propisuje sadržaj, procedure verifikacije ranjivosti, procedure za upravljanje tehničkim ranjivostima IKT proizvoda i IKT usluga, način upisa i vođenja registra.

Baza podataka o registraciji domena

Član 37

Organizacija koja je ovlašćena za upravljanje registrom domena najvišeg nivoa vodi spisak ovlašćenih registara za registraciju domena u Republici Srbiji.

Spisak iz stava 1. ovog člana obavezno sadrži sledeće podatke:

1) naziv ovlašćenog registra;

2) sedište i ažurne kontakt podatke ovlašćenog registra (adresu elektronske pošte, službeni telefon);

3) adresni opseg internet protokola (engl. "IP address range") koji pripada ovlašćenom registru, a koji obuhvata podatke o javnim statičkim IP adresama.

Ovlašćeni registar dužan je da u slučaju promene podataka iz stava 2. ovog člana o tome obavesti organizaciju koja je ovlašćena za upravljanje registrom domena najvišeg nivoa u roku od 15 dana od dana nastanka promene.

Organizacije koje su ovlašćene za upravljanje registrom domena najvišeg nivoa i pružanje usluga DNS-a obavezne su da prikupljaju, čuvaju i održavaju tačne i potpune podatke o registraciji domena u posebnoj bazi podataka, uz dužnu pažnju i uz primenu tehničkih,

organizacionih i bezbednosnih mera za zaštitu podataka, u skladu sa propisima o zaštiti podataka o ličnosti.

Baza podataka iz stava 4. ovog člana mora da sadrži najmanje sledeće podatke:

1) naziv domena;

2) datum registracije domena;

3) podatke o registrantu, i to: ime i prezime fizičkog lica, odnosno naziv pravnog lica, kontakt adresu elektronske pošte i broj telefona;

4) kontakt adresu elektronske pošte i broj telefona lica zaduženog za administraciju domena, ukoliko se razlikuju od podataka registranta.

Organizacije iz stava 4. ovog člana dužne su da usvoje i primene akte i procedure za verifikaciju tačnosti i potpunosti podataka u bazi podataka. Ove procedure moraju biti javno dostupne.

Organizacije iz stava 4. ovog člana dužne su da obezbede javnu dostupnost podataka koji ne predstavljaju podatke o ličnosti odmah po registraciji domena, a u skladu sa pravilima i uslovima registracije naziva nacionalnih internet domena.

Organizacije iz stava 4. ovog člana obavezne su da omoguće pristup podacima o registraciji domena koji nisu javno dostupni na osnovu zakonitih i obrazloženih zahteva ovlašćenih lica ili organa, u skladu sa ovlašćenjima dodeljenim propisima koji uređuju delokrug njihovog rada i u skladu sa propisima koji uređuju zaštitu podataka o ličnosti.

Odgovor na zahtev iz stava 7. ovog člana mora biti dostavljen bez odlaganja, a najkasnije u roku od 72 sata od prijema zahteva.

Organizacije iz stava 4. ovog člana dužne su da donesu i javno objave politike i procedure za postupanje po zahtevima za otkrivanje podataka o registraciji domena, u skladu sa ovim zakonom i propisima o zaštiti podataka o ličnosti. U skladu sa ovim članom, prikupljanje podataka o registraciji domena ne sme dovesti do dupliranja podataka. Organizacije iz stava 4. ovog člana dužne su da sarađuju radi izbegavanja dupliranja i osiguranja usklađenosti sa zakonom.

Ministar nadležan za informacionu bezbednost propisuje bliže uslove za prikupljanje, čuvanje, verifikaciju i objavljivanje podataka iz ovog člana, a u skladu sa najboljom praksom registara nacionalnih internet domena iz Evropske Unije, kao i Internet korporacije za dodeljene nazive i brojeve (ICANN).

Zaštita dece pri korišćenju informaciono-komunikacionih tehnologija

Član 38

Ministarstvo 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 radi postupanja u skladu sa utvrđenim nadležnostima.

Ministarstvo je ovlašćeno da vrši obradu podataka o licu koje se obrati Ministarstvu 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.

Podzakonski akt kojim se bliže uređuje način sprovođenja mera za bezbednost i zaštitu dece na internetu iz st. 1. i 3. ovog člana donosi Vlada na predlog Ministarstva.

IV KRIPTOBEZBEDNOST I ZAŠTITA OD KOMPROMITUJUĆEG ELEKTROMAGNETNOG ZRAČENJA

Nadležnost

Član 39

Ministarstvo nadležno za poslove odbrane je nadležno za poslove informacione bezbednosti koji se odnose na odobravanje kriptografskih proizvoda koji se koriste za zaštitu prenosa i čuvanja podataka koji su određeni kao tajni, 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 40

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

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

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

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

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

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

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

7) vrši funkciju nacionalnog organa za zaštitu od KEMZ;

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

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

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

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

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

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

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

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

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

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

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

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

Kompromitujuće elektromagnetno zračenje

Član 41

Mere zaštite od KEMZ u IKT sistemima za rukovanje sa tajnim podacima 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.

Podzakonski akt kojim se bliže uređuju uslovi za proveru KEMZ i način procene rizika od oticanja podataka putem KEMZ donosi Vlada, na predlog ministarstva nadležnog za poslove odbrane.

Mere kriptozaštite

Član 42

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.

Podzakonski akt kojim se uređuju tehnički uslovi 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 donosi Vlada, na predlog ministarstva nadležnog za poslove odbrane.

Odobrenje za kriptografski proizvod

Član 43

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.

Podzakonski akt kojim se bliže uređuju uslovi koje moraju da ispunjavaju kriptografski proizvodi iz stava 1. ovog člana donosi Vlada, na predlog ministarstva nadležnog za poslove odbrane.

Izdavanje odobrenja za kriptografski proizvod

Član 44

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 45 dana od dana podnošenja urednog zahteva, koji se može produžiti u slučaju posebne složenosti provere najviše za još 60 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. 2. i 3. ovog člana iz razloga novih saznanja vezanih za tehnička rešenja primenjena u proizvodu, a koja utiču na ocenu stepena zaštite koji pruža proizvod.

Podzakonski akt kojim se bliže uređuje sadržaj zahteva za izdavanje odobrenja za kriptografski proizvod, uslove za izdavanje odobrenja za kriptografski proizvod, način izdavanja odobrenja i vođenja registra izdatih odobrenja za kriptografski proizvod donosi Vlada, na predlog ministarstva nadležnog za poslove odbrane.

Opšte odobrenje za korišćenje kriptografskih proizvoda

Član 45

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 46

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.

Podzakonski akt kojim se bliže uređuje vođenje registara iz stava 1. ovog člana donosi Vlada, na predlog ministarstva nadležnog za poslove odbrane.

V NADLEŽNOSTI I ODGOVORNOSTI SUBJEKATA ZA NADZOR NAD SPROVOĐENJEM OVOG ZAKONA

Inspekcija za informacionu bezbednost

Član 47

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 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 48

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

1) naloži otklanjanje utvrđenih nepravilnosti i za to utvrdi razuman rok;

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

3) zahteva od operatora IKT sistema od posebnog značaja da izvrši skeniranje, konfiguraciju i penetraciono testiranje IKT sistema u cilju utvrđivanja eventualnih bezbednosnih ranjivosti, a u skladu sa procenom rizika;

4) naloži da nadzirani subjekt učini dostupnim javnosti informacije koje se tiču nepoštovanja odredbi ovog zakona, a za koje postoji opravdan interes javnosti na utvrđeni način;

5) naloži da nadzirani subjekt odredi lice sa tačno utvrđenim ovlašćenjima koje će u utvrđenom vremenskom periodu nadzirati i pratiti usaglašenost sa odredbama ovog zakona i naloženim merama;

6) predloži nadležnom organu, telu za ocenjivanje usaglašenosti ili drugom nadležnom telu da privremeno suspenduje ili povuče izdat sertifikat, dozvolu ili drugi akt kojim se potvrđuje ispunjenost uslova, ukoliko nadzirani subjekt ne otkloni nepravilnosti u ostavljenom roku;

7) pokrene postupak pred nadležnim sudom ili drugim nadležnim organom radi utvrđivanja privremene mere zabrane obavljanja upravljačkih funkcija licu koje u ime nadziranog subjekta vrši rukovodeće poslove, ako je njegovim postupanjem onemogućeno usaglašavanje sa ovim zakonom i naloženim merama.

Podzakonski akt kojim se bliže uređuje postupak skeniranja, konfiguracija i penetraciono testiranje IKT sistema u cilju utvrđivanja eventualnih bezbednosnih ranjivosti iz stava 1. tačka 3) ovog člana, zaštitni, tehnički i bezbednosni uslovi i mere koje mora da ispuni subjekat koji neposredno vrši aktivnosti iz stava 1. tačka 3) ovog člana, kao i procedura kojom se utvrđuju uslovi u cilju zaštite bezbednosti sistema, mreža i podataka kojima se pristupa i način izveštavanja nadležnog organa, donosi Vlada na predlog Ministarstva.

Stručni nadzor

Član 49

Stručni 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, vrši Kancelarija, a u skladu sa zakonom kojim se uređuje inspekcijski nadzor.

Poslove stručnog nadzora obavlja ovlašćeno lice zaposleno u Kancelariji (u daljem tekstu: ovlašćeno lice).

U postupku stručnog nadzora ovlašćeno lice ima pravo i obavezu da kontroliše:

1) adekvatnost procenjenih rizika s obzirom na stepen izloženosti riziku, veličinu operatora i izvesnost pojave incidenta i njegove ozbiljnosti, kao i njegov potencijalni društveni i ekonomski uticaj;

2) nivo bezbednosti tehnoloških postupaka i tehničkih sredstava koje operator IKT sistema od posebnog značaja upotrebljava radi primena mera zaštite;

3) odgovarajuće sprovođenje procesa provere usklađenosti primenjenih mera IKT sistema sa aktom o bezbednosti;

4) primenu preporuka i mera u slučaju incidenata koji značajno ugrožavaju informacionu bezbednost.

Ako u vršenju stručnog nadzora Kancelarija utvrdi nepravilnosti, nedostatke ili propuste u primeni ovog zakona i propisa donetih na osnovu njega, o tome obaveštava nadziranog subjekta i određuje mu rok u kome je dužan da ih otkloni.

Rok iz stava 4. ovog člana ne može biti kraći od osam dana od dana prijema obaveštenja, osim u slučajevima koji zahtevaju hitno postupanje.

Ako Kancelarija utvrdi da nadzirani subjekat nije, u ostavljenom roku, otklonio utvrđene nepravilnosti, nedostatke ili propuste u primeni ovog zakona i propisa donetih na osnovu njega, podnosi prijavu inspekciji.

Kancelarija je dužna da po zahtevu inspektora za informacionu bezbednost obavi stručni nadzor i dostavi informaciju o utvrđenom činjeničnom stanju.

Obrazac legitimacije i način izdavanja legitimacije ovlašćenog lica utvrđuje Kancelarija.

Legitimacija ovlašćenog lica obavezno sadrži: grb Republike Srbije i naziv Kancelarije, ime i prezime ovlašćenog lica, fotografiju ovlašćenog lica, službeni broj legitimacije, datum izdavanja legitimacije, pečat Kancelarije, potpis direktora Kancelarije, kao i odštampani tekst sledeće sadržine: "Imalac ove legitimacije ima ovlašćenja u skladu sa odredbama člana 49. st. 3. i 4. Zakona o informacionoj bezbednosti."

VI KAZNENE ODREDBE

Član 50

Novčanom kaznom u iznosu od 50.000,00 do 2.000.000,00 dinara kazniće se za prekršaj pravno lice koje je operator prioritetnog IKT sistema ako:

1) ne postupi u skladu sa odredbama o upisu u evidenciju iz člana 9. ovog zakona;

2) ne donese Akt o proceni rizika iz člana 11. stav 1. ovog zakona;

3) ne donese Akt o bezbednosti IKT sistema iz člana 12. stav 1. ovog zakona;

4) ne primeni mere zaštite određene Aktom o bezbednosti IKT sistema iz člana 12. stav 2. ovog zakona;

5) ne izvrši proveru usklađenosti primenjenih mera iz člana 12. stav 5. ovog zakona;

6) ne dostavi statističke podatke iz člana 25. stav 1. ovog zakona;

7) ne postupi po nalogu inspektora za informacionu bezbednost u ostavljenom roku iz člana 48. stav 1. tačka 1) ovog zakona.

Za prekršaj iz stava 1. ovog člana kazniće se fizičko lice u svojstvu registrovanog subjekta koje je operator prioritetnog IKT sistema novčanom kaznom u iznosu od 10.000,00 do 500.000,00 dinara.

Za prekršaj iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu ili organu koji je operator prioritetnog IKT sistema novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara.

Član 51

Novčanom kaznom u iznosu od 50.000,00 do 1.000.000,00 dinara kazniće se za prekršaj pravno lice koje je operator važnog IKT sistema ako:

1) ne postupi u skladu sa odredbama o upisu u evidenciju iz člana 9. ovog zakona;

2) ne donese Akt o proceni rizika iz člana 11. stav 1. ovog zakona;

3) ne donese Akt o bezbednosti IKT sistema iz člana 12. stav 1. ovog zakona;

4) ne primeni mere zaštite određene Aktom o bezbednosti IKT sistema iz člana 12. stav 2. ovog zakona;

5) ne izvrši proveru usklađenosti primenjenih mera iz člana 12. stav 5. ovog zakona;

6) ne dostavi statističke podatke iz člana 25. stav 1. ovog zakona;

7) ne postupi po nalogu inspektora za informacionu bezbednost u ostavljenom roku iz člana 48. stav 1. tačka 1) ovog zakona.

Za prekršaj iz stava 1. ovog člana kazniće se fizičko lice u svojstvu registrovanog subjekta koje je operator važnog IKT sistema novčanom kaznom u iznosu od 10.000,00 do 250.000,00 dinara.

Za prekršaj iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu ili organu koji je operator važnog IKT sistema novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara.

Član 52

Novčanom kaznom u iznosu od 50.000,00 do 500.000,00 dinara kazniće se za prekršaj pravno lice koje je operator prioritetnog IKT sistema ako:

1) o incidentima u IKT sistemu iz člana 13. stav 2. ovog zakona ne obavesti organe iz člana 14. st. 1. do 3. ovog zakona;

2) ne obavesti korisnike kojima pružaju usluge u slučaju incidenta koji može da izazove ili izaziva štetan uticaj na pružanje i korišćenje usluga u skladu sa članom 14. stav 5. ovog zakona;

3) ne dostavlja obaveštenja i izveštaje tokom i nakon završetka incidenta iz člana 24. ovog zakona.

Za prekršaj iz stava 1. ovog člana kazniće se fizičko lice u svojstvu registrovanog subjekta koje je operator prioritetnog IKT sistema novčanom kaznom u iznosu od 10.000,00 do 500.000,00 dinara.

Za prekršaje iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu ili organu koji je operator prioritetnog IKT sistema novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara.

Izuzetno od st. 1-3. ovog člana, ako operator prioritetnih IKT sistema od posebnog značaja iz člana 14. stav 2. ovog zakona ne obavesti Narodnu banku Srbije o incidentima u IKT sistemu od posebnog značaja ili ne obavesti korisnike o incidentima u skladu sa članom 14. stav 6. ovog zakona, Narodna banka Srbije izriče tom subjektu mere i kazne u skladu sa zakonom kojim se uređuje njegovo poslovanje.

Član 53

Novčanom kaznom u iznosu od 50.000,00 do 500.000,00 dinara kazniće se za prekršaj pravno lice koje je operator važnog IKT sistema ako:

1) o incidentima u IKT sistemu iz člana 13. stav 2. ovog zakona ne obavesti organe iz člana 14. st. 1. do 3. ovog zakona;

2) ne obavesti korisnike kojima pružaju usluge u slučaju incidenta koji može da izazove ili izaziva štetan uticaj na pružanje i korišćenje usluga u skladu sa članom 14. stav 5. ovog zakona;

3) ne dostavlja obaveštenja i izveštaje tokom i nakon završetka incidenta iz člana 24. ovog zakona.

Za prekršaj iz stava 1. ovog člana kazniće se fizičko lice u svojstvu registrovanog subjekta koje je operator prioritetnog IKT sistema novčanom kaznom u iznosu od 10.000,00 do 250.000,00 dinara.

Za prekršaje iz stava 1. ovog člana kazniće se i odgovorno lice u pravnom licu ili organu koje je operator važnog IKT sistema novčanom kaznom u iznosu od 5.000,00 do 50.000,00 dinara.

VII PRELAZNE I ZAVRŠNE ODREDBE

Rokovi za donošenje podzakonskih akata

Član 54

Podzakonska akta predviđena ovim zakonom doneće se u roku od 12 meseci od dana stupanja na snagu ovog zakona.

Plan za reagovanje u slučaju incidenta visokog nivoa i krize informacione bezbednosti iz člana 18. ovog zakona donosi se u roku od 18 meseci od dana stupanja na snagu ovog zakona.

Član 55

Operatori IKT sistema od posebnog značaja koji su određeni Zakonom o informacionoj bezbednosti ("Službeni glasnik RS", br. 6/16, 94/17 i 77/19) nastavljaju da postupaju u skladu sa obavezama utvrđenim čl. 6a-11b tog zakona do 31. decembra 2025. godine.

Na operatore IKT sistema od posebnog značaja koji su određeni Zakonom o informacionoj bezbednosti ("Službeni glasnik RS", br. 6/16, 94/17 i 77/19) do datuma iz stava 1. ovog člana primenjuju se kaznene odredbe iz čl. 30. i 31. tog zakona.

Operatori IKT sistema od posebnog značaja dužni su da donesu akt iz člana 11. stav 1. ovog zakona u roku od 18 meseci od dana stupanja na snagu ovog zakona.

Organ, odnosno organizacija u kojoj se obavljaju poslovi Nacionalnog CERT-a dužna je da, u roku od devet meseci od dana stupanja na snagu ovog zakona, donese opštu metodologiju za procenu rizika u IKT sistemima od posebnog značaja iz člana 11. stav 4. ovog zakona.

Operator IKT sistema od posebnog značaja dužan je da donese akt iz člana 12. ovog zakona u roku od 18 meseci od dana stupanja na snagu ovog zakona.

Član 56

Kancelarija za informacionu bezbednost se uspostavlja i počinje da obavlja poslove iz svoje nadležnosti propisane ovim zakonom od 1. januara 2027. godine.

Poslove Kancelarije za informacionu bezbednost propisane ovim zakonom, izuzev poslova Nacionalnog CERT-a, obavljaće Kancelarija za informacione tehnologije i elektronsku upravu u periodu koji počinje danom nastupanja šest meseci od dana stupanja na snagu ovog zakona i koji traje do 1. januara 2027. godine.

Regulatorno telo za elektronske komunikacije i poštanske usluge obavlja poslove Nacionalnog CERT-a utvrđene ovim zakonom do uspostavljanja Kancelarije za informacionu bezbednost odnosno do 1. januara 2027. godine.

Kancelarija za informacionu bezbednost preuzima prava, obaveze, zaposlene, predmete, opremu, sredstva za rad i arhivu od Regulatornog tela za elektronske komunikacije i poštanske usluge nastalu u obavljanju poslova Nacionalnog CERT-a potrebne za vršenje stručnih poslova utvrđenih ovim zakonom.

Kancelarija za informacionu bezbednost počev od datuma iz stava 1. ovog člana preuzima prava, obaveze, zaposlene, predmete, opremu, sredstva za rad i arhivu od Kancelarije za informacione tehnologije i elektronsku upravu nastalu u obavljanju poslova propisanih ovim zakonom iz nadležnosti Kancelarije za informacionu bezbednost.

Prestanak važenja Zakona o informacionoj bezbednosti

Član 57

Danom stupanja na snagu ovog zakona prestaje da važi Zakon o informacionoj bezbednosti ("Službeni glasnik RS", br. 6/16, 94/17 i 77/19), izuzev odredbi čl. 6a-11b i čl. 30. i 31. koje važe do 31. decembra 2025. godine.

Podzakonski akti doneti na osnovu Zakona o informacionoj bezbednosti ("Službeni glasnik RS", br. 6/16, 94/17 i 77/19) primenjivaće se do stupanja na snagu podzakonskih akata koji se donose u skladu sa ovim zakonom.

Stupanje na snagu

Član 58

Ovaj zakon stupa na snagu osmog dana od dana objavljivanja u "Službenom glasniku Republike Srbije", izuzev člana 29. ovog zakona koji počinje da se primenjuje od 1. januara 2027. godine.